deviceTRUST 23.1

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Welcome 21
- Quick setup 21
- More information 21

Architecture 22
- Local Scenario 22
  - deviceTRUST® Agent 22
  - Architecture - Microsoft Windows local devices 22
- Remote Scenario 23
  - deviceTRUST Agent 23
  - deviceTRUST Client Extension 24
  - Architecture - Windows, macOS, Ubuntu, eLux® RP or IGEL OS device 24
- Operating System Compatibility 24
  - Apple iOS and iPadOS 25
  - Apple macOS 25
  - IGEL OS 10 and 11 26
  - IGEL OS 12 27
  - Microsoft Windows 27
  - Stratodesk NoTouch 28
  - Ubuntu Desktop 28
  - Unicon™ eLux 29
- Platform Compatibility 29
  - Amazon Web Services 29
  - Citrix Systems 30
  - Microsoft 30
  - Parallels 31
  - VMware 31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting Started 33
Scenario: Remote 33
Scenario: Local 33
Getting Started for Local 33
Step 1: Download the deviceTRUST setup binaries 34
Step 2: Install the deviceTRUST Agent 34
Step 3: Install the deviceTRUST Console 34
Step 4: Enter your deviceTRUST License 35
Step 5: Enable the Unauthorized USB Drive use case 37
Step 6: Test the Unauthorized USB Device use case 40
Next steps 41
Troubleshooting 41
Getting Started for Remote 41
Step 1: Download the deviceTRUST setup binaries 42
Step 2: Install the deviceTRUST Agent 42
Step 3: Install the deviceTRUST Console 43
Step 4: Enter your deviceTRUST License 43
Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device 45
Step 6: Enable the Compliance Check use case 45
Step 7: Check that access is denied when the deviceTRUST Client Extension is not installed 50
Step 8: Test the Compliance Check use case from a Microsoft Windows device 51
Next steps 52
Troubleshooting 53
Download deviceTRUST 23.1 for Windows 54
Download deviceTRUST® Client Extensions 54
Software components 55
Installation 56
TABLE OF CONTENTS 56

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installing the deviceTRUST® Agent 56
Citrix Virtual Channel Security 59
Unattended Installation 59
Installing the deviceTRUST® Console 59
Unattended Installation 62
Installing the deviceTRUST® Client Extension 62
TABLE OF CONTENTS 62
Templates 63
Table of Contents 64
Local Templates 64
Table of Contents 65
Remote Templates 65
Table of Contents 66
SaaS Templates 67
Table of Contents 67
Compliance Check 68
TABLE OF CONTENTS 68
Reporting 69
Table of Contents 69
Splunk Dashboards 69
Step 1: Creating the Splunk Index 70
Step 1.1: Manually creating the Splunk Index 71
Step 1.2: Creating the Splunk Index by installing the app 73
Step 2: Creating the Splunk Data Inputs 73
Step 3: Importing the Splunk app 77
Step 3.1: Downloading the Splunk app 77
Step 3.2: Installing the Splunk app 79
Step 4: Configuring deviceTRUST 81

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4.1: The Device-Based Licensing Report 81
Step 4.2: The Status Report 86
ELK Stack Dashboards 91
Step 1: Components 92
Step 1.1: Components - GitHub 92
Step 1.2: Components - Templates 94
Step 2: The Device-Based Licensing Report 95
Step 2.1: Add Index Template to ELK Stack 95
Step 2.2: Import Saved Objects to ELK Stack 100
Step 2.3: Configuring deviceTRUST 102
Step 3: The Status Report 109
Step 3.1: Add Index Template to ELK Stack 109
Step 3.2: Import Saved Objects to ELK Stack 113
Step 3.3: Configuring deviceTRUST 116
Step 3.4: Edit index settings 119
Reference 123
TABLE OF CONTENTS 123
Properties 123
Agent Reference 125
TABLE OF CONTENTS 125
Client Extension Reference 125
TABLE OF CONTENTS 125
Console Reference 125
TABLE OF CONTENTS 125
Troubleshooting 126
Scenario: Remote 126
Scenario: Local 126
Open a support ticket with us 127

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Knowledge Base 128
TABLE OF CONTENTS 128
General 128
TABLE OF CONTENTS 128
Configuration 128
Table of Contents 128
Connectivity 129
Table of Contents 129
Diagnostics 129
Table of Contents 129
Installation 129
TABLE OF CONTENTS 129
Licensing 129
TABLE OF CONTENTS 129
Support 129
TABLE OF CONTENTS 129
Compatibility 130
Table of Contents 130
Properties 130
TABLE OF CONTENTS 130
Reporting 130
TABLE OF CONTENTS 130
Features 130
Table of Contents 130
Releases 131
TABLE OF CONTENTS 131
TABLE OF CONTENTS 131
IGEL OS 11 Client Extension 23.1.400 131

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for third party WHOIS providers in 23.1.300 132
Compatibility 132
IGEL OS 12 Client Extension 23.1.400 132
Remoting Clients 132
UMS Configuration 132
New COSMOS Properties 133
WHOIS proxy, proxy type and usage in 23.1.400 133
Bug fixes in 23.1.200 134
Minor enhancements in 23.1.200 134
Bug fixes in 23.1.210 134
Compatibility 134
iOS Client Extension 23.1.400 134
Passcode authentication for iOS 17 134
Location and Network Wi-Fi SSID/BSSID 135
Compatibility 136
macOS Client Extension 23.1.410 136
Support for third party WHOIS providers in 23.1.300 137
Support for Microsoft Intune detection and WHOIS proxy, proxy type and usage in 23.1.400 137
Nice DCV extension support including Amazon WorkSpaces WSP 137
Bug Fixes in 23.1.100 137
Bug Fixes in 23.1.110 137
Bug Fixes in 23.1.200 138
Bug Fixes in 23.1.400 138
Bug Fixes in 23.1.410 138
Known Issues 138
Compatibility 138
Stratodesk NoTouch OS Client Extension 23.1.100 138
Available Properties 139

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NoTouch Properties 139
Custom Properties for NoTouch Devices 140
Ubuntu Client Extension 23.1.400 140
Support for third party WHOIS providers in 23.1.300 140
Support for WHOIS proxy, proxy type and usage in 23.1.400 140
Bug Fixes in 23.1.300 140
Bug Fixes in 23.1.400 140
Compatibility 140
deviceTRUST 23.1.410 140
Microsoft Intune Detection 141
WHOIS Proxy Detection 141
Proxy Detection with IP2Location Web Services 141
Proxy Detection with MaxMind GeoIP2 Insights Web Service 142
Minor enhancements to 23.1.400 142
Bug fixes in 23.1.400 142
Bug fixes in 23.1.410 143
Compatibility 143
Previous Releases 143
layout: doc 143
index 144
Client installation on Unicon™ eLux RP6 devices 148
Import the deviceTRUST® certificate chain 148
Install the package 149
Deploy the ripe.stat root certificate 151
Client installation on IGEL OS devices 152
Enable deviceTRUST for Citrix Independent Computing Architecture (ICA®) 153
Enable deviceTRUST for Microsoft Remote Desktop Protocol (RDP) 153
Client Extension installation on iOS and iPadOS devices 154

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registering with the deviceTRUST Portal 154
Assigning roles to Entra ID users 155
Generating an API Key for use by the deviceTRUST Agent 155
Generating an App Registration code to register iOS and iPadOS devices 156
Registering an iOS or iPadOS device using a QR code 157
Registering an iOS or iPad device using an MDM managed app configuration 157
Naming the iOS device for compatibility with iOS 16 and deviceTRUST Agent 23.1.120 or earlier 158
Using passcodes with deviceTRUST Agent 23.1.200 or later 158
Client installation on Apple macOS devices 158
Client installation on Stratodesk NoTouch OS devices 163
Enable deviceTRUST Client Extension for Citrix Workspace™ App 164
Enable deviceTRUST Client Extension for FreeRDP 164
Enable deviceTRUST Client Extension for VMware Horizon View 165
Client installation on Ubuntu devices 166
Client Extension installation on Microsoft Windows devices 168
Client Extension Installation Command Line Options 170
Unattended Installation 171
Active Setup Components 171
deviceTRUST Channel Registration 64-bit component 171
deviceTRUST Channel Registration 32-bit component 171
deviceTRUST Citrix Cleanup 32-bit component 172
Check that the deviceTRUST® Agent service is running 172
Check that you are using the latest deviceTRUST® version 173
Configuration of the deviceTRUST® Client Extension virtual channel for ICA 174
Microsoft Windows (All Users) 174
Microsoft Windows (Per User) 175
Apple macOS 175

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ubuntu 176
deviceTRUST® Client Extension & Active Setup 176
Active Setup Components 176
deviceTRUST Channel Registration 64-bit component 177
deviceTRUST Channel Registration 32-bit component 177
deviceTRUST Citrix Cleanup 32-bit component 178
Enabling DCV extensions on Amazon WorkSpaces WSP 178
Installing the Administrative Templates 178
Configuring DCV Extensions 179
Additional Requirements 180
Silent removal of the deviceTRUST® Client Extension for Apple macOS 181
Make sure that you have a valid license 181
Valid deviceTRUST License 182
Check deviceTRUST License 183
Group Policy Object (GPO) deployed configuration 183
IGEL OS 12 - No IGEL Properties 184
Device Location 185
Location Information 185
Operating System Location Provider 186
Third-Party Location Provider 186
WHOIS Location Provider 186
Cellular Location Provider 187
GPS Location Providers 187
deviceTRUST Policy 187
Location and Network improvements in Windows 11 24H2 188
SD Card detection for Logical Disk properties 189
Updating the deviceTRUST Client Extension in IGEL OS 11 190
Azure Virtual Desktop 190

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMware Horizon View 191
Log data to Microsoft Teams 192
Policy Loading 193
Active Directory GPOs 193
File-Based Policies 194
Merging Policy Items 194
Product Events 195
Application Channel 195
deviceTRUST/Admin Channel 196
deviceTRUST/Usage Channel 226
iOS Managed App Configuration 227
deviceTRUST Portal MDM Templates 229
iOS Passcodes 230
Passcode complexity and expiry 230
Simplifying passcode entry with notifications 231
Redirecting back to the remoting client 231
Actions 231
TABLE OF CONTENTS 231
Audit Event Task 231
Citrix Policy Task 232
Custom Process Task 233
Deny Access Task 234
Microsoft Entra ID Task 235
FSLogix App Masking Task 236
Task Reference 237
TABLE OF CONTENTS 237
Logon Abort Task 238
Map Drive Task 238

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Map Printer Task 239
Microsoft Applocker Task 240
Popup Message Task 241
Screen Saver Task 243
Send Mail Task 243
Shortcut Task 244
Terminate App Task 245
User Session Task 246
Web Request Task 247
Windows Firewall Task 248
Windows Policy Task 249
Windows Registry Task 250
Advanced Settings 251
General Settings 252
Action Settings 252
Amazon Settings 253
Connection Settings 254
Property Settings 256
Auditing Settings 257
Licensing 257
Operational 257
Remote Device 258
Tasks 259
Triggers 259
Custom Properties Settings 260
Local Agent Custom Properties 260
Remote Windows Device Custom Properties 262
Remote Linux, IGEL or NoTouch Device Custom Properties 263

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating Custom Properties 264
Microsoft Entra ID Settings 264
File-Based Policy Settings 265
Importing 266
Settings 267
TABLE OF CONTENTS 267
Licensing Settings 268
Mail Server Settings 269
Map Drive Settings 270
Microsoft AppLocker Settings 271
Mobile Settings 271
Printer Settings 272
Property Settings 273
Property Filters 274
Property Queries 275
Access Point Queries 277
Certificate Queries 277
Display Queries 278
Firewall Queries 278
Logical Disk Queries 279
Mapped Drive Queries 279
Network Queries 280
Printer Queries 280
Security Product Queries 281
Text Constraints 281
Enumeration (Enum) Constraints 282
Number Constraints 282
Date Constraints 283

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Boolean Constraints 283
IpAddress Constraints 284
Version Constraints 284
Security Settings 284
System Messages Settings 285
Access Point Properties 286
Browser Properties 297
Cellular Properties 304
Certificate Properties 322
ChromeOS Properties 343
Custom Properties 346
deviceTRUST Properties 349
Display Properties 360
Domain Properties 377
eLux® Properties 383
Hardware Properties 398
IGEL Properties 417
Input Properties 442
iOS Properties 447
Location Properties 451
Logical Disk Properties 468
macOS Properties 482
macOS Firewall Properties 488
macOS Update Properties 497
Mapped Drive Properties 517
MDM Properties 527
Name Properties 534
Network Properties 540

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NoTouch Properties 552
OS Properties 562
Password Policy Properties 573
Performance Properties 582
Power Properties 587
Printer Properties 592
Region Properties 614
Remote Control Properties 622
Remoting Client Properties 638
Screen Saver Properties 646
Security Product Properties 652
Session Properties 662
Smartcard Reader Properties 673
User Properties 676
WHOIS Properties 699
Windows Properties 717
Windows Defender Properties 729
Windows Firewall Properties 765
Windows Registry Properties 802
Windows Update Properties 808
Adobe Reader DC Template 839
Step 1: Prerequisites 839
Step 2: Contexts 840
Step 3: Actions 842
Troubleshooting 846
Microsoft Visio Template 846
Step 1: Prerequisites 847
Step 2: Contexts 847

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions 850
Troubleshooting 854
Nuance PDF Template 854
Step 1: Prerequisites 855
Step 2: Contexts 855
Step 3: Actions 857
Troubleshooting 862
IP Address Template 862
Step 1: Prerequisites 862
Step 2: Contexts 862
Step 3: Actions 863
Troubleshooting 864
NetBIOS Name Template 864
Step 1: Prerequisites 865
Step 2: Contexts 865
Step 3: Actions 866
Troubleshooting 867
Wi-Fi Access Point Template 867
Step 1: Prerequisites 867
Step 2: Contexts 867
Step 3: Actions 868
Troubleshooting 869
Microsoft Teams Template 869
Step 1: Prerequisites 870
Step 2: Contexts 870
Step 3: Actions 870
Troubleshooting 872
Snipping Tool Template 872

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites 872
Step 2: Contexts 872
Step 3: Actions 873
Troubleshooting 873
Access Mode Template 873
Step 1: Prerequisites 874
Step 2: Contexts 874
Step 3: Actions 876
Troubleshooting 878
Adobe Acrobat DC Template 878
Step 1: Prerequisites 878
Step 2: Contexts 878
Step 3: Actions 881
Troubleshooting 885
Corporate Device Template 885
Step 1: Prerequisites 886
Step 2: Contexts 886
Step 3: Actions 889
Troubleshooting 891
Country Template 891
Step 1: Prerequisites 892
Step 2: Contexts 892
Step 3: Actions 893
Troubleshooting 895
Microsoft Visio Template 896
Step 1: Prerequisites 896
Step 2: Contexts 896
Step 3: Actions 899

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting 903
Nuance PDF Template 903
Step 1: Prerequisites 904
Step 2: Contexts 904
Step 3: Actions 907
Troubleshooting 911
Proximity Template 911
Step 1: Prerequisites 911
Step 2: Contexts 911
Step 3: Actions 912
Troubleshooting 914
Security State Template 914
Step 1: Prerequisites 915
Step 2: Contexts 915
Step 3: Actions 915
Troubleshooting 918
Wi-Fi Security Mode Template 918
Step 1: Prerequisites 918
Step 2: Contexts 918
Step 3: Actions 919
Troubleshooting 921
Working Time Template 921
Step 1: Prerequisites 922
Step 2: Contexts 922
Step 3: Actions 922
Troubleshooting 924
Application Log Template 925
Step 1: Prerequisites 925

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts 925
Step 3: Actions 930
Troubleshooting 930
ELK Stack Template 930
Step 1: Prerequisites 931
Step 2: Contexts 931
Step 3: Actions 936
Troubleshooting 937
Email Template 937
Step 1: Prerequisites 937
Step 2: Contexts 937
Step 3: Actions 942
Troubleshooting 942
Log File Template 942
Step 1: Prerequisites 943
Step 2: Contexts 943
Step 3: Actions 948
Troubleshooting 948
Splunk Template 948
Step 1: Prerequisites 949
Step 2: Contexts 949
Step 3: Actions 953
Troubleshooting 954
Conditional Access Template 955
Step 1: Prerequisites 955
Step 2: Contexts 955
Step 3: Actions 956
Troubleshooting 957

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conditional Application Access Template 957
Step 1: Prerequisites 957
Step 2: Contexts 957
Step 3: Actions 958
Troubleshooting 960
Unauthorized USB Device Template 960
Step 1: Prerequisites 961
Step 2: Contexts 961
Step 3: Actions 962
Troubleshooting 963
Conditional Access Template 963
Step 1: Prerequisites 963
Step 2: Contexts 963
Step 3: Actions 968
Troubleshooting 970

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Welcome

The deviceTRUST® documentation provides information about the installation, setup and a product reference for deviceTRUST.

Quick setup

To get started with deviceTRUST, choose your Architecture and then take a look at the Getting Started guide.

More information

- Architecture describes the different deployment scenarios.
- Getting Started provides the essential steps for a successful deviceTRUST installation.
- Download provides links that can be used to download the latest deviceTRUST Software.
- Installation details some important usage scenarios, plus how to install the deviceTRUST Console, Agent and Client Extension.
- Templates details the templates which can be used to quickly implement a use case.
- Reporting contains information about analyzing and reporting contextual information of your users and devices.
- Reference provides a set of reference material describing the more advanced features of deviceTRUST.
- Troubleshooting important steps are described to help troubleshoot the deviceTRUST installation and configuration.
- Knowledge Base provides a useful resource for common problems and resolutions.
- Releases contains the release notes detailing new features and bug fixes within the released deviceTRUST products.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Architecture

- Local Scenario
- Remote Scenario
- OS Compatibility
- Platform Compatibility

Local Scenario

deviceTRUST requires only one main component when installing on local devices, the deviceTRUST Agent. The deviceTRUST component can be installed and configured within minutes and can be fully integrated with existing deployment processes and management tools. No additional infrastructure (e.g. a database or a web server) is required for deviceTRUST to be installed in your environment.

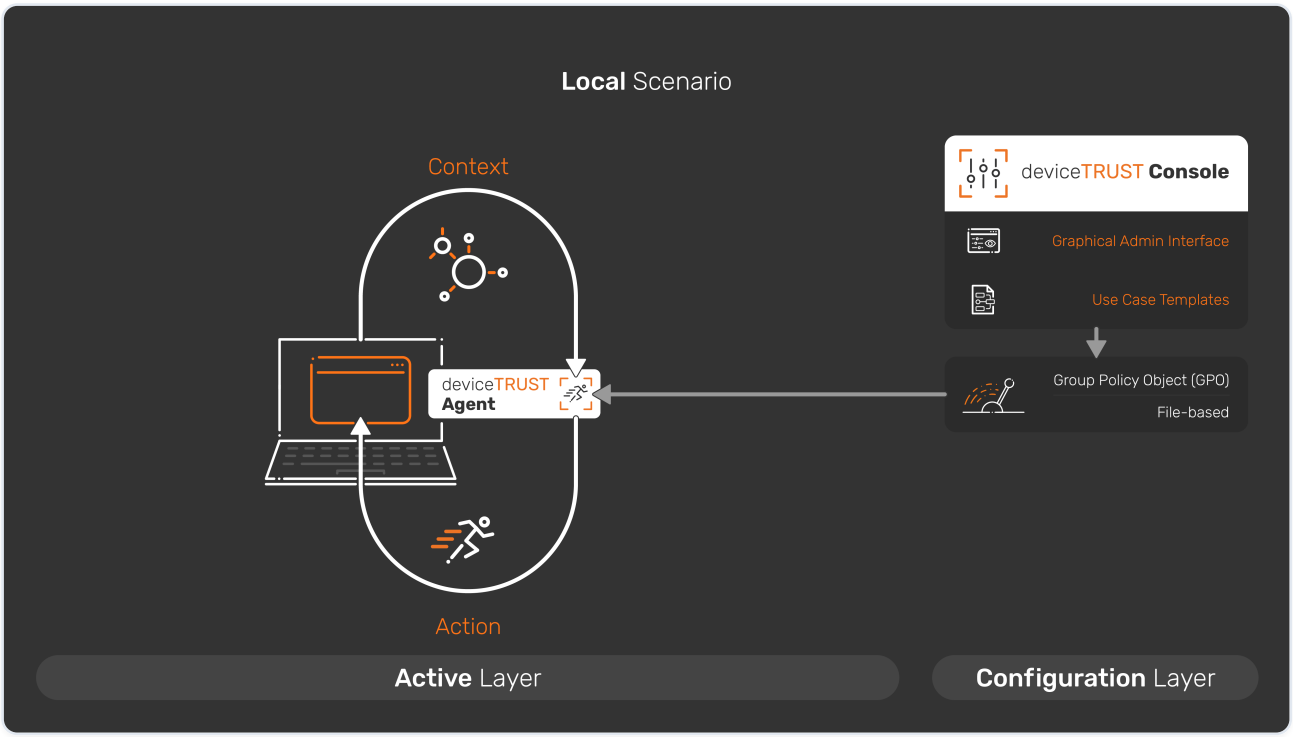
deviceTRUST® Agent

This component needs to be installed on the local device. The Property Reference describes which properties of the local agent are available within the users' session.

Architecture - Microsoft Windows local devices

The following diagram details the deviceTRUST architecture when the agent is installed on a Windows OS, with deviceTRUST making the user and device context information available within the local desktop session. Policy is made available to the deviceTRUST Agent using existing Microsoft Active Directory Group Policy Management or file-based. All operations performed by the deviceTRUST Agent are written to the Microsoft Windows Event Log.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remote Scenario

deviceTRUST consists of two main components when installing in remote environments, the deviceTRUST Agent and the deviceTRUST Client Extension. Both deviceTRUST components can be installed and configured within minutes and can be fully integrated with existing deployment processes and management tools. No additional infrastructure (e.g. a database or a web server) is required for deviceTRUST to be installed in your environment.

Solutions are provided by deviceTRUST® for both traditional and modern Operating Systems (OS). On a traditional OS such as Microsoft Windows, an extensibility framework is available that enables deviceTRUST to send user and device context within the communication channel between the clients and the Remote Desktop Services host. deviceTRUST also provides a solution for more modern OS's, such as Apple iOS, which offer no extensibility framework.

deviceTRUST Agent

This component needs to be installed on the remoting host that delivers the remote session to the users. The following technologies are supported by deviceTRUST: Amazon WorkSpaces, Citrix Virtual Apps and Desktops™ (CVAD), Microsoft Azure Virtual Desktop (AVD), Microsoft Remote Desktop Session Host (RDSH) or VMware Horizon View.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

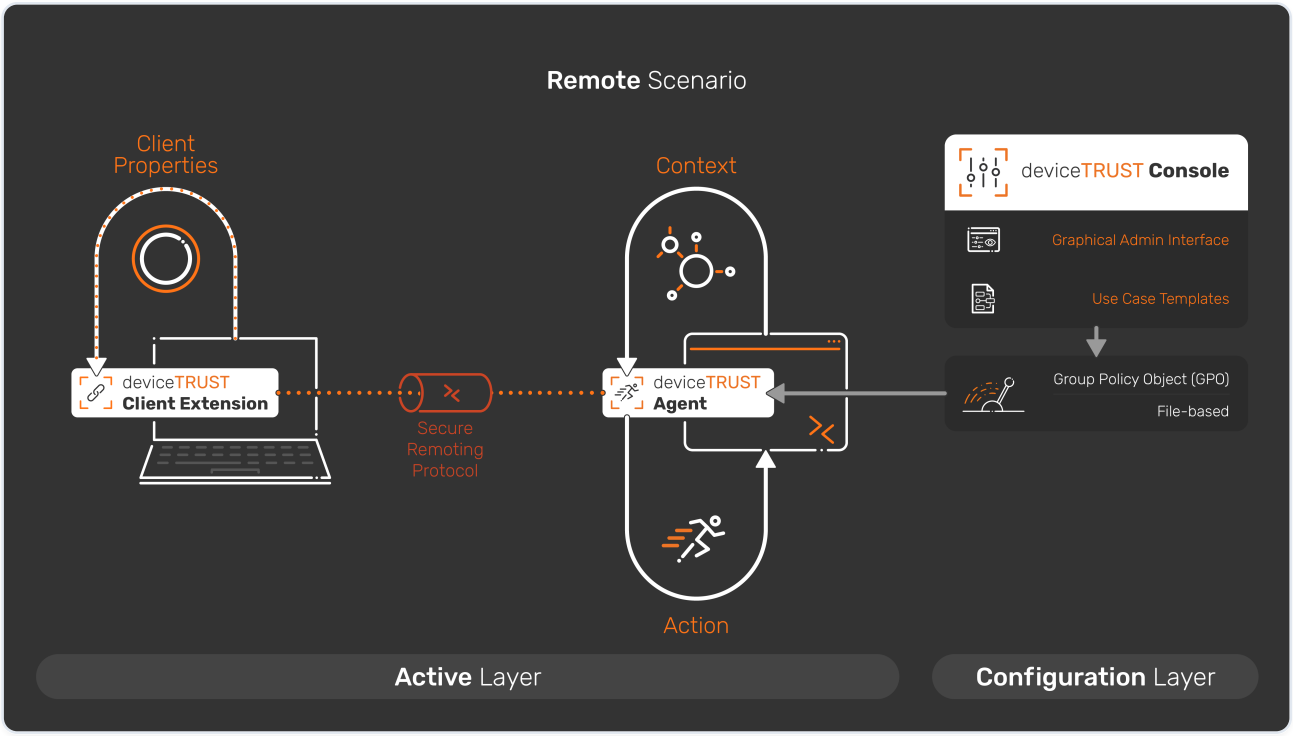
deviceTRUST Client Extension

This component needs to be installed on the remote device which will be used to connect to the remote host delivering the published applications and desktops. It is not required to have deviceTRUST Client Extension installed onto all of your remote devices but recommended to get the full range of context information about the remote device and its user into the users' virtual session.

In the absence of the deviceTRUST Client Extension on the remote device, deviceTRUST delivers the LOCAL_* properties into the users' remote session. The Property Reference describes which properties of the local agent and remote device are available within the users' session.

Architecture - Windows, macOS, Ubuntu, eLux® RP or IGEL OS device

The following diagram details the deviceTRUST architecture when the remote client is installed on a Windows, macOS, Ubuntu, eLux RP or IGEL OS device, with deviceTRUST sending the user and device context information within the communication channel offered by the remoting protocol. Policy is made available to the deviceTRUST Agent using existing Microsoft Active Directory Group Policy Management or file-based. All operations performed by the deviceTRUST Agent are written to the Microsoft Windows Event Log.



Operating System Compatibility

- Apple iOS and iPadOS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Apple macOS
- IGEL OS 10 and 11
- IGEL OS 12
- Microsoft Windows
- Stratodesk NoTouch
- Ubuntu Desktop
- Unicon eLux

Apple iOS and iPadOS

Compatible operating systems (deviceTRUST® Client Extension):

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

NOTE:

iOS 17 support requires deviceTRUST Agent 23.1.200 or later, and deviceTRUST Client Extension for iOS 23.1.200 or later.

Apple macOS

Compatible operating systems (deviceTRUST Client Extension):

- Apple macOS 10.15 and later

Compatible technologies:

- Amazon AppStream
- Amazon WorkSpaces (PCoIP) $_{1}$
- Amazon WorkSpaces (WSP) $_{2}$
- Citrix Virtual Apps™ and Desktops
- Citrix Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft Remote Desktop Services (via FreeRDP 2)
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

NOTE:

{1} Amazon WorkSpaces (PCoIP) no longer allows virtual channels to be loaded on Apple macOS. This can be worked around by installing Amazon WorkSpaces Client v5.3.0. {2} Amazon WorkSpaces (WSP) requires that the `<code class='language-plaintext highlighter-rouge'>Configure extensions</code> policy is set to <code class='language-plaintext highlighter-rouge'>Server` and `Client</code>` and there are additional software requirements. More information can be found in our `<a href='/docs/23-1/kb/general/installation/enabling_dcv_extensions_on_amazon_worlspaces_wsp/'>`Enabling DCV extensions on Amazon WorkSpaces WSP knowledge base article.

IGEL OS 10 and 11

Compatible technologies (deviceTRUST Client Extension):

- Amazon WorkSpaces (PCoIP) natively integrated in IGEL OS 11.08.200 and later {1}
- Citrix Virtual Apps and Desktops natively integrated in IGEL OS 10.03.500 and later
- Citrix Cloud natively integrated in IGEL OS 10.03.500 and later
- Microsoft Azure Virtual Desktop (AVD) natively integrated in IGEL OS 11.08.200 and later {1}
- Microsoft Remote Desktop natively integrated in IGEL OS 10.03.500 and later
- VMware Horizon View (Blast) natively integrated in IGEL OS 10.08.230 and later {1}
- VMware Horizon View (PCoIP) natively integrated in IGEL OS 10.08.230 and later {1}
- VMware Horizon View (RDP) natively integrated in IGEL OS 10.08.230 and later {1}

NOTE:

{1} Compatibility with previous IGEL OS releases is available by contacting deviceTRUST Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL OS 12

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops available for IGEL OS 12.01.120 and later {1}
- Citrix Cloud natively integrated available for IGEL OS 12.01.120 and later {1}
- Microsoft Azure Virtual Desktop (AVD) available for IGEL OS 12.01.120 and later {1}
- VMware Horizon View (Blast) available for IGEL OS 12.01.120 and later {1}
- VMware Horizon View (PCoIP) available for IGEL OS 12.01.120 and later {1}
- VMware Horizon View (RDP) available for IGEL OS 12.01.120 and later {1}

NOTE:

{1} The deviceTRUST Client Extension can be installed from the IGEL App Portal.

Microsoft Windows

Compatible operating systems (deviceTRUST Agent and Console):

- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later

Compatible operating systems (deviceTRUST Client Extension):

- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later

Compatible technologies:

- Amazon AppStream
- Amazon WorkSpaces (PCoIP)
- Amazon WorkSpaces (WSP) {1}
- Azure Virtual Desktop
- Azure Active Directory
- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nice DCV Standalone
- Parallels Remote Application Server
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

NOTE:

{1} Amazon WorkSpaces (WSP) requires that the `<code class='language-plaintext highlighter-rouge'>Configure extensions</code> policy is set to <code class='language-plaintext highlighter-rouge'>Server and Client</code>` and there are additional software requirements. More information can be found in our Enabling DCV extensions on Amazon WorkSpaces WSP knowledge base article.

Stratodesk NoTouch

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops on NoTouch OS 3.4.516 and later
- Citrix Cloud on NoTouch OS 3.4.516 and later
- Microsoft Remote Desktop on NoTouch OS 3.4.516 and later
- VMware Horizon View (Blast) on NoTouch OS 3.4.516 and later
- VMware Horizon View (PCoIP) on NoTouch OS 3.4.516 and later
- VMware Horizon View (RDP) on NoTouch OS 3.4.516 and later

Ubuntu Desktop

Compatible operating systems (deviceTRUST Client Extension):

- Ubuntu Desktop 18.04 LTS and later

Compatible technologies:

- Amazon WorkSpaces (PCoIP)
- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services (via FreeRDP 2)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

Unicon™ eLux

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops natively integrated in eLux® RP 6
- Citrix Cloud natively integrated in eLux RP 6
- Microsoft Remote Desktop natively integrated in eLux RP 6

Platform Compatibility

- Amazon Web Services
- Citrix Systems
- Microsoft
- Parallels
- VMware

Amazon Web Services

Compatible technologies:

- Amazon WorkSpaces (PCoIP)
- Amazon WorkSpaces (WSP) {2 & 3}
- Amazon AppStream {2}
- Nice DCV Standalone {2}

Compatible operating systems:

- Apple macOS 10.15 and later
- IGEL OS 11.08.200 and later versions of IGEL OS 11 {1}
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later
- Ubuntu Desktop 18.04 LTS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

{1} Compatibility with previous IGEL OS releases is available by contacting deviceTRUST® Support. Compatibility with IGEL OS 12 is not yet available. {2} Amazon WorkSpaces (WSP), Amazon AppStream and Nice DCV Standalone currently require Microsoft Windows or Apple macOS clients. {3} Amazon WorkSpaces (WSP) requires that the `Configure extensions` policy is set to `Server and Client` and there are additional software requirements. More information can be found in our Enabling DCV extensions on Amazon WorkSpaces WSP

Citrix Systems

Compatible technologies:

- Citrix Virtual Apps and Desktops™ {1}
- Citrix Cloud™ {1}

Compatible operating systems:

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later
- Apple macOS 10.15 and later
- IGEL OS 10.03.500 and later
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later
- Stratodesk NoTouch OS 3.4.516 and later
- Ubuntu Desktop 18.04 LTS and later
- Unicon™ eLux RP 6

NOTE:

{1} Compatibility with HTML5 delivered apps and desktops is not yet available.

Microsoft

Compatible technologies:

- Microsoft Remote Desktop Services

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Azure Virtual Desktop {1}
- Azure Active Directory {2}

Compatible operating systems:

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later
- Apple macOS 10.15 and later (via FreeRDP 2)
- IGEL OS 11.08.200 or later {3}
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS and later (via FreeRDP 2)

NOTE:

{1} Compatibility with Azure Virtual Desktop is available on Microsoft Windows and IGEL OS only. {2} Compatibility with Azure Active Directory provided by deviceTRUST Agent on Microsoft Windows only. {3} Compatibility with previous IGEL OS releases is available by contacting deviceTRUST Support. Compatibility with IGEL OS 12 is currently limited to Azure Virtual Desktop.

Parallels

Compatible technologies:

- Parallels Remote Application Server

Compatible operating systems:

- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later

VMware

Compatible technologis:

- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compatible operating systems:

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later
- Apple macOS 10.15 and later
- IGEL OS 10.08.230 or later {1}
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later
- Stratodesk NoTouch OS 3.4.516 and later
- Ubuntu Desktop 18.04 LTS and later

NOTE:

{1} Compatibility with previous IGEL OS releases is available by contacting deviceTRUST Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting Started

deviceTRUST® requires some simple but essential configuration steps to be performed to enable deviceTRUST functionality for your remoting environments or for your local devices.

Scenario: Remote

In remote scenarios, deviceTRUST transports the context information from the users remote device into the virtual session where the configuration is enforced. Please visit Getting Started for Remote Devices to begin the guide.

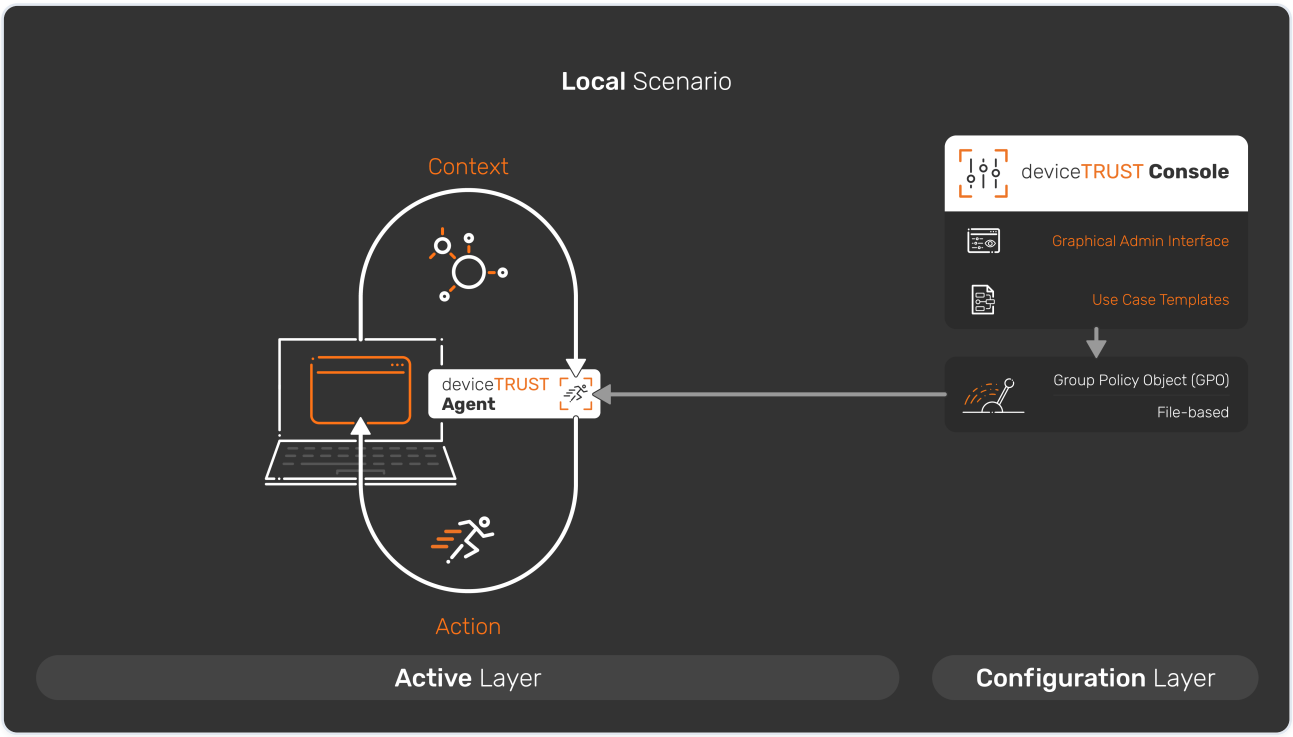
Scenario: Local

In local scenarios, deviceTRUST collects context information and executes actions locally. Please visit Getting Started for Local Devices to begin the guide.

Getting Started for Local

deviceTRUST® requires some simple but essential configuration steps to be performed to enable deviceTRUST functionality for your local devices. We will guide you step-by-step through simple deviceTRUST installation and configuration steps to enable deviceTRUST with an unauthorized USB drives use case for your local devices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



We will perform the following steps:

- Step 1: Download the deviceTRUST setup binaries
- Step 2: Install the deviceTRUST Agent
- Step 3: Install the deviceTRUST Console
- Step 4: Enter your deviceTRUST License
- Step 5: Enable the Unauthorized USB Drive use case
- Step 6: Test the Unauthorized USB Device use case

Step 1: Download the deviceTRUST setup binaries

The latest deviceTRUST software can be found on our Download page and your personalized license can be found within your product license certificate.

Step 2: Install the deviceTRUST Agent

Start the installation of the deviceTRUST Agent on your local device. Follow the steps in the section Installing the Agent to complete the installation.

Step 3: Install the deviceTRUST Console

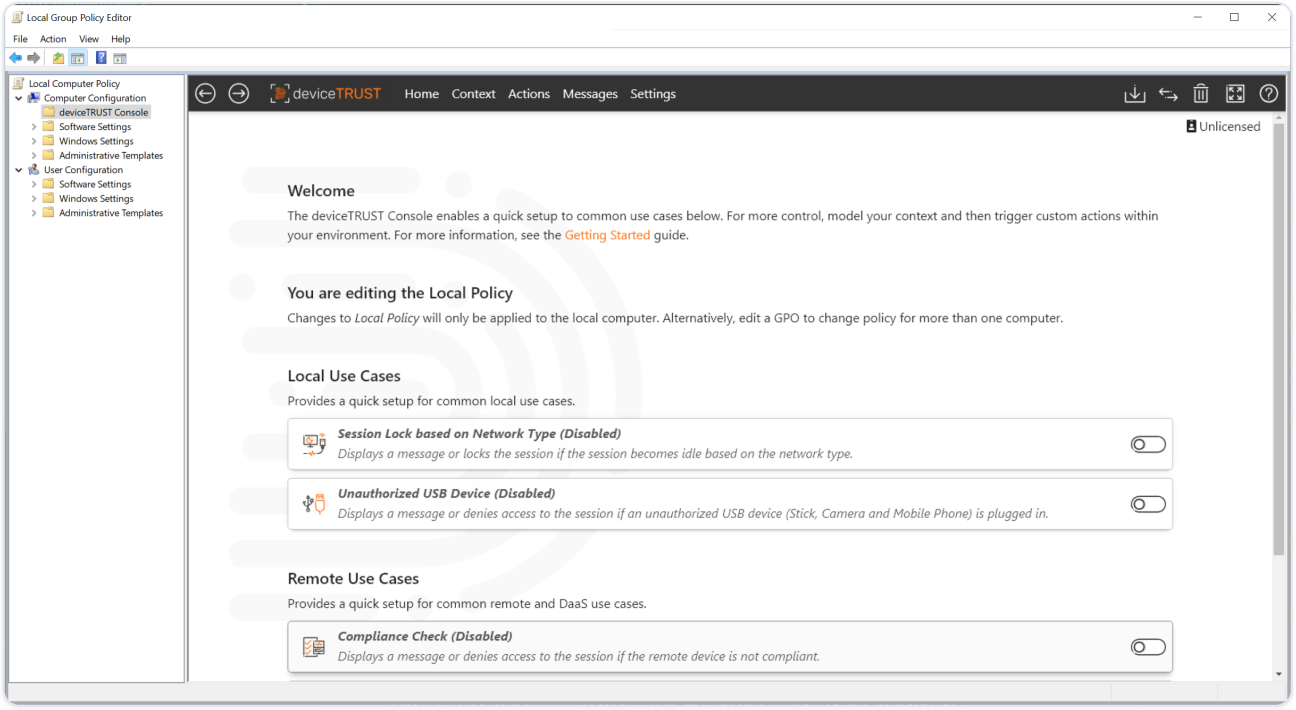
To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

contextual security policies to the deviceTRUST Agent. Those options are using the Local Policy Editor, a Group Policy Object (GPO) or file-based.

Within the Getting Started Guide, for simplicity, we use the Local Policy Editor to quickly and efficiently create, edit, and use contextual security policies. Follow the steps in the section Installing the Console to complete the installation.

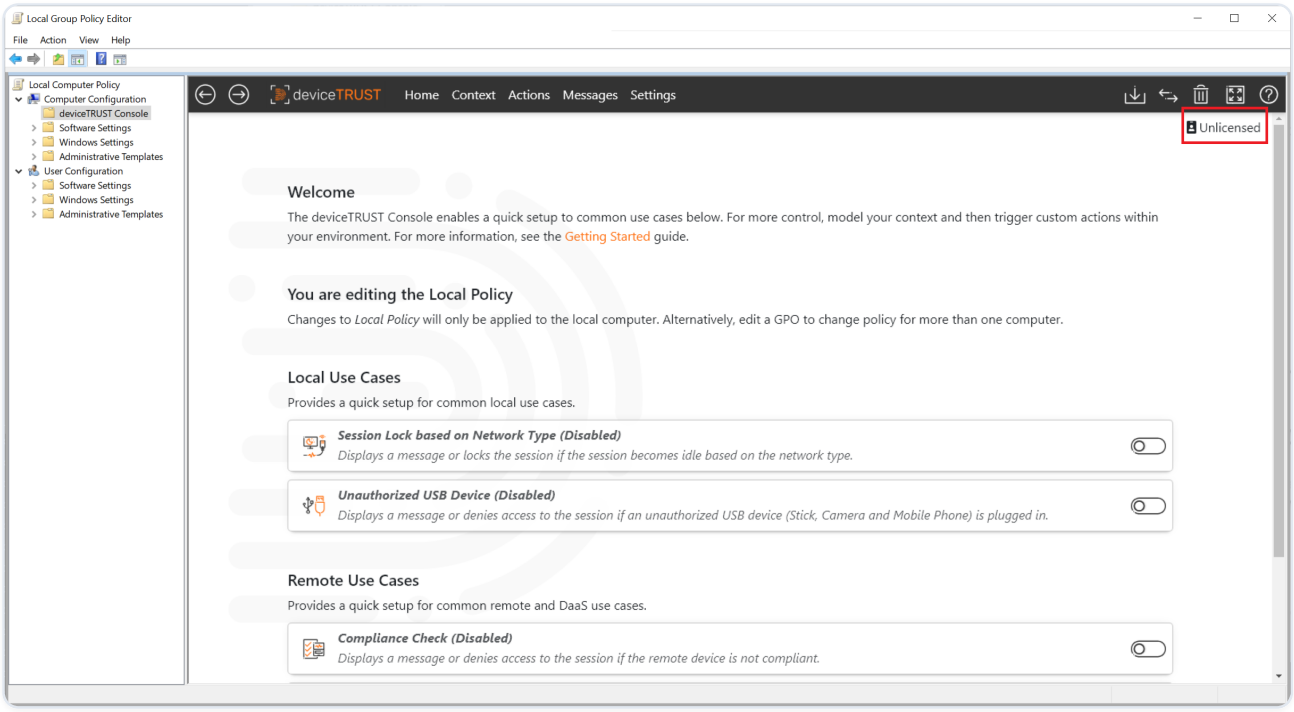
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



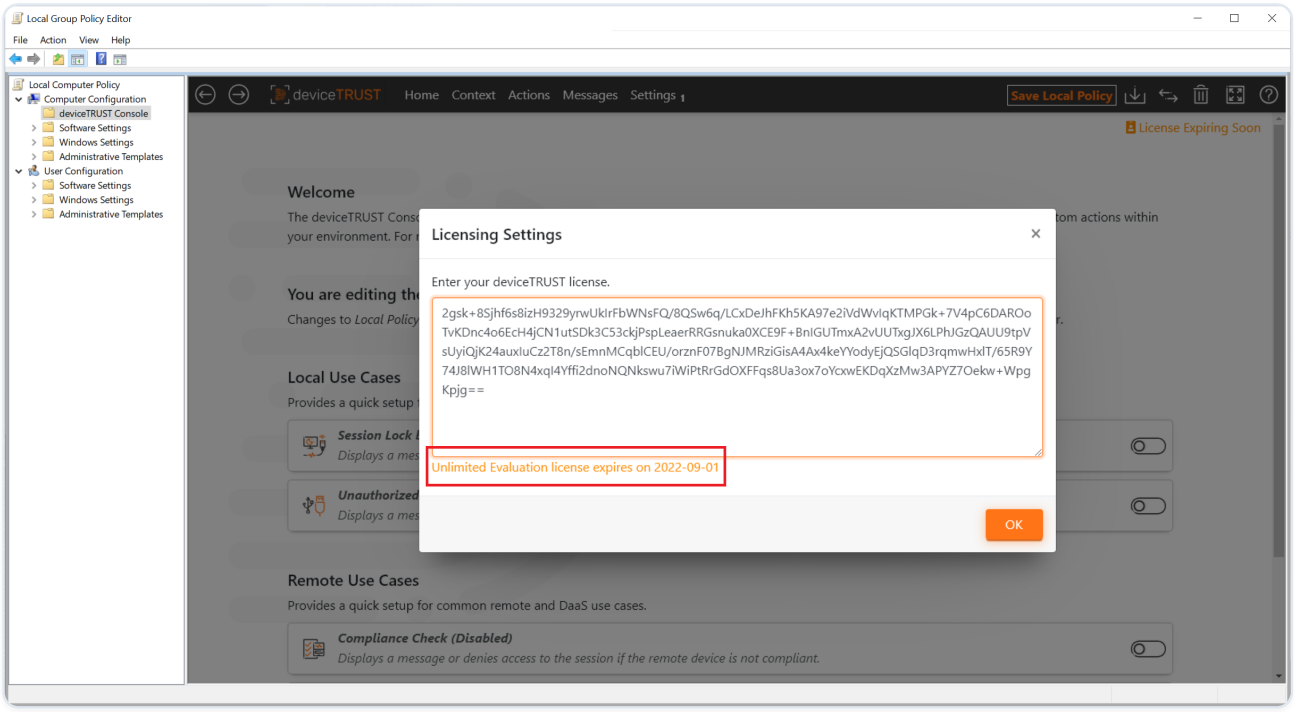
Step 4: Enter your deviceTRUST License

To add the license into the deviceTRUST contextual security policy open the Local Policy Editor and navigate to `DEVICETRUST CONSOLE` and click on the `UNLICENSED` link on the homepage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

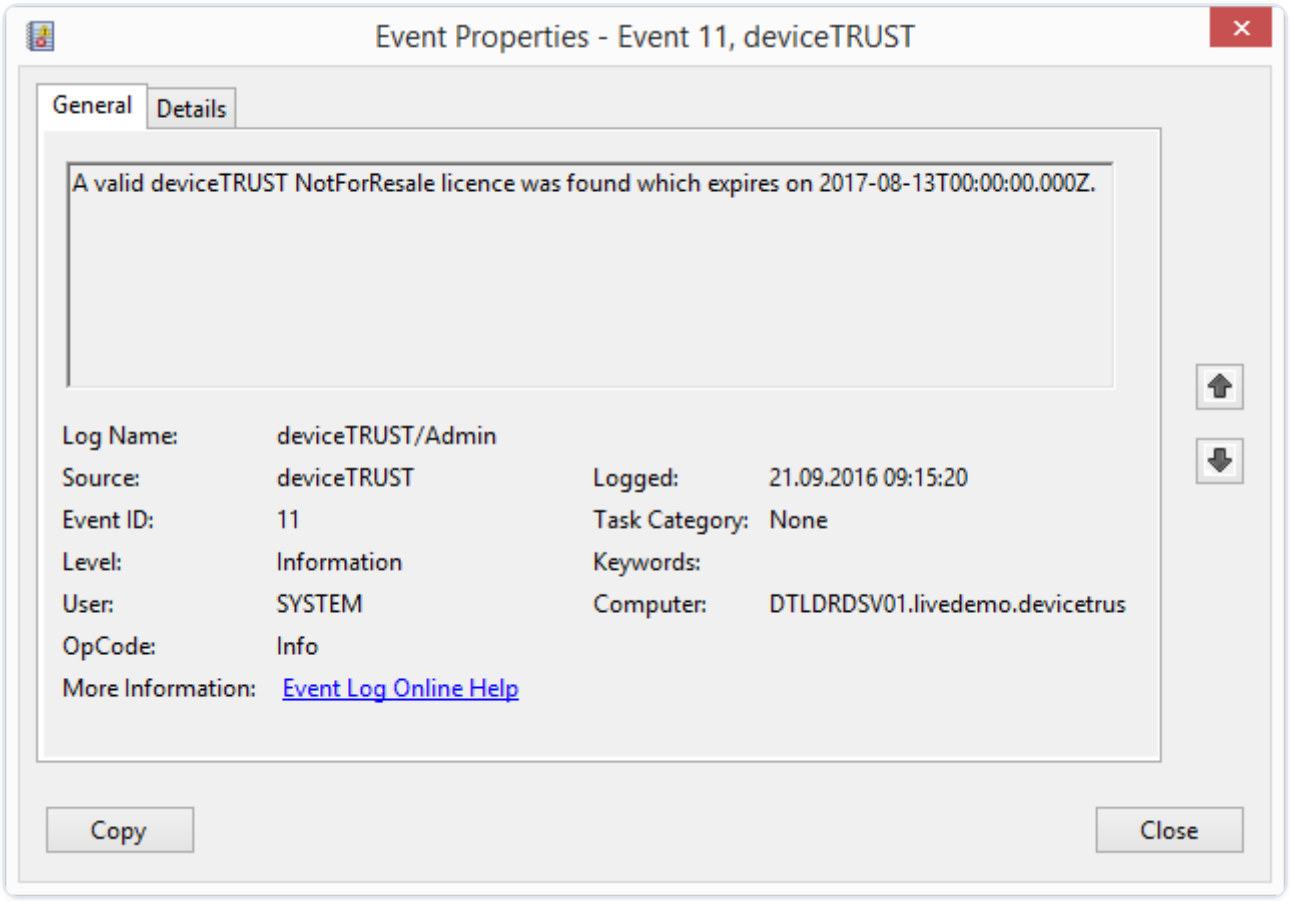


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.



deviceTRUST is now enabled and will work for all users except local administrators connecting to that remoting or DaaS host system with deviceTRUST Agent installed. To check if you have added a valid deviceTRUST license, open the Windows Event Log and navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN` and check for the existence of event ID 11 which states that your deviceTRUST license is valid.

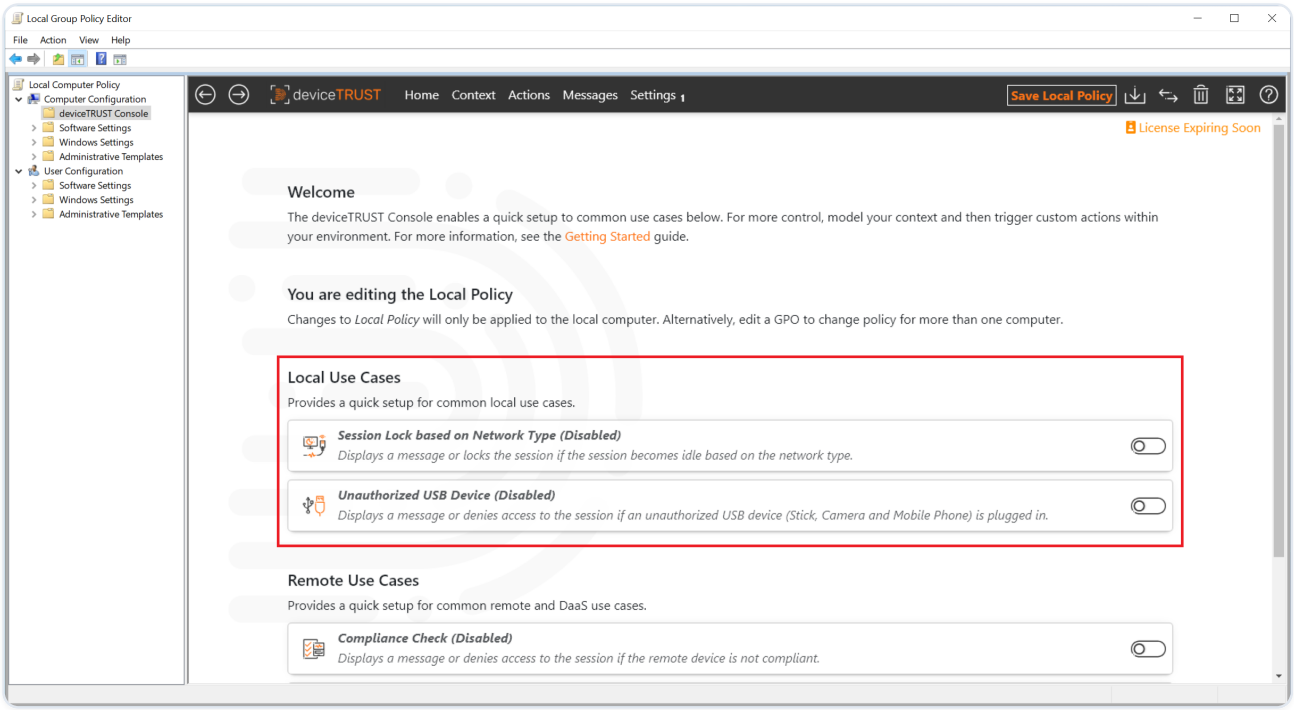
© 1997–2026 Citrix Systems, Inc. All rights reserved.



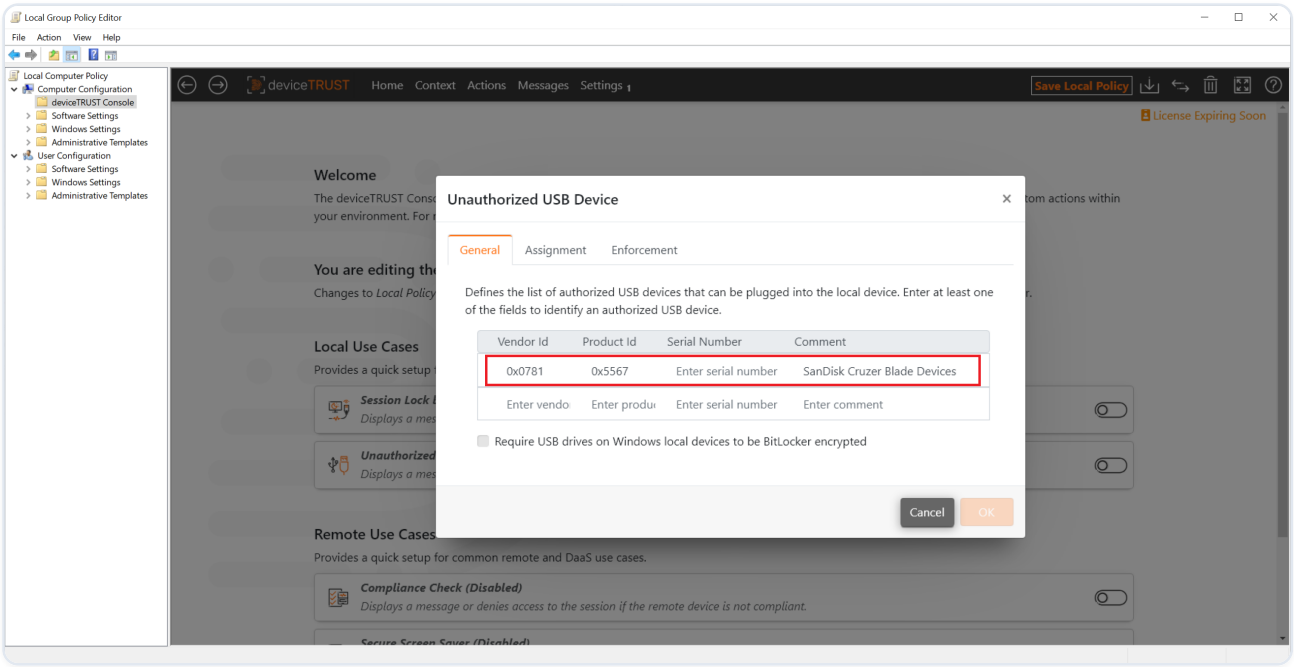
Step 5: Enable the Unauthorized USB Drive use case

We will use the deviceTRUST Console to create a contextual security policy that makes access to the session dependent on whether the USB device being used has been authorized. The deviceTRUST Console includes a set of use cases which can be used to quickly implement a use case. Launch the deviceTRUST Console and navigate to `LOCAL USE CASES` on the homepage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

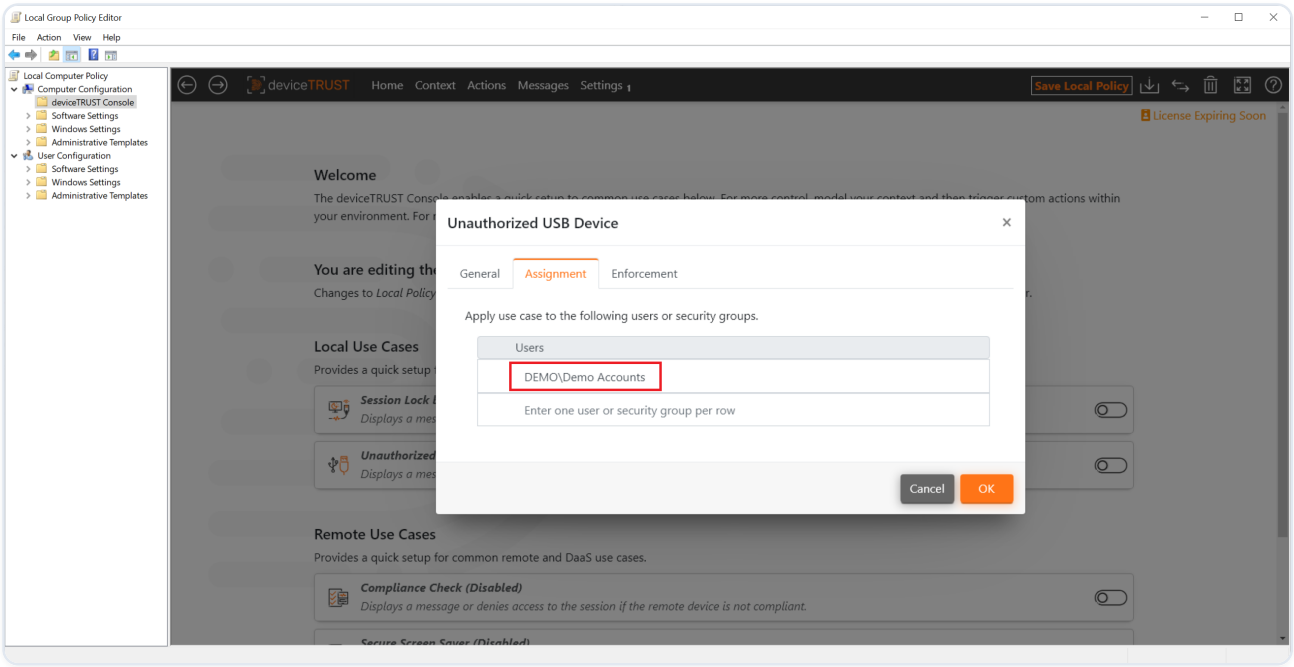


Select the `UNAUTHORIZED USB DEVICE` use case and add authorized USB devices on the `GENERAL` tab into the list of authorized USB devices.

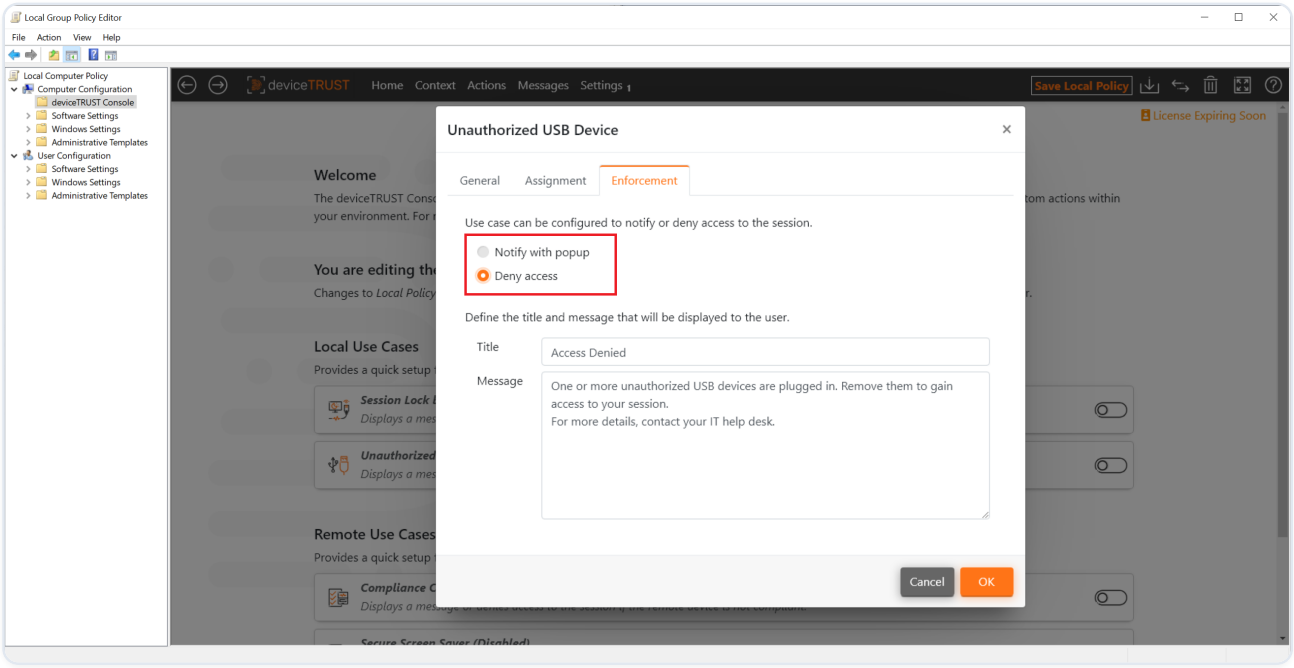


Click on the `ASSIGNMENT` configuration tab and add `USERS` and / or `SECURITY GROUPS` to apply the use case for.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

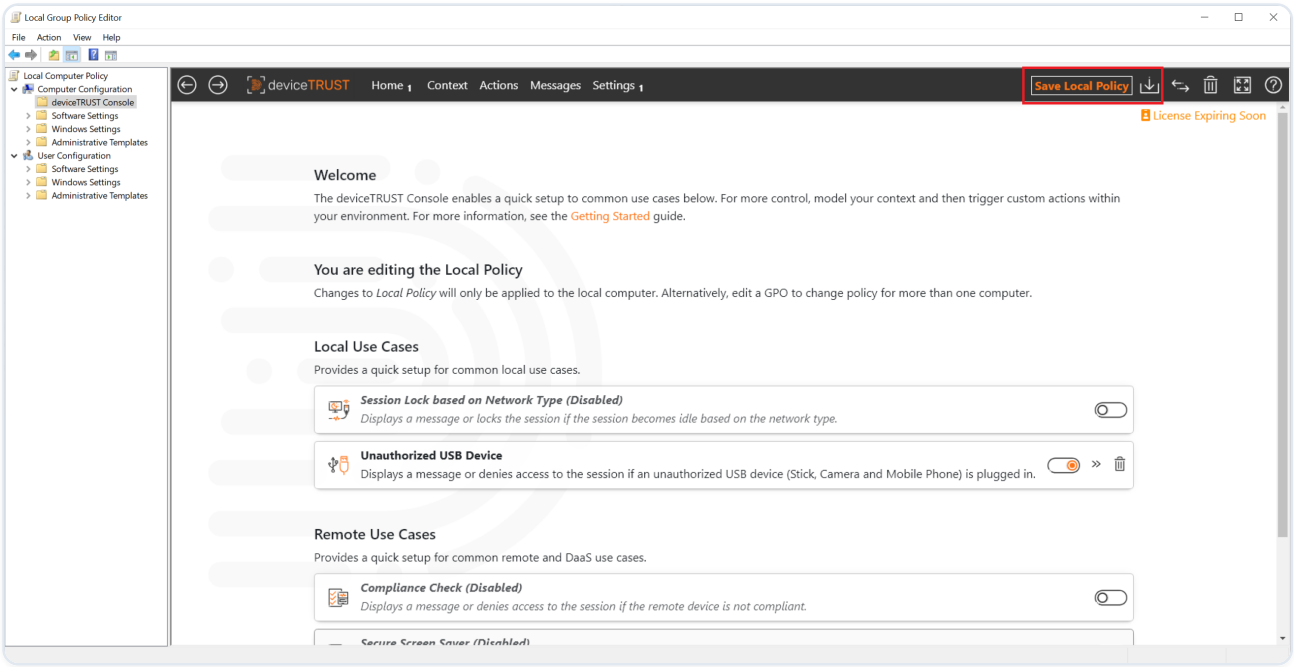


Click on the `ENFORCEMENT` configuration tab and select `DENY ACCESS`.



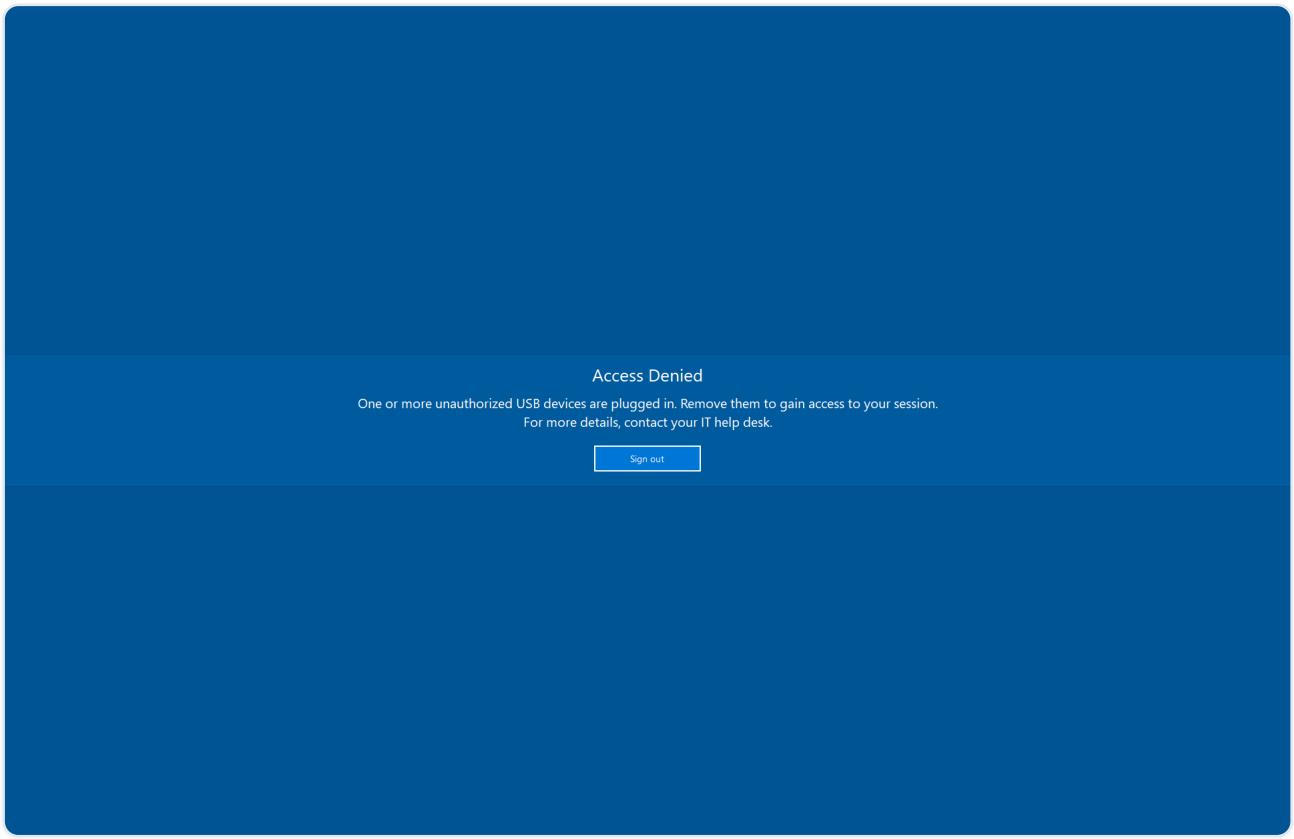
Click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar to save the unauthorized USB device use case to the local computer policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 6: Test the Unauthorized USB Device use case

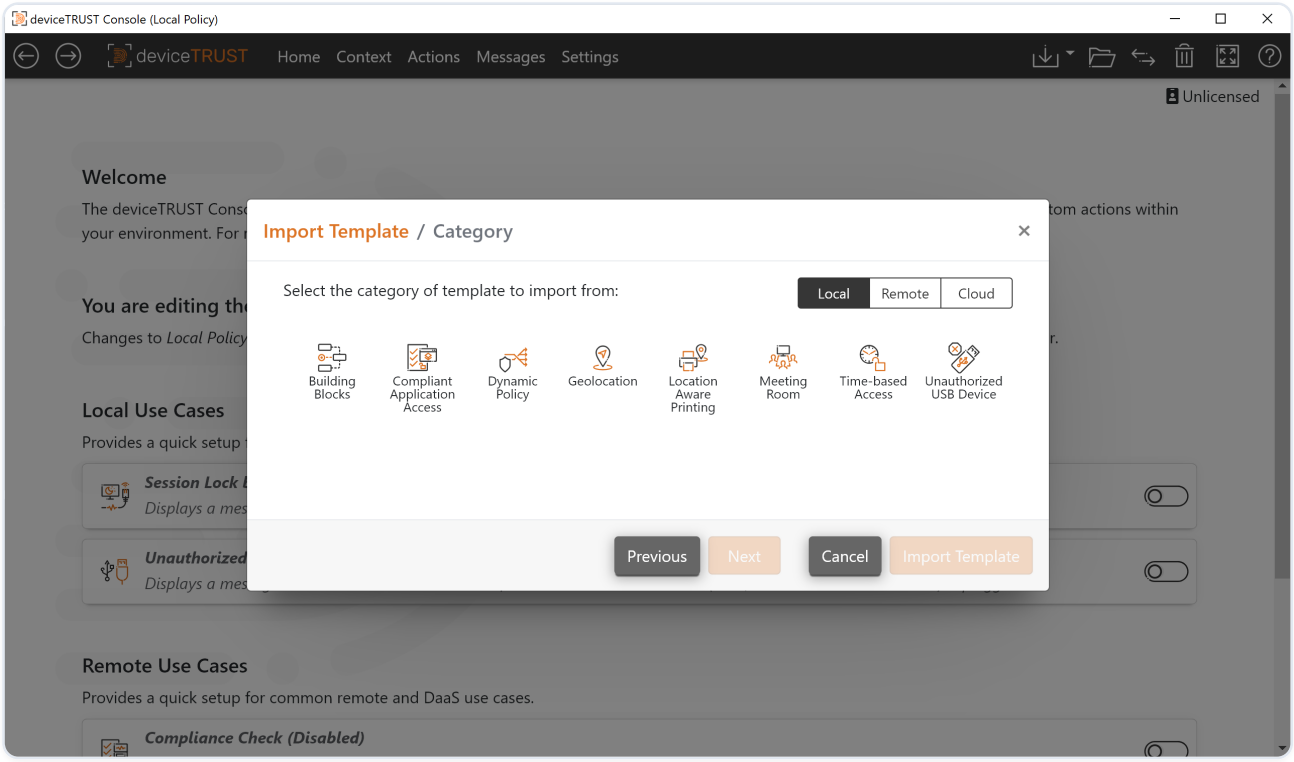
Sign in with a non-administrative user account to the local device and then plug in an authorized USB device at runtime. The authorized USB device is displayed in Windows Explorer and can be used. Now plug in an unauthorized USB device in addition or exclusively to see how deviceTRUST can easily and dynamically control access to the session depending on the USB device in use.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Next steps

You have now successfully implemented your first use case with deviceTRUST for your local devices. Feel free to check out our additional use cases provided on the deviceTRUST Console homepage under `LOCAL USE CASES`. In addition, the deviceTRUST Console gives you access to many more configuration Templates for a wide variety of use cases.



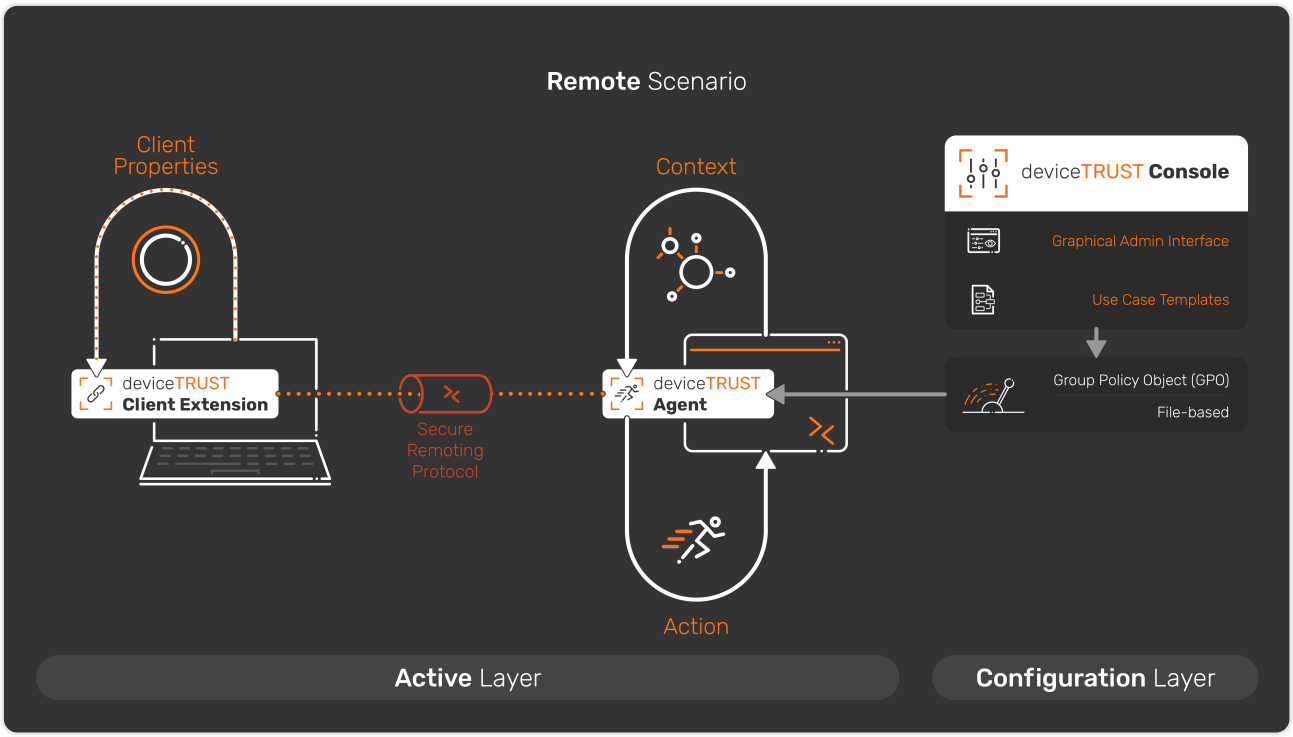
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Getting Started for Remote

deviceTRUST® requires some simple but essential configuration steps to be performed to enable deviceTRUST functionality for your remote environments. We will guide you step-by-step through simple deviceTRUST installation and configuration steps to enable deviceTRUST with a compliance check use case within your remote environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



We will perform the following steps:

- Step 1: Download the deviceTRUST setup binaries
- Step 2: Install the deviceTRUST Agent
- Step 3: Install the deviceTRUST Console
- Step 4: Enter your deviceTRUST License
- Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device
- Step 6: Enable the Compliance Check use case
- Step 7: Check that access is denied when the deviceTRUST Client Extension is not installed
- Step 8: Test the Compliance Check use case from a Microsoft Windows device

Step 1: Download the deviceTRUST setup binaries

The latest deviceTRUST software can be found on our Download page and your personalized license can be found within your product license certificate.

Step 2: Install the deviceTRUST Agent

Start the installation of the deviceTRUST Agent on your remoting or DaaS host system, which can be Amazon WorkSpaces, Citrix Virtual Apps and Desktops (CVAD), Microsoft Azure Virtual Desktop (AVD), Microsoft Remote Desktop Session Host (RDSH) or VMware Horizon View. Follow the steps in the section Installing the Agent to complete the installation.

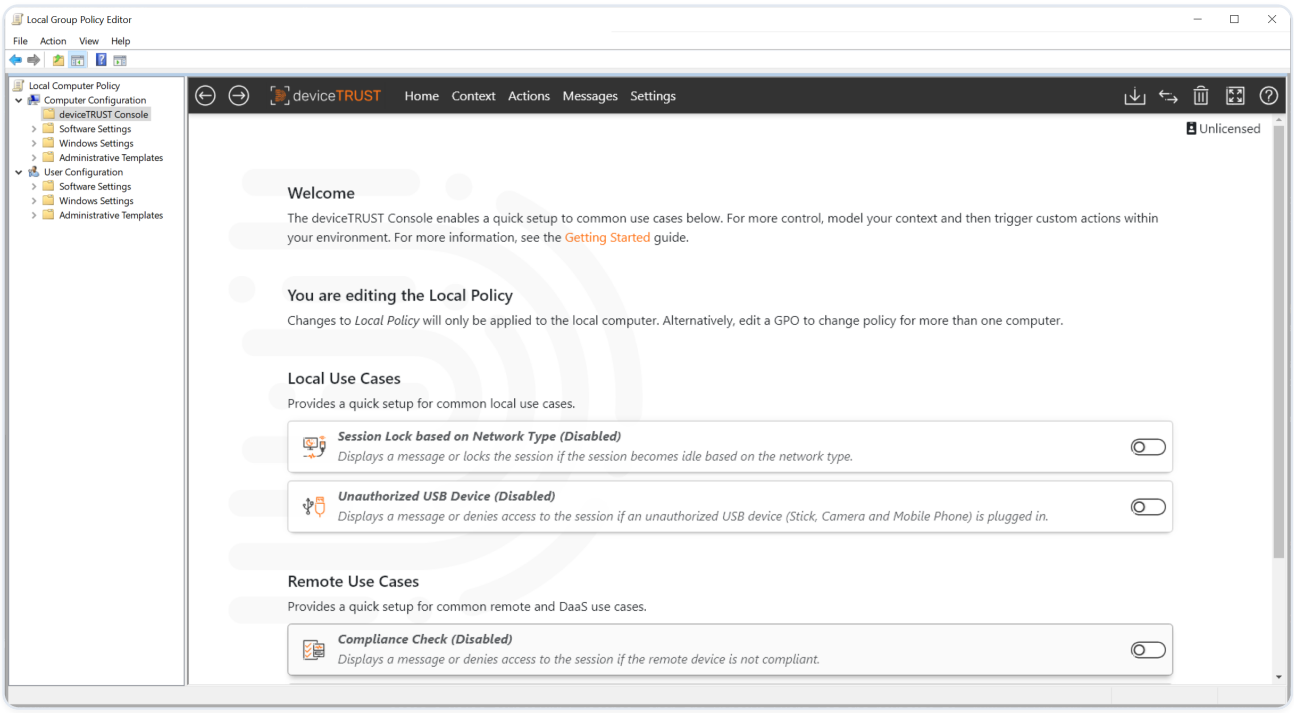
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Install the deviceTRUST Console

To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the contextual security policies to the deviceTRUST Agent. Those options are using the Local Policy Editor, a Group Policy Object (GPO) or file-based.

Within the Getting Started Guide, for simplicity, we use the Local Policy Editor to quickly and efficiently create, edit, and use contextual security policies. Follow the steps in the section Installing the Console to complete the installation.

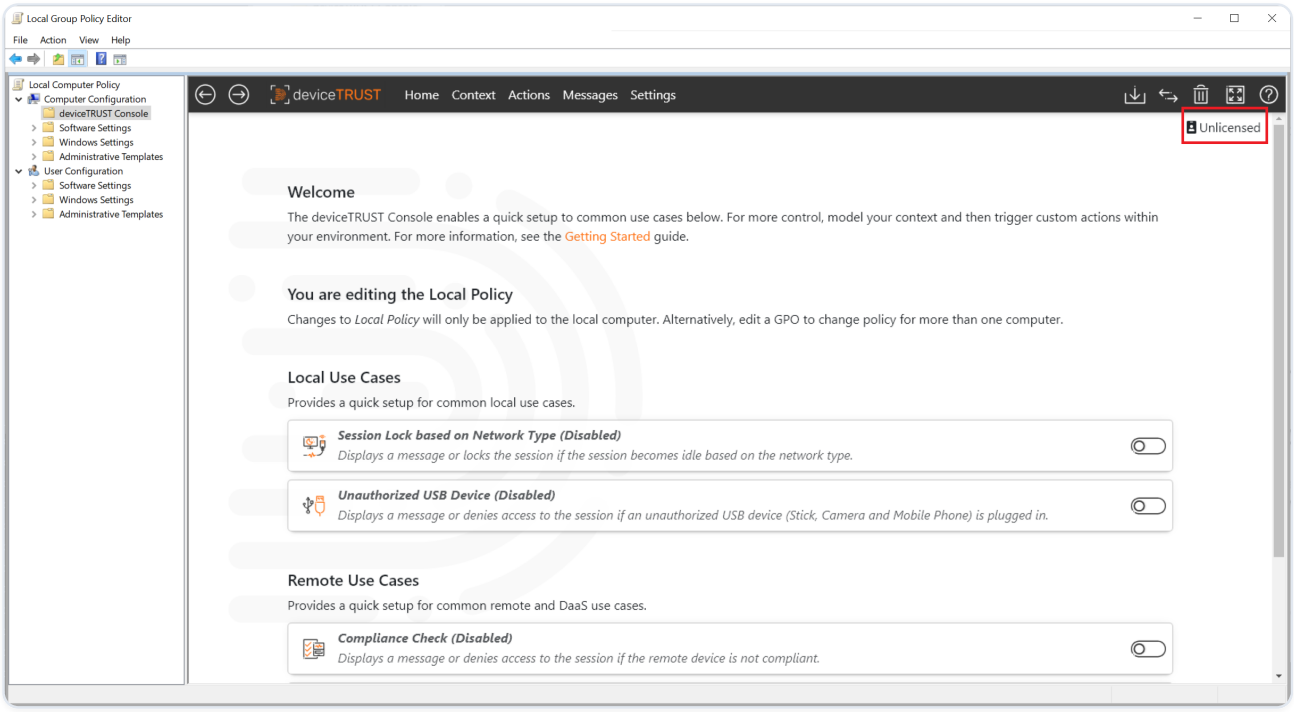
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



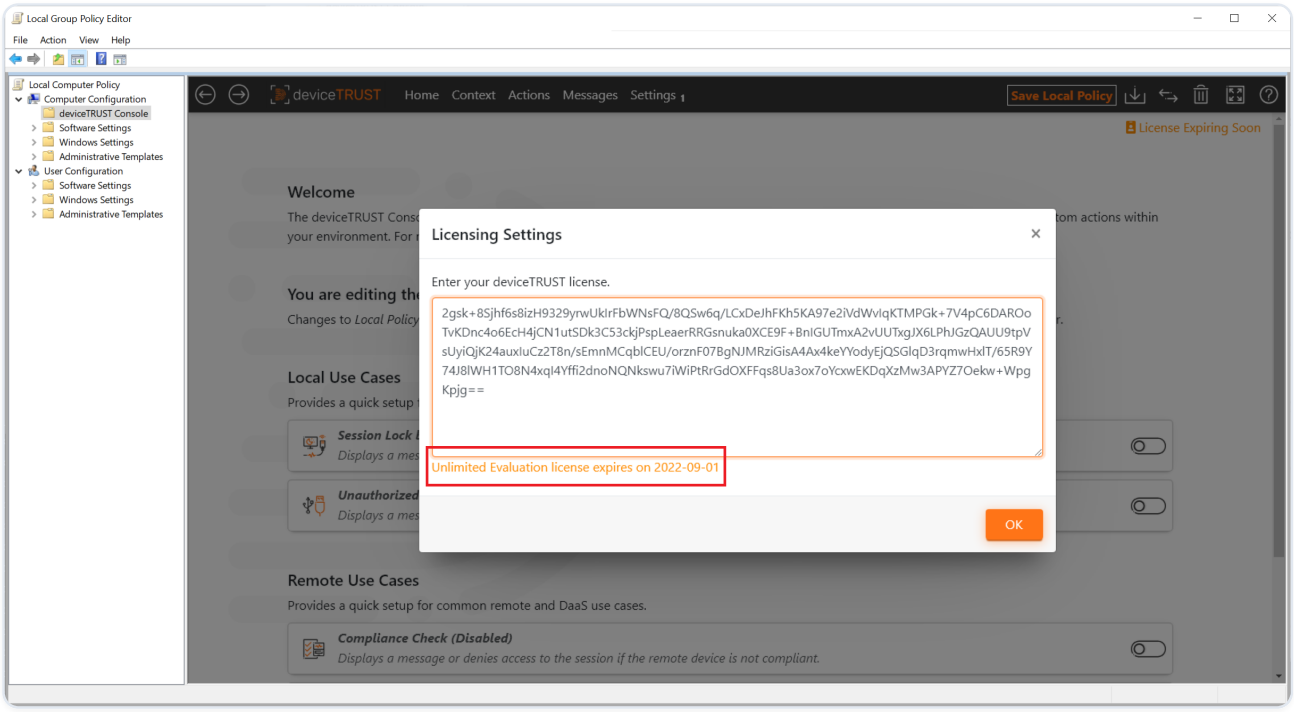
Step 4: Enter your deviceTRUST License

To add the license into the deviceTRUST contextual security policy open the Local Policy Editor and navigate to `DEVICETRUST CONSOLE` and click on the `UNLICENSED` link on the homepage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

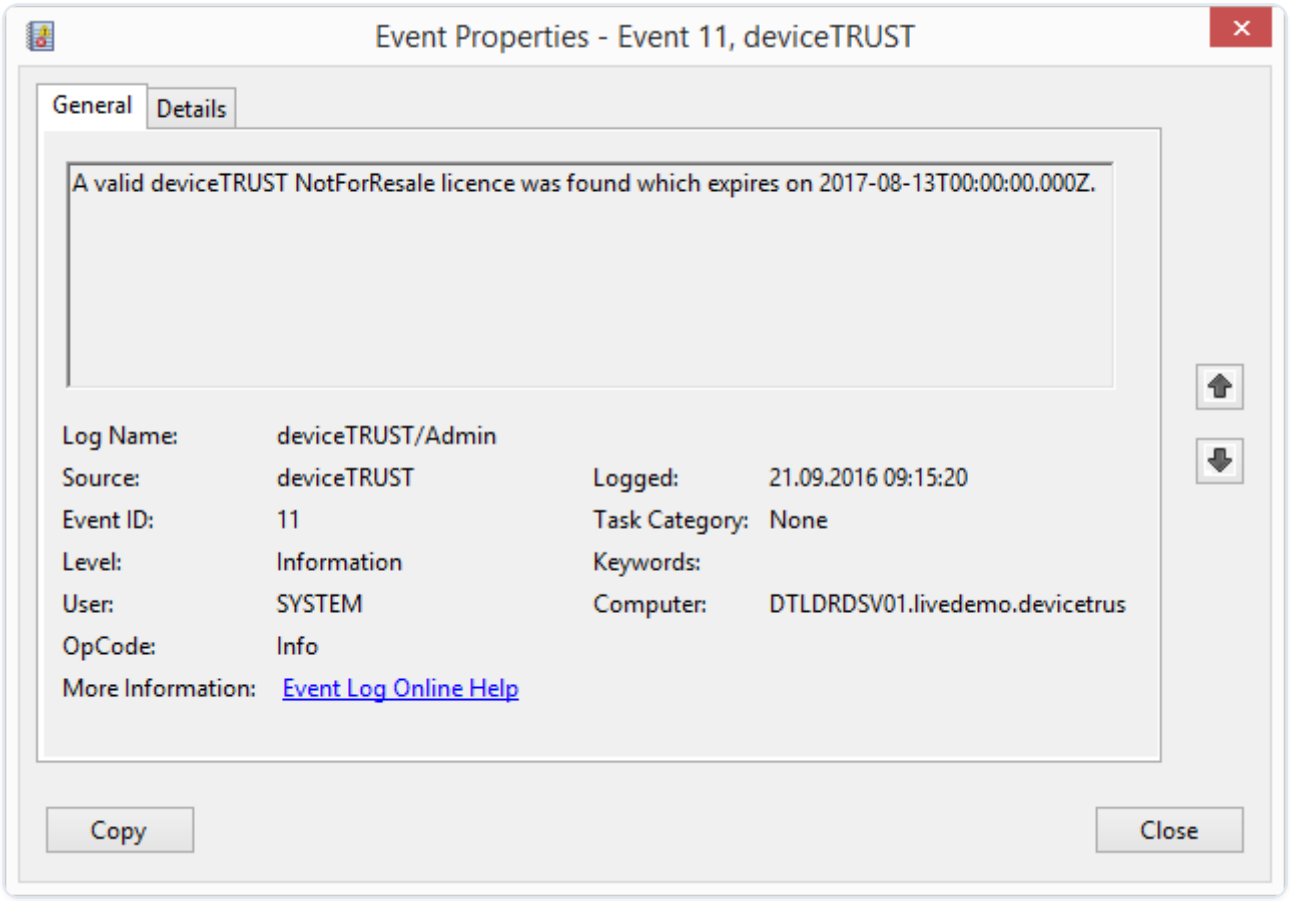


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.



deviceTRUST is now enabled and will work for all users except local administrators connecting to that remoting or DaaS host system with deviceTRUST Agent installed. To check if you have added a valid deviceTRUST license, open the Windows Event Log and navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN` and check for the existence of event ID 11 which states that your deviceTRUST license is valid.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



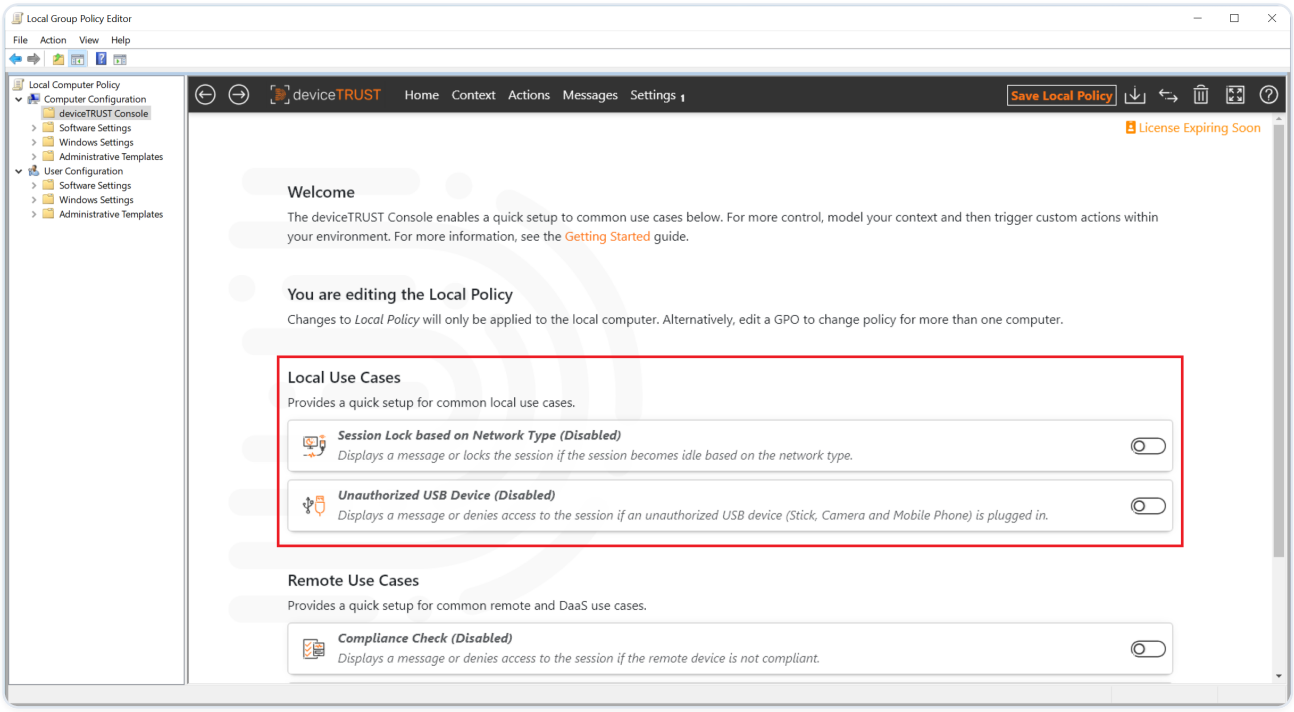
Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device

Within the Getting Started Guide, for simplicity, we will only install the deviceTRUST Client Extension on a Microsoft Windows device. Other device operating systems are also supported and an overview of how to install the deviceTRUST Client Extension on the particular operating system can be found on the Installation Client Extension page. Now follow the steps in the section Installing the Client Extension on Microsoft Windows device to complete the installation.

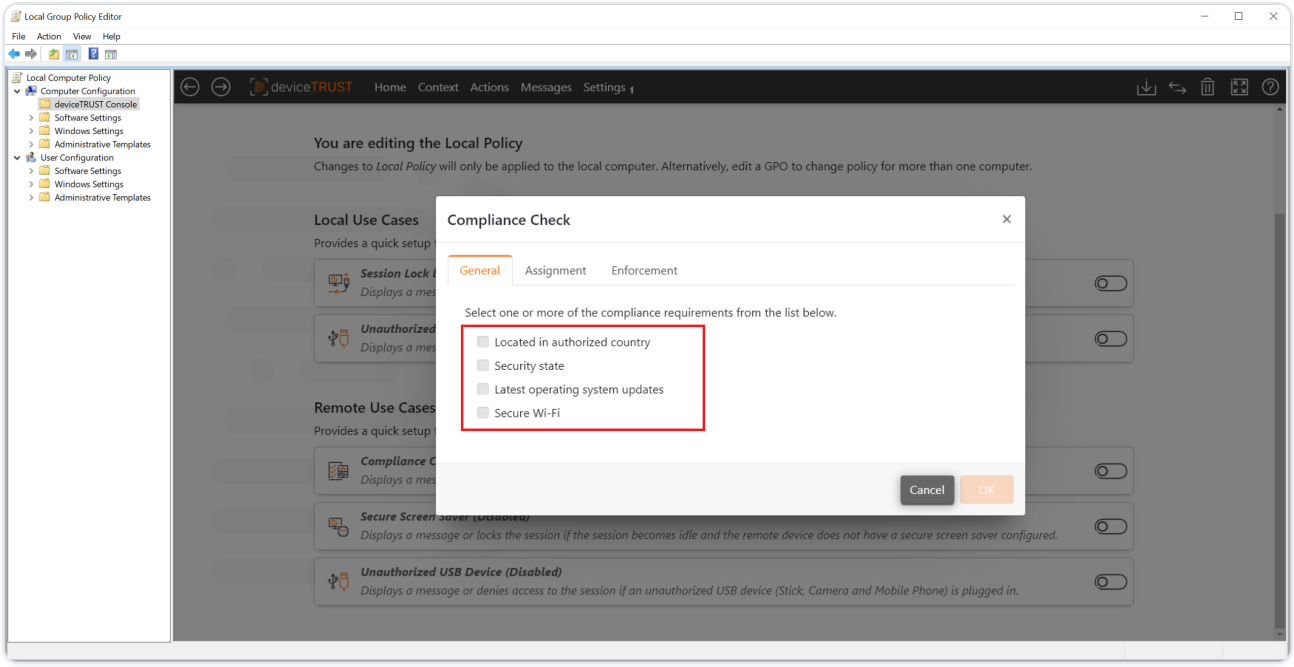
Step 6: Enable the Compliance Check use case

We will use the deviceTRUST Console to create a contextual security policy which controls access to the session depending upon the compliance state of the remote device. The deviceTRUST Console includes a set of use cases which can be used to quickly implement a use case. Launch the deviceTRUST Console and navigate to `REMOTE USE CASES` on the homepage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

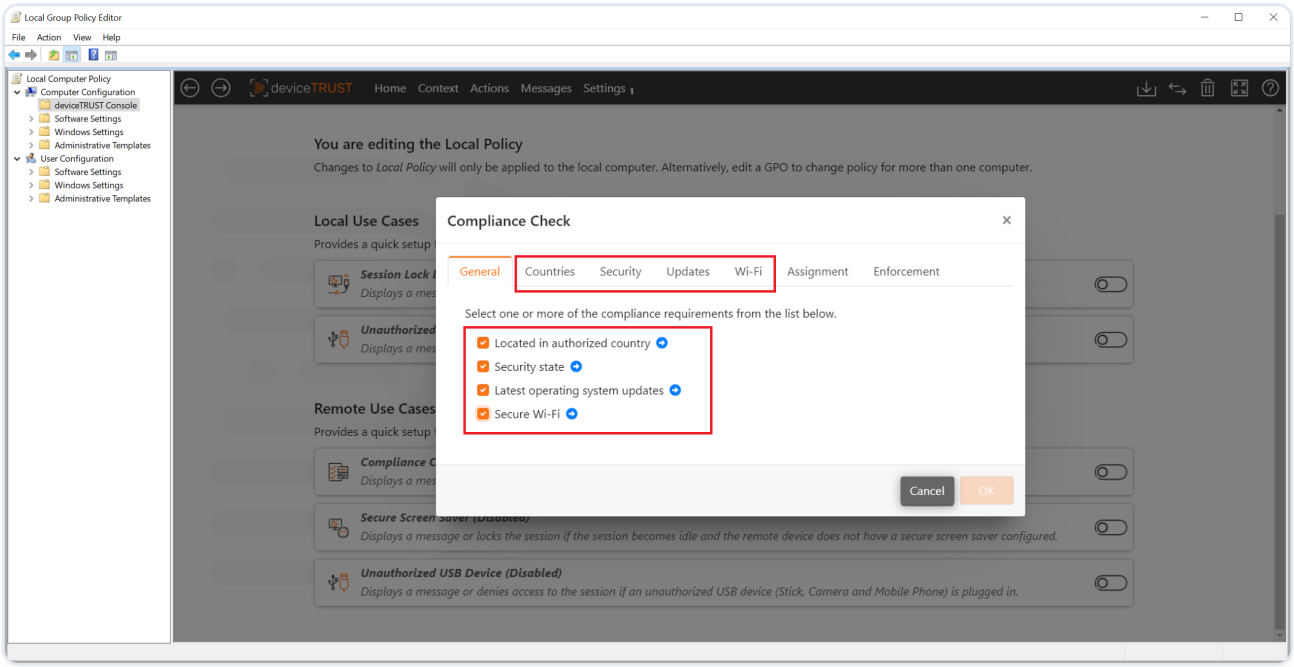


Select the `COMPLIANCE CHECK` use case, select on the `GENERAL` tab all options to be included in the compliance check.

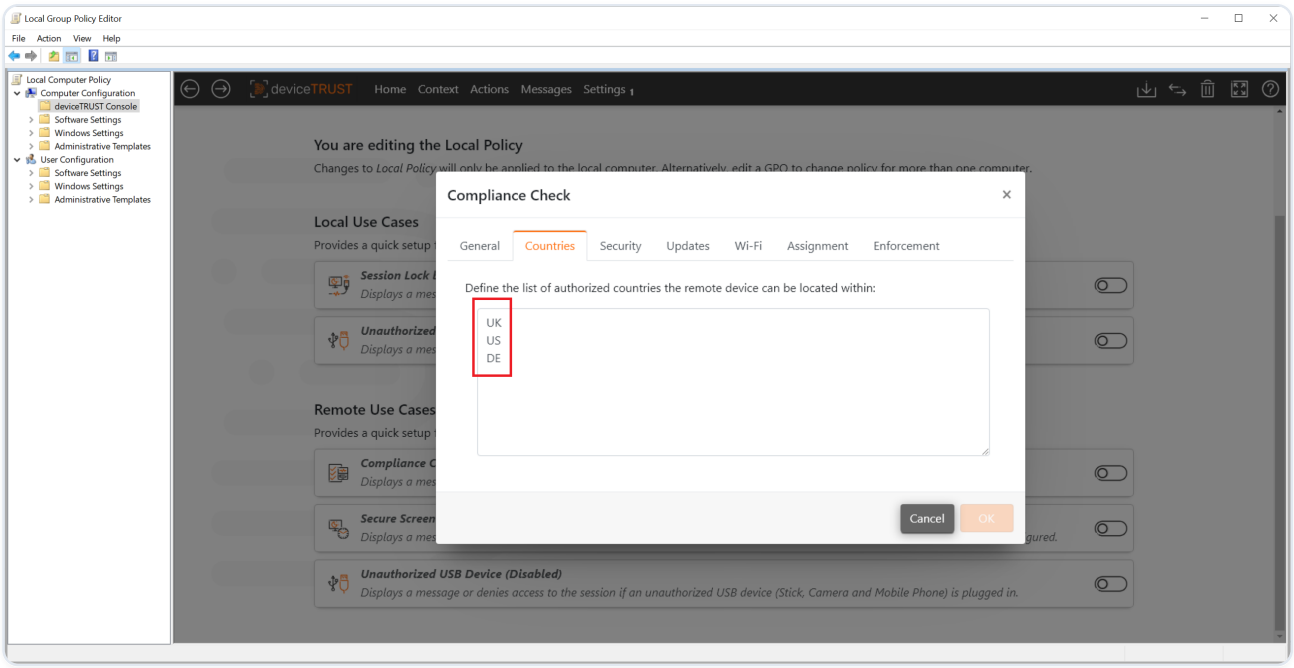


New configuration tabs will become visible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

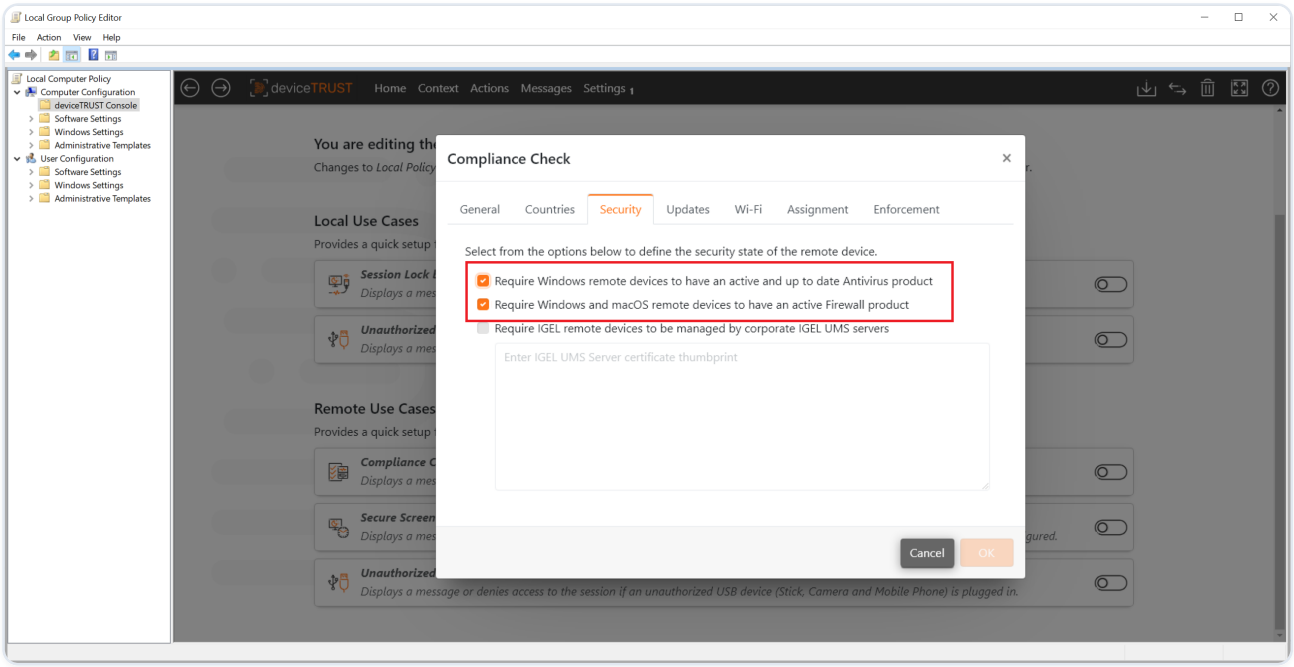


Click on the `COUNTRY` configuration tab and add all authorized countries using ISO 3166-1 Alpha-2 code.

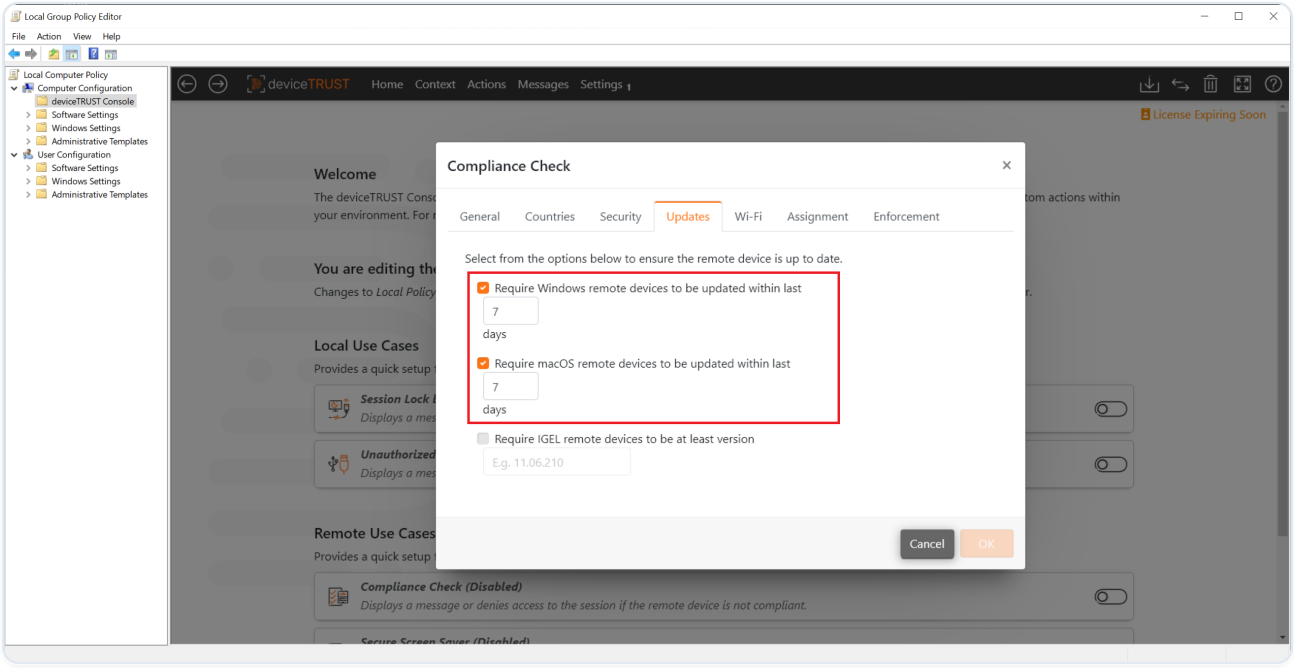


Click on the `SECURITY` configuration tab and enable the `REQUIRE WINDOWS REMOTE DEVICES TO HAVE AN ACTIVE AND UP TO DATE ANTIVIRUS PRODUCT` and `REQUIRE WINDOWS AND MACOS REMOTE DEVICES TO HAVE AN ACTIVE FIREWALL PRODUCT` options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

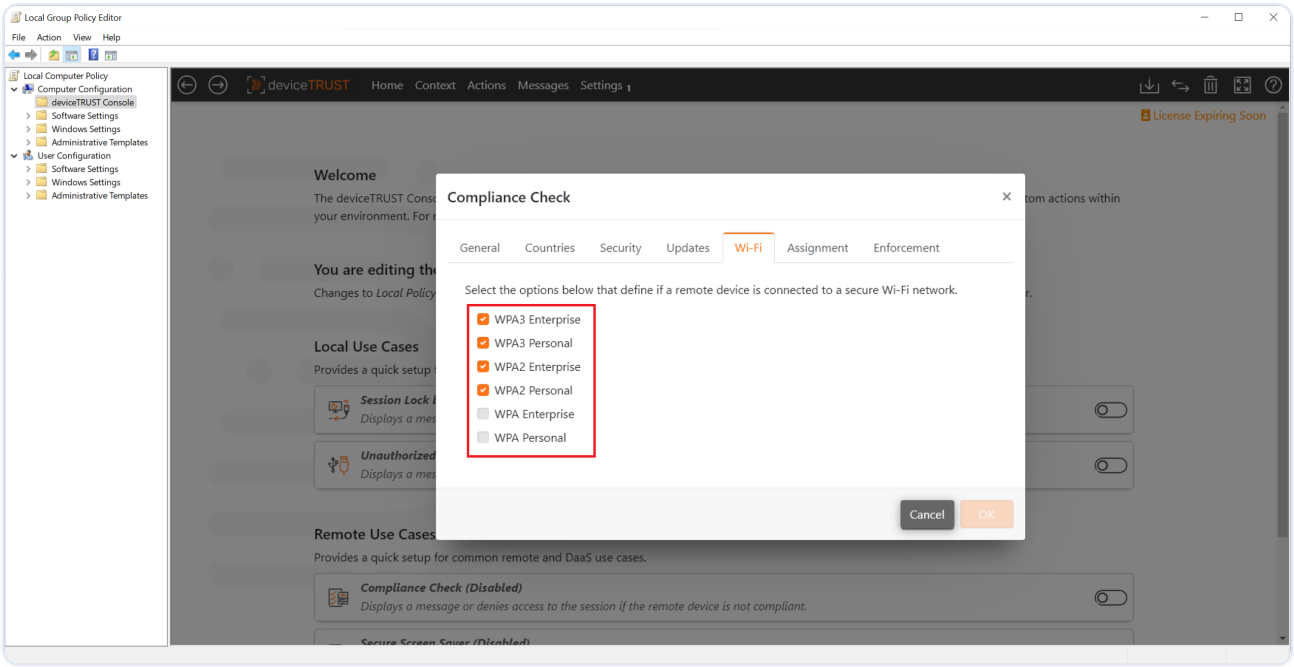


Click on the `UPDATES` configuration tab and enable the `REQUIRE WINDOWS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` and `REQUIRE MACOS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` options.

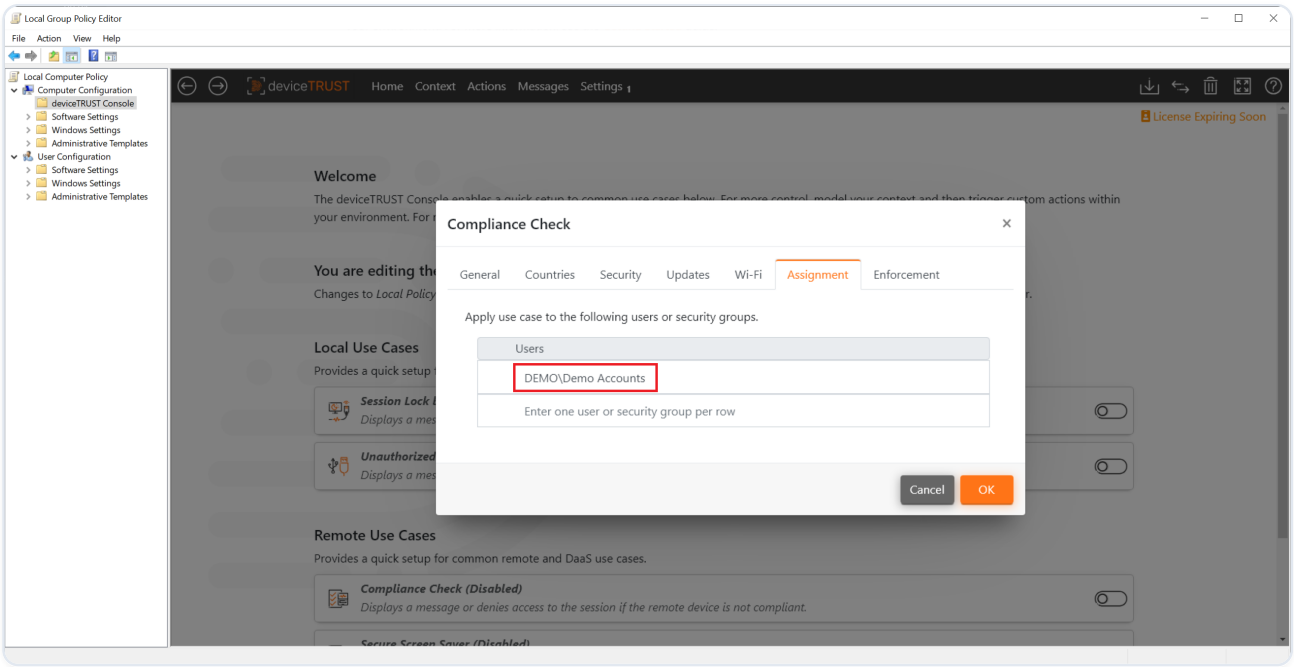


Click on the `WI-FI` configuration tab and enable the `WPA3 ENTERPRISE`, `WPA3 PERSONAL`, `WPA2 ENTERPRISE` and `WPA2 PERSONAL` options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

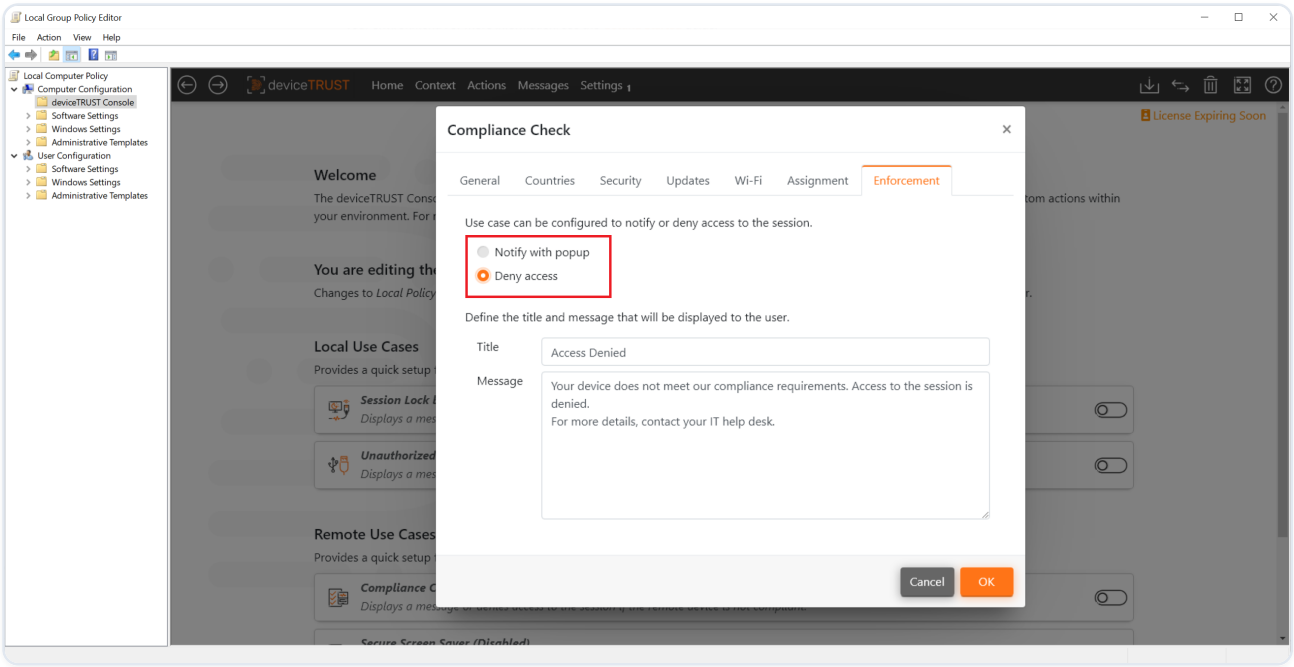


Click on the `ASSIGNMENT` configuration tab and add `USERS` and / or `SECURITY GROUPS` to apply the use case for.

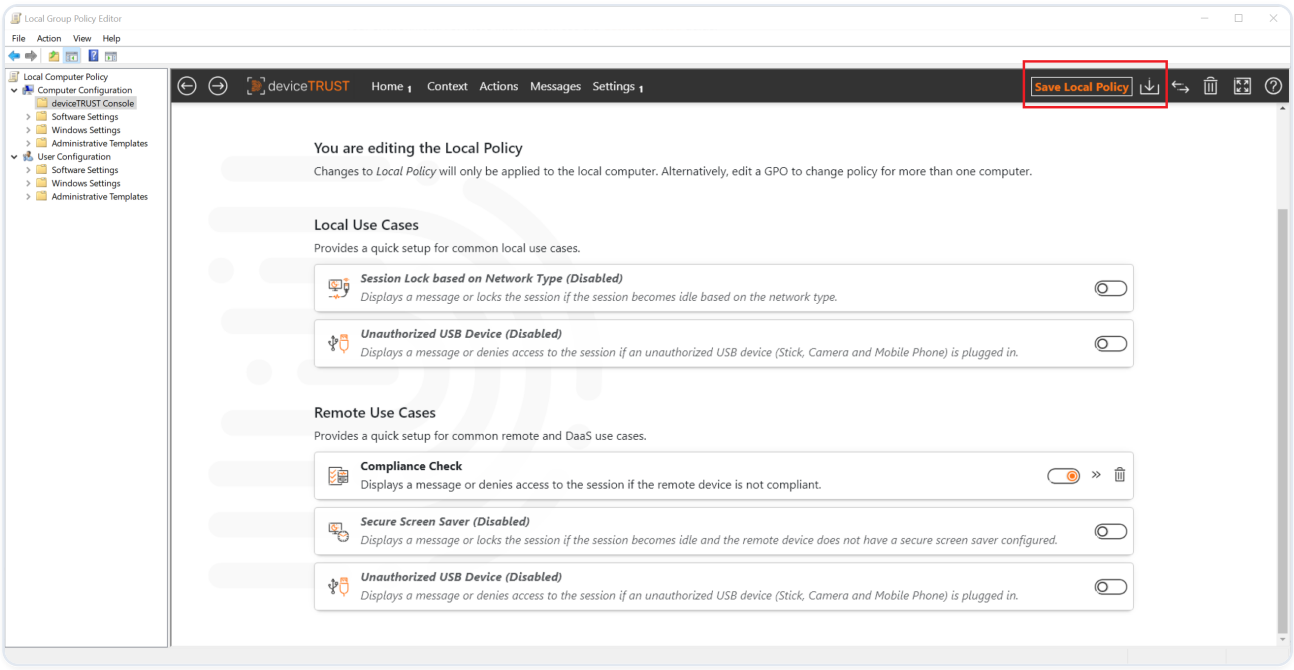


Click on the `ENFORCEMENT` configuration tab and select `DENY ACCESS`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



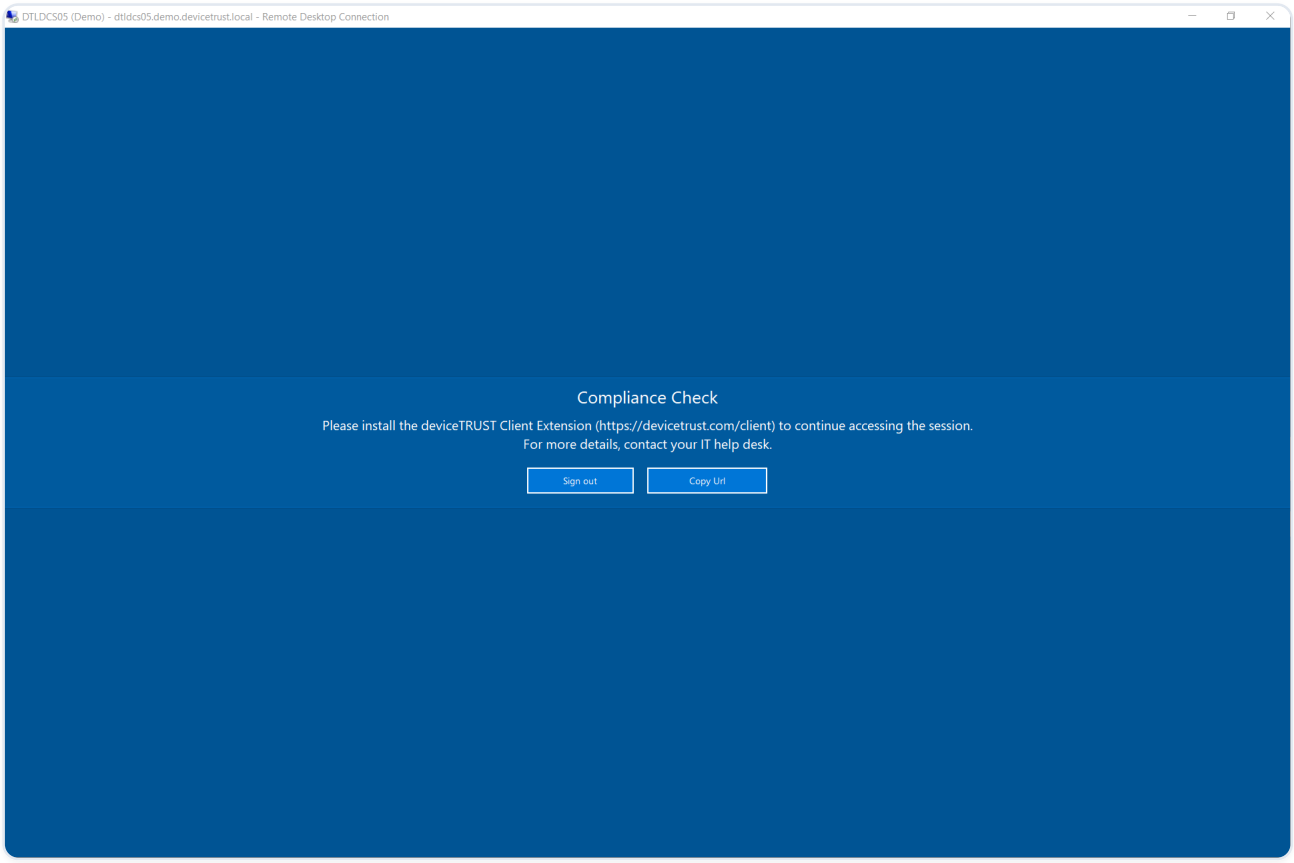
Click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar to save the complianc check use case to the local computer policy.



Step 7: Check that access is denied when the deviceTRUST Client Extension is not installed

From a device without the deviceTRUST Client Extension installed, connect to your remoting or DaaS host system. Because the remote device does not have an active deviceTRUST Client Extension, the access will be denied with the following message:

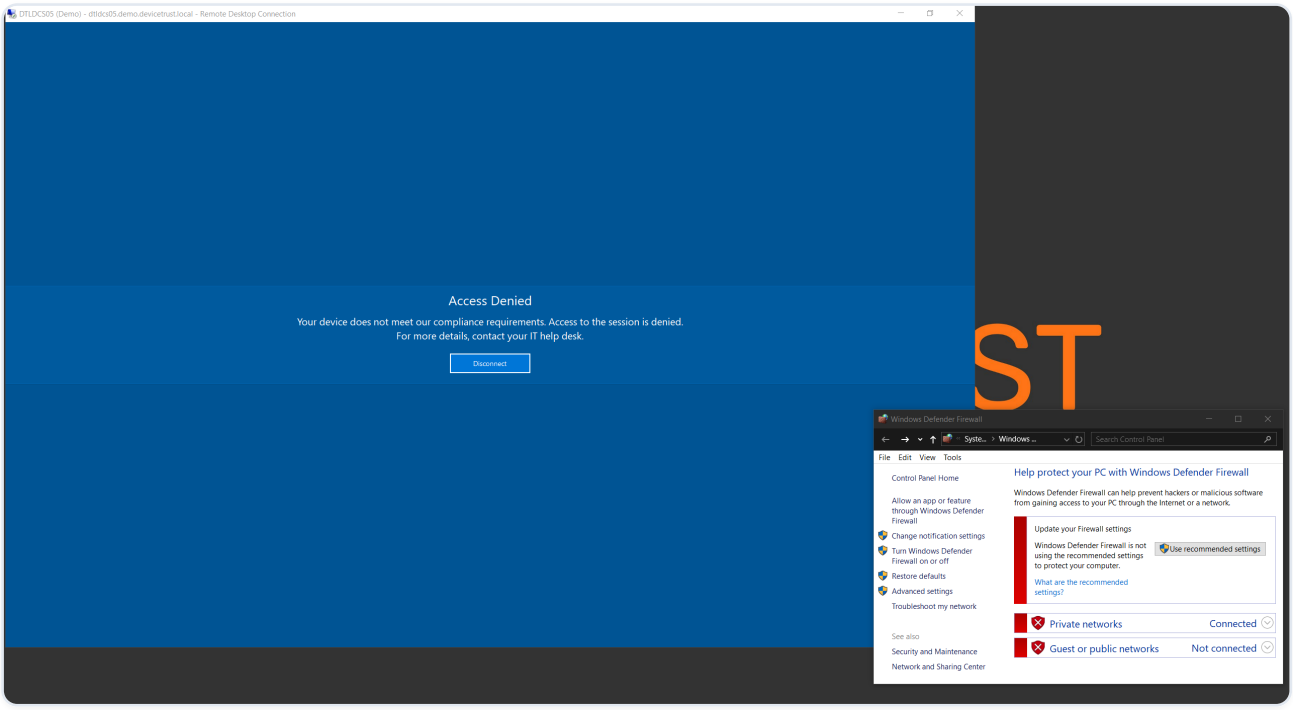
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 8: Test the Compliance Check use case from a Microsoft Windows device

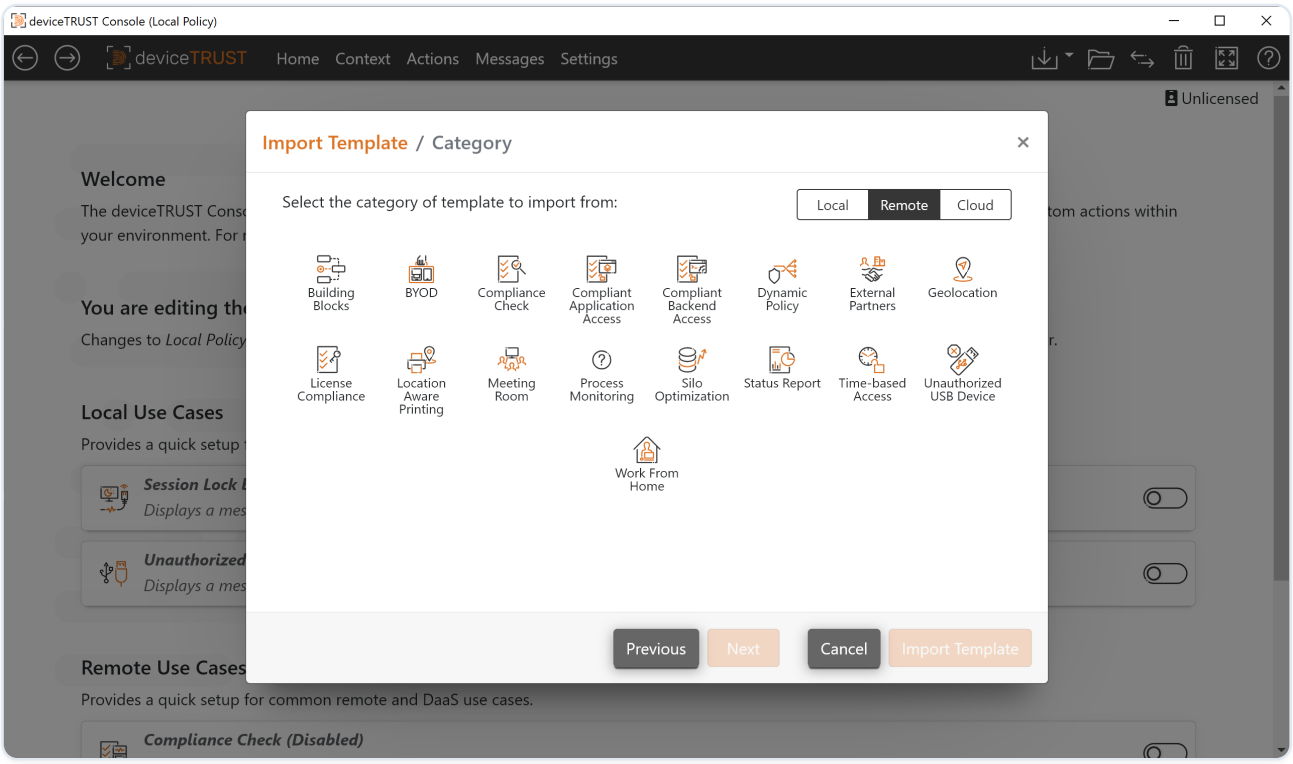
From a Microsoft Windows device with the deviceTRUST Client Extension installed, connect to your remoting or DaaS host system. Toggle the state of the Windows Defender Firewall to see how deviceTRUST can simply and dynamically control access to the session depending on the firewall state of the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Next steps

You have now successfully implemented your first use case with deviceTRUST for your remoting and DaaS environment. Feel free to check out our additional use cases provided on the deviceTRUST Console homepage under `REMOTE USE CASES`. In addition, the deviceTRUST Console gives you access to many more configuration Templates for a wide variety of use cases.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Download deviceTRUST 23.1 for Windows

The latest deviceTRUST 23.1 binaries, including the deviceTRUST Agent, Console and Client Extension can be downloaded from the link below:

Version	23.1.410
Release Date	21st October 2024
URL	https://storage.devicetrust.com/download/deviceTRUST-23.1.410.zip
SHA256 Hash	04F5F434178FBE97D25F965A5F29239FF4EB117F04A5140C9D8F7F07F45E47C0

Previous releases of these components can be downloaded download.

Download deviceTRUST® Client Extensions

The latest client extensions for Microsoft Windows, Apple macOS and Ubuntu can be download by end users from thedeviceTRUST Client Extension Download page.

The latest client extensions for IGEL OS and Unicon™ eLux are built into the respective products.

The latest Stratodesk NoTouch OS client extension can be found below:

Version	23.1.100
Release Date	19th May 2023
NoTouch Citrix URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient_ica.so
NoTouch Citrix SHA256	B5AF15C3338646A62EA4090AEB41C2DD2609B7B9228085C6B0DF7B90567A3C62

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NoTouch RDP URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient_rdp.so
NoTouch RDP SHA256	1E4F5DF9ABBA115BF9E0FD62A7EDA54C46C8C47ABE9EC12B737B4BA3CE40801D
NoTouch VMware URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient_vmware.so
NoTouch VMware SHA256	27B80D37F28DC90727560527FD04BDA56F33C919EEE17C9E860D593D04707E34

NOTE:

```
deviceTRUST may change these urls in the future. To ensure you don't
experience any downtime you should copy these files and host them within
your own environment.
```

Software components

After downloading the deviceTRUST software, you will find the following components:

COMPONENT	DESCRIPTION
DTAGENT-X64-RELEASE-x.x.x.x.MSI	The deviceTRUST Agent installer.
DTCLIENT-EXTENSION-RELEASE-x.x.x.x.EXE	The deviceTRUST Client Extension installer.
DTCONSOLE-X64-RELEASE-x.x.x.x.MSI	The deviceTRUST Console installer.
DTPOLICYDEFINITIONS-x.x.x.x.ZIP	The deviceTRUST ADMX policy definitions for configuring legacy options in the software from Microsoft Active Directory Group Policy (GPO).

NOTE:

deviceTRUST Agent, Console and Client Extension components require administrative privileges for the installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

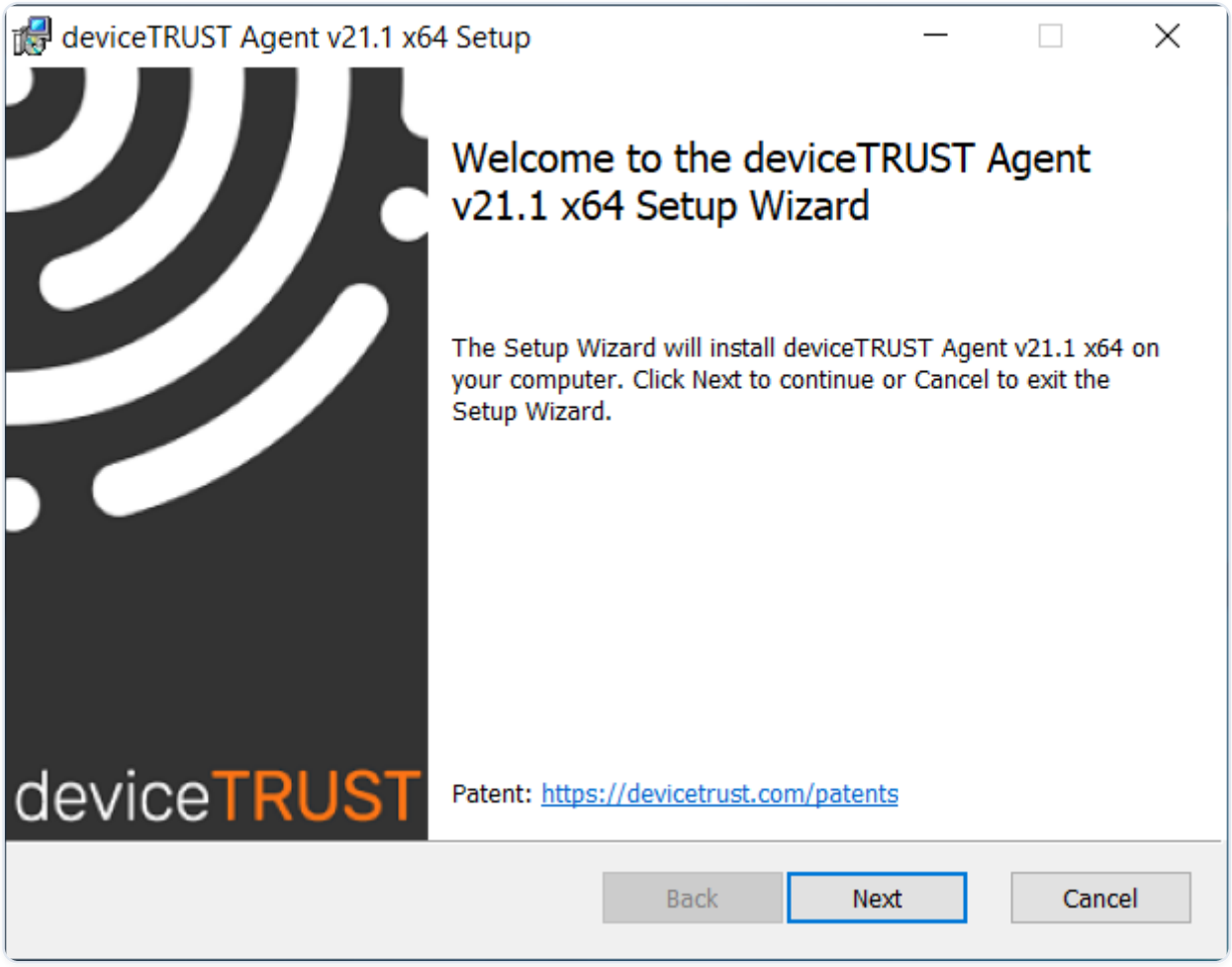
Installation

TABLE OF CONTENTS

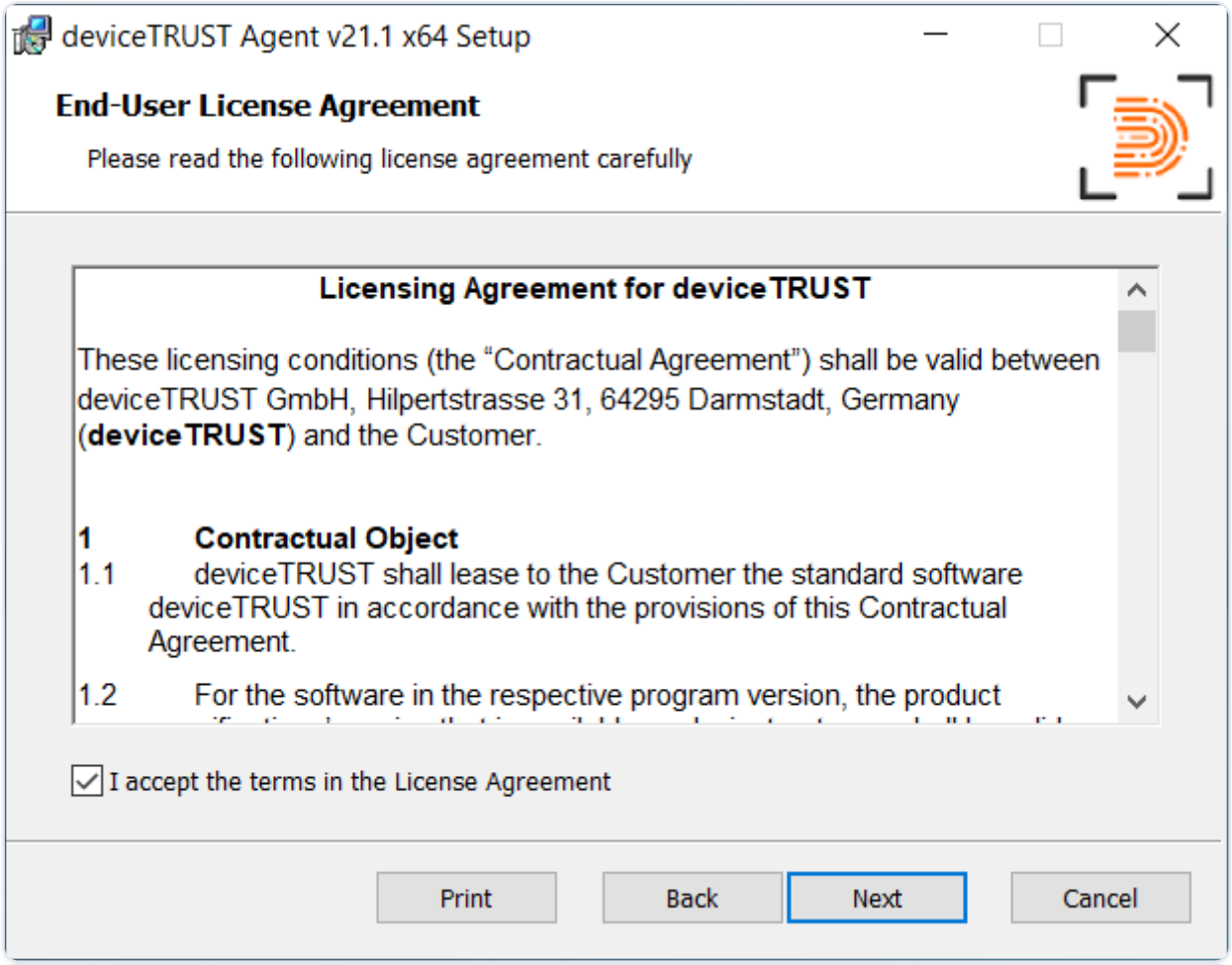
- Agent
- Console
- Client Extension

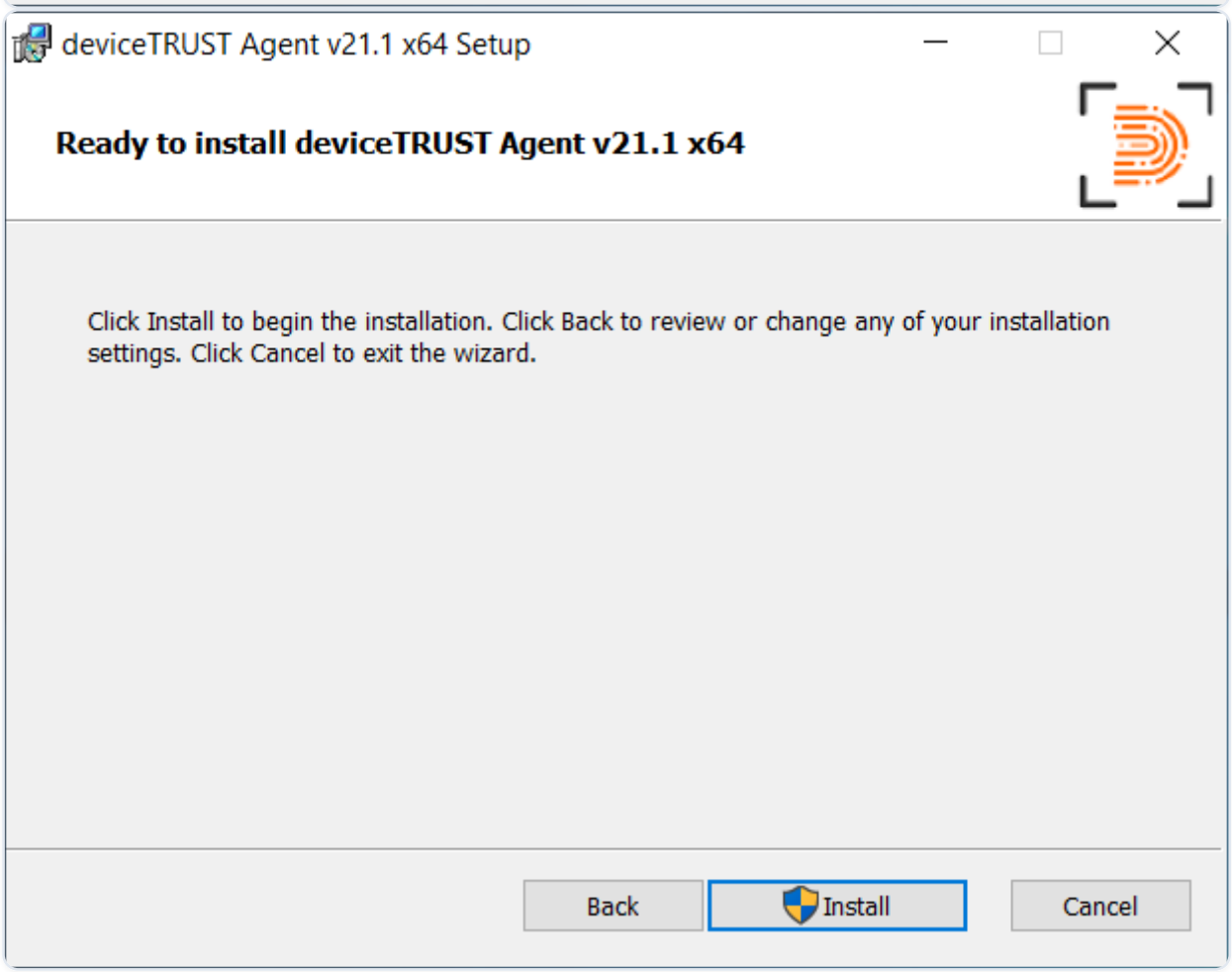
Installing the deviceTRUST® Agent

The deviceTRUST Agent requires a user account with local administrative privileges to install the deviceTRUST Agent on the target system. The installation can be performed by following the steps of the deviceTRUST Agent installer.

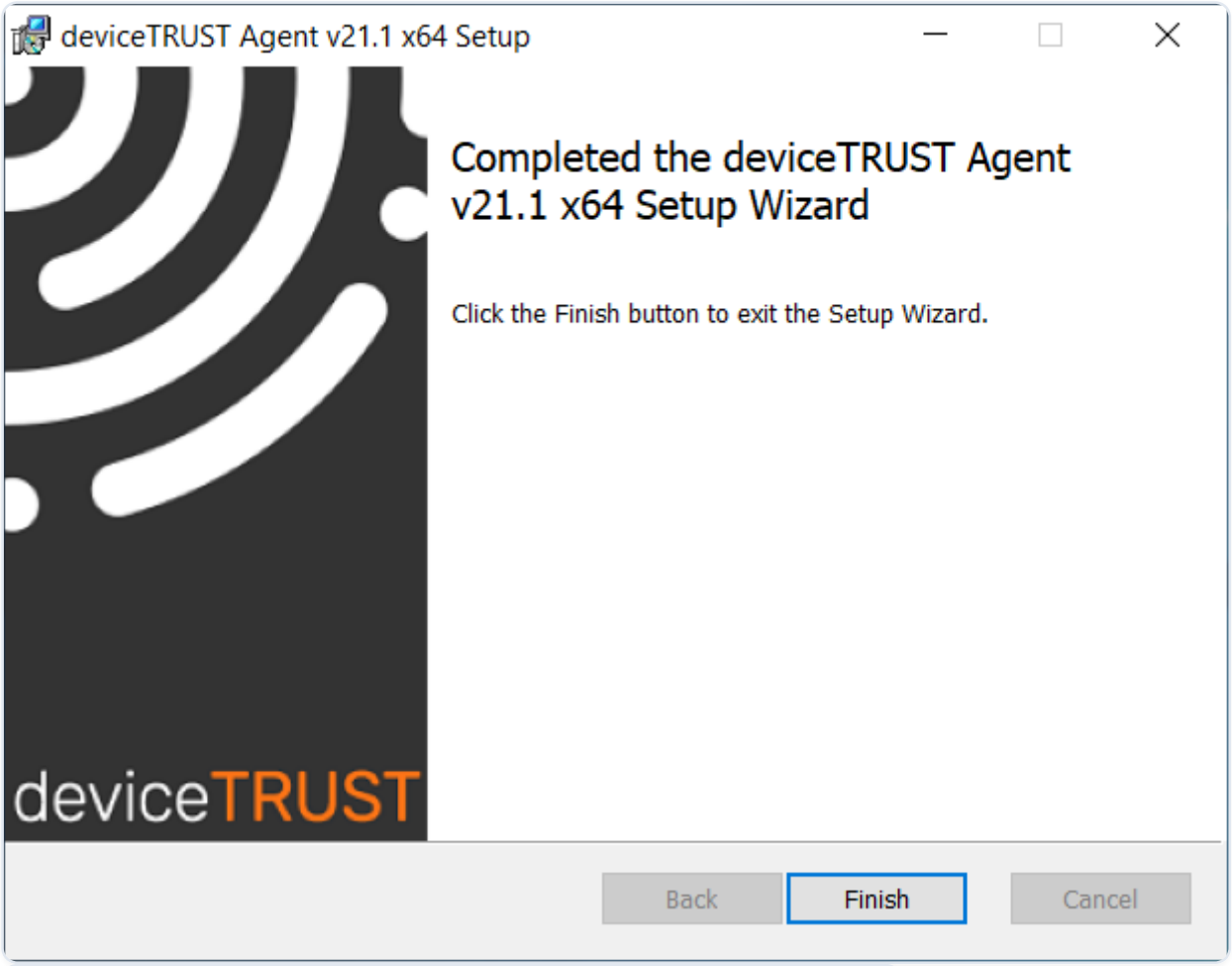


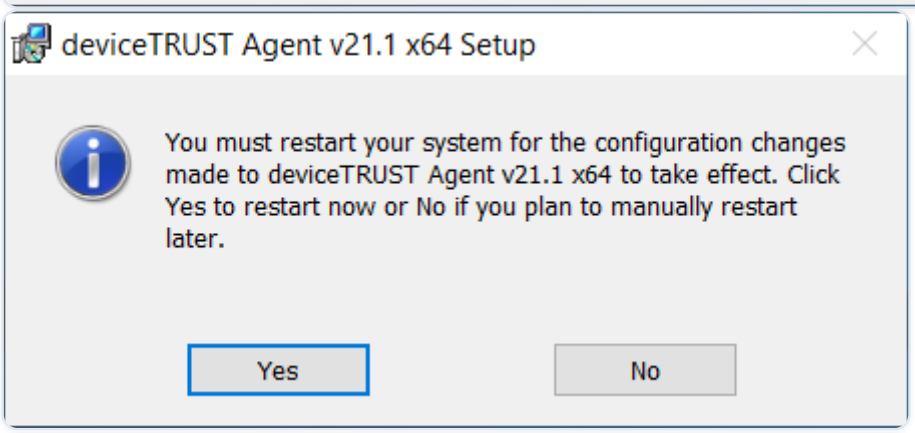
© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.





NOTE:

Installation path: %PROGRAMFILES%\DEVICETRUST\AGENT

If the installation of the deviceTRUST Agent has finished successfully, a reboot is required to enable deviceTRUST to get system notifications to act on.

If the *Remote Desktop Services* server role is added after installing the deviceTRUST Agent, the deviceTRUST Agent will need to be reinstalled.

The deviceTRUST Agent will not function until a valid license is applied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Channel Security

When using Citrix Virtual Apps and Desktops, you may need to edit the `Virtual channel allow list` policy to allow the deviceTRUST Agent to open a virtual channel to the deviceTRUST Client. More details can be found on the Knowledge Base.

Unattended Installation

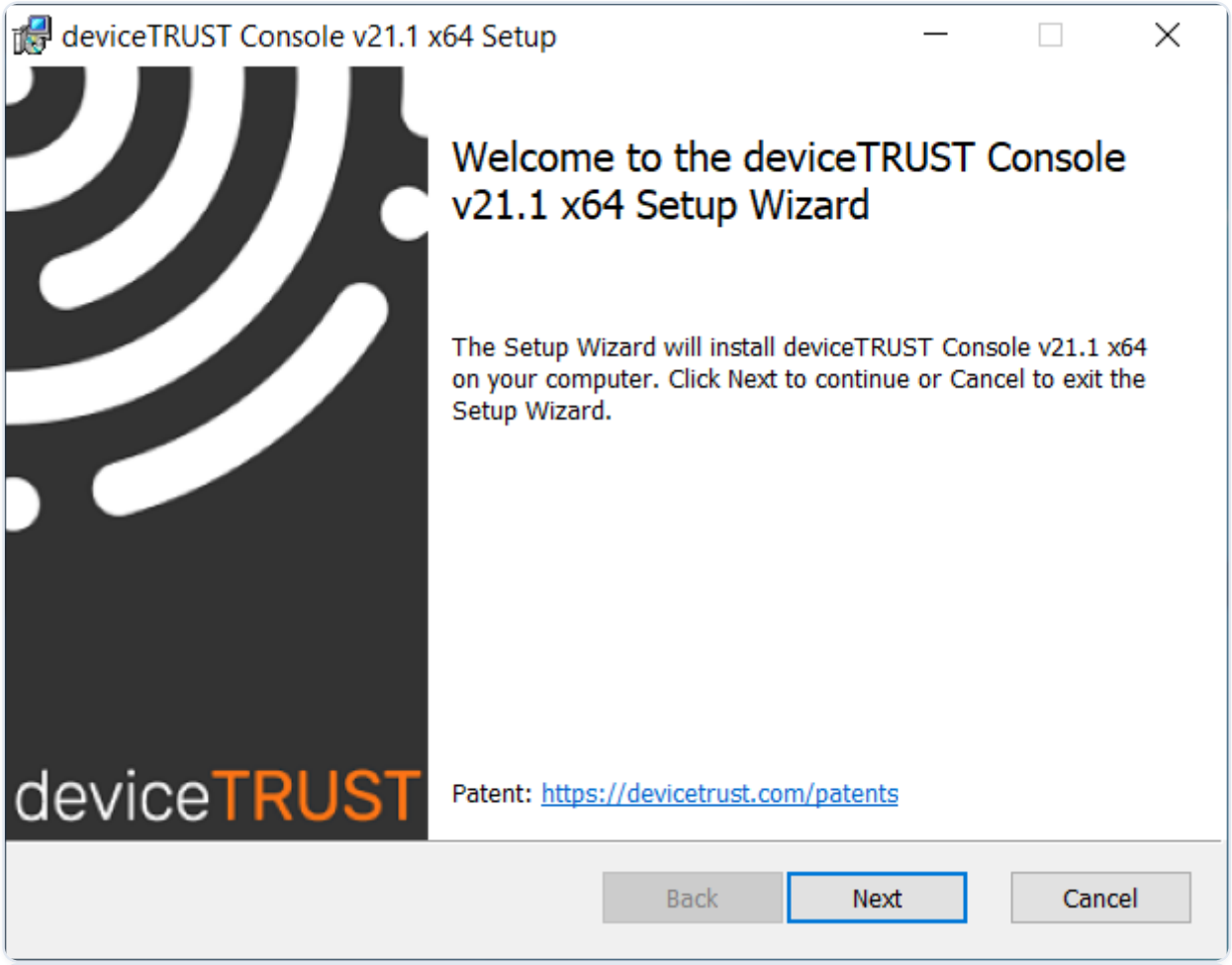
The deviceTRUST Agent can be installed unattended from the command line interface with the following options:

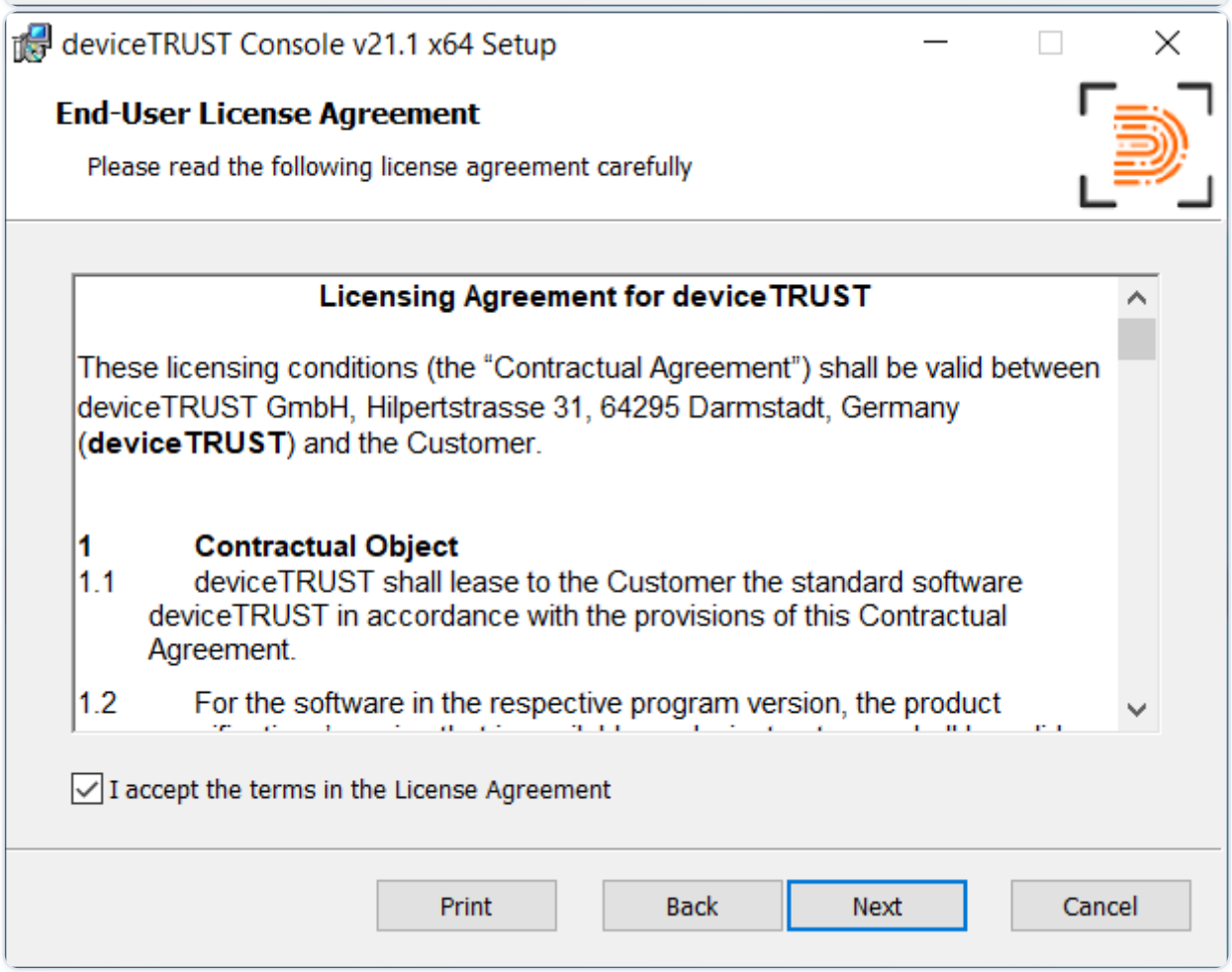
COMPONENT	COMMANDLINE	
dtagent-x64-release-x.x.x.x.msi	The deviceTRUST Agent installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters `MSIEXEC.EXE /I DTAGENT-X64-RELEASE-X.X.X.X.MSI /PASSIVE /FORCERESTART`	

Installing the deviceTRUST® Console

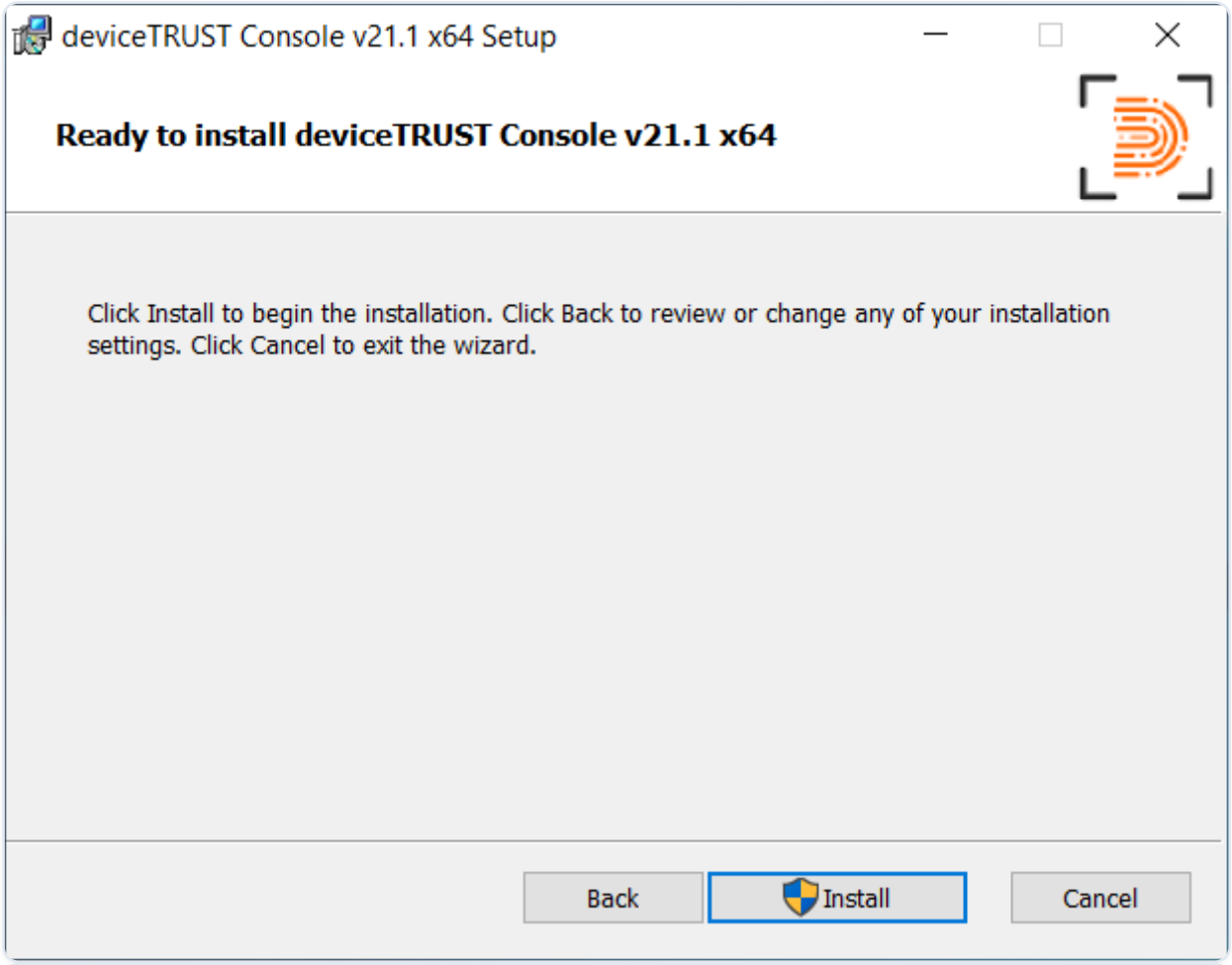
The deviceTRUST Console requires a user account with local administrative privileges to install the deviceTRUST Console on the targeting system. The installation can be performed by following the steps of the deviceTRUST Console installer.

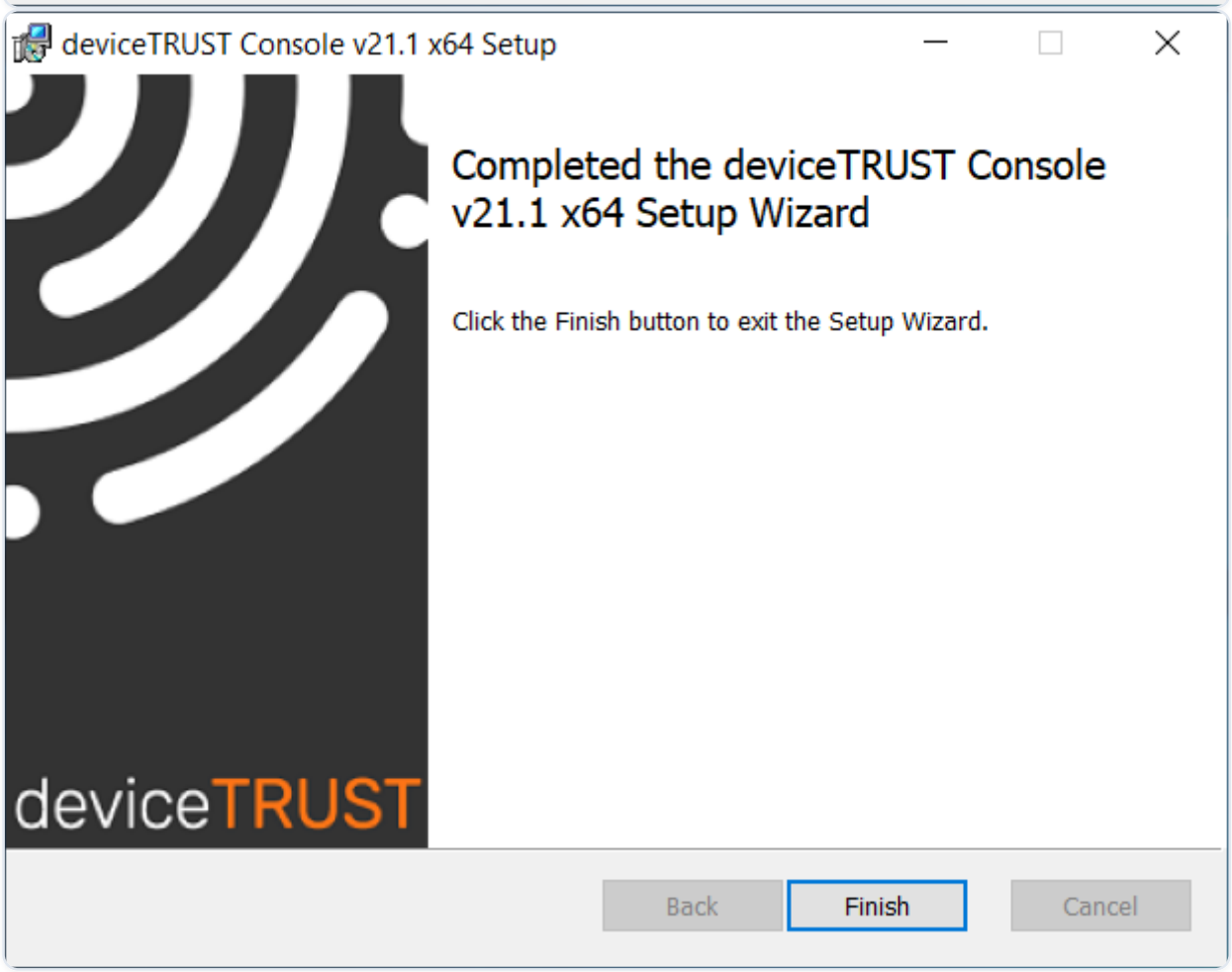
© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Installation path: `%PROGRAMFILES%\DEVICETRUST\CONSOLE`

Unattended Installation

The deviceTRUST Console can be installed unattended from the command line interface with the following options:

COMPONENT	COMMANDLINE	
dtconsole-x64-release-x.x.x.x.msi	The deviceTRUST Console installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters `MSIEXEC.EXE /I DTCONSOLE-X64-RELEASE-X.X.X.X.MSI /PASSIVE`	

Installing the deviceTRUST® Client Extension

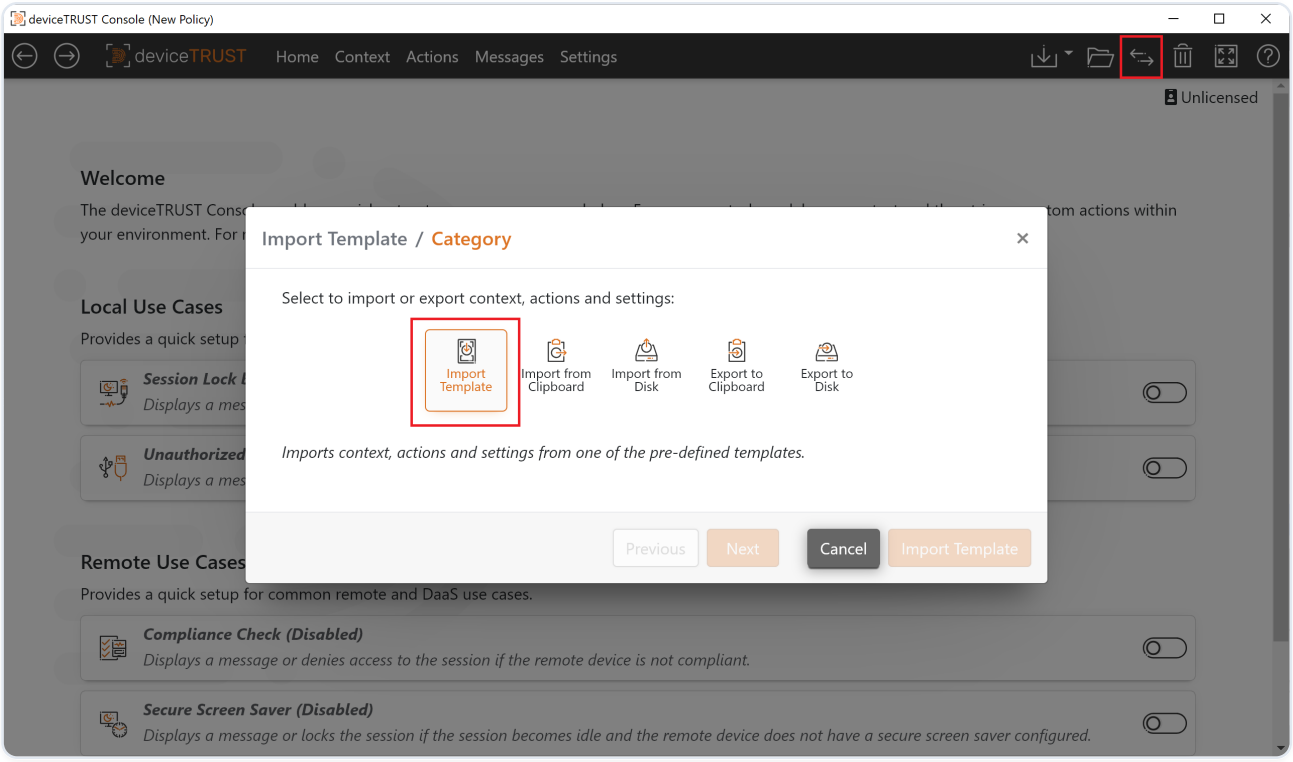
TABLE OF CONTENTS

- Microsoft Windows
- Apple macOS
- Apple iOS and iPadOS
- Ubuntu
- IGEL OS
- Stratodesk NoTouch OS
- Unicon eLux RP6

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Templates

The deviceTRUST® Console includes a set of templates which can be used to quickly implement a use case. Launch the deviceTRUST Console and select **SHARING** in the top right of the navigation bar, then choose **IMPORT TEMPLATE**.



The deviceTRUST use cases are summarized in the following categories for each target platform. Use the filter to select the desired target platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

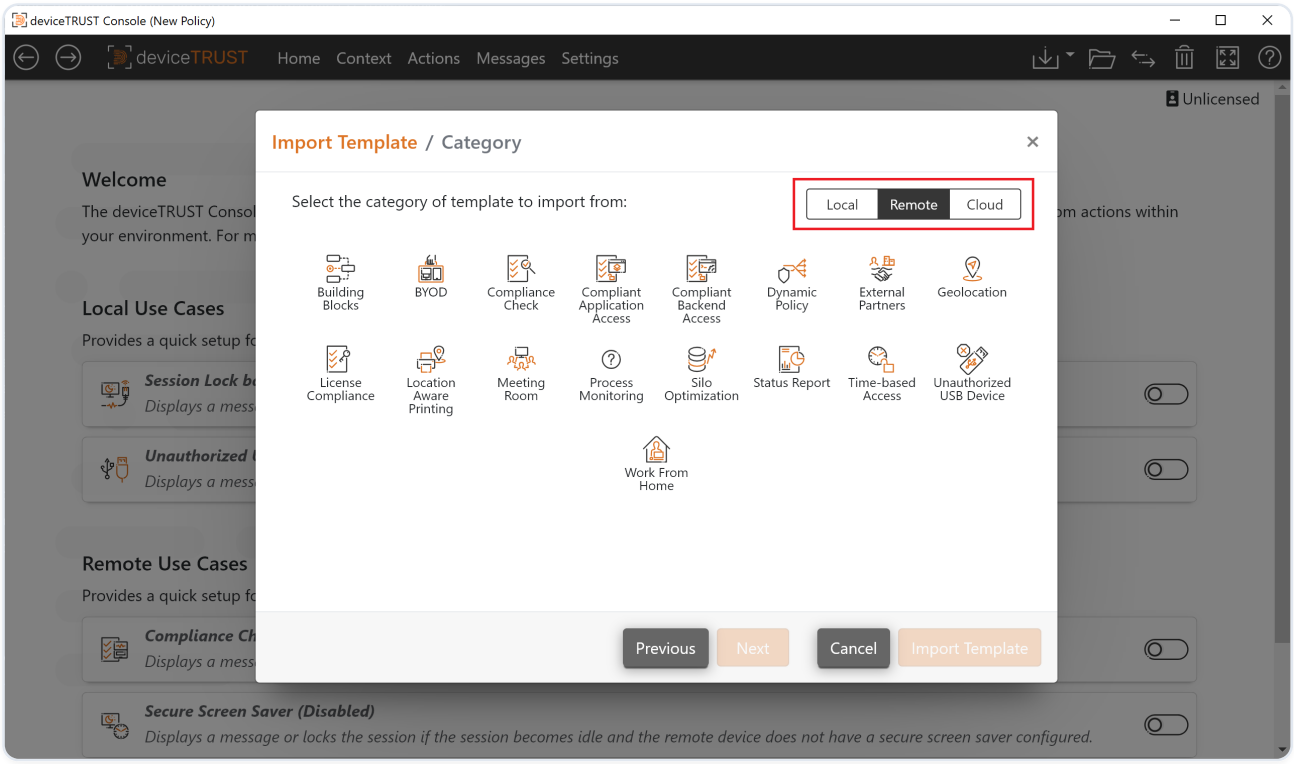


Table of Contents

- Local - Local Templates
- Remote - Remote Templates
- SaaS - SaaS Templates

Local Templates

The deviceTRUST® use cases for local devices are summarized within the following categories.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

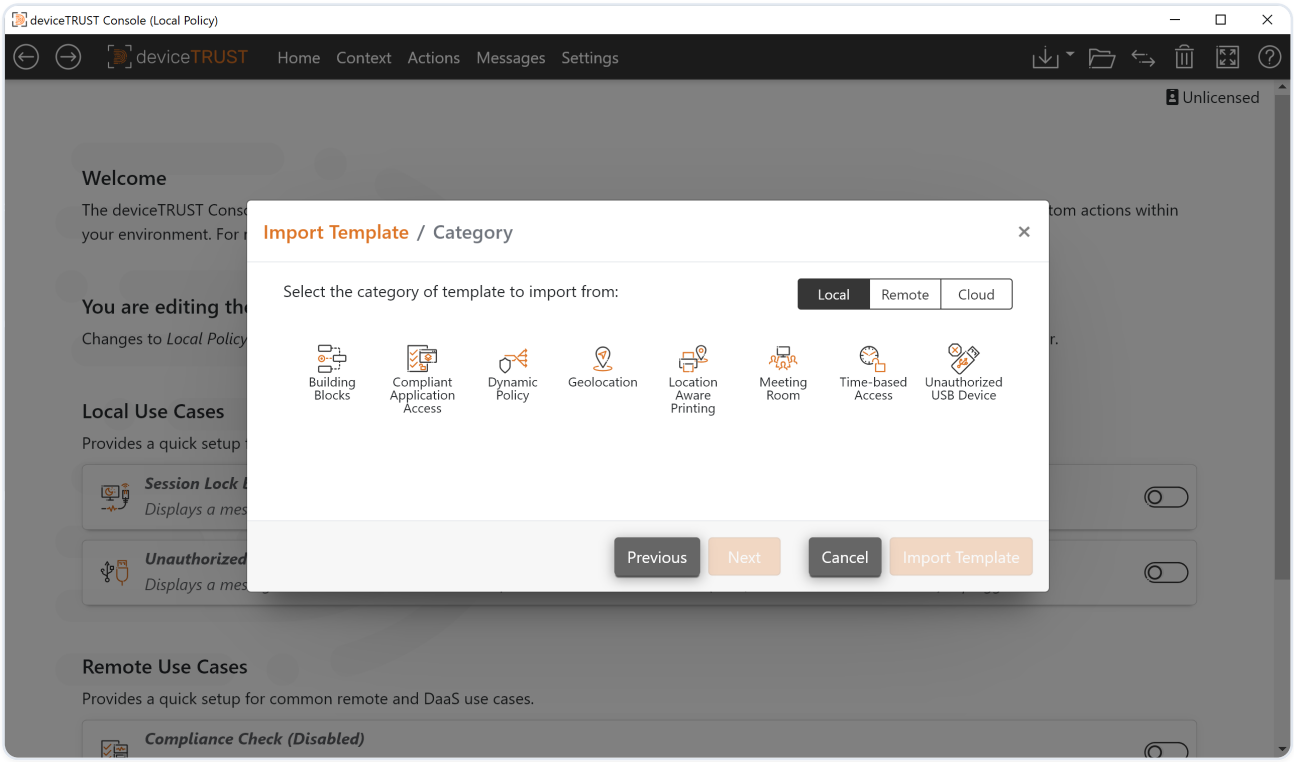


Table of Contents

- Building Blocks - Individual contexts and actions that can be used as building blocks within your configuration.
- Compliant Application Access - Controls access to applications within the session.
- Dynamic Policy - Applies a dynamic policy within the session.
- Geolocation - Validates and controls access based on geolocation information of the local device.
- Location Aware Printing - Maps network printers and defines a default printer based on the device placement within a building.
- Status Report - Reports the status of the local device to various destinations.
- Time-based Access - Controls access to the session or applications when accessed outside of working hours.
- Unauthorized USB Device - Denies access to the session when an unauthorized USB device is plugged in.

Remote Templates

The deviceTRUST® use cases for remoting and DaaS are summarized within the following categories.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

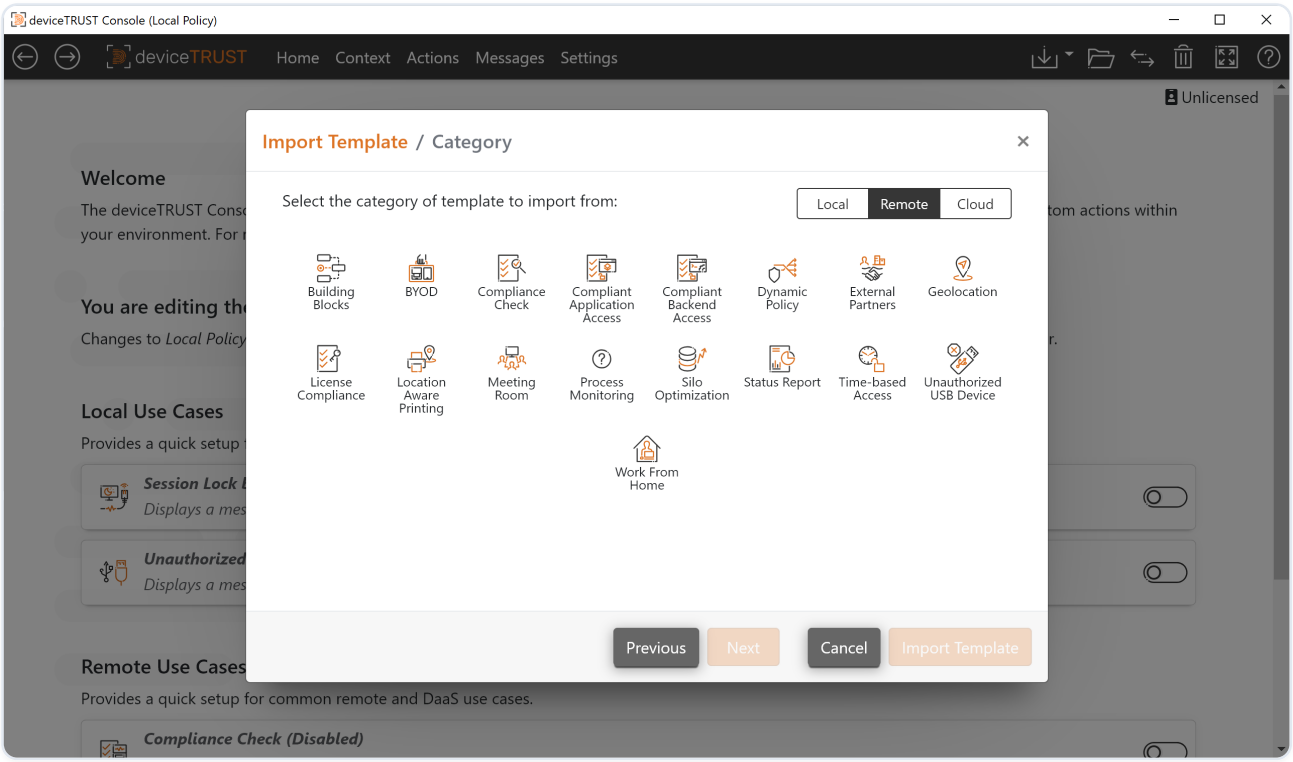


Table of Contents

- Building Blocks - Individual contexts and actions that can be used as building blocks within your configuration.
- BYOD (Bring Your Own Device) - Controls access to the session or applications when compliance requirements for BYOD users are not satisfied.
- Compliance Check - Display a message or denies access to the session when compliance requirements on a remote device are not satisfied.
- Compliant Application Access - Controls access to applications within the session.
- Compliant Backend Access - Display a message or denies access to backend servers when compliance requirements are not satisfied.
- Dynamic Policy - Applies a dynamic policy within the session.
- External Partners - Controls access to the session and applications when compliance requirements for external partners are not satisfied.
- Geolocation - Validates and controls access based on geolocation information of the local device.
- License Compliance - Controls access to applications within the session if the remote device is not licensed.
- Location Aware Printing - Maps network printers and defines a default printer based on the device placement within a building.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Process Monitoring - Controls access to applications or the session based on running processes on the remote device.
- Silo Optimization - Reduces the number of silos by controlling application access for remote devices within a single silo.
- Status Report - Reports the status of the local device to various destinations.
- Time-based Access - Controls access to the session or applications when accessed outside of working hours.
- Unauthorized USB Device - Denies access to the session when an unauthorized USB device is plugged in.
- Work From Home - Validates and controls access based on the remote device for home office users.

SaaS Templates

The deviceTRUST® use cases for SaaS connected devices are summarized within the following categories.

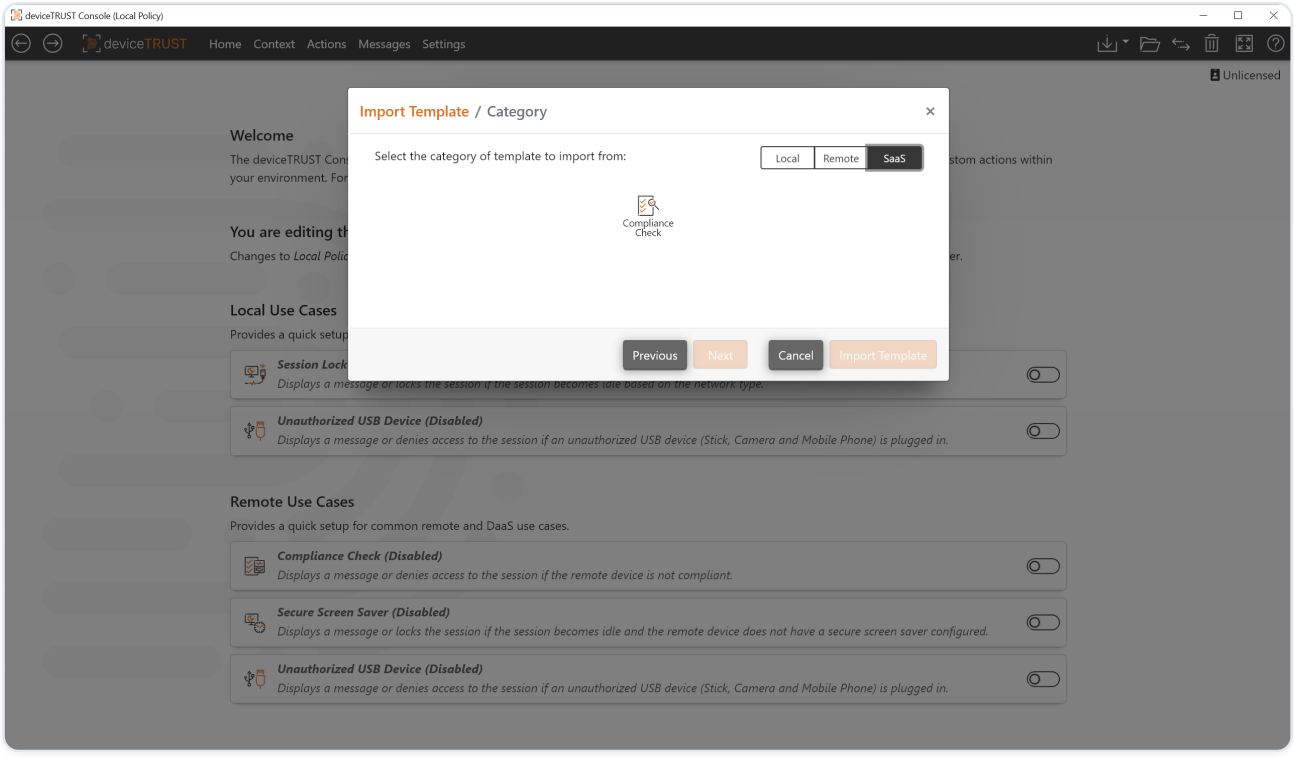


Table of Contents

- Compliance Check - Display a message or deny access to the session when compliance requirements on a remote device are not satisfied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compliance Check

Sets Microsoft Entra ID properties based on the compliance requirements of a local device.

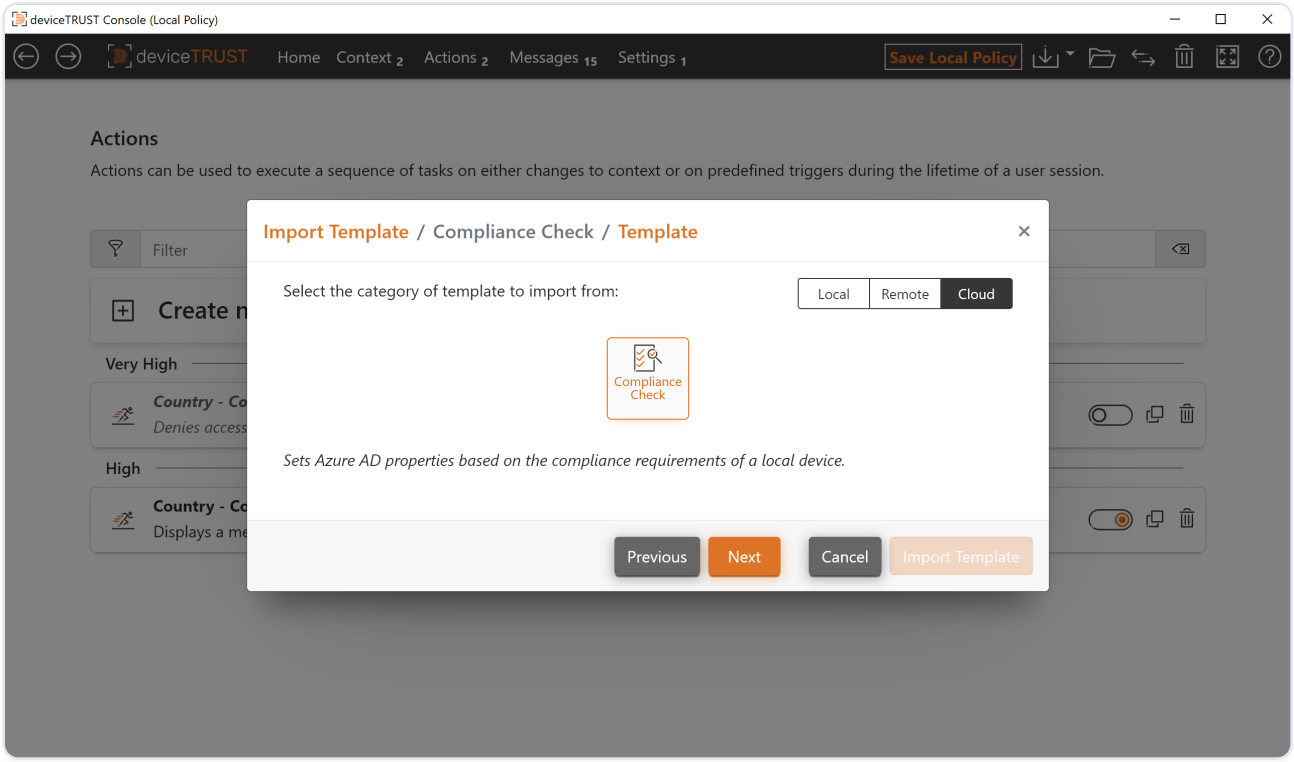


TABLE OF CONTENTS

- Country - Sets Microsoft Entra ID properties based on the country of the local device.
- Operating System Update State - Sets Microsoft Entra ID properties based on the operating system update state of the local device.
- Remote Controlled - Sets Microsoft Entra ID properties based on if the local device is remote controlled.
- Security State - Sets Microsoft Entra ID properties based on the security state of the local device.
- Threat Detection - Sets Microsoft Entra ID properties based on if a threat is detected or the local device has not been scanned recently.
- User Privileges - Sets Microsoft Entra ID properties based on the privileges of the user logged into the local device.
- Wi-Fi Security Mode - Sets Microsoft Entra ID properties based on the Wi-Fi security mode of the local device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reporting

Table of Contents

- Splunk Dashboards
- ELK Stack Dashboards

Splunk Dashboards

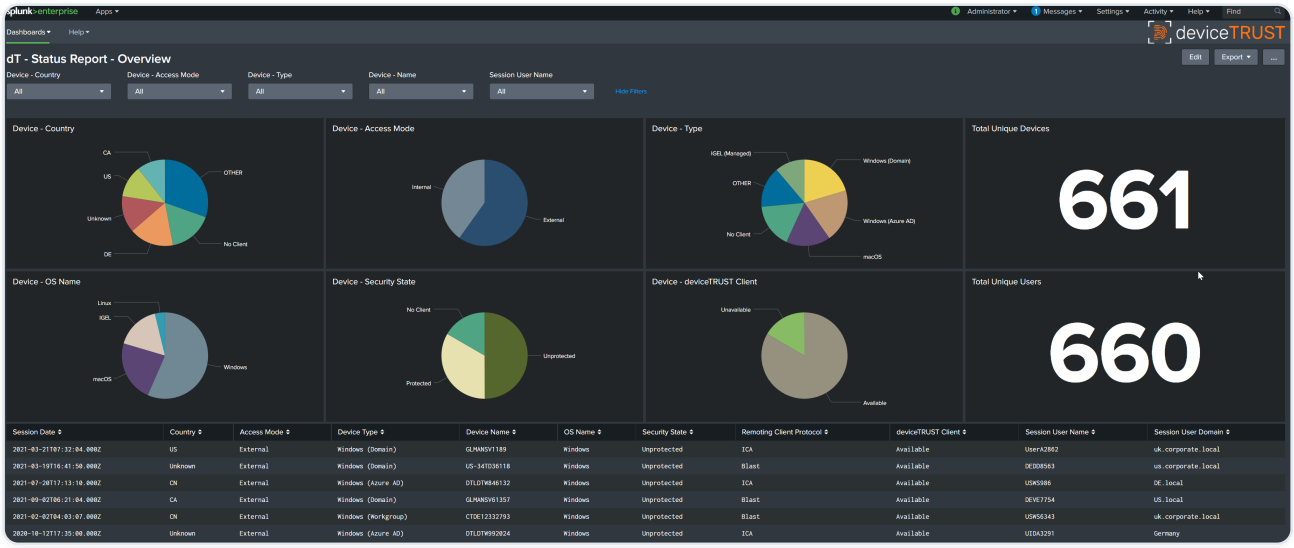
deviceTRUST® includes a Splunk app to easily create a Splunk dashboard to monitor the contextual status of your remoting and DaaS environment.

The License Compliance Templates can be used with the Splunk app to monitor or enforce Device-Based Licensing requirements for one or more applications:



The Splunk Status Report Template can be used to monitor the status of your remoting and DaaS environment:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



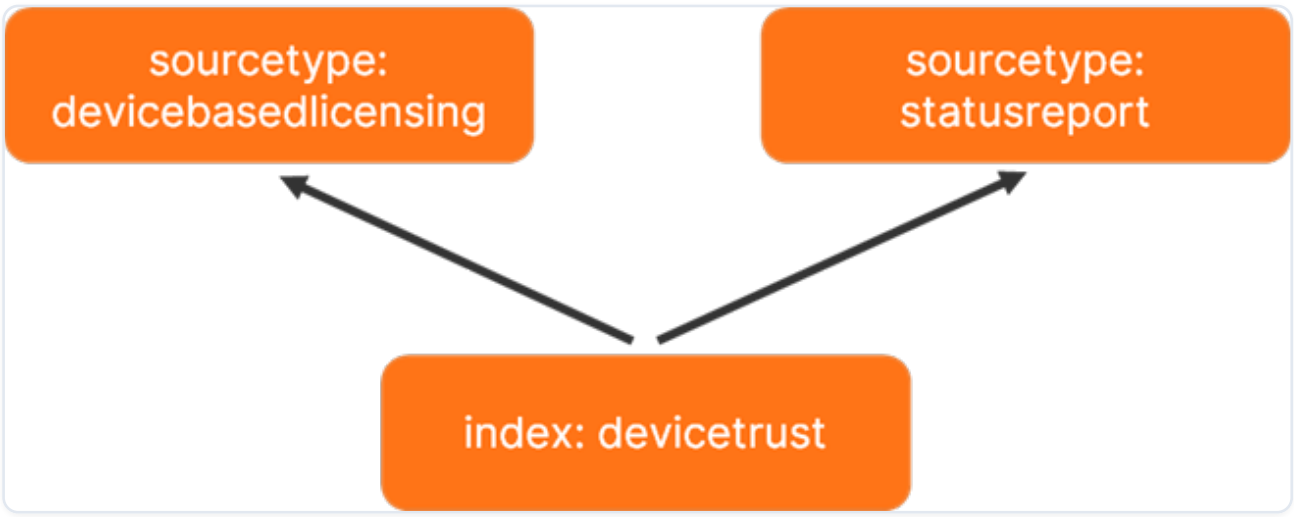
The following steps will be performed:

Step 1: Creating the Splunk Index

Splunk collects data in *indexes* which holds the log data and make it searchable. There are different methods for working with indexes. Data can, for example, flow into one common index. Alternatively, multiple indexes can be created, one for each use case or scenario.

The deviceTRUST reports use one common index `devicetrust` for storing the data. The separation for the different uses cases is done by applying *sourcetypes* `devicebasedlicensing` and `statusreport`.

Our deviceTRUST reports are built on the described combination of index and sourcetypes. If your implementation differs, the reports will have to be adjusted accordingly. Make sure to let us know, we'll happily assist.



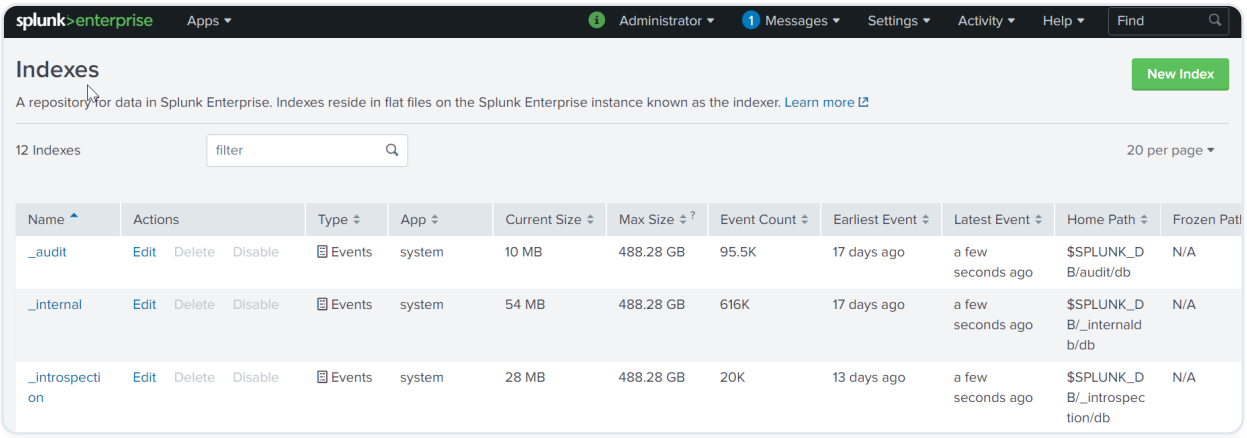
You can either create the index `devicetrust` manually or by importing our prepared app `dt_index`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1.1: Manually creating the Splunk Index

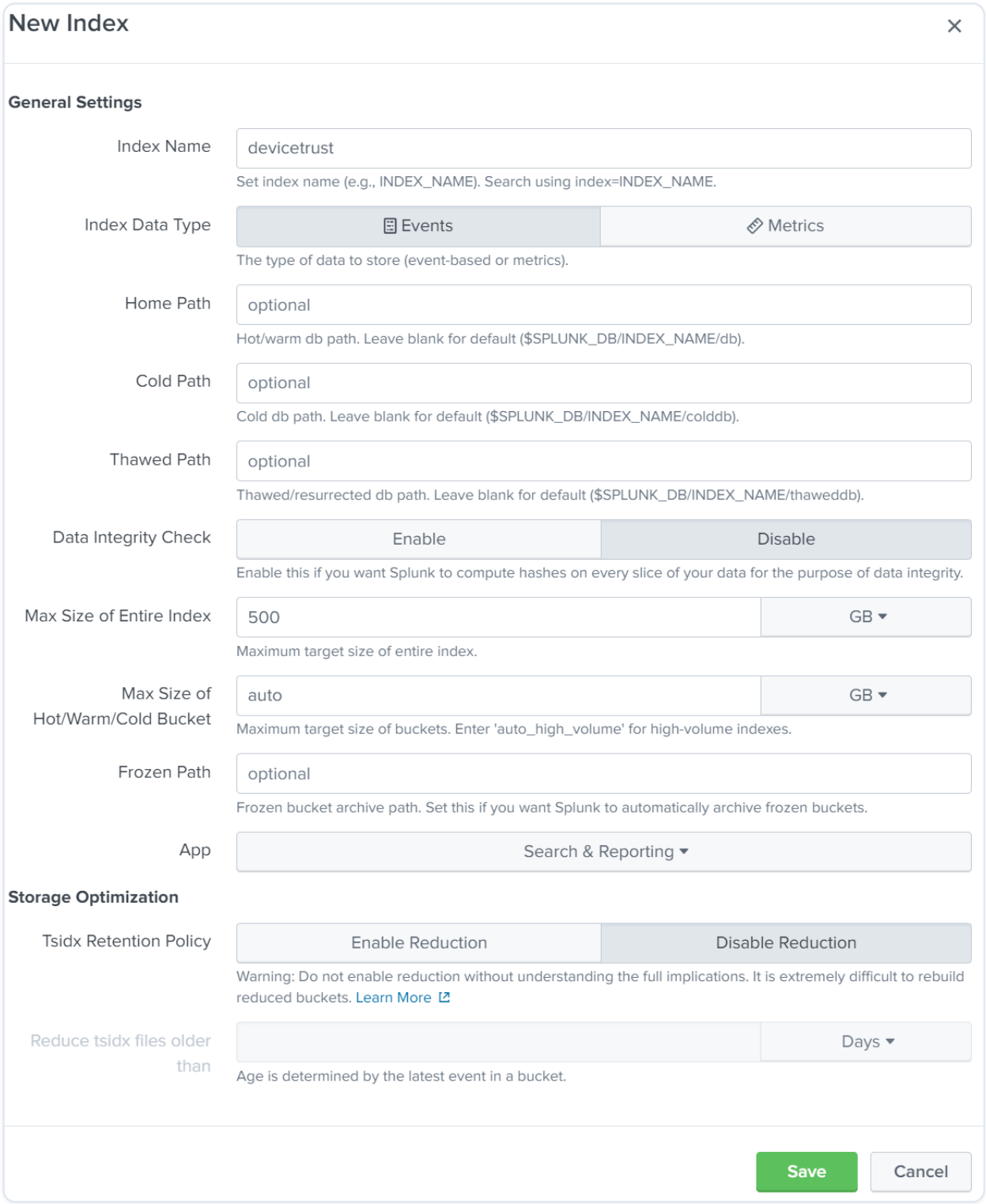
Implementing the index manually does not require any special configuration.

- Open your Splunk management GUI
- Navigate to `Settings\Indexes` and click `New Index`.

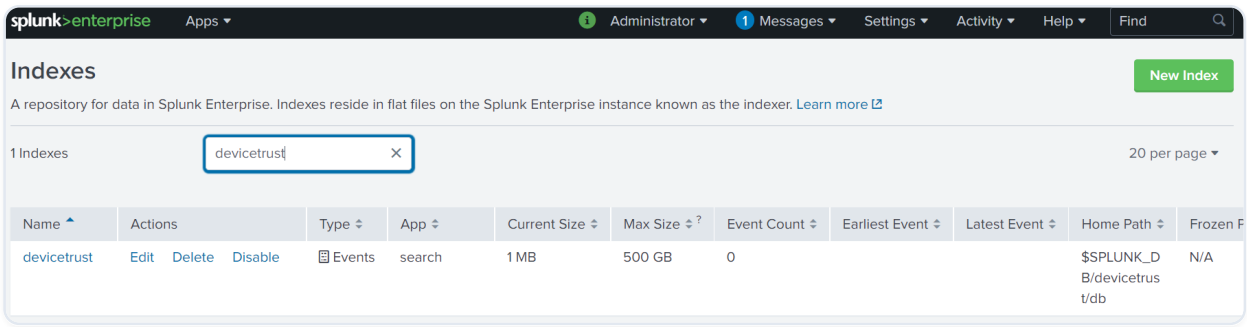


- Set the name to `devicetrust` and all other options are optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Click `Save` and the index will be created.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

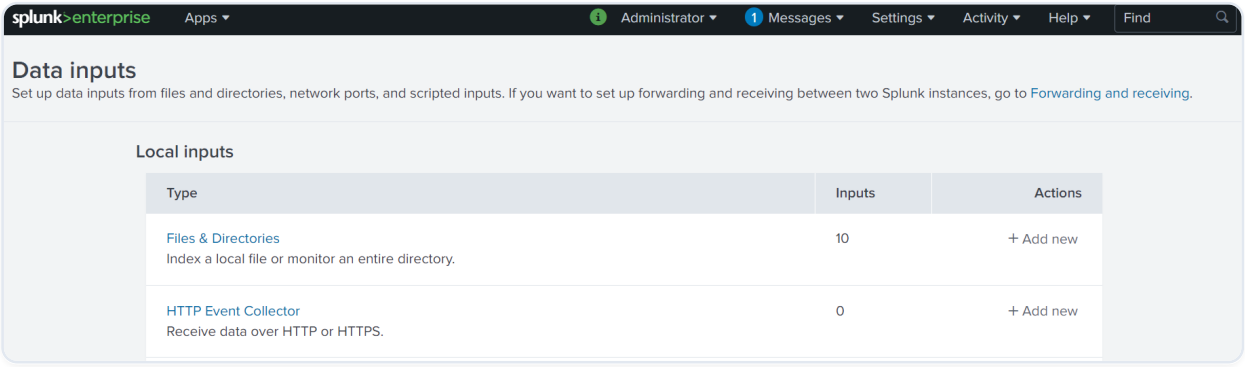
Step 1.2: Creating the Splunk Index by installing the app

To create the index from the app, please refer to Step 3.2: Installing the Splunk app within this guide. The app `dt_index` does not contain any elements besides the index definition for the index `devicetrust`.

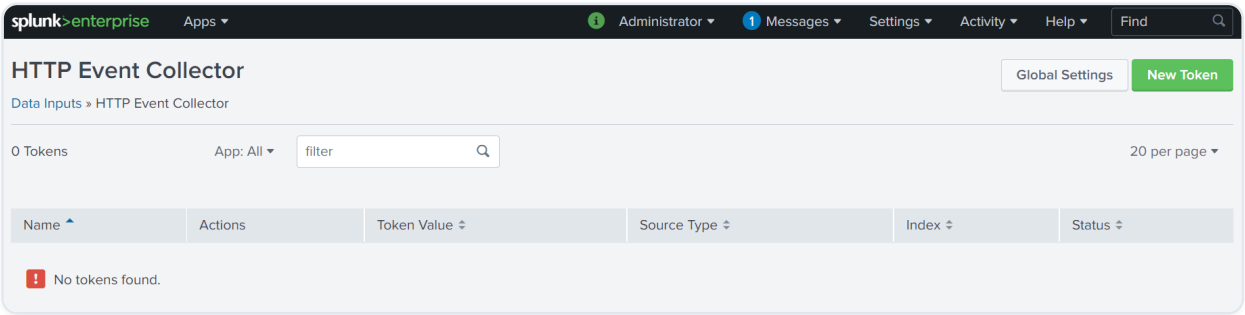
Step 2: Creating the Splunk Data Inputs

Data is sent to the Splunk server by using REST API calls. Splunk needs to be configured to accept http-based inputs. An authentication token is generated, that will be added to the deviceTRUST Console configuration later.

- Open your splunk management GUI and navigate to `Settings\Data Inputs`.

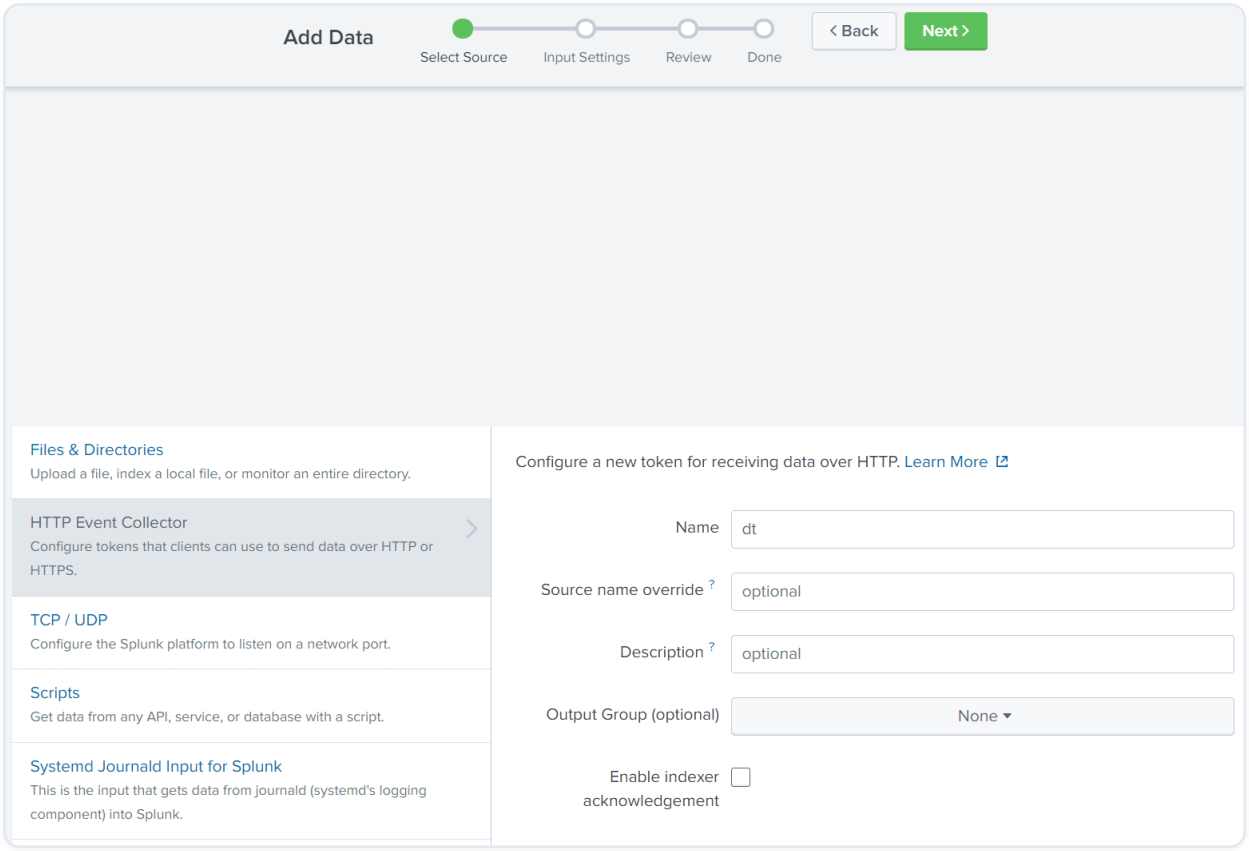


- Select `HTTP Event Collector`
- Click `New Token



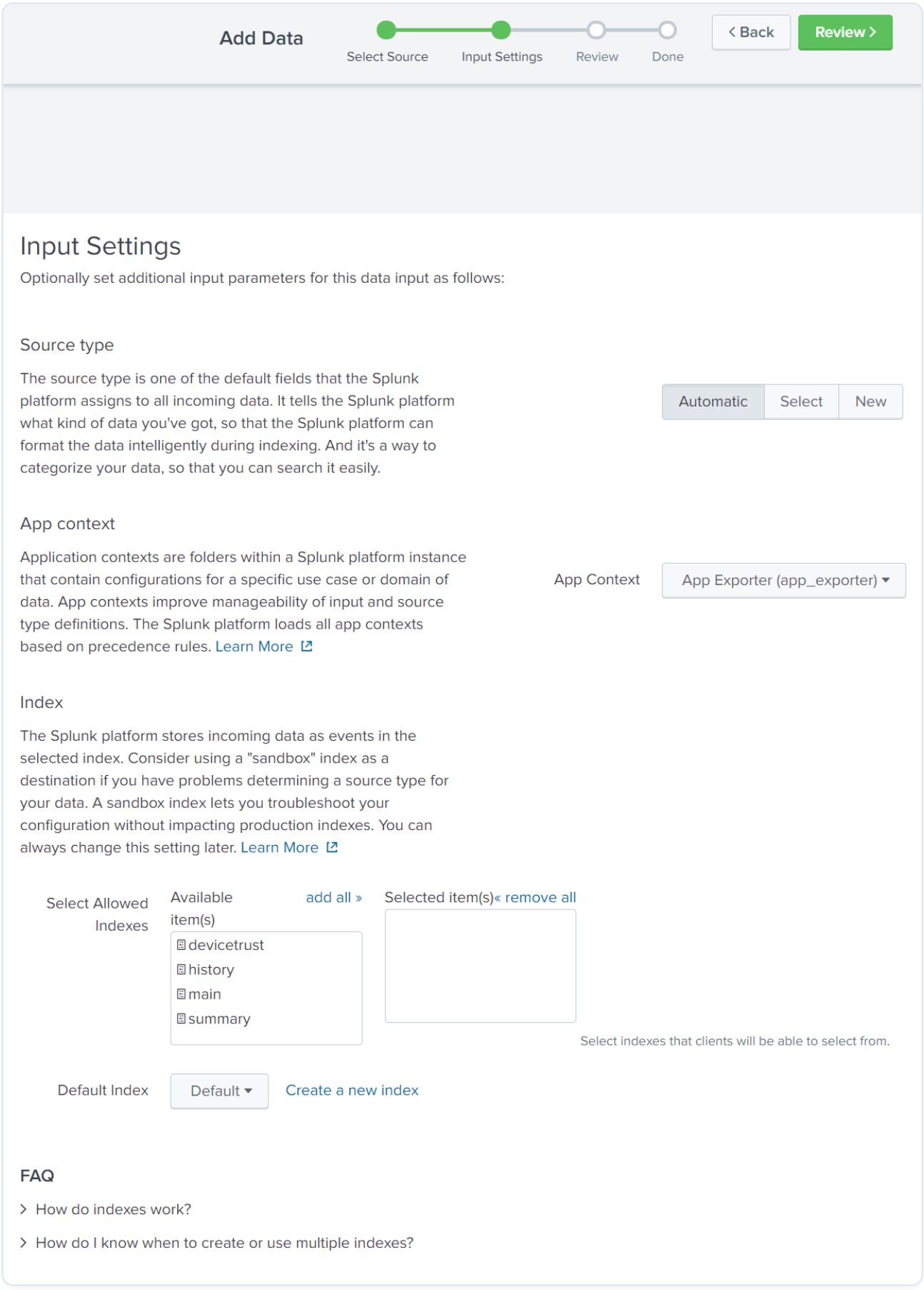
- Set a `name` of your choice.
- All other settings are optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



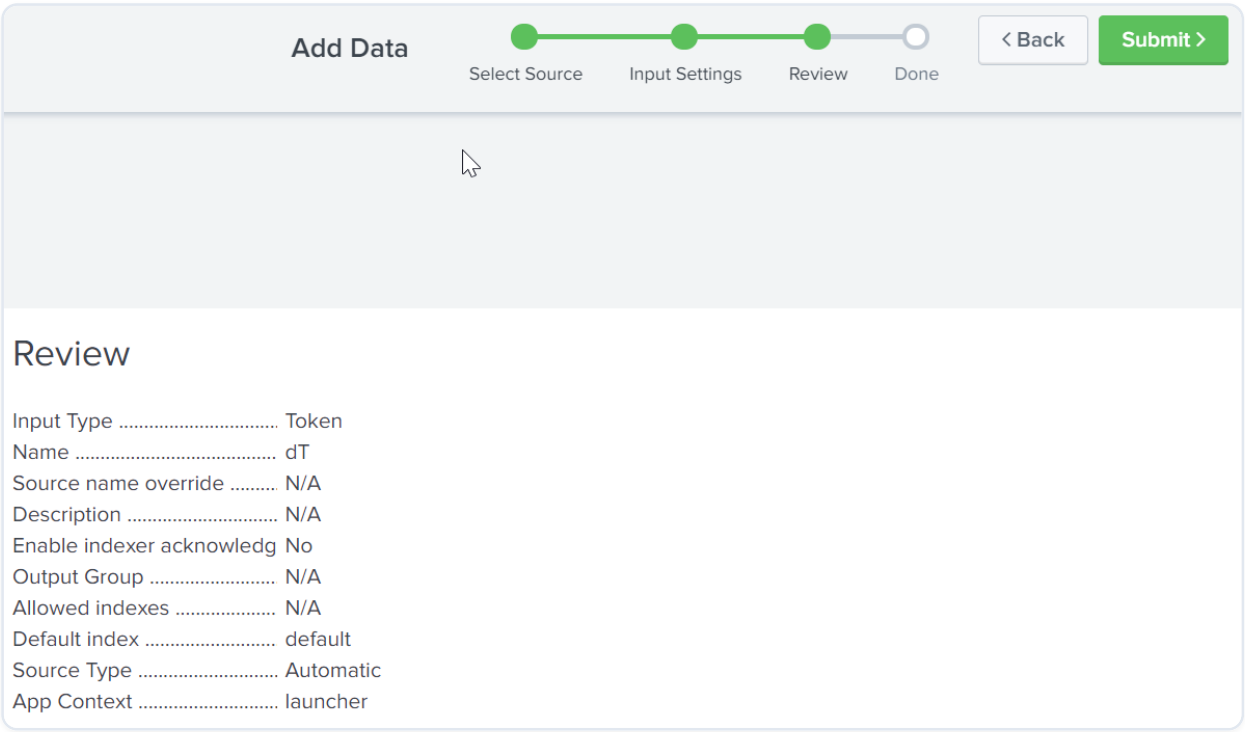
`Input settings` does, for example, allow to restrict access for this data input to certain indexes. Any of these settings may be relevant for your environment. The function of the deviceTRUST reports will not be affected by setting them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

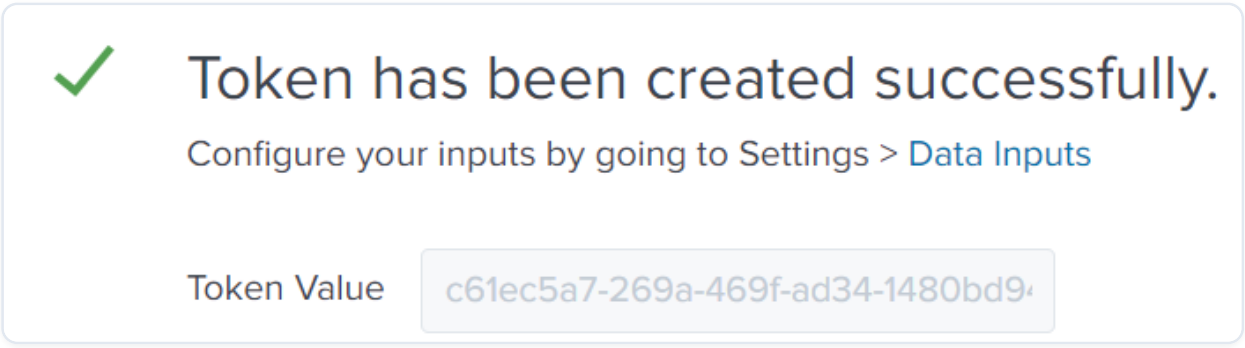


- Review the Settings.
- Click `Submit`.

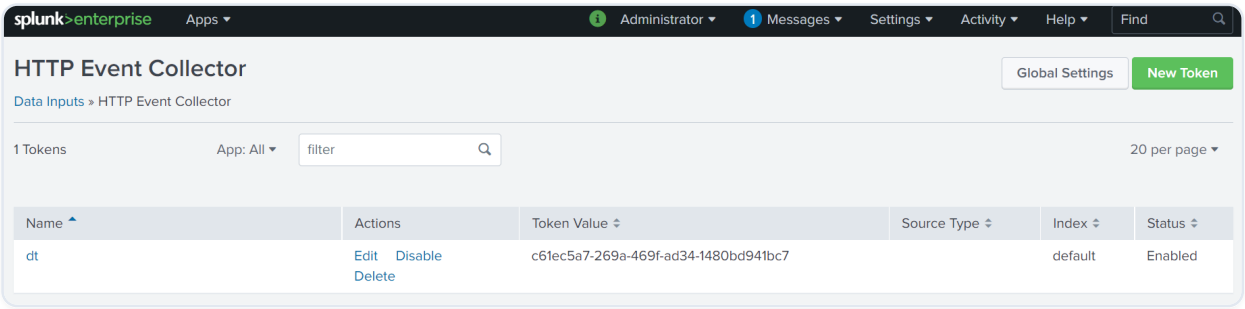
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The created token is shown.



- The created token is also be displayed in the token overview page.

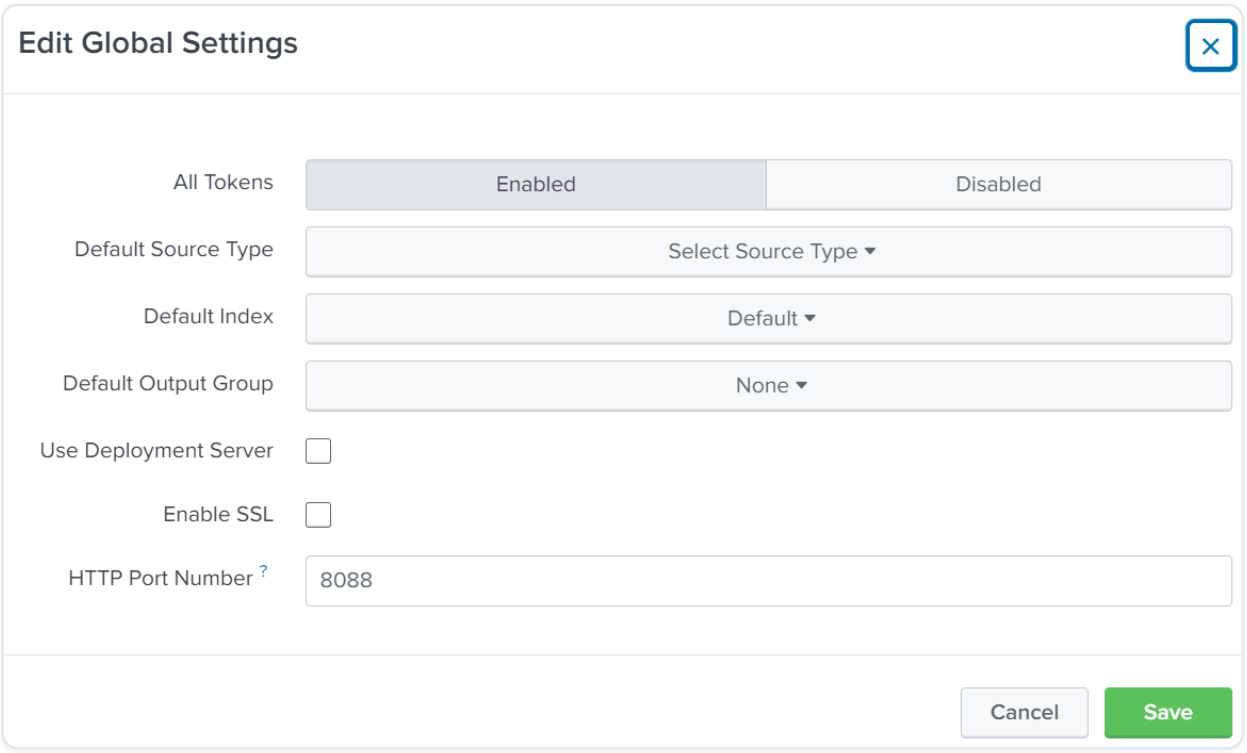


Additionally, the http input method has to be configured. In the most basic configuration, we make sure SSL is not active and all tokens are enabled.

These settings may differ in your environment. The function of the deviceTRUST reports will not be affected by setting them accordingly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Open your splunk management GUI and navigate to `Settings\Data Inputs\HTTP Data Collector`.
- Click `Global Settings`
- Set `All Tokens` to Enabled.
- Set `Enable SSL` to Off.



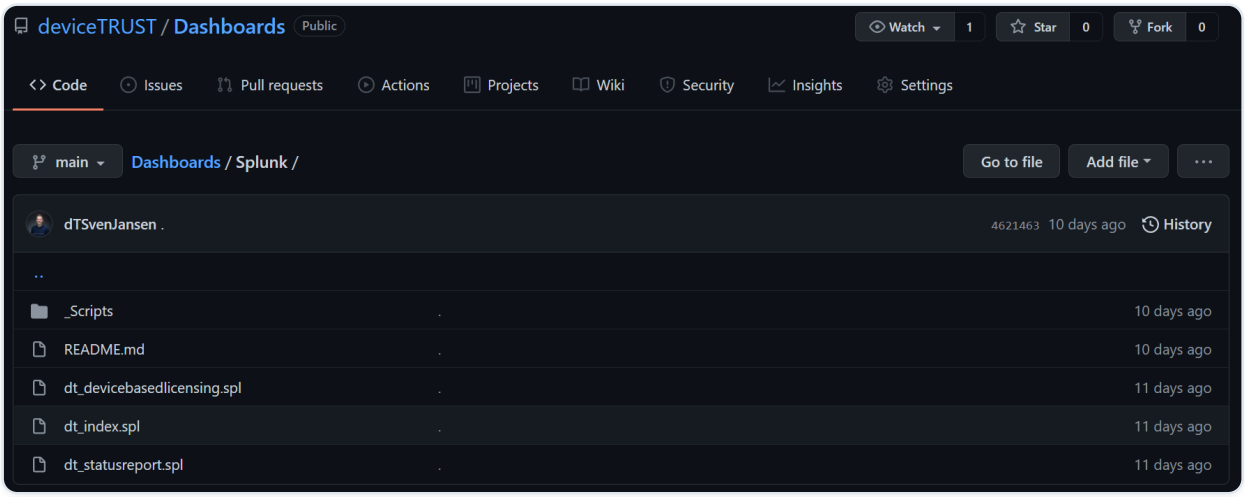
Step 3: Importing the Splunk app

Step 3.1: Downloading the Splunk app

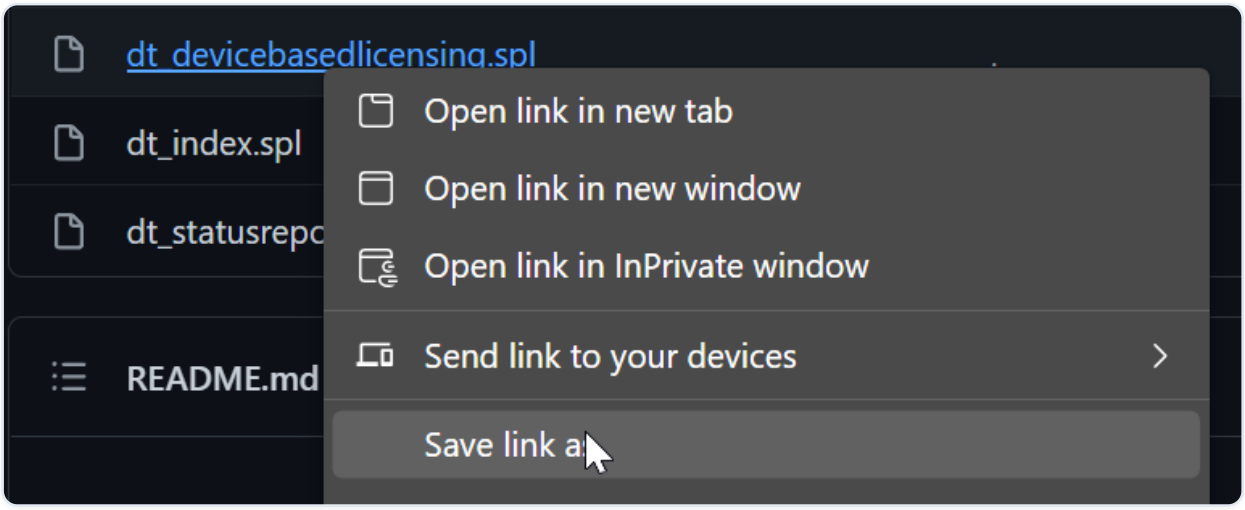
The deviceTRUST reports are delivered as Splunk apps. The apps is available from the deviceTRUST GitHub repository.

- Navigate to the repository and find the Splunk apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The apps are provided as "spl" files which should be downloaded.



- Alternatively the "spl" files can be synchronized via the GIT command line.

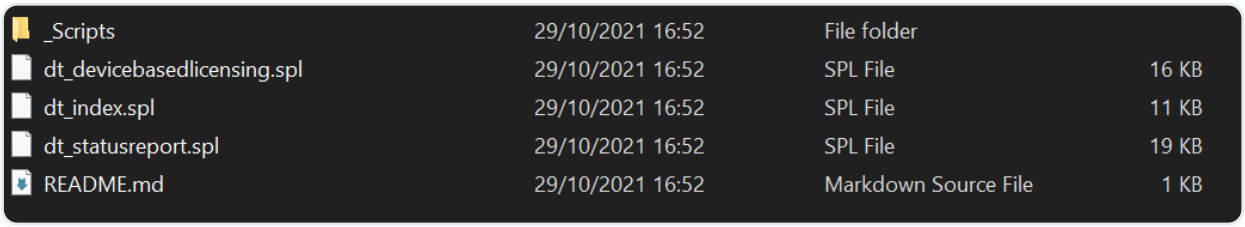
```
PS C:\_Data\GIT> git clone https://github.com/deviceTRUST/Dashboards.git
Cloning into 'Dashboards'...
remote: Enumerating objects: 205, done.
remote: Counting objects: 100% (205/205), done.
remote: Compressing objects: 100% (140/140), done. eceiving objects:  13% (27/205)
remote: Total 205 (delta 72), reused 184 (delta 54), pack-reused 0
Receiving objects: 100% (205/205), 319.08 KiB | 3.39 MiB/s, done.
Resolving deltas: 100% (72/72), done.
PS C:\_Data\GIT> cd .\Dashboards\Splunk\
PS C:\_Data\GIT\Dashboards\Splunk> ls


    Directory: C:\_Data\GIT\Dashboards\Splunk


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/29/2021   4:52 PM                _Scripts
-a----        10/29/2021   4:52 PM          15444 dt_devicebasedlicensing.spl
-a----        10/29/2021   4:52 PM          11195 dt_index.spl
-a----        10/29/2021   4:52 PM          19415 dt_statusreport.spl
-a----        10/29/2021   4:52 PM            810 README.md
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

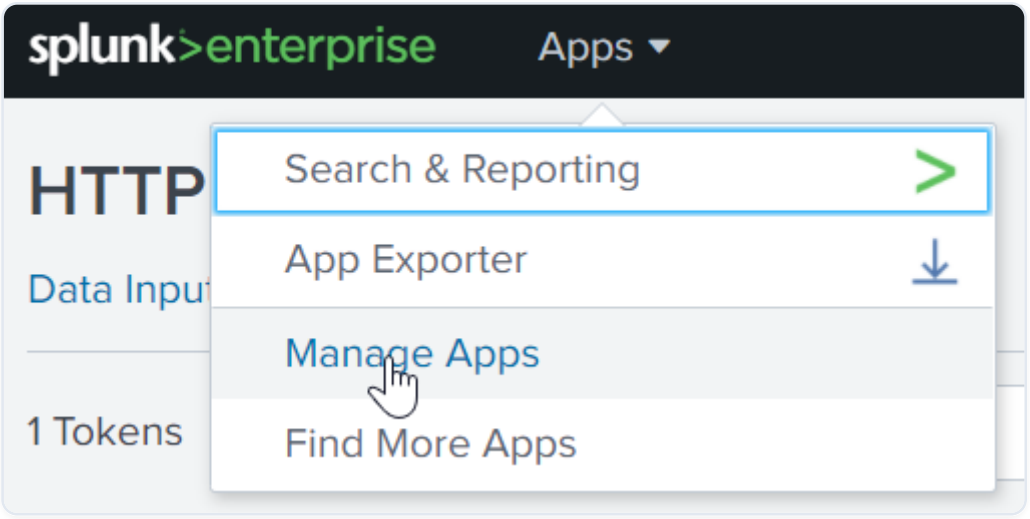
- With the apps available locally, they can be imported into Splunk.



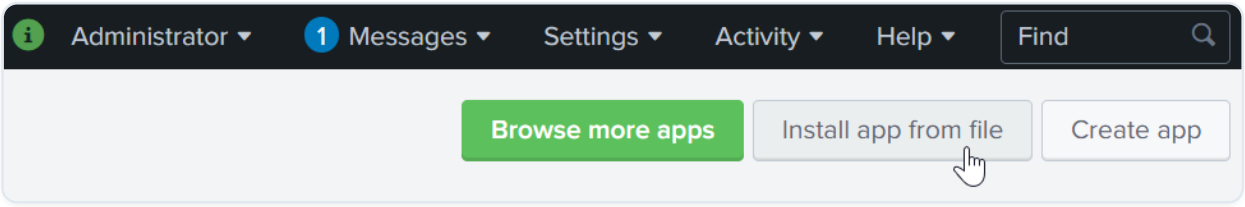
Step 3.2: Installing the Splunk app

All three deviceTRUST apps are installed the same way. Thus, the app installation is described by using one example.

- Open your Splunk management console.
- Click `Manage Apps` in the apps menu.

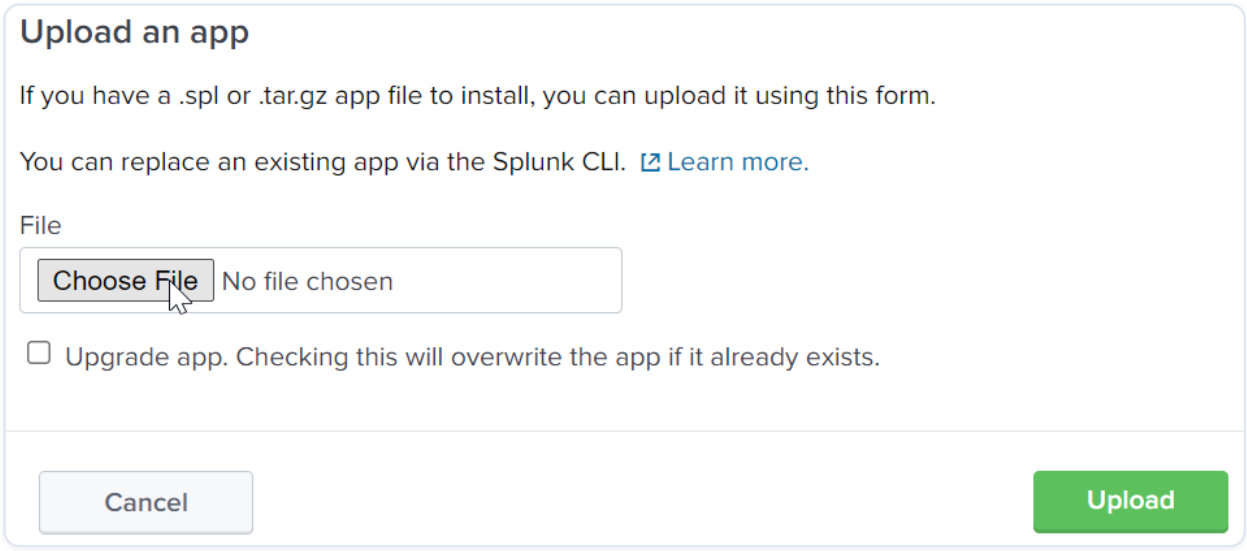


- Click `Install app from file`.

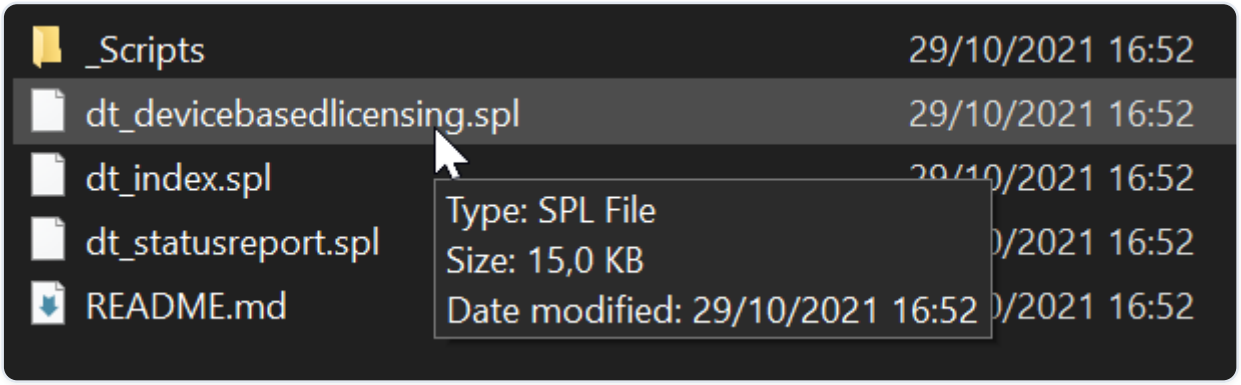


- Click `Choose File`.

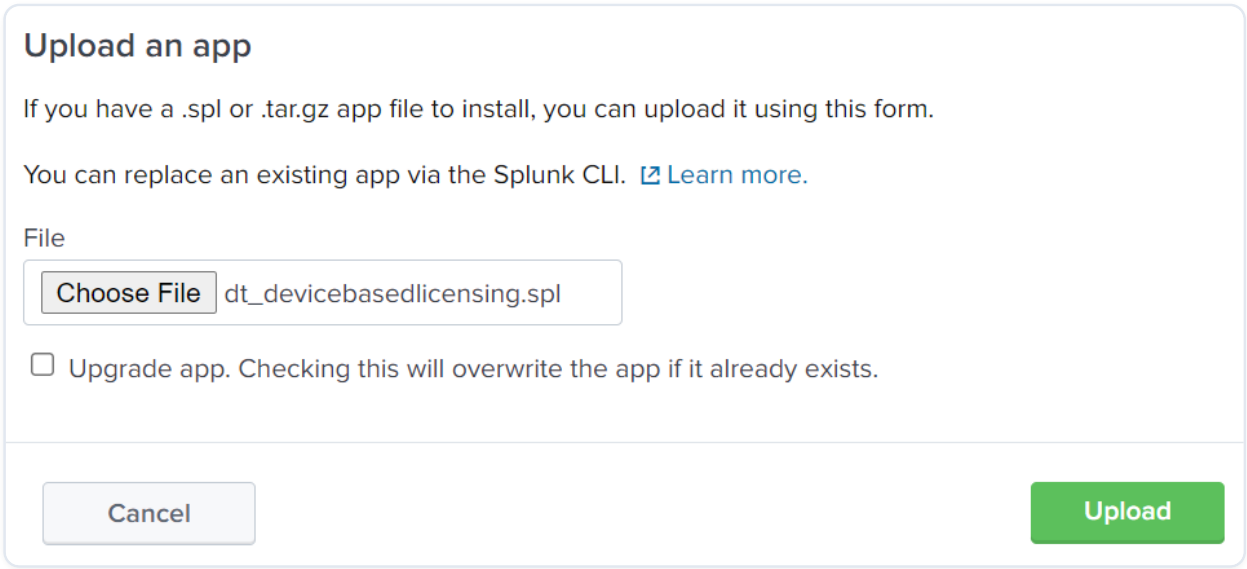
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Select your app file.

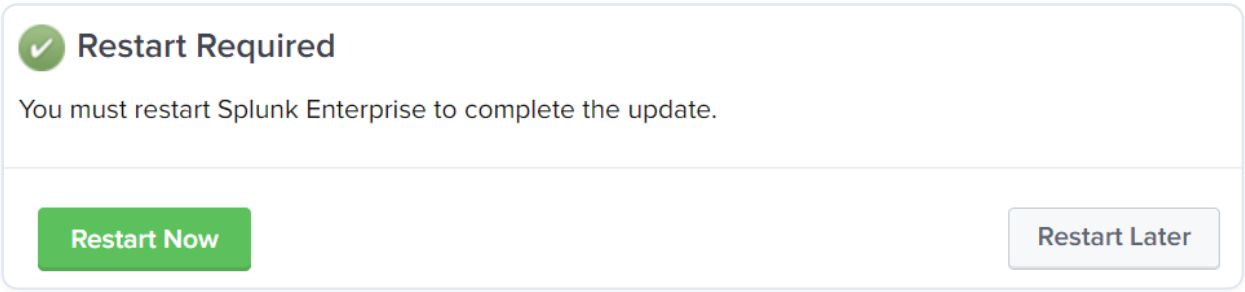


- Confirming your selection.
- Optionally select to upgrade apps, if applicable.
- Click `Upload`.

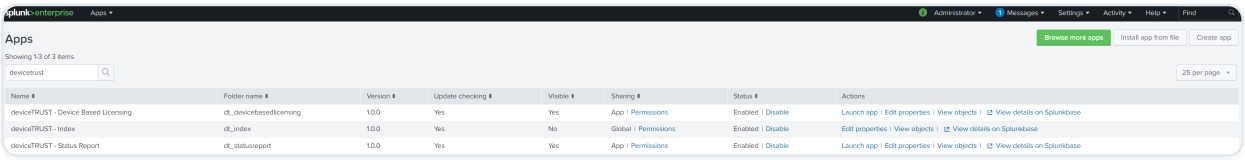


- Splunk will ask to restart the service. This is only required after importing the last app.
- Choose `Restart Now` or `Restart Later` accordingly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The menu `Apps\Manage Apps` displays all apps that are installed in your Splunk environment.



Step 4: Configuring deviceTRUST

After the the index has been created, the data input object added and all apps have been imported, Splunk is ready to accept, store and compute data for the deviceTRUST reports.

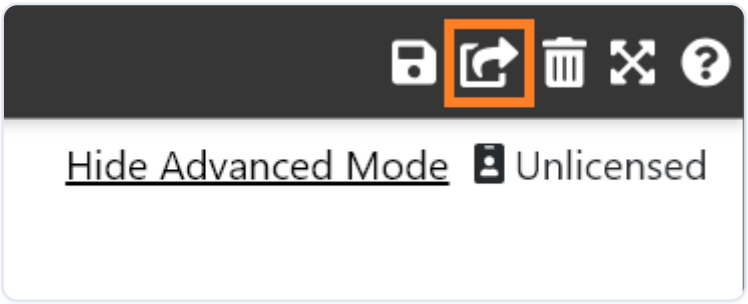
As both reports `Device-Based Licensing` and `Status Report` differ in their details, both are described here separately.

Step 4.1: The Device-Based Licensing Report

This step describes the configuration to be added to the deviceTRUST Console to send `Device-Based Licensing` data to Splunk.

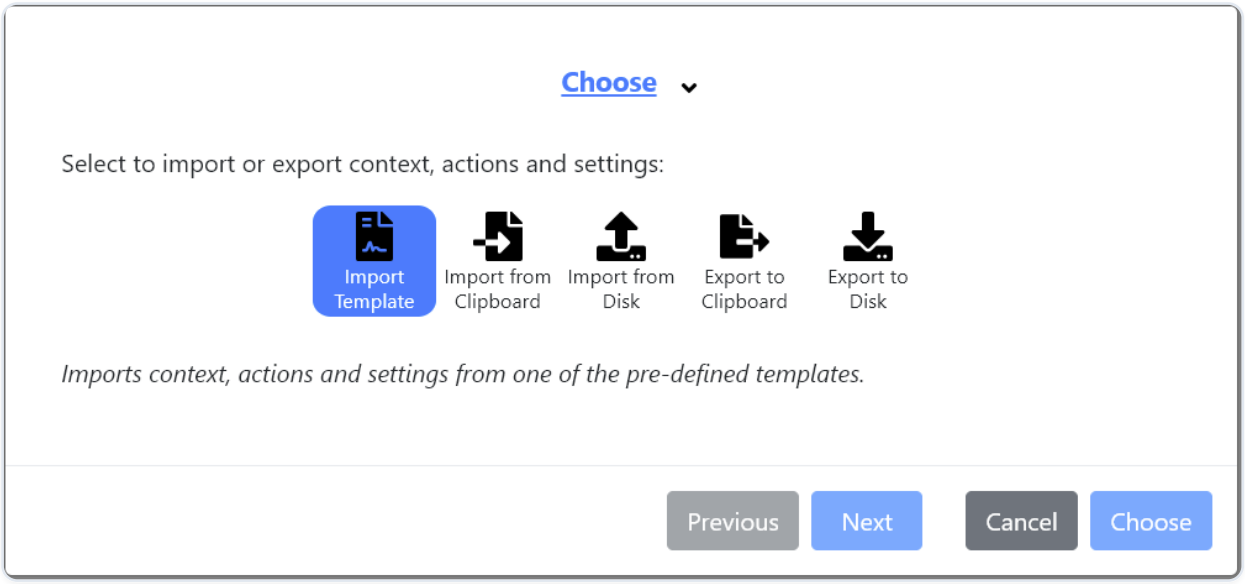
The integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. These five example applications can be easily edited for your own applications, or cloned to represent new applications. The elements are contexts, actions, messages and settings.

- Open the `deviceTRUST Console`.
- Click `Sharing` in the top right menu. You may need to click `Show Advanced View` if this button is not visible.

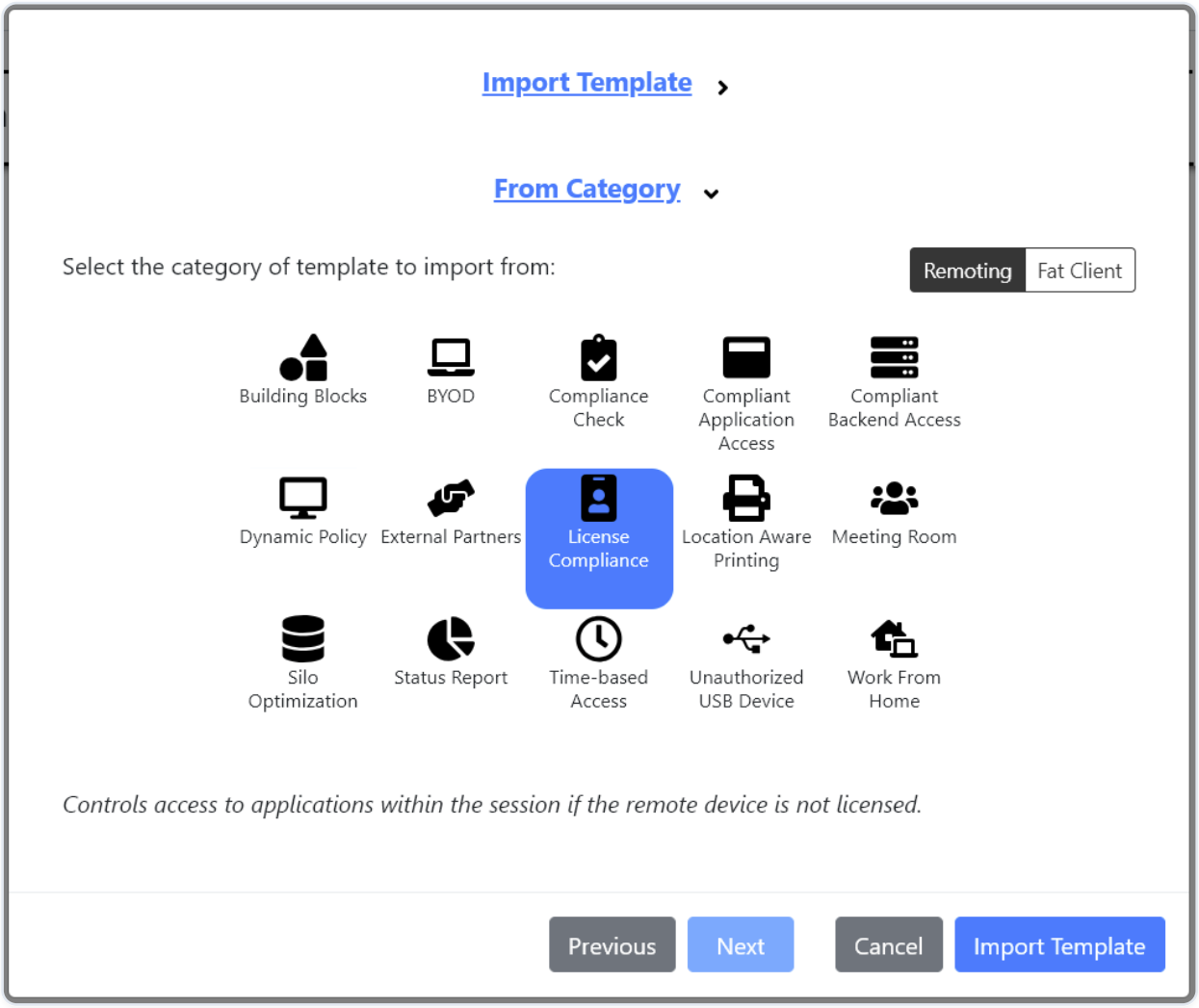


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select `Import Template`

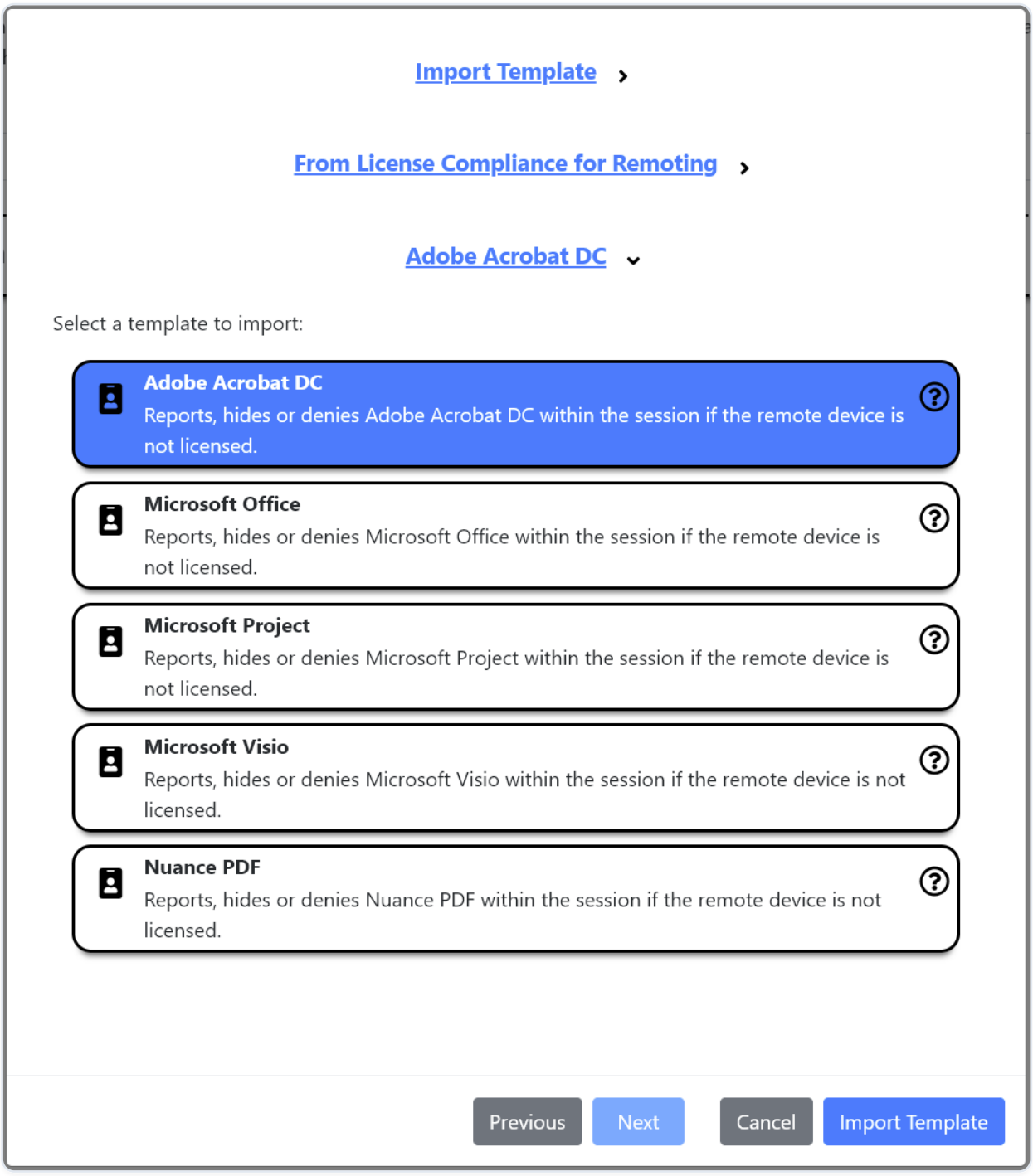


- The report `Device-Based Licensing` can be found within the template category `License Compliance` when `Remoting` is selected.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

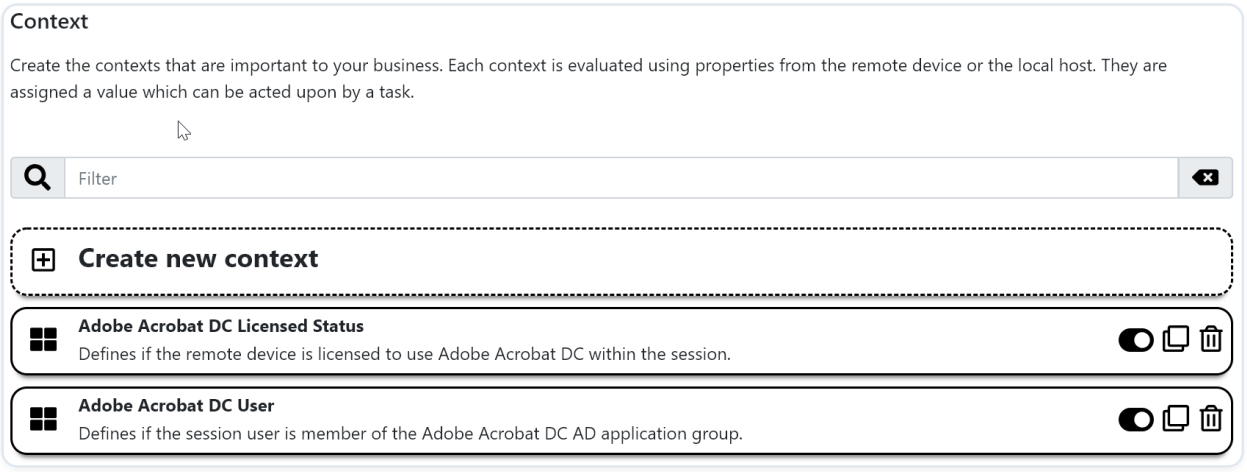
- The category contains templates for different example applications. We use `Adobe Acrobat DC` as an example here.



Two contexts are included within the template:

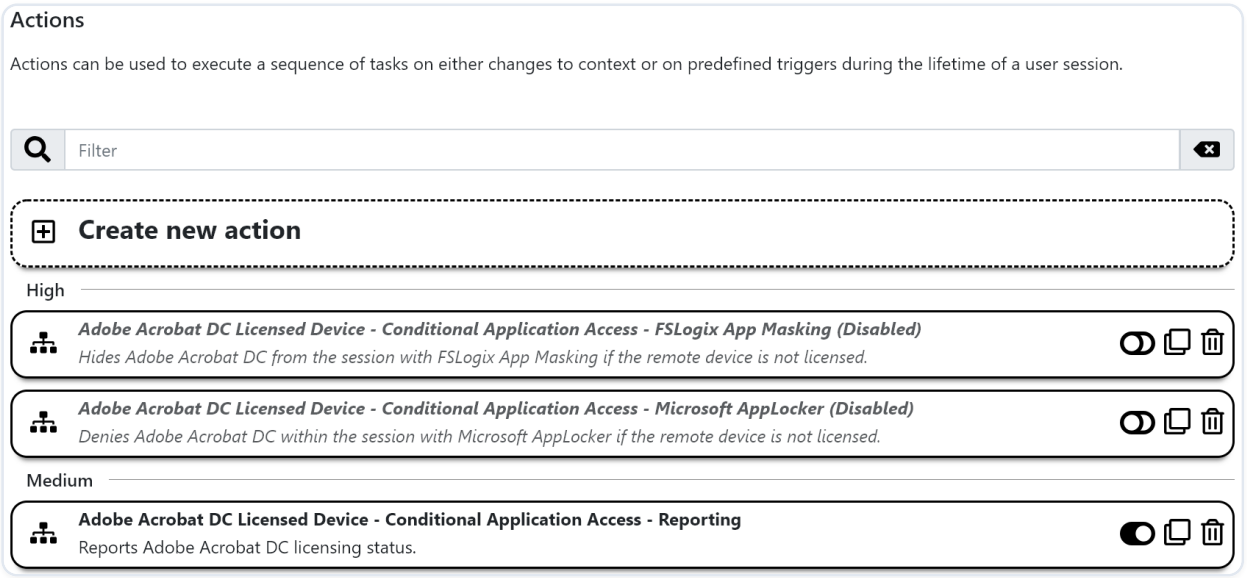
- `Adobe Acrobat DC Licensed Status` to evaluate the device license status.
- `Adobe Acrobat DC User` to define if the accessing user is licensed to use the software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



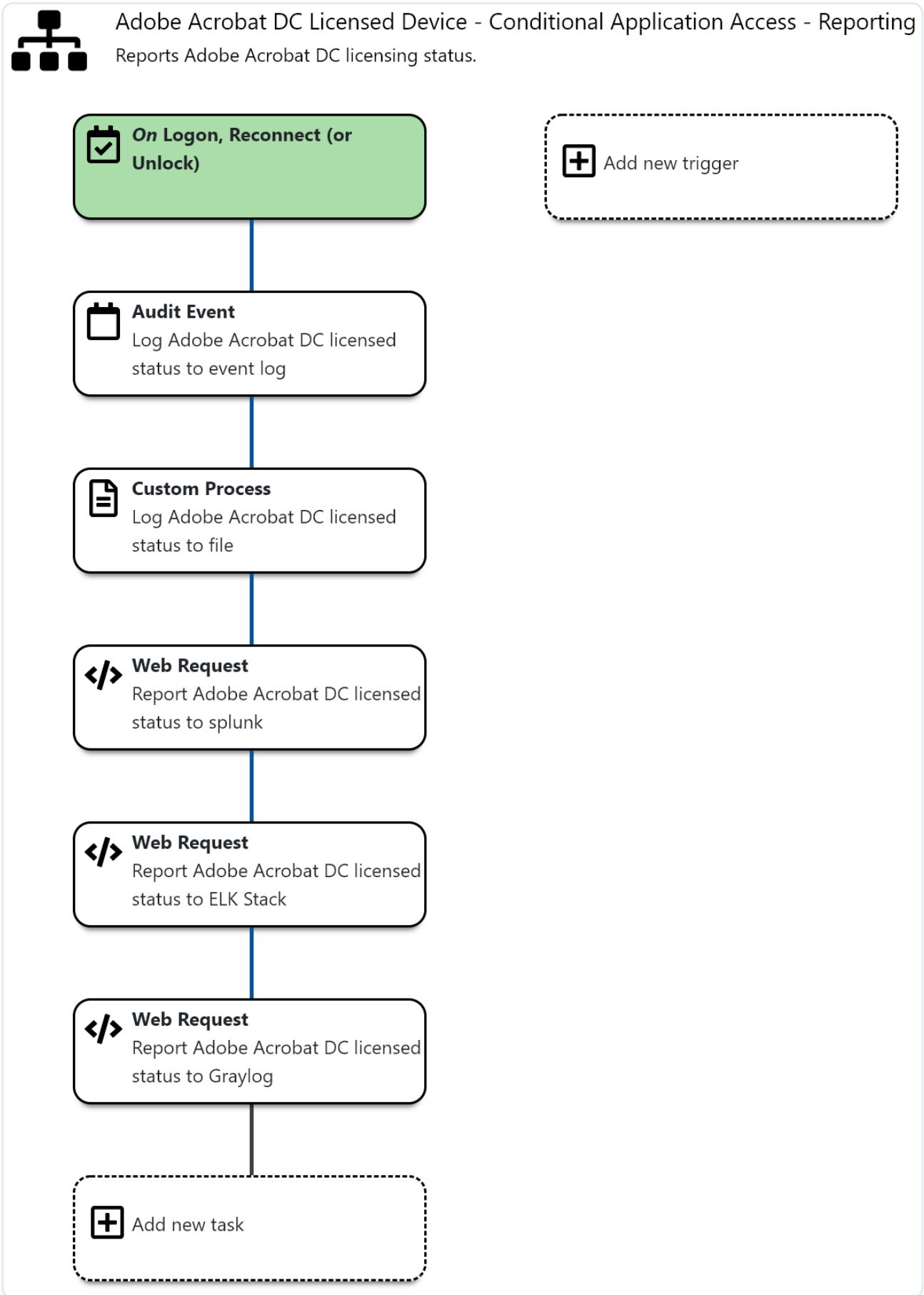
Three actions are included within the template:

- `Adobe Acrobat DC Licensed Device - Conditional Application Access - FSLogix App Masking` is used for application control via `FSLogix App Masking` and can be ignored or deleted for the reporting use case.
- `Adobe Acrobat DC Licensed Device - Conditional Application Access - Microsoft AppLocker` is used for application control via `Microsoft AppLocker` and can be ignored or deleted for the reporting use case.
- `Adobe Acrobat DC Licensed Device - Conditional Application Access - Reporting` the only action required for reporting.



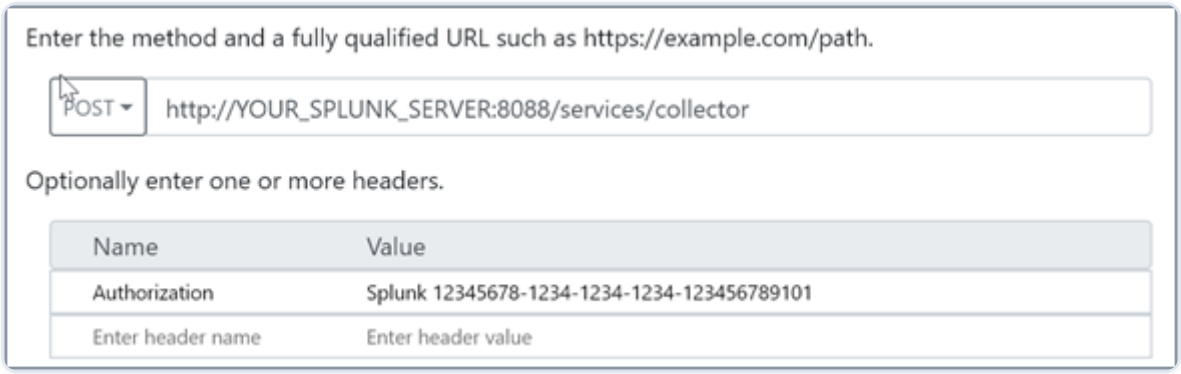
- The action contains uses the `Web Request` task to send data to Splunk. The `Audit Event`, `Custom Process` and also the `Web Request` tasks for ELK Stack and Graylog can be deleted, as we are configuring Splunk here.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

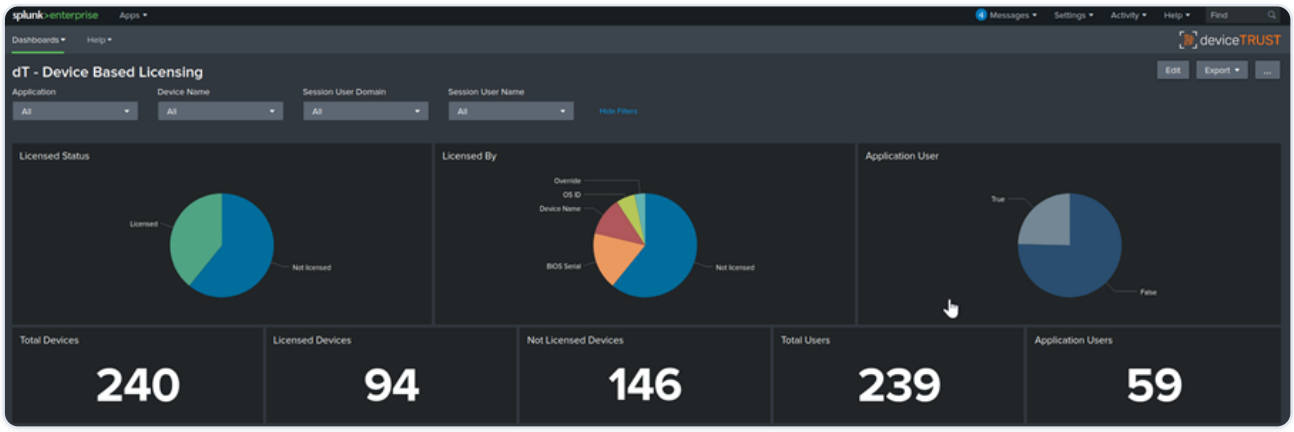


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Splunk `Web Request` task needs to be edited to suit your environment. If you do not require SSL transport, you'll only have to configure your `server's fqdn` and the `authorization token` (http data input). Make sure to leave the keyword `splunk` and only add/change your authorization token's GUID.



The use case has successfully been configured. deviceTRUST will now send `Device-Based Licensing` data on every access to the Splunk server. The data will be presented using dashboards.



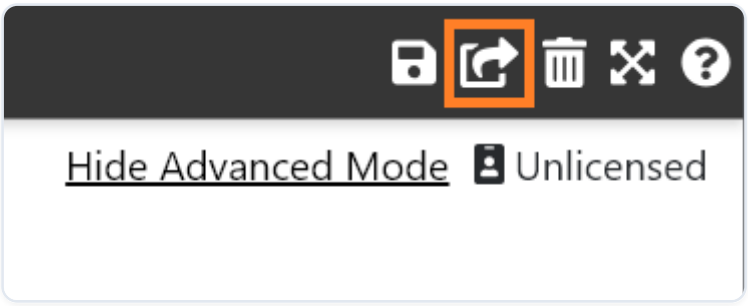
Step 4.2: The Status Report

This step describes the configuration, that is to be added to the deviceTRUST console to send `Status Report` data to splunk.

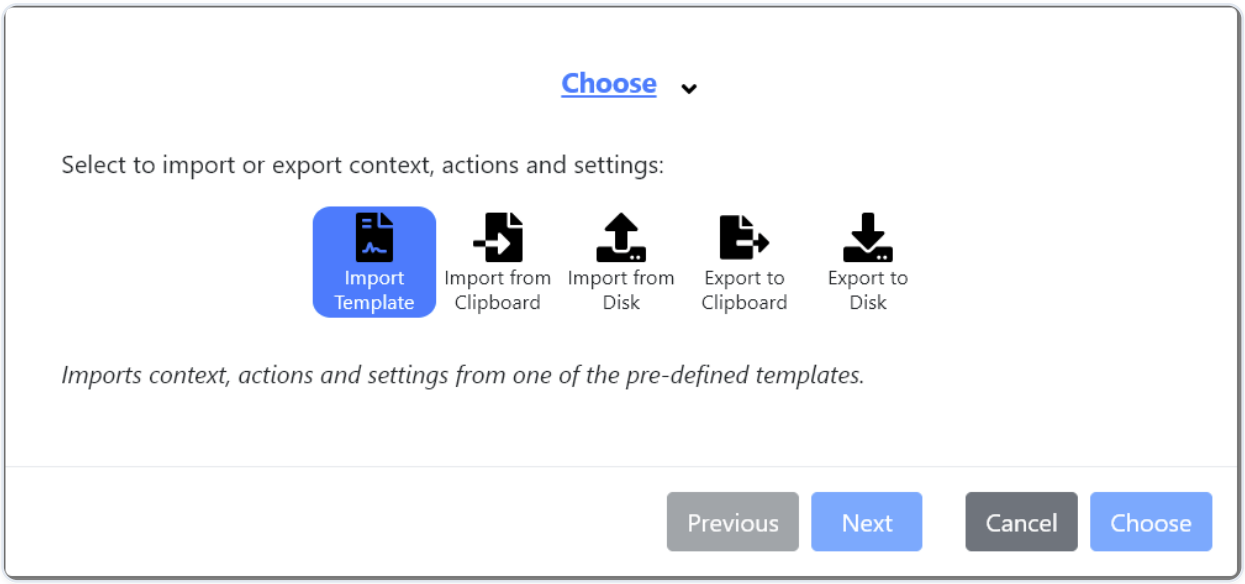
Our integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. The elements are contexts, actions, messages and settings.

- Open the deviceTRUST console and click `Sharing` in the top right menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

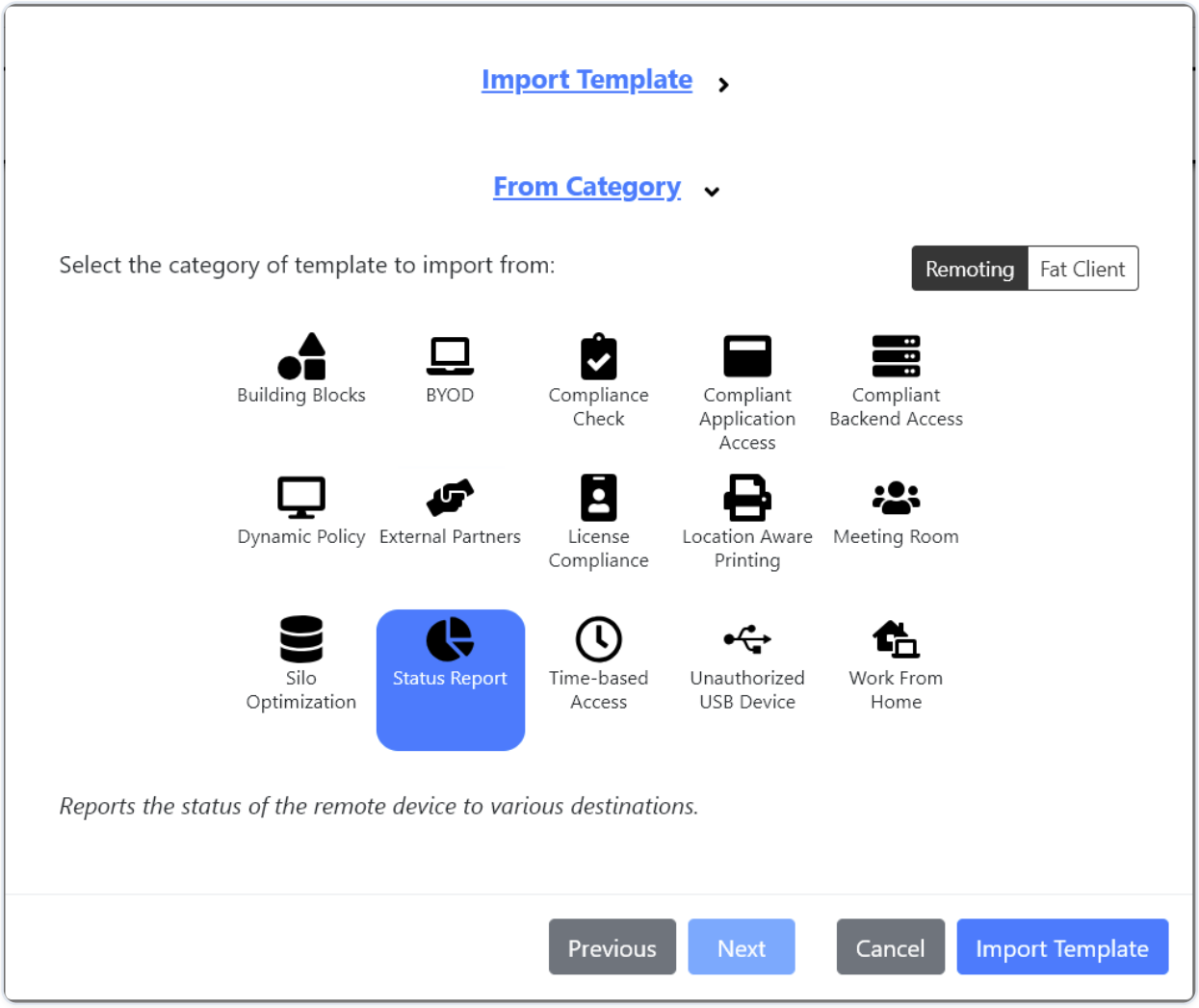


- Select `Import Template`



- The `Status Report` template can be found within the template category `Status Report` when `Remoting` is selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



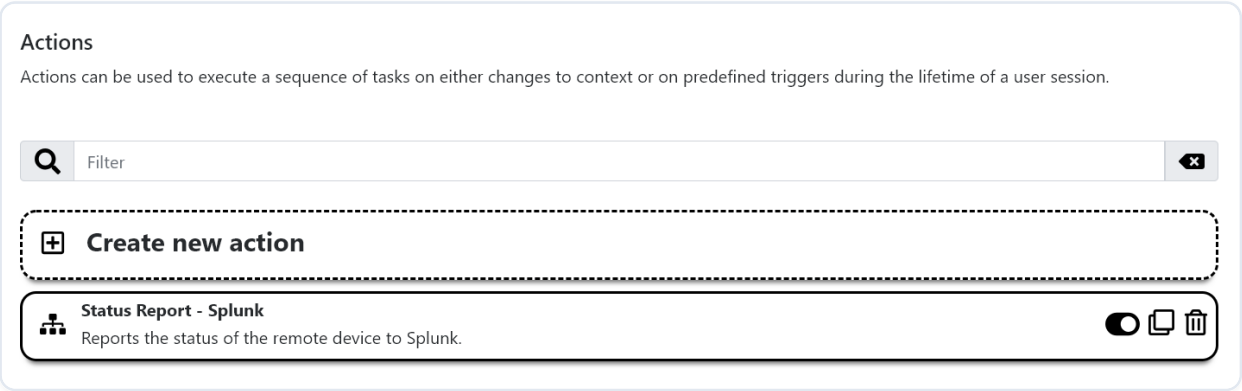
- This category contains templates for several ways of storing data. Choose `Splunk`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

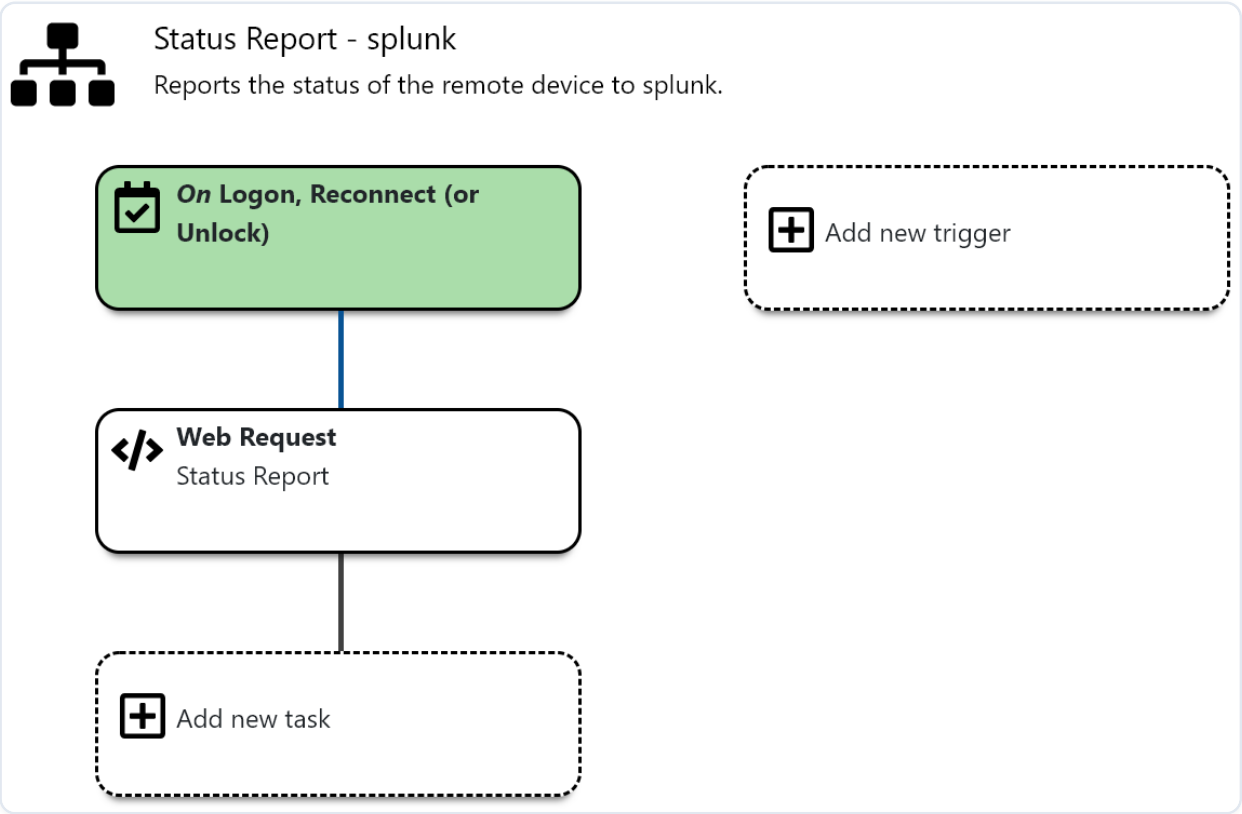


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – Splunk` collects all relevant data and sends them over to Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

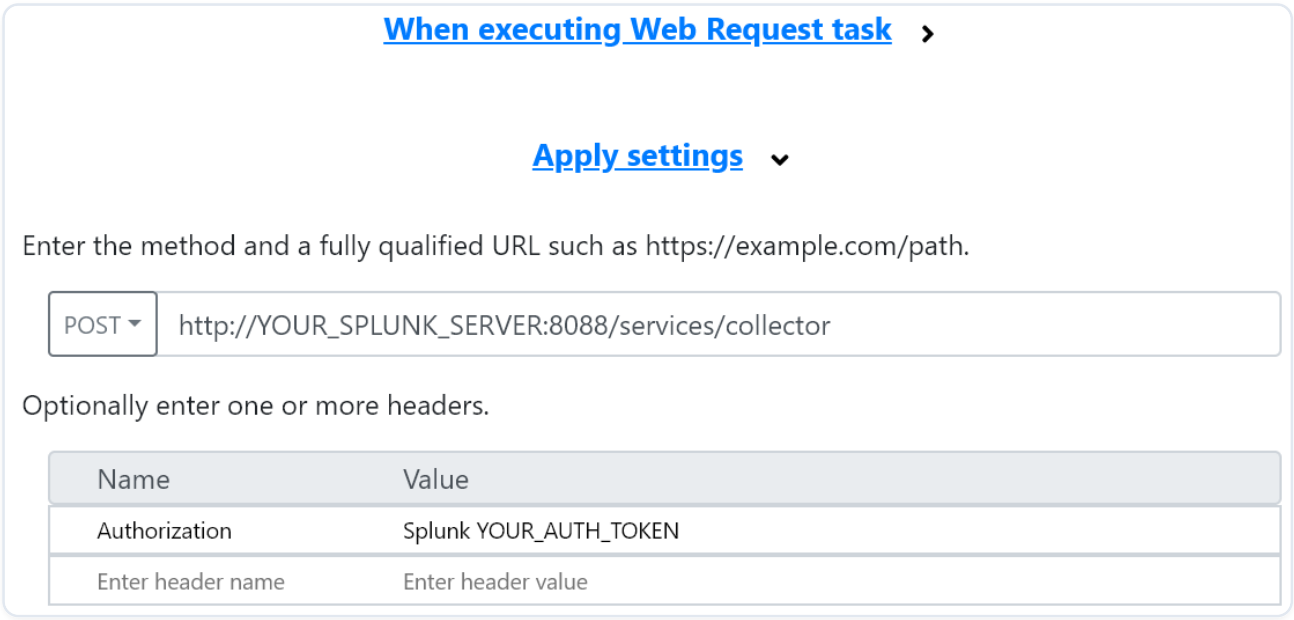


- Sending data to Splunk is configured by using a `Web Request` task.

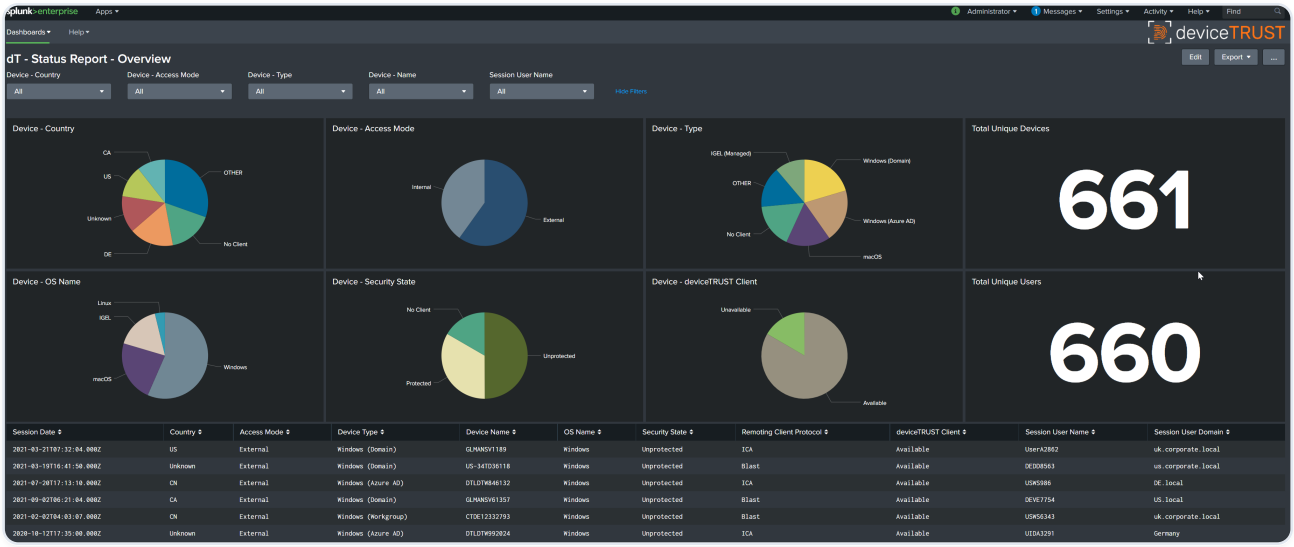


The Web Request task needs to be edited to suit your environment. If you do not require SSL transport, you'll only have to configure your `server's fqdn` and the `authorization token` (http data input). Make sure to leave the keyword `splunk` and only change your authorization token's GUID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The use case has successfully been configured. deviceTRUST will now send `Status Report` data on every access to the remoting platform to the splunk server. There, the data will be presented using dashboards.

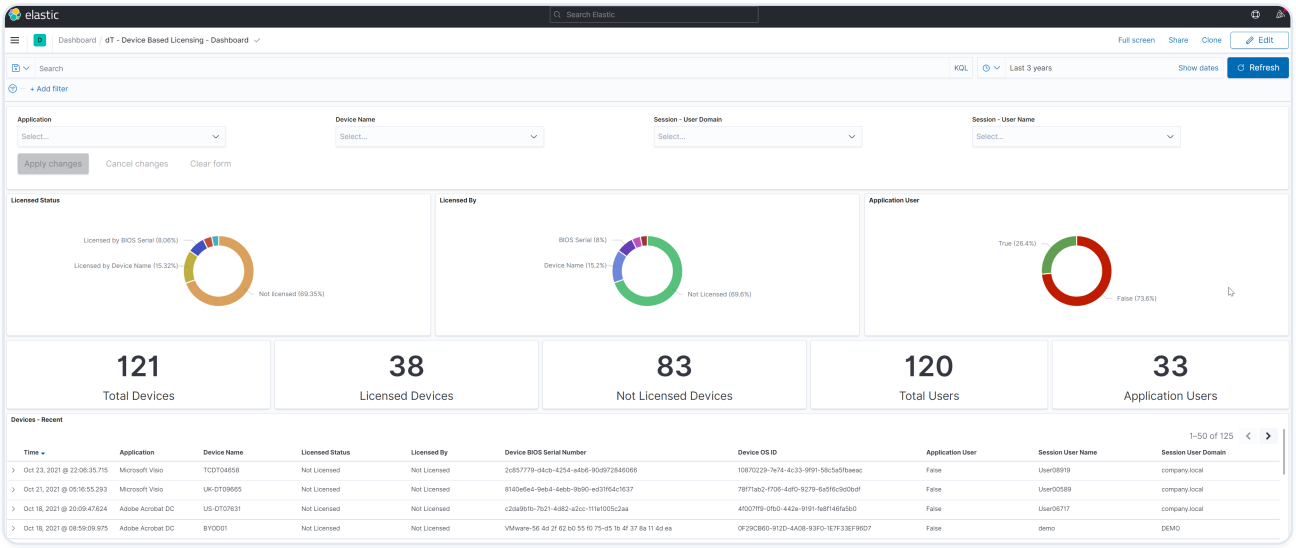


ELK Stack Dashboards

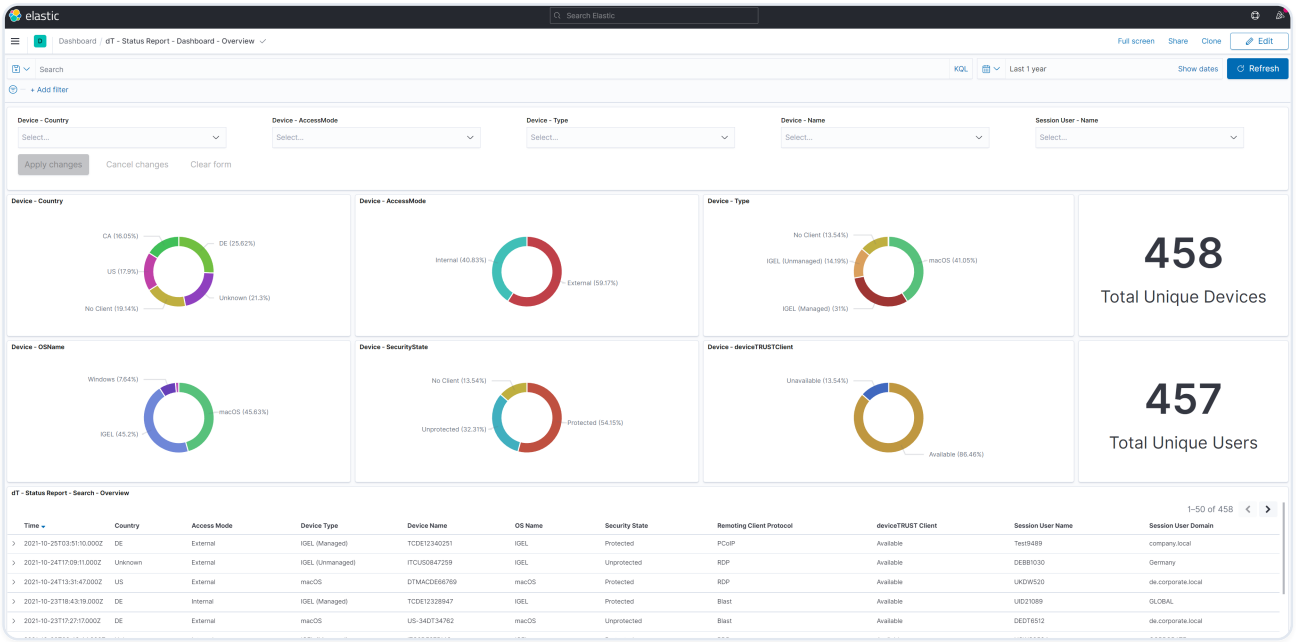
deviceTRUST® includes components for an ELK Stack to easily create a dashboard to monitor the contextual status of your remoting and DaaS environment.

The License Compliance Templates can be used with your ELK Stack to monitor or enforce Device-Based Licensing requirements for one or more applications:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The ELK Stack Status Report Template can be used to monitor the status of your remoting and DaaS environment:



Step 1: Components

The deviceTRUST dashboards for ELK Stack consist of several components. All elements that need to be imported on the ELK Stack side can be found on GitHub. The configuration for the deviceTRUST Agent is available as a template within the deviceTRUST Console.

Step 1.1: Components - GitHub

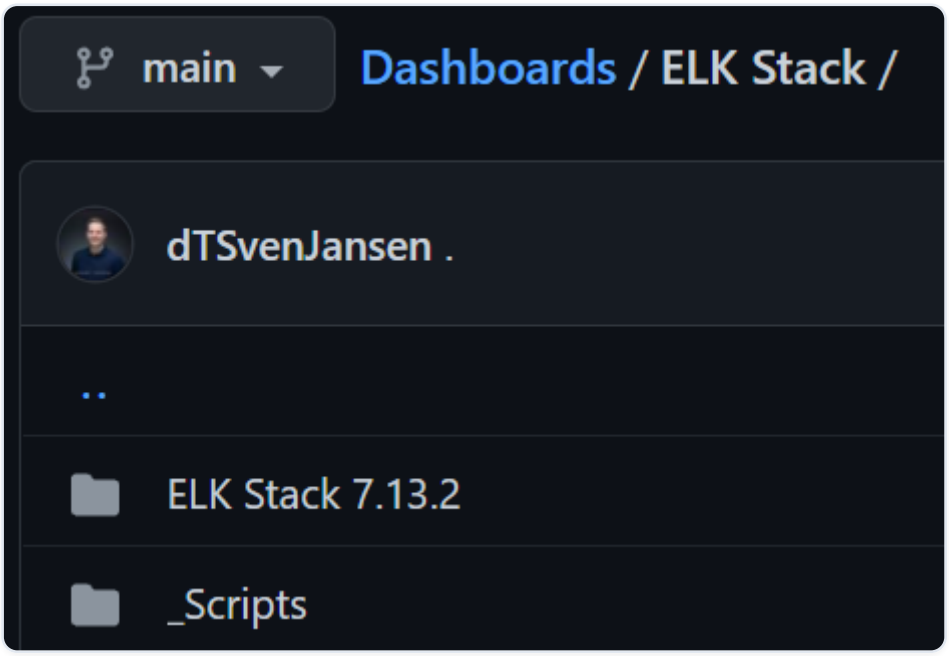
All required components for ELK Stack can be found on our GitHub repository.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

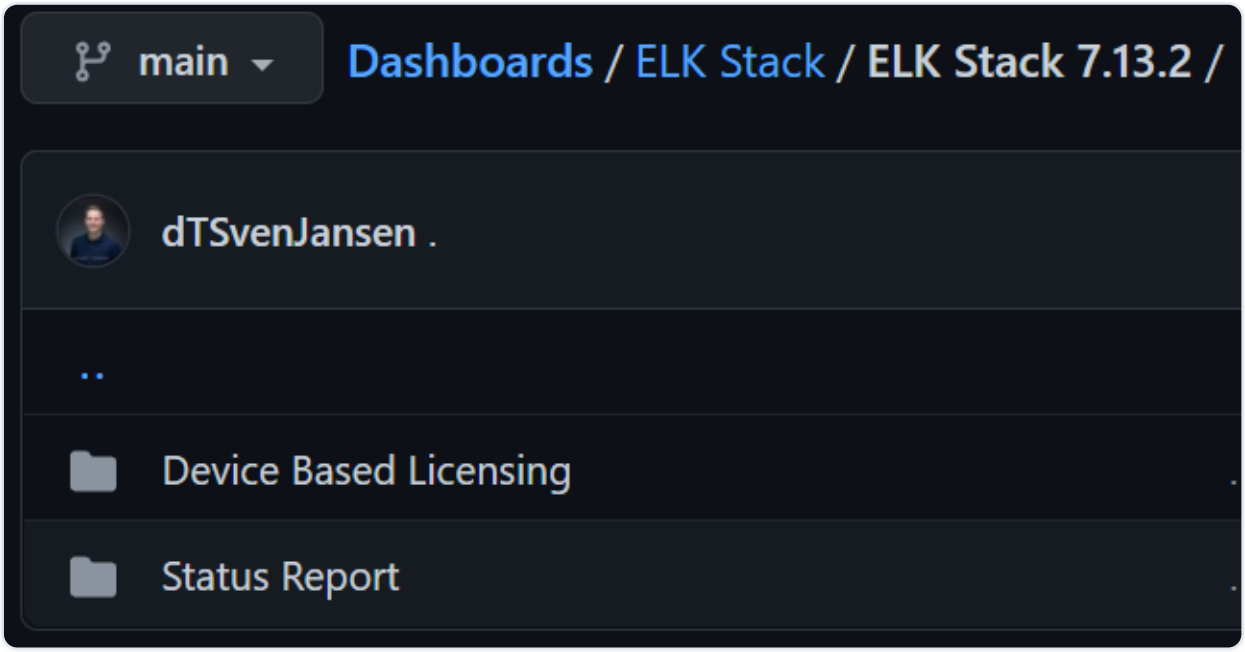
NOTE:

Saved objects for ELK are not backward compatible. Please use only versions matching or older than your system.

- Select the version number matching your ELK Stack system and download the files. You can of course also clone the whole repository if you like.



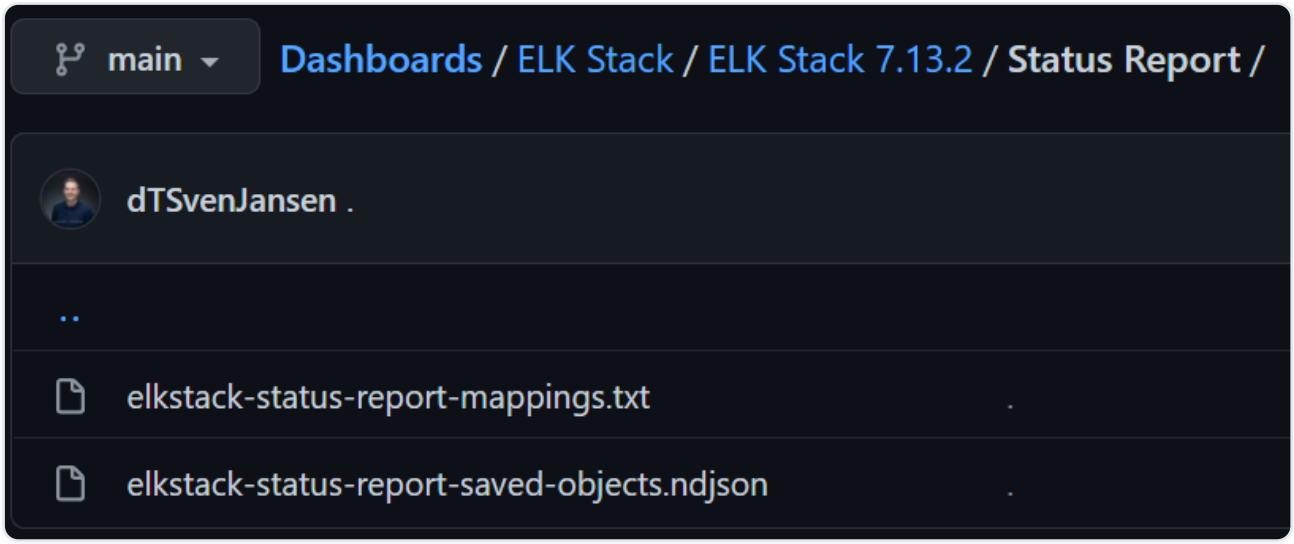
Every version folder contains folders for each use case. Each of these use case folders contains the relevant stored object and mapping files.



Each use case folder contains the following files:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

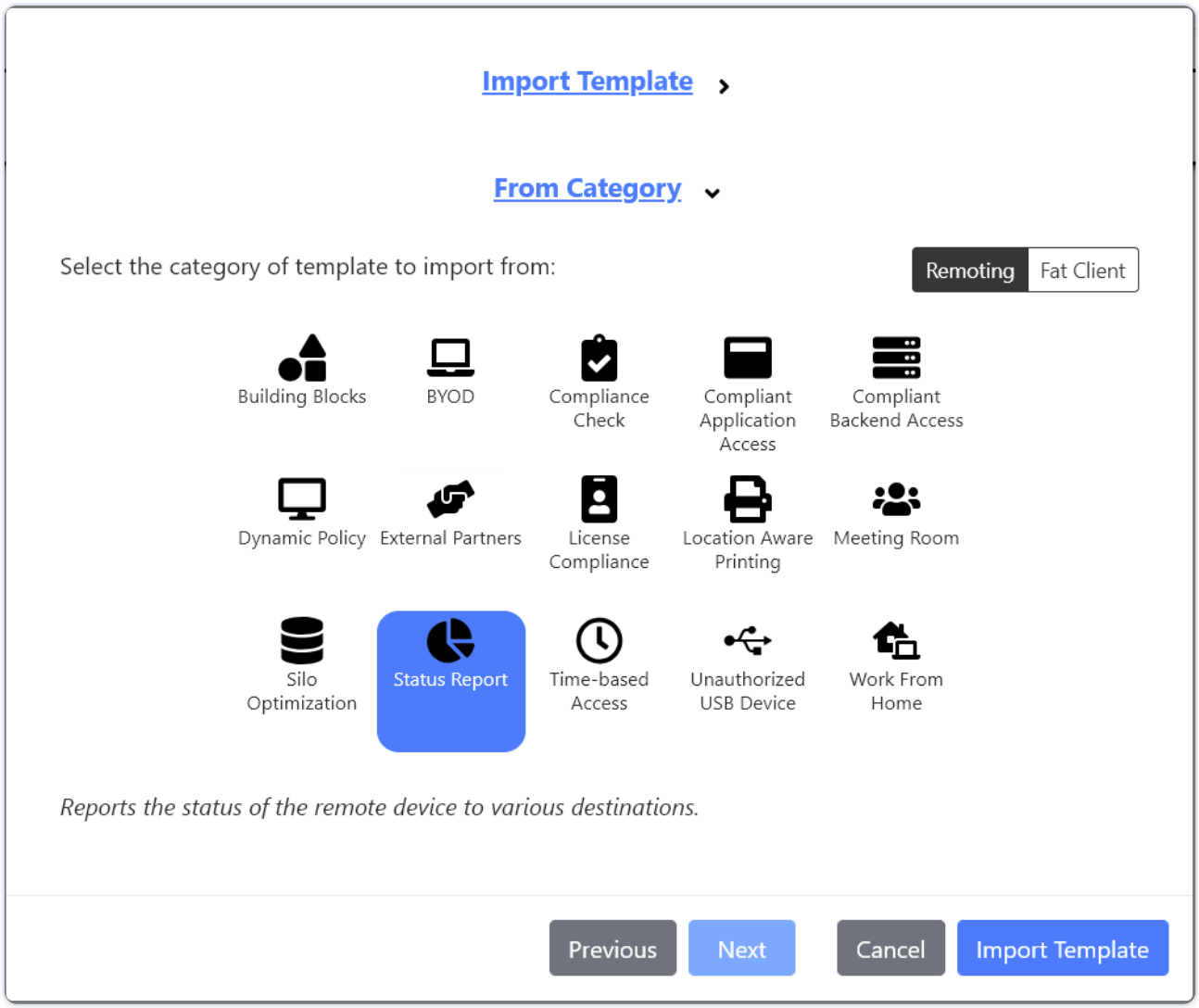
- `elkstack-<use case>-mappings.txt` contains data definitions for the data being sent to ELK Stack index mapping.
- `elkstack-<use case>-saved-objects.ndjson` contains all objects that are required to store, search and visualize data, such as indexes, scripted fields, dashboards and searches.



Step 1.2: Components - Templates

deviceTRUST must be configured to send the required data for each use case. Templates for both use cases are included in the deviceTRUST Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 2: The Device-Based Licensing Report

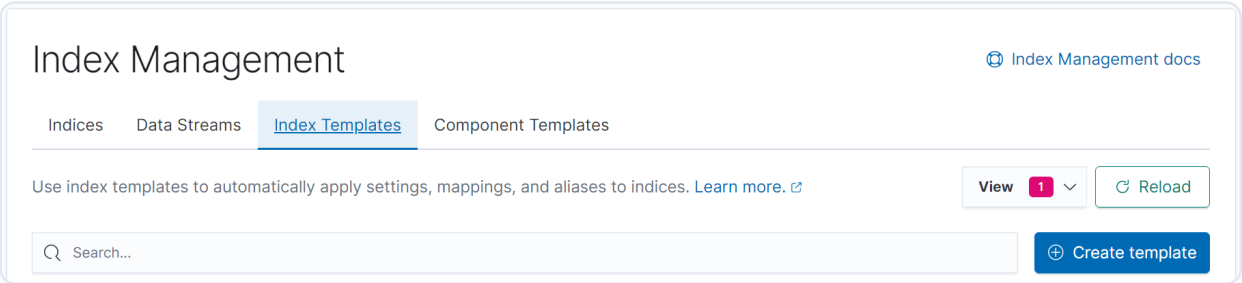
This part of the guide relates to `Device-Based Licensing`. It lists all steps that are required to configure the ELK Stack, and also how to configure the deviceTRUST Agent.

Step 2.1: Add Index Template to ELK Stack

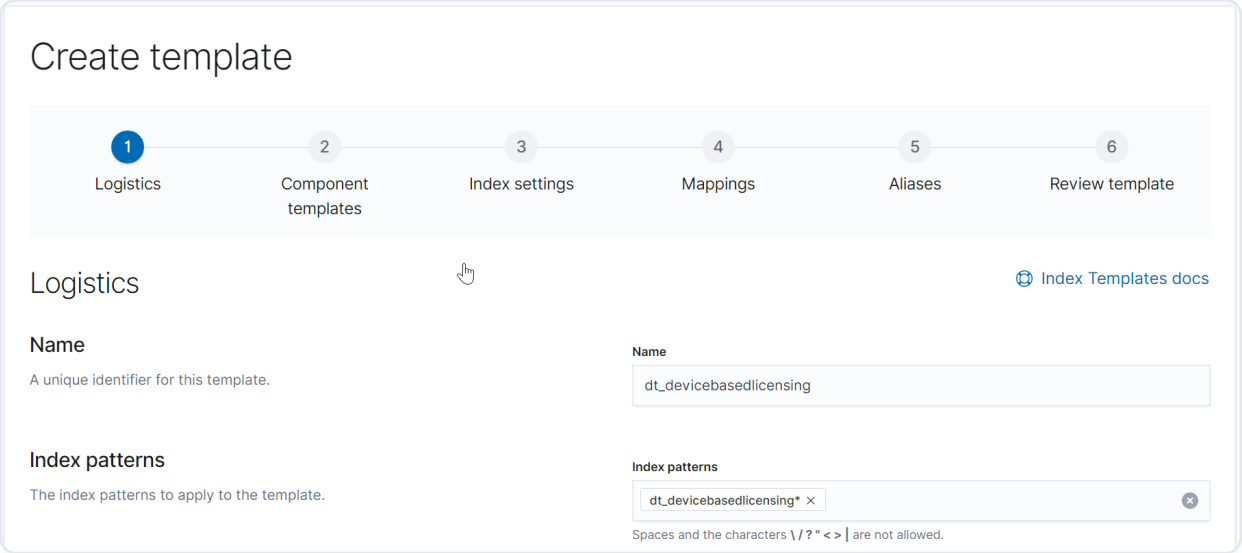
The first step is to create an `Index Template`. Index Templates describe the data that is being sent to an index. They make sure that every date is treated according to its type.

- Within the ELK Stack management console, navigate to `Menu\Stack Management\Index Management\Index Templates`.
- Click `Create Template`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

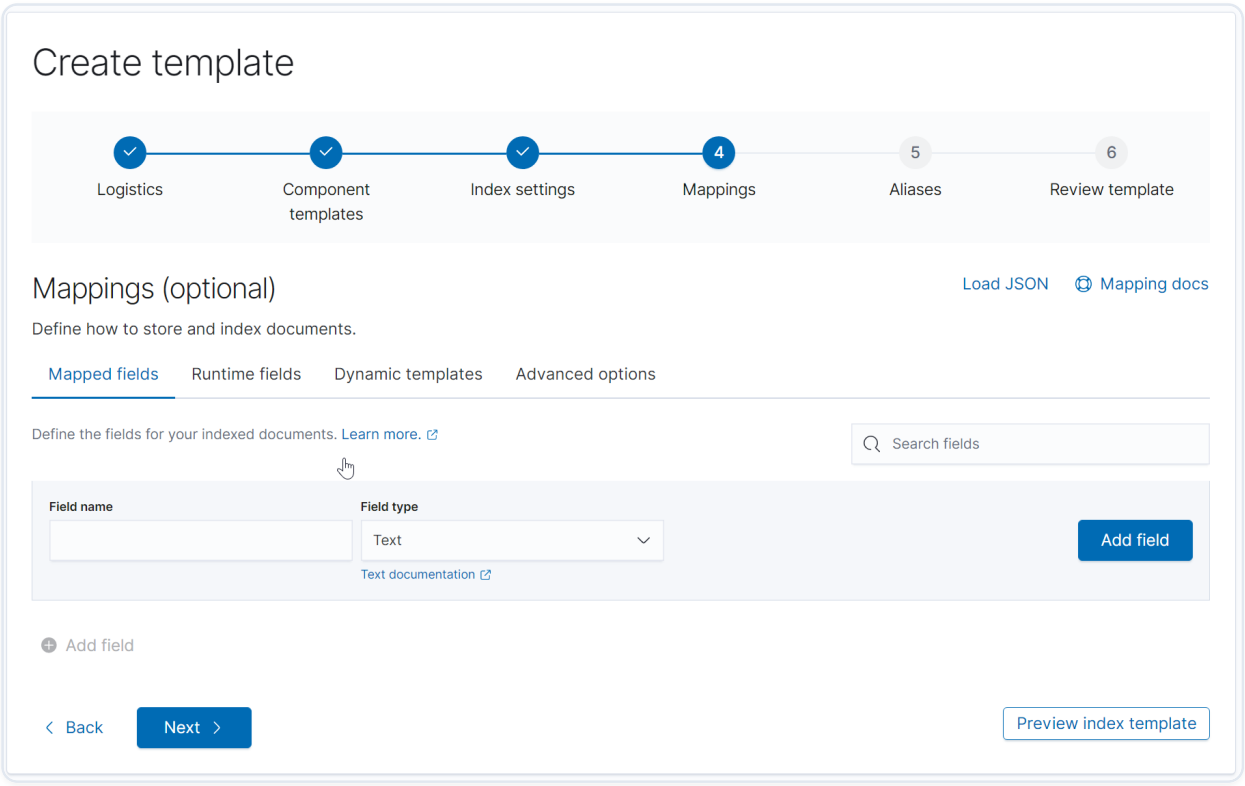


- Set `Name` to `dt_devicebasedlicensing`.
- Set `Index Patterns` to `dt_devicebasedlicensing*`.



- Skip all options until `Mappings`.
- Select `Load Json` to import the file `elkstack-device-based-licensing-mappings.txt` that was downloaded in Step 1.1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Proceed with `Load and overwrite`.

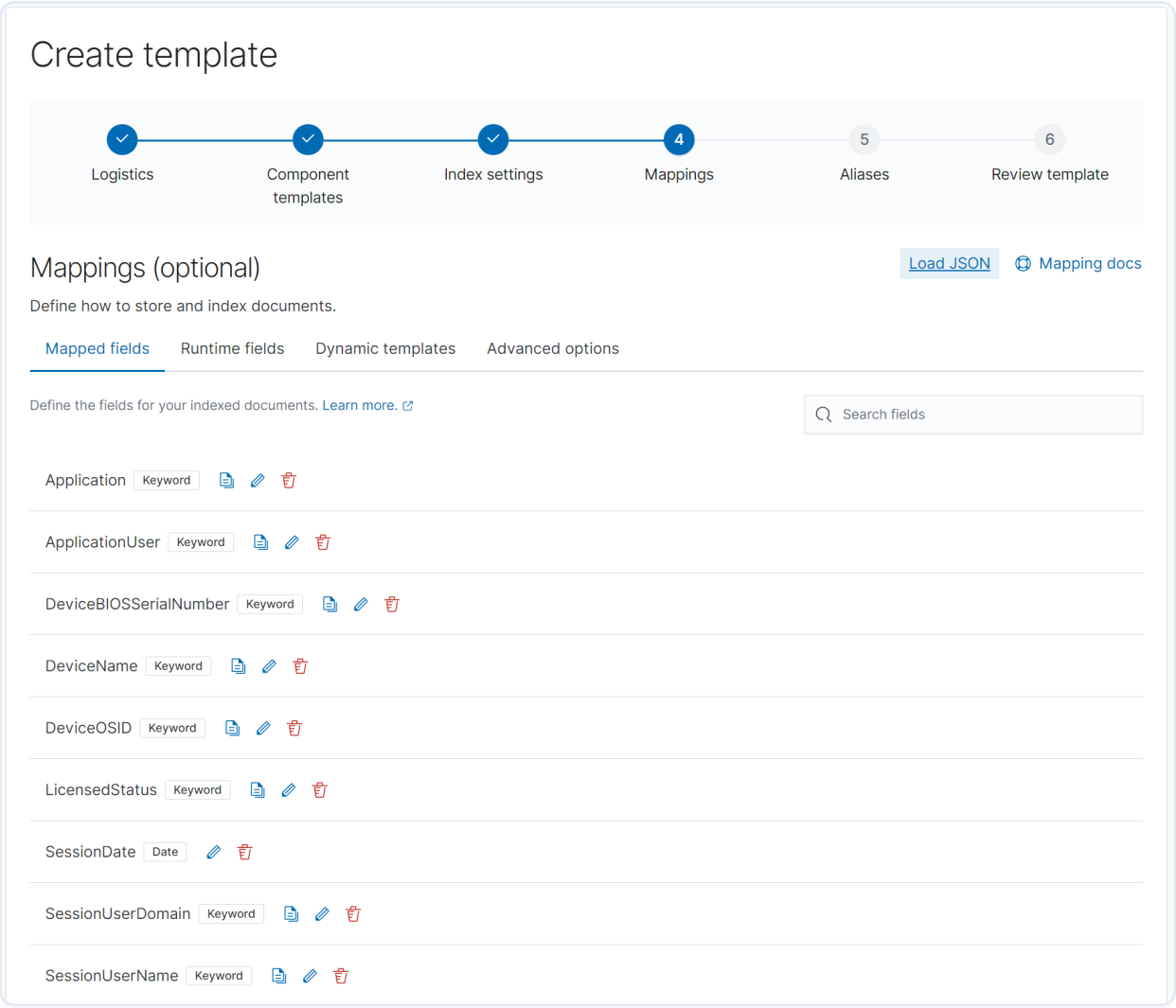
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The imported mappings are displayed. Please review them carefully.

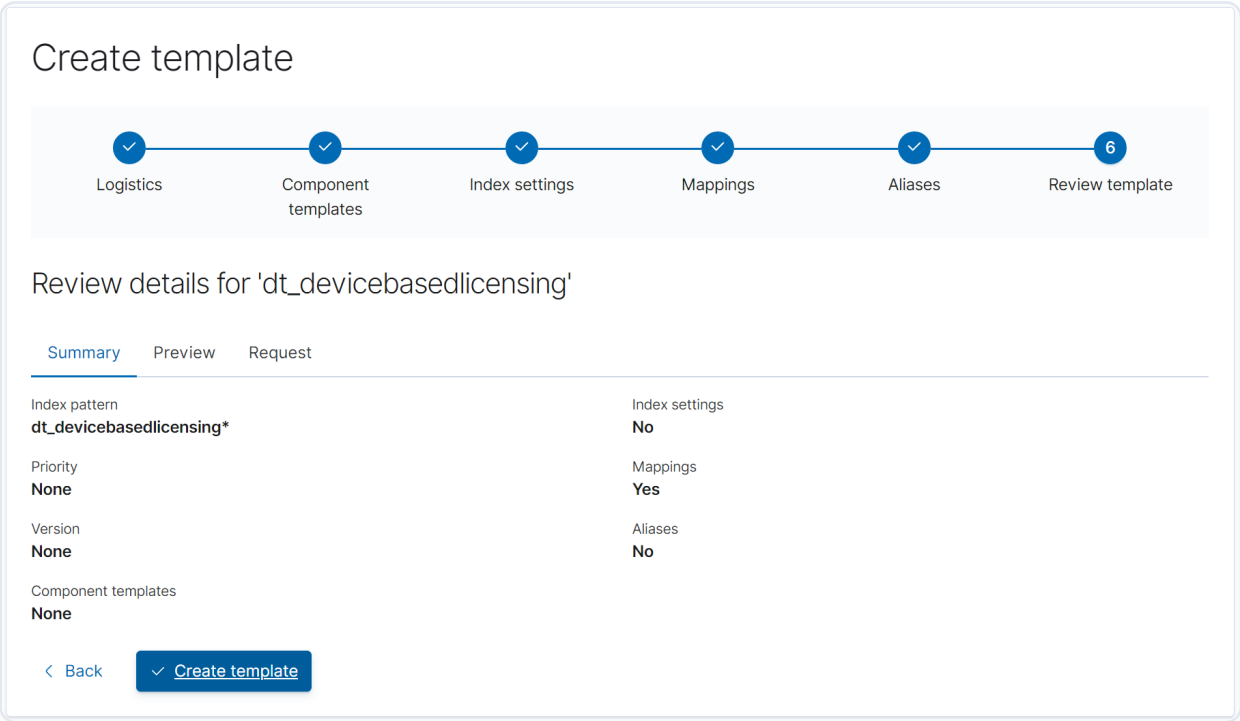
- `SessionDate` needs to be recognized as type `Date` for the report to function properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

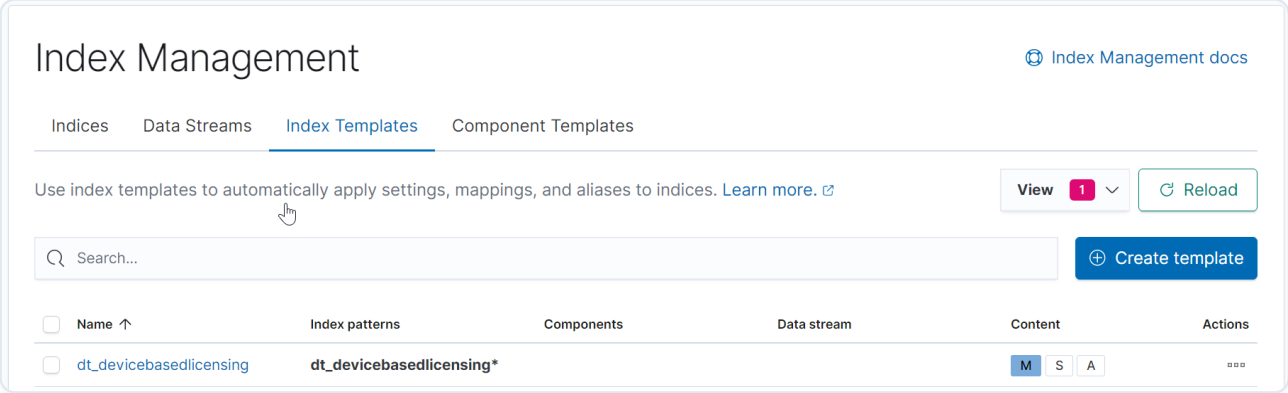


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You'll be given an overview of the created template. A blue marked `M` in the `Content` section indicates that mappings are available.

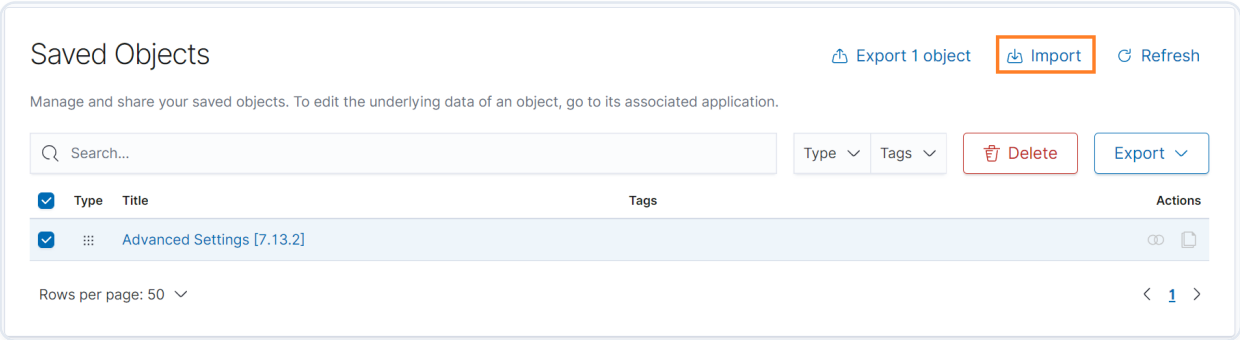


Step 2.2: Import Saved Objects to ELK Stack

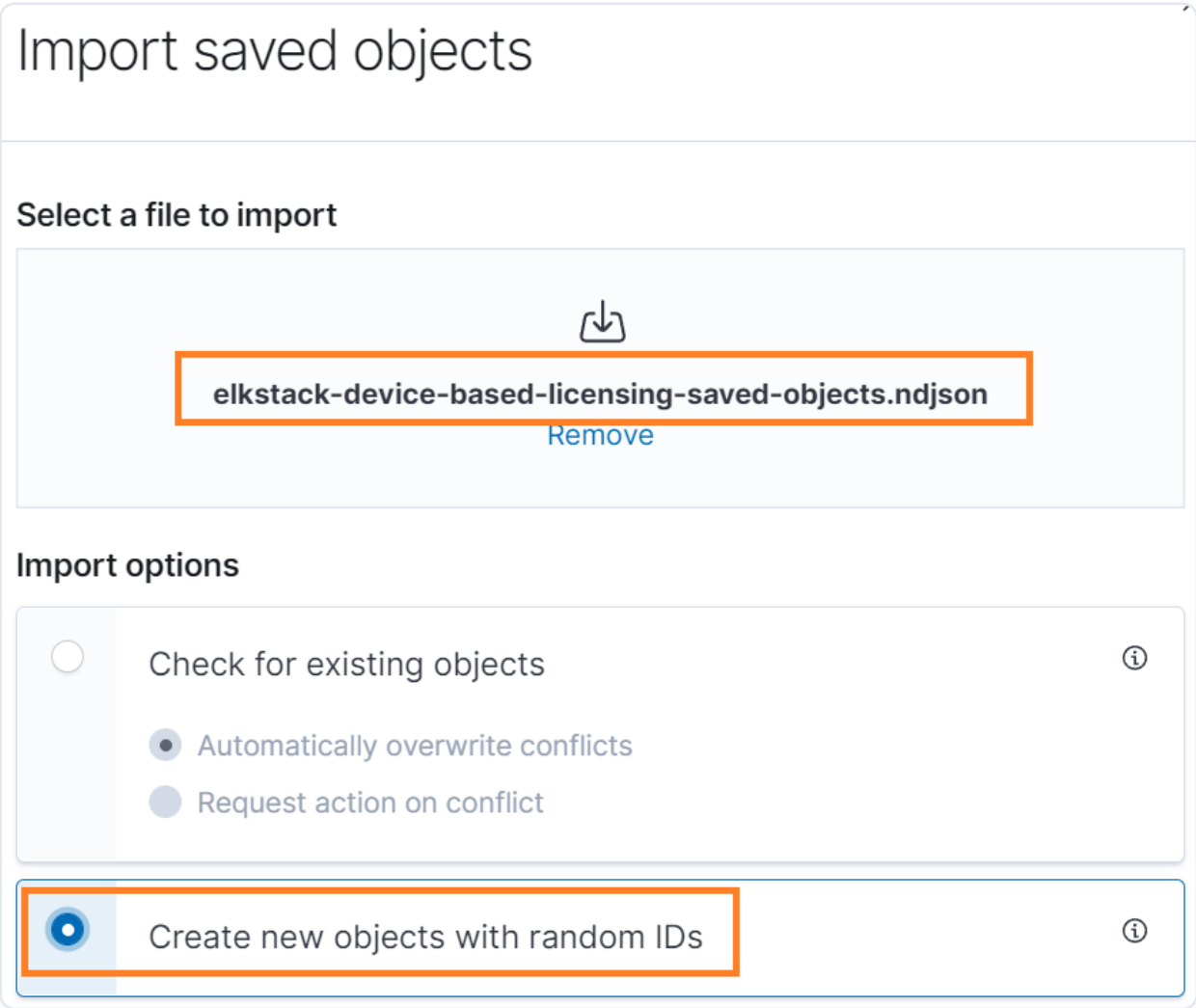
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

- Navigate to `Menu\Stack Management\Saved Objects` in your ELK Stack management console.
- Click `Import`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

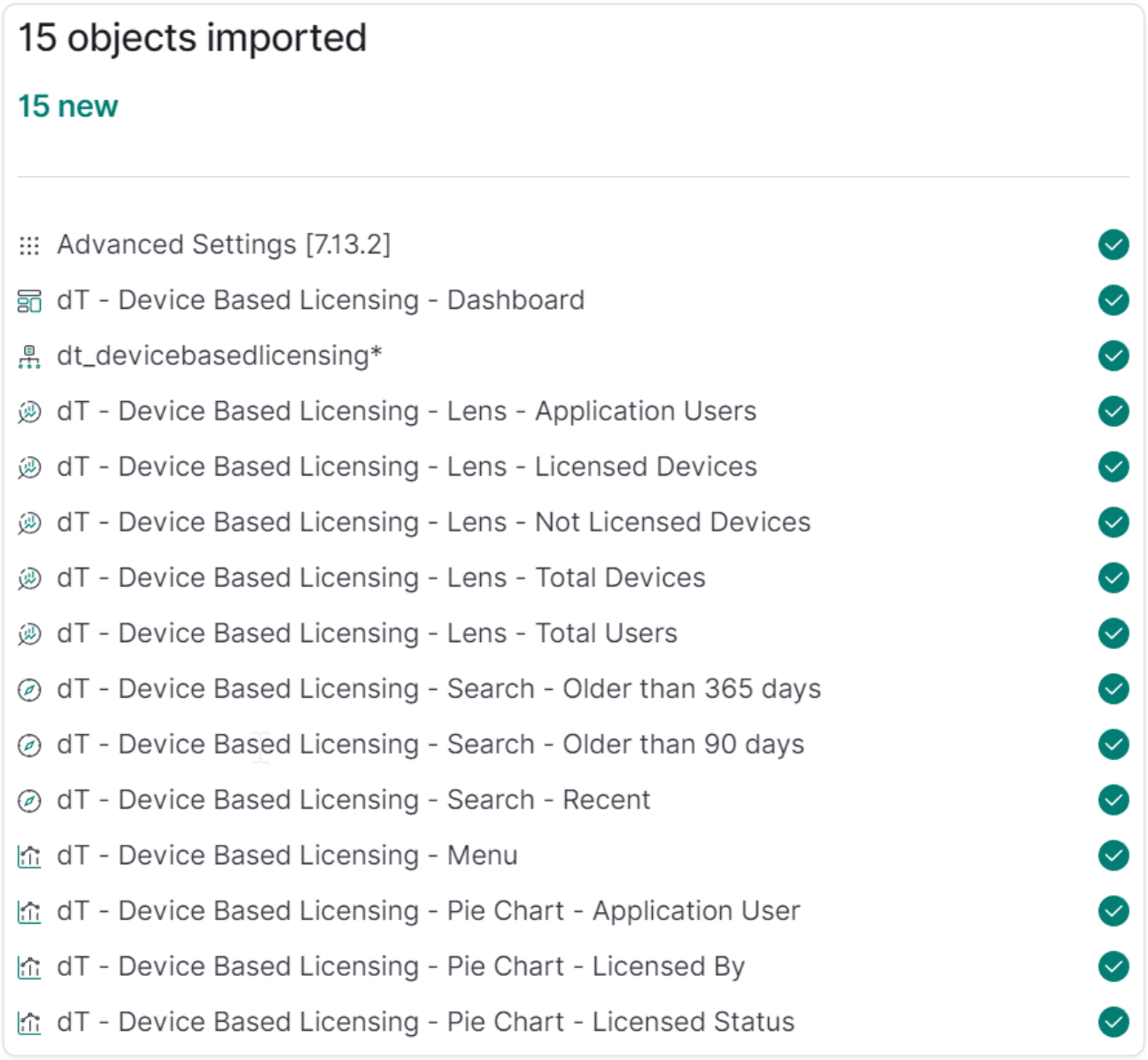


- Select the file `elkstack-device-based-licensing-saved-objects.ndjson`.
- Check `Create new objects with random IDs` to make sure no existing objects are altered.



After importing, an overview of the imported objects will be displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



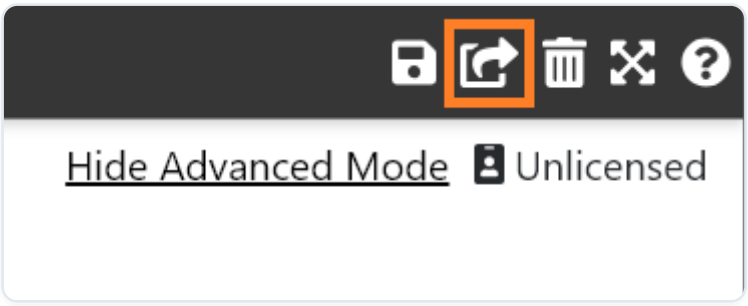
Step 2.3: Configuring deviceTRUST

After the Index Mapping has been created and the Saved Objects are included, the ELK Stack is prepared for storing, sorting, and displaying your data.

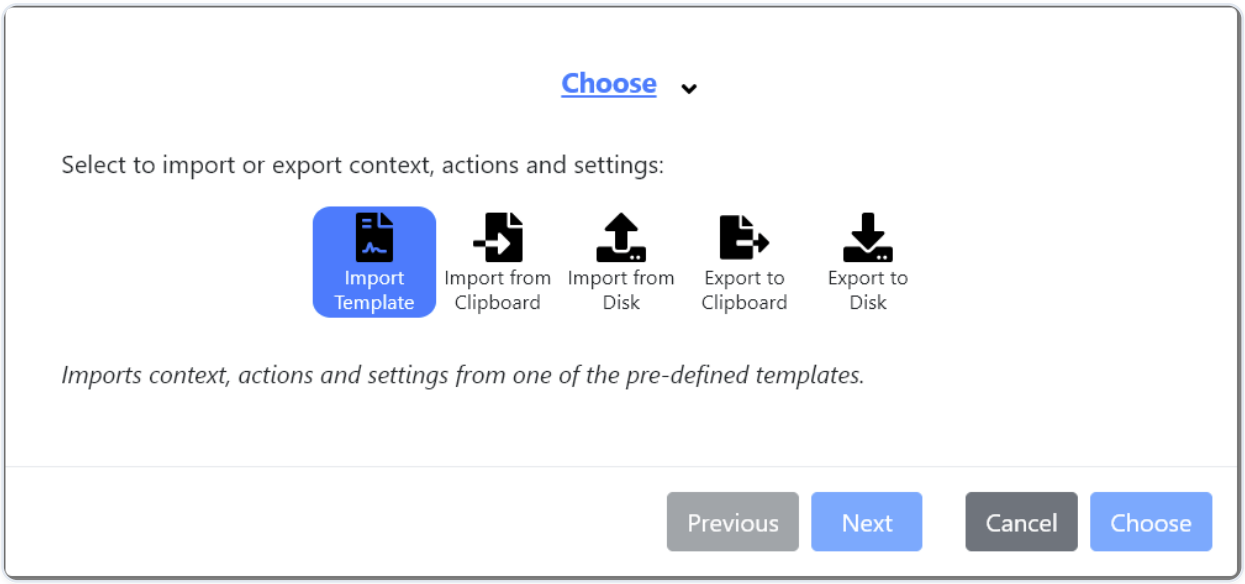
The final step is to create the deviceTRUST configuration that will make sure all the required data is provided.

- Open the `deviceTRUST Console`.
- Click `Sharing` in the top right menu. You may need to click `Show Advanced View` if this button is not visible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

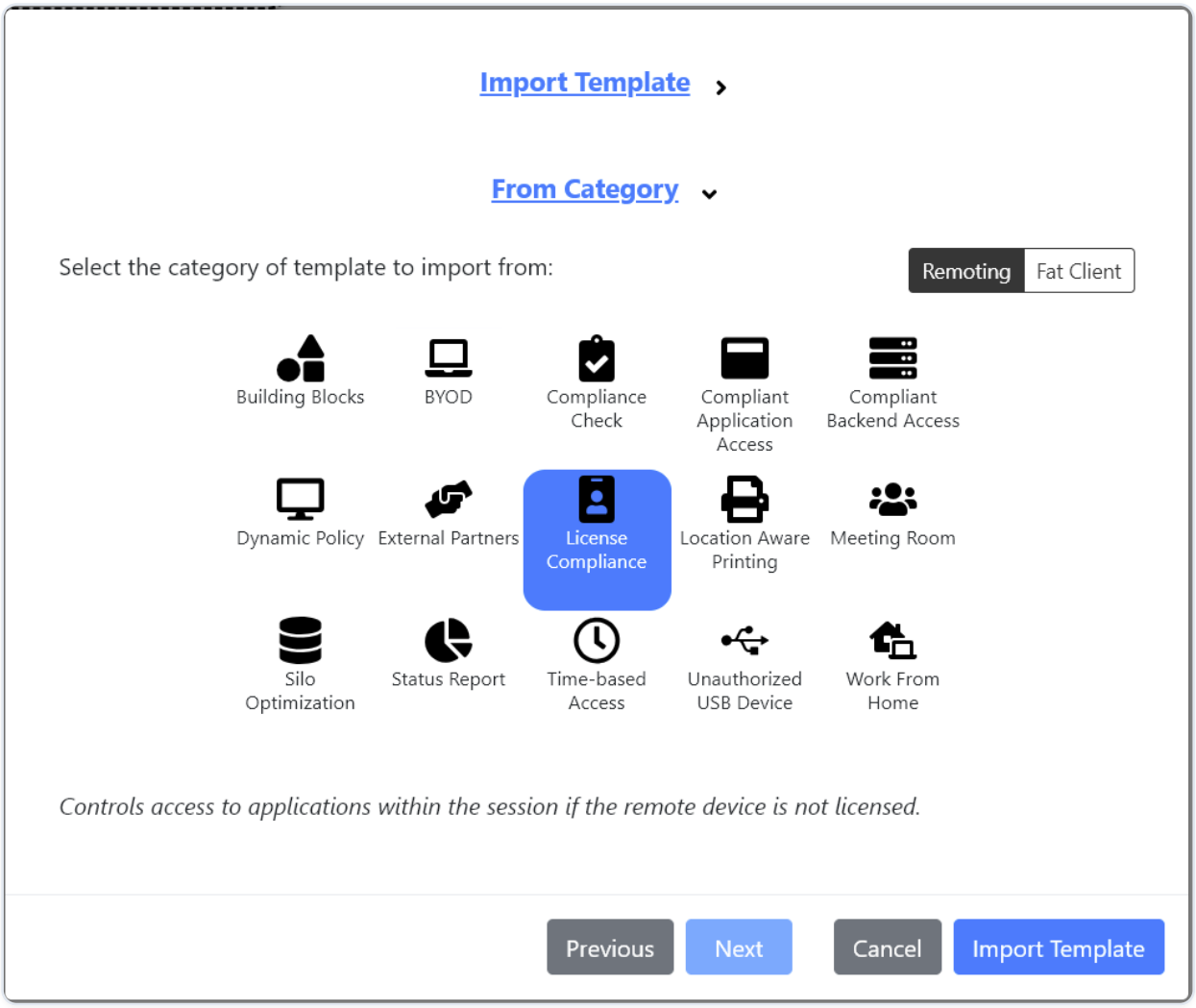


- Select `Import Template`.



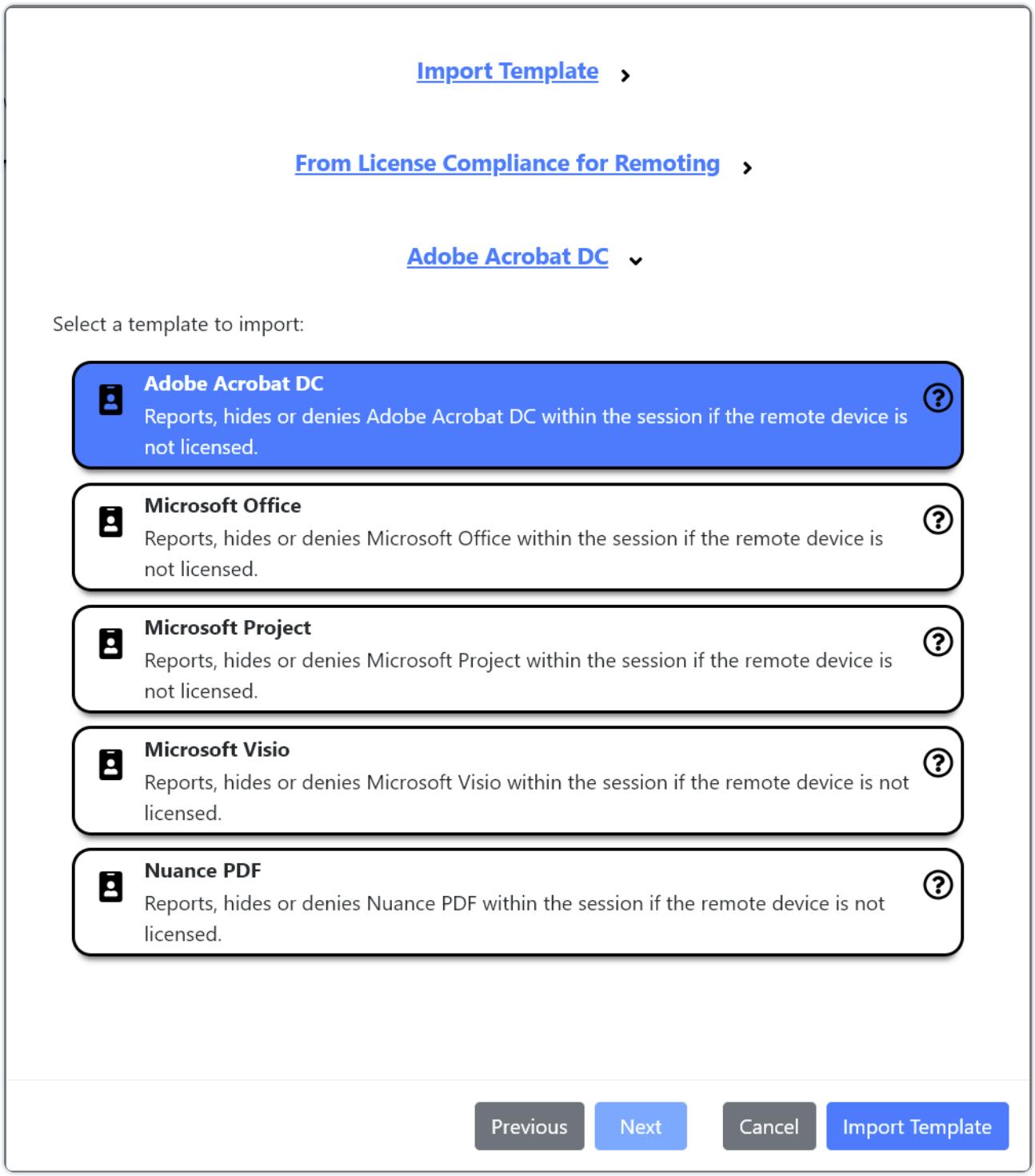
- For `Device-Based Licensing`, the template category `License Compliance` is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This category contains templates for several software products. This example uses `Acrobat DC`, but can easily be customised for other applications.

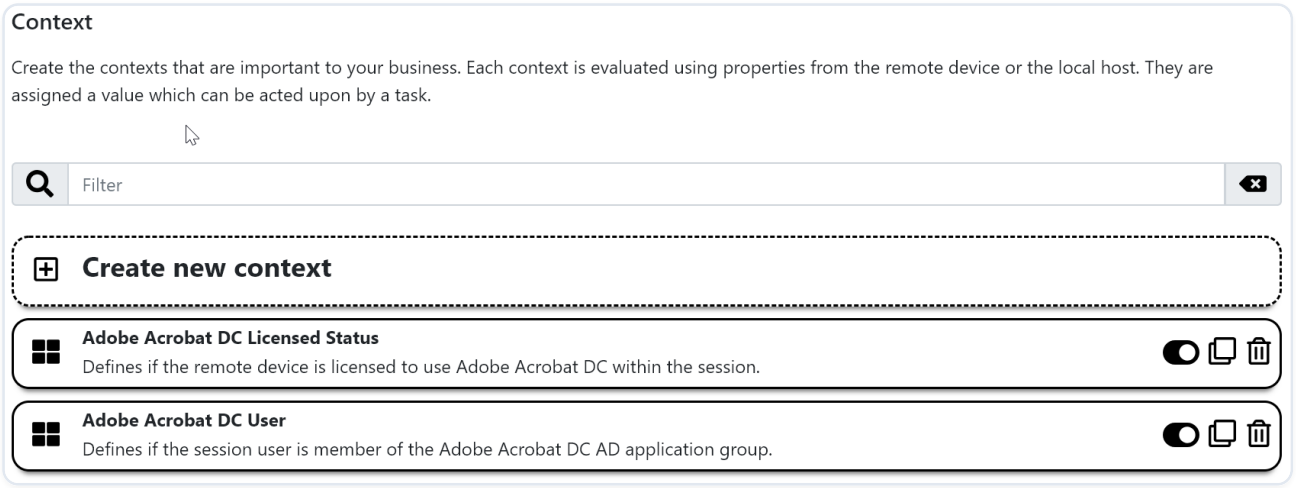
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Two contexts are included:

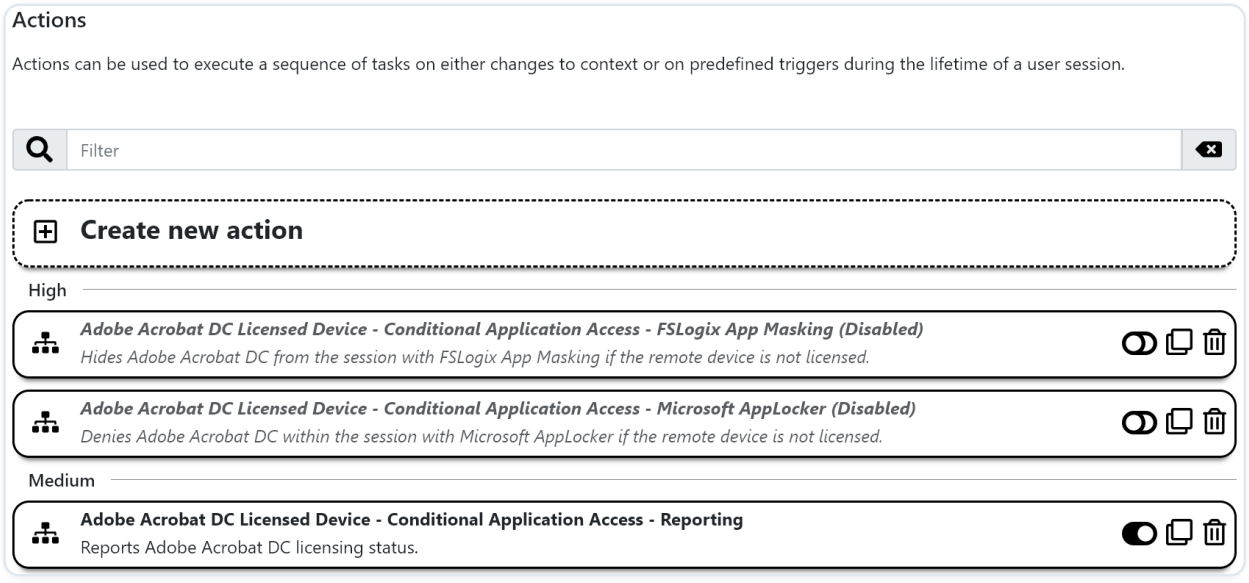
- `Adobe Acrobat DC Licensed Status` to evaluate the device's license status.
- `Adobe Acrobar DC User` to define if the accessing user shall or shall not be using the software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



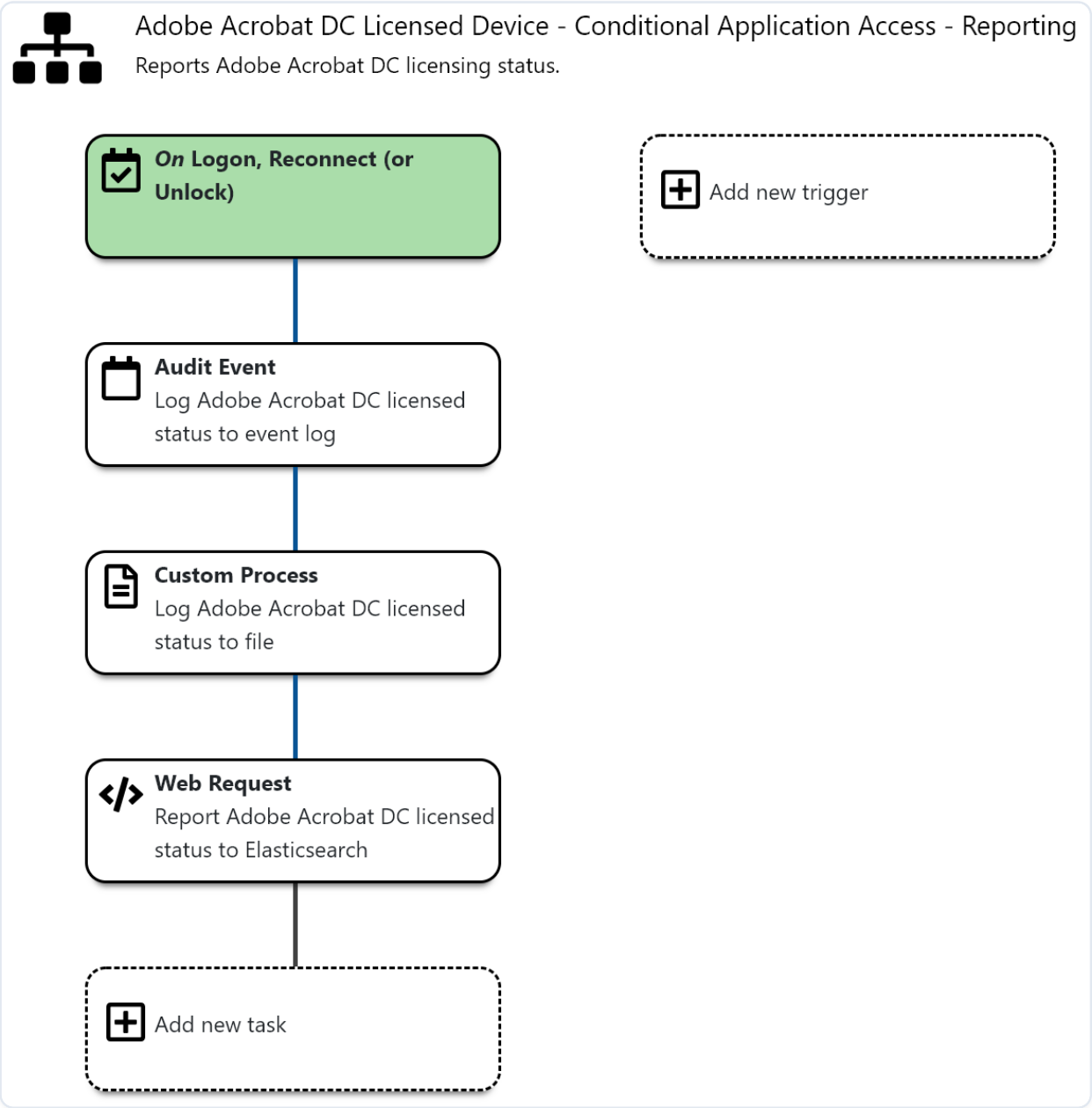
Three actions are included:

- `Adobe Acrobat DC Licensed Device - Conditional Application Access - FSLogix App Masking` is used for controlling access to the software using FSLogix App Masking. This action can be ignored or removed for now.
- `Adobe Acrobat DC Licensed Device - Conditional Application Access - Microsoft AppLocker` is used for controlling access to the software using Microsoft Applocker. This action can be ignored or removed for now.
- `Adobe Acrobat DC Licensed Device - Conditional Application Access - Reporting` is the only action required for reporting.



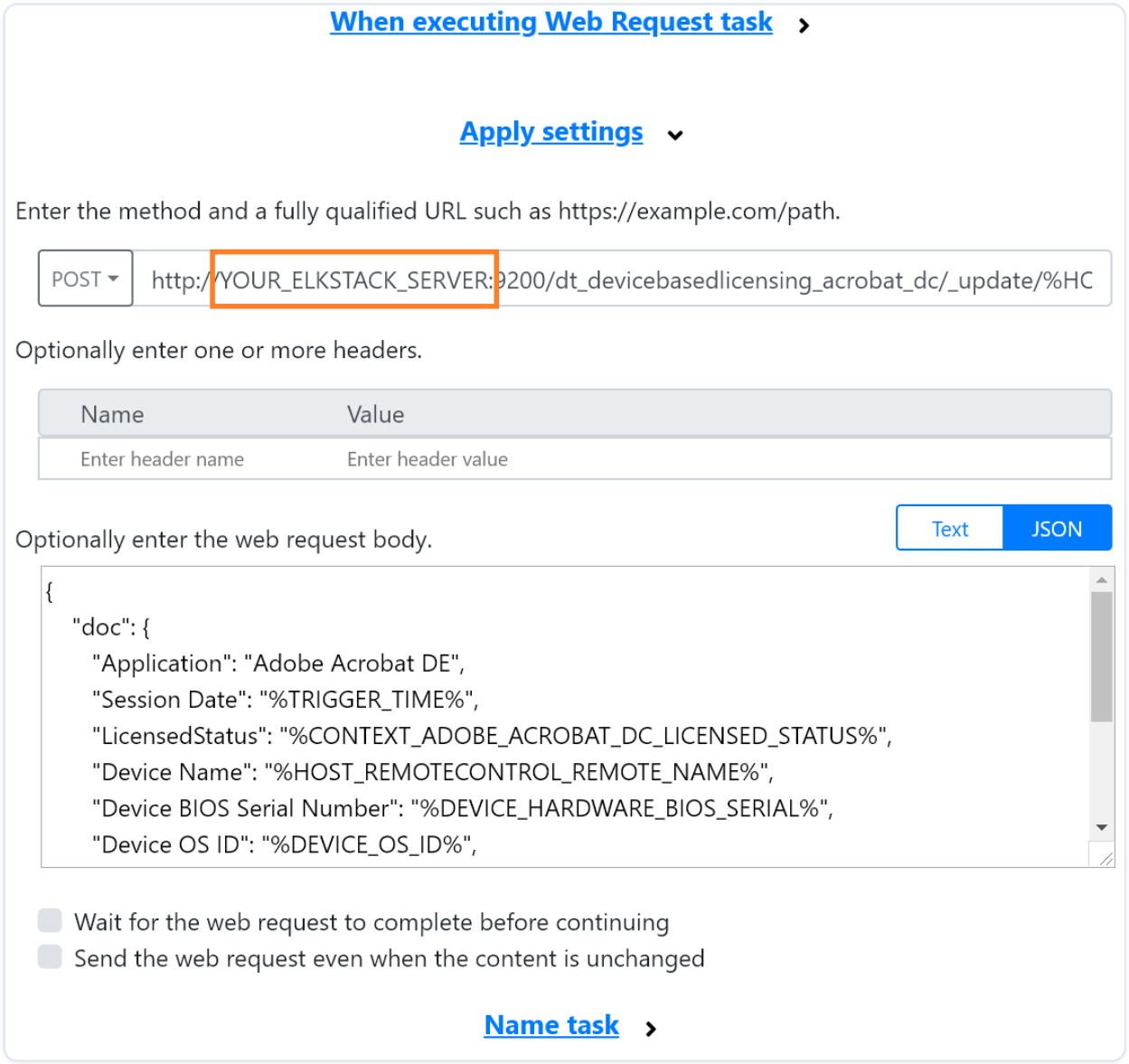
- The action contains multiple ways to store the data. Sending data to ELK Stack is configured by using a `Web Request` task. The `Audit Event`, `Custom Process`, as well as the `Web Request` Tasks for Splunk and Graylog can be deleted, as we are looking at ELK Stack here.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The Web Request task must be edited to suit your environment. If you use a basic setup without SSL or authorization, adding `your server's fqdn` is the only required configuration change.

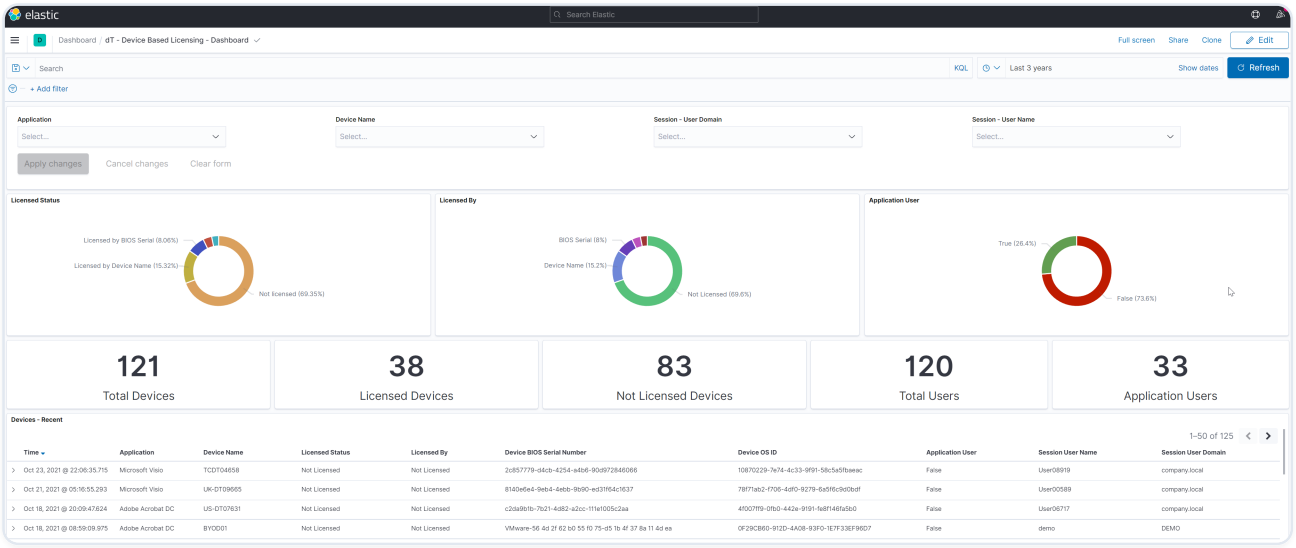
© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the index template has been created, the saved objects are imported and the agent-side has been configured, the use case `Device-Based Licensing` has been implemented successfully.

deviceTRUST now sends status data about the application usage and the required hardware information to ELK Stack on every access to the remoting system. The data is presented in the created dashboards.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



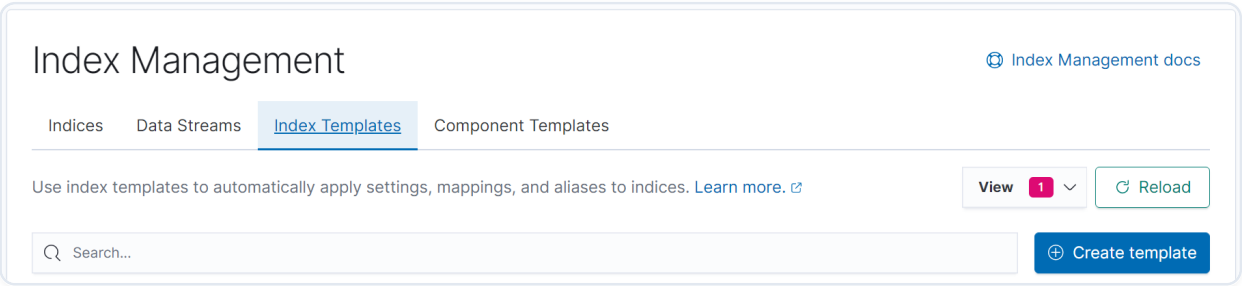
Step 3: The Status Report

This part of the guide relates to the `Status Report`. It lists all steps that are required to configure the use case on the agent-side, as well as on the ELK Stack side.

Step 3.1: Add Index Template to ELK Stack

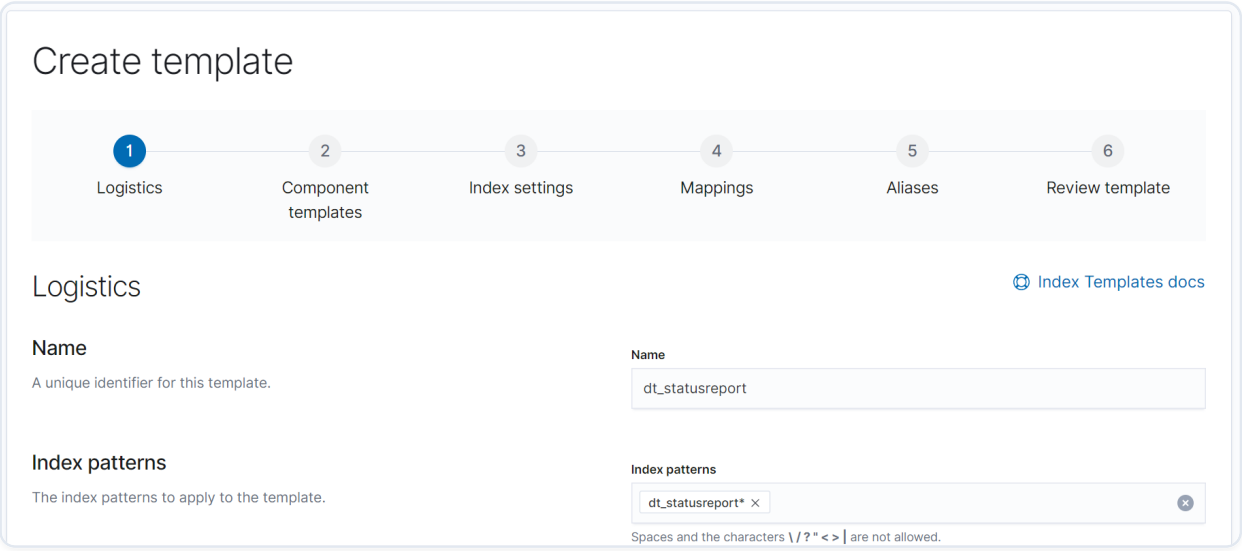
The first step is to create an `Index Template`. Index Templates describe the data that is being sent to an index. They make sure, that every date is treated according to its type.

- Within the ELK Stack management console, navigate to `Menu\Stack Management\Index Management\Index Templates`.
- Click `Create Template`.

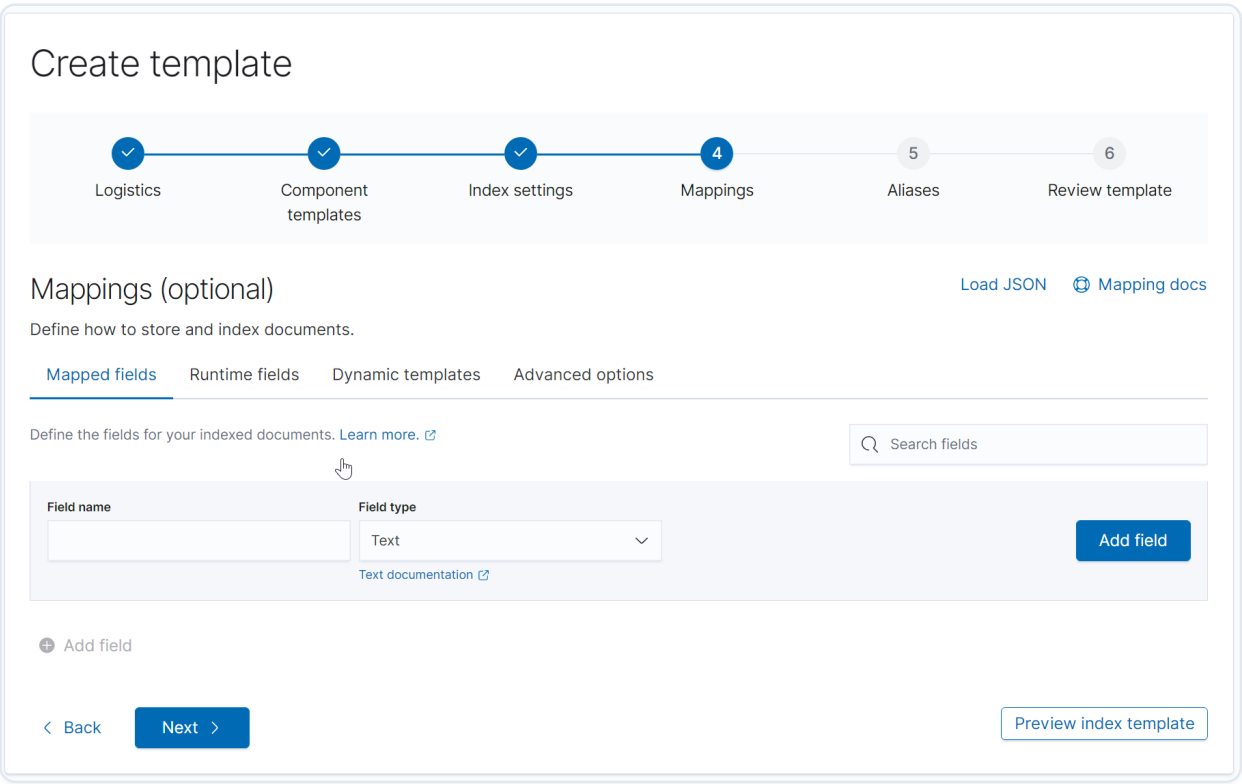


- Set `Name` to `dt_statusreport`.
- Set `Index Patterns` to `dt_statusreport*`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Skip all options until `Mappings`.
- Select `Load Json` to import the `elkstack-status-report-mappings.txt` that was downloaded in Step 1.1.



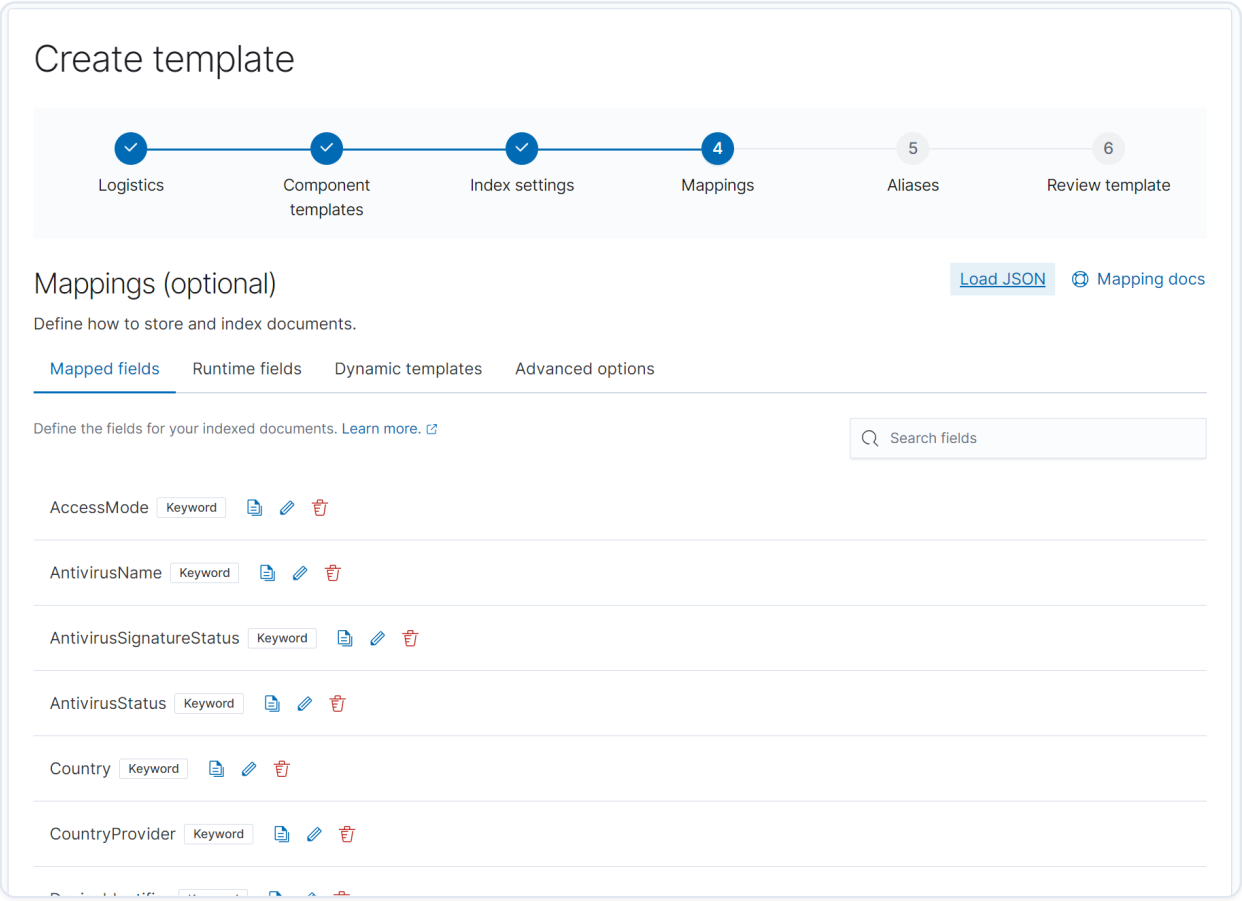
- Proceed with `Load and overwrite`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

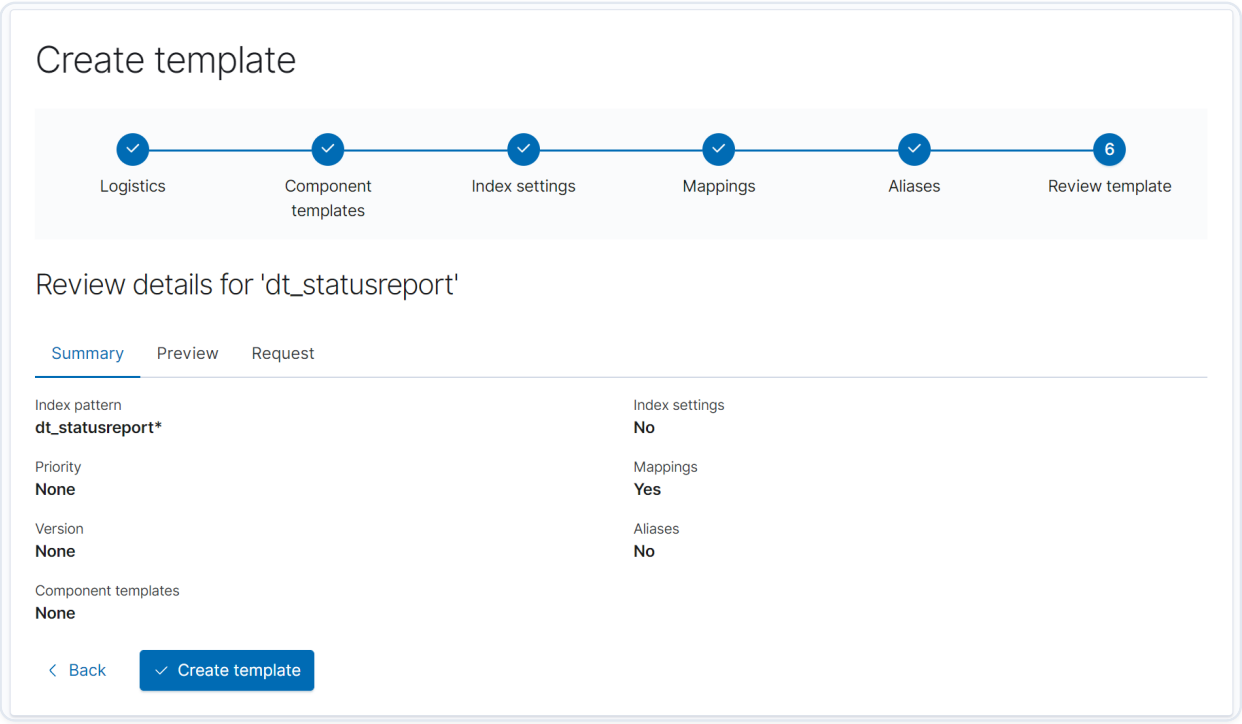


- The imported mappings are displayed. Please review them carefully. `Session Date`, `Anti-Virus Timestamp` and `Hardware BIOS Release Date` need to be recognized as type `Date` for the report to function properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

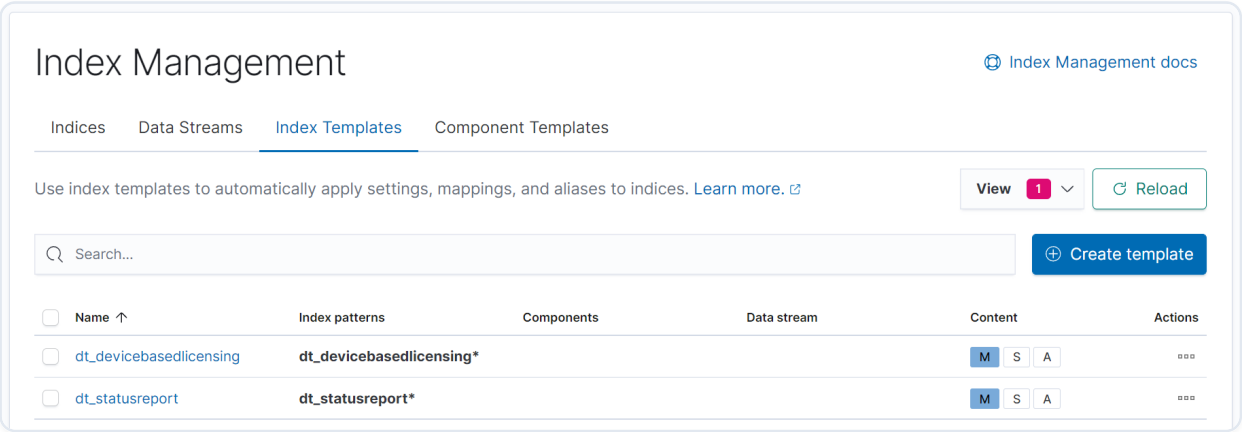


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.



- You'll be given an overview of the created template. A blue marked `M` in the `Content` section indicates, that mappings are available.

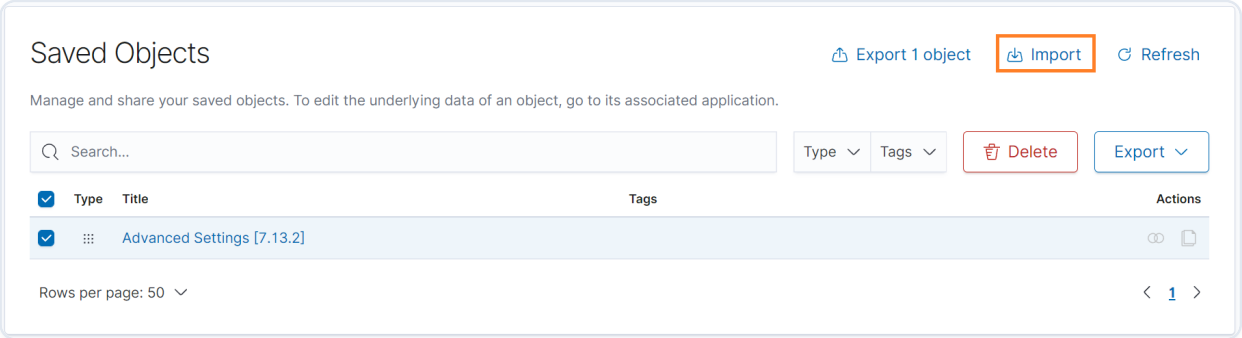
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3.2: Import Saved Objects to ELK Stack

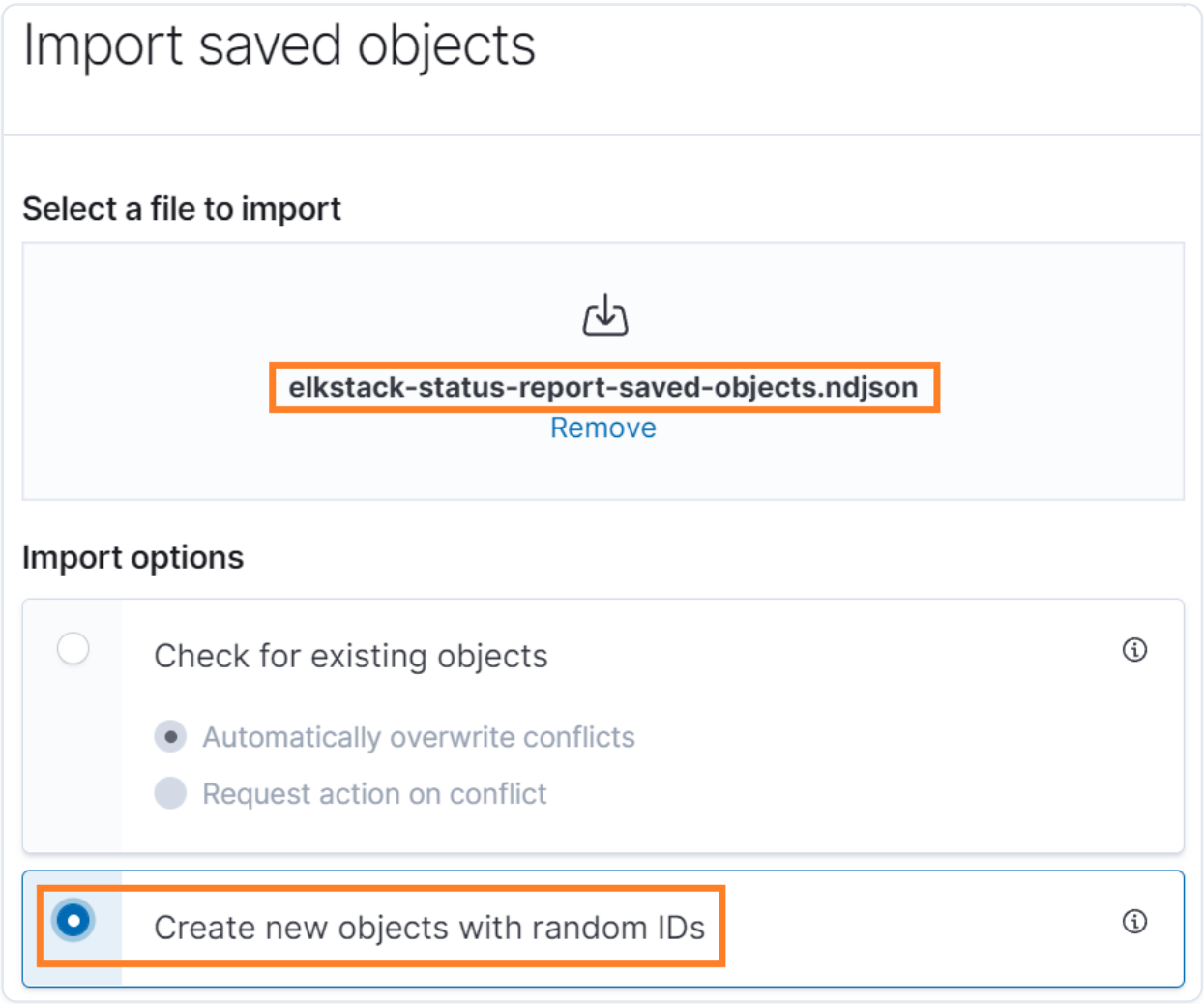
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

- Navigate to `Menu\Stack Management\Saved Objects` in your ELK Stack management console.
- Click `Import`.



- Select the file `elkstack-status-report-saved-objects.ndjson`.
- Check `Create new objects with random IDs` to make sure no existing objects are altered.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After importing, an overview of the imported objects will be displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Import saved objects

60 objects imported

60 new

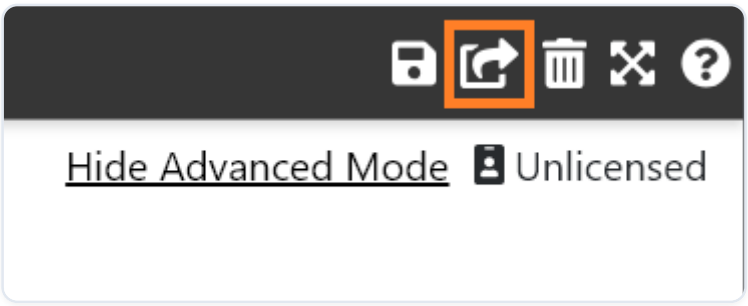
- Advanced Settings [7.13.2]
- dT - Status Report - Dashboard - Hardware
- dT - Status Report - Dashboard - Location
- dT - Status Report - Dashboard - Network
- dT - Status Report - Dashboard - OS
- dT - Status Report - Dashboard - Overview
- dT - Status Report - Dashboard - Remote User
- dT - Status Report - Dashboard - Security
- dT - Status Report - Dashboard - Software
- dt_statusreport*
- dT - Status Report - Lens - Protected Devices
- dT - Status Report - Lens - Protected Devices Over Time
- dT - Status Report - Lens - Total Unique Devices
- dT - Status Report - Lens - Total Unique Users
- dT - Status Report - Lens - Unprotected Devices
- dT - Status Report - Search - Hardware
- dT - Status Report - Search - Location
- dT - Status Report - Search - Network
- dT - Status Report - Search - OS
- dT - Status Report - Search - Overview
- dT - Status Report - Search - Remote User
- dT - Status Report - Search - Security
- dT - Status Report - Search - Software
- dT - Status Report - Menu
- dT - Status Report - Vis - Remote Device - AccessMode
- dT - Status Report - Vis - Remote Device - AntivirusStatus

Step 3.3: Configuring deviceTRUST

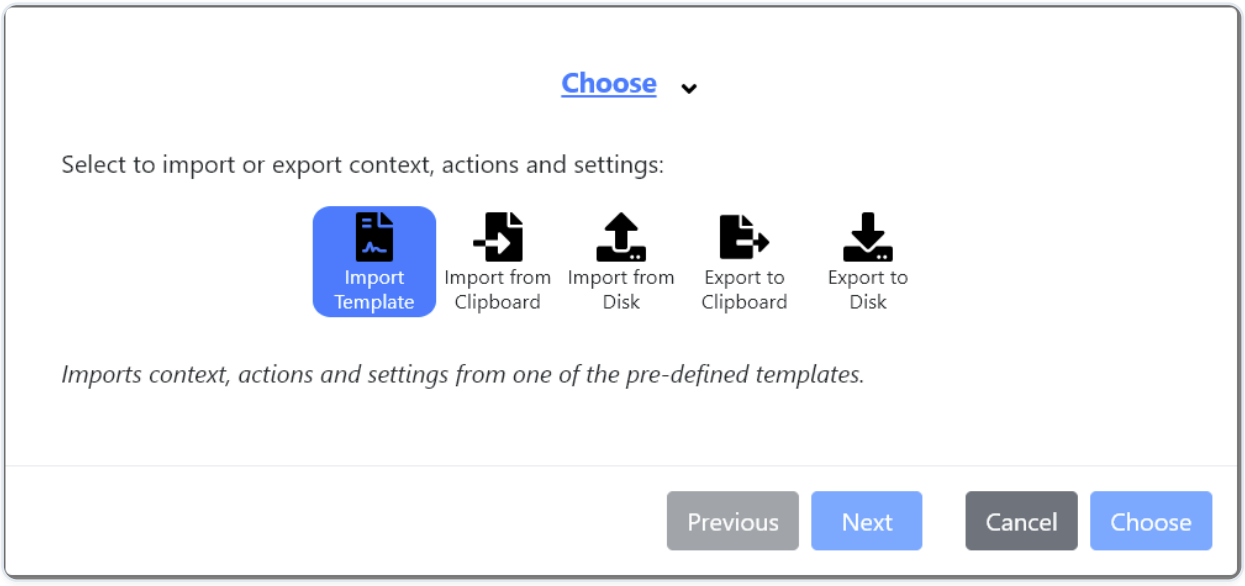
After the Index Mapping has been created, the Saved Objects are included the index has been edited and the agent-side has been configured, the ELK Stack is prepared for storing, sorting, and displaying your data.

The last step is to create the deviceTRUST configuration, that will make sure all required data is provided.

- Open the `deviceTRUST Console`.
- Click `Sharing` in the top right menu. You may need to click `Show Advanced View` if this button is not visible.



- Select `Import Template`.

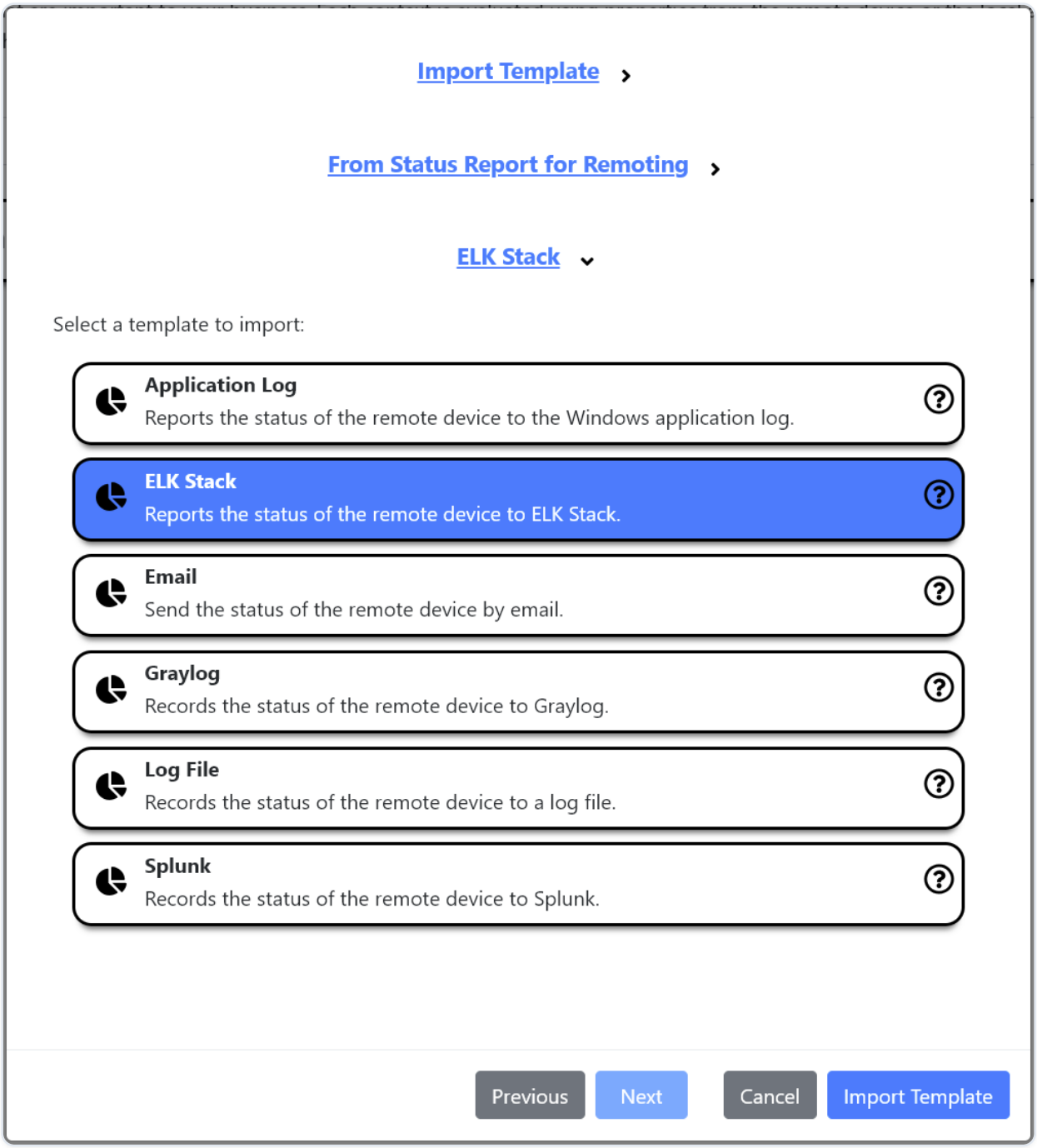


- For `Status Report`, the template category `Status Report` is used.

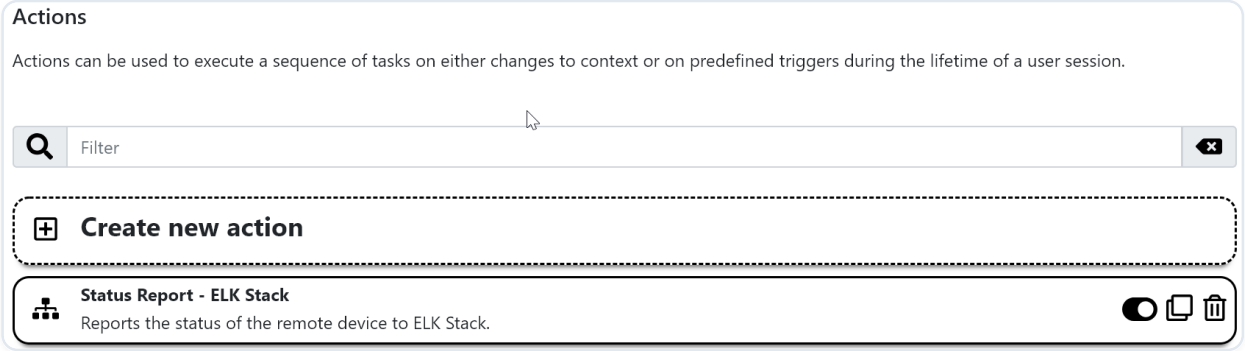


- This category contains templates for several ways of storing data. Choose `ELK Stack`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

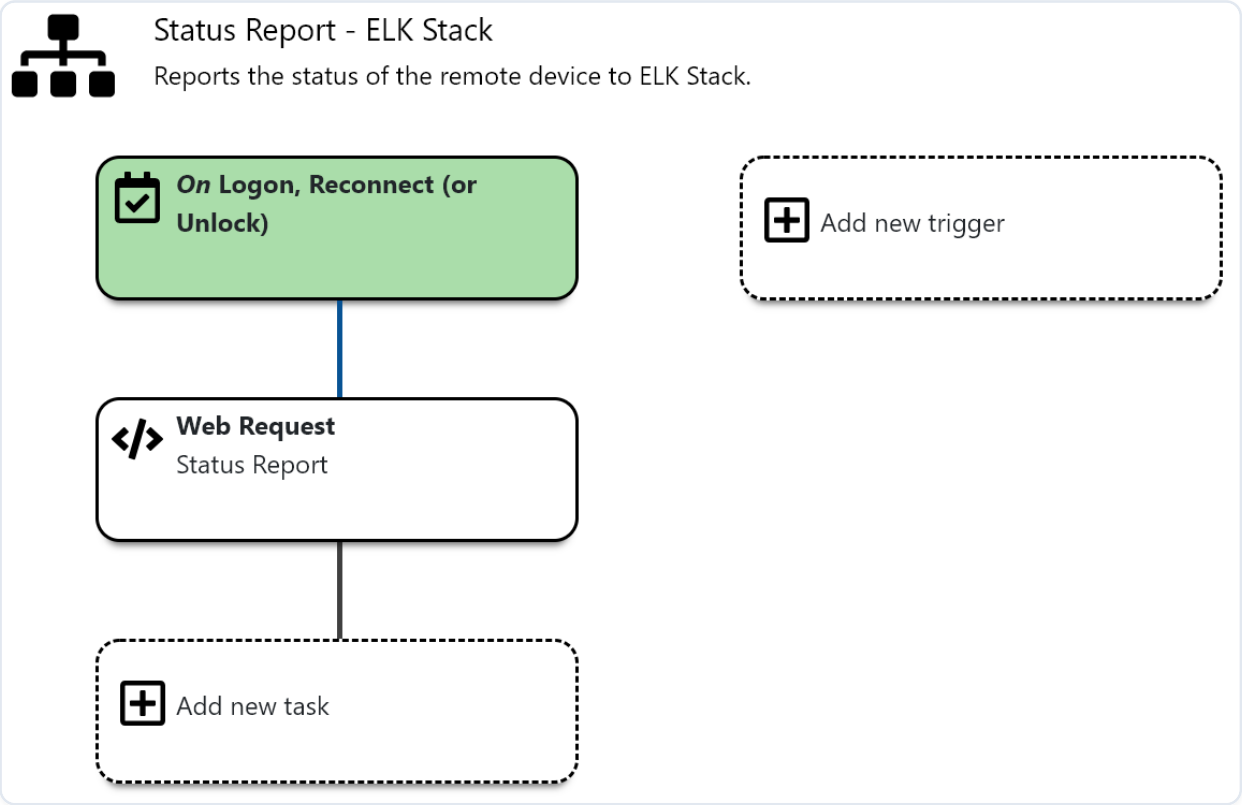


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – ELK Stack` collects all relevant data and sends them over to the ELK Stack.



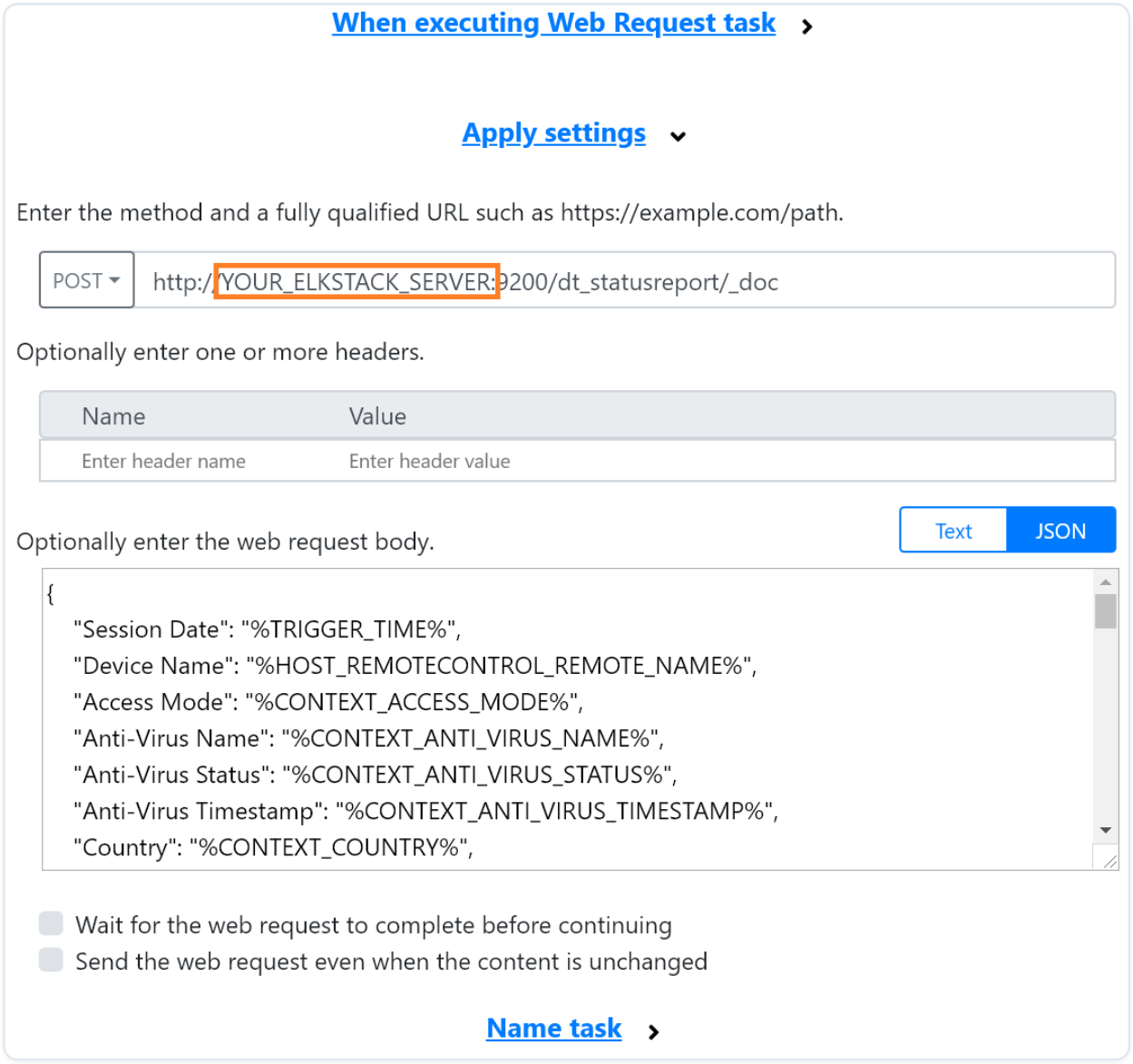
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sending data to ELK Stack is configured by using a `Web Request` task.



- The Web Request task must be edited to suit your environment. If you use a basic setup without SSL or authorization, simply adding your `server's fqdn` will do.

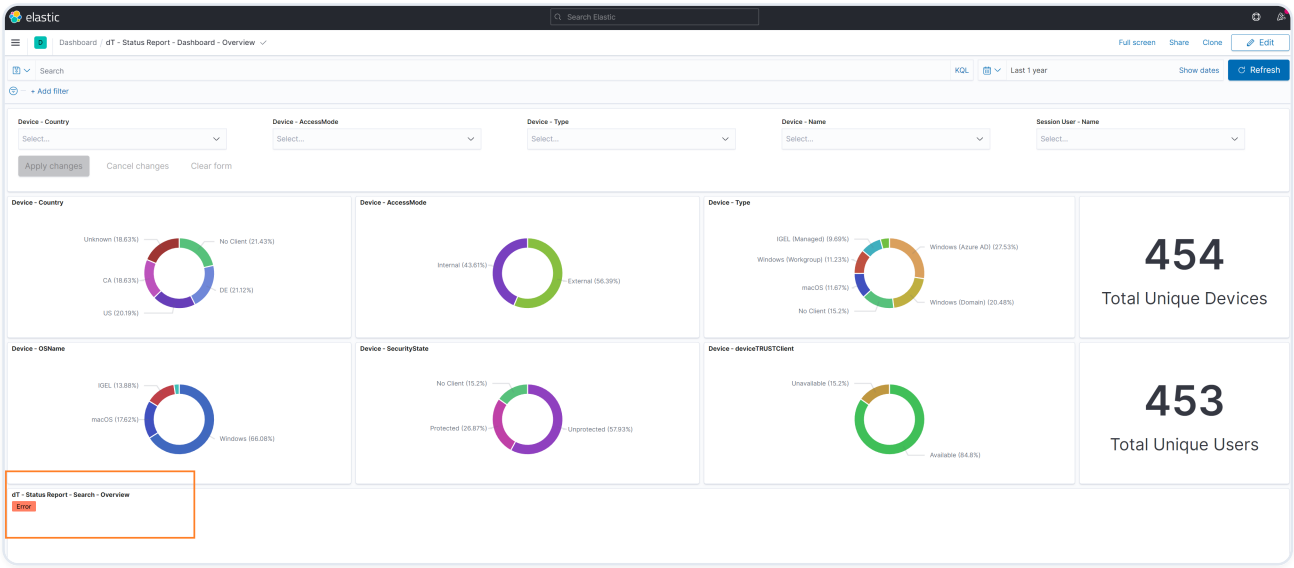
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3.4: Edit index settings

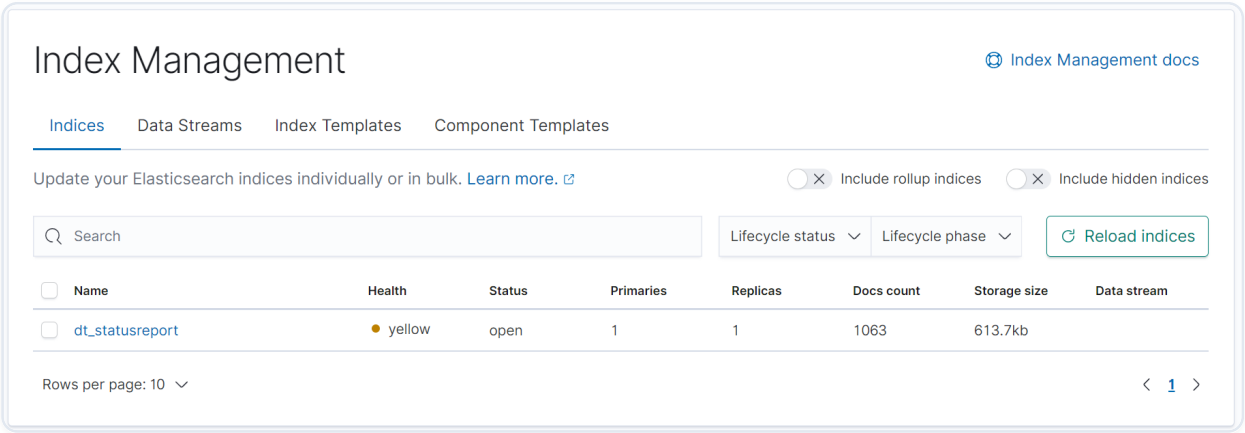
For the Status Report Dashboards to work properly, a configuration needs to be made at the index level: In a basic setting, ELK Stack allows to use 25 "calculated fields" per index. For the Status Report Dashboard, 48 calculated fields are used. Thus, the `allowed number of calculated fields` needs to be set to a higher value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



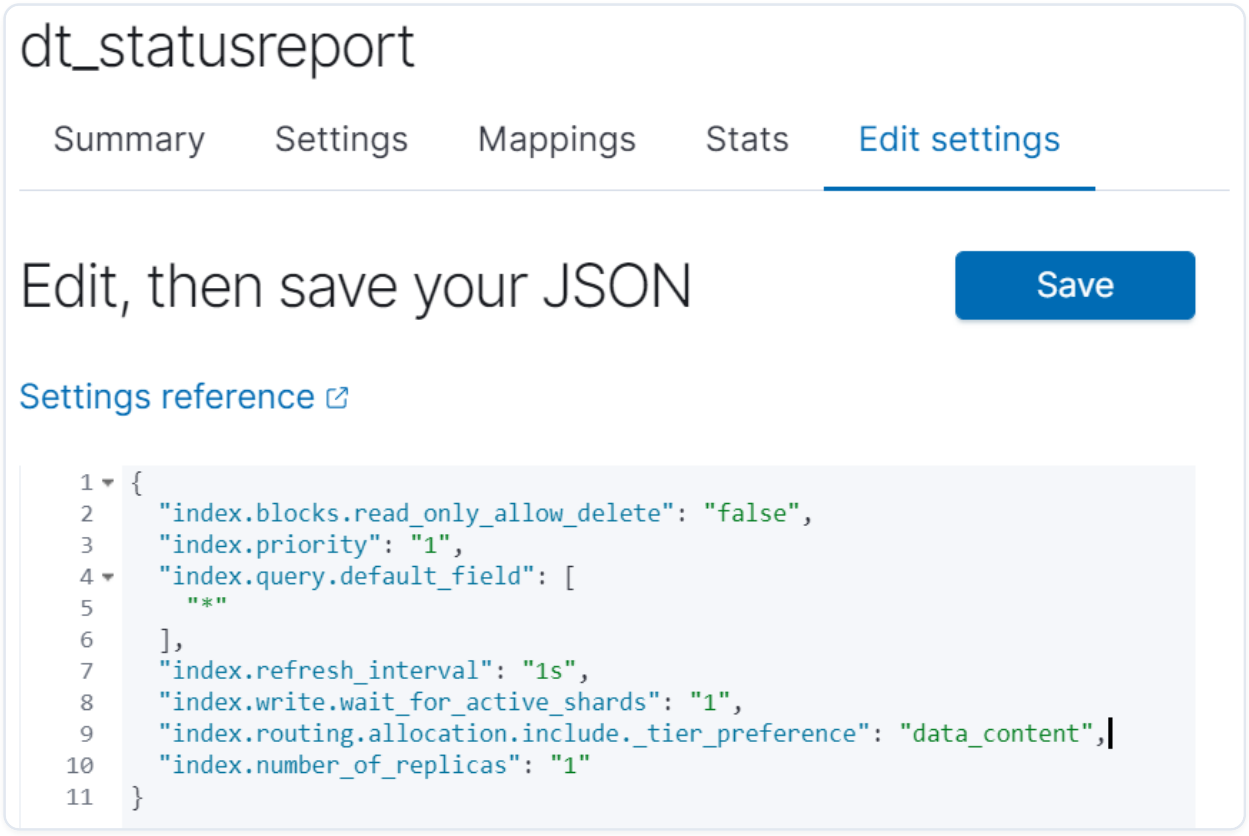
You need to send data to ELK Stack first. Sending data will create the index with basic settings. It can then be edited.

- After sending your first data, you will find the index `dt_statusreport` has been created in the Index Management Menu.

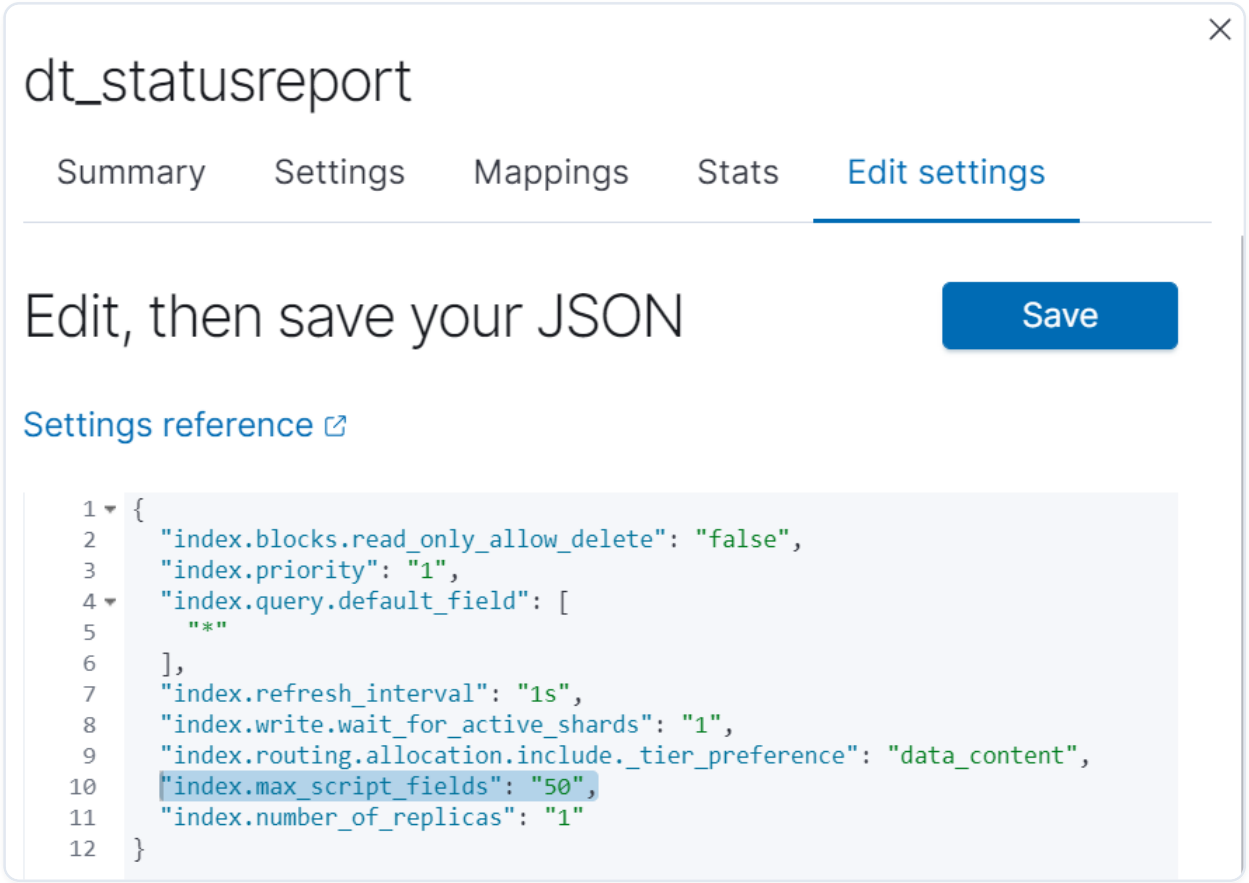


- Select the Index and chose `Edit Settings`. You'll be presented a json configuration view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



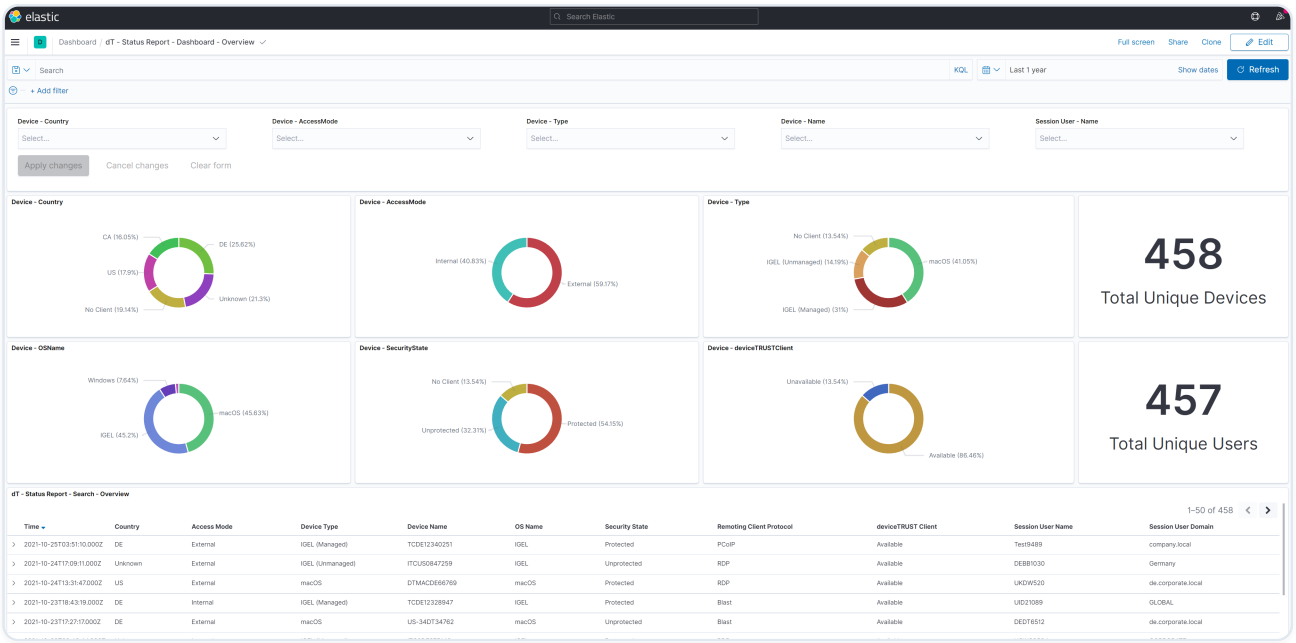
- Add `"index.max_script_fields": "50"` as a new line, making sure to keep the correct json formatting.
- Save your changes.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Your Dashboard will now be displayed without errors.

After the index template has been created and the saved objects are imported, the use case `Status Report` has been implemented successfully. deviceTRUST now sends status data to ELK Stack on every access to the remoting system. The data is presented in the created dashboards.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reference

TABLE OF CONTENTS

- Properties
- Agent
- Client Extension
- Console

Properties

- Access Point Properties - Describes the available Wi-Fi access points.
- Browser Properties - Describes installed internet browsers.
- Cellular Properties - Describes the active cellular capabilities of an endpoint.
- Certificate Properties - Describes the private certificates available within the users certificate store.
- ChromeOS Properties - Provides properties unique to a Google ChromeOS device.
- Custom Properties - Provides a condition that can operate on any property, including custom properties created using 'dtcmd.exe'.
- deviceTRUST Properties - Provides information about whether a connection to a deviceTRUST Client Extension has been established, the version of the deviceTRUST software and the status of the deviceTRUST license.
- Display Properties - Describes the displays available to the user session.
- Domain Properties - Describes the domain membership of the endpoint.
- eLux Properties - Provides properties unique to a Unicon eLux device.
- Hardware Properties - Describes the hardware and its capabilities.
- IGEL Properties - Provides properties unique to an IGEL device.
- Input Properties - Describes the input devices available to the user session.
- iOS Properties - Provides properties unique to an Apple iOS endpoint.
- Location Properties - Describes the geographical location of the endpoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Logical Disk Properties - Describes the logical disks available to the user.
- macOS Properties - Describes properties unique to an Apple macOS endpoint.
- macOS Firewall Properties - Provides real-time properties describing the state of the macOS Firewall.
- macOS Update Properties - Describes the status of macOS Software Update settings and updates.
- Mapped Drive Properties - Describes the mapped drives available within a user session.
- MDM Properties - Provides dynamic properties describing the current mobile device management (MDM) solution.
- Multihop Properties - Describes the number of hops taken by the user over deviceTRUST connected sessions.
- Name Properties - Identifies the endpoint.
- Network Properties - Describes the network adapters and their bound network addresses.
- NoTouch Properties - Provides properties unique to a Stratodesk NoTouch device.
- OS Properties - Provides information about the operating system installed on the endpoint.
- Password Policy Properties - Describes the password policy of the logged in user.
- Performance Properties - Describes the performance of the remoting protocol.
- Power Properties - Describes the power profile of the endpoint.
- Printer Properties - Describes the printers available to the user session.
- Region Properties - Describes the regional information of the user session.
- Remote Control Properties - Determines whether the user session is being remote controlled and provides information about the remote controlling endpoint.
- Remoting Client Properties - Provides properties about the remoting client used to remote control the user session.
- Screen Saver Properties - Describes the screen saver applied to the user session.
- Security Product Properties - Provides real-time properties describing the state of the installed Antivirus, Antispyware and Firewall security products.
- Session Properties - Provides information describing the user's logon session.
- Smartcard Reader Properties - Describes the connected smart-card readers available to the user.
- User Properties - Identifies the logged in user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WHOIS Properties - Provides the results of a WHOIS lookup of the endpoint.
- Windows Properties - Provides real-time properties unique to a Microsoft Windows device.
- Windows Defender Properties - Provides real-time properties describing the state of Microsoft Windows Defender Antivirus.
- Windows Firewall Properties - Provides real-time properties describing the state of the Microsoft Windows Firewall.
- Windows Registry Properties - Provides access to Windows Registry entries.
- Windows Update Properties - Describes the status of Microsoft

Agent Reference

TABLE OF CONTENTS

- Policy Loading
- Product Events

Client Extension Reference

TABLE OF CONTENTS

- iOS Managed App Configuration - iOS Managed App Configuration Reference
- iOS Passcodes - iOS Passcodes Reference

Console Reference

TABLE OF CONTENTS

- Actions - Actions Reference
- Settings - Settings Reference

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, then the Knowledge Base is a useful resource for common problems and resolutions. The following sections detail some useful knowledge base articles depending upon your deployment scenario:

Scenario: Remote

In remote scenarios, deviceTRUST® transports the context information from the user's remote device to the virtual session where the configuration is enforced. Please check the following knowledge base articles:

- Step 1: Make sure that you have a valid license
- Step 2: Check that your contextual security policy has been saved and deployed
- Step 3: Check that the user is managed by deviceTRUST
- Step 4: Check that the deviceTRUST Client Extension is installed on the remote device
- Step 5: Check that Citrix Virtual Channel Security is configured (Citrix Only)
- Step 6: Check that your contexts are correctly defined
- Step 7: Exclude specific users from the deviceTRUST policy
- Step 8: Check that the deviceTRUST Agent service is running
- Step 9: Check that you are using the latest deviceTRUST version

Scenario: Local

In local scenarios, deviceTRUST collects context information and executes actions locally. Please check the following knowledge base articles:

- Step 1: Make sure that you have a valid license
- Step 2: Check that your contextual security policy has been saved and deployed
- Step 3: Check that the user is managed by deviceTRUST
- Step 4: Check that your contexts are correctly defined
- Step 5: Exclude specific users from the deviceTRUST policy

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 6: Check that the deviceTRUST Agent service is running
- Step 7: Check that you are using the latest deviceTRUST version

Open a support ticket with us

Additional articles may be found by searching the Knowledge Base. However, if you are still experiencing difficulties please raise a ticket with the Citrix Support Portal at https://support.citrix.com.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Knowledge Base

TABLE OF CONTENTS

- Features
- General
- Properties
- Reporting

General

TABLE OF CONTENTS

- Compatibility
- Configuration
- Connectivity
- Diagnostics
- Installation
- Licensing
- Support

Configuration

Table of Contents

- Check that the user is managed by deviceTRUST
- Check that your contextual security policy has been saved and deployed
- Custom Process + PowerShell Cert signing
- Deny Access, Logout or Disconnect
- Exclude specific users from the deviceTRUST policy
- GPO name is not updated in deviceTRUST policy when copying a GPO within group policy editor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connectivity

Table of Contents

- Access denied to virtual sessions when using iOS 16 or later
- Check that the deviceTRUST Client Extension is installed on the remote device
- Configuring Citrix Virtual Channel Security

Diagnostics

Table of Contents

- deviceTRUST debug log locations

Installation

TABLE OF CONTENTS

- Check that the deviceTRUST Agent service is running
- Check that you are using the latest deviceTRUST version
- Configuration of the deviceTRUST Client Extension virtual channel for ICA
- deviceTRUST Client Extension & Active Setup
- Enabling DCV extensions on Amazon WorkSpaces WSP
- Silent removal of the deviceTRUST Client Extension for Apple macOS

Licensing

TABLE OF CONTENTS

- Make sure that you have a valid license

Support

TABLE OF CONTENTS

- IGEL OS 12 - No IGEL Properties

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compatibility

Table of Contents

- deviceTRUST + Apple Silicon support
- deviceTRUST + CVE-2021-44228 “Log4Shell”

Properties

TABLE OF CONTENTS

- Device Location
- Location and Network improvements in Windows 11 24H2
- SD Card detection for Logical Disk properties
- Updating the deviceTRUST Client Extension in IGEL OS 11

Reporting

TABLE OF CONTENTS

- Log data to Microsoft Teams

Features

Table of Contents

- azure-enterprise-application-for-aad-conditional-access-integration
- Check that your contexts are correctly defined
- Multi-Hop with deviceTRUST
- Process monitoring

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Releases

TABLE OF CONTENTS

- Next Release (25.3)
- IGEL OS 12 Client 23.1.400
- IGEL OS 11 Client 23.1.400
- macOS Client 23.1.410
- deviceTRUST 23.1.410
- Ubuntu Client 23.1.400
- iOS Client 23.1.400
- NoTouch Client 23.1.100
- Previous Release (21.1)

TABLE OF CONTENTS

- deviceTRUST 25.3
- macOS Client 25.3
- eLux Client 25.3
- Ubuntu Client 25.3
- Previous Release (23.1)

IGEL OS 11 Client Extension 23.1.400

This release includes minor enhancements to the deviceTRUST Client Extension for IGEL OS 11. This release has been submitted to IGEL for native integration into IGEL OS 11, however this has not been released yet. To integrate into currently available IGEL OS releases, please consult our Updating the deviceTRUST Client Extension in IGEL OS 11 Knowledge Base article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for third party WHOIS providers in 23.1.300

The IGEL OS 11 Client Extension 23.1.400 includes compatibility with the WHOIS changes introduced in deviceTRUST 23.1.300, including support for the IP2Location Web Services WHOIS Provider and the MaxMind GeoIP and GeoLite Web Services WHOIS Provider.

Compatibility

There are no other compatibility concerns with this release of the deviceTRUST® IGEL OS 11 Client Extension.

IGEL OS 12 Client Extension 23.1.400

We are very proud to make available our first deviceTRUST Client Extension for IGEL OS 12 devices. This release is available to install from the IGEL App Portal.

Release 23.1.200 includes bugfixes and minor enhancements to the deviceTRUST Client Extension.

Release 23.1.210 includes bugfixes to the deviceTRUST Client Extension to ensure compatibility with IGEL OS 12.3.1 and later.

Release 23.1.400 adds support for WHOIS proxy, proxy type and usage introduced in release 23.1.400 of the deviceTRUST Agent and Console.

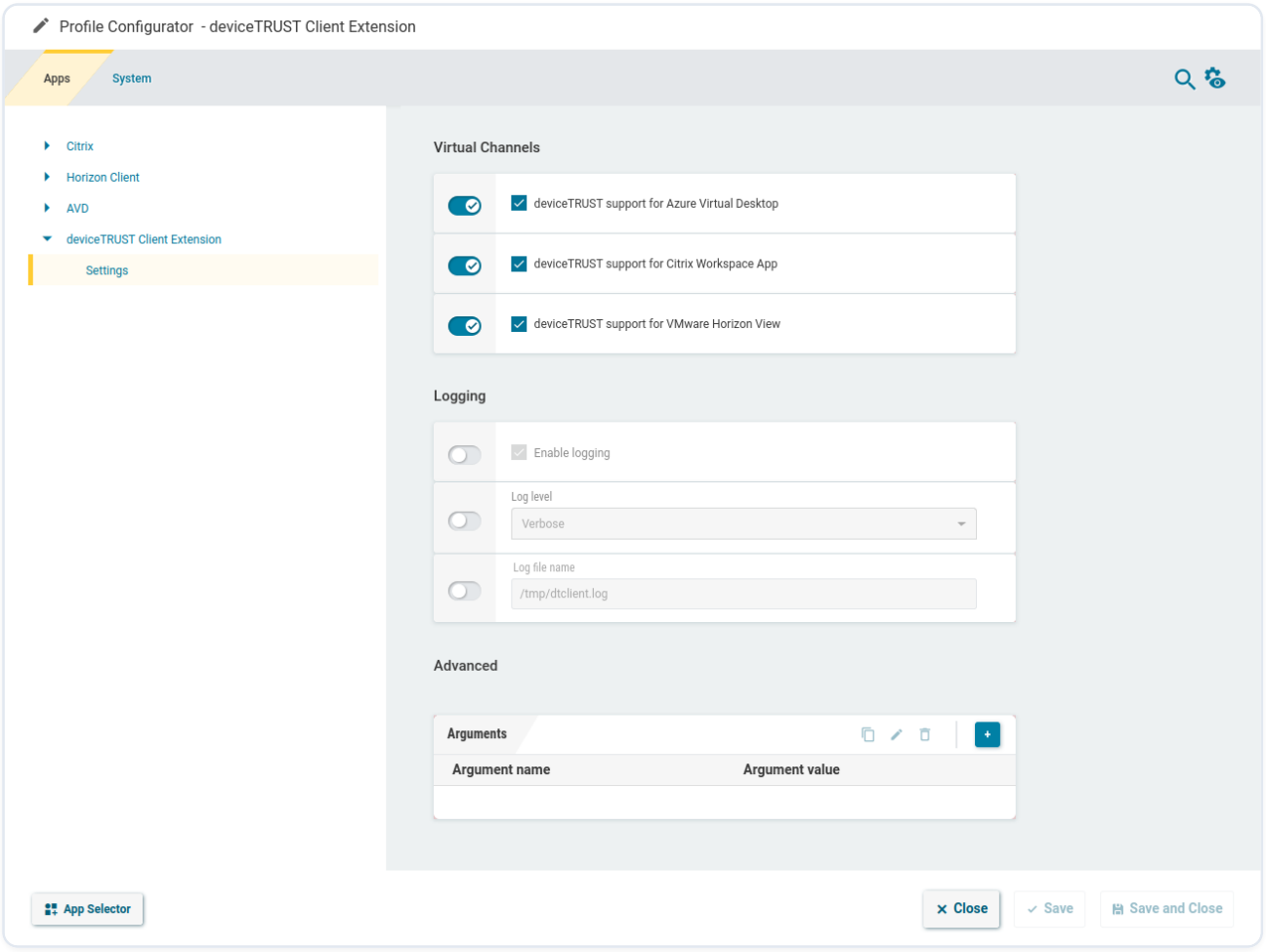
Remoting Clients

IGEL OS 12.01.120 and later supports native integration of the deviceTRUST Client Extension for Citrix Workspace App, Microsoft Azure Virtual Desktop and VMware Horizon View. For more information, see Supported IGEL Operating Systems for Client Extension.

UMS Configuration

The deviceTRUST® Client Extension for IGEL OS 12 can be configured directly within the UMS 12 Web App.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



New COSMOS Properties

IGEL OS 12 devices no longer distinguish between a UMS and ICG server. As a result, the previous ICG and UMS properties are no longer populated, and the following properties have been added to the IGEL category:

- **COSMOS Server** - The name and port of the COSMOS server.
- **COSMOS Cert Count** - The number of certificates from the COSMOS chain of trust.
- **COSMOS Cert Serial** - The serial number of the certificate from the COSMOS chain of trust.
- **COSMOS Cert Subject** - The subject of the certificate from the COSMOS chain of trust.
- **COSMOS Cert Thumbprint SHA256** - The SHA256 thumbprint of the certificate from the COSMOS chain of trust.

More information can be found at IGEL Properties.

WHOIS proxy, proxy type and usage in 23.1.400

Support for the detection of WHOIS proxy, proxy type and usage via either IP2Location Web Services or MaxMind GeoIP and GeoLite Web Services has been added in release 23.1.400.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bug fixes in 23.1.200

- Fixed an issue where COSMOS Server property was empty even when the device was managed.

Minor enhancements in 23.1.200

- Added support for the Volume ID of Logical Disk Properties on Linux based devices.
- Network Properties are now dynamic on Linux based devices.
- Logging of the deviceTRUST Client Extension is now disabled by default. Logging can be enabled within the UMS Configuration.

Bug fixes in 23.1.210

- Fixed an issue where some IGEL COSMOS properties could not be queried on IGEL OS 12.3.1 or later.
- Fixed an issue where the Hardware Bios Serial property appeared as Unavailable.
- Fixed an issue with VMware Horizon View where the deviceTRUST Client Extension would not load when using IGEL OS 12.3.1 or later.

Compatibility

There are no other compatibility concerns with this release of the deviceTRUST IGEL Client Extension.

iOS Client Extension 23.1.400

This release brings support for iOS and iPadOS 17 and later, and is available to download from the App Store.

Release 23.1.400 includes support for WHOIS proxy, proxy type and usage. This functionality required version 23.1.400 of the deviceTRUST Agent and Console.

Please refer to the Client Extension installation on iOS and iPadOS devices for more information.

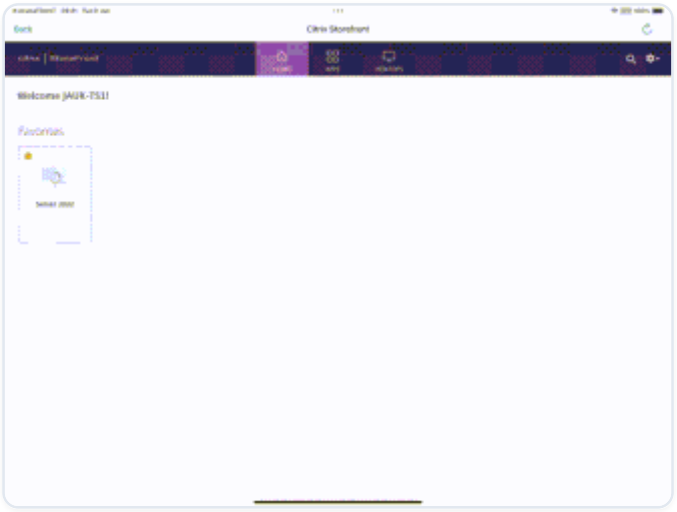
Passcode authentication for iOS 17

Previously when connecting to a virtual session with an iOS device, the deviceTRUST Agent matched the *client name* taken from the remoting protocol with the name of the registered iPhone or iPad within the deviceTRUST Portal. However with Apple's continued push towards user privacy, the ability to query the name of the device is now limited to apps meeting specific criteria and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

requesting the necessary entitlement. Neither the deviceTRUST Client Extension for iOS, or any of the popular remoting clients, have been granted this entitlement. Having lost the only information we have that identifies the remote iOS device, a new approach to matching the remote device is required.

We now support the use of passcodes to match the remote device. When connecting from a remote iOS device, the deviceTRUST® Agent will now display a passcode to the user of configurable length. The user must then switch to the deviceTRUST Client Extension for iOS and enter that passcode. They can then return to the virtual session to gain access to their desktop or published application.



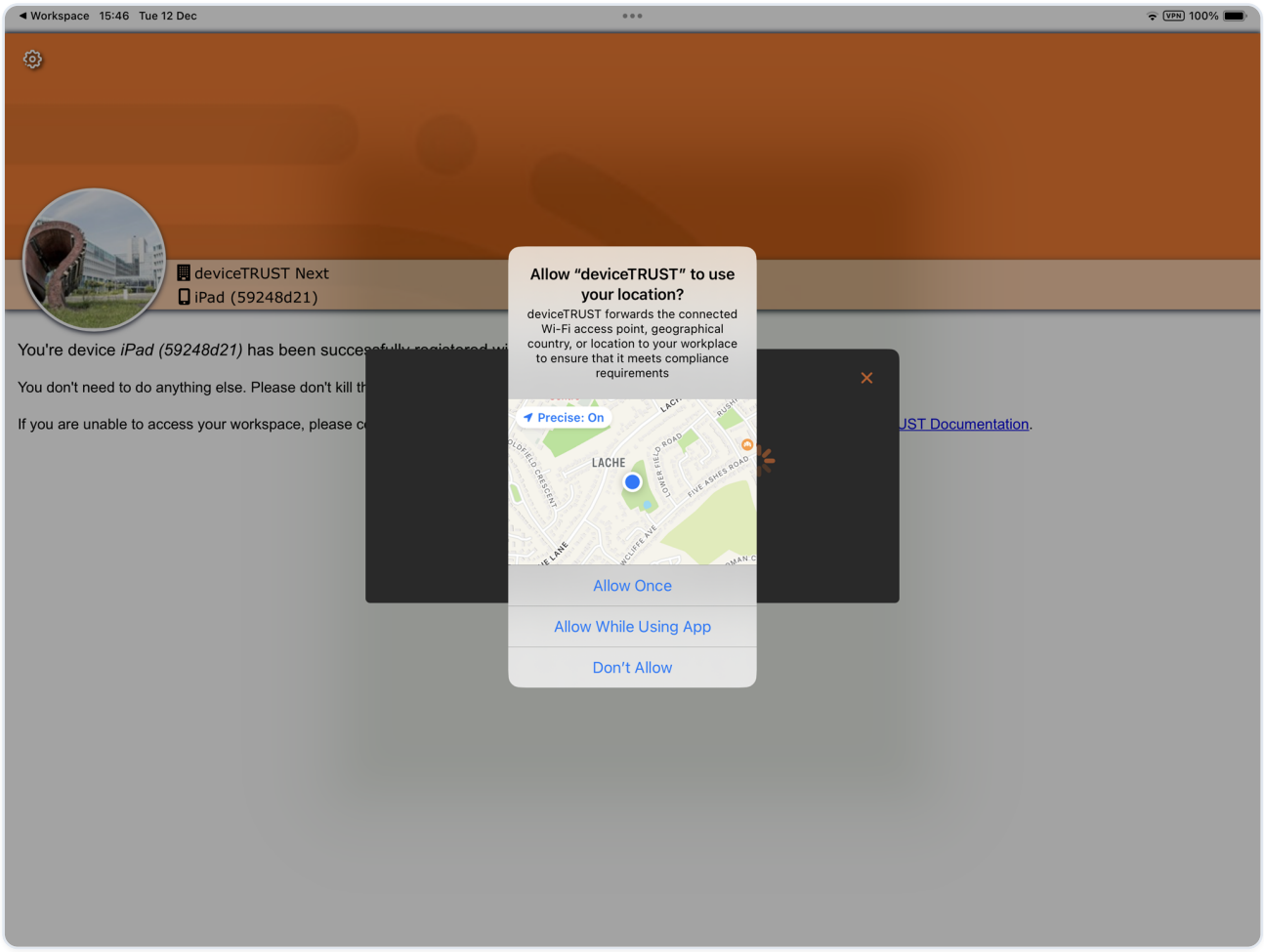
By using passcodes, we now support iOS as a remote device on Citrix Virtual Apps and Desktops, Citrix Cloud, Microsoft Remote Desktop Services and VMware Horizon View. For more information, see OS Compatibility.

More information can be found in the iOS Passcodes reference.

Location and Network Wi-Fi SSID/BSSID

We've added support for Location and Network Wi-Fi SSID and BSSID properties from iOS remote devices. Users must consent to location privileges when either Location or Network Wi-Fi SSID and BSSID are first requested. Since these properties potentially require user interaction, they are only available when using passcode authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Compatibility

This version of the deviceTRUST Client Extension for iOS is backwards compatible with previous deviceTRUST Agents. However the new passcode authentication functionality is required for compatibility with iOS 17 and later, and requires deviceTRUST Agent 23.1.200 or later.

macOS Client Extension 23.1.410

This release includes enhancements and bug fixes to the deviceTRUST® Client Extension for macOS.

Release 23.1.110 includes a bug fix to address changes in macOS Sonoma that now require apps to request location permission to be able to access Wi-Fi information of the connected networks.

Release 23.1.200 includes a bug fix to address compatibility issues with macOS 10.15 Catalina.

Release 23.1.300 includes compatibility with third party WHOIS providers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release 23.1.400 includes bug fixes to address compatibility issues with macOS 15.0 Sequoia, as well as support for new Microsoft Intune and WHOIS properties introduced in release 23.1.400 of the deviceTRUST Agent and Console.

Release 23.1.410 includes a single bug fix to the security properties.

Support for third party WHOIS providers in 23.1.300

The macOS Client Extension 23.1.300 includes compatibility with the WHOIS changes introduced in deviceTRUST 23.1.300, including support for the IP2Location Web Services WHOIS Provider and the MaxMind GeoIP and GeoLite Web Services WHOIS Provider.

Support for Microsoft Intune detection and WHOIS proxy, proxy type and usage in 23.1.400

Support for the detection of Microsoft Intune, and for WHOIS proxy, proxy type and usage via either IP2Location Web Services or MaxMind GeoIP and GeoLite Web Services has been added in release 23.1.400.

Nice DCV extension support including Amazon WorkSpaces WSP

We now include a Nice DCV extensions within the deviceTRUST Client Extension for macOS bringing support for the latest Nice DCV Standalone, Amazon WorkSpaces WSP, Amazon AppStream and more.

On Amazon WorkSpaces WSP, the `Configure extensions` policy must be set to `Server and Client` and there are additional software requirements. More information can be found in our Enabling DCV extensions on Amazon WorkSpaces WSP knowledge base article.

Bug Fixes in 23.1.100

- Fixed an issue where the macOS Update Enabled property could be inaccurate on macOS 13.0 Ventura and later.

Bug Fixes in 23.1.110

- Fixed an issue where the Network Wi-Fi properties were inaccurate on macOS 14 .0 Sonoma, with the *Wi-Fi Security* property was set to "Other (-1)" and *Wi-Fi BSSID* and *Wi-Fi SSID* both empty. This issue was caused by macOS Sonoma now requiring permission to access the user location in order to determine these properties, and as a result the deviceTRUST Client Extension for macOS now prompts for location permissions when these properties are requested.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bug Fixes in 23.1.200

- Fixed an issue where the deviceTRUST Client Extension would fail to load on macOS 10.15 Catalina.

Bug Fixes in 23.1.400

- Fixed an issue with macOS 15.0 Sequoia where the macOS Firewall properties were all Unavailable. As part of these changes, the Version, Inbound Exception Rules and Inbound Service Rules properties have been deprecated.
- Fixed an issue with macOS 15.0 Sequoia where the Location properties were initially set to Unavailable. The location properties provided by macOS 15.0 Sonoma can take longer to load than in previous OS releases, so support for the Loading state has been added.

Bug Fixes in 23.1.410

- Fixed an issue in the 23.1.400 release where the macOS Firewall must have Stealth Mode enabled for the firewall to appear as Active within the Security Products properties.

Known Issues

- Amazon WorkSpaces no longer allows PCoIP virtual channels to be loaded. This can be worked around by installing Amazon WorkSpaces Client v5.3.0.

Compatibility

If you are using the macOS Firewall's Version, Inbound Exception Rules or Inbound Service Rules properties within a Context, these conditions should be removed.

For Amazon WorkSpaces WSP support, please ensure you are using deviceTRUST 23.1.112 or later to ensure reliable connectivity between the deviceTRUST Agent and the deviceTRUST Client Extension for macOS.

Stratodesk NoTouch OS Client Extension 23.1.100

We are very proud to make available our first deviceTRUST Client Extension for Stratodesk NoTouch devices. This first release includes support for Citrix Workspace App, FreeRDP and VMware Horizon View. Please check out Client installation on Stratodesk NoTouch OS devices for details on the installation. This client extension requires deviceTRUST Agent and Console version 23.1.100 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Available Properties

We've added support for the following categories of properties:

- deviceTRUST - Provides the version of the deviceTRUST software.
- Display - Describes the displays available to the user session.
- Hardware - Describes the hardware and its capabilities.
- Input* - Describes the input devices available to the user session.
- Location - Describes the geographical location of the endpoint.
- Logical Disk - Describes the logical disks available to the user.
- Name - Identifies the endpoint.
- Network - Describes the network adapters and their bound network addresses.
- NoTouch - Provides properties unique to a Stratodesk NoTouch device.
- OS - Provides information about the operating system installed on the endpoint.
- /en-us/device-trust/reference/properties/power/) - Describes the power profile of the endpoint.
- Region - Describes the regional information of the user session.
- Smartcard Reader - Describes the connected smart-card readers available to the user.
- User - Identifies the logged in user.
- WHOIS - Provides the results of a WHOIS lookup of the endpoint.

NoTouch Properties

The following properties are available within the NoTouch category:

- **NoTouch Center URL** - The Management URL of the NoTouch Center.
- **NoTouch Center Cert Serial** - The serial number of the certificate used to connect to the NoTouch Center.
- **NoTouch Center Cert Subject** - The subject of the certificate used to connect to the NoTouch Center.
- **NoTouch Center Cert Thumbprint SHA256** - The SHA256 thumbprint of the certificate used to connect to the NoTouch Center.
- **Environment Variable Count** - The number of NoTouch Center environment variables.
- **Environment Variable Name** - The name of the NoTouch Center environment variable.
- **Environment Variable Value** - The value of the NoTouch Center environment variable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Custom Properties for NoTouch Devices

The Custom Properties Settings includes support for remote NoTouch OS devices. This allows a custom script to return any property from the remote device by writing `REMOTE_CUSTOM_NAME=VALUE` to the output.

Ubuntu Client Extension 23.1.400

Release 23.1.300 includes support for third party WHOIS providers.

Release 23.1.400 includes support for WHOIS proxy, proxy type and usage.

Support for third party WHOIS providers in 23.1.300

The Ubuntu Client Extension 23.1.300 includes compatibility with the WHOIS changes introduced in deviceTRUST 23.1.300, including support for the IP2Location Web Services WHOIS Provider and the MaxMind GeoIP and GeoLite Web Services WHOIS Provider.

Support for WHOIS proxy, proxy type and usage in 23.1.400

Support for the detection of WHOIS proxy, proxy type and usage via either IP2Location Web Services or MaxMind GeoIP and GeoLite Web Services has been added in release 23.1.400.

Bug Fixes in 23.1.300

- Fixed an issue loading the virtual channels on Ubuntu 22.04 or later due to a missing dependency on libssl.

Bug Fixes in 23.1.400

- Fixed an issue where wireguard VPN devices would not identify a VPN within the WHOIS properties.

Compatibility

There are no compatibility concerns with this release of the deviceTRUST® Ubuntu Client.

deviceTRUST 23.1.410

This service pack adds detection for Microsoft Intune and introduces the detection of proxies using IP2Location Web Services or MaxMind GeoIP2 Insights Web Service providers. Please refer to Compatibility for changes that may impact users upgrading from previous releases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The deviceTRUST 23.1.410 patch includes bugfixes to the deviceTRUST Agent and Console. This release includes no changes to the deviceTRUST Client Extension and therefore has not been released on https://devicetrust.com/download.

Microsoft Intune Detection

Microsoft Intune can now be detected using our new MDM properties. Microsoft Intune detection is supported on Microsoft Windows and Apple macOS devices.

WHOIS Proxy Detection

The WHOIS properties have been extended with support for proxy, proxy type and usage properties. These properties are taken from the response fields of the IP2Location or MaxMind provider when an appropriate plan is selected.

As part of this change, we've renamed `LOCAL_WHOIS_VPN` and `REMOTE_WHOIS_VPN` to `LOCAL_WHOIS_ADAPTER_VPN` and `REMOTE_WHOIS_ADAPTER_VPN` respectively to ensure clarity with the new proxy properties.

Proxy Detection with IP2Location Web Services

IP2Location Web Services provides proxy detection from the following IP2Location response fields and is available with the following plans:

PROPERTY	RESPONSE FIELD	FREE PLAN	STARTER PLAN	PLUS PLAN	SECURITY PLAN
Proxy	`is_proxy <sup>1</sup>`	✓	✓	✓	✓
Proxy Type	`proxy.proxy_type`				✓
Usage	`usage_type`		✓	✓	✓

NOTE:

The accuracy of the `is_proxy` field is dependent upon the selected plan.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Proxy Detection with MaxMind GeoIP2 Insights Web Service

MaxMind GeoIP and GeoLite Web Services provides proxy detection from the following MaxMind response fields and is available with the following plans:

PROPERTY	RESPONSE FIELD	GEOIP2 COUNTRY	GEOIP2 CITY PLUS	GEOIP2 INSIGHTS	GEOLITE COUNTRY	GEOLITE CITY
Proxy	`is_anonymous`			✓		
Proxy Type	`is_hosting_provider`, `is_anonymous_vpn`, `is_public_proxy`, `is_residential_proxy`, `is_tor_exit_node`			✓		
Usage	`user_type`			✓		

Minor enhancements to 23.1.400

- Renamed Microsoft Azure AD to Microsoft Entra ID throughout the console.
- Added a `Use remote client names to connect to iOS devices` advanced setting, which forces the deviceTRUST® Agent to connect to iOS devices by matching the remote client names with those registered within the iOS Portal.

Bug fixes in 23.1.400

- Fixed an issue where a virtual session could be logged off during a live reconnect to a session that had never shown the desktop to the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Fixed an issue with the Logical Disk Identity operator where the None Of operator was shown as Not Equals.

Bug fixes in 23.1.410

- Fixed an issue on Citrix® virtual sessions when running a client OS, where the logoff process could get stuck and require a restart of the deviceTRUST Agent before allowing additional logons.
- Fixed an issue within the deviceTRUST Console where a context custom condition would fail to load when the custom condition targeted data types of IP or Position.

Compatibility

This compatibility section builds on our general approach to compatibility which can be found on the compatibility page.

We've renamed `LOCAL_WHOIS_VPN` and `REMOTE_WHOIS_VPN` to `LOCAL_WHOIS_ADAPTER_VPN` and `REMOTE_WHOIS_ADAPTER_VPN` respectively to ensure clarity with the new proxy properties. deviceTRUST Policies will upgrade automatically, but if these properties are referenced within scripts, or Web Request tasks, they may need to be manually updated.

If upgrading from a release prior to 23.1.400, be sure to check out the deviceTRUST 23.1.300 compatibility notes.

The deviceTRUST Agents can read policies created by previous releases of the deviceTRUST Console. However, they cannot read policies created by a newer console. Therefore, you must ensure that the deviceTRUST Agent 23.1.400 is deployed before applying policy that has been written by the deviceTRUST Console 23.1.400 or later.

Previous Releases

layout: doc

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Client installation on Unicon™ eLux RP6 devices
- Client installation on IGEL OS devices
- Client Extension installation on iOS and iPadOS devices
- Client installation on Apple macOS devices
- Client installation on Stratodesk NoTouch OS devices
- Client installation on Ubuntu devices
- Client Extension installation on Microsoft Windows devices
- Check that the deviceTRUST® Agent service is running
- Check that you are using the latest deviceTRUST® version
- Configuration of the deviceTRUST® Client Extension virtual channel for ICA
- deviceTRUST® Client Extension & Active Setup
- Enabling DCV extensions on Amazon WorkSpaces WSP
- Silent removal of the deviceTRUST® Client Extension for Apple macOS
- Make sure that you have a valid license
- IGEL OS 12 - No IGEL Properties
- Device Location
- Location and Network improvements in Windows 11 24H2
- SD Card detection for Logical Disk properties
- Updating the deviceTRUST Client Extension in IGEL OS 11
- Log data to Microsoft Teams
- Policy Loading
- Product Events
- iOS Managed App Configuration
- iOS Passcodes
- Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Audit Event Task
- Citrix Policy Task
- Custom Process Task
- Deny Access Task
- Microsoft Entra ID Task
- FSLogix App Masking Task
- Task Reference
- Logon Abort Task
- Map Drive Task
- Map Printer Task
- Microsoft Applocker Task
- Popup Message Task
- Screen Saver Task
- Send Mail Task
- Shortcut Task
- Terminate App Task
- User Session Task
- Web Request Task
- Windows Firewall Task
- Windows Policy Task
- Windows Registry Task
- Advanced Settings
- Auditing Settings
- Custom Properties Settings
- Microsoft Entra ID Settings
- File-Based Policy Settings
- Settings
- Licensing Settings
- Mail Server Settings
- Map Drive Settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft AppLocker Settings
- Mobile Settings
- Printer Settings
- Property Settings
- Security Settings
- System Messages Settings
- Access Point Properties
- Browser Properties
- Cellular Properties
- Certificate Properties
- ChromeOS Properties
- Custom Properties
- deviceTRUST Properties
- Display Properties
- Domain Properties
- eLux® Properties
- Hardware Properties
- IGEL Properties
- Input Properties
- iOS Properties
- Location Properties
- Logical Disk Properties
- macOS Properties
- macOS Firewall Properties
- macOS Update Properties
- Mapped Drive Properties
- MDM Properties
- Name Properties
- Network Properties
- NoTouch Properties

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- OS Properties
- Password Policy Properties
- Performance Properties
- Power Properties
- Printer Properties
- Region Properties
- Remote Control Properties
- Remoting Client Properties
- Screen Saver Properties
- Security Product Properties
- Session Properties
- Smartcard Reader Properties
- User Properties
- WHOIS Properties
- Windows Properties
- Windows Defender Properties
- Windows Firewall Properties
- Windows Registry Properties
- Windows Update Properties
- Adobe Reader DC Template
- Microsoft Visio Template
- Nuance PDF Template
- IP Address Template
- NetBIOS Name Template
- Wi-Fi Access Point Template
- Microsoft Teams Template
- Snipping Tool Template
- Access Mode Template
- Adobe Acrobat DC Template
- Corporate Device Template

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Country Template
- Microsoft Visio Template
- Nuance PDF Template
- Proximity Template
- Security State Template
- Wi-Fi Security Mode Template
- Working Time Template
- Application Log Template
- ELK Stack Template
- Email Template
- Log File Template
- Splunk Template
- Conditional Access Template
- Conditional Application Access Template
- Unauthorized USB Device Template
- Conditional Access Template

Client installation on Unicon™ eLux RP6 devices

Import the deviceTRUST® certificate chain

The deviceTRUST eLux Client is signed with a certificate that must first be trusted by both ELIAS and the eLux devices. Full details of how to import certificates into ELIAS and deploy them to eLux devices can be found by searching for 'Organizing certificates for package validation' within the eLux documentation. The latest deviceTRUST certificate chain can be downloaded Download certificate chain.

NOTE:

The import of the deviceTRUST certificate chain is only necessary when the eLux® environment is configured to check the signatures of packages. However, it is good practice to ensure that the packages match the certificates.

Within ELIAS:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Import `devicetrust-gmbh-20210321.pem` into `Trusted Issuer`.
- Import `globalsign-extended-validation-codesigning-ca-sha256-g3-20240615.pem` and `globalsign-intermediate-20280128.pem` into `Intermediate CA`.
- Import `globalsign-20280128.pem` into `Trusted Root CA`.

Within the Scout console:

- Deploy all of the above `pem` files into the `/setup/cacerts/` folder of the eLux device.

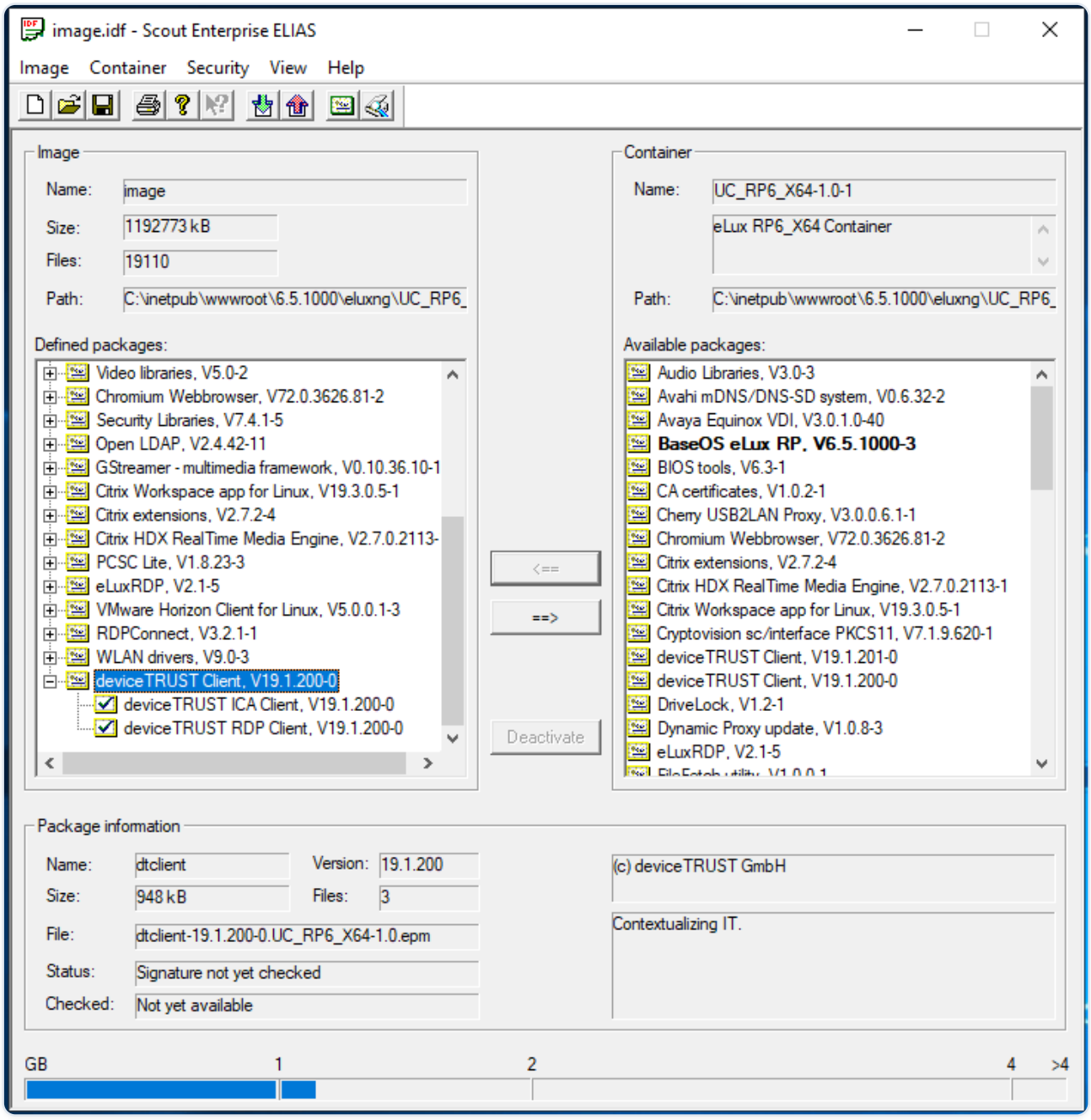
Install the package

Within ELIAS:

- Ensure that the required 'deviceTRUST Client' package has been imported into the package library.
- If you've imported the deviceTRUST certificate chain, then check the signatures of the package.
- Assign the 'deviceTRUST Client' package to the image.

For ICA support, ensure the 'deviceTRUST ICA Client, Vx.x.x-x' option is active under the defined package 'deviceTRUST Client, Vx.x.x-x'. For RDP support, ensure the 'deviceTRUST RDP Client, Vx.x.x-x' option is active under the defined package 'deviceTRUST Client, Vx.x.x-x'.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

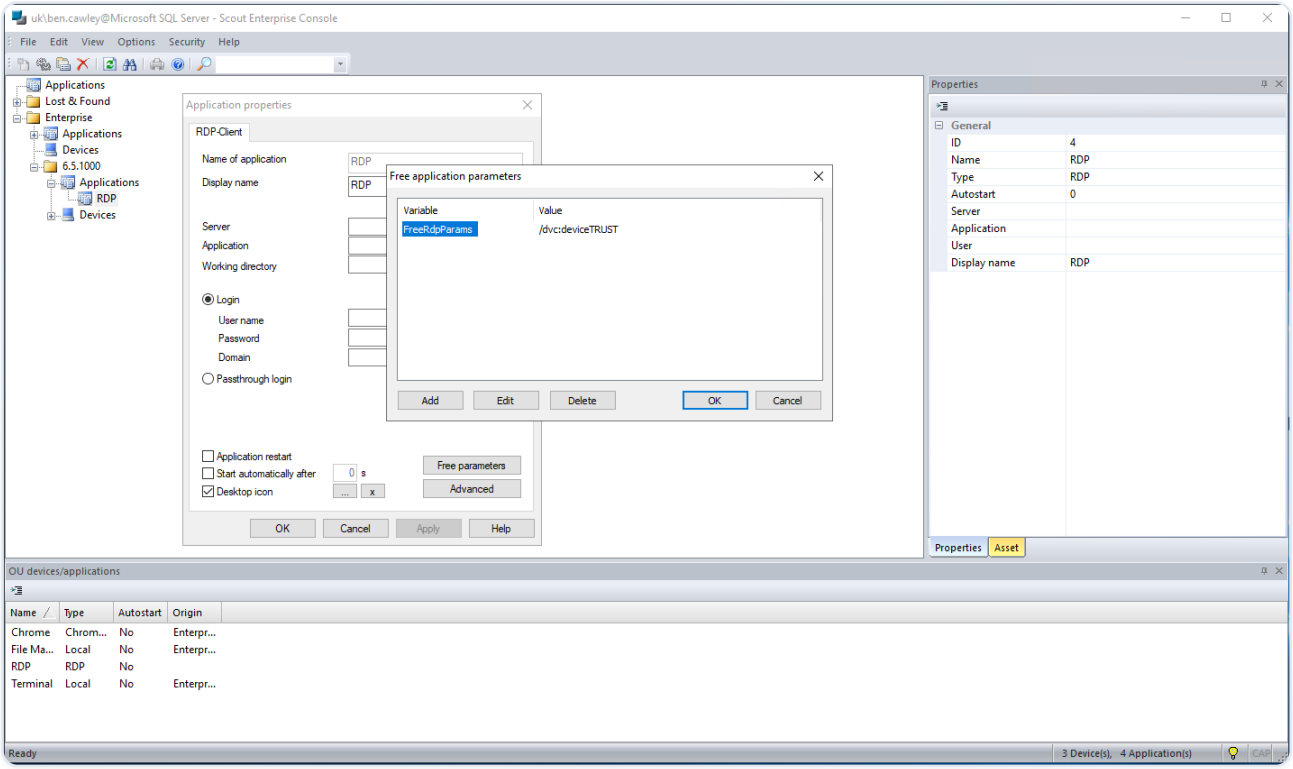


Within the Scout console:

- Update your eLux devices.

To enable the RDP virtual channel, within your eLux Scout console navigate to Enterprise > > Applications > RDP, and select properties, then 'Free parameters'. Add variable 'FreeRdpParams' with value '/dvc:deviceTRUST'.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



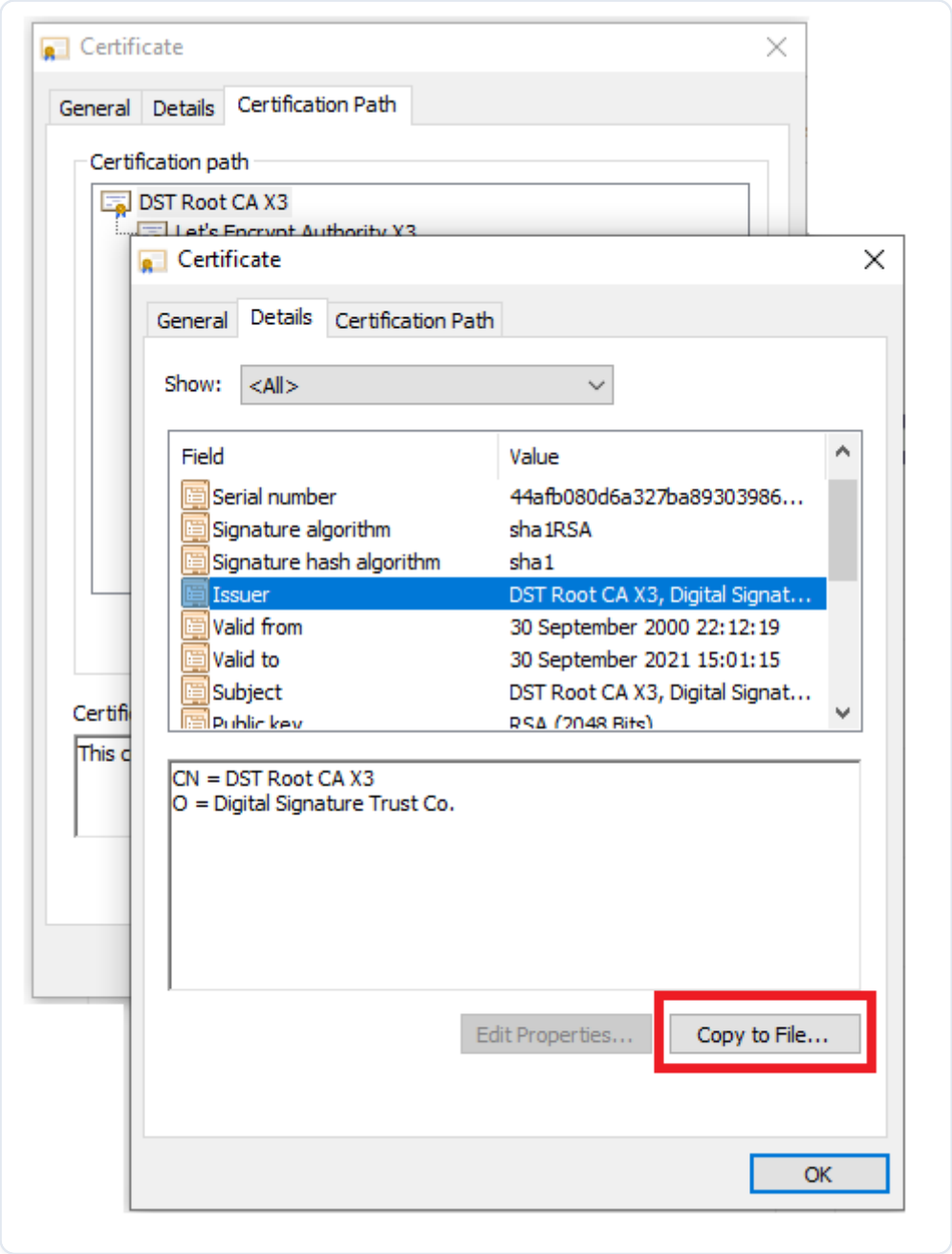
Next time you connect using ICA® or RDP to a server with a licensed deviceTRUST Host, the properties of your eLux device will be available within your virtual session.

Deploy the ripe.stat root certificate

To ensure the deviceTRUST eLux client can successfully obtain whois information you will need to ensure that the required root certificate is deployed to all your eLux devices.

To obtain the root certificate, navigate to stat.ripe.net within your browser and save the certificate to disk as a base-64 encoded X. 509 file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Within the Scout console select 'Advanced device configuration\Files' on the device container, import the certificate and deploy to your device certificate store location.

Client installation on IGEL OS devices

deviceTRUST is already integrated within the IGEL OS release 10.03.500 or higher and supports the Microsoft Remote Desktop Protocol (RDP) and the Citrix Independent Computing Architecture (ICA). Within the default IGEL profile, deviceTRUST is not enabled and needs to be enabled for both remoting protocols independently.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

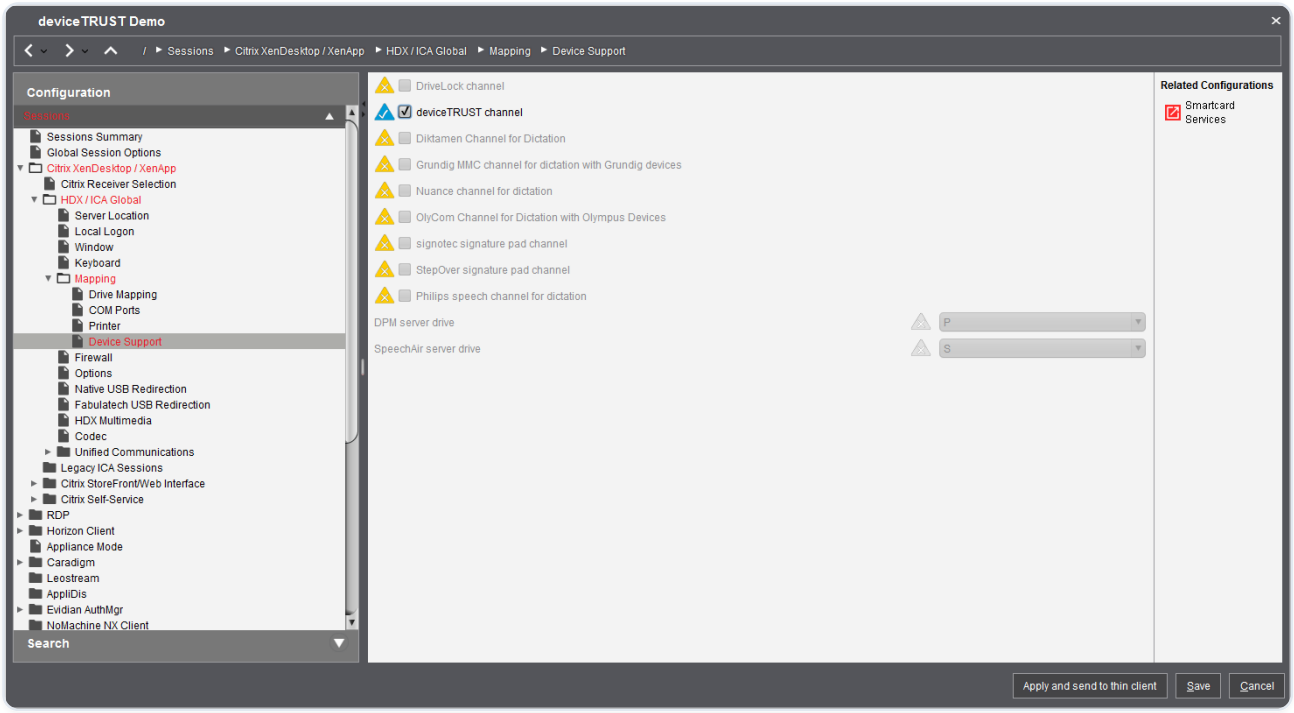
NOTE:

To enable deviceTRUST® within the IGEL OS you can use the IGEL Universal Management Suite (UMS) or the local administrative interface.

IGEL devices must be restarted after enabling deviceTRUST.

Enable deviceTRUST for Citrix Independent Computing Architecture (ICA®)

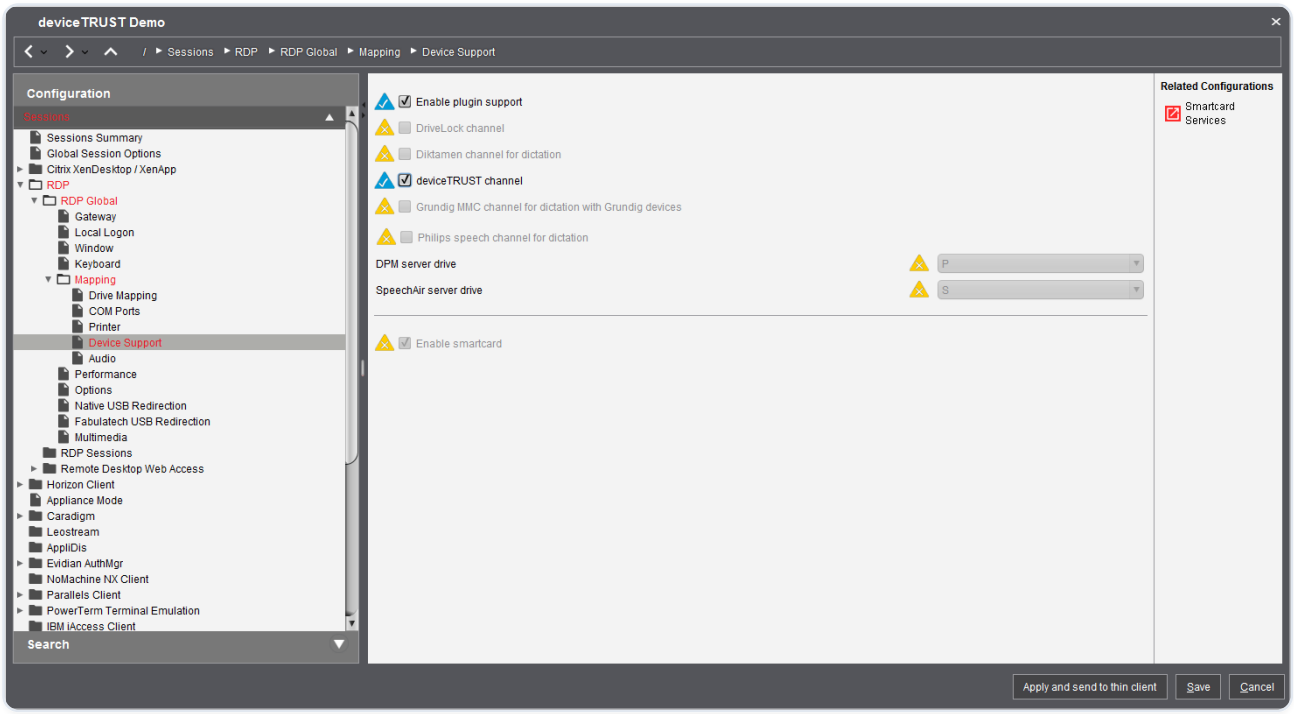
Open the target profile (local or through the UMS) and navigate to SESSIONS\CITRIX XENDESKTOP / XENAPP\HDX / ICA GLOBAL\MAPPING and activate the DEVICETRUST CHANNEL option.



Enable deviceTRUST for Microsoft Remote Desktop Protocol (RDP)

Open the target profile (local or through the UMS) and navigate to SESSIONS\RDP\RDP GLOBAL\MAPPING and activate the DEVICETRUST CHANNEL option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Client Extension installation on iOS and iPadOS devices

The deviceTRUST iOS Client Extension is available to download from the App Store. The iOS Client Extension is currently only compatible with *Citrix Virtual Apps and Desktops* and *Citrix Cloud*. For more information, see Platform Compatibility.

Before using the iOS Client Extension, the deviceTRUST® Agent must be supplied with an API Key, and the deviceTRUST iOS Client Extension must be registered with either a QR Code, or with an MDM managed app configuration.

Registering with the deviceTRUST Portal

The deviceTRUST Portal must be registered to your organisation using a registration link available from your deviceTRUST representative. Registration can be performed against one of the following accounts:

- *Microsoft Account* - Great for Proof-of-Concepts or small business use with single user administration. No Microsoft Entra ID domain required.
- *Work Account* - Great for medium or larger corporate use with multi user administration. Requires a Microsoft Entra ID domain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assigning roles to Entra ID users

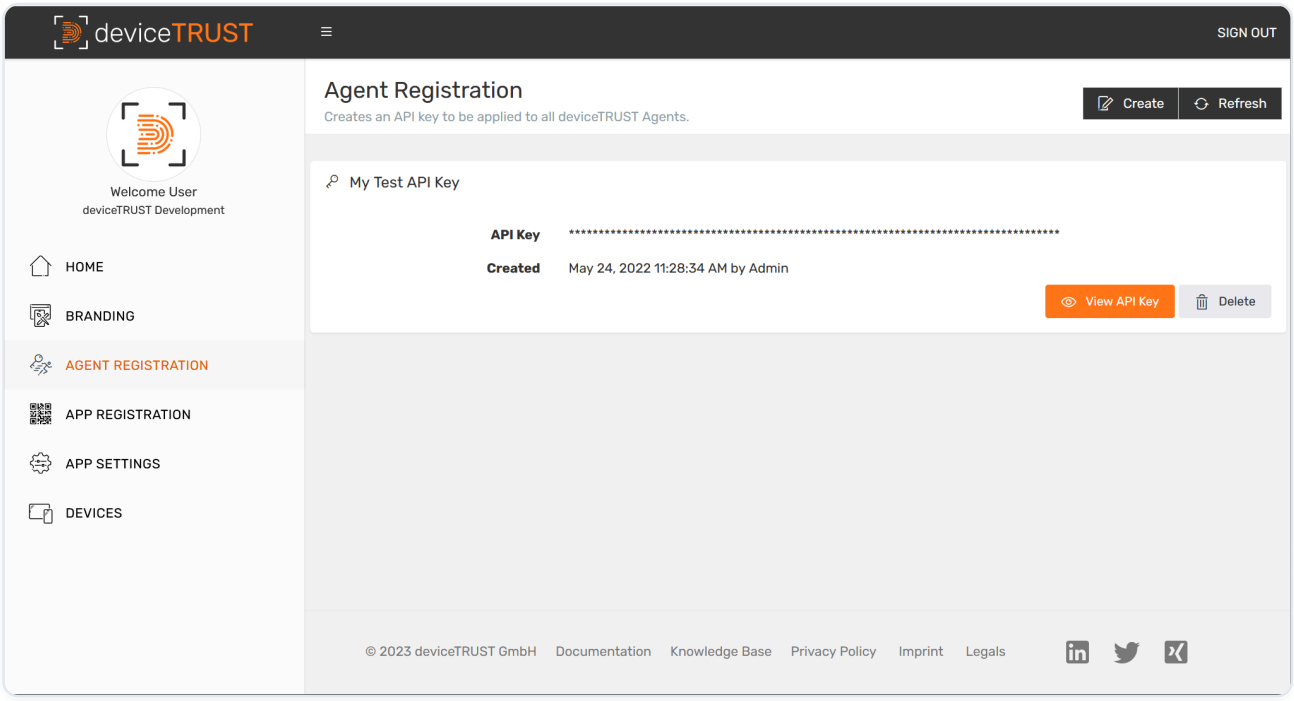
After a *Work Account* has been used to register an organization with the deviceTRUST Portal, other users within the organization must be assigned the correct role within Microsoft Entra ID for them to be able to sign-in to the deviceTRUST Portal.

When signed into the Azure portal:

- Navigate to the Microsoft Entra ID that belongs to the tenant of the user that registered with the deviceTRUST Portal.
- Navigate to Manage -> Enterprise applications.
- Click on the application named *deviceTRUST Portal* to view the Enterprise Application.
- Navigate to Manage -> Users and groups.
- To enable an existing user or members of a group to sign-in, click *Edit assignment* and change the role to *Portal Administrator* before clicking *Save*.
- To add a new user or members of a group, click *Add user/group*, select an appropriate identity and ensure the role is set to *Portal Administrator* before clicking *Save*.

Generating an API Key for use by the deviceTRUST Agent

An API Key must be allocated within the *Agent Registration* section of the deviceTRUST Portal. Click *Create*, enter a name and click *OK*. Click *View API Key* to view the API Key and copy to the clipboard.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once generated, the API Key can be entered within the Administrative Templates of the deviceTRUST Policy. Launch a suitable policy editor and navigate to Administrative Templates -> deviceTRUST and enter the API Key within the `Mobile: Determine properties from remote devices by connecting to a server`. Paste the API Key into the relevant field.

NOTE

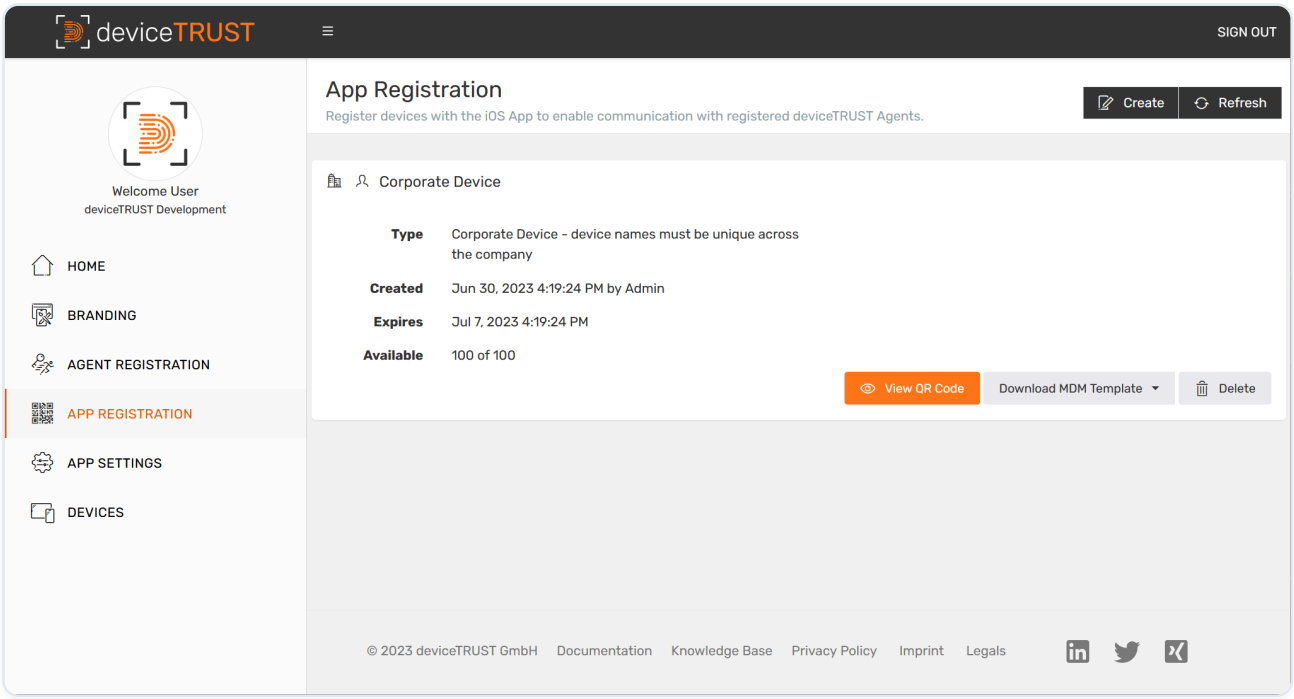
- API Keys remain valid as long as they exist within the deviceTRUST Portal.
- If the API Key is deleted, any deviceTRUST Agent that uses the API Key will no longer be able to communicate with iOS devices."

Generating an App Registration code to register iOS and iPadOS devices

An *App Registration* can be generated within the similarly named section of the deviceTRUST Portal. Click *Create* and populate the following fields:

- *Friendly Name* - A user friendly name of the registration.
- *Quantity* - The number of iOS devices that the QR code can register.
- *Expiry* - Enter a suitable time period of the iOS device enrollment. After the QR code has expired, new iOS devices will be unable to register, but devices already registered will continue to function.
- *Personal Devices* - Select Personal Devices to create a registration for a specific user. A personal device name must be unique for the specified user name and domain name.
- *Corporate Devices* - Select Corporate Devices to create a registration for your entire company. A corporate device name must be unique for all devices within the company.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

- App Registrations allow an iOS Client Extension to register with the deviceTRUST Portal. Deleted or expired App Registration's will prevent new registrations, but will not impact iOS devices that are already registered."

Registering an iOS or iPadOS device using a QR code

To register an iOS device using a QR code, navigate to the *App Registration* section of the deviceTRUST Portal and click *View QR Code* next to an App Registration. Within the iOS Client Extension, click *Register* and point the camera at the QR code. The iOS device will register with the deviceTRUST Portal.

Registering an iOS or iPad device using an MDM managed app configuration

Registration of an iOS device using an MDM managed app configuration depends upon the MDM provider that is being used. However, a *plist* file containing the app configuration profile can be downloaded by navigating to the *App Registration* section of the deviceTRUST Portal and clicking *Download MDM Template*. The downloaded plist file can be uploaded to your MDM provider, for more information see the iOS Managed App Configuration.

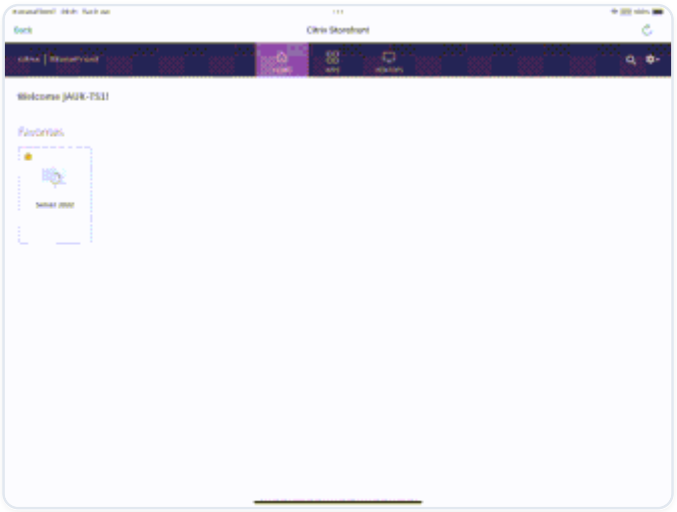
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Naming the iOS device for compatibility with iOS 16 and deviceTRUST Agent 23.1.120 or earlier

In iOS 16.0, apps require a special entitlement to be able to query the user assigned device name of an iPhone or iPad. The iOS Client Extension does not yet have this entitlement, and therefore can only read the device name as either `iPhone` or `iPad`. A unique device name is required for each device to successfully establish a connection between the deviceTRUST Agent and the iOS Client Extension. This limitation can be worked around by renaming devices within the deviceTRUST Portal, or by using an MDM app configuration policy to inform the iOS Client Extension of the real device name.

Using passcodes with deviceTRUST Agent 23.1.200 or later

Support for iOS 17 or later requires passcode authentication introduced in deviceTRUST Agent 23.1.200. During logon or reconnect, the user is shown a passcode. The user is responsible to switch to the deviceTRUST Client Extension and enter the passcode before switching back to the remoting client.

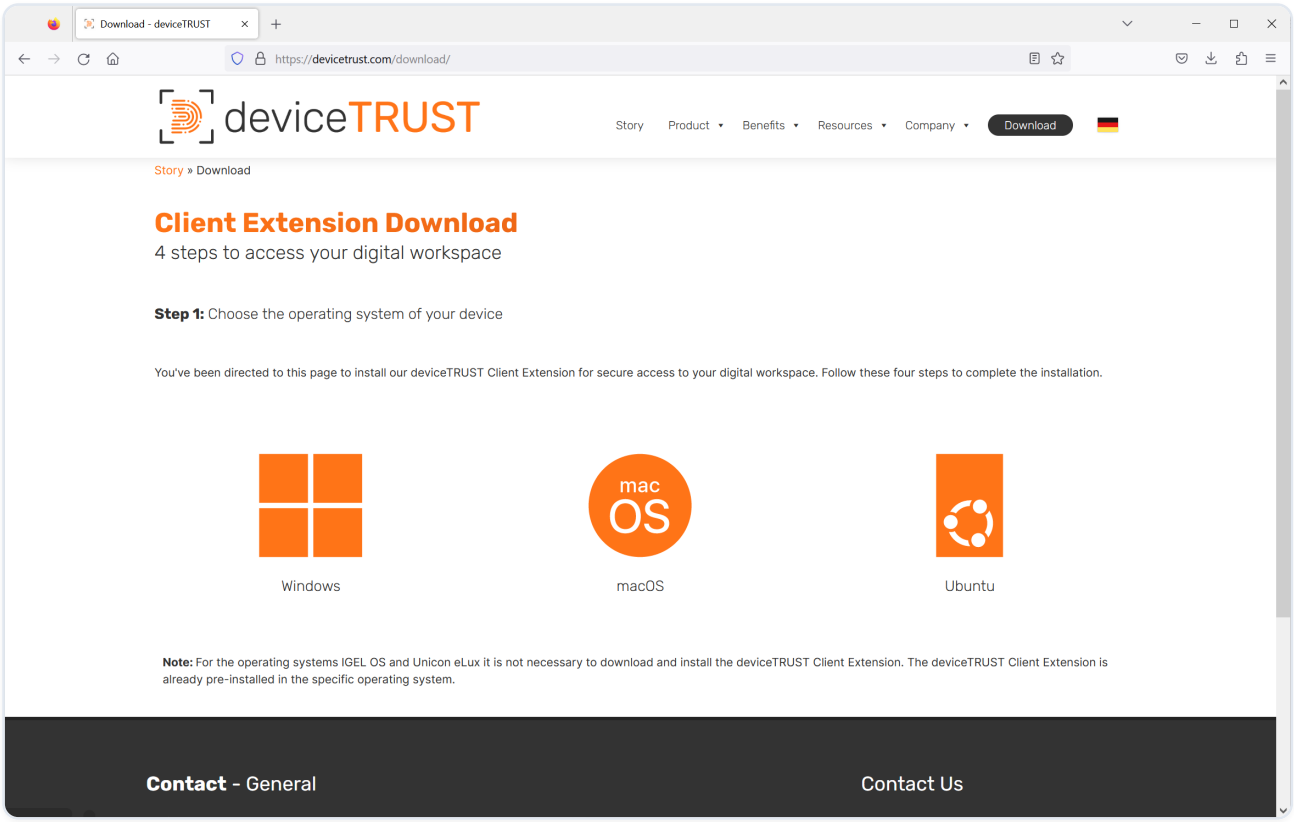


More information can be found within the iOS Passcodes reference.

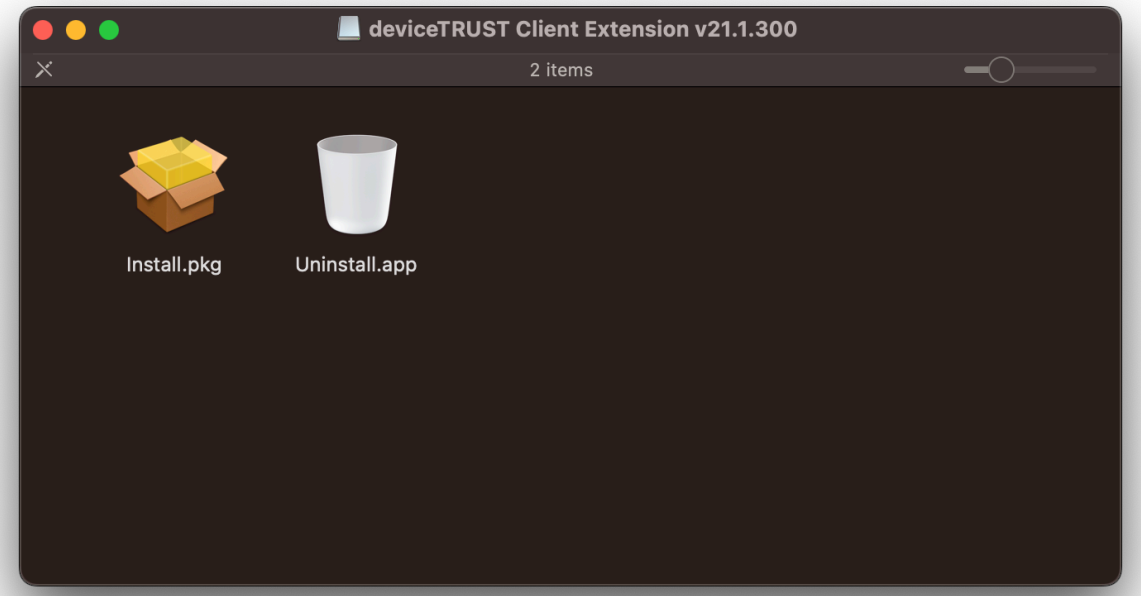
Client installation on Apple macOS devices

The deviceTRUST macOS Client can be downloaded by following the steps on the deviceTRUST Client Extension Download page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

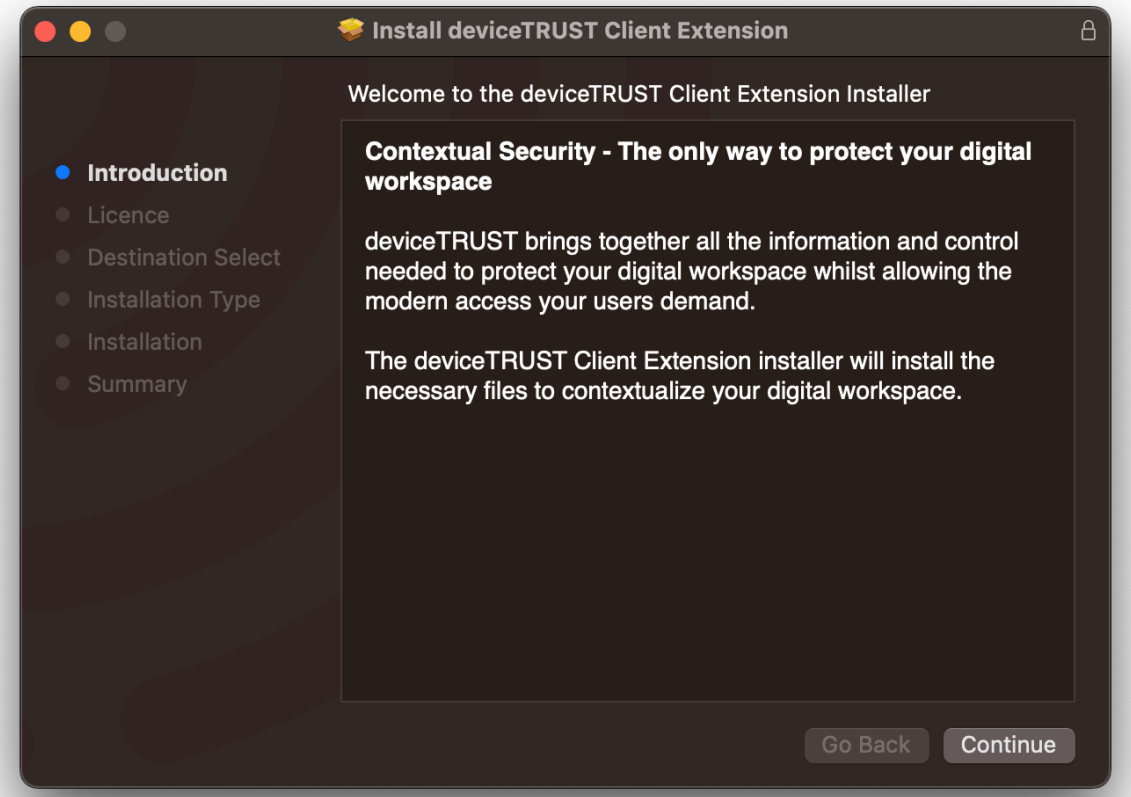


To access the installer, double click on the downloaded 'dtclient-extension-macos-universal-release-W.X.Y.Z.dmg' file.



Launch the installer by double clicking on othe 'Install.pkg' file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

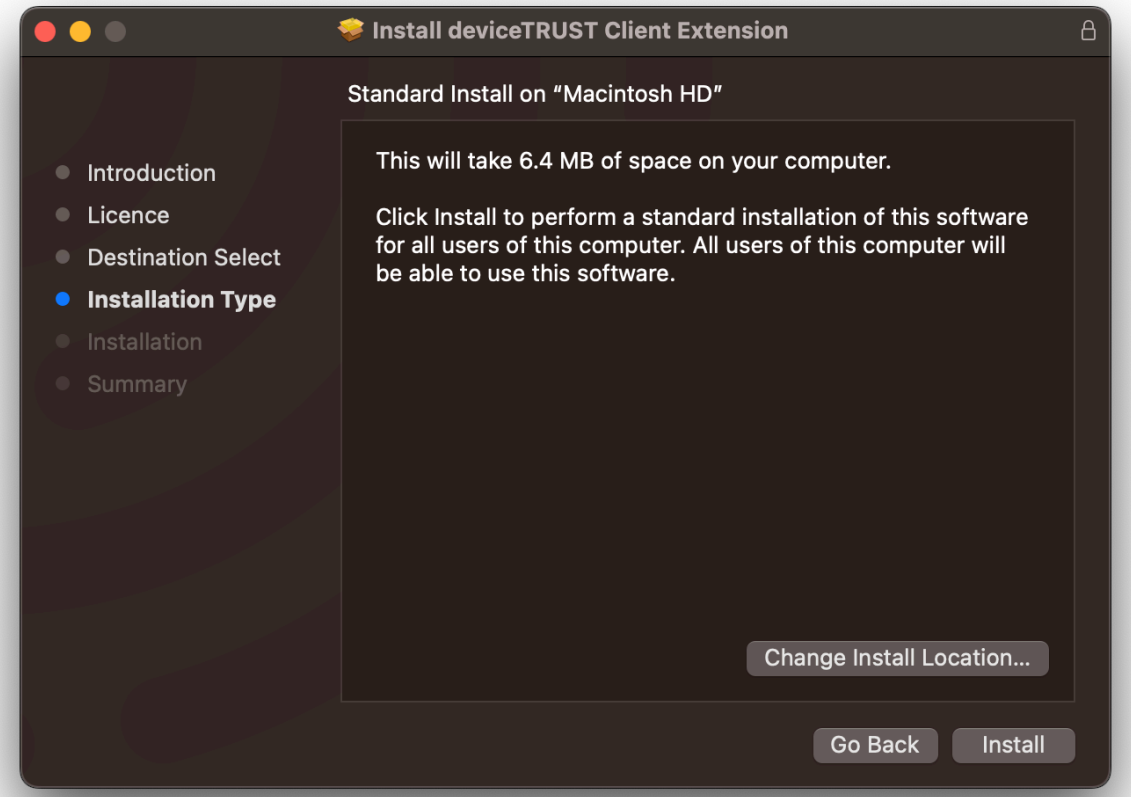


Continue through the installation steps until complete.

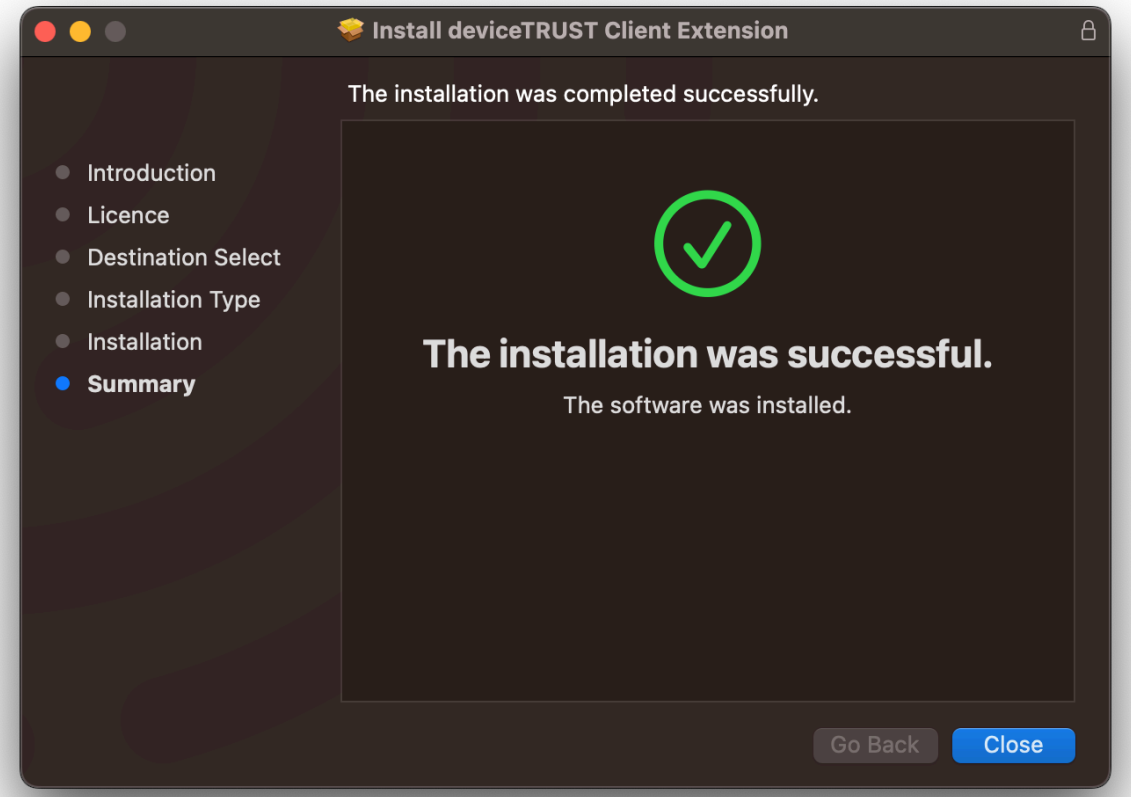
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Client installation on Stratodesk NoTouch OS devices

deviceTRUST is integrated into Stratodesk NoTouch release 3.4.516 or higher and supports the Microsoft Remote Desktop Protocol (RDP), Citrix Independent Computing Architecture (ICA) and VMware Horizon View (Blast, PCoIP and RDP). The deviceTRUST Client Extension binaries are not distributed with NoTouch OS or NoTouch Center, but a URL can be provided for the deviceTRUST Client Extension to be automatically downloaded and installed.

The instructions below use Stratodesk NoTouch Center to configure the environment, however similar steps can be performed with the *Configuration* application available locally on Stratodesk NoTouch OS.

NOTE:

NoTouch OS devices must be restarted after enabling the deviceTRUST® Client Extension.

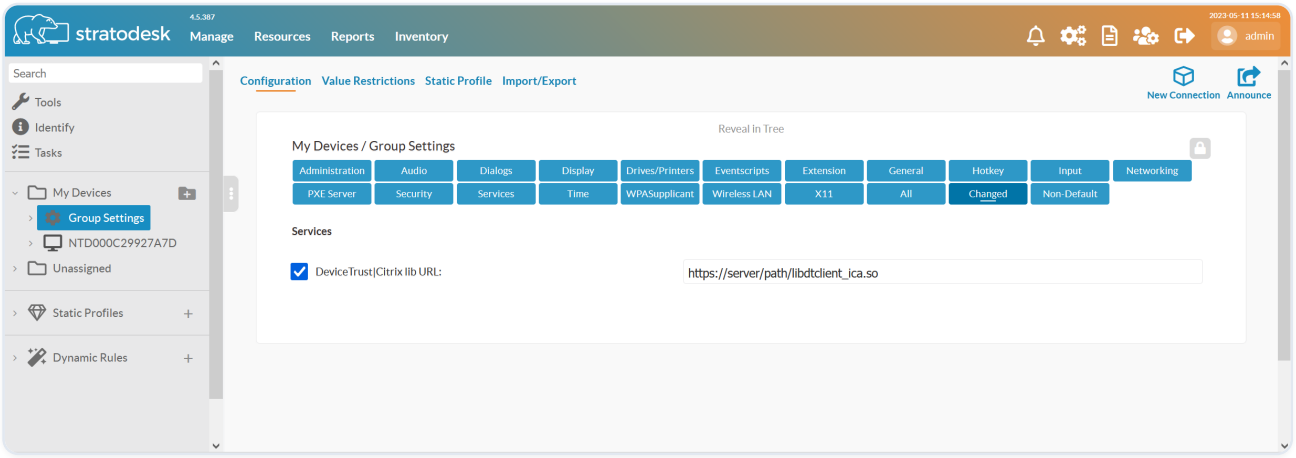
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable deviceTRUST Client Extension for Citrix Workspace™ App

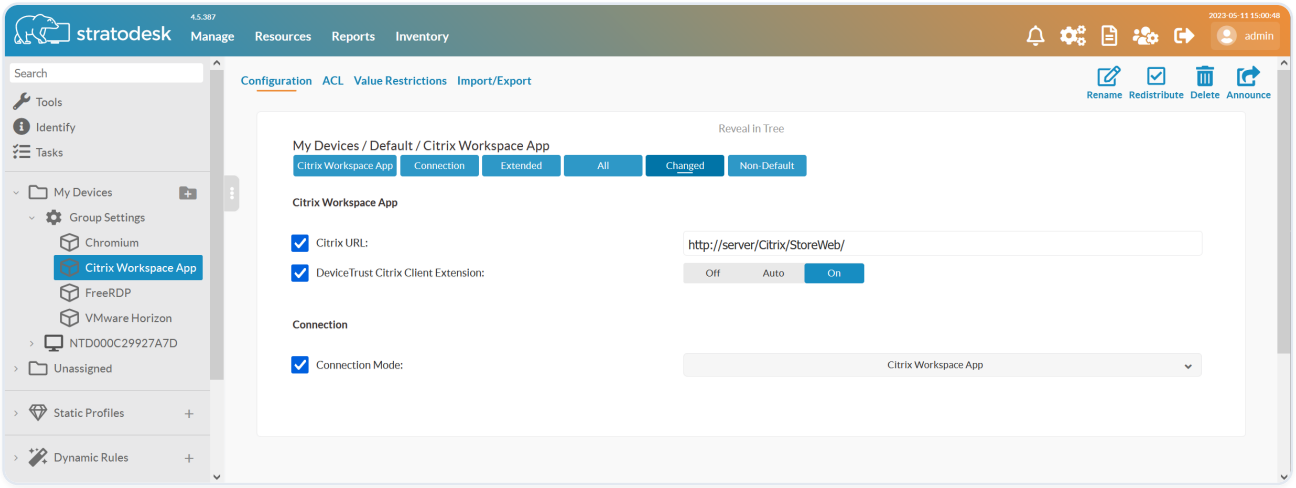
Navigate to `SERVICES` and set `deviceTRUST | Citrix lib URL` to the *NoTouch Citrix URL* available on the Download page.

NOTE:

items="Although this URL can be used for testing, deviceTRUST may change it in the future. To ensure you don't experience any downtime you should copy the file and host it within your own environment."



Finally, within a connection where the connection mode is set to `CITRIX WORKSPACE APP` or `CHROMIUM`, navigate to the `CITRIX WORKSPACE APP` tab and set `deviceTRUST Citrix Client Extension` to `ON`.



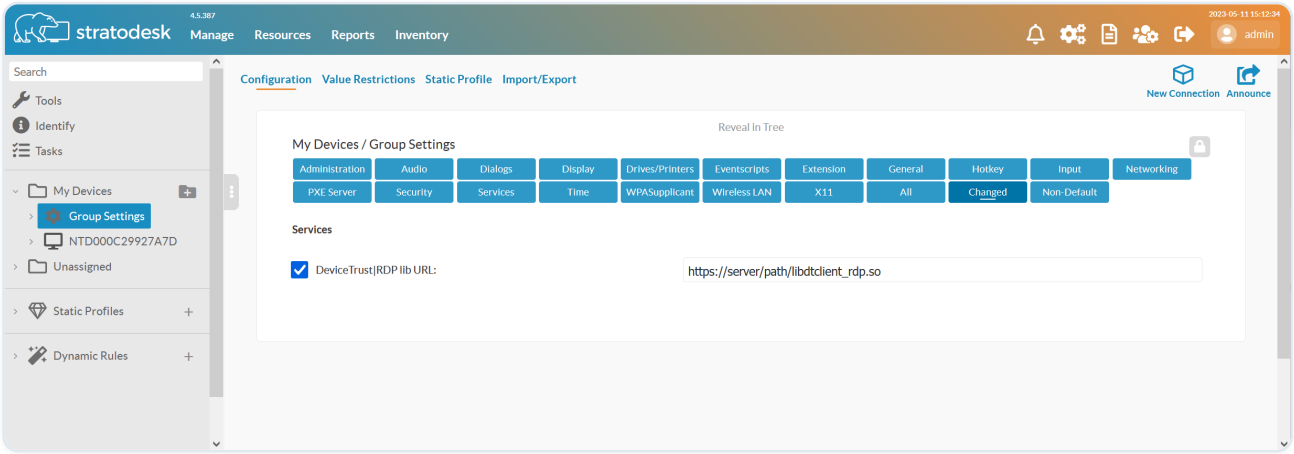
Enable deviceTRUST Client Extension for FreeRDP

Navigate to `SERVICES` and set `deviceTRUST | RDP lib URL` to the *NoTouch RDP URL* available on the Download page.

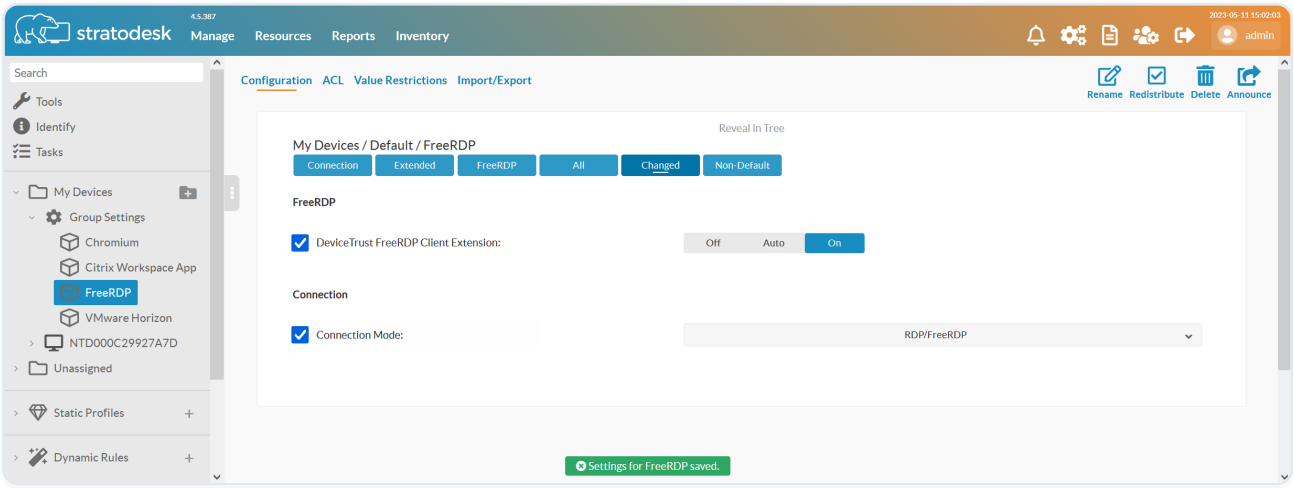
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Although this URL can be used for testing, deviceTRUST may change it in the future. To ensure you don't experience any downtime you should copy the file and host it within your own environment.



Finally, within a connection where the connection mode is set to `RDP/FreeRDP`, navigate to the `FreeRDP` tab and set `deviceTRUST FreeRDP Client Extension` to `ON`.



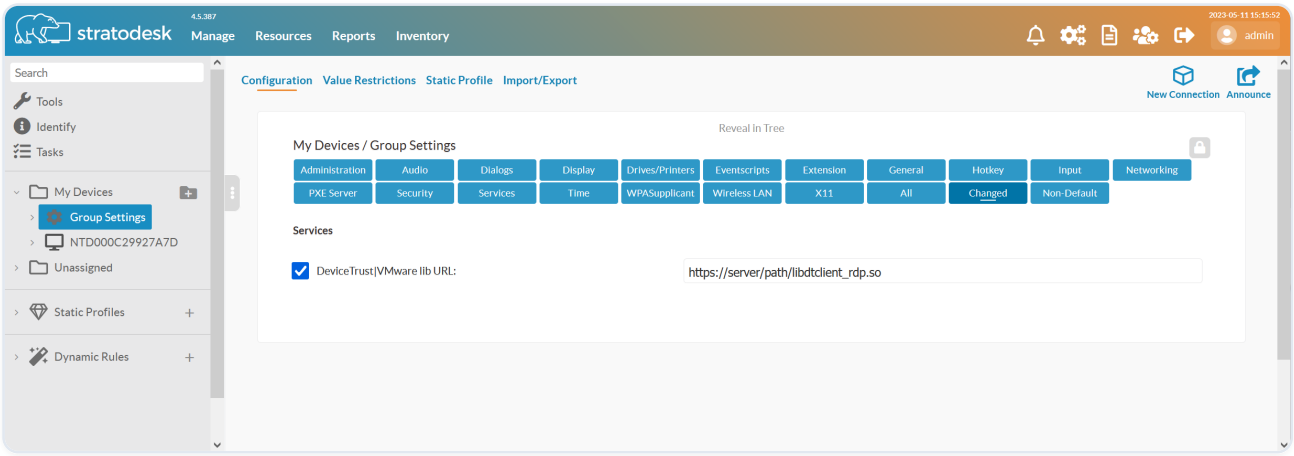
Enable deviceTRUST Client Extension for VMware Horizon View

Navigate to `SERVICES` and set `deviceTRUST | VMware lib URL` to the *NoTouch VMware URL* available on the Download page.

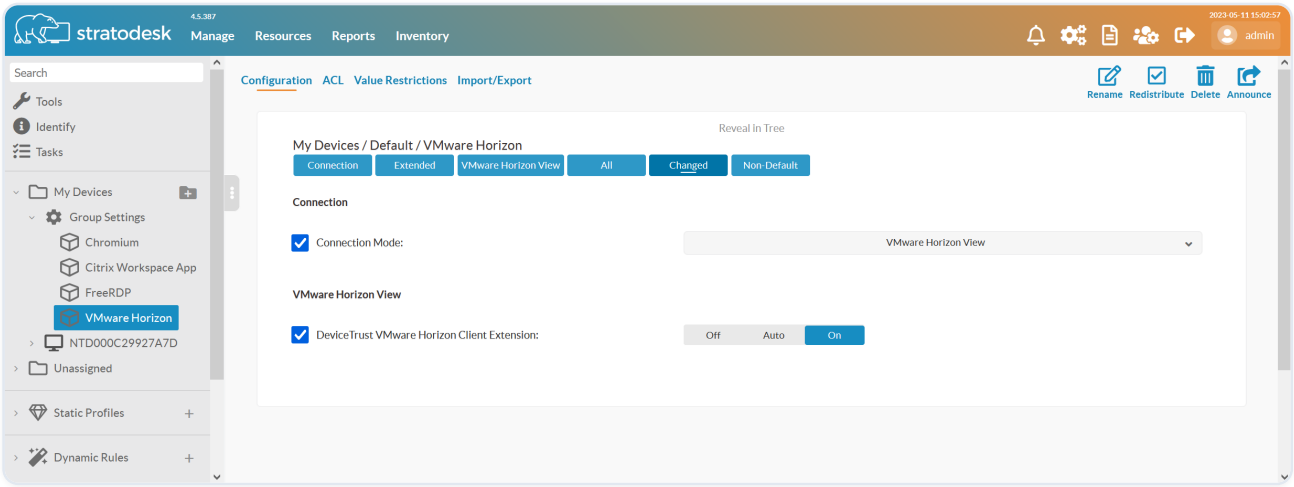
NOTE:

Although this URL can be used for testing, deviceTRUST may change it in the future. To ensure you don't experience any downtime you should copy the file and host it within your own environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



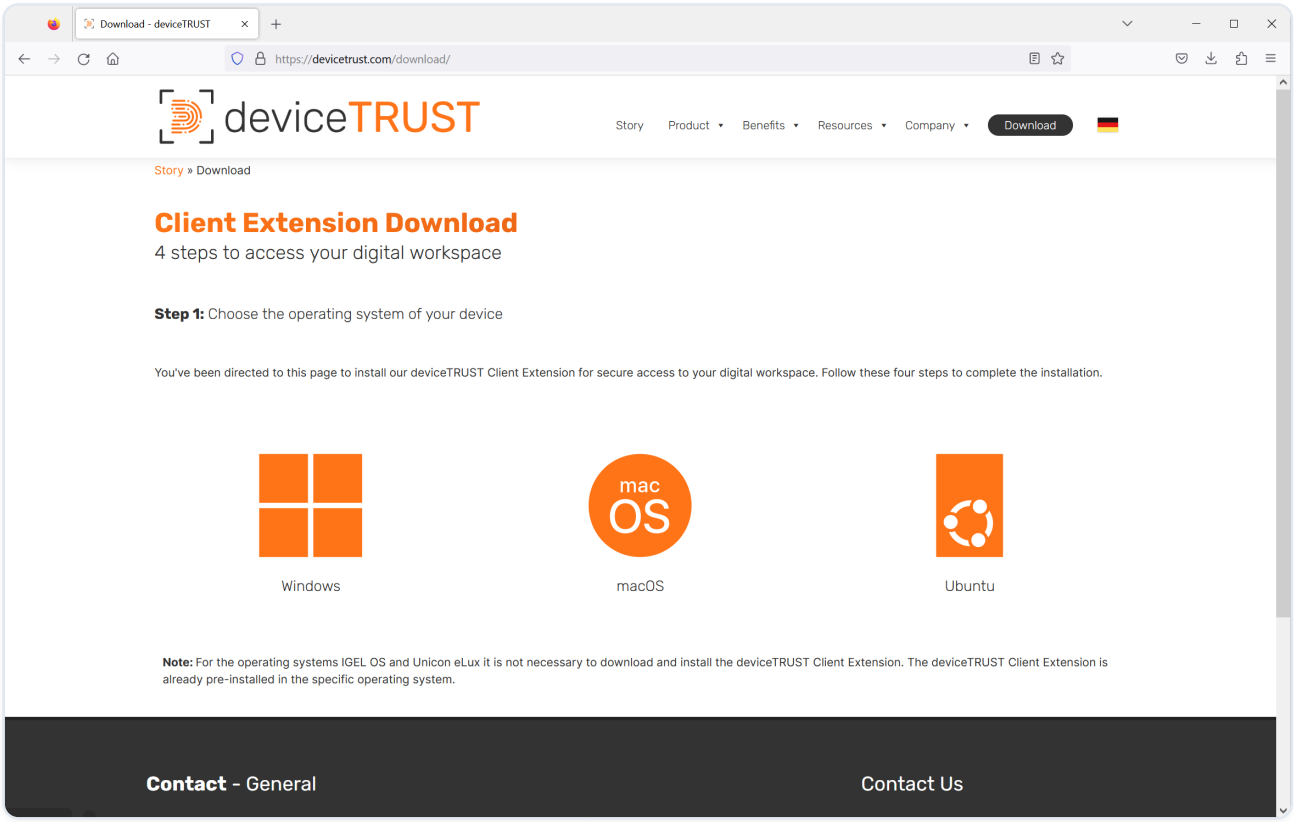
Finally, within a connection where the connection mode is set to `VMware Horizon View` navigate to the `VMware Horizon View` tab and set `deviceTRUST VMware Horizon Client Extension` to `ON`.



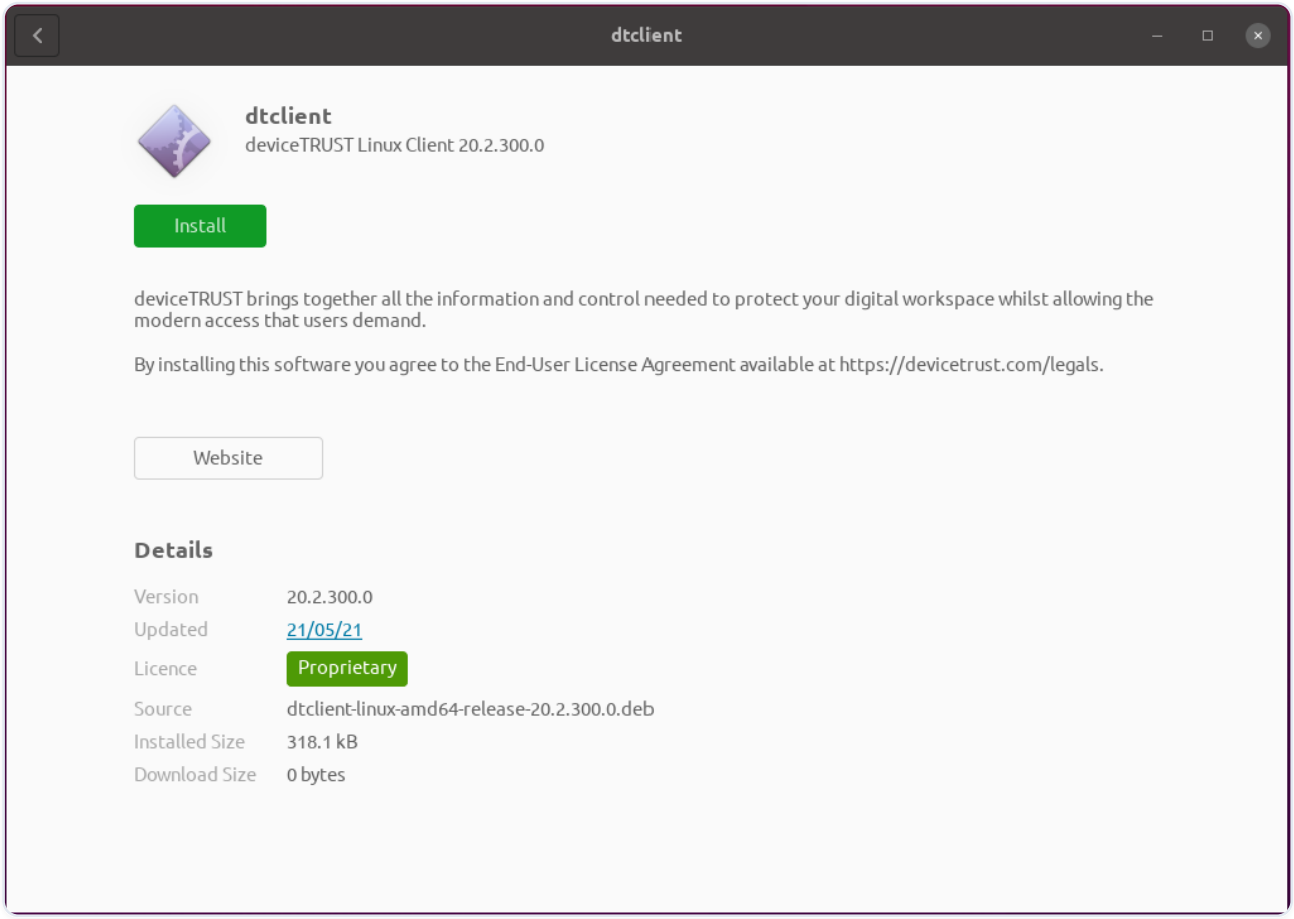
Client installation on Ubuntu devices

The deviceTRUST Ubuntu Client can be downloaded by following the steps on the deviceTRUST Client Extension Download page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

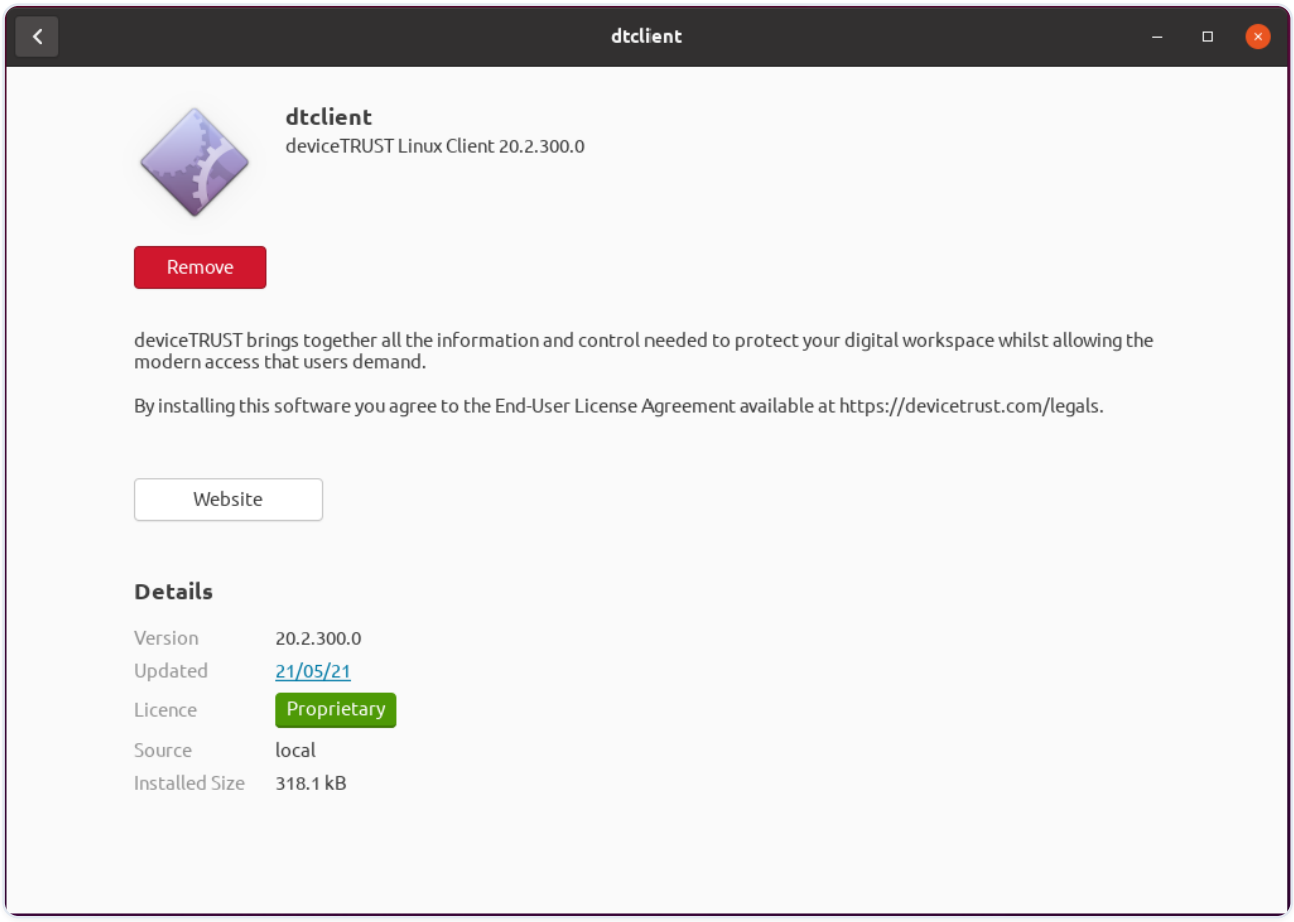


To access the installer, double click on the downloaded 'dtclient-linux-amd64-release-W.X.Y.Z.deb' file.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click *Install* to complete the installation. An *Authentication Required* popup will be displayed and administrative credentials must be entered.

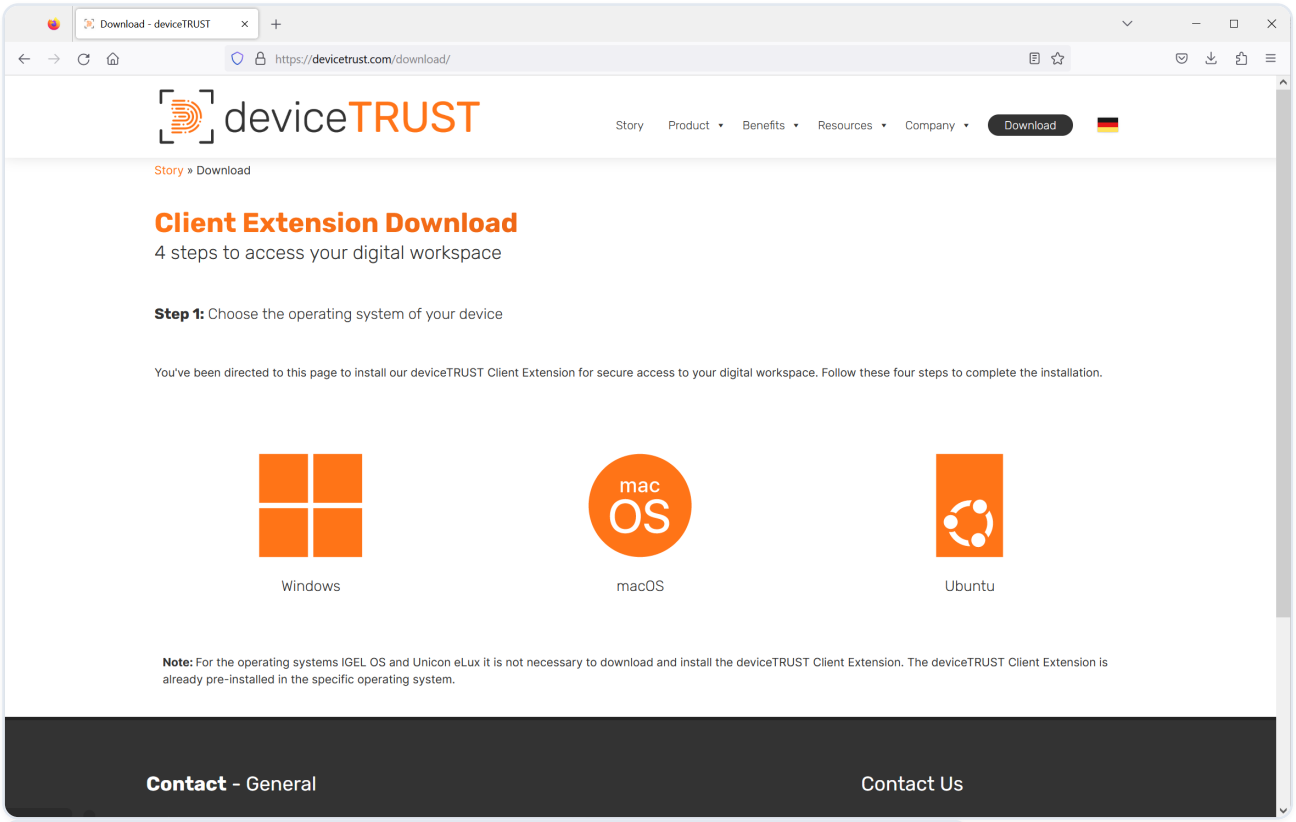


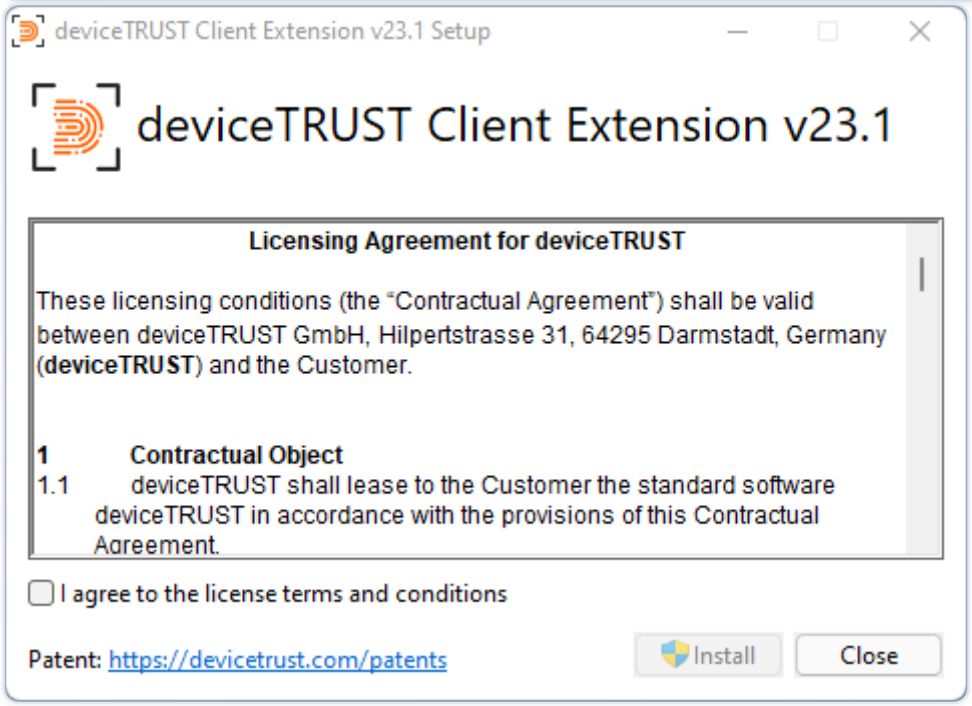
Client Extension installation on Microsoft Windows devices

The deviceTRUST Client Extension can be downloaded by following the steps on the deviceTRUST Client Extension Download page. The installation of the deviceTRUST Client Extension requires one-time administrative privileges of the user installing the deviceTRUST Client Extension.

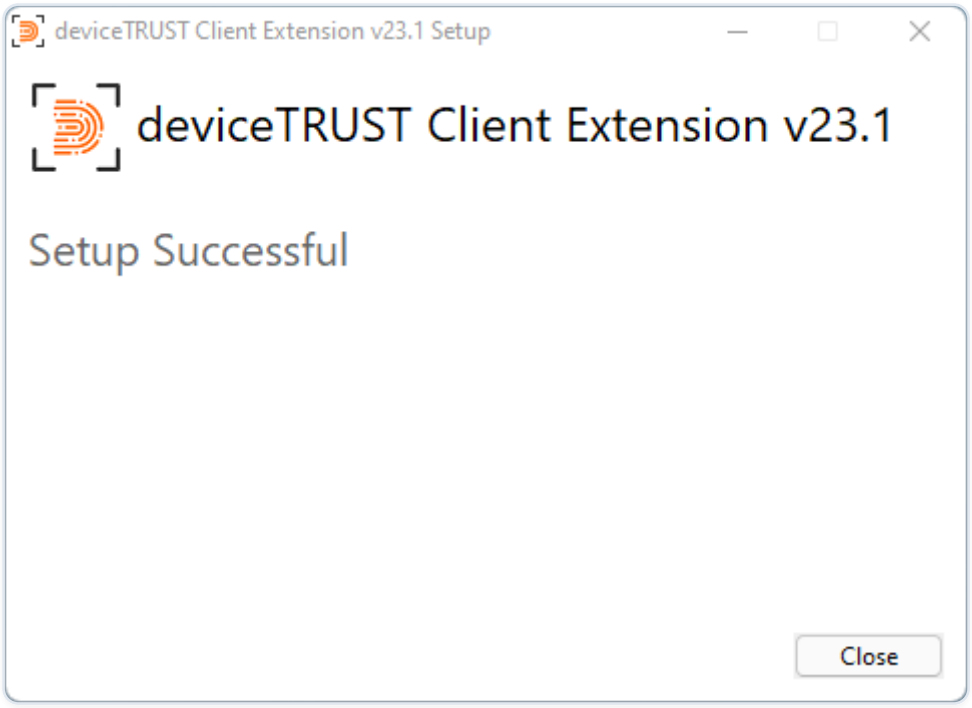
The deviceTRUST® Client Extension for unmanaged Microsoft Windows devices supports an auto-update functionality. If a newer deviceTRUST Client Extension is available, the administrator of the remoting and DaaS environment can enforce a transparent update installation of the local deviceTRUST Client Extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.



IMPORTANT:

When using Microsoft RDP or VMware Horizon, when installing with custom credentials the user must logoff from their session before the installation is effective.

Client Extension Installation Command Line Options

The following command line options are available to the deviceTRUST Client Extension installer:

- `DTCLIENT-EXTENSION-RELEASE-X.X.X.EXE /INSTALL|REPAIR|UNINSTALL` - Installs, repairs or uninstalls the deviceTRUST Client Extension.
- `DTCLIENT-EXTENSION-RELEASE-X.X.X.EXE /PASSIVE|QUIET` - Passive displays a minimal user interface with no prompts for input. Quiet displays no user interface.
- `DTCLIENT-EXTENSION-RELEASE-X.X.X.EXE /NORESTART` - Surpresses any attempt to restart the local device.
- `DTCLIENT-EXTENSION-RELEASE-X.X.X.EXE /LOG <log.txt>` - Logs to a specific file. By default, logs are created within %TEMP%.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

One or more of the above options can be combined. Installation path: %PROGRAMFILES% \DEVICETRUST\CLIENT The deviceTRUST Client Extension installer installs both the 32-bit and 64-bit deviceTRUST Client Extension components depending on the Windows operating system platform.

Unattended Installation

The deviceTRUST Client Extension installer can be installed unattended from the command line interface with the following options:

COMPONENT	COMMANDLINE	
dtclient-extension-release-x.x.x.exe	An unattended installation can be achieved with the following parameters `DTCLIENT-RELEASE-X.X.X.EXE /INSTALL /QUIET`	

Active Setup Components

The deviceTRUST Client Extension uses Active Setup to make changes to the users profile. This involves the creation of the following Active Setup components.

deviceTRUST Channel Registration 64-bit component

Registry Key: `HKLM\Software\Microsoft\Active Setup\Installed Components\{2f780db6-903f-4c83-9d60-9d138e054dc9}`

This Active Setup component is created during installation, and is responsible for the registration of the 64-bit Microsoft RDP Virtual Channel within the users profile. When not using the 64-bit Microsoft RDP Virtual Channel, it is safe to remove this key after the deviceTRUST Client Extension has been installed.

deviceTRUST Channel Registration 32-bit component

Registry Key: `HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{8a4445d6-867e-4e60-8cc5-05bc2e3a2512}` (or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`HKLM\Software\Microsoft\Active Setup\Installed Components\{8a4445d6-867e-4e60-8cc5-05bc2e3a2512}` on a 32-bit OS)

This Active Setup component is created during installation, and is responsible for:

- The registration of the 32-bit Microsoft RDP Virtual Channel.
- The registration of the 32-bit Citrix ICA® Virtual Channel with per-user installations of Citrix Workspace™ within the users profile.
- The registration of the 32-bit Amazon WorkSpaces Virtual Channel with per-user installations of Amazon WorkSpace within the users profile. When not using 32-bit Microsoft RDP or per-user installations of Citrix Workspace App or Amazon WorkSpaces Client, it is safe to remove this key after the deviceTRUST Client Extension has been installed.

deviceTRUST Citrix Cleanup 32-bit component

Registry Key: `HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{3d65bd68-a307-4d64-af9c-17bc9c4b36e3}`

This Active Setup component is created during uninstallation and is responsible for removing the registration of the 32-bit Citrix ICA Virtual Channel with per-user installations of Citrix Workspace within the users profile. When not using per-user installations of Citrix Workspace, it is safe to remove this key after the deviceTRUST Client Extension has been uninstalled.

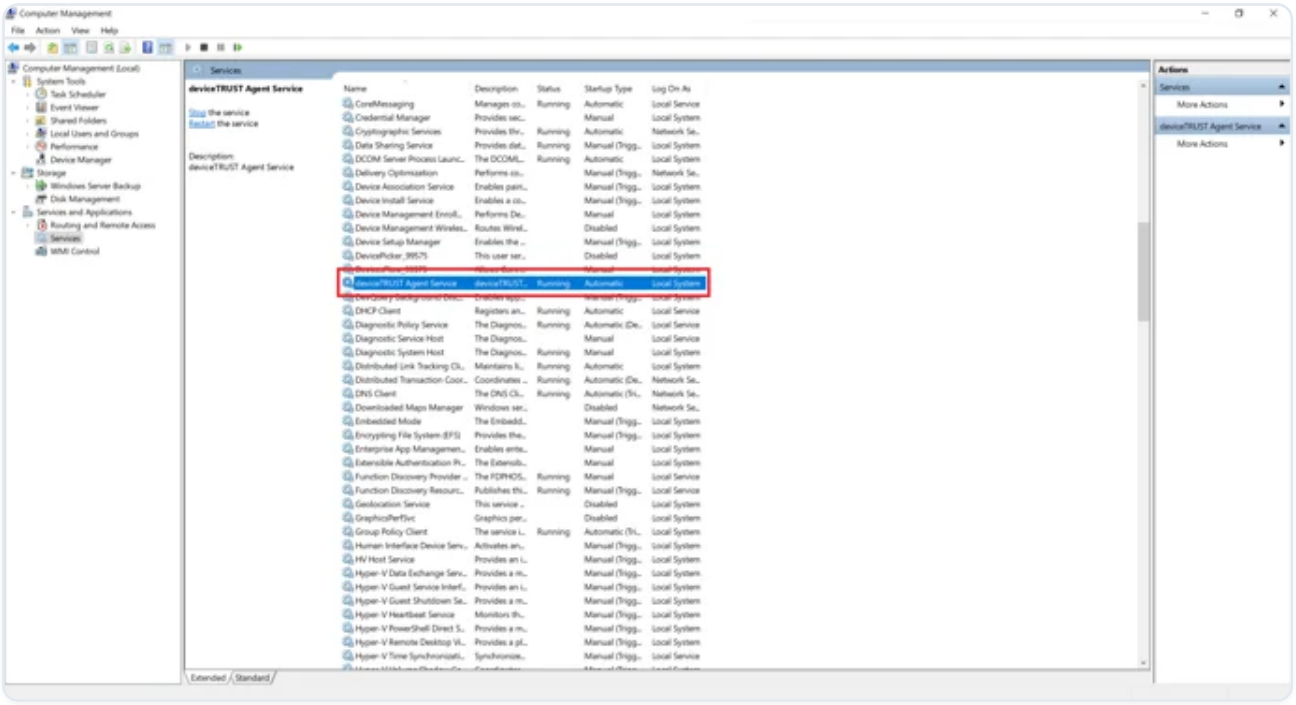
Check that the deviceTRUST® Agent service is running

The deviceTRUST Agent service must be running on the host system for it to enforce the policy. If this service is not running, then no deviceTRUST contextual security policies can be applied to the users.

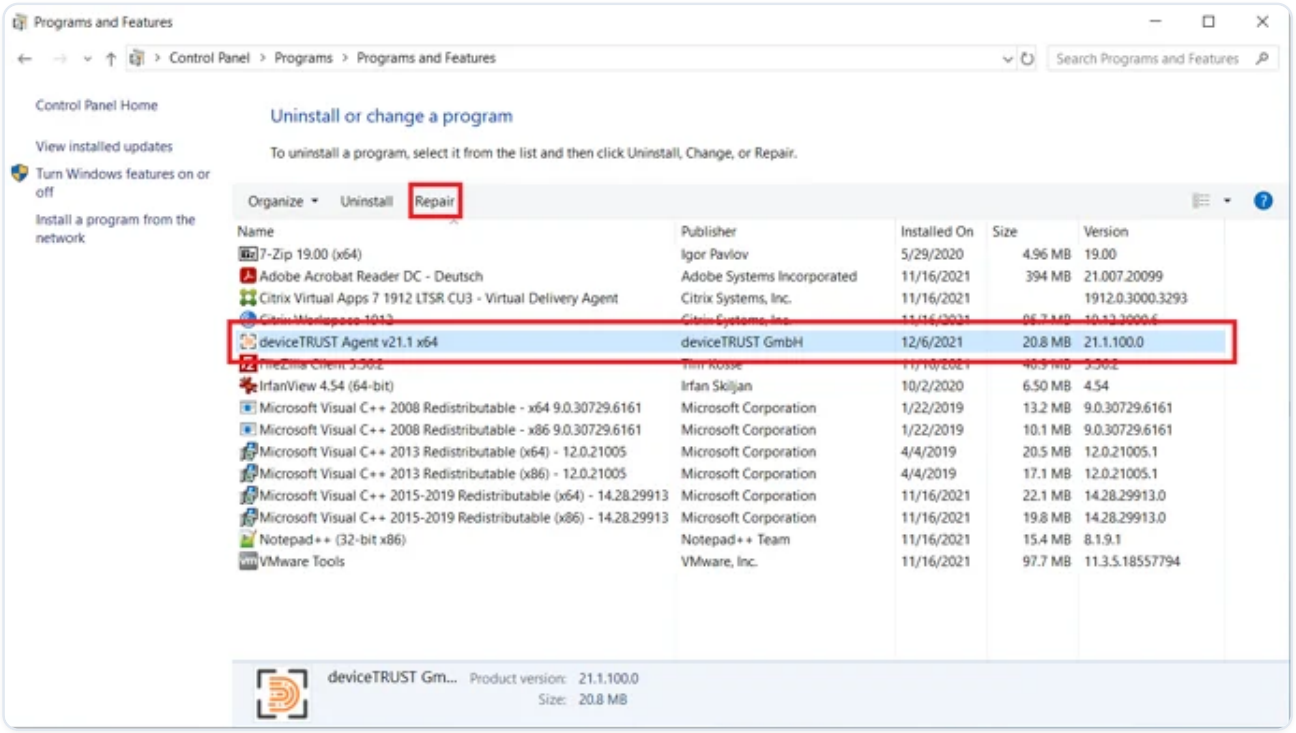
The deviceTRUST Agent service is monitored by standard operating system functions and recovered if necessary.

Open the COMPUTER MANAGEMENT on the host system, navigate to SERVICES AND APPLICATIONS, select SERVICES and check that the DEVICETRUST AGENT SERVICE is running. If the service is not running, try to start it from the menu or context menu by selecting START.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the deviceTRUST Agent service does not start you can repair the deviceTRUST Agent installation. To do this, please open the CONTROL PANEL, navigate to PROGRAMS and open PROGRAMS AND FEATURES. Select DEVICETRUST AGENT VXX.X X64 and start the repair of the installation with the REPAIR button. Repair deviceTRUST Agent installation



Check that you are using the latest deviceTRUST® version

The latest deviceTRUST releases may contain bugfixes that were present in previous releases, or compatibility fixes that have since been discovered with other third party components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Therefore, it is recommended to upgrade to the latest deviceTRUST version from time to time. This can be done very easily by transparently updating the corresponding deviceTRUST component (Agent, Console and Client Extension) by running the newer installer.

Before upgrading, refer to the Upgrading section of the compatibility guide, and ensure that you have read the release notes. The latest deviceTRUST software can be found on our Download page.

Configuration of the deviceTRUST® Client Extension virtual channel for ICA

This article details the files and configuration involved in the registration of the deviceTRUST Client Extension virtual channel for the ICA® protocol on Microsoft Windows, Ubuntu and Apple macOS platforms.

Microsoft Windows (All Users)

The following registry entries are required for the All Users install of Citrix Workspace™:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA
Client\Engine\Configuration\Advanced\Modules\ICA 3.0"

VirtualDriverEx (REG_SZ) = deviceTRUST



"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA
Client\Engine\Configuration\Advanced\Modules\deviceTRUST"

DriverName (REG_SZ) = Unsupported

DriverNameWin16 (REG_SZ) = Unsupported

DriverNameWin32 = dtclient.dll
```

Additionally, the installation folder identified by "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Install\ICA Client" value InstallFolder (REG_SZ) and defaulting to "C:\Program Files (x86)\Citrix\ICA Client" must contain a copy of the 32-bit dtclient.dll from "%ProgramFiles(x86)%\deviceTRUST\Client\Bin\dtclient.dll".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All of the above registry keys and the file on disk are monitored by the 'dtclient' Windows Service. If any of the values are modified then they are automatically reverted to their correct values.

Microsoft Windows (Per User)

The following registry entries are required for the Per User install of Citrix Workspace:

```
"HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\ICA
Client\Engine\Configuration\Advanced\Modules\ICA 3.0"

VirtualDriverEx (REG_SZ) = deviceTRUST



"HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA
Client\Engine\Configuration\Advanced\Modules\deviceTRUST"

DriverName (REG_SZ) = Unsupported

DriverNameWin16 (REG_SZ) = Unsupported

DriverNameWin32 = dtclient.dll
```

Additionally, the installation folder identified by "HKEY_CURRENT_USER\SOFTWARE\Citrix\Install\ICA Client" value InstallFolder (REG_SZ) and defaulting to "C:\Program Files (x86)\Citrix\ICA Client" must contain a copy of the 32-bit dtclient.dll available at "%ProgramFiles(x86)%\deviceTRUST\Client\Bin\dtclient.dll".

All of the above registry keys and the file on disk are monitored by the 'dtclient' Windows Service. If any of the values are modified then they are automatically reverted to their correct values.

Apple macOS

The file "~/Library/Application Support/Citrix Receiver/Modules" must contain the following entries:

```
[ICA 3.0]

VirtualDriver=deviceTRUST

deviceTRUST=On
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[deviceTRUST]

DriverName=dtclient.dll
```

Additionally the folder "/Library/Application Support/Citrix/PlugIns/deviceTRUST" must contain the deviceTRUST virtual channel extension for Citrix ICA.

Neither the Modules file or the files on disk are monitored for incorrect values. To repair, perform an uninstall and reinstall of the installation.

If using an Apple M1 or later processor, please refer to deviceTRUST + Apple M1 support for Citrix Workspace.

Ubuntu

The module.ini file at "/opt/Citrix/ICAClient/config/module.ini" must contain the following entries:

```
[ICA 3.0]

VirtualDriver=deviceTRUST

deviceTRUST=On



[deviceTRUST]

DriverName=dtclient.dll
```

Additionally, "/opt/Citrix/ICAClient/dtclient.dll" must be a symbolic link to "/opt/deviceTRUST/Client/Bin/libdtclient.so".

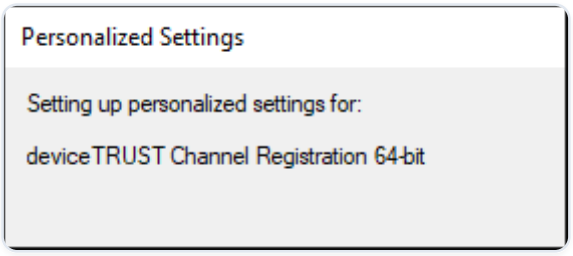
Neither the module.ini or the files on disk are monitored for incorrect values. To repair, perform an uninstall and reinstall of the installation.

deviceTRUST® Client Extension & Active Setup

Active Setup Components

The deviceTRUST Client Extension uses Active Setup to make changes to the users profile. This involves the creation of the following Active Setup components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



deviceTRUST Channel Registration 64-bit component

Registry Key:

```
HKLM\Software\Microsoft\Active Setup\Installed
Components\{2f780db6-903f-4c83-9d60-9d138e054dc9}
```

This Active Setup component is created during installation, and is responsible for the registration of the 64-bit Microsoft RDP Virtual Channel within the users profile. When not using the 64-bit Microsoft RDP Virtual Channel, it is safe to remove this key after the deviceTRUST Client Extension has been installed.

deviceTRUST Channel Registration 32-bit component

Registry Key:

```
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
Components\{8a4445d6-867e-4e60-8cc5-05bc2e3a2512}

HKLM\Software\Microsoft\Active Setup\Installed
Components\{8a4445d6-867e-4e60-8cc5-05bc2e3a2512} (on a 32-bit OS)
```

This Active Setup component is created during installation, and is responsible for:

- The registration of the 32-bit Microsoft RDP Virtual Channel.
- The registration of the 32-bit Citrix ICA® Virtual Channel with per-user installations of Citrix Workspace™ within the users profile.
- The registration of the 32-bit Amazon WorkSpaces Virtual Channel with per-user installations of Amazon WorkSpace within the users profile. When not using 32-bit Microsoft RDP or per-user installations of Citrix Workspace App or Amazon WorkSpaces Client, it is safe to remove this key after the deviceTRUST Client Extension has been installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST Citrix Cleanup 32-bit component

Registry Key:

```
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
Components\{3d65bd68-a307-4d64-af9c-17bc9c4b36e3}
```

This Active Setup component is created during uninstallation and is responsible for removing the registration of the 32-bit Citrix ICA Virtual Channel with per-user installations of Citrix Workspace within the users profile. When not using per-user installations of Citrix Workspace, it is safe to remove this key after the deviceTRUST Client Extension has been uninstalled.

Enabling DCV extensions on Amazon WorkSpaces WSP

The deviceTRUST® Agent uses a DCV extension to communicate with the deviceTRUST Client Extension within a Nice DCV environment. Amazon WorkSpaces with the WSP protocol is built on the same Nice DCV technology, but requires DCV extensions to be enabled for this to work.

Installing the Administrative Templates

To enable the DCV extensions, you must first copy the ADMX/ADML administrative templates from the Amazon WorkSpaces instance to the machine used to configure policy for the Amazon WorkSpaces environment.

If your tools use local policy definitions, such as if you are using the Local Group Policy Editor, or using Group Policy Management Tools not configured for a Central Store, then the following files need to be copied from the Amazon WorkSpaces environment to the local file system:

- Copy `C:\Program Files\Amazon\WSP\wsp.admx` to `C:\Windows\PolicyDefinitions\wsp.admx`
- Copy `C:\Program Files\Amazon\WSP\wsp.adml` to `C:\Windows\PolicyDefinitions\en-US\wsp.adml`

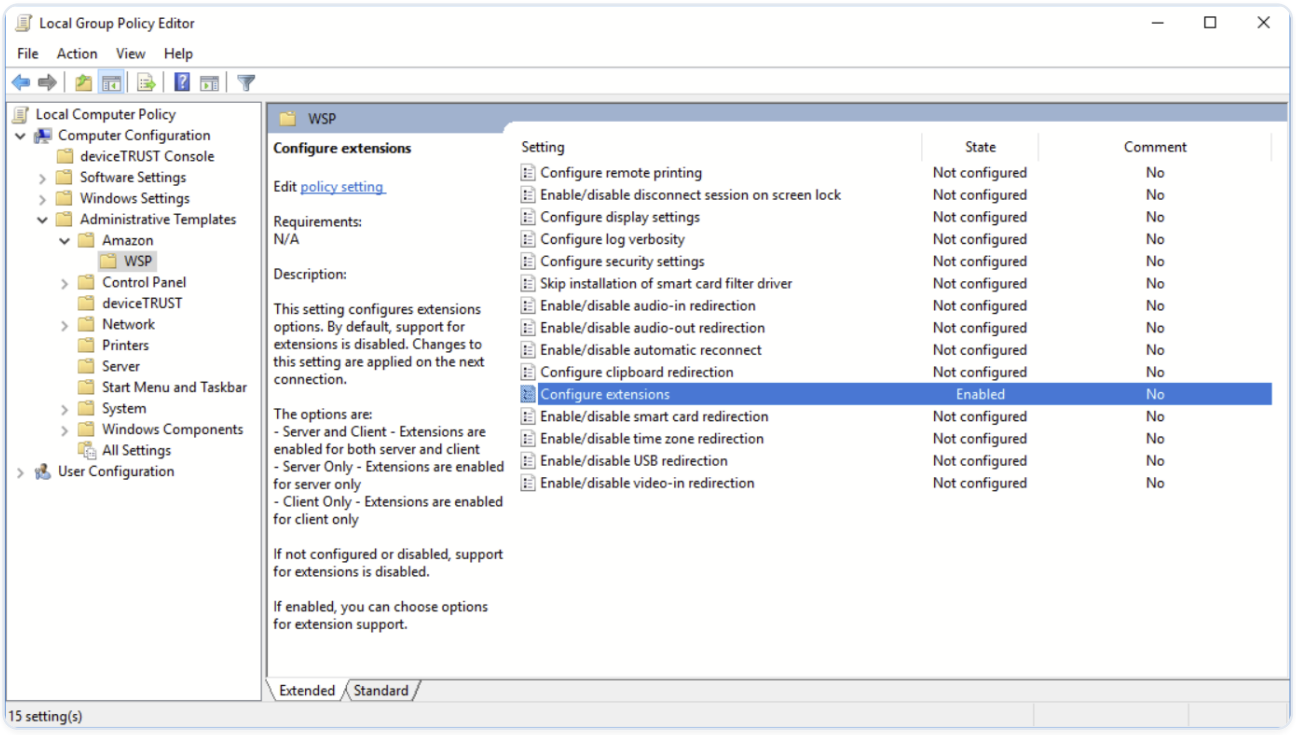
If however you are using a Central Store, then the following files need to be copied to the Central Store:

- Copy `C:\Program Files\Amazon\WSP\wsp.admx` to `\\<forest.root>\SysVol<forest.root>\Policies\PolicyDefinitions\wsp.admx`
- Copy `C:\Program Files\Amazon\WSP\wsp.adml` to `\\<forest.root>\SysVol<forest.root>\Policies\PolicyDefinitions\en-US\wsp.adml`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

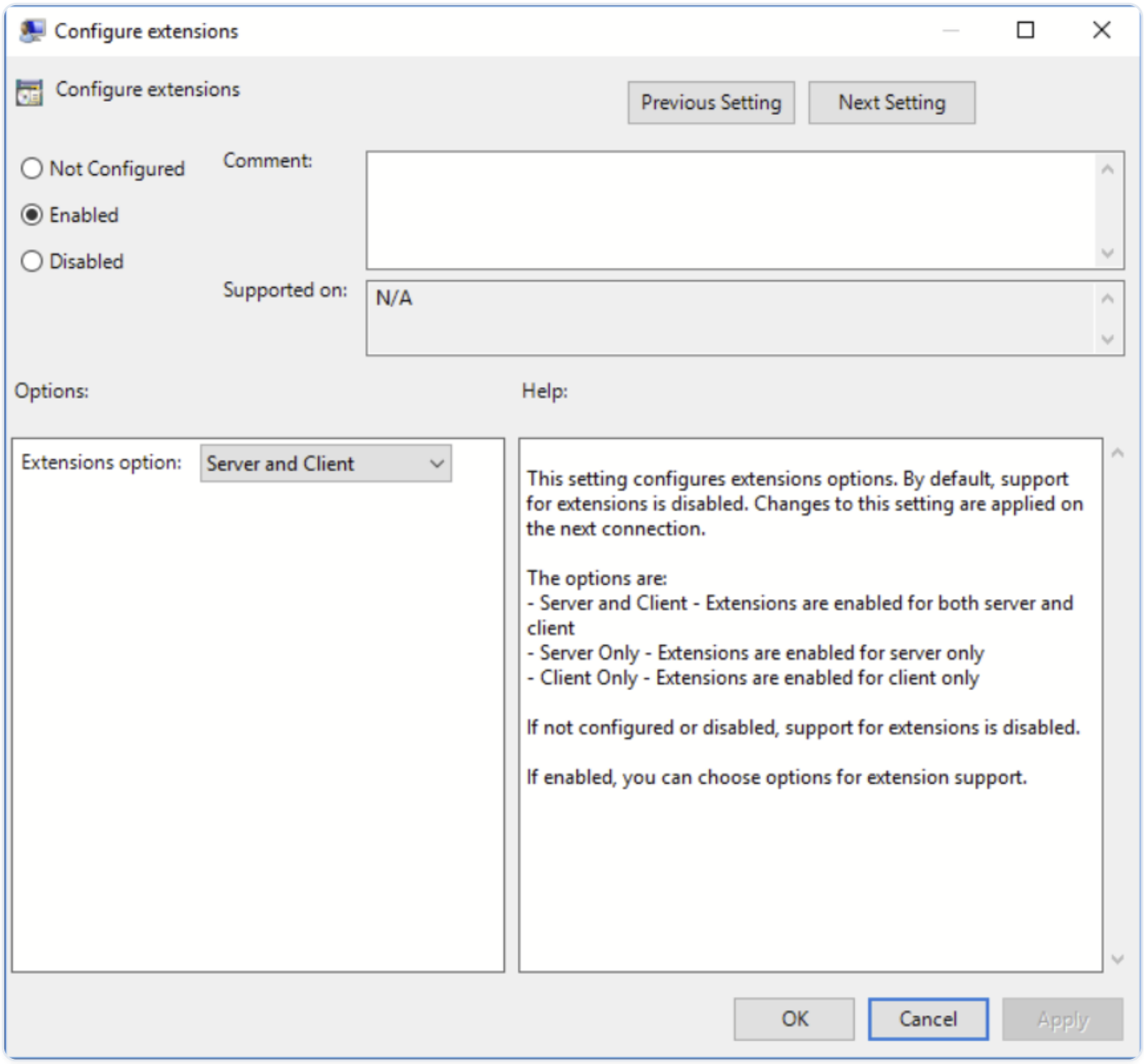
Configuring DCV Extensions

Within the policy editor of your choice, navigate to Administrative Templates -> Amazon -> WSP and enable the Configure extensions setting:



The Configure extensions setting must be set to Server and Client to ensure that both the server and client DCV extensions can be loaded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Additional Requirements

Ensure that your Amazon WorkSpaces instances are configured as follows:

- Using the WSP protocol.
- Have a WSP application installed versioned 2.0.0.799 or greater.
- Have a licensed deviceTRUST Agent version 23.1.100 or greater.

Your end users must:

- Have a Amazon WorkSpaces Client versioned 5.9.0.4129 or greater.
- Have a deviceTRUST Client Extension version 23.1.100 or greater.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Silent removal of the deviceTRUST® Client Extension for Apple macOS

The deviceTRUST Client extension for macOS ships with an Uninstall.app requiring input from the user to manually run the Uninstall.app. To remove the Client Extension for macOS without using the Uninstaller.app please use the following steps.

Steps to silently remove the Client Extension for macOS

Open Terminal and type the following commands:

- cd /Library/Application \ Support/deviceTRUST/Client/Bin
- sudo ./install.sh UNINSTALL
- sudo rm -rf /Library/Application\ Support/deviceTRUST

This will remove the deviceTRUST Client Extension from the macOS computer.

Make sure that you have a valid license

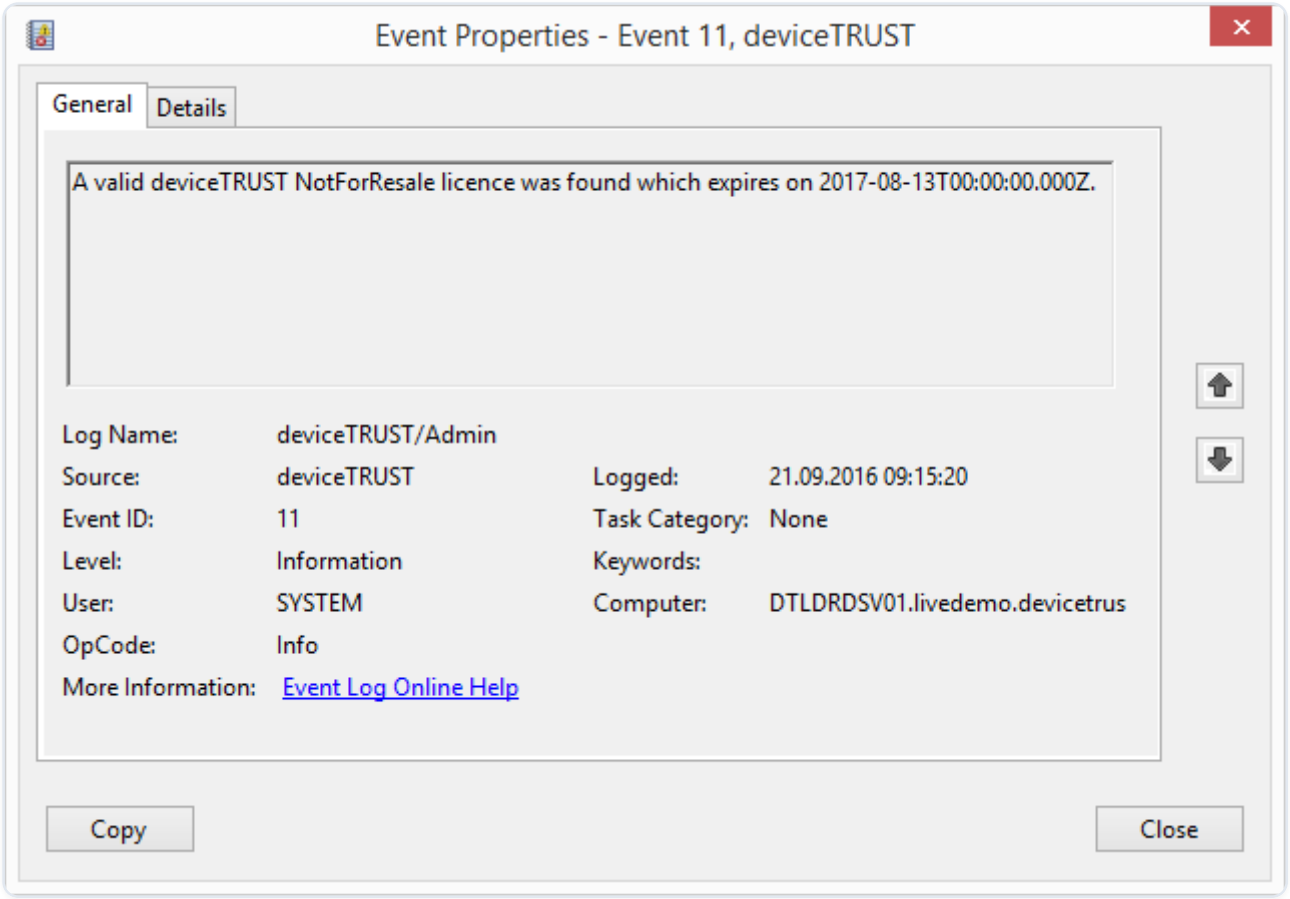
If your deviceTRUST License has not been configured, or has expired, then you may find that the deviceTRUST functionality is disabled.

To check if licensing is causing a problem, open the Windows Event Log on the host system running the deviceTRUST Agent and navigate to APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN and look for an Event ID between 11 and 16.

- Event ID 11 is used to report a valid license.
- Event ID 12 and 13 are used to report a license that will soon expire.
- Event ID 14, 15 and 16 are used to report an invalid license.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Valid deviceTRUST License

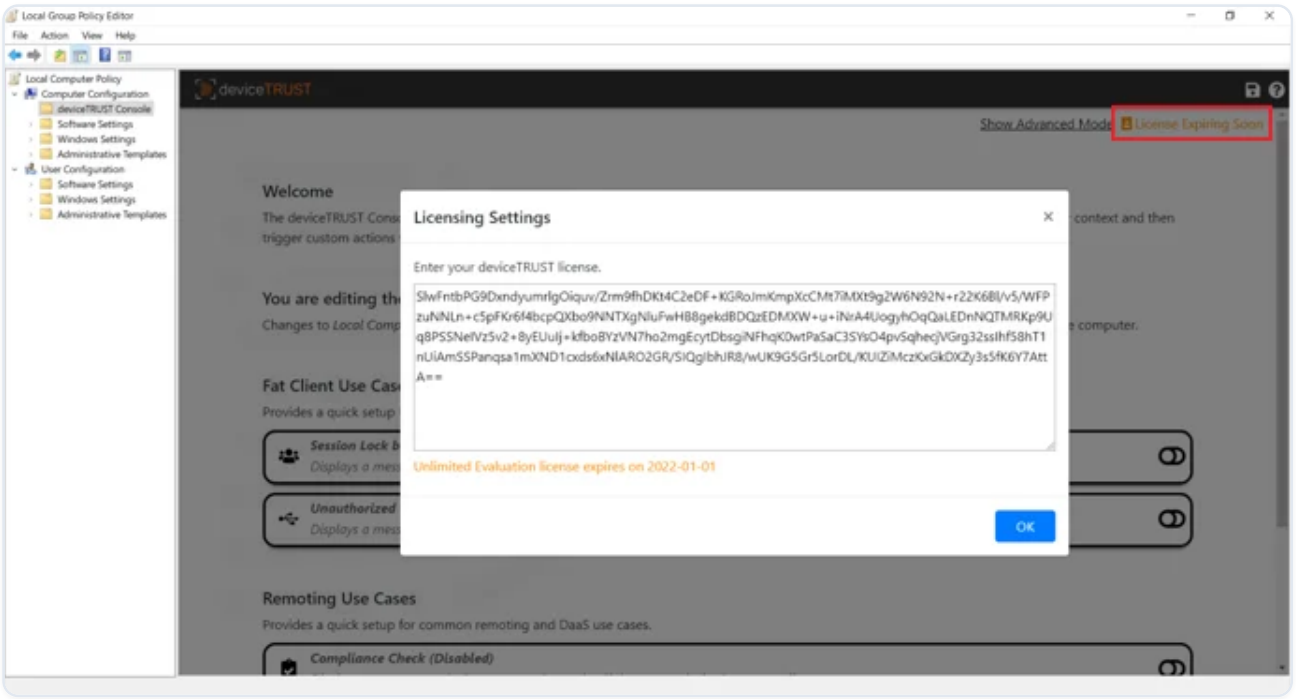


If your Windows Event Log reports a licensing event other that Event ID 11, then you should check your license.

Within the deviceTRUST Console navigate to the Homepage and look in the top right corner for a licensing warning or error, which can be clicked to display more information. If a wrong or incorrect license was entered, correct the license, click OK and then save your active deviceTRUST Policy before updating it on the remoting host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Check deviceTRUST License



Depending on the method used to deploy the deviceTRUST Policy, the corresponding deviceTRUST Policy must be opened to check the licensing status.

- Local Policy
- Group Policy Object (GPO)
- File-based

Group Policy Object (GPO) deployed configuration

If you choose to deploy deviceTRUST the configuration, including the license by GPO, there are several potential reasons why a license might not be applied.

Start your evaluation in the Windows event log. deviceTRUST reports policy application with "Event ID 3". This event contains information about all configuration content the deviceTRUST Agent could extract from GPO, Local Policy, or file.

Check if the correct policy has been applied and shows a valid last modified timestamp. The displayed timestamp always uses the UTC timezone.

- *The correct policy has not been applied:* Check
- If the policy is linked correctly in your AD
- If the latest policy changes have been replicated all over your AD controllers
- If the policy application works well for the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use "gpresult" in an administrative context to see the policies applied to the machine. This will show you if your AD configuration is correct for the machine.
- *The correct policy has been applied, but does not show the correct timestamp:* Update your policies via "gpupdate" (or similar). The machine did not receive the latest policies and thus might not hold the correct configuration/license. Also check your AD domain for potential replication issues.
- *The correct policy has been applied and shows the correct timestamp:* Check the configuration in the deviceTRUST console.
- Is the license information imported correctly?
- Does the console show "licensed"?
- You might have several deviceTRUST policies. Please make sure only one holds the licensing information.
- *Still seeing license issues?* That's a case for the support team.

IGEL OS 12 - No IGEL Properties

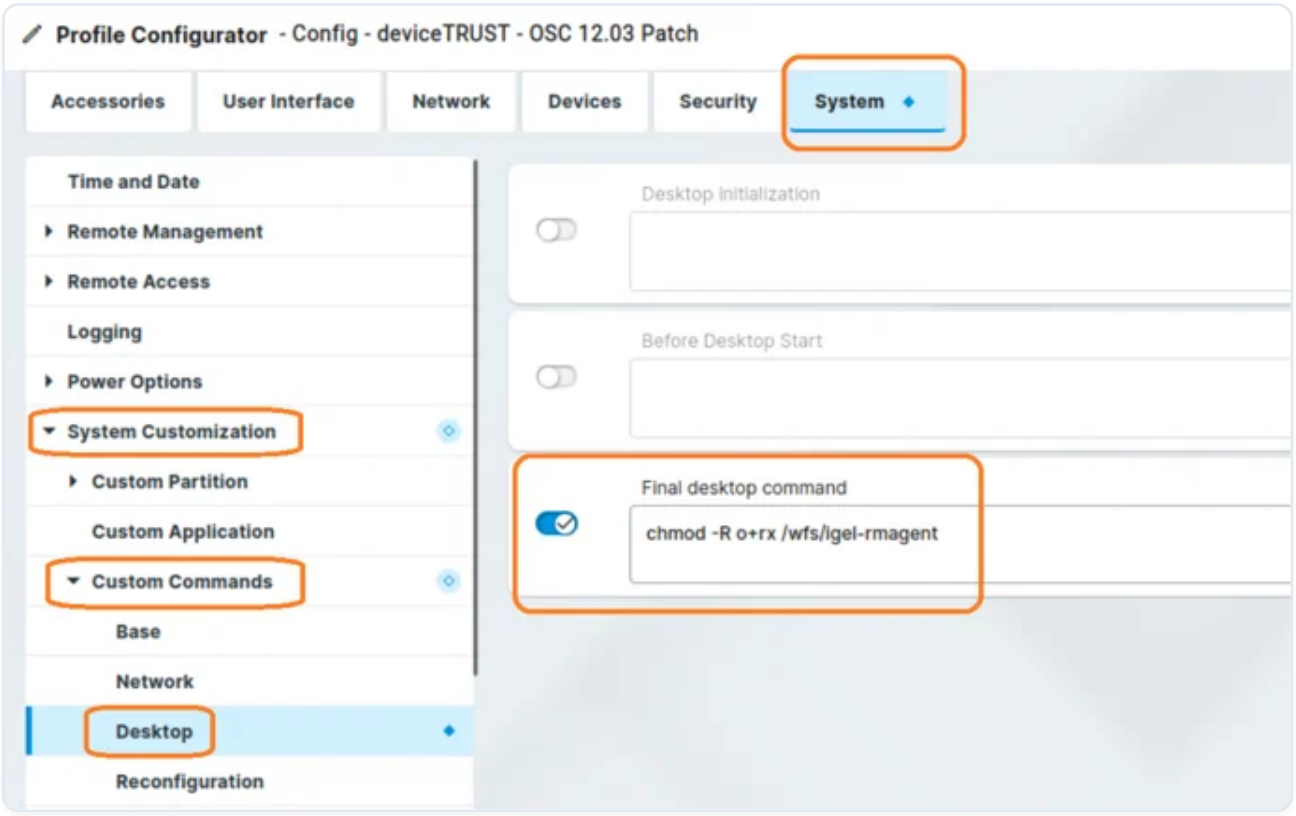
IGEL OS 12, created with OSC 12.03 and younger, does not provide IGEL-specific properties in deviceTRUST. Here's why and how to fix.

Problem: No IGEL-specific deviceTRUST® properties are supplied by IGEL OS 12

Reason: IGEL has changed the file system rights starting with clients rolled out based on OSC 12.03. The folder "/wfs/igel-rmagent" can now only be read by root, no longer by other entities. deviceTRUST needs access to the folder in order to be able to read various properties. Our process recognizes the missing rights and ends the evaluation. Therefore, no IGEL-specific values are evaluated and shown in the session.

Workaround: A "custom command" for setting authorization provides a remedy. We have tested various scenarios and narrowed down the required rights so that a recursive "o+rx" (add read and execute for "others") is sufficient: chmod -R o+rx /wfs/igel-rmagent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



We assume that the setting of the rights was no coincidence and are working on a solution to mitigate this behavior without requiring this workaround. Until then, please implement the workaround to make sure deviceTRUST can operate as desired.

Device Location

A summary of how device location is determined by deviceTRUST.

Location Information

deviceTRUST can make available location information about either a physical device or a remote device when connecting to a virtual session. The location information made available depends upon the deviceTRUST Policy but may include:

- *Source* - the source of the location, such as IP Address, Wi-Fi, Cell Tower or GPS Sensor
- *Provider* - the provider that produced the location, such as the Operating System
- *Position* - the coordinates of the device
- *Accuracy* - the accuracy of the coordinates
- *Address* - the geocoded address of the coordinates
- *Country* - the country that the coordinates represent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Important: deviceTRUST offers of granular control of the geolocation's details. It is your choice to simply evcaluate the country, or to be more granular by adding state, city or full address.

Operating System Location Provider

Operating system location providers are functions inside the user's device's operating system. deviceTRUST can retrieve the information, the providers offer and use them for context evaluation.

On Microsoft Windows, the operating system location provider is capable, with the consent of the user, of determining the position (coordinates) of a device, in addition to the source and accuracy. deviceTRUST enhances this position with country information.

A third-party location provider can be used with this data to determine more granular information, such as an address.

On Apple macOS and iOS, the operating system location provider is capable, with the consent of the user, of determining the position (coordinates) of a device, in addition to the source, accuracy, and address including country.

Third-Party Location Provider

Third-party location providers offer additional services for geolocation evaluation. In cases where operating system location services are either not available, disabled, or do not provide information on a detailed level, third-party providers can be utilized to evaluate or refine the location information.

When the deviceTRUST policy is configured with a third-party location provider, such as Google Geolocation, the Wi-Fi access points local to the device are sent to configured services and a position is returned. deviceTRUST enhances this position with country information.

A geocoding service can also be defined within the deviceTRUST Policy which is capable of determining an address and country from any location provider's position.

Important: Third-party location providers are not integrated with deviceTRUST. They are additional services that most often require a subscription. deviceTRUST, as with os location services, gathers the information from those third parties and uses the information for context evaluation.

WHOIS Location Provider

WHOIS is the process of determining a location, such as the Country of a device based on its public IP address. deviceTRUST comes with built-in functions to use WHOIS from users' devices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Determining the location via WHOIS requires the user's device to be connected to the internet. Using a public API, deviceTRUST first evaluates the device's public IP address. This IP address is then looked up in an online database to get the device's country information.

Important: Due to its design, WHOIS can be tricked by using VPN connections. If a user starts a VPN connection from country A to country B, basic WHOIS evaluation will always evaluate the device to be in country B, as the public IP now is where the VPN tunnel ends.

deviceTRUST's VPN recognition and network adapter prioritization features tackle this challenge and make sure that the WHOIS information is correct and give you better insight.

Cellular Location Provider

A Cellular Location Provider refers to a technology or service that determines the geographical location of a mobile device based on its connection to cellular networks. Mobile devices, such as smartphones and tablets, constantly communicate with nearby cell towers as part of their normal operation. The process of determining the location of a device using cellular networks is known as cell site triangulation or cell tower triangulation.

If your user's devices are equipped with cellular cards, deviceTRUST can read the information those cards provide and use it for Context evaluation.

GPS Location Providers

Devices might come with internal GPS location devices. While these provide very exact information outside, they are not optimal for in-building usage. If you need GPS information for your use case, deviceTRUST will be able to retrieve the information from GPS location providers as well.

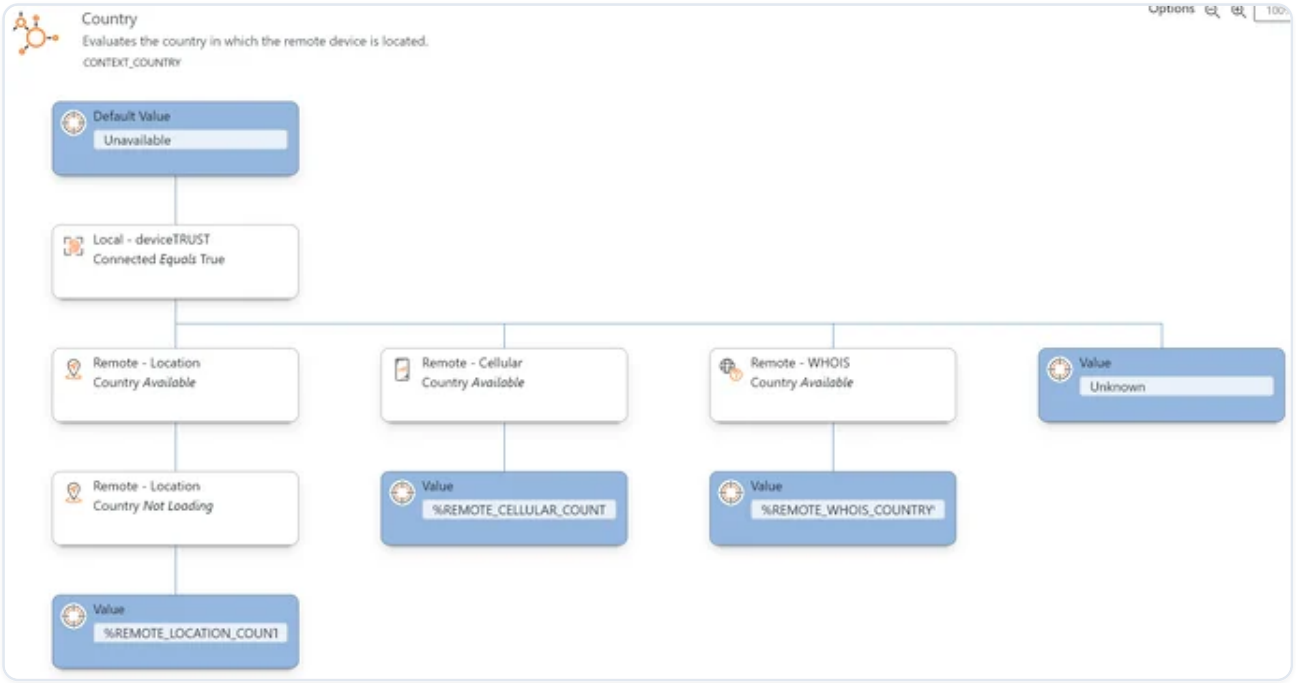
deviceTRUST Policy

deviceTRUST's policy framework allows for full control of the information you evaluate, how you prioritize it, and how you use it for access control.

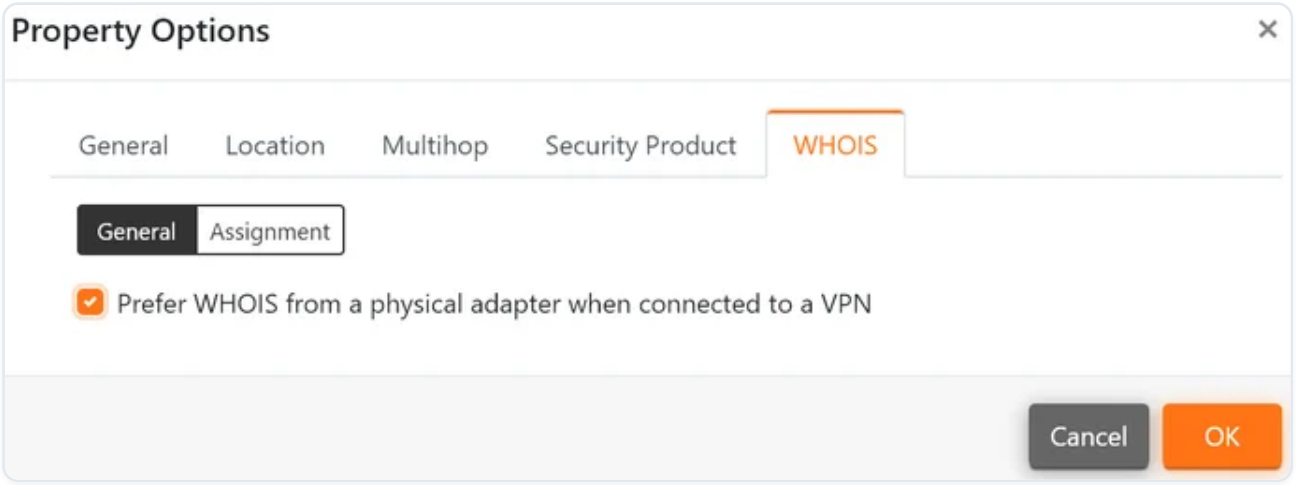
This example configuration is designed to

- Retrieve information from remote devices
- Evaluate country information only
- By ordering them from left to right prioritizes OS location services over cellular information over WHOIS
- Reports back the country code of the user's device

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In addition, the option to prioritize WHOIS information from physical adapters is set to get more valid information in case WHOIS is used.



This configuration will allow for reliable evaluation of a remote device's country. By defining the OS location services as the primary source of information and adding cellular as well as VPN-safe WHOIS information, country evaluation will be as exact as the underlying technology allows.

Location and Network improvements in Windows 11 24H2

In 24H2 new controls were added to help manage which apps have access to the list of Wi-Fi networks around you, which could be used to determine your location.

The location options can be accessed in Settings > Privacy & security > Location > 'Let desktop apps access your location'

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this setting is disabled deviceTRUST® is unable to access device location and Wi-Fi Security information.

This will result in the location and Wi-Fi Security properties not being populated with the correct data. If these properties are referenced within your config then please enable this feature for the deviceTRUST Client Extension,

- REMOTE_LOCATION_ACCURACY=Unavailable
- REMOTE_LOCATION_BUILDING=Unavailable
- REMOTE_LOCATION_COUNTRY=Unavailable
- REMOTE_LOCATION_COUNTY=Unavailable
- REMOTE_LOCATION_POSITION=Unavailable
- REMOTE_LOCATION_POSTCODE=Unavailable
- REMOTE_LOCATION_PROVIDER=Unavailable
- REMOTE_LOCATION_SOURCE=Unavailable
- REMOTE_LOCATION_STATE=Unavailable
- REMOTE_LOCATION_STREET=Unavailable
- REMOTE_LOCATION_TOWN=Unavailable
- REMOTE_LOCATION_URL=Unavailable
- REMOTE_NETWORK_X_WIFI_BSSID=
- REMOTE_NETWORK_X_WIFI_SECURITY=Unknown
- REMOTE_NETWORK_X_WIFI_SSID=
- REMOTE_NETWORK_X_WIFI_STRENGTH=0

More information regarding the changes in Windows 11 24H2 can be found here.

SD Card detection for Logical Disk properties

The detection of SD cards on Microsoft Windows and Linux operating systems remains unreliable and is highly dependent upon the hardware used and the driver stack.

When using an SD card, the Logical Disk Type, Serial Number, Vendor and Product ID may be incorrect.

We recommend detecting specific SD cards with the 'Volume ID' property that was implemented in version 23.1.120.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The 'Volume ID' number is regenerated when the SD card is formatted.

Updating the deviceTRUST Client Extension in IGEL OS 11

It may be necessary to update the deviceTRUST Client Extension version built into IGEL OS 11. This article demonstrates how this can be achieved using the UMS server.

Applies to: IGEL OS 11.08.200 and earlier

Azure Virtual Desktop

In IGEL OS 11.08.110 and earlier Azure Virtual Desktop connections are incompatible with RDP. In its default configuration Remote Desktop connections will work, Azure Virtual Desktop will fail to connect to a remote session with deviceTRUST enabled.

To resolve this the deviceTRUST Client Extension requires updating on the remote IGEL device.

In the UMS Console add a New File

- [ ] Browse and select the libdtclient_avd_legacy.so file supplied by deviceTRUST Support

With the file selected configure the options below:

- Device file location /services/avd/lib/libdeviceTRUST-client.so
- Access Rights for 'Others' to Read & Execute
- Set Owner as root

- [ ] Click OK

Now that the file has been added to the UMS Server, select the file and drag it to the folder that contains the IGEL devices you wish to update. This will assign the file to the remote endpoint.

- [ ] The File Copy setting will be persisted for your IGEL devices and the updated deviceTRUST Client Extension will be copied to the relevant directory.

- [ ] Azure Virtual Desktop should now successfully connect to remote sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The deviceTRUST Client Extension is enabled for Azure Virtual Desktop via the IGEL OS registry in the following location:

System > Registry sessions > wvd0 > plugins >deviceTRUST

NOTE:

With the above configuration set Remote Desktop connections will no longer work. Should you require RDP then remove the settings above.

VMware Horizon View

In IGEL OS 11.08.200 and earlier the deviceTRUST Client Extension is not natively integrated with VMware Horizon View. The IGEL OS requires updating for VMware Horizon View connections to function with deviceTRUST.

As above add a New File to the UMS Server.

Browse and select the libdtclient_rdp_pcoip.so file supplied by deviceTRUST Support.

With the file selected configure the options below:

- Device file location /usr/lib/vmware/rdpvcbridge/libdeviceTRUST-client.so
- Access Rights for 'Others' to Read & Execute
- Set Owner as root

Assign the file to the folder containing the IGEL devices you wish to update to deploy the Client Extension to the IGEL devices.

With the Client Extension applied for Horizon View deviceTRUST will be loaded and REMOTE deviceTRUST properties will be present in the user session.

NOTE:

Native IGEL OS integration for VMware Horizon View is coming soon. Please refer to our Supported Technologies page for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log data to Microsoft Teams

deviceTRUST can be used to send log data to a variety of services. Learn how Microsoft Teams can be used here!

deviceTRUST can use context information for a variety of purposes. In addition to reacting to certain information with matching controls, you might want to send data to some endpoint to have persistent logging or trigger ticket creation, for example. This article describes the integration of deviceTRUST with Microsoft Teams. You might want to use this approach for supporting your help desk with the required information

1. Teams channel selection: Chose to add a channel to Teams for this purpose or use an existing one. Make sure to have the information ready for step 2!
2. Setup a "web hook" in MS Teams: Data is being sent to MS Teams via REST technology. On the Teams side, a so called "Incoming Webhook" needs to be implemented for receiving the data. Please follow this Microsoft Technet article: Create an Incoming Webhook - Teams | Microsoft Docs.
3. Add the logging task to your deviceTRUST configuration: You'll find a "web request" task in the deviceTRUST console's action pane.



Select this type of task and fill information as required:

- URL: Your MS Teams Webhook's URL (from step 2)
- Headers: ContentType: application/json
- JSON body (example):

```
{"@type"      : "MessageCard",

    "@context"  : "http://schema.org/extensions",

    "summary"   : "Security State %LOCAL_NAME%:%LOCAL_USER_NAME%",

    "themeColor" : "0078D7",

    "title"      : "Security State changed on %LOCAL_NAME%:
%LOCAL_USER_NAME%",

    "text"       : "Security State:%CONTEXT_SECURITY_STATE%"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

NOTE

This configuration uses the variable %LOCAL_NAME%, %LOCAL_USER_NAME% and %CONTEXT_SECURITY_STATE%, which are to be seen exemplarily. Edit as required.

This is how a fully configured web request task could look like.

1. Check Teams for data being received and displayed: Configuring the web request task as shown above will send information to MS Teams looking like this:

You can, of course, always change the content, add information and personalize the data as required.

Policy Loading

deviceTRUST® policy can be distributed either as part of a Group Policy Object (GPO) or as a File-Based Policy. The deviceTRUST Agent merges the policies first from the GPOs and then from the File-Based Policies.

Active Directory GPOs

Policies written to either GPOs or Local Policy are merged into a single policy by the OS and loaded by the deviceTRUST Agent before any File-Based Policies.

The following merge order is used to process each GPO. This behavior is built into the OS and cannot be modified by deviceTRUST:

- The Local Policy
- GPOs linked to the site.
- GPOs linked to the domain.
- GPOs linked to organizational units (OUs) are applied. For nested OUs, GPOs linked to parent OUs are applied before GPOs linked to child OUs.

The Merging Policy Items rules are followed when merging Contexts, Actions, Messages and Settings across multiple policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File-Based Policies

File-Based Policy files are loaded from `%ProgramData%\deviceTRUST\Policy` after loading any GPOs. By default the deviceTRUST Agent will load all policy files it finds in this location. This behavior can be overridden and changed within the File-Based Policy Settings to either only load policies imported by `dtcmd IMPORT`, or to never load policies from disk (which must be defined within a GPO).

The folder containing the File-Based Policy files is secured by the agent with read access to Local Users, and full access to Local Administrators.

When File-Based Policy is enabled, files are loaded in alphabetical order. This ensures that when policy files are named beginning with a timestamp, the newest policy files take precendent over the older policy files. As an example, the file names listed below would be loaded in the following order:

- 2023-12-12_DenyAccessNonCompliantDevices.dtpol
- 2023-12-10_DenyAccessUnauthorizedUSB.dtpol
- 2023-11-01_MappedDriveSettings.dtpol

The Merging Policy Items rules are followed when merging Contexts, Actions, Messages and Settings across multiple policies.

Merging Policy Items

When Contexts, Actions, Messages and Settings are merged from multiple policies, either from Active Directory GPOs, Local Policy or File-Based Policies, the following rules apply:

- Where a *Context* with the same name has already been included, subsequent contexts with this name are ignored.
- Where an *Action* with the same name has already been included, subsequent actions with this name are ignored.
- Where a *Message* with the same name has already been included, subsequent messages with this name are ignored.
- Where a *Setting* has already been included, subsequent settings of the same type are ignored.
- Where a *Use Case* has already been included, subsequent use cases of the same type are ignored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Product Events

deviceTRUST® delivers information about its runtime behavior to the Windows Event Log for easy integration into existing Security Information and Event Management (SIEM) and reporting solutions. This information includes detailed properties of the remote device during user logon, reconnect, and also includes all properties that are changed whilst the user session is active.

Application Channel

The APPLICATION channel refers to the system Windows Event Log under WINDOWS LOGS\APPLICATION. The following events are included:

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
1311	Event Info	Information	Event)	A custom information event was created by the Audit Event task set to Information.
1312	Event Warning	Warning	Event)	A custom information event was created by the Audit Event task set to Warning.
1313	Event Error	Error	Event)	A custom information event was created by the Audit Event task set to Error.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST/Admin Channel

The ADMIN channel can be found within the Windows Event Log under APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN, or queried programmatically using the deviceTRUST/Admin channel. The following events are included:

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
1	Service Started	Information	Service Status)	The deviceTRUST Agent Service has started.
2	Service Stopped	Information	Service Status)	The deviceTRUST Agent Service has stopped.
3	Policy Loaded	Information	Policy Loaded)	The deviceTRUST Agent Service loaded new policies.
4	Policy Load Failed	Error	Policy Load Failed)	The deviceTRUST Agent Service attempted to load new policies but an error occurred.
11	License Validated	Information	License)	The license has been read, is valid, and is not yet expired, or within the expiry threshold.
12	License Expires Soon	Warning	License)	The license is valid, but it expires within

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				the expiry threshold (30 days).
14	License Expired	Error	License)	The license is valid, but has expired. The software will no longer function.
16	License Invalid	Error	License Invalid)	The license does not exist or contains invalid data.
17	Unmanaged User Logon	Information	Unmanaged User Logon)	An unmanaged user logged on.
101	Logon	Information	Connection)	A user successfully logged onto a new session.
102	Reconnect	Information	Connection)	A user successfully reconnected to an existing session.
103	Logoff	Information	Session)	A user which previously successfully logged onto a session was logged off.
104	Disconnect	Information	Session)	A user which previously successfully logged onto a session was

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				disconnected from that session.
105	Property Changed	Information	Property Changed)	One or more local or remote properties were added, removed or changed.
106	Context Changed	Information	Context Changed)	One or more context values changed.
111	Untrusted Device Blocked	Warning	Untrusted Device Blocked)	A user attempted to logon or reconnect to an existing session, but the deviceTRUST Client Extension failed to provide properties of the remote connected device, and the policy determines that this information is required.
112	Trusted Device Blocked	Warning	Trusted Device)	A trusted device, i.e. a device with the deviceTRUST Client Extension installed, was

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				blocked from access due to not meeting version or encryption minimum requirements.
113	Trusted Device Auto Update Succeeded	Information	Trusted Device Auto Update)	A trusted device was successfully auto-updated.
114	Trusted Device Auto Update Failed	Error	Trusted Device Auto Update Failed)	A trusted device failed to auto-update.
201	Custom Process Executed	Information	Custom Process)	A custom process was executed.
202	Custom Process Succeeded	Information	Custom Process Complete)	A custom process finished executing and the process did not report an error.
203	Custom Process Failed	Error	Custom Process Failed)	A custom process finished executing, but the process either timed out or reported an error.
301	Access Allowed	Information	Access Allowed)	Access to the shell was allowed after a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				Deny Access task was reverted.
302	Access Denied	Warning	User Message)	Access to the shell was denied by a Deny Access task.
303	Access Failed	Error	Access Failed)	A request to change access to the shell failed.
304	Logon Aborted	Warning	Logon Aborted)	The logon process was aborted.
311	Event Info	Information	Event)	A custom information event was created by the Audit Event task set to Information.
312	Event Warning	Warning	Event)	A custom information event was created by the Audit Event task set to Warning.
313	Event Error	Error	Event)	A custom information event was created by the Audit Event

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				task set to Error.
321	AppLocker Rule	Information	AppLocker Rule)	The Microsoft AppLocker task generated a new rule.
322	AppLocker Rule Failed	Error	AppLocker Rule Failed)	The Microsoft AppLocker task failed to generate a new rule.
323	AppLocker Policy	Information	AppLocker Policy)	The Microsoft AppLocker Policy was generated following a change to the Microsoft AppLocker Policy Settings or a call to dtcmd APPLOCKER.
324	AppLocker Policy Failed	Error	AppLocker Policy)	An attempt to generate the Microsoft AppLocker Policy resulted in one or more errors.
325	AppLocker PowerShell Allowed	Information	AppLocker PowerShell)	A PowerShell Script or Cmdlet was allowed to execute.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
326	AppLocker PowerShell Prevented	Error	AppLocker PowerShell)	A PowerShell Script or Cmdlet was prevented from executing.
331	Application Terminated	Information	Application Terminated)	An application was terminated because a user failed to close an application discovered by the Terminate App task.
332	Application Shutdown	Information	Application Shutdown)	A user was asked to shutdown an application discovered by the Terminate App task.
341	Popup Shown	Information	Popup Shown)	A popup message was shown to the user.
342	Popup Failed	Error	Popup Failed)	An attempt to display a popup message to the user failed.
351	Registry Updated	Information	Registry Updated)	The registry was updated.
352	Registry Warning	Warning	Registry Warning)	A warning was generated while updating the registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
353	Registry Failed	Error	Registry Failed)	An attempt to update the registry failed.
361	Printer Mapped	Information	Printer Operation)	Printers were successfully mapped.
362	Printer Map Failed	Error	Printer Operation Failed)	An attempt to map printers failed.
363	Printer Unmapped	Information	Printer Operation)	Printers were successfully unmapped.
364	Printer Unmap Failed	Error	Printer Operation Failed)	An attempt to unmap printers failed.
365	Printer Set Default	Information	Printer Operation)	A printer was set as default.
366	Printer Set Default Failed	Error	Printer Operation Failed)	An attempt to set a default printer failed.
367	Printer Map Warning	Warning	Printer Operation Failed)	A warning was generated when attempting to map a printer.
368	Printer Set Default Warning	Warning	Printer Operation Failed)	A warning was generated when attempting to set a default printer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
371	App Masking Update	Information	App Masking Update)	A Microsoft FSLogix App Masking update was successfully applied.
372	App Masking Update Failed	Error	App Masking Update Failed)	A Microsoft FSLogix App Masking update failed.
381	Send Mail Succeeded	Information	Send Mail Succeeded)	A send mail task succeeded.
382	Send Mail Failed	Error	Send Mail Failed)	A send mail task failed.
391	Web Request Succeeded	Information	Web Request Succeeded)	A web request task succeeded.
392	Web Request Failed	Error	Web Request Failed)	A web request task failed.
401	Windows Firewall Succeeded	Information	Windows Firewall)	The Windows Firewall task succeeded to create a rule.
402	Windows Firewall Failed	Error	Windows Firewall Failed)	The Windows Firewall task failed to create a rule.
411	Drive Map	Information	Drive Operation)	A network drive was mapped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
412	Drive Map Warning	Warning	Drive Operation Failed)	A network drive failed to map, but the failover drive was successfully mapped.
413	Drive Map Failed	Error	Drive Operation Failed)	A network drives and any failover drives failed to map.
414	Drive Unmap	Information	Drive Operation)	A network drive was unmapped.
415	Drive Unmap Failed	Error	Drive Operation Failed)	A network drive failed to unmap.
421	Shortcut Creation Succeeded	Information	Shortcut Operation)	A shortcut was successfully created.
422	Shortcut Creation Failed	Error	Shortcut Operation Failed)	A shortcut failed to be created.
423	Shortcut Deletion Succeeded	Information	Shortcut Operation)	A shortcut was successfully deleted.
424	Shortcut Deletion Failed	Error	Shortcut Operation Failed)	A shortcut failed to be deleted.
441	Microsoft Entra ID Update	Information	Microsoft Entra ID Update)	Successfully updated current device within Microsoft Entra ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
442	Microsoft Entra ID Update Failed	Error	Microsoft Entra ID Update Failed)	Failed to update current device within Microsoft Entra ID.

The above events report the following event data:

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Service Status	Name (1)	TEXT	The name of the service, e.g. deviceTRUST Agent Service.
License	CustomerId (1)	GUID	An identifier that uniquely identifies the customer.
	LicenseId (2)	GUID	An identifier that uniquely identifies the license.
	IssueDate (3)	SYSTEMTIME	The date that the license was issued.
	ExpiryDate (4)	SYSTEMTIME	The date that the license expires.
	Type (5)	TEXT	The type of license, e.g. Subscription.
	Quantity (6)	INT	The quantity of units that can consume a license.
	Unit (7)	TEXT	The unit of license, e.g. User.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Days (8)	INT	The number of days remaining on the license.
License Invalid	Message (1)	TEXT	A description of the reason why the license is invalid.
Unmanaged User Logon	LogonId (1)	GUID	An identifier representing the user logon.
	LogonTime (2)	SYSTEMTIME	The time that the user logged onto the session.
	SessionId (3)	INT	The session id that the user is connected to.
	UserName (4)	TEXT	The name of the user logged into the session.
	UserDomain (5)	TEXT	The domain of the user logged into the session.
	UserSID (6)	TEXT	The security identifier of the user logged into the session.
Policy Loaded	Name (1)	TEXT	The name of the service, e.g. deviceTRUST Agent Service.
	Policies (2)	TEXT	A list of the policies that were loaded and the timestamp that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			the policy was saved.
Policy Load Failed	Error (3)	TEXT	A description of the error that occurred.
Session	LogonId (1)	GUID	Uniquely identifies events from the same logon session. By filtering on this field, all events related to a single logon session can be determined.
	LogonTime (2)	SYSTEMTIME	The time that the user logged onto the session.
	ConnectedId (3)	GUID	Uniquely identifies events from the same connection. Unlike the LogonId, the value of this field changes every time a new connection is established to an existing session.
	ConnectedTime (4)	SYSTEMTIME	The time that the user logged on, or reconnected, to the session.
	SessionId (5)	INT	The session id that the user is connected to.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	UserName (6)	TEXT	The name of the user logged into the session.
	UserDomain (7)	TEXT	The domain of the user logged into the session.
	UserSID (8)	TEXT	The security identifier of the user logged into the session.
Connection (extends Session)	DeviceId (9)	TEXT	Uniquely identifies the remote connected device. All activity originating from the same device can be queried by filtering on this field. This field is blank for local console sessions.
	DeviceName (10)	TEXT	The name of the remote connected device. This field is blank for local console sessions.
	DeviceOS (11)	TEXT	The operating system of the remote connected device. This field is blank for local console sessions, and if the deviceTRUST Client Extension did not provide details of the operating system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Properties (12)	TEXT	A textual representation of all local and remote properties. The properties are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
	Contexts (13)	TEXT	A textual representation of all contexts. The contexts are formatted with the name and value separated by an equals symbol (=), and multiple contexts separated by a newline (\n) character. E.g. CONTEXT1=VALUE1\nCONTEXT2=VALUE2\n
	Errors (14)	TEXT	A description of any errors that occurred whilst obtaining properties.
	Timings (15)	TEXT	Lists the five local and remote property

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			providers that took the longest to return, in milliseconds.
	Duration (16)	INT	The number of milliseconds it took for all deviceTRUST property providers to return.
Property Changed	AddedProperties (9)	TEXT	A textual representation of all properties that were added. The properties are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
	RemovedProperties (10)	TEXT	A textual representation of all properties that were removed. The properties are formatted with the name of each property, with multiple properties separated by a newline (\n) character. E.g.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			PROPERTY1 \nPROPERTY2 \n
	ChangedProperties (11)	TEXT	A textual representation of all properties that were changed. The properties are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
	PreviousProperties (12)	TEXT	A textual representation of the previous value of all properties that were changed or removed. The properties are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
Context Changed	ChangedContexts (9)	TEXT	A textual representation of all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			contexts that were changed. The contexts are formatted with the name and value separated by an equals symbol (=), and multiple contexts separated by a newline (\n) character. E.g. CONTEXT_ONE=VALUE1\nCONTEXT_TWO=VALUE2\n
	PreviousContexts (10)	TEXT	A textual representation of the previous value of all contexts that were changed or removed. The contexts are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. CONTEXT_ONE=PREVIOUSVALUE1\nCONTEXT_TWO=PREVIOUSVALUE2\n
	TriggeredBy (11)	TEXT	The name of the property that changed that ultimately caused the context to change.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Trigger (12)	TEXT	The name of the trigger that generated the context change event.
Untrusted Device Blocked	ClientName (9)	TEXT	The Operating System reported name of the connecting device.
Trusted Device	ClientName (9)	TEXT	The deviceTRUST Client Extension reported name of the connected device.
	ClientVersion (10)	TEXT	The version number of the deviceTRUST Client Extension on the remote device.
	MinimumVersion (11)	TEXT	The minimum version of the deviceTRUST Client Extension as defined by policy.
	Encrypted (12)	BOOLEAN	Set to true when application level encryption was used in addition to the encryption offered by the underlying protocol.
Trusted Device Auto Update	AutoUpdateUrls (13)	TEXT	The auto-update URLS that were used to upgrade the deviceTRUST Client Extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Trusted Device Auto Update Failed	ErrorMessage (14)	TEXT	An error message reported by the upgrade of the deviceTRUST Client Extension.
Custom Process (extends Session)	TriggerName (9)	TEXT	The name of the trigger that launched the custom process, e.g. Logon or Reconnect.
	TriggerTime (10)	TIME	The time that the custom process was executed.
	TriggeredBy (11)	TEXT	The properties that resulted in the execution of the custom process.
	ActionName (12)	TEXT	The name of the action where the Custom Process task is located.
	SequenceIndex (13)	TEXT	The zero based index of the sequence within the action where the Custom Process task is located.
	TaskName (14)	TEXT	The name of the Custom Process task.
	CommandLine (15)	TEXT	The command line that was executed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	RunAs (16)	TEXT	Either ‘USER’ or ‘SYSTEM’, depending upon the configuration of the trigger that was executed.
	Identity (17)	TEXT	The user name of the custom process.
	Pid (18)	INT	The Process ID of the custom process.
	Location (19)	TEXT	Determines whether the custom process was executed locally or remotely.
Custom Process Complete (extends Custom Process)	Duration (20)	INT	The time taken for the custom process to complete, in milliseconds.
	Output (21)	TEXT	The output messages returned by the custom process.
	Error (22)	TEXT	The error messages returned by the custom process.
Custom Process Failed (extends Custom Process)	Duration (20)	INT	The time taken for the custom process to complete, in milliseconds.
	Output (21)	TEXT	The output messages returned

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			by the custom process.
	Error (22)	TEXT	The error messages returned by the custom process.
User Message (extends Session)	Title (9)	TEXT	A message title displayed to the user.
	Message (10)	TEXT	The message displayed to the user.
	Timeout (11)	INT	The timeout period that the message is displayed to the user.
Access Allowed (extends Session)	Message (9)	TEXT	The message reported by a call to dtcmd.exe ACCESS.
Access Failed (extends Session)	Reason (9)	TEXT	The reason that a call dtcmd.exe ACCESS failed.
	Message (10)	TEXT	The message supplied to a call to dtcmd.exe ACCESS that would have been displayed to the user if the call succeeded.
	Timeout (11)	INT	The timeout period that the user would have had before being disconnected from the session, if the call to dtcmd.exe

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			ACCESS succeeded.
Logon Aborted (extends Session)	Message (9)	TEXT	The message displayed to the user detailing why the logon failed.
	Timeout (10)	INT	The timeout period that the user would have had before being logged out from the session.
Event (extends Session)	Message (9)	TEXT	A user supplied message from a call to dtcmd.exe EVENT.
	Report (10)	INT	Set to 1 when the report fields have been populated, or 0 otherwise.
	ReportTrigger (11)	TEXT	The trigger that resulted in the task being executed, such as Logon or ContextChanged.
	ReportAction (12)	TEXT	The name of the action that generated the event.
	ReportDeviceName (13)	TEXT	The name of the remote device that the user was connecting from.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	ReportDeviceOSName (14)	TEXT	The OS name of the remote device that the user was connecting from.
	ReportDeviceOSType (15)	TEXT	The OS type, such as Client or Server that the user was connecting from.
	ReportClientVersion (16)	TEXT	The version of the deviceTRUST Client Extension that was used to establish the remote device information.
	ReportContexts (17)	TEXT	The name and value of all contexts.
	ReportProperties (18)	TEXT	The name and value of all properties.
AppLocker Rule (extends Session)	Name (9)	TEXT	The name of the rule.
	Operation (10)	TEXT	The operation of the AppLocker rule, either Allow, Deny or Delete.
	Target (11)	TEXT	The target of the AppLocker rule, either Executable, Dll, Installer, Script or Package.
	Duration (12)	INT	The time taken for the AppLocker rule to become effective.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Rule (13)	TEXT	The AppLocker XML fragment that defines the rule.
AppLocker Rule Failed (extends Session)	Name (9)	TEXT	The name of the rule.
	Operation (10)	TEXT	The operation of the AppLocker rule, either Allow, Deny or Delete.
	Target (11)	TEXT	The target of the AppLocker rule, either Executable, Dll, Installer, Script or Package.
	Duration (12)	INT	The time taken for the AppLocker rule to become effective.
	Message (13)	TEXT	A message explaining why the rule failed to apply.
AppLocker Policy	Event (1)	TEXT	The event that triggered the regeneration of policy, either ‘Policy Change’ or ‘External Process’.
	Message (2)	TEXT	A description of the changes that were made.
	Duration (3)	INT	The time taken for the AppLocker Policy

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			to be generated, in milliseconds.
AppLocker PowerShell (extends Session)	ImageName (9)	TEXT	The full path of the process that attempted to run the script or cmdlet.
	Pid (10)	INT	The process identifier of the process that attempted to run the script or cmdlet.
	Type (11)	INT	Set to 0 whenever PowerShell was running a cmdlet, or 1 when running a script.
	Script (12)	TEXT	The full path to the script that attempted to execute.
Application Terminated (extends Session)	Title (9)	TEXT	The title displayed to the user following a call to dtcmd.exe APPTERMINATE.
	Message (10)	TEXT	The message displayed to the user following a call to dtcmd.exe APPTERMINATE.
	Applications (11)	TEXT	A comma separated list of all processes and their PID’s that were terminated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Application Shutdown (extends Application Terminated)	Termination Time (12)	DATE/TIME	The time that the applications will be terminated.
Popup Shown (extends Session)	Title (9)	TEXT	The popup title.
	Message (10)	TEXT	The popup message.
	Timeout (11)	INT	The timeout in seconds to display the popup.
Popup Failed (extends Session)	Reason (9)	TEXT	The reason that the popup failed to shown.
	Title (10)	TEXT	The popup title.
	Message (11)	TEXT	The popup message.
	Timeout (12)	INT	The timeout in seconds to display the popup.
Registry Updated (extends Session)	Values (9)	TEXT	The registry values.
	Persist (10)	TEXT	How to persist the registry values.
	Protect (11)	BOOLEAN	Whether the registry key is protected.
Registry Warning (extends Registry Updated)	Warnings (12)	TEXT	The warning messages generated by the update.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Registry Failed (extends Session)	Source (9)	TEXT	The source of the registry update.
	Reason (10)	TEXT	The reason the registry update failed.
Printer Operation (extends Session)	Printer (9)	TEXT	The path to the printers.
Printer Operation Failed (extends Printer Operation)	Reason (10)	TEXT	The reason that the printer operation failed.
App Masking Update (extends Session)	Path (9)	TEXT	The path to the Microsoft FSLogix App Masking Rule Assignment file.
	Operation (10)	TEXT	The type of operation.
	Entry (11)	TEXT	The entry to apply to the file.
App Masking Update Failed (extends App Masking Update)	Error (12)	TEXT	The reason that the Microsoft FSLogix App Masking update failed.
Send Mail (extends Session)	Host Name (9)	TEXT	The host name of the SMTP server.
	Recipients (10)	TEXT	A list of the recipients of the mail message.
	Subject (11)	TEXT	The subject of the mail message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Status Code (12)	INT	The status code reported by the SMTP server representing the success of the mail message.
	Duration (13)	INT	The time in milliseconds taken to send the mail message.
Send Mail Succeeded (extends Send Mail)	Message Id (14)	TEXT	Uniquely identifies the sent mail message.
Send Mail Failed (extends Send Mail)	Error (14)	TEXT	An error message representing the problem that occurred.
	Response (15)	TEXT	The response from the SMTP server.
Web Request Succeeded (extends Session)	Method (9)	TEXT	The method used in the web request.
	URL (10)	TEXT	The URL that the web request was sent.
	Status Code (11)	INT	The status code reported by the web server.
	Duration (12)	INT	The time in milliseconds taken to perform the web request.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Request Id (13)	INT	Uniquely identifies the web request.
Web Request Failed (extends Web Request Succeeded)	Error (14)	TEXT	An error message representing the problem that occurred.
	Response (15)	TEXT	The response from the web server.
Windows Firewall (extends Session)	Action (9)	TEXT	Whether the firewall rule was an Allow or a Deny.
	RuleName (10)	TEXT	The name of the rule created.
Windows Firewall Failed (extends Windows Firewall)	Error (11)	TEXT	A description of the error that occurred.
Drive Operation (extends Session)	Drive (9)	TEXT	The drive that was mapped or unmapped.
Drive Operation Failed (extends Drive Operation)	Error (10)	TEXT	A description of the error that occurred.
Shortcut Operation (extends Session)	Shortcut Name (9)	TEXT	The name of the shortcut.
	Shortcut Directories (10)	TEXT	A list of directories that the shortcut should be created.
	Target Path (11)	TEXT	The path where the target file exists.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Target Args (12)	TEXT	Any arguments to supply to the shortcut target.
Shortcut Operation Failed (extends Shortcut Operation)	Error (13)	TEXT	A description of the error that occurred.
Microsoft Entra ID Update (extends Session)	DeviceId (9)	TEXT	The identifier of the device within Microsoft Entra ID.
	Update (10)	TEXT	A description of the update that occurred.
	Duration (11)	INT	The time in milliseconds taken to perform the update.
Microsoft Entra ID Update Failed (extends Microsoft Entra ID Update)	Error (12)	TEXT	A description of the error that occurred.

deviceTRUST/Usage Channel

The USAGE channel can be found within the Windows Event Log under APPLICATION AND SERVICE LOGS\DEVICETRUST\USAGE, or queried programmatically using the deviceTRUST/Usage channel. The following event is included.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
21	Usage	Information	Usage)	Raised when a license unit, e.g. a User, logs into the local device for the first time within a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				calendar month.

The above event reports the following event data:

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Usage	TrackingId (1)	TEXT	Uniquely identifies the license unit, e.g. the User, that logged in. For a user, this is a Base64 encoded SHA256 hash of the user's security identifier.
	TrackingName (2)	TEXT	The name of the license unit that logged in, e.g. the user name.
	TrackingUnit (3)	TEXT	The unit of license, e.g. User.

iOS Managed App Configuration

The following fields define the *Managed App Configuration* that can be deployed by an MDM provider to control the behavior of the deviceTRUST® iOS Client Extension.

NAME	TYPE	DESCRIPTION	EXAMPLE
deviceName	string	Provides the user assigned device name.	`$DEVICE_NAME$`
deviceSerialNumber	string	Provides the serial number of the device. This is used	`$DEVICE_SN$`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	TYPE	DESCRIPTION	EXAMPLE
		to populate the REMOTE_HARDWARE_BIOS_SERIAL property.	
userName	string	Defines the user name that the device is assigned to.	
userDomain	string	Defines the user domain name of the user that the device is assigned to.	
userPrincipleName	string	Defines the user principle name (UPN) of the user that the device is assigned to.	
permitAddRegistration	boolean	Determines whether the *Add Registration* menu item is available once the device has been registered.	`false`
permitRemoveRegistration	boolean	Determines whether the *Remove Registration* menu item is available once the device has been registered.	`false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	TYPE	DESCRIPTION	EXAMPLE
registrationKey	string	Defines the App Registration's key. When defines, the iOS Client Extension will automatically register instead of using the device camera to scan a QR code.	
customProperty0..15	string	Defines up to 16 custom properties available to the MDM provider. Custom properties must be prefixed with *REMOTE_CUSTOM_* followed by a name and value separated by an equals symbol.	`REMOTE_CUSTOM_PHONE_NUMBER=$PHONE_NUMBER$`

The **userName** and **userDomain** fields, or alternatively the **userPrincipleName** field, can be used to optionally identify the user that the iOS device belongs to. This can be used to generate a notification simplifying the entry of the passcode.

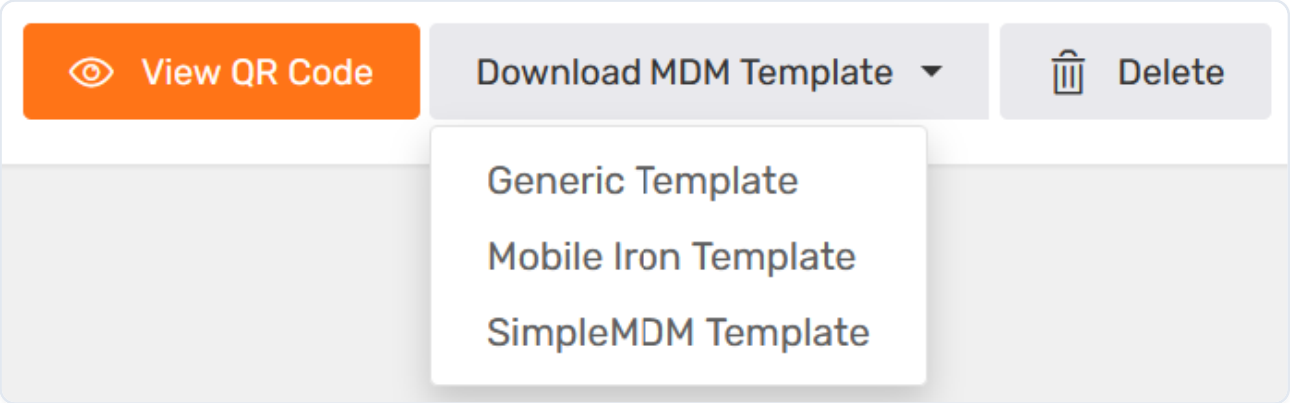
NOTE:

Each MDM provider includes its own format to push MDM attributes into the managed app configuration. The examples above are represented as an attribute name separated by `$` symbols. Check your MDM provider documentation for more information.

deviceTRUST Portal MDM Templates

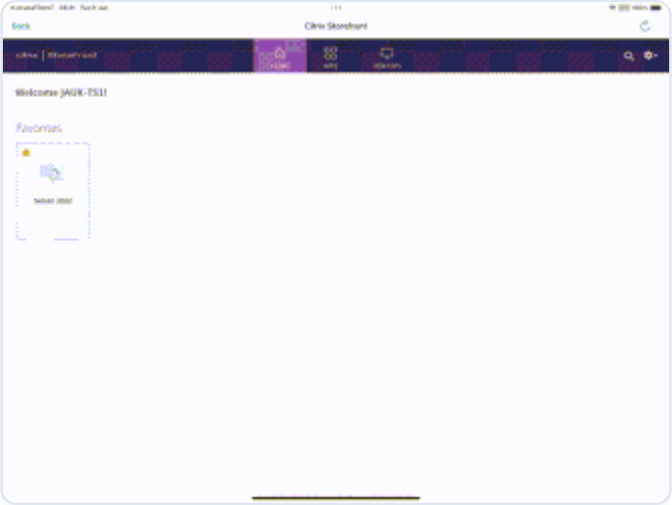
An MDM Template *plist* file can be downloaded from the deviceTRUST Portal within the *App Registration* section. This file contains all of the fields above, and can be edited with values suitable for your environment before uploading to your MDM provider.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



iOS Passcodes

iOS passcodes provide a mechanism to link a virtual session to a registered iOS device. A passcode is shown within the virtual session during the initial remote connection. That passcode must then be entered within the deviceTRUST® Client Extension for iOS for the connection to be established. Passcodes are unique to your organisation.



Passcode complexity and expiry

The passcode complexity and expiry can be changed within Mobile Settings. The passcode complexity controls the number of digits within a passcode, and can be set to 3, 4, 5 or 6 digits. Smaller organisations may choose a smaller passcode complexity so that they are easier to remember. Larger organisations should choose a larger passcode complexity.

Passcodes remain valid for the passcode expiry time which can be from 30 seconds to 3 minutes. Shorter passcode expiry times gives the user less time to enter the passcode. Longer passcode expiry times give the user more time to enter the passcode. Once a connection has been established with the iOS device, or the passcode expires, then the passcode is removed from the system and may be reused for other connections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Simplifying passcode entry with notifications

Organisations that issue a single iOS device to each user may associate each device with that user within the deviceTRUST Portal . Each device has the following fields that enable this:

- *userName* - The name of the user within Active Directory.
- *userDomain* - The name of the user domain within Active Directory.
- *userPrincipleName* - The user principle name of the user within Active Directory.

When a user logs in from an iOS device, a check is performed to determine if that user has a single device associated with them. The check is performed against the user name and domain, or the user principle name. If a single device is found, then a notification containing the passcode is sent to the device. If the user clicks on that notification, the passcode is automatically entered.

The user fields above can be automatically updated within the deviceTRUST Portal by deploying an MDM Managed App Configuration to the iOS devices.

Redirecting back to the remoting client

Once the user passcode has been entered, the deviceTRUST Client Extension for iOS can optionally redirect back to the remoting client. Within the Mobile Settings is a *Success Link* field which is opened whenever the properties of the iOS device have successfully been sent to the deviceTRUST Agent. The Success Link control contains predefined values for Citrix Workspace, Microsoft Remote Desktop and VMware Horizon Client.

Actions

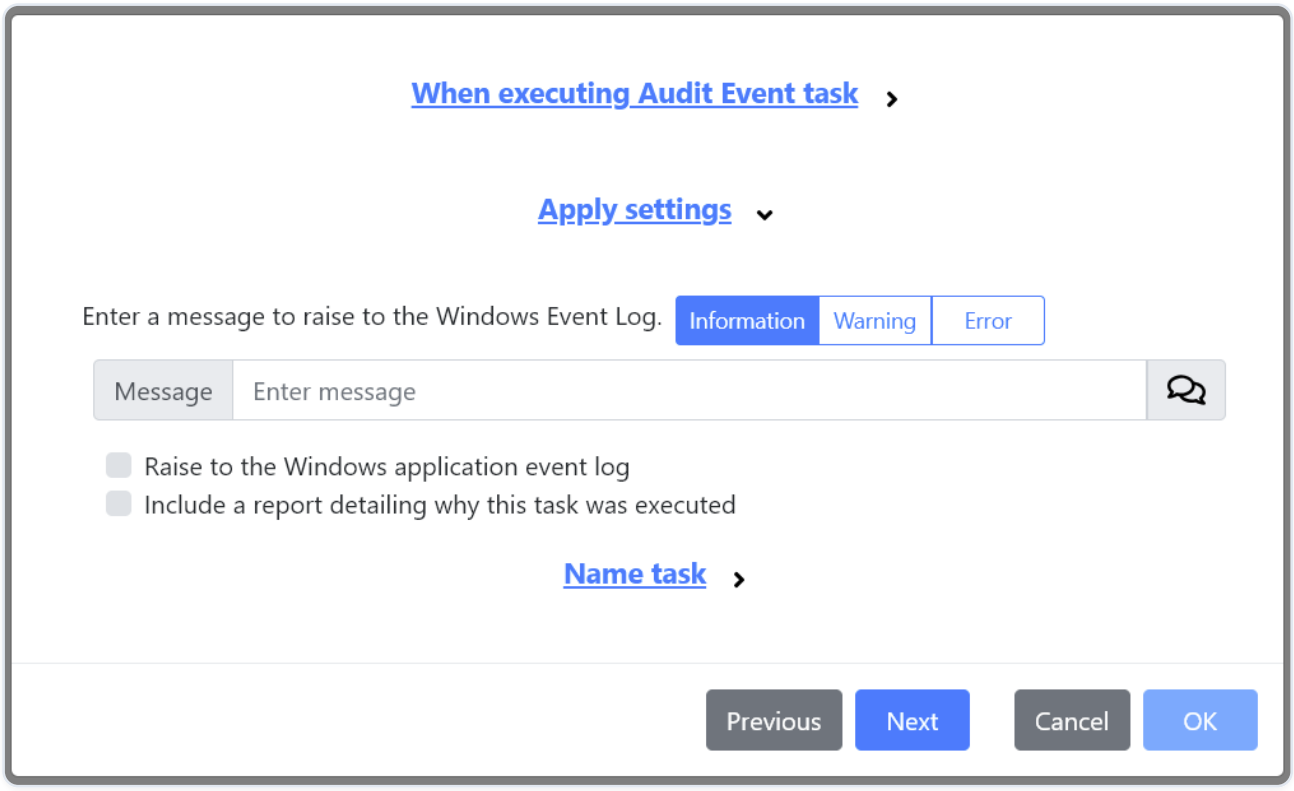
TABLE OF CONTENTS

- Tasks - Task Reference

Audit Event Task

The `Audit Event` task raises an Information, Warning or Error event to the Windows Event Log.

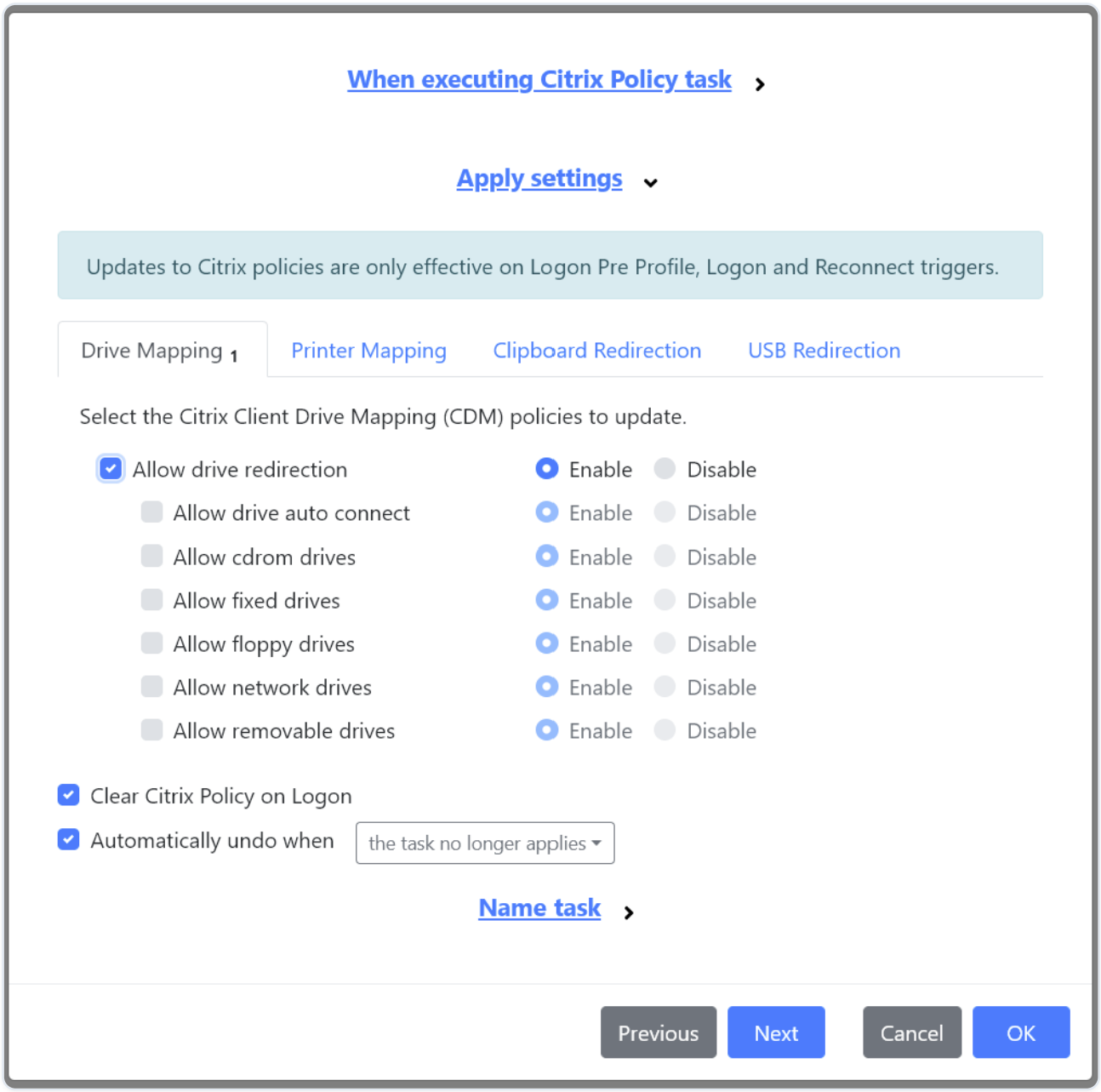
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Policy Task

The `Citrix Policy` task updates Citrix policies which control the sharing of data with the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



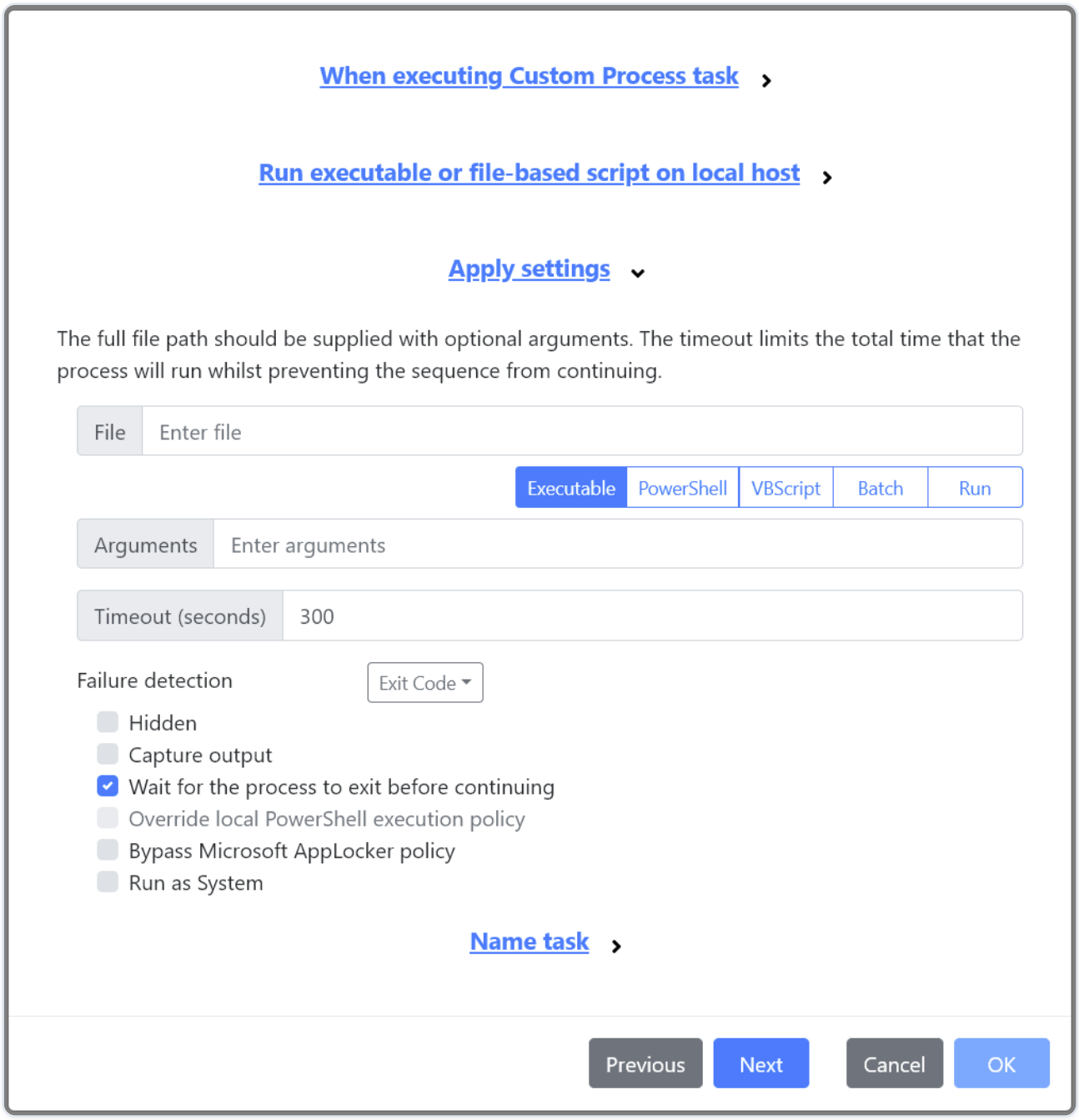
The following controls are available:

- *Clear Policy on Logon* - When enabled, the Citrix policy at `HKLM\Software\Policies\Citrix\<SESSIONID>` is deleted during early logon. This policy will be rebuilt by Citrix later in the logon process.

Custom Process Task

The `Custom Process` task runs an executable or script on the local or remote device.

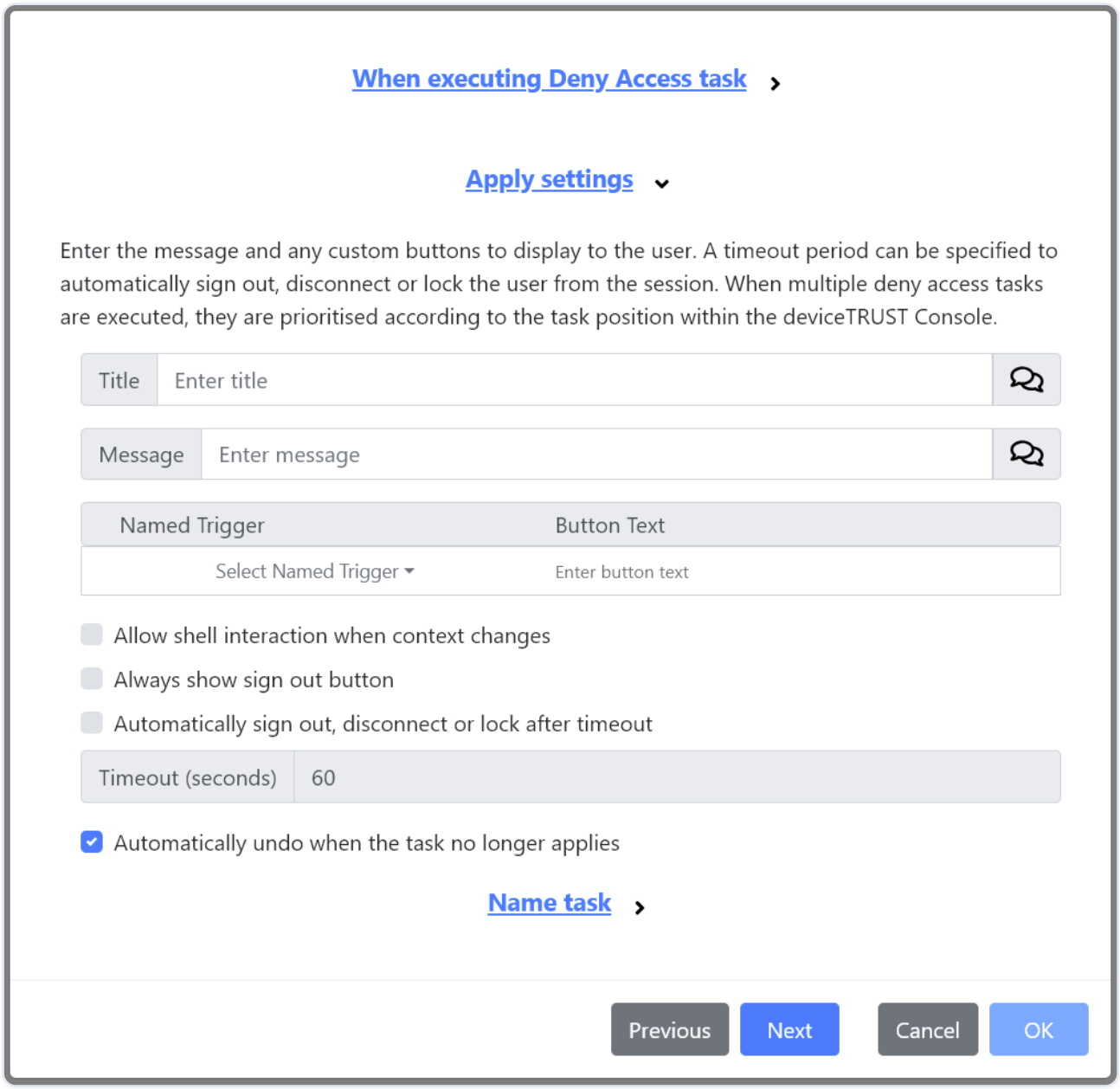
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deny Access Task

The `Deny Access` task controls access to the shell, optionally signing out, disconnecting or locking the user after the specified timeout period.

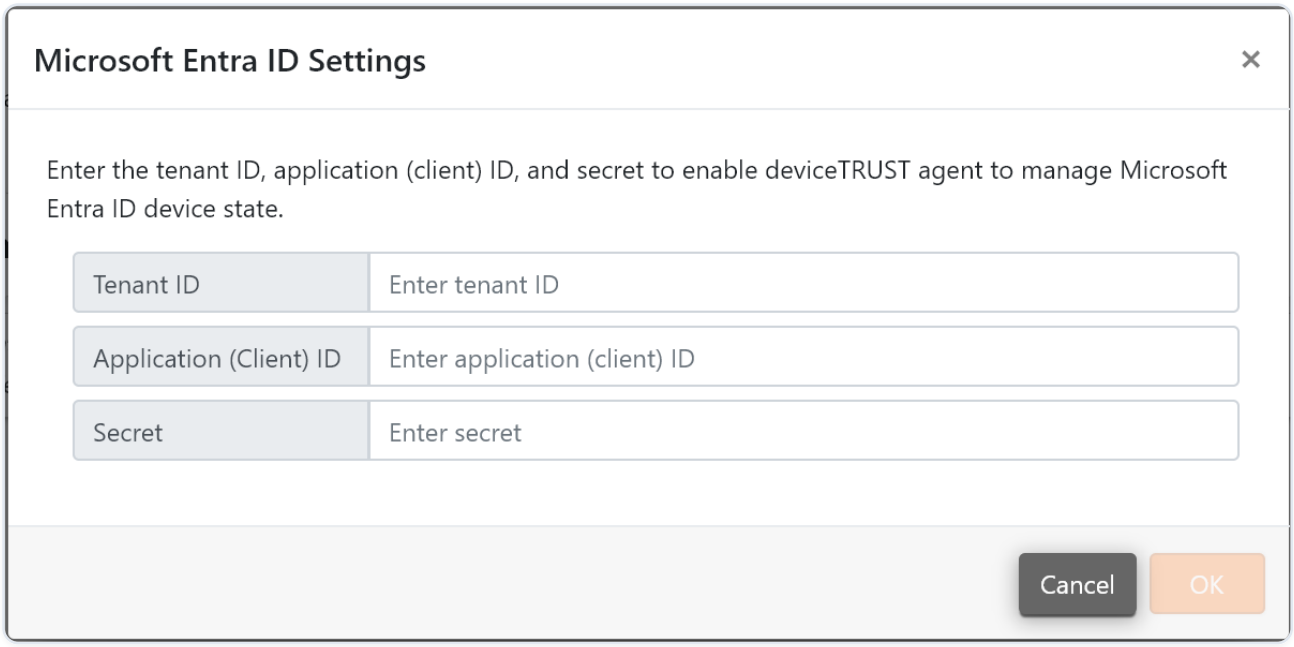
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Entra ID Task

The `Microsoft Entra ID` task updates domain joined device compliance or extension attribute value within Microsoft Entra ID.

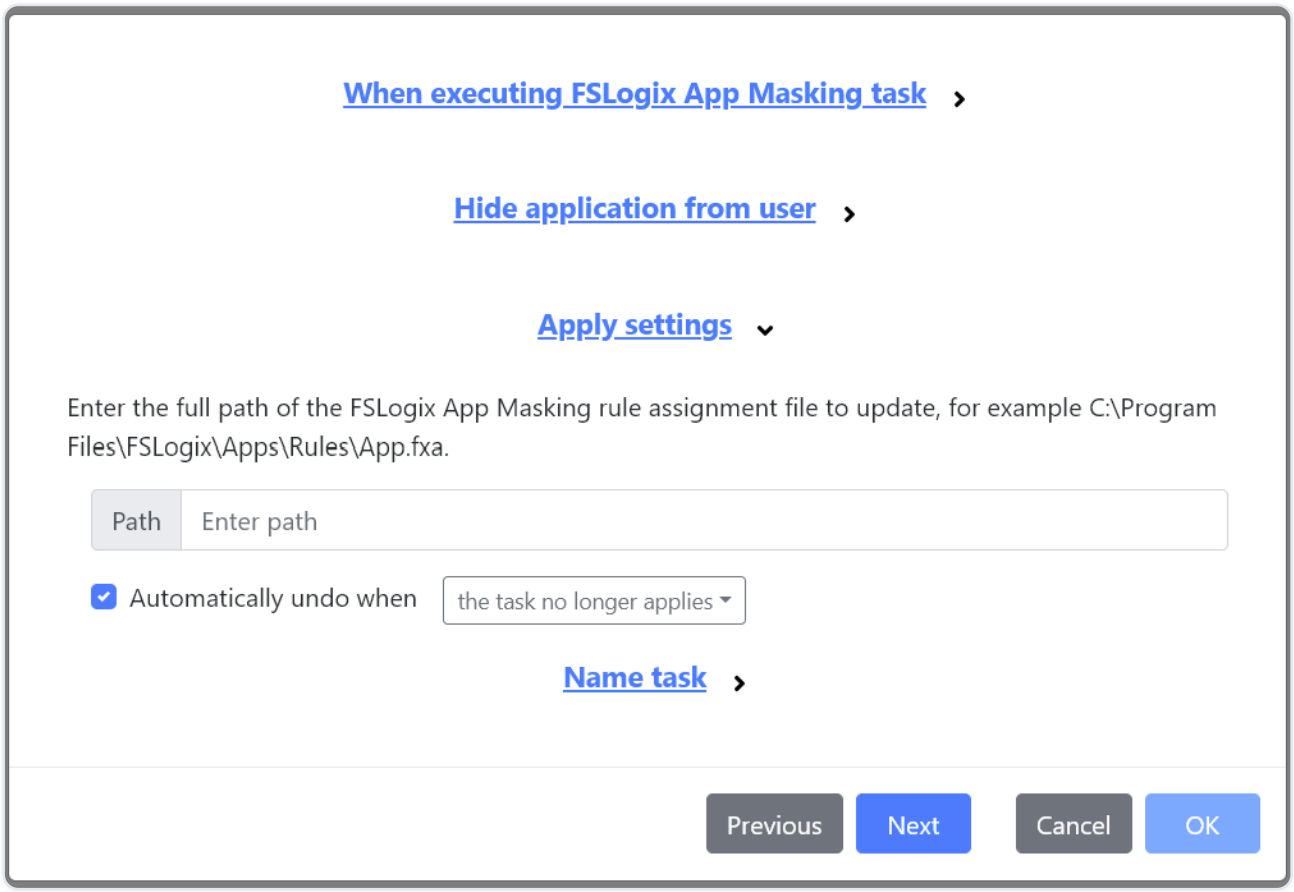
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Entra ID Settings must be configured with Device.ReadWrite.All permissions to Microsoft Graph.

FSLogix App Masking Task

The `FSLogix App Masking` task manages the user assignments of a FSLogix App Masking Rule Set, controlling the availability of an application within the user session.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Task Reference

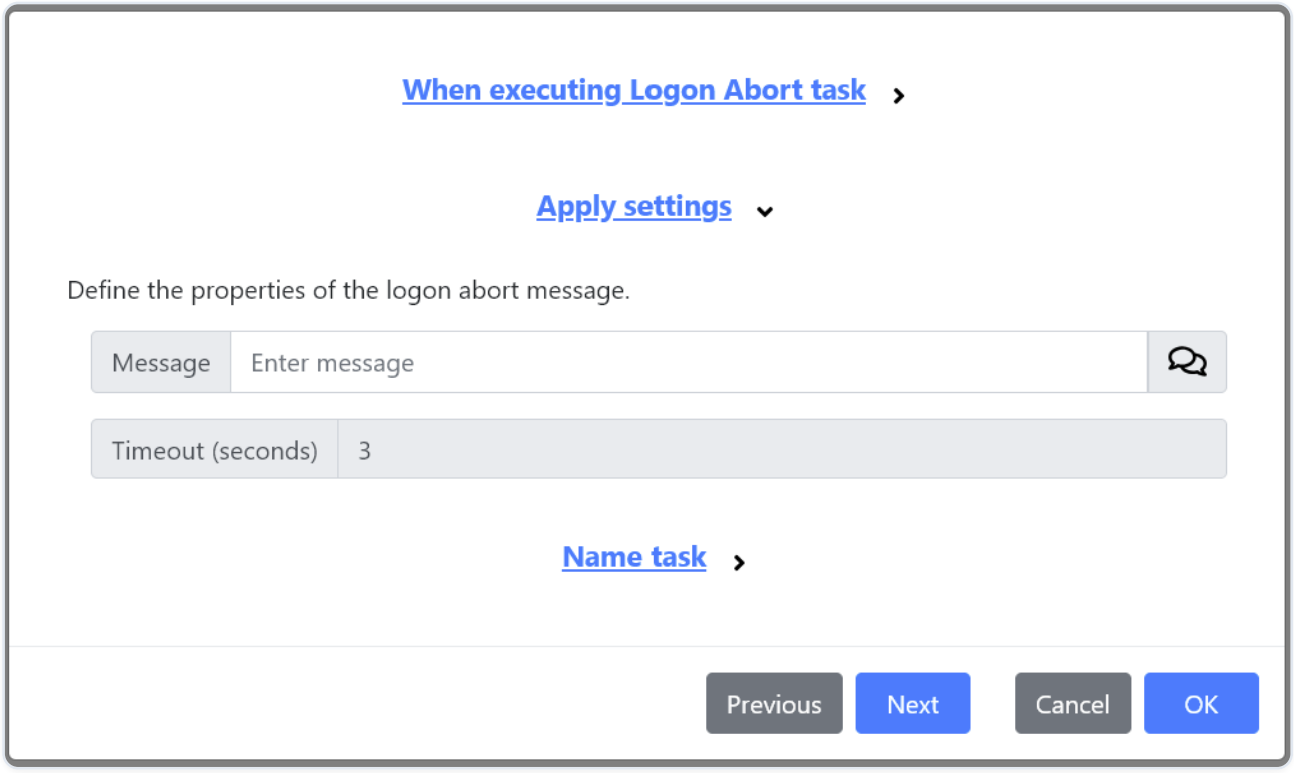
TABLE OF CONTENTS

- Audit Event - Raises an Information, Warning or Error event to the Windows Event Log.
- Citrix Policy - Updates Citrix policies which control the sharing of data with the remote device.
- Custom Process - Runs an executable or script on the local or remote device.
- Deny Access - Controls access to the shell, optionally signing out, disconnecting or locking the user after the specified timeout period.
- FSLogix App Masking - Manages the user assignments of a FSLogix App Masking Rule Set, controlling the availability of an application within the user session.
- Logon Abort - Aborts the logon process, preventing the creation of the user session.
- Map Drive - Maps and unmaps network drives within the user session.
- Map Printer - Maps and unmaps network printers within the user session, and sets the default printer.
- Microsoft AppLocker - Creates, updates and deletes Microsoft AppLocker rules for the logged in user.
- Microsoft Entra ID - Updates domain joined device compliance or extension attribute value within Microsoft Entra ID.
- Popup Message - Displays a popup message to the user, either in a top level popup window, or using an Action Center notification when available.
- Screen Saver - Updates the screen saver settings within the session.
- Send Mail - Sends an email with the defined content.
- Shortcut - Creates a shortcut within the user session.
- Terminate App - Terminates applications that should not be running within the user session.
- User Session - Locks, Disconnects, or Signs out the user session.
- Web Request - Invokes a web request.
- Windows Firewall - Creates a Windows Firewall outbound rule to allow or deny access to a remote resource for the logged in user.
- Windows Policy - Updates Windows policies allowing control of removable storage devices on the local device.
- Windows Registry - Updates or deletes values from the Windows Registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon Abort Task

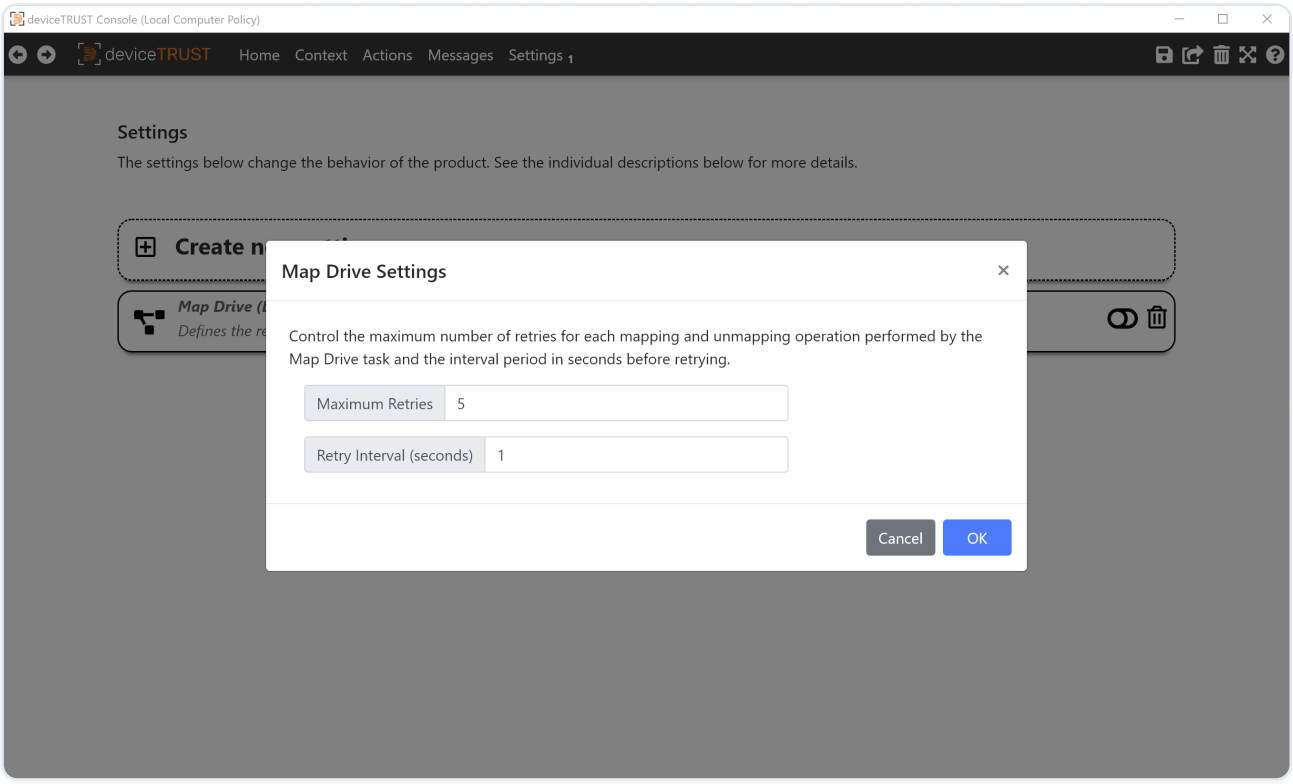
The `Logon Abort` task aborts the logon process, preventing the creation of the user session. When run as part of a Logon Pre Profile trigger, ensures that the user policy is not created. A message is displayed to the user briefly before reverting to an Operating System dependent access denied screen.



Map Drive Task

The `Map Drive` task maps and unmaps network drives within the user session.

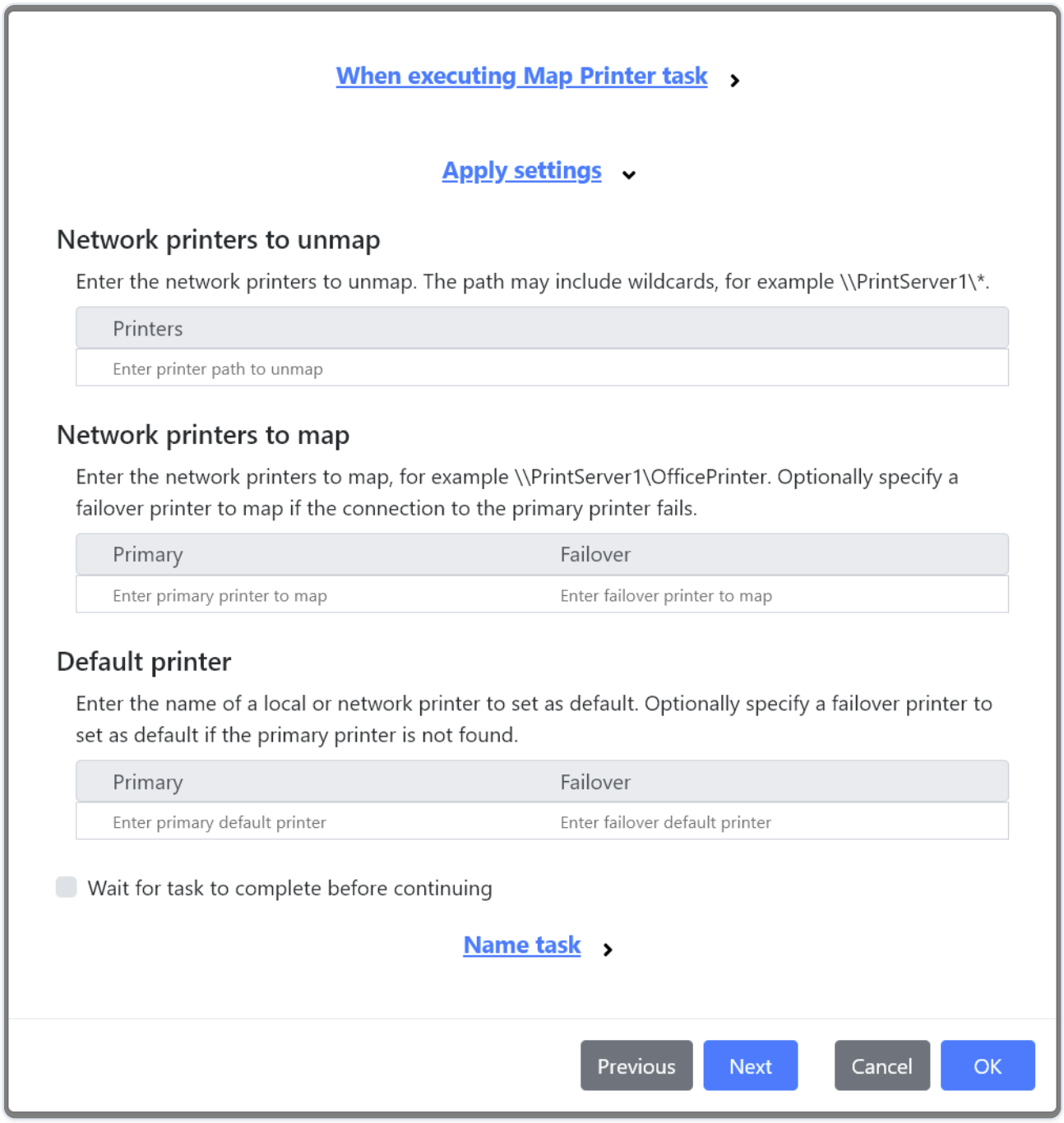
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Printer Task

The `Map Printer Task` task maps and unmaps network printers within the user session, and sets the default printer.

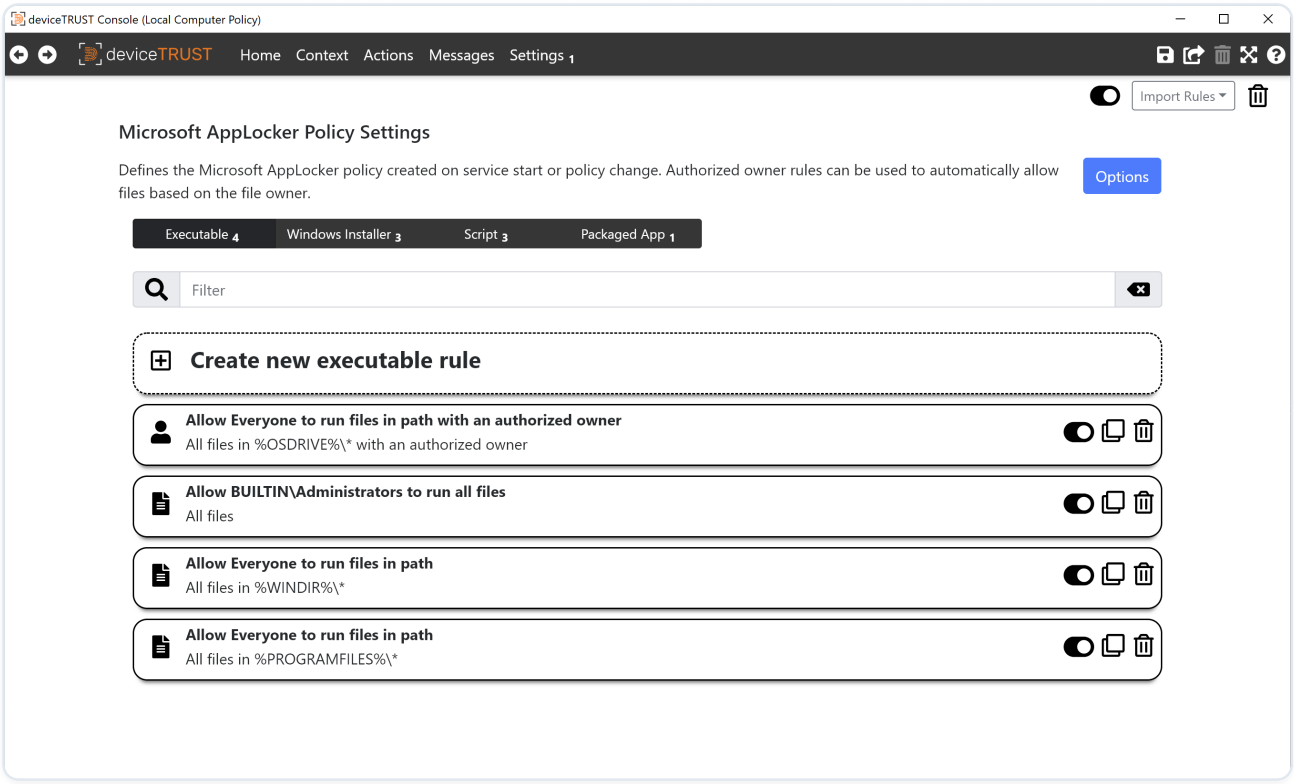
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Applocker Task

The `Microsoft Applocker` task creates, updates and deletes Microsoft AppLocker rules for the logged in user. Microsoft AppLocker must be configured and running for the rule to be effective.

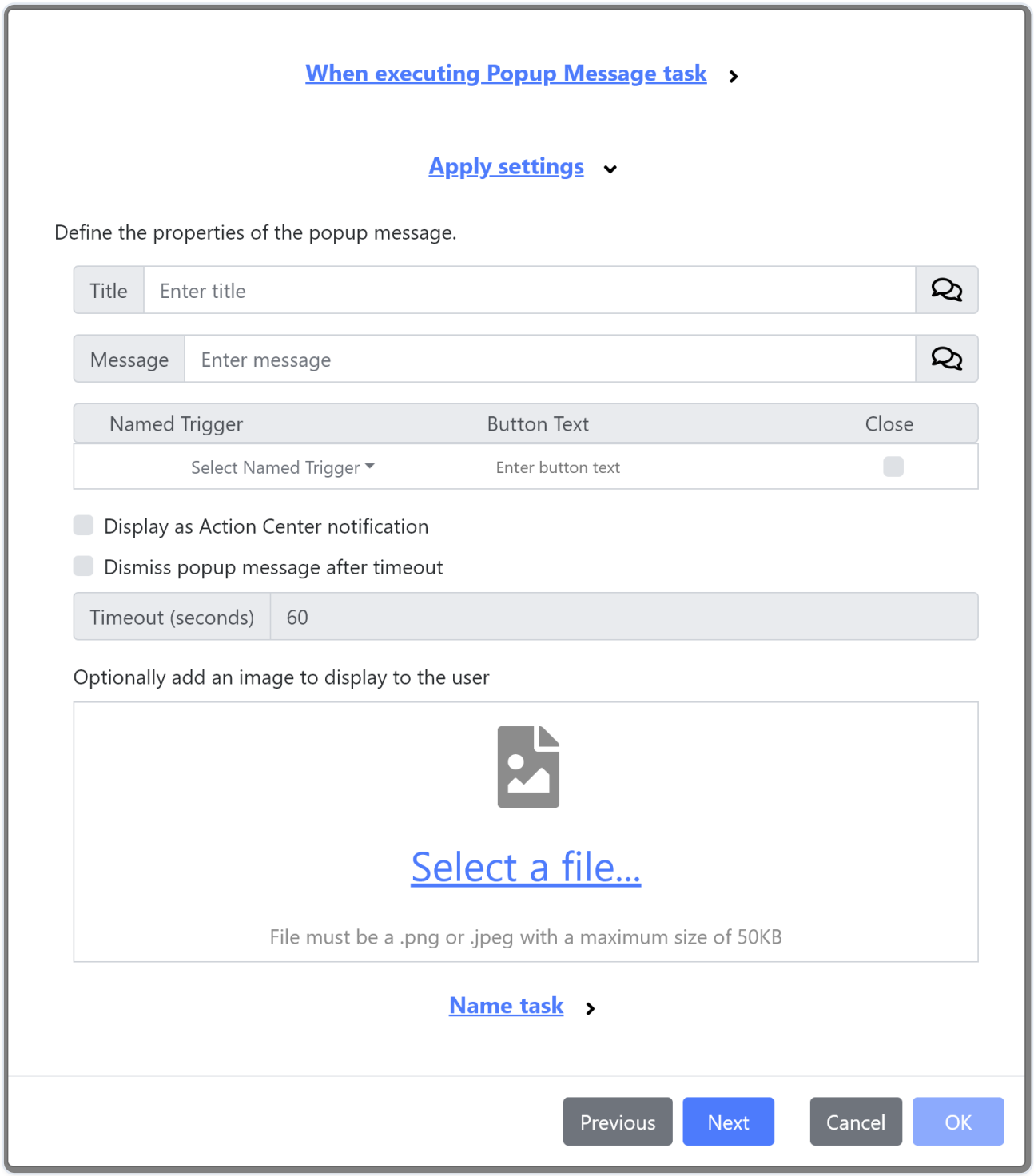
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Popup Message Task

The `Popup Message` task displays a popup message to the user, either in a top level popup window, or using an Action Center notification when available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following controls are available:

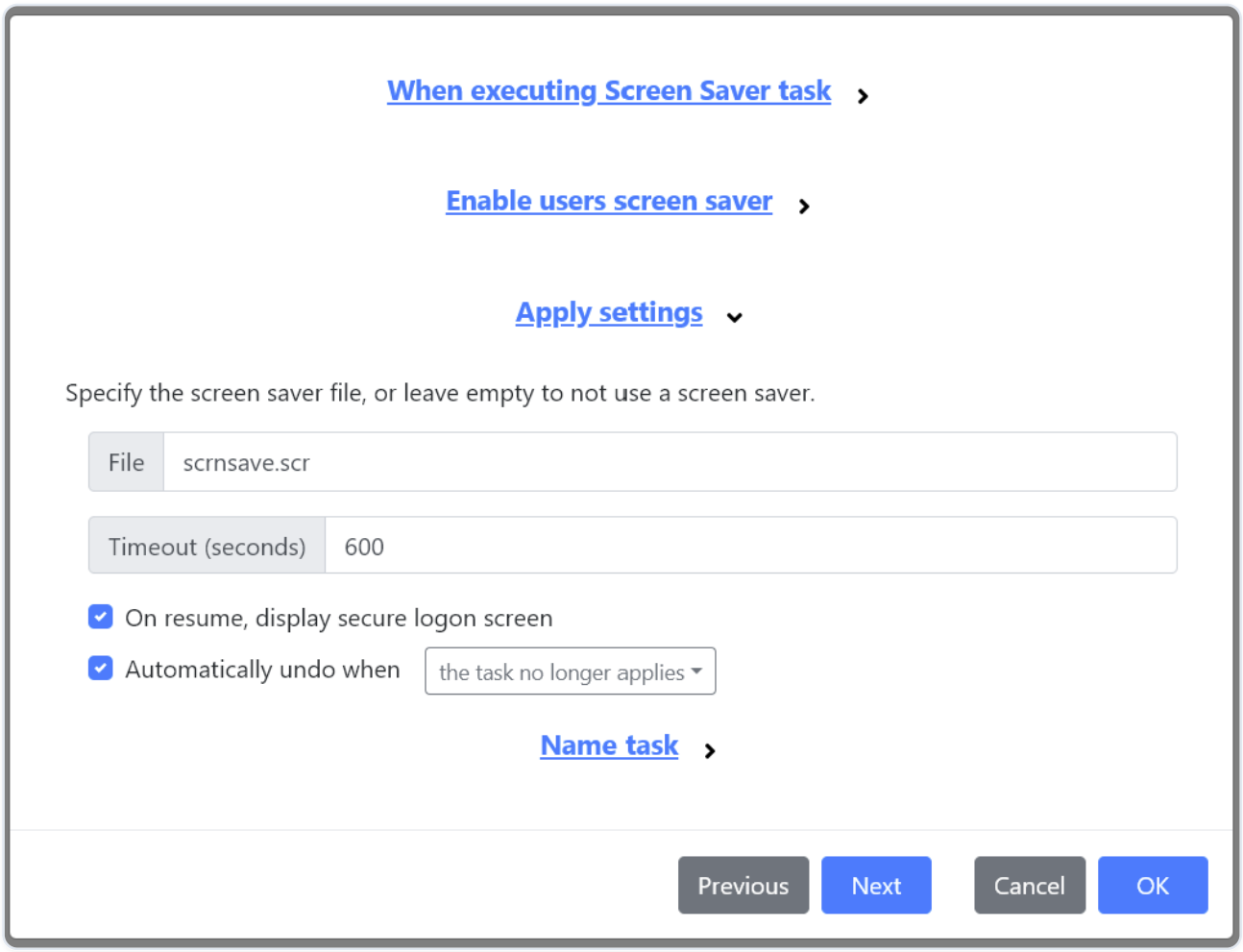
- *Title* - The title of the message displayed to the user.
- *Message* - The message displayed to the user.
- *Buttons* - Optionally, one or more additional buttons to add to the popup:
- *Named Trigger* - The name of a named trigger to execute when the user clicks the button.
- *Button Text* - The text displayed to the user on the button.
- *Close* - When checked, the popup message is closed when the user clicks the button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- *Display as Action Center Notification* - When checked, the popup message is shown using the OS notifications.
- *Dismiss popup message after timeout* - When checked, the popup message is automatically closed after the specified time period.
- *Image* - An optional image displayed on the popup.

Screen Saver Task

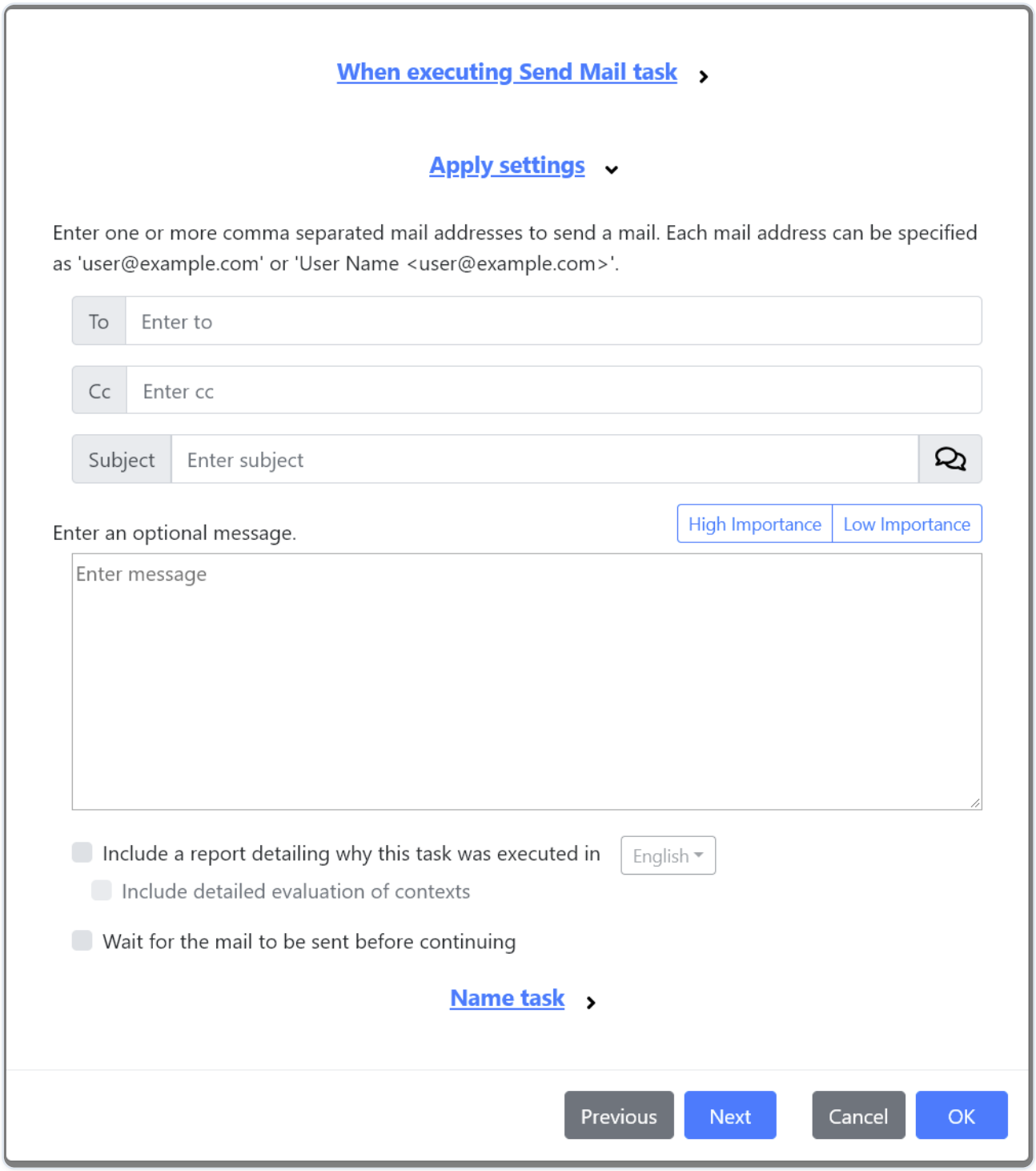
The `Screen Saver` task updates the screen saver settings within the session.



Send Mail Task

The `Send Mail` task sends an email with the defined content. Mail Server Settings must be configured.

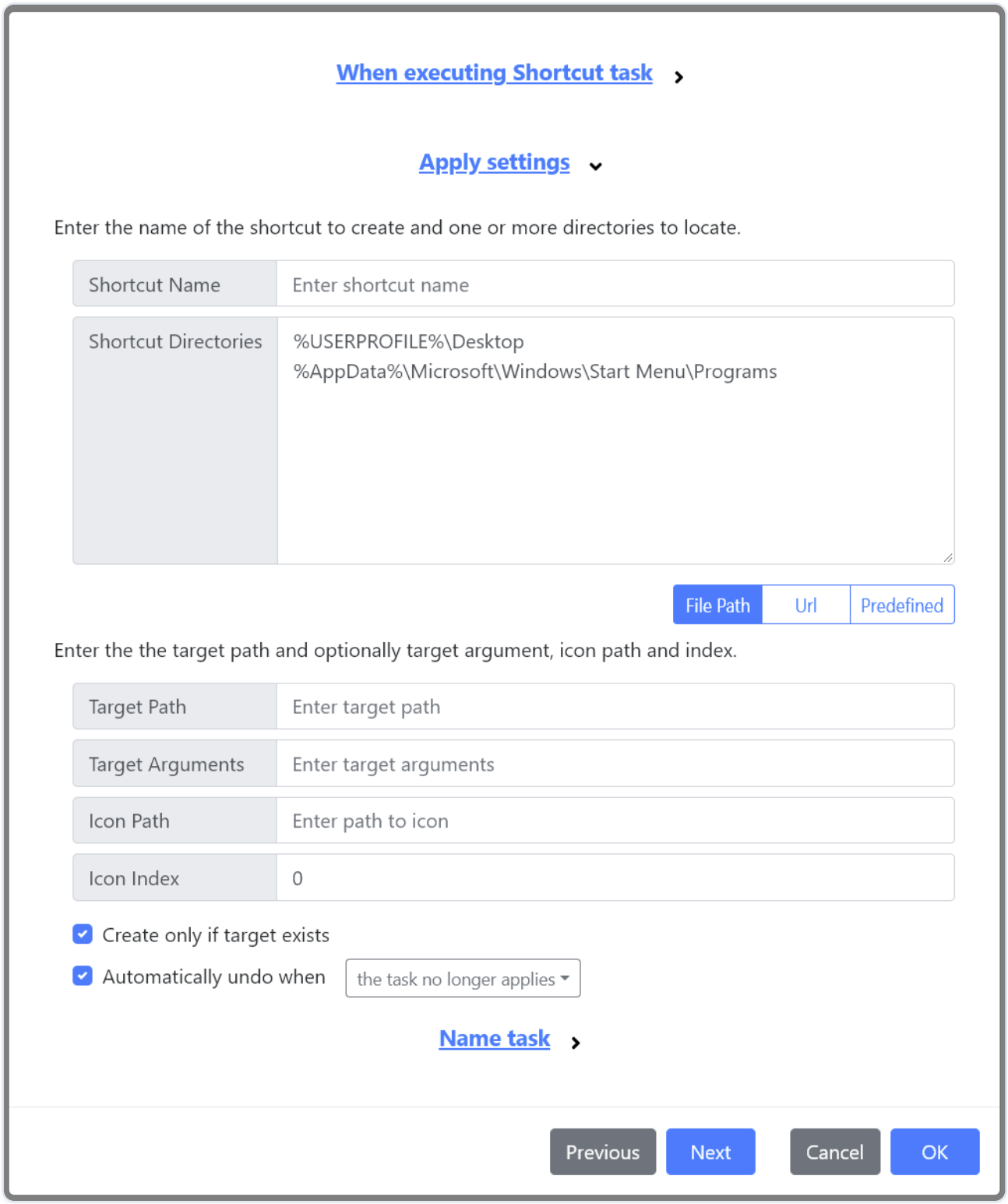
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Shortcut Task

The `Shortcut` task creates a shortcut within the user session.

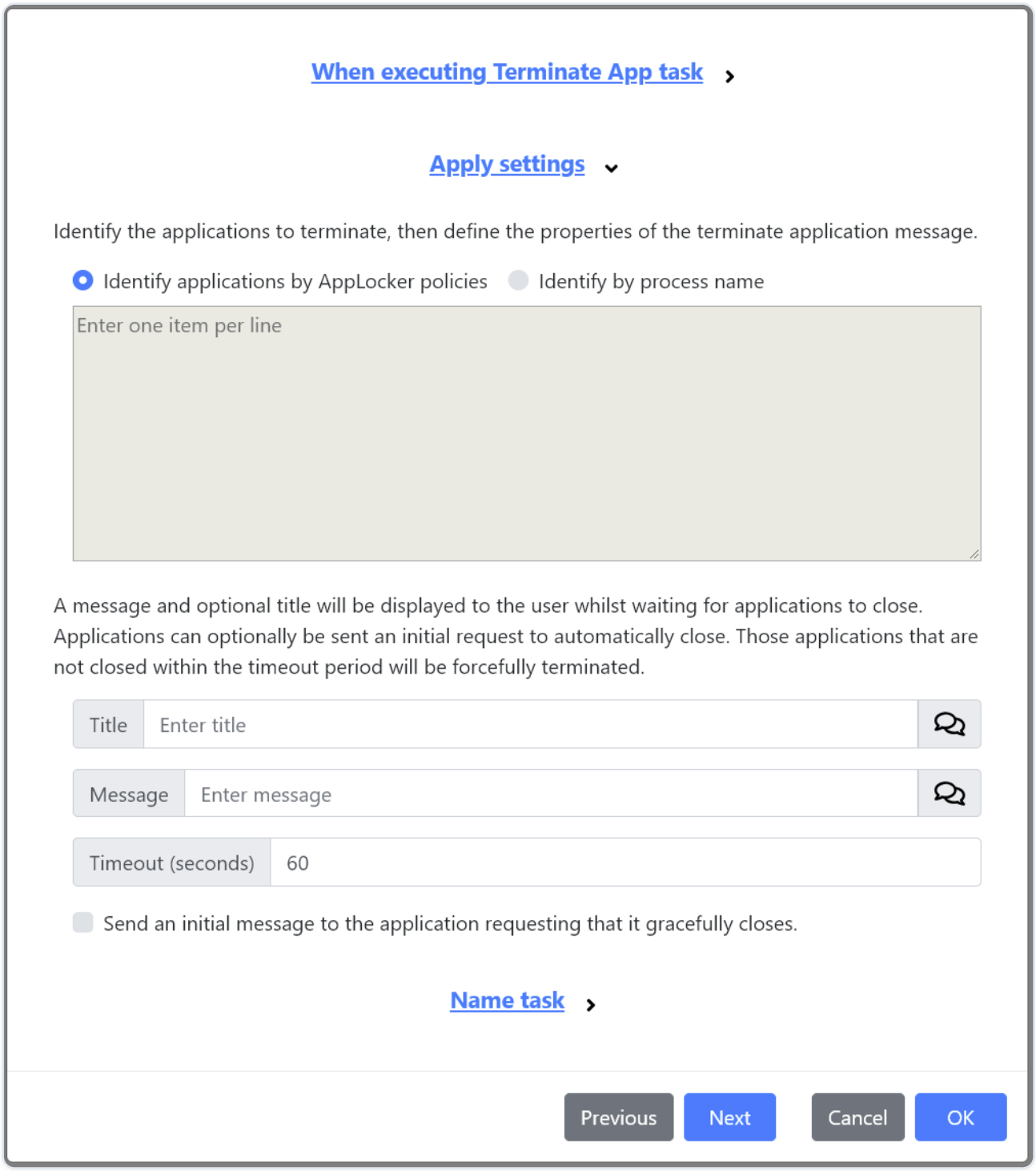
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Terminate App Task

The `Terminate App` task terminates applications that should not be running within the user session. Applications can either be identified by the current AppLocker policy, or by the name of the process.

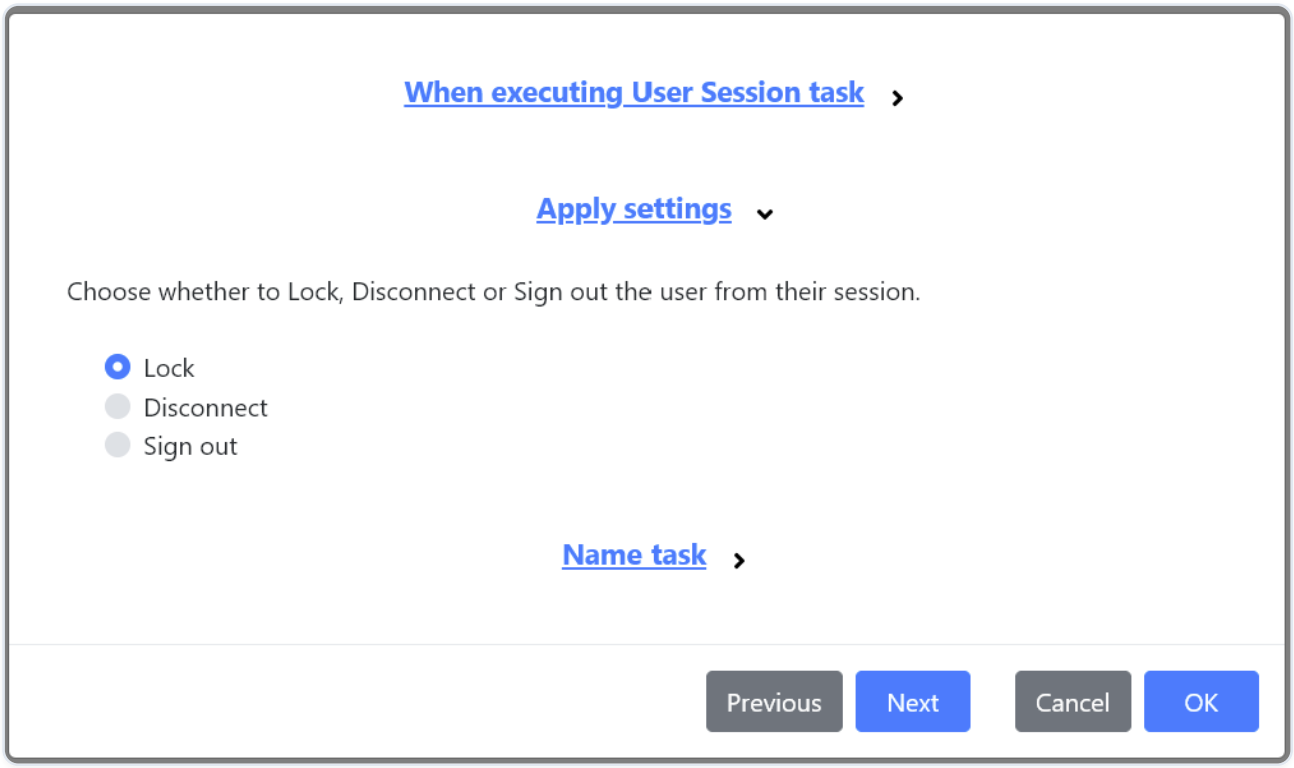
© 1997–2026 Citrix Systems, Inc. All rights reserved.



User Session Task

The `User Session` task locks, disconnects, or signs out the user session.

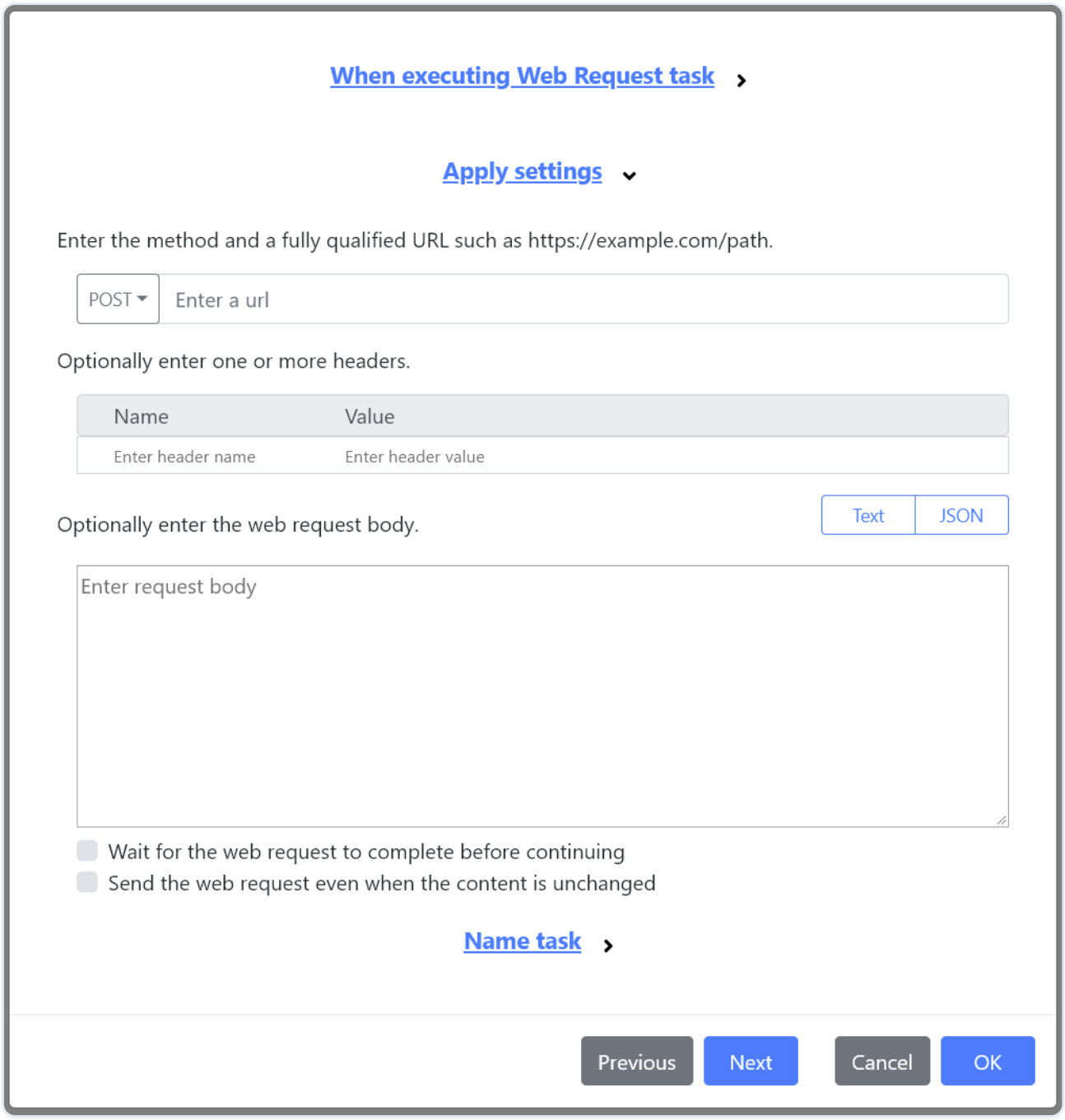
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Web Request Task

The `Web Request` task invokes a web request. This may be used to track events or properties of a user or device within a reporting and analytics engine.

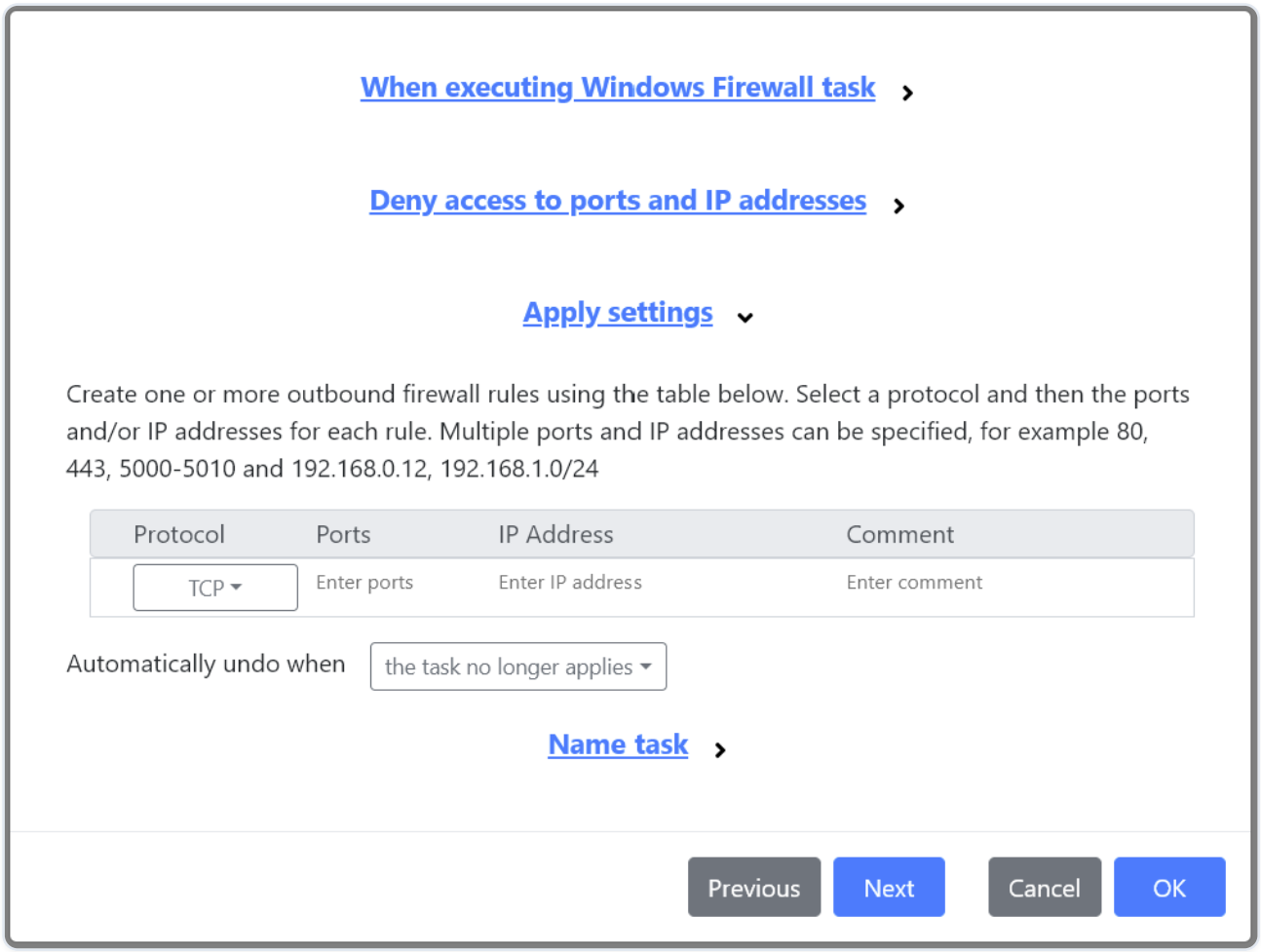
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Firewall Task

The `Windows Firewall` task creates a Windows Firewall outbound rule to allow or deny access to a remote resource for the logged in user.

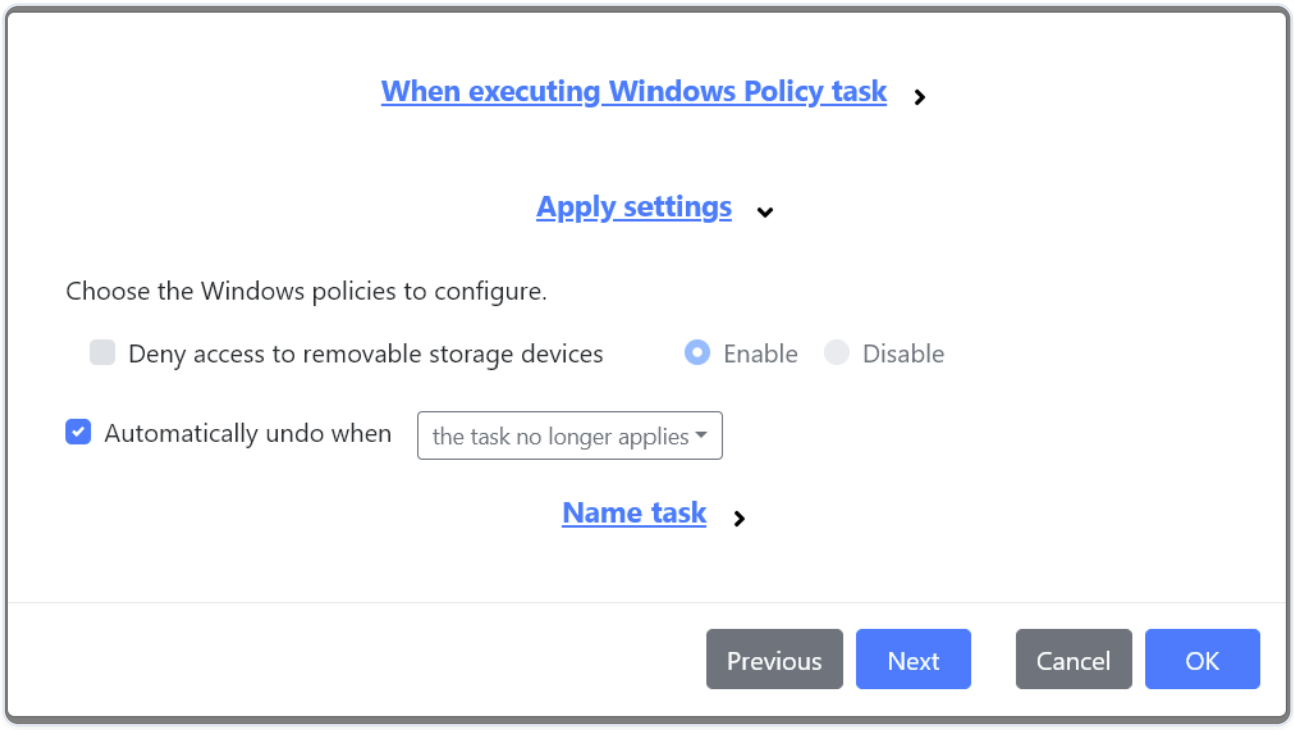
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Policy Task

The `Windows Policy` task updates Windows policies allowing control of removable storage devices on the local device.

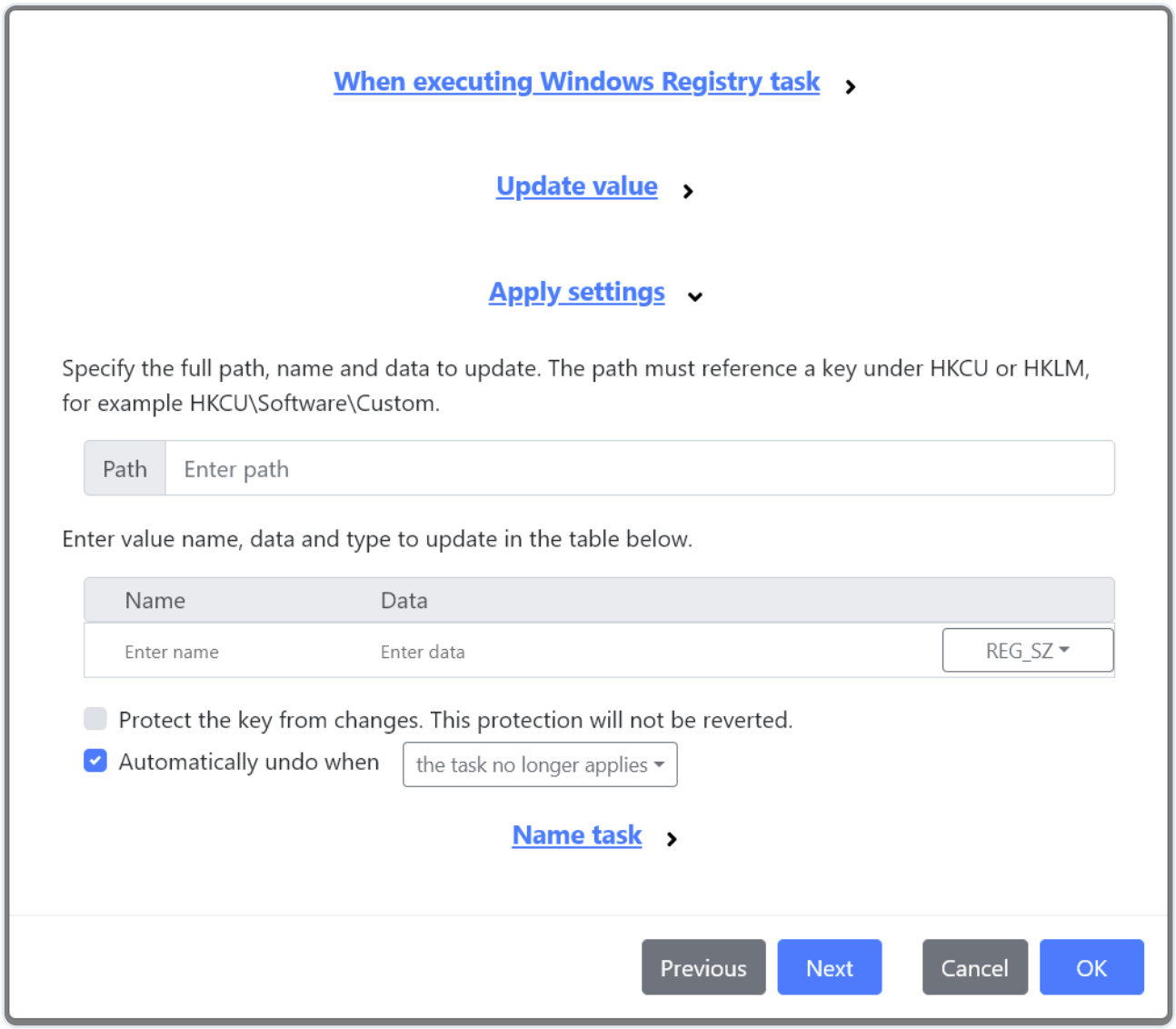
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Registry Task

The `Windows Registry` task updates or deletes values from the Windows Registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

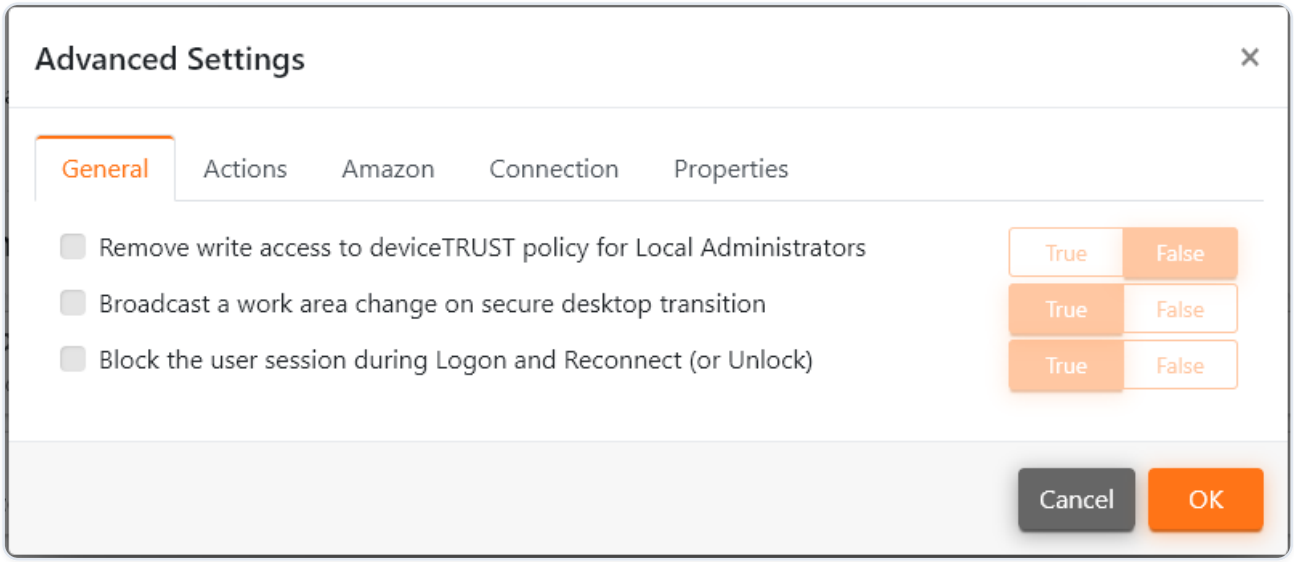


Advanced Settings

The `Advanced Settings` defines the advanced settings for configuring deviceTRUST behavior. These settings are described below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

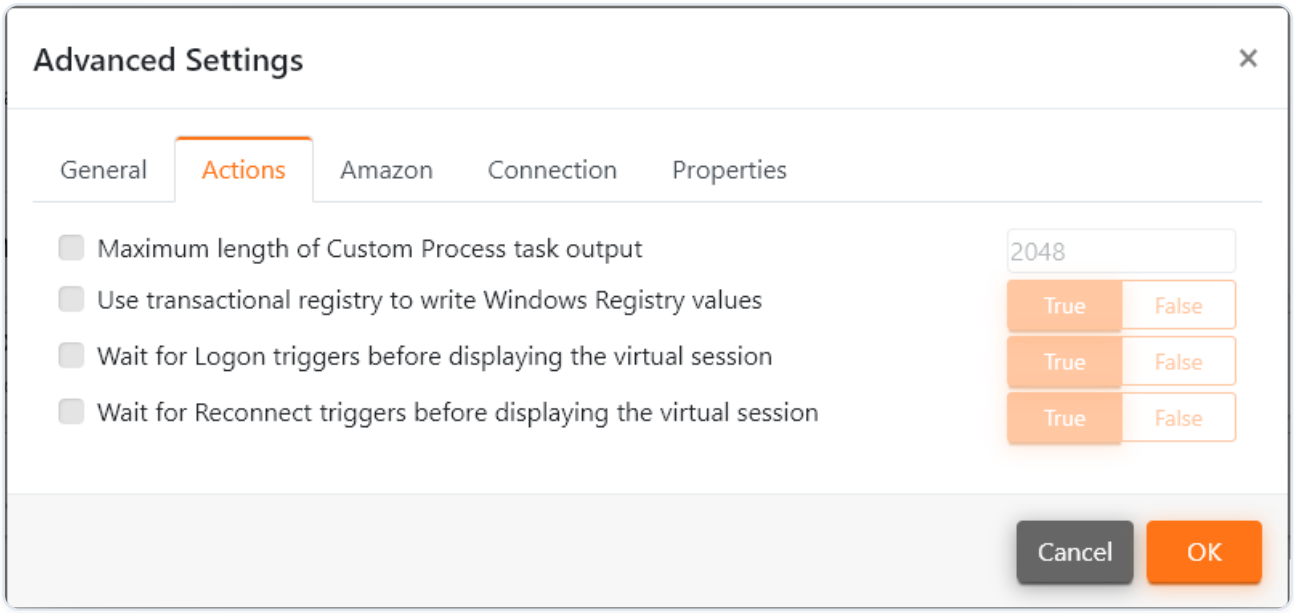
General Settings



The following controls are available:

- `Remove write access to deviceTRUST policy for Local Administrators` - Determines whether write access to the HKLM\\Software\\Policies\\deviceTRUST registry key should be removed for Local Administrators.
- `Block the user session during Logon and Reconnect (or Unlock)` - Determines whether deviceTRUST blocks Logon and Reconnect (or Unlock) sessions whilst properties are read from the remote device.
- `Broadcast a work area change on secure desktop transition` - Determines whether deviceTRUST broadcasts a message notifying top level windows of a work area change when transitioning in and out of a secure desktop.

Action Settings

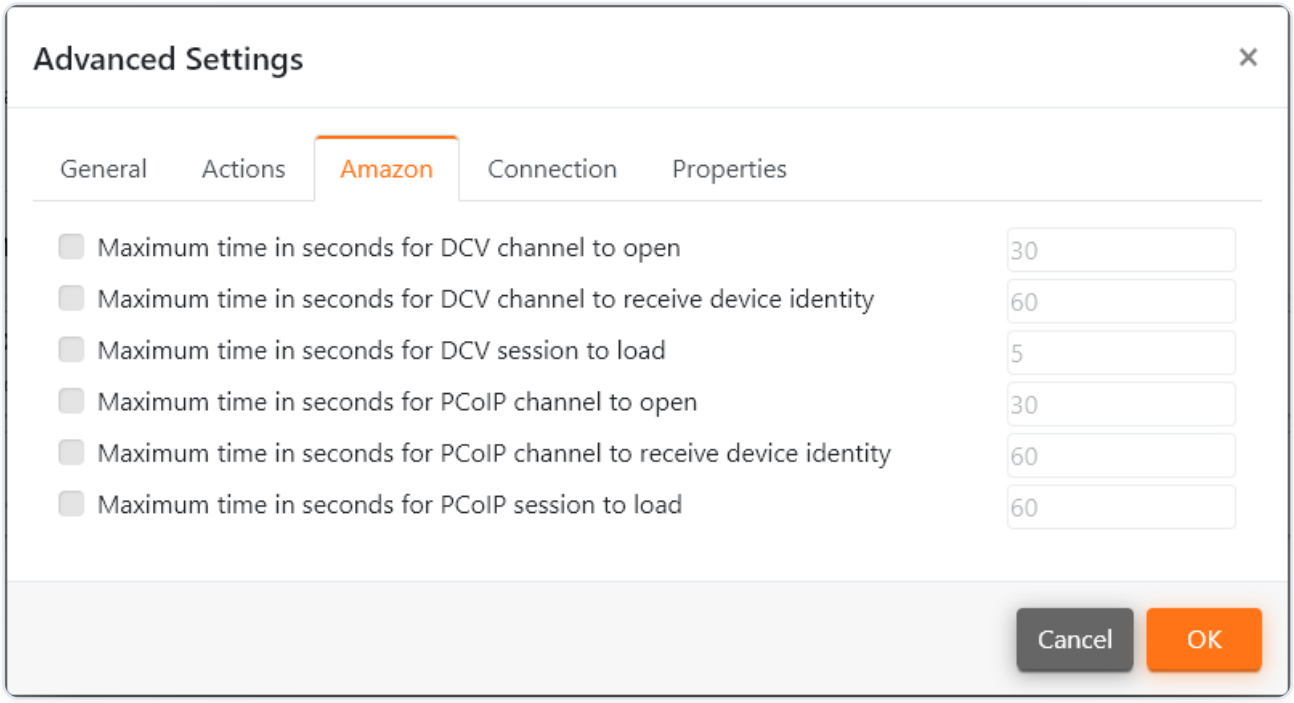


© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following controls are available:

- `Maximum length of Custom Process task output` - Determines the maximum number of characters to capture from the Custom Process task output.
- `Use transactional registry to write Windows Registry values` - Determines whether to use transactional registry operations when writing registry values within the Windows Registry, Screen Saver and Citrix Policy tasks.
- `Wait for Logon triggers before displaying the virtual session` - Determines whether the virtual session is blocked until Logon triggers have completed.
- `Wait for Reconnect triggers before displaying the virtual session` - Determines whether the virtual session is blocked until Reconnect triggers have completed.

Amazon Settings



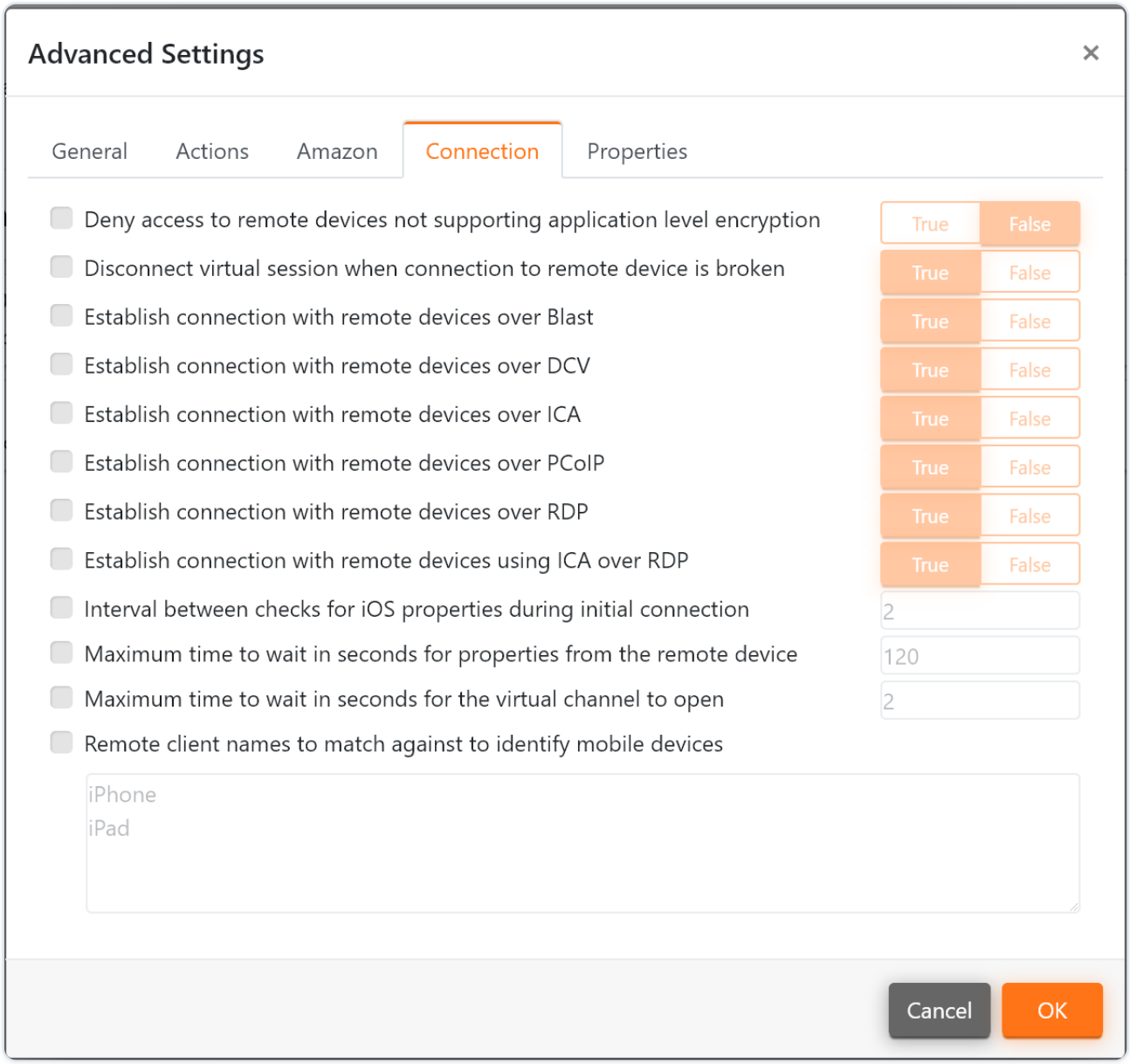
The following controls are available:

- `Maximum time in seconds for DCV channel to open` - Determines how long new connections should wait for the DCV virtual channel to open.
- `Maximum time in seconds for DCV channel to receive device identity` - Determines how long new connections should wait for the DCV virtual channel to receive the remote device identity.
- `Maximum time in seconds for DCV session to load` - Determines how long new connections should wait to recognise the user session as a DCV session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Maximum time in seconds for PCoIP channel to open` - Determines how long new connections should wait for the PCoIP virtual channel to open.
- `Maximum time in seconds for PCoIP channel to receive device identity` - Determines how long new connections should wait for the PCoIP virtual channel to receive the remote device identity.
- `Maximum time in seconds for PCoIP session to load` - Determines how long new connections should wait to recognise the user session as a PCoIP session.

Connection Settings



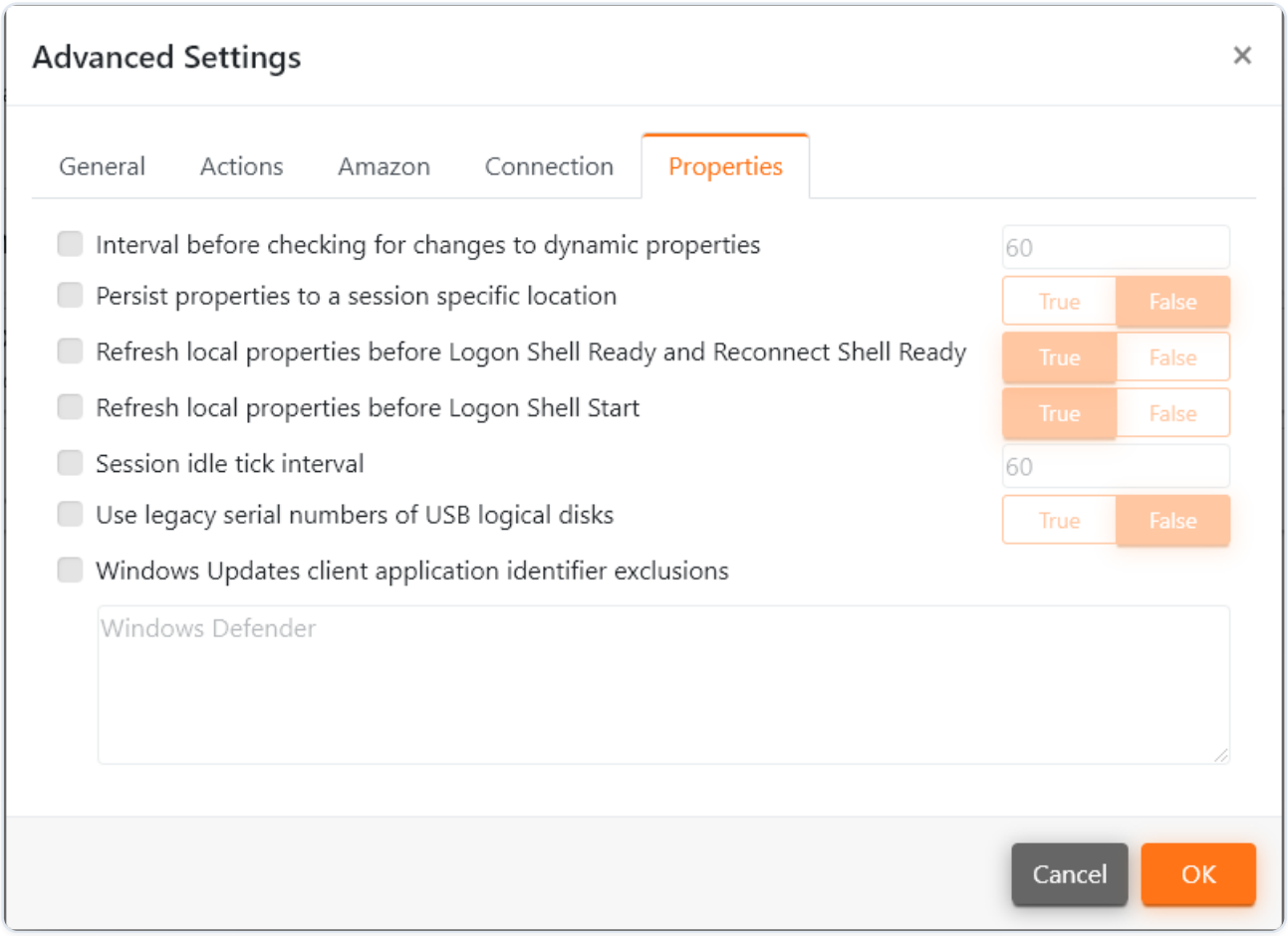
The following controls are available:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Deny access to remote devices not supporting application level encryption` - Defines whether to deny access to remote devices that do not support application level encryption.
- `Disconnect virtual session when connection to remote device is broken` - Determines whether to disconnect the virtual session when the connection to the client on remote device is broken.
- `Establish connection with remote devices over Blast` - Determines whether a connection to a remote device can be established over Blast.
- `Establish connection with remote devices over DCV` - Determines whether a connection to a remote device can be established over DCV.
- `Establish connection with remote devices over ICA®` - Determines whether a connection to a remote device can be established over ICA.
- `Establish connection with remote devices over PCoIP` - Determines whether a connection to a remote device can be established over PCoIP.
- `Establish connection with remote devices over RDP` - Determines whether a connection to a remote device can be established over RDP.
- `Establish connection with remote devices using ICA over RDP` - Determines whether a connection to a remote device can be established using the RDP virtual channel protocol for ICA sessions.
- `Interval between checks for iOS properties during initial connection` - Defines the interval in seconds between checks for properties from the iOS Client Extension during Logon or Reconnect.
- `Maximum time to wait in seconds for properties from the remote device` - Determines how long in seconds to wait for properties from the remote device.
- `Maximum time to wait in seconds for the virtual channel to open` - Determines how long to continue retrying to open a virtual channel.
- `Remote client names to match against to identify mobile devices` - Determines which remote client names identify a mobile device to display a passcode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Property Settings



The following controls are available:

- `Interval before checking for changes to dynamic properties` - Defines the interval in seconds before checking for changes to dynamic properties.
- `Persist properties to a session specific location` - Defines if the properties should be persisted to a session specific location witin `HKCU\\Software\\deviceTRUST\\Properties` and `HKCU\\Volatile Environment`.
- `Refresh local properties before Logon Shell Ready and Reconnect Shell Ready` - Determines whether local properties are refreshed before the Logon Shell Ready and Reconnect Shell Ready triggers are executed.
- `Refresh local properties before Logon Shell Start` - Determines whether local properties are refreshed before the Logon Shell Start trigger is executed.
- `Session idle tick interval` - Defines the interval in seconds that the session must remain idle for each increment of the session idle period.
- `Use legacy serial numbers of USB logical disks` - Determines whether to use the OS reported serial numbers of USB logical disks on Microsoft Windows platforms. These OS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

reported serial numbers do not always reflect the serial numbers of the underlying USB logical disk.

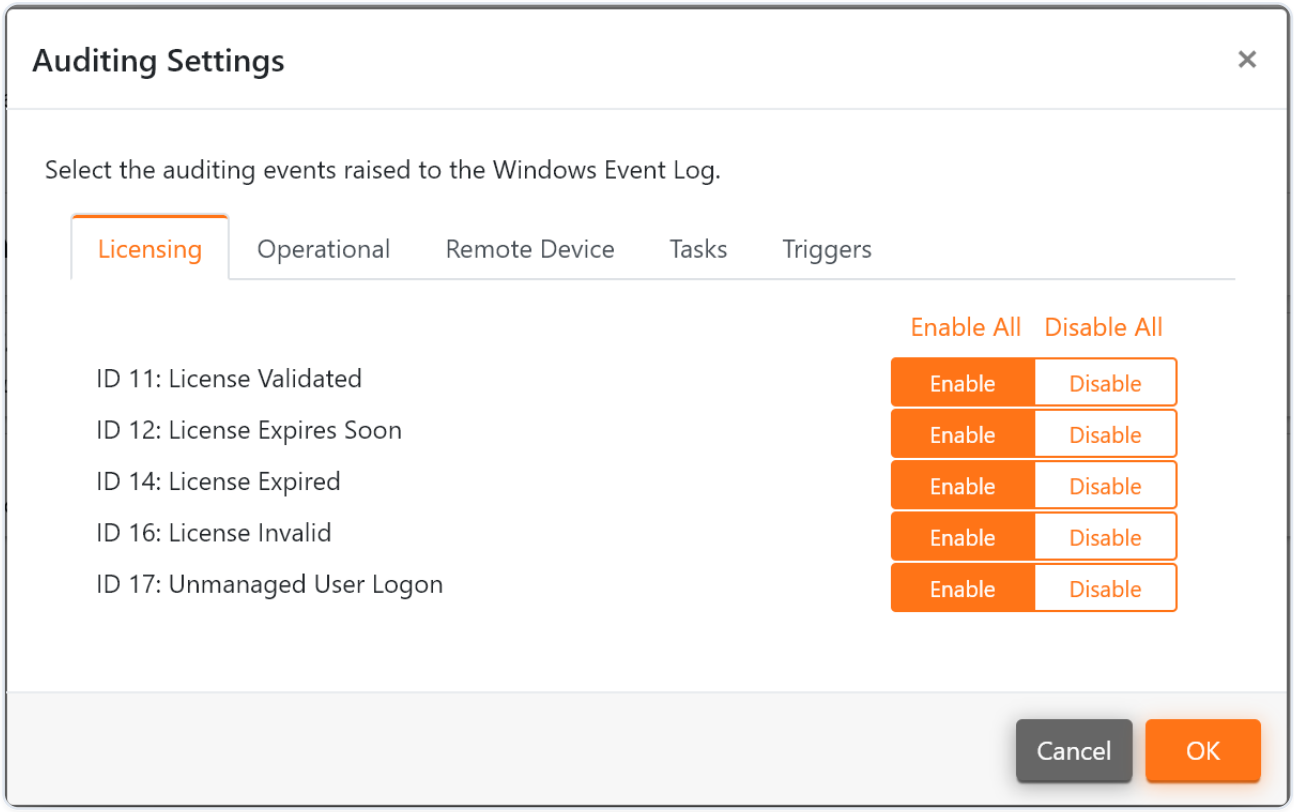
- `Windows Updates client application identifier exclusions` - List of client application identifiers of Windows Updates to ignore when calculating the last install time.

Auditing Settings

The `Auditing Settings` defines the audit events that are raised to the Windows Event Log.

Licensing

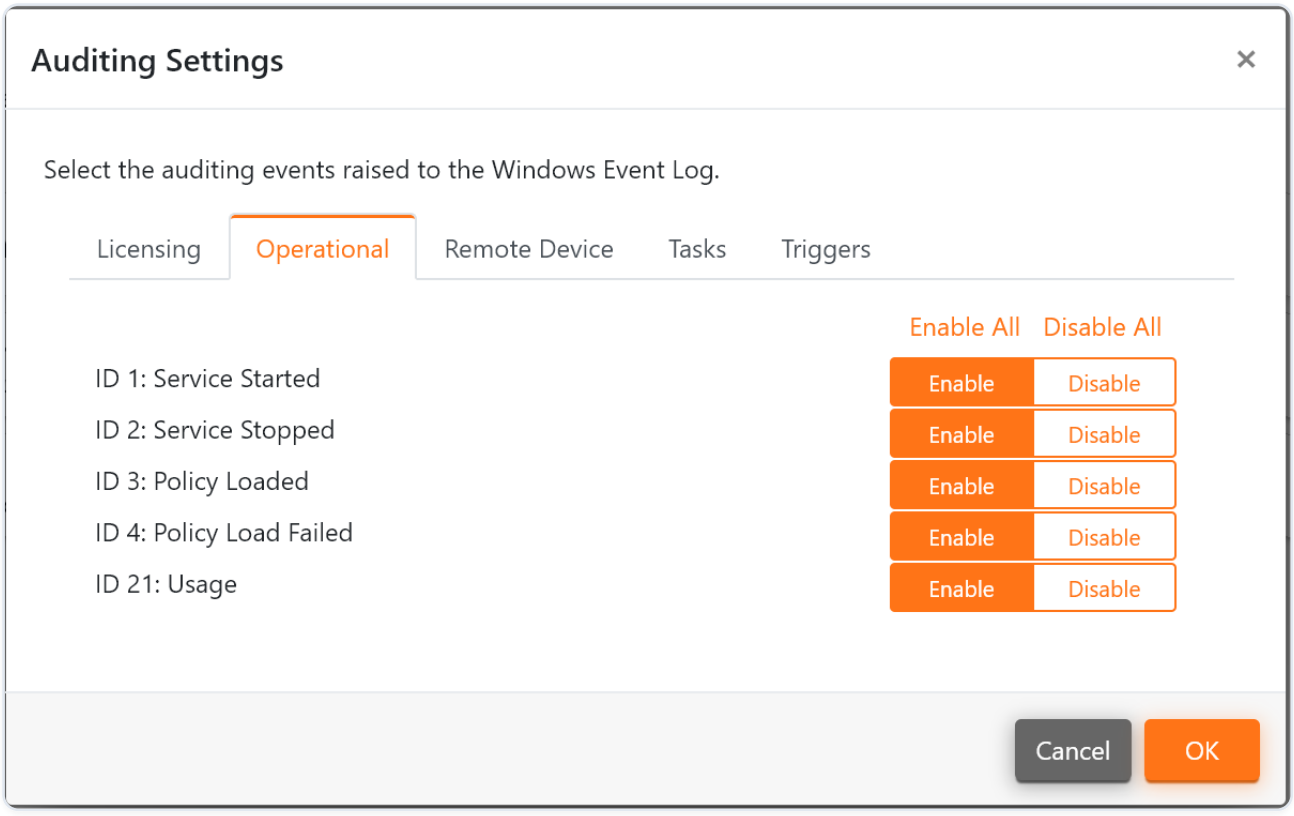
This section allows the control of events relating to the licensing of the deviceTRUST® product. All events are turned on by default but this can be customized by changing which events are enabled.



Operational

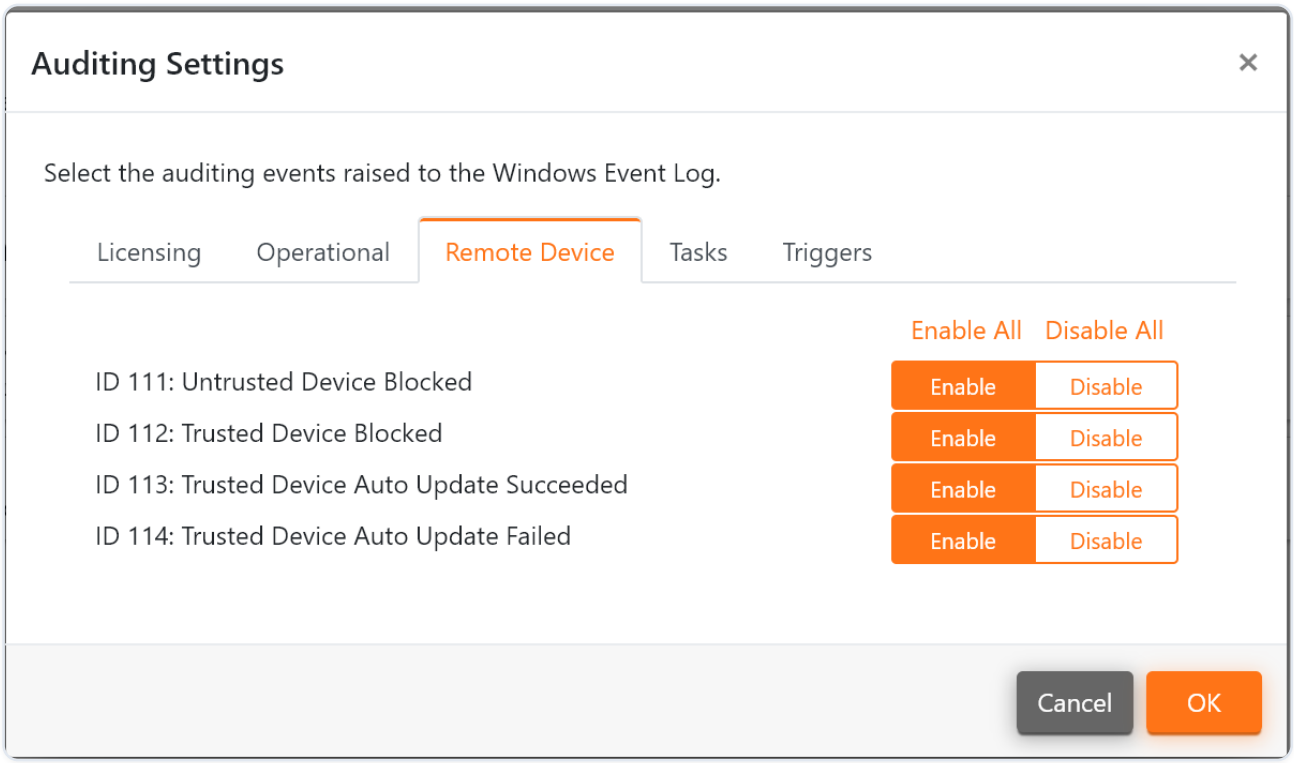
This section allows the control of events relating to the operation of the deviceTRUST product. All events are turned on by default but this can be customized by changing which events are enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remote Device

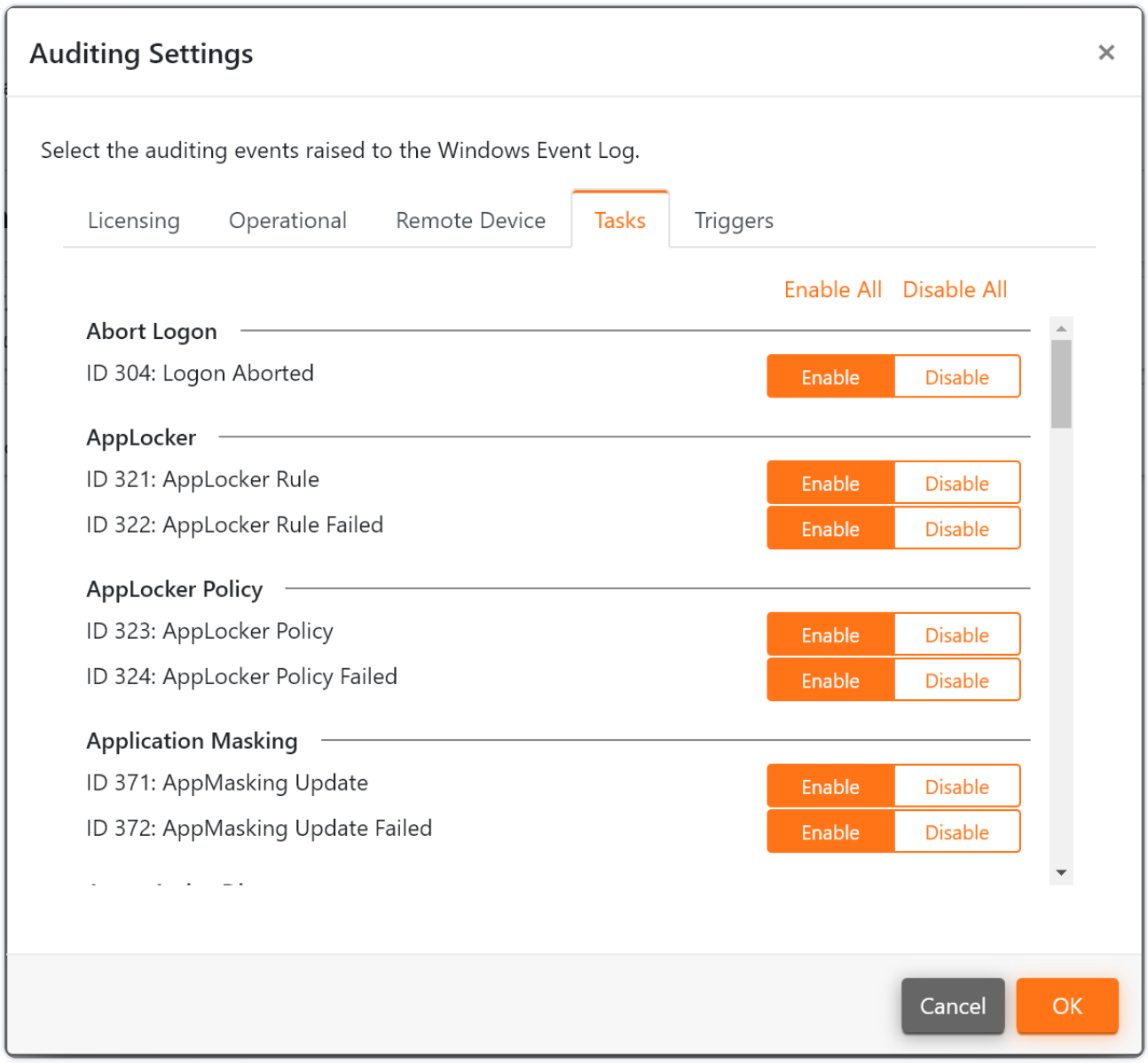
This section allows the control of events relating to the trust of a remote device attempting to establish a connection and also the status of the auto-update. All events are turned on by default but this can be customized by changing which events are enabled.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tasks

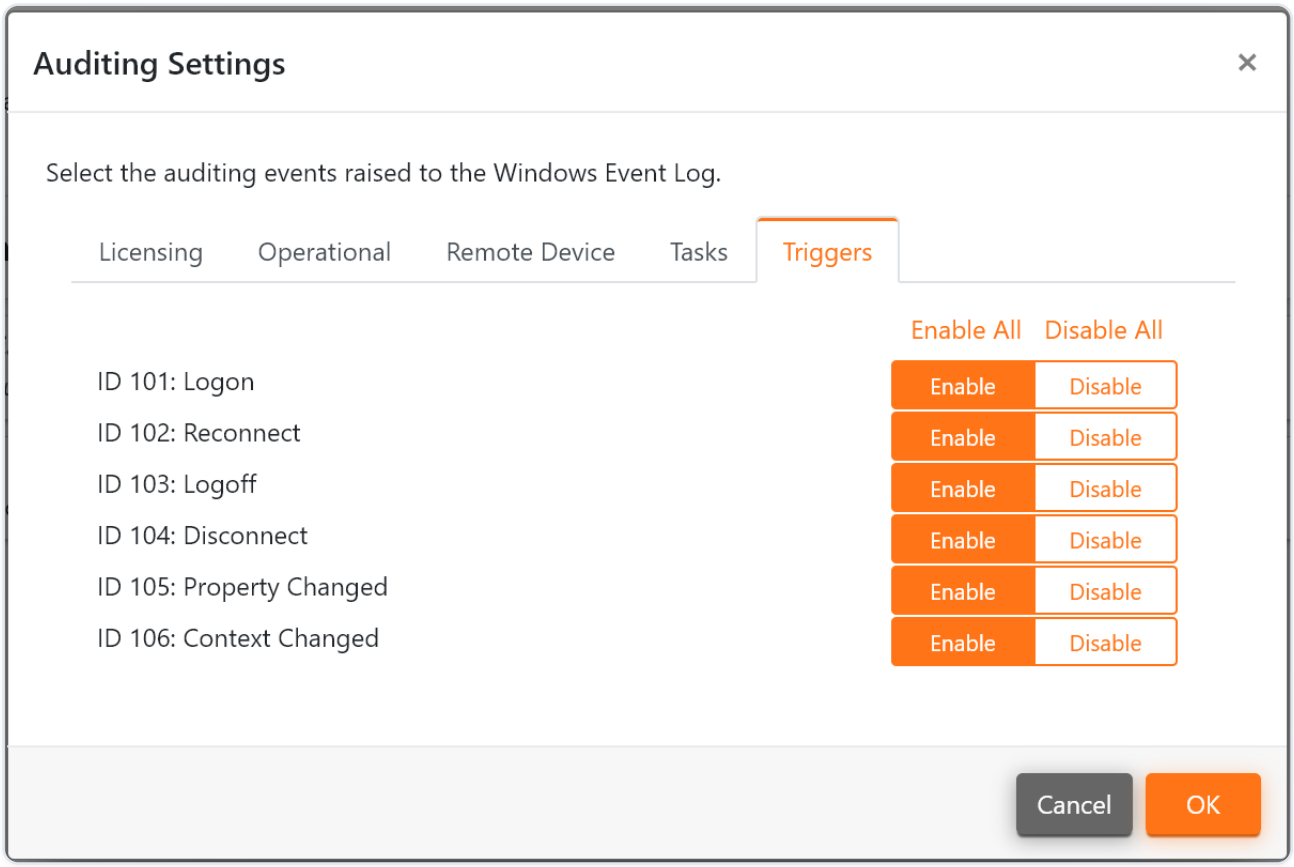
This section allows the control of events relating to the execution of tasks by the deviceTRUST product. This section groups the events per-task as described by each header. All events are turned on by default but this can be customized by changing which events are enabled.



Triggers

This section allows the control of events relating to the triggers of the deviceTRUST product. All events are turned on by default but this can be customized by changing which events are enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Custom Properties Settings

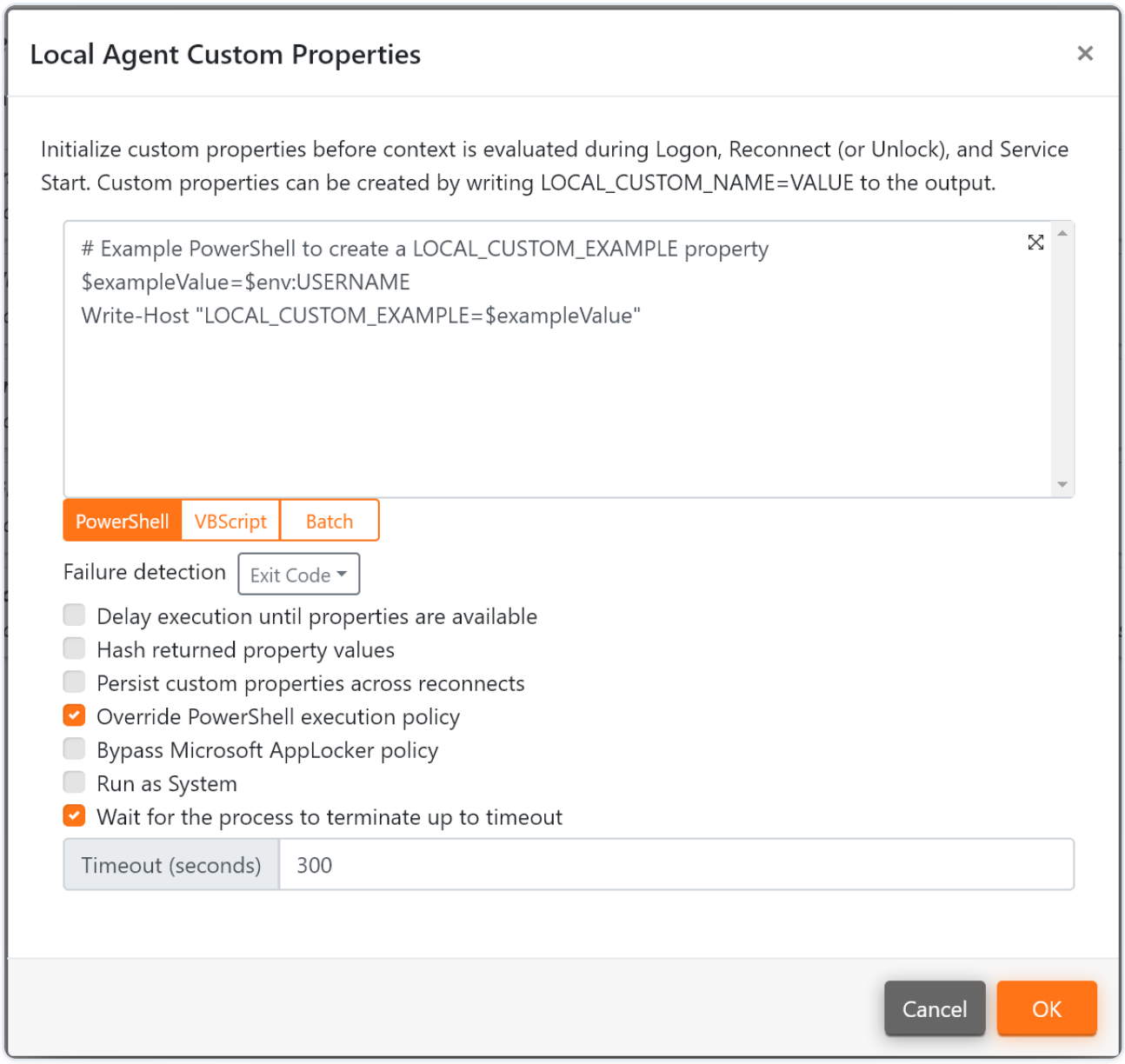
The `Custom Properties Settings` defines scripts that can be launched during a session to determine additional properties of the local agent or remote device before the context is first evaluated.

- Local Agent Custom Properties
- Remote Windows Device Custom Properties
- Remote Linux, IGEL or NoTouch Device Custom Properties
- Creating Custom Properties

Local Agent Custom Properties

When defined for the local agent, scripts are launched on Logon, Reconnect (or Unlock), and Service Start.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following controls are available for the Local Agent:

- `Embedded Script` - Defines the script that will be evaluated on the local agent.
- `Embedded Script Language` - Set to either PowerShell, VBScript or Batch, and defines the scripting language used by the embedded script.
- `Delay execution until properties are available` - When checked, will execute the script after the all properties have been determined. The properties are available either from the Windows Registry, or as environment variables within the script.
- `Hash returned property values` - When checked, any returned custom properties are converted to a SHA256 hash.
- `Persist custom properties across reconnects` - When checked, the script is only evaluated on Logon and Service Start. Any custom properties that are created remain

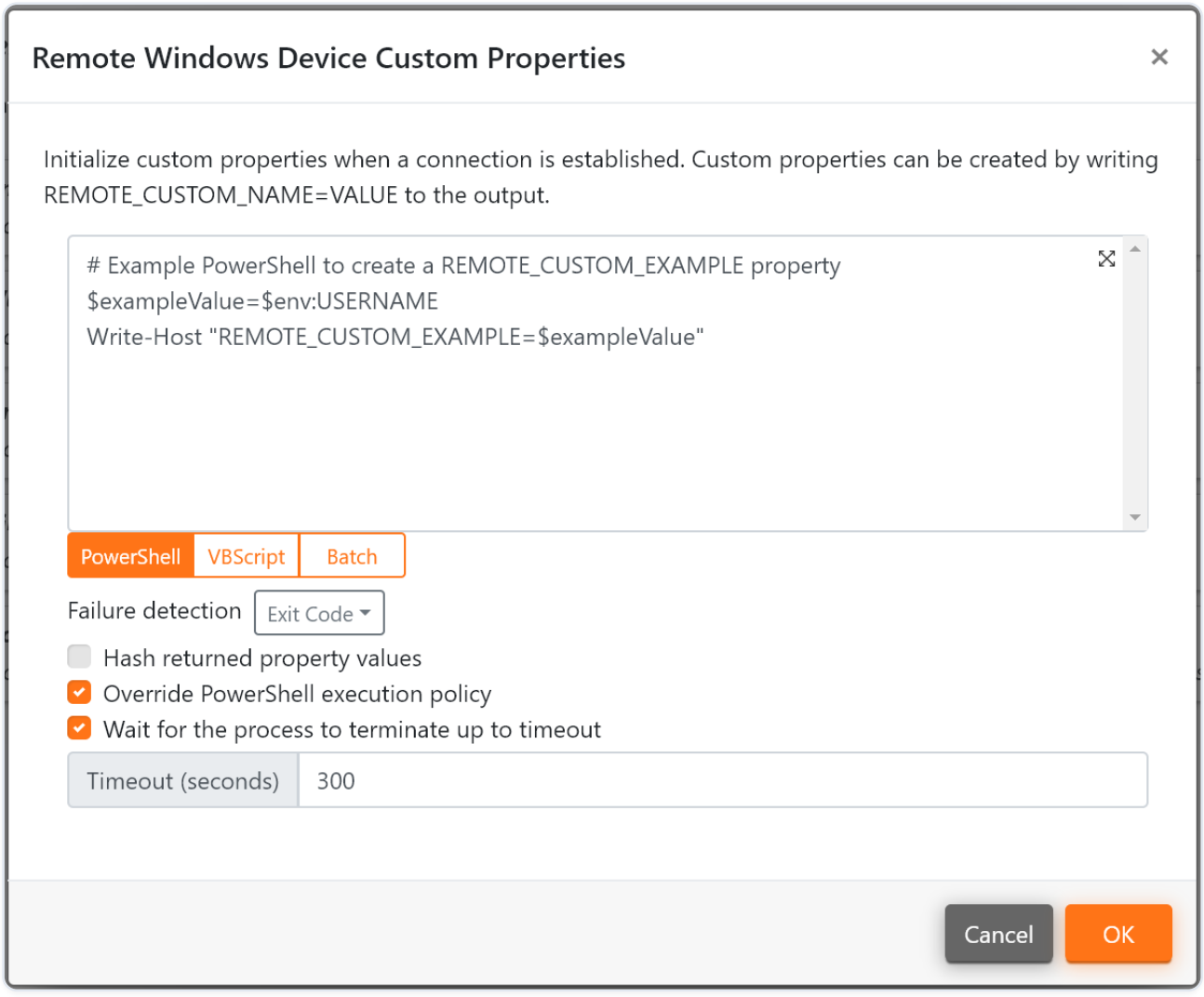
© 1997–2026 Citrix Systems, Inc. All rights reserved.

unchanged if a user Reconnects to a virtual session. When unchecked, any custom properties are discarded when the session is disconnected and the script is relaunched on a Reconnect.

- `Override PowerShell execution policy` - When checked, any PowerShell scripts are launched with an execution policy set to `Unrestricted`.
- `Bypass Microsoft AppLocker policy` - When checked, any PowerShell based Microsoft AppLocker rules are bypassed by the executed script.
- `Run as System` - When checked, the script is launched as the `System` user. When unchecked, the script is launched as the user logging into the session.
- `Wait for the process to terminate up to timeout` - Defines a timeout period after which the Logon or Reconnect process will no longer be held up if the script has not completed.

Remote Windows Device Custom Properties

When defined for the Remote Windows Device, scripts are launched on connecting Windows devices at the start of the virtual session.



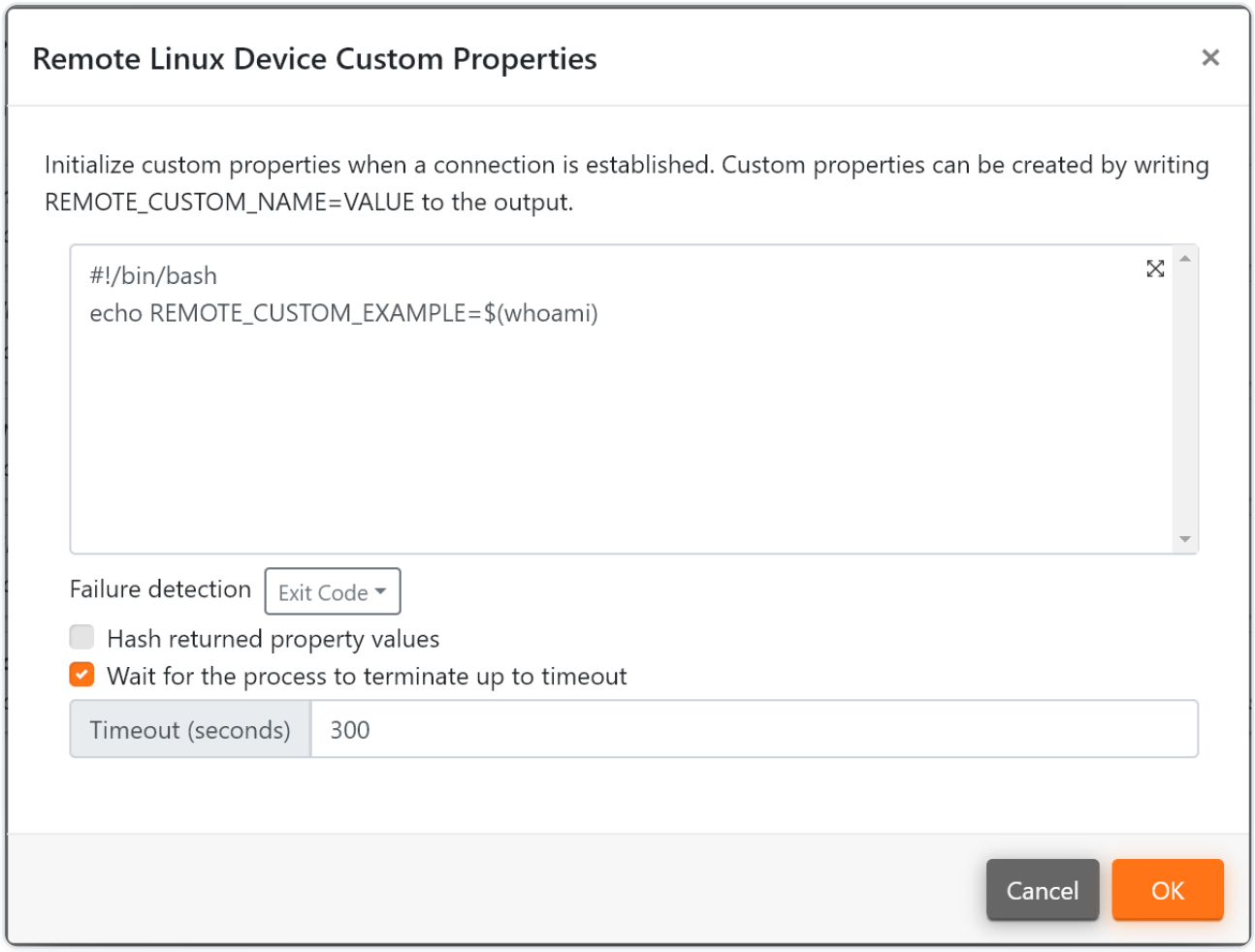
The following controls are available for the Remote Windows Device:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Embedded Script` - Defines the script that will be evaluated on the remote Windows device.
- `Embedded Script Language` - Set to either PowerShell, VBScript or Batch, and defines the scripting language used by the embedded script.
- `Hash returned property values` - When checked, any returned custom properties are converted to a SHA256 hash.
- `Override PowerShell execution policy` - When checked, any PowerShell scripts are launched with an execution policy set to `Unrestricted`.
- `Wait for the process to terminate up to timeout` - Defines a timeout period after which the process will no longer be held up if the script has not completed.

Remote Linux, IGEL or NoTouch Device Custom Properties

When defined for the Remote Linux, IGEL or NoTouch Device, scripts are launched on connecting Linux based devices at the start of the virtual session.



The following controls are available:

- `Embedded Script` - Defines the script that will be evaluated on the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Hash returned property values` - When checked, any returned custom properties are converted to a SHA256 hash.
- `Wait for the process to terminate up to timeout` - Defines a timeout period after which the process will no longer be held up if the script has not completed.

Creating Custom Properties

Custom Properties scripts can create a custom property by writing either `LOCAL_CUSTOM_<NAME>=<VALUE>`, or `REMOTE_CUSTOM_<NAME>=<VALUE>` to the output. On Windows, this can be achieved by calling `Write-Host` in PowerShell, `WScript.Echo` in VBScript or `echo` within a Batch script. On Linux based clients, this can be achieved in bash using `echo`.

Custom Properties scripts can stay resident in memory for the lifetime of the session, perhaps by entering a loop or by registering for events. Custom properties can be created in the usual way, or deleted by outputing `DELETE LOCAL_CUSTOM_<NAME>` or `DELETE REMOTE_CUSTOM_<NAME>`. After all properties are emitted to the output, a single line stating `CONTINUE` should be written to the output.

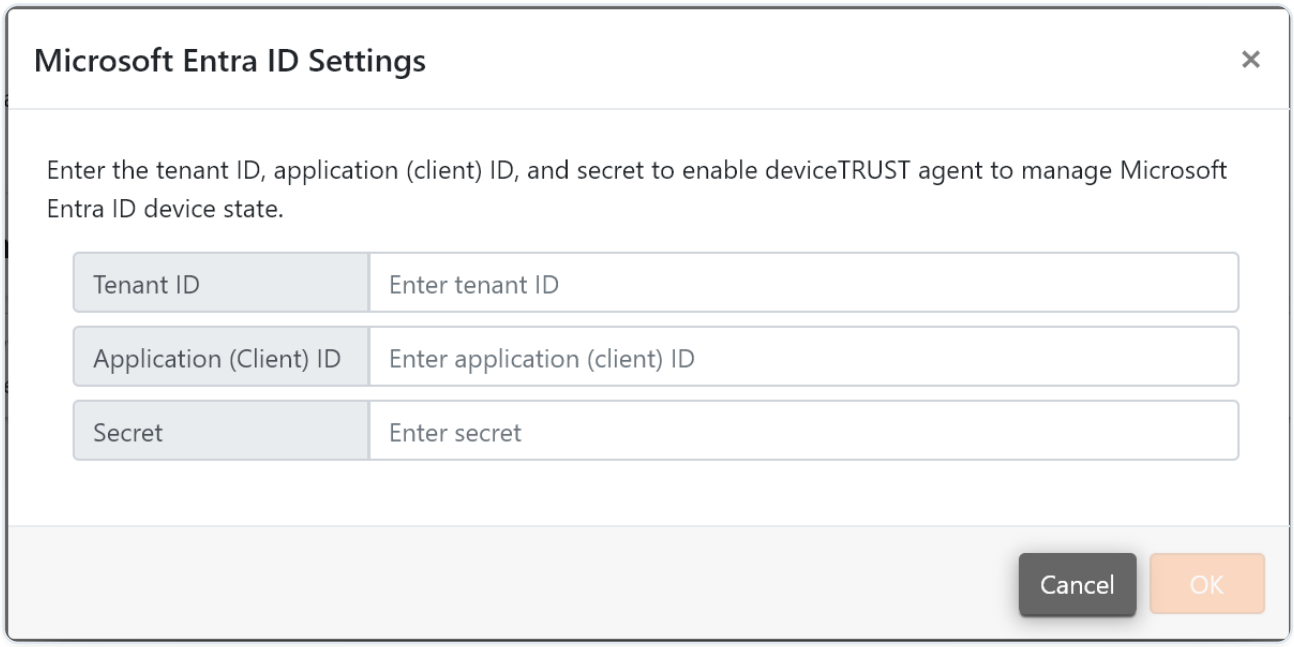
The `Wait for the process to terminate up to timeout` option should be unchecked for resident scripts. Any custom properties scripts that are still executing will be terminated when it is no longer needed.

Microsoft Entra ID Settings

The `Microsoft Entra ID Settings` defines the Tenant ID, Application (Client) ID and Secret required to manage Microsoft Entra ID (formerly Microsoft Azure AD).

To integrate with Entra ID, create a new `App Registration` within the Azure Portal. Within the App Registrations `API permissions`, ensure to grant admin consent for Microsoft Graph's `Device.ReadWrite.All`. Finally, within `Certificates & secrets`, create a `New client secret`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following controls are available:

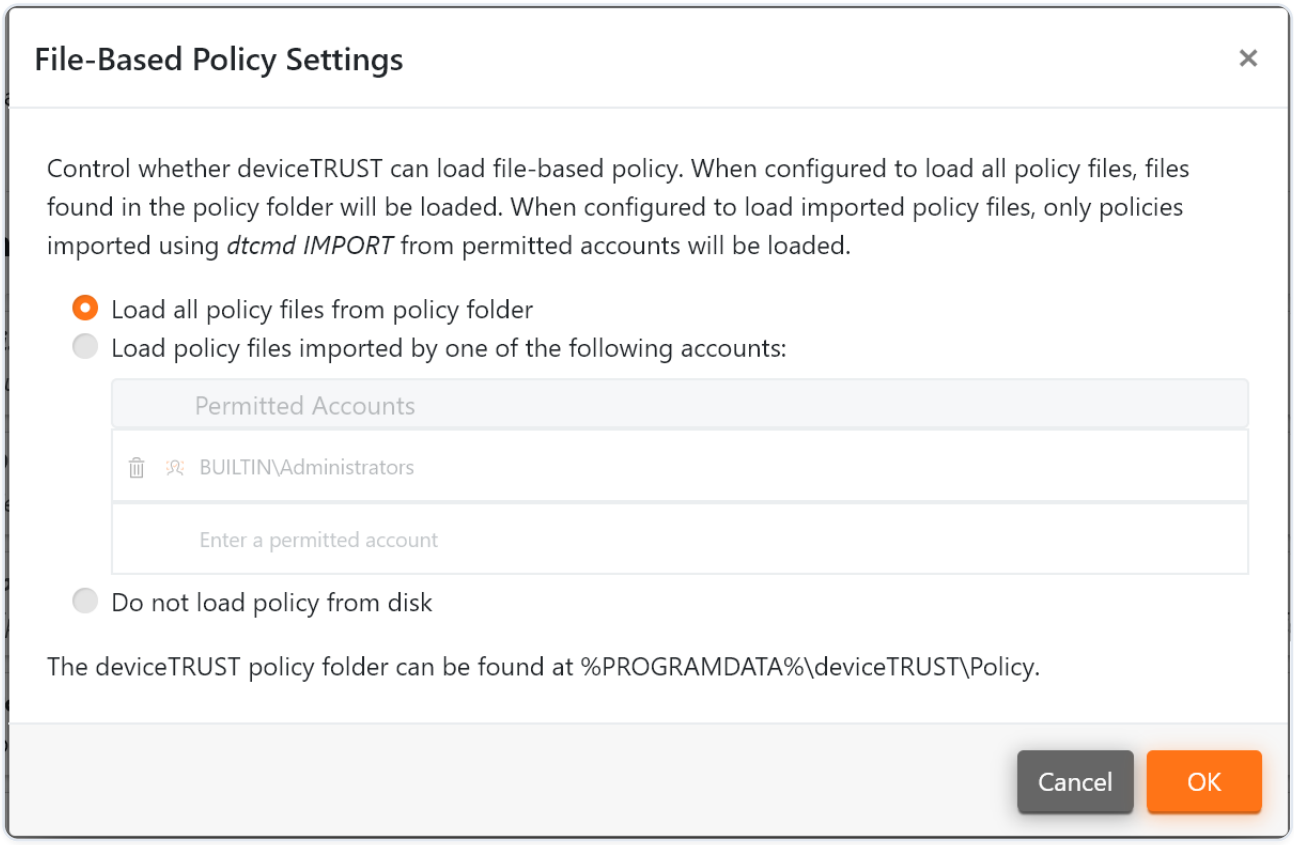
- `Tenant ID` - The Tenant ID of the Microsoft Entra ID tenant. This can be copied from the App Registrations `Overview` page.
- `Application (Client) ID` - The Application (client) ID field from the App Registrations `Overview` page.
- `Secret` - The `Value` field of the client secret.

File-Based Policy Settings

The `File-Based Policy Settings` defines the behavior of File-Based Policy.

The default behavior is for the deviceTRUST® agent to load File-Based Policy located within the deviceTRUST policy folder. This behavior can be customized to only load File-Based Policy imported into the policy folder by an authorized user, or to never load file-based policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following controls are available:

- `Load all policy files from policy folder` - When selected, any file located within the policy folder will be loaded.
- `Load policy files imported by one of the following accounts` - When selected, only users within the `Permitted Accounts` can import File-Based Policy into the policy folder using the dtcmd tool. See Importing below.
- `Do not load policy from disk` - When selected, policy files will not be imported from the policy folder. This option is only used when defined within a GPO.

Importing

When `Load policy files imported by one of the following accounts` has been enabled, only users within the `Permitted Accounts` can import File-Based Policy into the policy folder using the dtcmd tool.

Permitted users can import file-based policy using the following command:

```
dtcmd IMPORT /add:<filepath>
```

Permitted users can remove file-based policy using the following command:

```
dtcmd IMPORT /remove:<filepath>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permitted users can remove all file-based policy using the following command:

```
dtcmd IMPORT /clear
```

For more information on deviceTRUST policy see Policy Loading

Settings

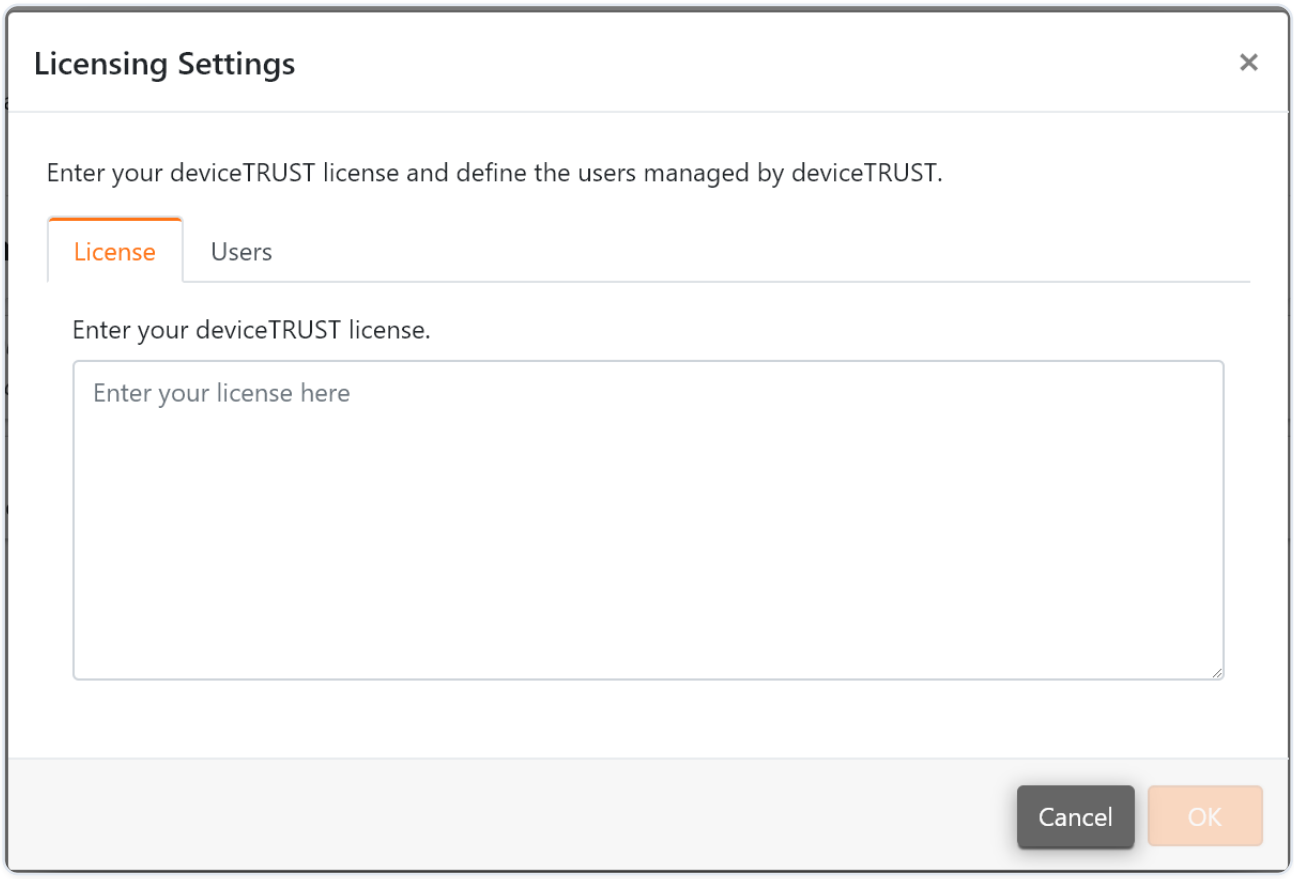
TABLE OF CONTENTS

- Advanced - Defines the advanced settings for configuring deviceTRUST behavior.
- Auditing - Defines the audit events that are raised to the Windows Event Log.
- Custom Properties - Defines a script launched on Logon, Reconnect (or Unlock), and Service Start to initialise custom properties before context evaluation.
- File-Based Policy - Defines the behavior of file-based policy.
- Licensing - Defines your deviceTRUST license and the users managed by deviceTRUST.
- Mail Server - Defines the mail server used by the Send Mail task.
- Map Drive - Defines the retry and timeout settings for the Map Drive task.
- Microsoft AppLocker - Defines the Microsoft AppLocker policy to control the applications, installers and scripts that can be launched.
- Microsoft Entra ID - Defines the Tenant ID, Application (Client) ID and Secret required to manage Microsoft Entra ID.
- Mobile - Defines the mobile settings for managing iOS devices.
- Printer - Defines the printer management options and the retry and timeout settings for the Map Printer task.
- Property - Defines the collection, persistence, and settings of the properties.
- Security - Defines which external processes have permission to get or set properties, modify the registry, and invoke triggers.
- System Messages - Defines the messages shown when connecting to a user session or when access is denied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

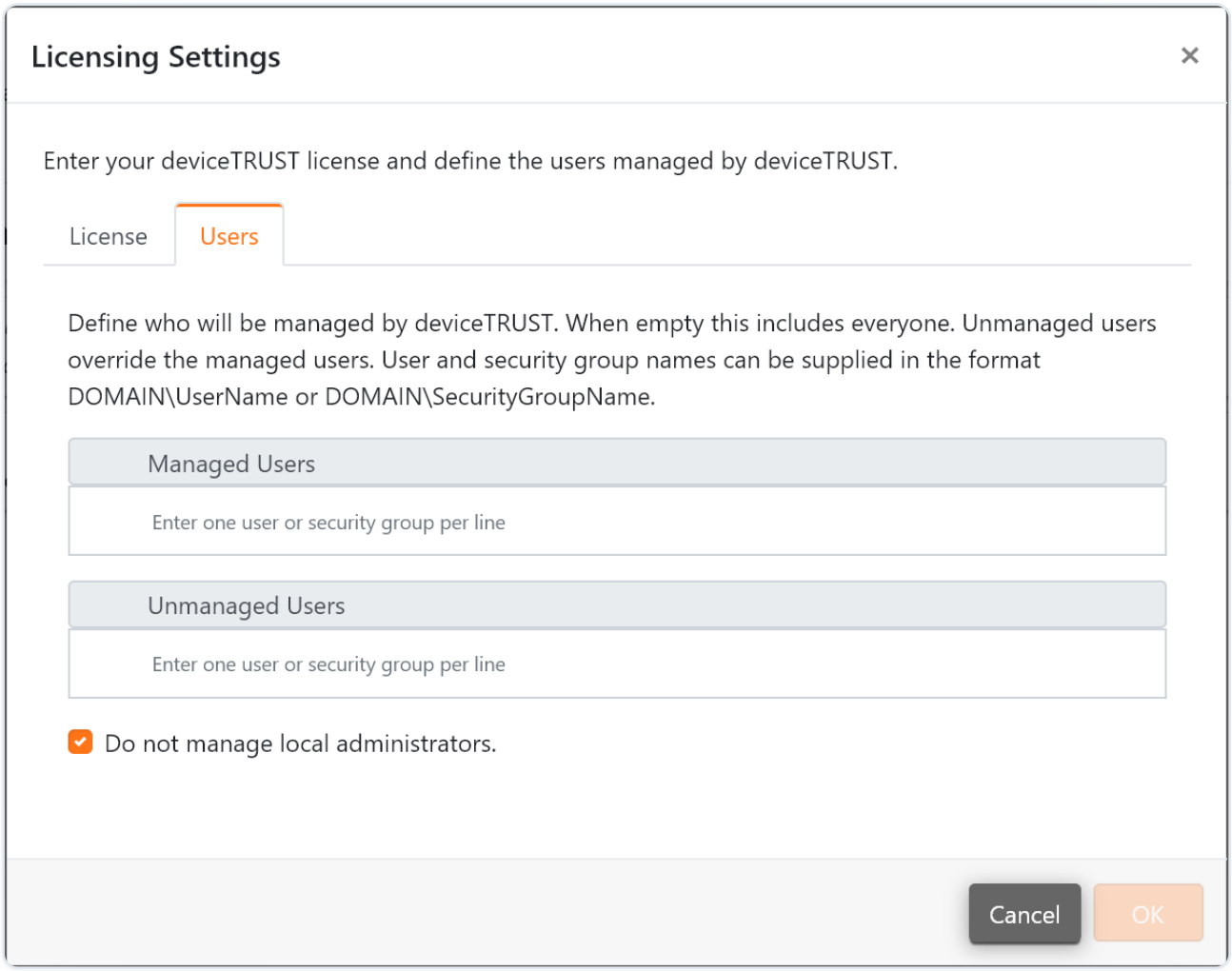
Licensing Settings

The `Licensing Settings` defines your deviceTRUST license and the users managed by deviceTRUST. The deviceTRUST product can be licensed by entering a license key within the `Enter your deviceTRUST license` text area.



By default deviceTRUST will manage all users except users within the Local Administators group. This can be configured by entering the security groups containing the users that deviceTRUST should manage. Local Administrators can be managed by deviceTRUST by unchecking the `Do not manage local administrators` checkbox.

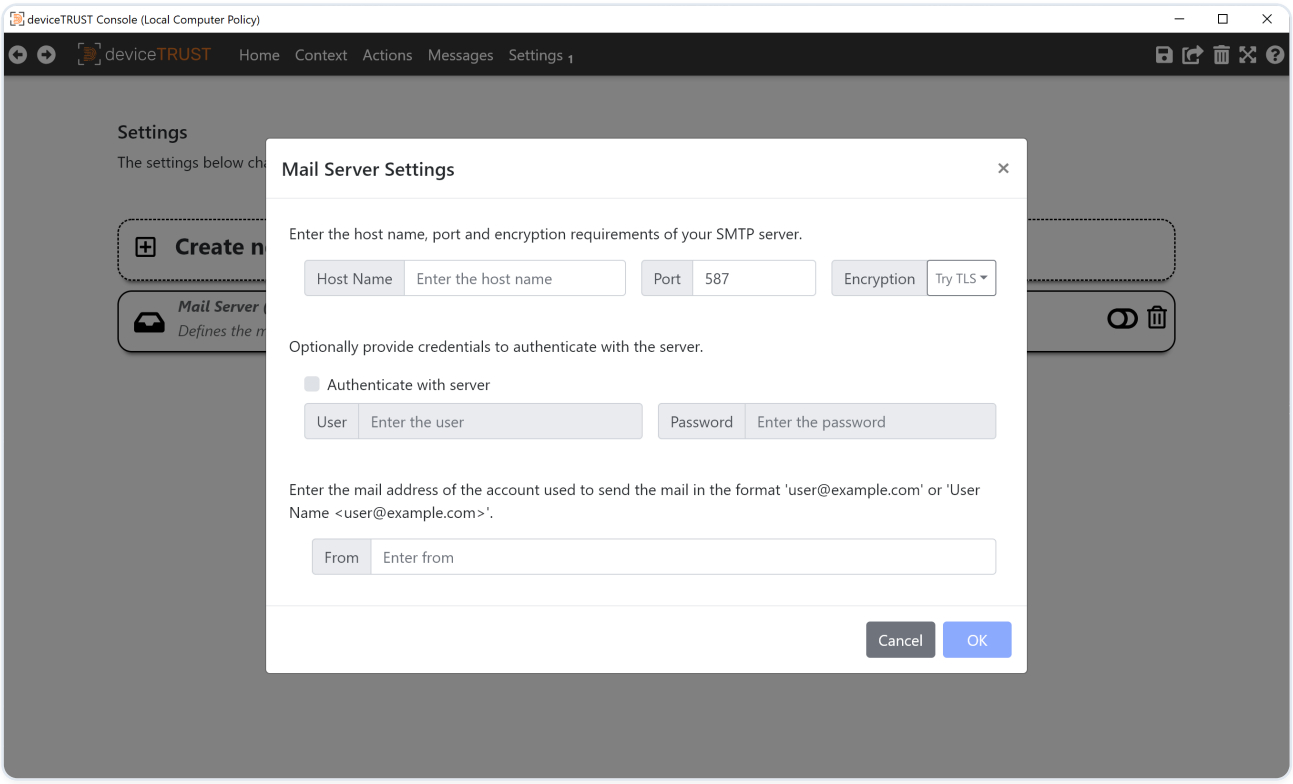
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Mail Server Settings

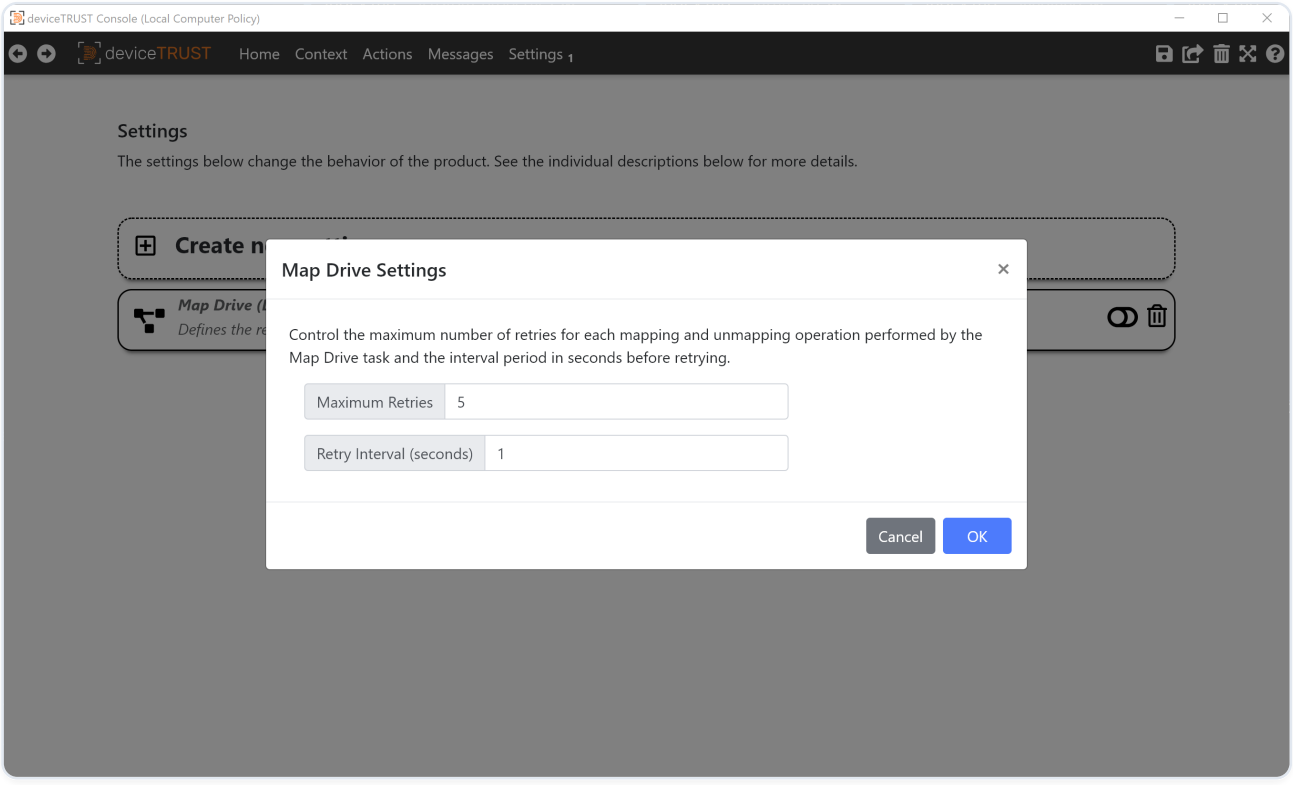
The `Mail Server Settings` defines the mail server used by the Send Mail task.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Drive Settings

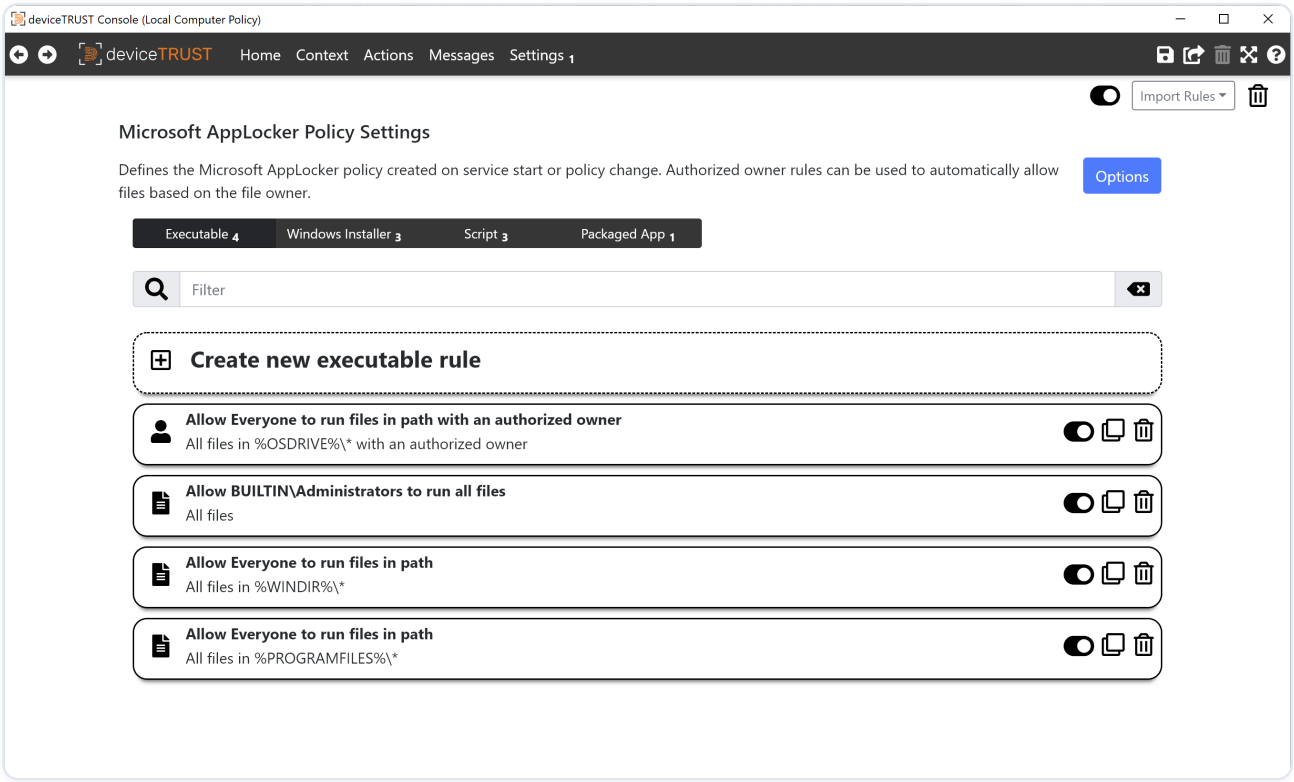
The `Map Drive Settings` define the retry and timeout settings for the Map Drive task.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft AppLocker Settings

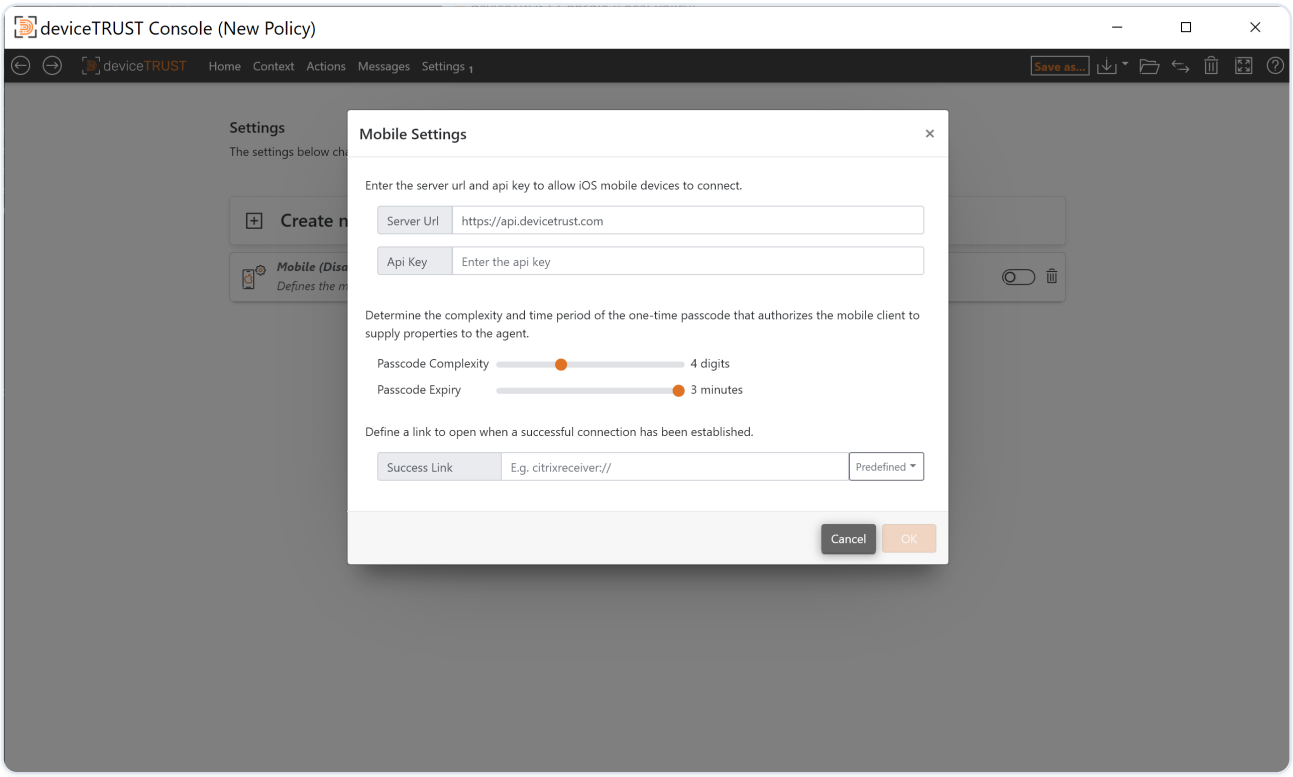
The `Microsoft AppLocker Settings` define the Microsoft AppLocker policy to control the applications, installers and scripts that can be launched.



Mobile Settings

The `Mobile Settings` define the mobile settings for managing iOS devices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following controls are available:

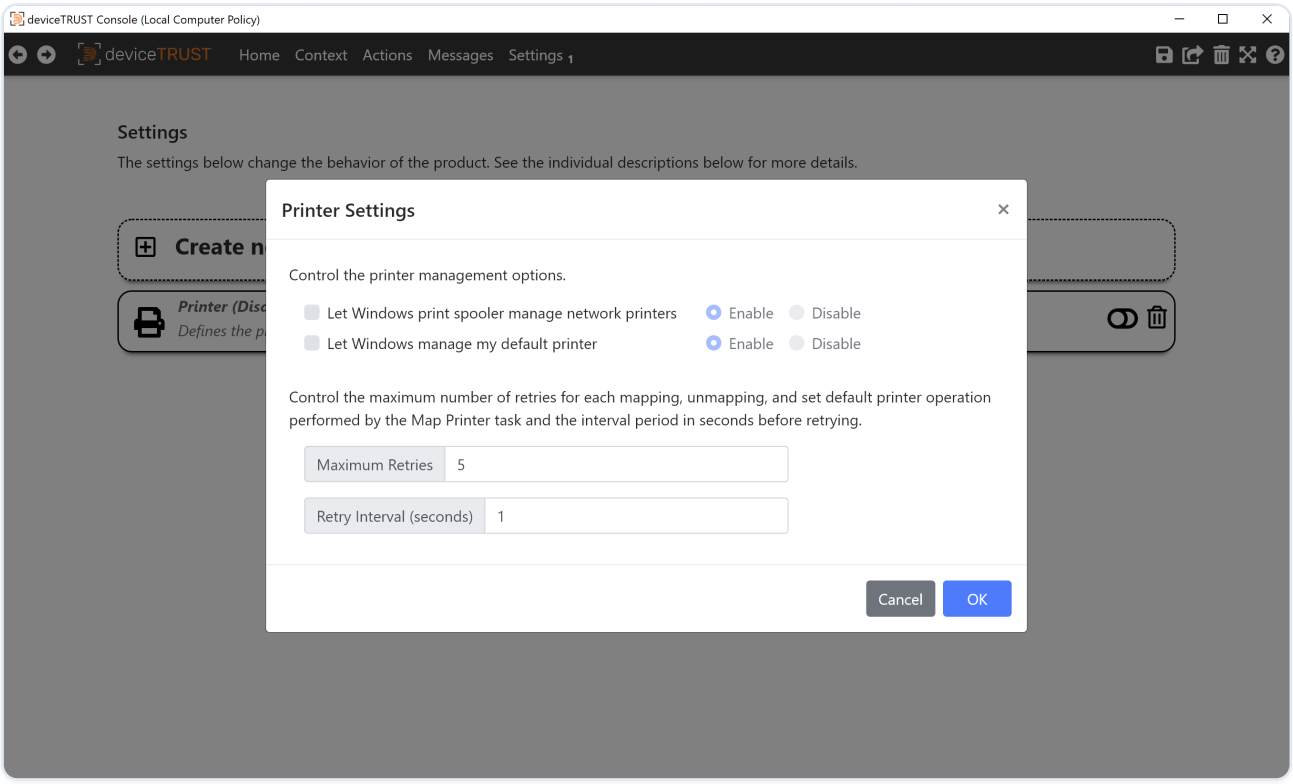
- *Server Url* - This is the URL used by the deviceTRUST® Agent to facilitate a connection to a remote iOS device. The default value should remain unchanged.
- *Api Key* - This is an API Key generated from the *App Registration* section of the deviceTRUST Portal.
- *Passcode Complexity* - Determines the number of digits displayed to the user when connecting from a remote iOS device.
- *Passcode Expiry* - Determines the length of time that the passcode remains valid allowing the user to enter their passcode.
- *Success Link* - Determines a URL that is invoked by the deviceTRUST Client Extension for iOS after successfully providing properties to the deviceTRUST Agent.

The *Success Link* can be used to seamlessly redirect the user back to their remoting client.

Printer Settings

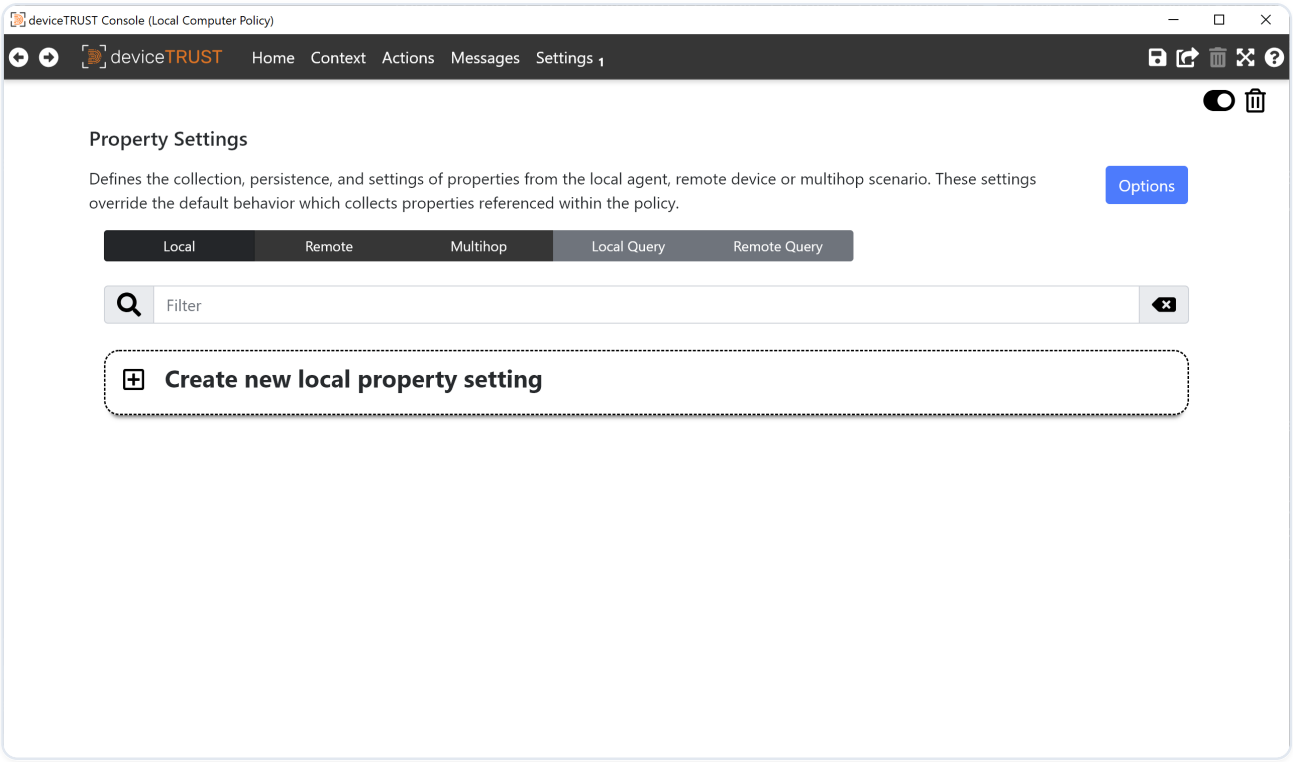
The `Printer Settings` define the printer management options and the retry and timeout settings for the Map Printer task.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Property Settings

The `Property Settings` defines the collection, persistence, and settings of properties from the local agent, remote device or multihop scenario. These settings override the default behavior which collects properties referenced within the policy. Additional options for Location, Security Product and Whois are also available.

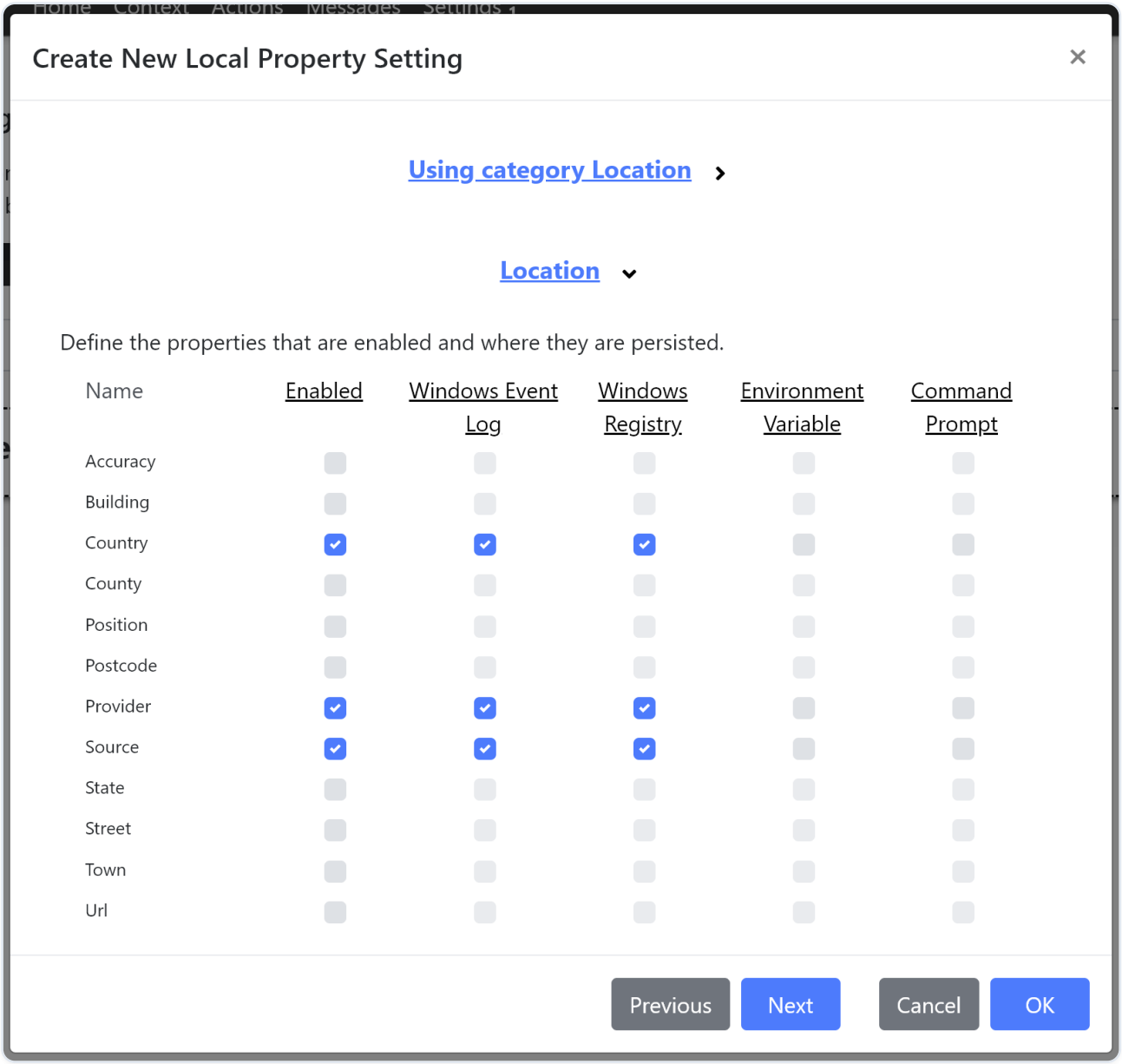


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Property Filters

A property filter can be used to determine which properties are collected from the local or remote device, and where they are persisted. By default, all properties that are referenced within a Context are collected from the local or remote device, and are persisted according to the settings defined within the `Options`.

Properties can be configured for the local agent by selecting the `Local` tab and clicking `Create new local property setting`. Alternatively, properties can be configured for the remote device by selecting the `Remote` tab and clicking `Create new remote property setting`.



The available properties for the selected category are listed on the left hand side. Each property can be selected to be collected and persisted by the deviceTRUST® Agent under the following headers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

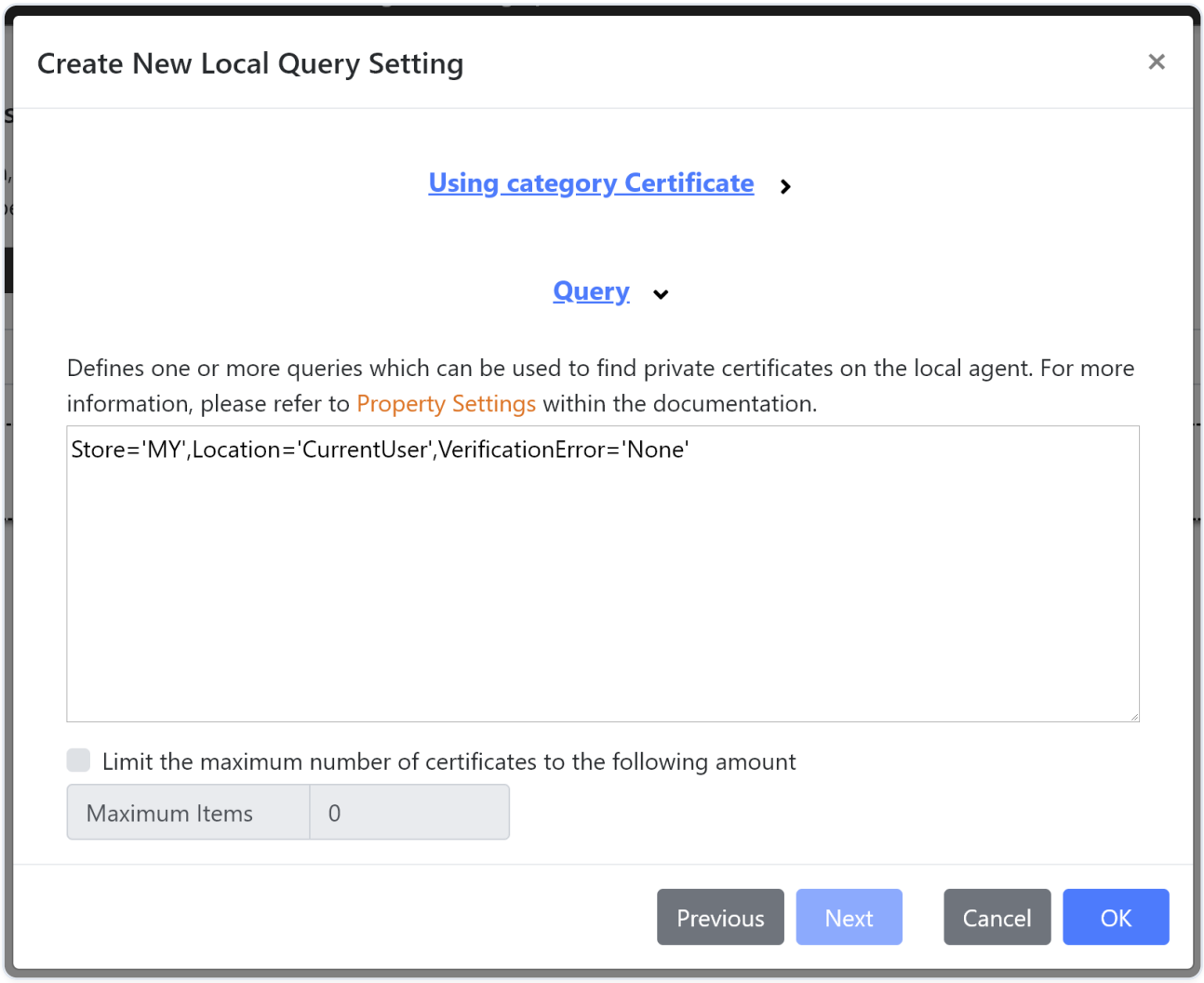
- `Enabled` - determines whether the property is collected from the device.
- `Windows Event Log` - determines whether the property is written to the Windows Event Log.
- `Windows Registry` - determines whether the property is written to the Windows Registry at `HKCU/Software/deviceTRUST/Properties`.
- `Environment Variable` - determines whether the property is available to other processes through an environment variable.
- `Command Prompt` - determines whether the property is available on the command prompt via a call to `dtcmd.exe GET`.

Property Queries

deviceTRUST provides a default query to provide specific displays, networks, access points, printers and certificates into the properties available for the local or remote device. However, the default queries may not be suitable, or may simply contain too much information. Therefore, the queries can be independently customized for both the local and remote device within the policy assigned to the agent.

Queries can be added for the local agent by selecting the `Local Query` tab and clicking `Create new local query`. Alternatively, queries can be added for the remote device by selecting the `Remote Query` tab and clicking `Create new remote query`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Queries consist of one or more query strings, each containing one or more constraints. All constraints within any of the query strings must be matched for an item to be included in the results. For example, take the following 2 printer query strings:

- Server='\\\\PRINTSERVER??', Name='Finance Printer'
- Default='true'

The first of the two queries in the example above includes 2 constraints. Server='\\\\PRINTSERVER??' ensures that printers returned from the first query have a server matching the wildcard expression, such as \\\\PRINTSERVER01. Name='Finance Printer' ensures that only printers matching the given name are returned. In the second query, Default='true' ensures that default printers are returned. Since printers will be returned if they match any of the statements, default printers will always be returned, even if they are not the 'Finance Printer'. Similarly, finance printers will be returned even if they are not the default printer.

The constraints available to a query depend upon whether it is targeting displays, networks, access points, printers or certificates. The operations available to a constraint depend upon the underlying data type. For example, the name of a printer is textual, hence string comparisons can be

© 1997–2026 Citrix Systems, Inc. All rights reserved.

performed using wildcard characters. Alternatively, the speed of a network is numeric, hence comparisons can be made against a number.

Access Point Queries

Access Point queries can be used to discover access points on the local or remote device. The following constraints are supported:

- Text constraints for SSID and BSSID.
- Number constraints for Strength, Quality and Frequency.
- Boolean constraint for Secure.

For example:

- SSID=’MyAccessPoint’, Strength>=’-50’ – Matches access points with the SSID ‘MyAccessPoint’ and a RSSI strength greater than -50.
- Secure=’true’ – Matches all secure access points.

By default, no access points are queried.

Certificate Queries

Certificate queries can be used to discover certificates on the local or remote device. The following constraints are available:

- Text constraints for Store, Name, Subject, Issuer, SignatureAlgorithm, SerialNumber, ThumbprintSha1, Template, ExtendedUsage, RootName and RootThumbprintSha1.
- Enum constraint for Location with values CurrentUser and LocalMachine.
- Enum constraint for Version with values V1, V2 and V3.
- Enum constraint for VerificationError with values None, CannotBeVerified, Revoked, UntrustedRoot, UntrustedTestRoot, Chaining, Expired, Critical and NoRevocationCheck.
- Enum constraint for Usage with values EncipherOnly, CrlSigning, CertificateSigning, KeyAgreement, DataEncipherment, KeyEncipherment, NonReduiation, DigitalSignature and DecipherOnly.
- Date constraints for NotBefore and NotAfter.

For example:

- Template='*CompanyCert*', ExtendedUsage='*1.3.6.1.5.5.7.3.2*' - All certificates assigned by a template containing the name 'CompanyCert' for use with client authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VerificationError='*' - All certificates, regardless of their verification errors.
- VerificationError='None;Expired', Issuer='*TrustedAuthority*' - All valid or expired certificates whose issuer contains the text 'TrustedAuthority'.

The default value is ''Store='My', Location='CurrentUser', VerificationError='None'''. Store defaults to 'My' unless specified. Location defaults to 'CurrentUser' unless specified. VerificationError defaults to 'None' unless specified.

Display Queries

Display queries can be used to discover the displays on the local or remote device. The following constraints are supported:

- Text constraint for Name.
- Number constraints for Width, Height and Bpp.

For example:

- Width>='1024', Height>='768' queries all displays which have a width greater than or equal to 1024 pixels, and a height greater than or equal to 768.

By default, all displays are queried.

Firewall Queries

Unlike other queries, the firewall queries are used to exclude firewall rules from the local or remote device. The following constraints are available:

- Text constraints for Name, Description, Group, Program, Service, Package, PackageName, PackageDescription, PackageFullName and PortName.
- Enum constraint for Type with values Program, Package, Service, System and Any.
- Enum constraint for Direction with values Inbound and Outbound.
- Enum constraint for Protocol with values Any, HOPOPT, ICMPv4, IGMP, TCP, UDP, IPv6, IPv6Route, IPv6Frag, GRE, ICMPv6, IPv6NoNxt, IPv6Opts, VRRP, PGM, L2TP, or any protocol number from IANA protocol numbers.
- Enum constraint for Profile with values Domain, Private, Public.
- Number constraints for Port, with additional option to use * to match rules that target any port.

For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Direction='Inbound', Program='*\MyApp.exe', Port>=3000, Port<=3002 - Excludes all inbound traffic to MyApp.exe to ports 3000, 3001 and 3002. The default value does not filter the Firewall rules.

Logical Disk Queries

Logical Disk queries can be used to filter the logical disks that are discovered on the local or remote device. The following constraints are available:

- Enum constraint for Type with values Removable, Fixed, Cdrom and Ramdisk.
- Enum constraint for Flags with values NotReady, PreservedNames, CaseSensitiveSearch, DaxVolume, SupportsCompression, NamedStreams, PersistentAcls, ReadOnly, SequentialWriteOnce, SupportsEncryption, ExtendedAttributes, HardLinks, ObjectIds, OpenByFileId, ReparsePoints, SparseFiles, Transactions, UsnJournal, UnicodeFileNames, IsCompressed, SupportsQuotas.
- Text constraints for Label, FileSystem, Drive and Path.
- Number constraints for TotalMB and FreeMb.
- Boolean constraints for Encrypted.

For example:

- Drive='D:,E:,F:,G:' - Returns any drive mapped to letters D, E, F or G.
- Type='Removable' - Returns only removable disks.

The default value returns all logical disks represented by a drive letter (e.g. Flags!='NotReady', Drive!='').

Mapped Drive Queries

Mapped Drive queries can be used to filter the mapped drives that are discovered on the local or remote device. The following constraints are available:

- Text constraints for Drive, Server, Share, User and Provider.

For example:

- Drive='D:' - Returns any drives mapped to a local D:.
- User='DOMAIN*' - Returns any mapped drives authenticated by a member of the 'DOMAIN' domain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Server='\\\\SERVERNAME' - Returns any mapped drives using a remote server name of '\\\\SERVERNAME'.

The default value returns all mapped drives.

Network Queries

Network queries can be used to discover networks on the local or remote device. The following constraints are supported:

- Text constraints for Name, Description, Mac, GatewayMac, WifiSsid, WifiBssid, WifiSecurity and DnsSuffix.
- Enum constraint for Status with values Up, Down, Testing, Unknown, Dormant, NotPresent and LowerLayerDown.
- Enum constraint for Type with values Other, Ethernet, TokenRing, PPP, SoftwareLoopback, ATM, WiFi, Tunnel, Firewire and Mobile.
- Enum constraint for Category with values Public, Private and Domain.
- Boolean constraint for DhcpEnabled.
- Number constraints for Speed and WifiStrength.
- IpAddress constraints for IP, Gateway, DNS, WINS and DhcpServer.

For example:

- DhcpEnabled='true', DhcpServer='192.168.100.1-2', GatewayMac='01-02-03-04-05-06-07' - Matches networks assigned an ip address from a DHCP Server of address 192.168.100.1 or 192.168.100.2 configured with a gateway using MAC address 01-02-03-04-05-06-07.

The default value is "Status='Up', Type='Ethernet;WiFi'". Status defaults to 'Up' unless specified and type defaults to 'Ethernet;WiFi' unless specified.

Printer Queries

Printer queries can be used to discover printers on the local or remote device. The following constraints are available:

- Text constraints for Name, Server, Share, Port, Location, Driver, DriverFile and DriverManufacturer.
- Boolean constraint for Default, Local, DirectoryPublished and KeepPrintJobs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enum constraint for Errors with values Paused, Error, PendingDeletion, PaperJam, PaperOut, PaperProblem, Offline, OutputBinFull, NotAvailable, TonerLow, NoToner, CannotPrintPage, UserIntervention, OutOfMemory, DoorOpen, ServerUnknown, ServerOffline and DriverUpdateNeeded.
- Version constraint for DriverVersion.

For example:

- Default='true' - Returns just the default printer.
- Share='\\\\SERVER??*', Errors='*' - Returns printers which have a share matching the wildcard '\\\\SERVER??*' regardless of the error value.

The default value is ''Errors!='Offline;ServerOffline;NotAvailable'''. Errors defaults to all values except 'Offline;ServerOffline;NotAvailable' unless specified.

Security Product Queries

Defines queries which can be used to limit the security products. The following constraints are available:

- Text constraint for Name.
- Enum constraint for Category with values AntiVirus, AntiSpyware and Firewall.
- Enum constraint for Status with values Active, Out-Of-Date and Inactive.
- Date constraint for Timestamp.

For example:

- Status=’Active’, Category=’AntiVirus’ - Queries all AntiVirus security products with a status of Active. For full details, please see deviceTRUST Property Queries within the deviceTRUST Administration Guide.

The default query includes all security products.

Text Constraints

Text constraints are used to match textual properties of an item, such as a name or description. The text is case insensitive and must match in full. Operators of equals ‘=’ and not equals ‘!=’ are supported. The asterisk ‘*’ wildcard character matches zero or more unspecified characters, and the question mark ‘?’ character matches a single digit. Multiple text matches can be specified by separating them with a semi-colon ‘;’.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example:

- Name=’ABC*’ – matches any name starting with ABC, such as ABC, ABCD, ABCDE, abc, etc.
- Name=’*ABC*’ – matches any name containing ABC, such as ABC, ABCD, 1234ABCD, etc.
- Name=’A?C’ – matches any name with 3 digits, starting with A and ending in C, such as AAC, ABC, ADC, etc.
- Name!=’*ABC*’ – matches any name which does not contain ABC, such as AB, ABD, etc.
- Name=’*ABC*;*XYZ*’ – matches any name which contains the text ABC or DEF, such as 1234ABCD or XYZ987, etc.

Enumeration (Enum) Constraints

Enum constraints are used to match properties which have a predefined set of potential values, such as a network type which can be Ethernet, WiFi, Mobile, etc. The values which can be contained within the property are specific to each property. Operators of equals ‘=’ and not equals ‘!=’ are supported. The asterisk ‘*’ wildcard can be used to match any value, which becomes useful to override the default behavior of a constraint. Multiple enum matches can be specified by separating them with a semi-colon ‘;’.

For example:

- Type=’WiFi’ – matches a type of WiFi.
- Type=’WiFi;Ethernet’ – matches a type of WiFi or Ethernet.
- Type!=’WiFi’ – matches any type which is not WiFi.
- Type!=’WiFi;Ethernet’ – matches a type which is neither WiFi or Ethernet.
- Type=’*’ – matches any type.

Number Constraints

Number constraints are used to match properties which are numeric, such as the speed of a network. The following operators are supported:

- Equals ‘=’ – matches the number exactly.
- Not Equals ‘!=’ – matches all numbers except the one specified.
- Greater Than ‘>’ – matches all number greater but not equal to that specified.
- Greater Than or Equals ‘>=’ – matches all numbers greater than or equal to the one specified.
- Less Than ‘<’ – matches all numbers less but not equal to the one specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Less Than or Equals ‘<=’ – matches all numbers less than or equals to that specified.

Constraints can be specified multiple times to form range constraints.

For example:

- Speed=’1000’ – matches the speed when it is equal to 1000.
- Speed>=’1000’ – matches the speed when it is greater than or equal to 1000.
- Speed>=’1000’, Speed<’2000’ – matches the speed between the range 1000 and 1999.

Date Constraints

Date constraints are used to match properties which represent a date, such as the NotBefore and NotAfter properties of a certificate. Date constraints support the same operators as the number constraints. Dates can either be specified as a specific RFC2822 or ISO 8601 date string, such as ‘2016-03-21’, as a positive or negative number representing the number of days relative to the current date. Constraints can be specified multiple times to form range constraints.

For example:

- Expiry=’2016-03-21’ – matches the expiry of 21st March 2016.
- Expiry>=’2016-03-21’ – matches any expiry greater than or equals to 21st March 2016.
- Expiry>=’2016-03-21’, Expiry<’2017-03-21’ – matches any expiry between the dates of 21st March 2016 and 20th March 2017.
- Expiry=’1’ – matches the expiry of tomorrow.
- Expiry>’0’, Expiry<=’7’ – matches any expiry in the next week.
- Expiry<’0’, Expiry>=’-7’ – matches any expiry in the past week.

Boolean Constraints

Boolean constraints are used to match properties which can only be ‘true’ or ‘false’. Operators of equals ‘=’ and not equals ‘!=’ are supported, and values of ‘true’, ‘false’ and asterisk ‘*’ to match any value.

For example:

- Default=’true’ – matches the default of true.
- Default=’false’ – matches the default of false.
- Default=’*’ – matches either true or false.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IpAddress Constraints

IpAddress constraints are used to match properties which represent one or more IP addresses, such as a network's IP or Gateway. Operators of equals '=' and not equals '!=' are supported. Values can be either IPv4 or IPv6 addresses, and are only compared for the level of detail supplied in the constraint. For example, '192.168' will match any address starting with 192.168. An asterisk '*' can be supplied to match any digit within the address, and a dash '-' can be used to define a valid range of numbers.

For example:

- IP='192.168.100.1' – matches the exact address 192.168.100.1.
- IP='192.168' – matches any address starting with 192.168, such as 192.168.100.1.
- IP='192.168.*.1' – matches any address starting with 192.168 and ending in 1.
- IP='192.168.100.1-2' – matches the addresses 192.168.100.1 and 192.168.100.2.
- IP!='192.168.100.1-2' – matches all addresses except 192.168.100.1 and 192.168.100.2.

Version Constraints

Version constraints are used to match properties which represent a dot '.' delimited version number, such as the printer driver's version number. Operators of equals '=' and not equals '!=' are supported. Values are compared for the level of detail supplied in the constraint. For example, '18.1' will match any version starting with 18.1. An asterisk '*' can be supplied to match any digit within the version number, and a dash '-' can be used to define a valid range of numbers.

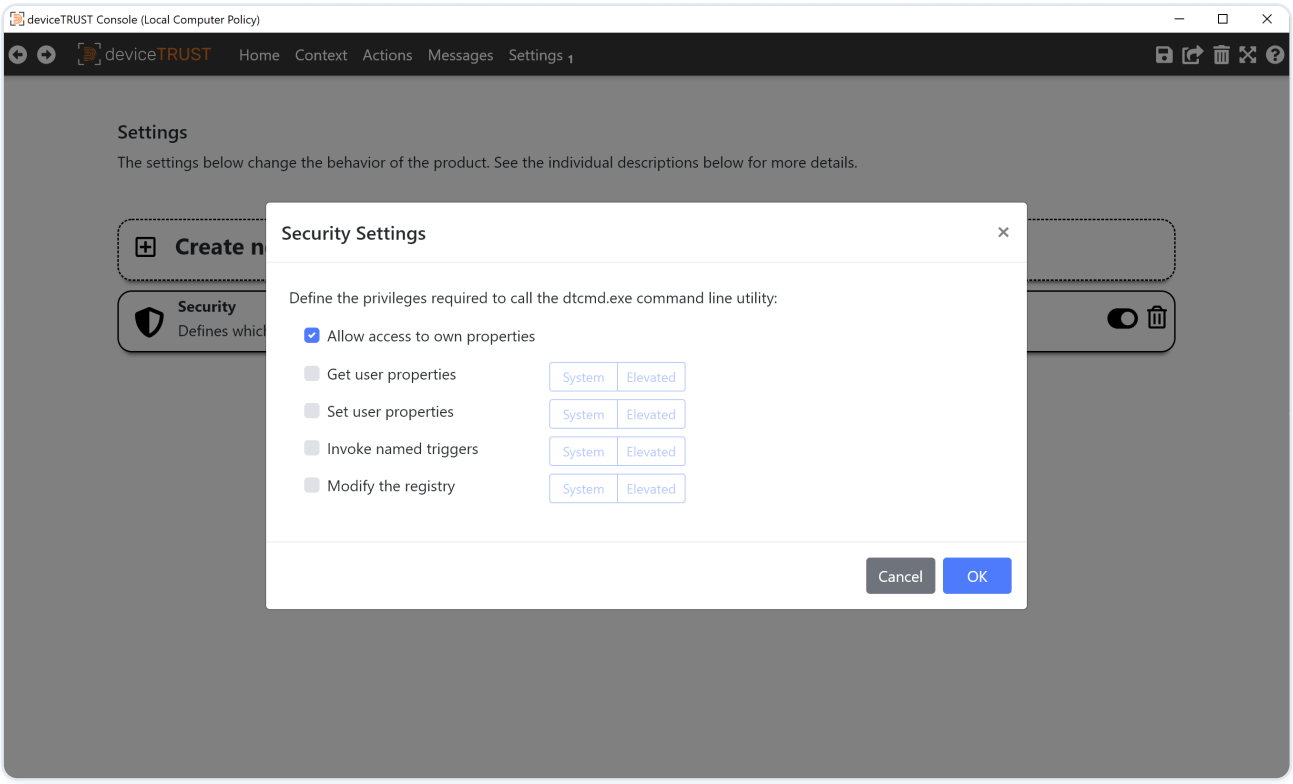
For example:

- Version='18.1.100.0' – matches the exact version 18.1.100.0.
- Version='18.1' – matches any version starting with 18.1.
- Version='18.1.*.0' – matches any version starting with 18.1 and ending in 0.
- Version='18.1.100-200.0' – matches any version starting with 18.1, having a third digit between 100 and 200, and a fourth digit of zero.
- Version!='18.1' – matches any version which doesn't start with 18.1.

Security Settings

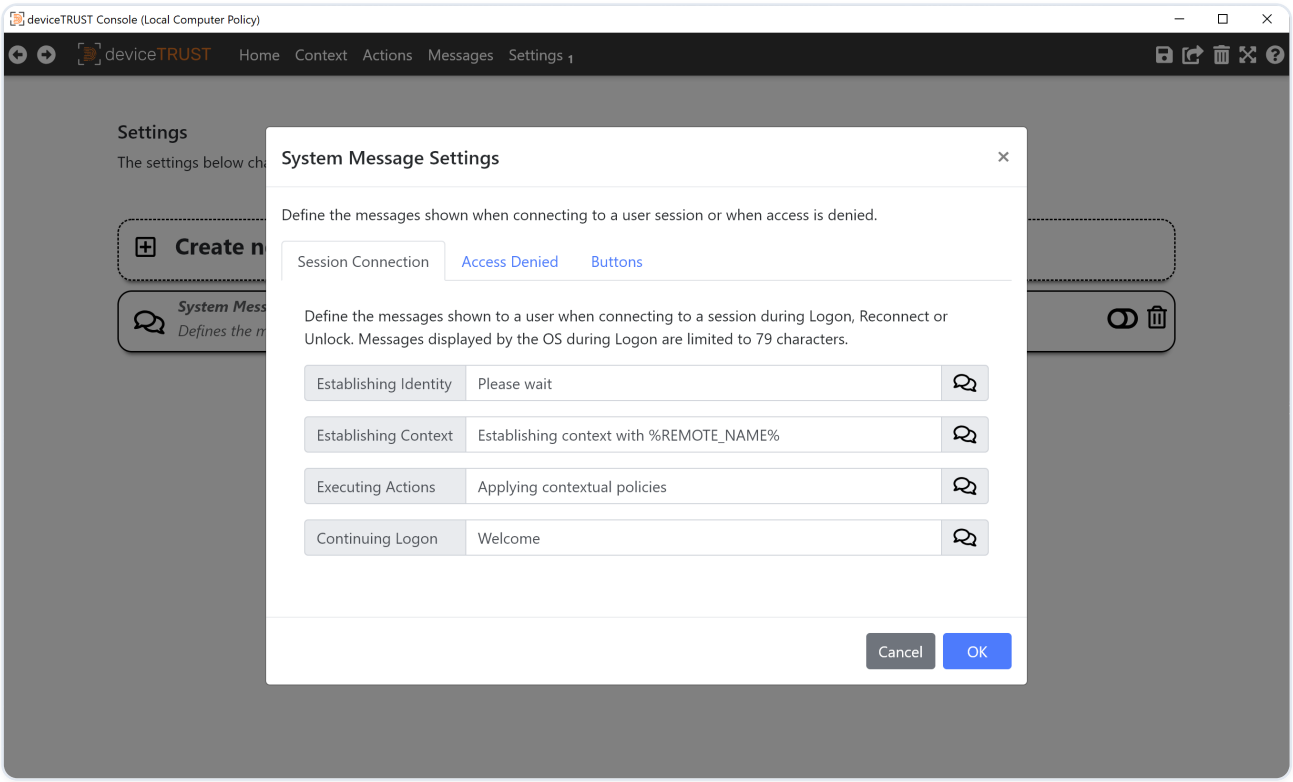
The `Security Settings` defines which external processes have permission to get or set properties, modify the registry, and invoke triggers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



System Messages Settings

The `System Messages Settings` defines the messages shown when connecting to a user session or when access is denied.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Point Properties

ACCESS POINT	AGENT	CLIENT EXTENSION							
Describes the available Wi-Fi access points.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
BSSID									
The Basic Service Set Identifier (BSSID) of the access point. Dynamic property with text data type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
Persists as LOCAL_ACCESSPOINT_X_BSSID for the local agent and REMOTE_ACCESSPOINT_X_BSSID for the remote device.									
Count									
The number of available acce	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
ss points. Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_COUNT for the local agent and REMOTE_ACCESSPOINT_COUNT for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
remote device.									
Frequency									
The frequency of the response received from the access point, measured in kilohertz (kHz). Dynamic property with number data type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
Persists as LOCAL_ACCESSPOINT_X_FREQUENCY for the local agent and REMOTE_ACCESSPOINT_X_FREQUENCY for the remote device.									
Quality									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
The link quality measured as a percentage, with 100 being the highest link quality. Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_X_QUALITY	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
for the local agent and REMOTE_ACCESSPOINT_X_QUALITY for the remote device.									
Secure									
Set to true if the access point is secured. Dynamic property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
boolean data type. Persists as LOCAL_ACCESSPOINT_X_SECURE for the local agent and REMOTE_ACCESSPOINT_X_SECURE for the remote device.									
SSID									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
The Service Set Identifier (SSID) of the access point. Dynamic property with text data type. Persists as LOCAL_ACCESSPOINT_X_SSID for the local agent and REMOTE	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
_ACCESSPOINT_X_SSID for the remote device.									
Strength									
The Received Signal Strength Indicator (RSSI) value measured in units of decibels referenced to 1.0	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
milliwatts (dBm). Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_X_STRENGTH for the local agent and REMOTE_ACCESSPOINT_X_STRENG									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACCESS POINT	AGENT	CLIENT EXTENSION							
TH for the remote device.									

Browser Properties

BROWSER	AGENT	CLIENT EXTENSION							
Describes installed internet browsers.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Count									
The number of internet browsers. Realtime	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
property with number data type. Persists as `LOCAL_BROWSER_COUNT` for the local agent and `REMOTE_BROWSER_COUNT` for the remote device.									
Default									
Determine	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
s whether the browser is the default. Realtime property with boolean data type. Persists as `LOCAL_BROWSER_X_DEFAULT` for the local agent and `REMOTE_BROWSER_X_DE`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
`FAULT` for the remote device.									
File Path									
The file path of the internet browser executable. Realtime property with text data type. Persists as `LOCAL_BROWS`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
`ER_X_FILE_PATH` for the local agent and `REMOTE_BROWSER_X_FILE_PATH` for the remote device.									
Name									
The name of the internet browser. Realtime property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_BROWSER_X_NAME` for the local agent and `REMOTE_BROWSER_X_NAME` for the remote device.									
Version									
The version of the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
internet browser executable. Realtime property with version data type. Persists as `LOCAL_BROWSER_X_VERSION` for the local agent and `REMOTE_BROWSER_X_VERSION` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BROWSER	AGENT	CLIENT EXTENSION							
the remote device.									

Cellular Properties

CELLULAR	AGENT	CLIENT EXTENSION							
Describes the active cellular capabilities of an endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Class									
The cellular data class of the activ	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
e connection to the network provider. Realtime property with enum, text data types with options GPRS, EDGE, UTMS, HSDPA, HSUPA, HSPA, HSPA+, LTE, WCD									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
MA, 1xRTT, 1xEVDO, 1xEVDV, 3xRTT, UMB, HRPD, NRNSA, NRSA. Persists as `LOCAL_CELLULAR_CLASS` for the local agent and `REMOTE_CELLULAR_CLASS` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
remote device.									
Country									
The ISO-3166 country name of the country where the connected network provider resides. This value is only available for GSM devices. Realti	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
me property with text data type. Persists as `LOCAL_CELLULAR_COUNTRY` for the local agent and `REMOTE_CELLULAR_COUNTRY` for the remote device.									
Country Code									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION						
The mobile country code (MCC) of the connected network provider. This value is only available for GSM devices. Realtime property with number data type. Persists as	✓	✓		✓				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
`LOCAL_CELLULAR_COUNTRY_CODE` for the local agent and `REMOTE_CELLULAR_COUNTRY_CODE` for the remote device.									
ID									
For GSM devices, this is the 15 digit IMEI	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
number. For CDMA devices, this is the 11 digit ESN or the 17 digit MEID. Realtime property with text data type. Persists as `LOCAL_CELLULAR_ID` for the local agent									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
and `REMOTE_CELLULAR_ID` for the remote device.									
Network Code									
The mobile network code (MNC) of the connected network provider. This value is only avail	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
able for GSM devices. Realtime property with number data type. Persists as `LOCAL_CELLULAR_NETWORK_CODE` for the local agent and `REMOTE_CELLULAR_NETWORK_CODE` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
the remote device.									
Network Name									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION						
The name of the connected network provider. Realtime property with text data type. Persists as `LOCAL_CELLULAR_NETWORK` for the local agent and `REMOTE_CELLULAR_NETWORK`	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
for the remote device.									
Product									
The product name of the device providing the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLU`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
`LAR_PRODUCT` for the local agent and `REMOTE_CELLULAR_PRODUCT` for the remote device.									
Roaming									
Determines whether the connected network provider is differ	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION
ent to the home provider defined by the SIM. Realtime property with boolean data type. Persists as `LOCAL_CELLULAR_ROAMING` for the local agent and `REMOTE_CELLULAR_ROA`		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
`MING` for the remote device.									
Type									
The cellular communication type supported by the device. Realtime property with enum data type with options GSM, CDMA.	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_CELLULAR_TYPE` for the local agent and `REMOTE_CELLULAR_TYPE` for the remote device.									
Vendor									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
The vendor name of the device providing the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLULAR_VENDOR` for the local agent and `REM`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CELLULAR	AGENT	CLIENT EXTENSION							
`OTE_CELLULAR_VENDOR` for the remote device.									

Certificate Properties

CERTIFICATE	AGENT	CLIENT EXTENSION							
Describes the private certificates available within the user's certificate store.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
Count									
The number of installed certificates. Dynamic property with number data type. Persists as `LOCAL_CERTIFICATE_COUNT` for the local agent and `REMOTE_CERT`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
`IFICATE_COUNT` for the remote device.									
Extended Usage									
The valid extended usages of the certificate. Dynamic property with text data type. Persists as `LOC`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
`AL_CERTIFICATE_X_EXTENDEDUSAGE` for the local agent and `REMOTE_CERTIFICATE_X_EXTENDEDUSAGE` for the remote device.									
Issuer									
The name of the certificate	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
authority that issued the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_ISSUER` for the local agent and `REMOTE_CERTIFICATE_X_ISSUER`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
for the remote device.									
Location									
The location of the certificate, such as 'CurrentUser'. Dynamic property with enum data type with options Current User, Local Machine.	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_CERTIFICATE_X_LOCATION` for the local agent and `REMOTE_CERTIFICATE_X_LOCATION` for the remote device.									
Name									
The name of the certifi	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
cate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_NAME` for the local agent and `REMOTE_CERTIFICATE_X_NAME` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION						
Not After								
The date after which the certificate expires. Dynamic property with datetime data type. Persists as `LOCAL_CERTIFICATE_X_NOTAFTER` for the local agent and `REM`	✓	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
`OTE_CERTIFICATE_X_NOTAFTER` for the remote device.									
Not Before									
The date after which the certificate becomes valid. Dynamic property with datetime data type.	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_CERTIFICATE_X_NOTBEFORE` for the local agent and `REMOTE_CERTIFICATE_X_NOTBEFORE` for the remote device.									
Policies									
The certificate	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
policies identifying the intended purpose of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_POLICIES` for the local agent and `REMOTE_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
`CERTIFICATE_X_POLICIES` for the remote device.									
Root Name									
The root name of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTI`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
`FICATE_X_ROOT_NAME` for the local agent and `REMOTE_CERTIFICATE_X_ROOT_NAME` for the remote device.									
Thumbprint SHA256									
The SHA256 Thumbprint of the certifi	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
cate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_THUMBPRINT_SHA256` for the local agent and `REMOTE_CERTIFICATE_X_THUMBPRINT_SHA256`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
for the remote device.									
Usage									
The valid usages of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_USAGE` for the	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_CERTIFICATE_X_USAGE` for the remote device.									
Verification Error									
Describes why the certificate failed verification. Dynamic property with	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
enum data type with options None, Cannot Be Verified, Revoked, Untrusted Root, Untrusted Test Root, Chaining, Wrong Usage, Expired, Invalid Name, Invalid Policy,									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
Basic Constraints, Critical, Validity Period Nesting, No Revocation Check, Revocation Offline. Persists as `LOCAL_CERTIFICATE_X_VERIFICATIONERROR` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_CERTIFICATE_X_VERIFICATIONERROR` for the remote device.									
Version									
The x509 format version of the certificate. Dynamic property	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
with enum data type with options Version 1, Version 2, Version 3. Persists as `LOCAL_CERTIFICATE_X_VERSION` for the local agent and `REMOTE_CERTIFICATE_X_VERSION` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CERTIFICATE	AGENT	CLIENT EXTENSION							
remote device.									

ChromeOS Properties

CHROME OS	AGENT	CLIENT EXTENSION							
Provides properties unique to a Google ChromeOS device.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Asset ID									
The administrator-annotated Asset						✓			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHROME OS	AGENT	CLIENT EXTENSION							
ID. Static property with text data type. Persists as `REMOTE_CHROMEOS_ASSETID` for the remote device.									
Directory Device ID									
The directory device ID. Static property						✓			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHROME OS	AGENT	CLIENT EXTENSION							
with text data type. Persists as `REMOTE_CHROMEOS_DIRECTORYDEVICEID` for the remote device.									
Location									
The administrator-annotated Location. Static property						✓			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHROME OS	AGENT	CLIENT EXTENSION							
with text data type. Persists as `REMOTE_CHROMEOS_LOCATION` for the remote device.									

Custom Properties

CUSTOM	AGENT	CLIENT EXTENSION							
Provides a condition that can operate on any	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CUSTOM	AGENT	CLIENT EXTENSION							
property, including custom properties created using `dtcmd.exe`.									
Condition									
This is a placeholder custom property to allow the creation of a custom condition. This text	✓	✓			✓		✓	✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CUSTOM	AGENT	CLIENT EXTENSION							
does not appear within the console. Realtime property with text, number, boolean, datetime, ip, position data types. Persists as `LOCAL_CUSTOM_CONDITION` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CUSTOM	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_CUSTOM_CONDITION` for the remote device.									

deviceTRUST Properties

DEVICETRUST	AGENT	CLIENT EXTENSION							
Provides information about whether a connection to a deviceTR	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
UST Client Extension has been established, the version of the deviceTRUST software and the status of the deviceTRUST license.									
Connected									
Determines whether the devic	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION
eTRUST Agent has established a connection with the deviceTRUST Client Extension. Static property with boolean data type. Persists as `LOCAL_DEVICETRUST_CONNECTED` for		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
the local agent.									
License Count									
Determines the number of deviceTRUST licensed units. Static property with number data type. Persists as `LOCAL_DEVICETRUST_L`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
`ICENSE_COUNT` for the local agent.									
License Expiry Date									
Determines the date that the deviceTRUST license expires. Static property with datetime data type. Persists	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
as `LOCAL_DEVICETRUST_LICENSE_EXPIRYDATE` for the local agent.									
License Issue Date									
Determines the date that the deviceTRUST license was issued. Static prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
rty with datetime data type. Persists as `LOCAL_DEVICETRUST_LICENSE_ISSUEDATE` for the local agent.									
License Type									
Determines the deviceTRUST license type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
Static property with text data type. Persists as `LOCAL_DEVICETRUST_LICENSE_TYPE` for the local agent.									
License Unit									
Determines the deviceTRUST licensable unit,	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
e.g., a User or Device. Static property with enum data type with options User, Device, Unlimited. Persists as `LOCAL_DEVICETRUST_LICENSE_UNIT` for the local agent.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
License Valid									
Determines whether the deviceTRUST license is valid. Static property with boolean data type. Persists as `LOCAL_DEVICETRUST_LICENSE_VALID` for the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
local agent.									
Version									
The version of the deviceTRUST software. Static property with version data type. Persists as `LOCAL_DEVICETRUST_VERSION` for the local	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DEVICETRUST	AGENT	CLIENT EXTENSION							
agent and `REMOTE_DEVICETRUST_VERSION` for the remote device.									

Display Properties

DISPLAY	AGENT	CLIENT EXTENSION							
Describes the displays available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
Adapter Product									
The product name of the display adapter. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_ADAPTER_PRODUCT` for the local agent	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
and `REMOTE_DISPLAY_X_ADAPTER_PRODUCT` for the remote device.									
Adapter Vendor									
The vendor of the display adapter. Realtime property with text data type.	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_DISPLAY_X_ADAPTER_VENDOR` for the local agent and `REMOTE_DISPLAY_X_ADAPTER_VENDOR` for the remote device.									
BPP									
The number of bits	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
per pixel. Realtime property with number data type. Persists as `LOCAL_DISPLAY_X_BPP` for the local agent and `REMOTE_DISPLAY_X_BPP` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
Count									
The number of displays. Realtime property with number data type. Persists as `LOCAL_DISPLAY_COUNT` for the local agent and `REMOTE_DISPLAY_COUNT` for the	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
remote device.									
DPI									
The number of dots per inch. Realtime property with number data type. Persists as `LOCAL_DISPLAY_X_DPI` for the local agent and `REMOTE_`	✓	✓	✓		✓		✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
`DISPLAY_X_DPI` for the remote device.									
Height									
The height of the screen in pixels. Realtime property with number data type. Persists as `LOCAL_DISPL`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
`AY_X_HEIGHT` for the local agent and `REMOTE_DISPLAY_X_HEIGHT` for the remote device.									
Monitor External									
Set to true when the monitor is external to the devic	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
e. Realtime property with boolean data type. Persists as `LOCAL_DISPLAY_X_MONITOR_EXTERNAL` for the local agent and `REMOTE_DISPLAY_X_MONITOR_EXTERNAL` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
remote device.									
Monitor Product									
The monitor's product name. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_PRODUCT` for	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_DISPLAY_X_MONITOR_PRODUCT` for the remote device.									
Monitor Serial Number									
The serial number of the monitor. Realtime property with	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_SERIALNUMBER` for the local agent and `REMOTE_DISPLAY_X_MONITOR_SERIALNUMBER` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
Monitor Vendor									
The vendor of the monitor. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_VENDOR` for the local agent and `REMOTE_`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
`DISPLAY_X_MONITOR_VENDOR` for the remote device.									
Name									
The name of the display adapter. Realtime property with text data type. Persists as `LOCAL_DISPL`	✓				✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
`AY_X_NAME` for the local agent and `REMOTE_DISPLAY_X_NAME` for the remote device.									
Width									
The width of the screen in pixels. Realtime property with number	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISPLAY	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_DISPLAY_X_WIDTH` for the local agent and `REMOTE_DISPLAY_X_WIDTH` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Domain Properties

DOMAIN	AGENT	CLIENT EXTENSION							
Describes the domain membership of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
DNS									
The Domain Name System (DNS) name of the domain. Static property with text data type. Persi	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DOMAIN	AGENT	CLIENT EXTENSION							
sts as `LOCAL_DOMAIN_DNS` for the local agent and `REMOTE_DOMAIN_DNS` for the remote device.									
ID									
A unique identifier of the domain. When joined to	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DOMAIN	AGENT	CLIENT EXTENSION
Active Directory this is the domain SID. When joined to Microsoft Entra ID this is the tenant ID. Static property with text data type. Persists as `LOCAL_DOMAIN_ID` for the		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DOMAIN	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_DOMAIN_ID` for the remote device.									
Join									
Determines the type of domain that is joined. Static property with enum data type with options None	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DOMAIN	AGENT	CLIENT EXTENSION							
, Workgroup, Domain, Entra ID. Persists as `LOCAL_DOMAIN_JOIN` for the local agent and `REMOTE_DOMAIN_JOIN` for the remote device.									
Name									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DOMAIN	AGENT	CLIENT EXTENSION							
The name of the domain. Static property with text data type. Persists as `LOCAL_DOMAIN_NAME` for the local agent and `REMOTE_DOMAIN_NAME` for the remote device.	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

eLux® Properties

ELUX	AGENT	CLIENT EXTENSION							
Provides properties unique to a Unicon eLux device.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon eLux
Environment Variable Count									✓
The number of ELUX environment variables. Static property with numb									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
er data type. Persists as `REMOTE_ELUX_ENVIRONMENT_COUNT` for the remote device.									
Environment Variable Name									✓
The name of the ELUX environment									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
variable. Static property with text data type. Persists as `REMOTE_ELUX_ENVIRONMENT_X_NAME` for the remote device.									
Environment Variable Value									✓
The value of the									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
ELUX environment variable. Static property with text, number, boolean, datetime, ip data types. Persists as `REMOTE_ELUX_ENVIRONMENT_X_VALUE` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
device.									
Host ID									✓
The Host ID assigned to the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_HOSTID` for the remote device.									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
Info1									✓
The Info1 property of the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_INFO1` for the remote device.									✓
Info2									✓
The Info2 prope									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
rty of the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_INFO2` for the remote device.									
Info3									✓
The Info3 property of the eLux device. Static									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `REMOTE_ELUX_INFO3` for the remote device.									
Organization Unit ID									✓
The ID property of the Organization Unit containing									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
the eLux device. Static property with number data type. Persists as `REMOTE_ELUX_OU_ID` for the remote device.									
Scout Cert Serial									✓
The serial number of the certificate									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
used to connect to the eLux Scout server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_SERIALNUMBER` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
Scout Cert Subject									✓
The subject of the certificate used to connect to the eLux Scout server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICA`									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
`TE_SUBJECT` for the remote device.									
Scout Cert Thumbprint SHA 256									✓
The SHA 256 thumbprint of the certificate used to connect to the eLux Scout server. Static property with									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									
Scout IP									✓
The IP address of the eLux Scout server.									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_IP` for the remote device.									
Scout Name									✓
The name of the eLux Scout server. Static property with									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
text data type. Persists as `REMOTE_ELUX_SCOUT_NAME` for the remote device.									
Scout Version									✓
The version number of the eLux Scout server. Static property with									✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELUX	AGENT	CLIENT EXTENSION							
version data type. Persists as `REMOTE_ELUX_SCOUT_VERSION` for the remote device.									

Hardware Properties

HARDWARE	AGENT	CLIENT EXTENSION							
Describes the hardware and its capa	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
bilities.									
BIOS Release Date									
The date of release of the BIOS. Static property with datetime data type. Persists as `LOCAL_HARDWARE_BIOS_RELEASEDATE` for the	✓	✓			✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_HARDWARE_BIOS_RELEASEDATE` for the remote device.									
BIOS Serial Number									
The serial number of the BIOS of the device. Static property with text	✓	✓	✓		✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_HARDWARE_BIOS_SERIAL` for the local agent and `REMOTE_HARDWARE_BIOS_SERIAL` for the remote device.									
BIOS Version									
The versi	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
on number of the BIOS. Static property with version data type. Persists as `LOCAL_HARDWARE_BIOS_VERSION` for the local agent and `REMOTE_HARDWARE_BIOS_VERSION` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
the remote device.									
CPU									
The CPU available on the device. Static property with text data type. Persists as `LOCAL_HARDWARE_CPU` for the local agent and `REM`	✓	✓	✓		✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
`OTE_HARDWARE_CPU` for the remote device.									
CPU Count									
The number of CPUs. Static property with number data type. Persists as `LOCAL_HARDWARE_CPU_COUN`	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
`T` for the local agent and `REMOTE_HARDWARE_CPU_COUNT` for the remote device.									
CPU Speed									
The speed of the CPU in MHz. Static property with number	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_HARDWARE_CPU_SPEED` for the local agent and `REMOTE_HARDWARE_CPU_SPEED` for the remote device.									
Lid									
Determines if the lid of	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
the device is open or closed. Realtime property with enum data type with options Open, Closed. Persists as `LOCAL_HARDWARE_LID` for the local agent and `REMOTE_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
`HARDWARE_LID` for the remote device.									
Model									
The model of the device. Static property with text data type. Persists as `LOCAL_HARDWARE_MODEL` for the local	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
agent and `REMOTE_HARDWARE_MODEL` for the remote device.									
Role									
The role of the device, such as Laptop, Tablet, or Desktop. Static property with enum data type	✓	✓	✓		✓		✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
with options Server, Desktop, Laptop, Tablet, Virtual. Persists as `LOCAL_HARDWARE_ROLE` for the local agent and `REMOTE_HARDWARE_ROLE` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
Secure Boot									
Determines if the device was booted using secure boot. Static property with boolean data type. Persists as `LOCAL_HARDWARE_SECUREBOOT` for the	✓	✓		✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_HARDWARE_SECUREBOOT` for the remote device.									
System Memory									
The amount of physical memory in MB. Static property with number data	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_HARDWARE_SYSTEMMEMORY` for the local agent and `REMOTE_HARDWARE_SYSTEMMEMORY` for the remote device.									
Vendor									
The vendor of the	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
device. Static property with text data type. Persists as `LOCAL_HARDWARE_VENDOR` for the local agent and `REMOTE_HARDWARE_VENDOR` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
Virtualization									
The type of virtualization used to host the device. Static property with enum data type with options None, VMware, Xen®, VirtualPC, Parallels, Virtu	✓	✓	✓		✓		✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HARDWARE	AGENT	CLIENT EXTENSION							
alBox, Hyper-V. Persists as `LOCAL_HARDWARE_VIRTUALIZATION` for the local agent and `REMOTE_HARDWARE_VIRTUALIZATION` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL Properties

IGEL	AGENT	CLIENT EXTENSION							
Provides properties unique to an IGEL device.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
COSMOS Cert Count									
The number of certificates from the COSMOS chain of trust. Available with IGEL OS 12.							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
Static property with number data type. Persists as `REMOTE_IGEL_COSMOS_CERTIFICATE_COUNT` for the remote device.									
COS MOS Cert Serial									
The serial number of the							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
certificate from the COS MOS chain of trust. Available with IGEL OS 12. Static property with text data type. Persists as `REMOTE_IGEL_COSMOS_CERTIFICATE_X_SERIALNUMBER`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
for the remote device.									
COSMOS Cert Subject									
The subject of the certificate from the COSMOS chain of trust. Available with IGEL OS 12. Static property with text data							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
type. Persists as `REMOTE_IGEL_COSMOS_CERTIFICATE_X_SUBJECT` for the remote device.									
COSMOS Cert Thumbprint SHA 256									
The SHA 256 thumbprint of the certificate							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
from the COSMOS chain of trust. Available with IGEL OS 12. Static property with text data type. Persists as `REMOTE_IGEL_COSMOS_CERTIFICATE_X_THUMBPRINT_SHA256` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
the remote device.									
COSMOS Server									
The name and port of the COSMOS server. Available with IGEL OS 12. Static property with text data type. Persists as `REMOTE_`							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
`IGEL_COSMOS_SERVER` for the remote device.									
Environment Variable Count									
The number of IGEL environment variables. Static property with number data type. Persi							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
sts as `REMOTE_IGEL_ENVIRONMENT_COUNT` for the remote device.									
Environment Variable Name									
The name of the IGEL environment variable. Static property							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
with text data type. Persists as `REMOTE_IGEL_ENVIRONMENT_X_NAME` for the remote device.									
Environment Variable Type									
Determines whether IGEL environme							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
nt variable is fixed or dynamic. Static property with enum data type with options Fixed, Dynamic. Persists as `REMOTE_IGEL_ENVIRONMENT_X_TYPE` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
device.									
Environment Variable Value									
The value of the IGEL environment variable. Static property with text, number, boolean, datetime, ip data types. Persists as `REM`							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
`OTE_IGEL_ENVIRONMENT_X_VALUE` for the remote device.									
ICG Cert Serial									
The serial number of the certificate used to connect to the ICG server. Available with IGEL							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_ICG_CERTIFICATE_SERIALNUMBER` for the remote device.									
ICG Cert Subject									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
The subject of the certificate used to connect to the ICG server. Available with IGEL OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_ICG`							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
`_CERTIFICATE_SUBJECT` for the remote device.									
ICG Cert Thumbprint SHA 256									
The SHA 256 thumbprint of the certificate used to connect to the ICG server. Available							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
with IGEL OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_ICG_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
ICG Server									
The name of the ICG server. Available with IGEL OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_ICG_SERVER` for the							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
remote device.									
Structure Tag									
The structure tag of the IGEL device. Static property with text data type. Persists as `REMOTE_IGEL_STRUCTURETAG` for the remote							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
device.									
UMS Cert Serial									
The serial number of the certificate used to connect to the UMS server. Available with IGEL OS 11 and earlier. Static property with text data type.							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
Persists as `REMOTE_IGEL_UMS_CERTIFICATE_SERIALNUMBER` for the remote device.									
UMS Cert Subject									
The subject of the certificate used to connect to the UMS							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
server. Available with IGEL OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_UMS_CERTIFICATE_SUBJECT` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
UMS Cert Thumbprint SHA 256									
The SHA 256 thumbprint of the certificate used to connect to the UMS server. Available with IGEL OS 11 and earlier. Static property with text							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
data type. Persists as `REMOTE_IGEL_UMS_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									
UMS Server									
The name and port of the UMS server. Avail							✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IGEL	AGENT	CLIENT EXTENSION							
able with IGEL OS 11 and earlier. Static property with text data type. Persists as `REMOTE_IGEL_UMS_SERVER` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Input Properties

INPUT	AGENT	CLIENT EXTENSION							
Describes the input devices available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Keyboard									
Set to true when the remote device has a keyboard available. Dynamic property with	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INPUT	AGENT	CLIENT EXTENSION							
boolean data type. Persists as `LOCAL_INPUT_KEYBOARD` for the local agent and `REMOTE_INPUT_KEYBOARD` for the remote device.									
Mouse									
Set to true when	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INPUT	AGENT	CLIENT EXTENSION							
the remote device has a mouse. Dynamic property with boolean data type. Persists as `LOCAL_INPUT_MOUSE` for the local agent and `REMOTE_INPUT_MOUSE` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INPUT	AGENT	CLIENT EXTENSION							
remote device.									
Pen									
Set to true when the remote device has a pen. Dynamic property with boolean data type. Persists as `LOCAL_INPUT_PEN` for the local agent	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INPUT	AGENT	CLIENT EXTENSION							
and `REMOTE_INPUT_PEN` for the remote device.									
Touch									
Set to true when the remote device has a touch screen. Dynamic property with boolean data type. Persi	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INPUT	AGENT	CLIENT EXTENSION							
sts as `LOCAL_INPUT_TOUCH` for the local agent and `REMOTE_INPUT_TOUCH` for the remote device.									

iOS Properties

IOS	AGENT	CLIENT EXTENSION							
Provides properties uniqu	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IOS	AGENT	CLIENT EXTENSION							
e to an Apple iOS endpoint.								uch OS	
Biometrics									
Determines the biometrics configured to authenticate the user. Static property with enum data type with options None, TouchID, FaceID.				✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IOS	AGENT	CLIENT EXTENSION							
Persists as `REMOTE_IOS_BIOMETRICS` for the remote device.									
Jailbroken									
Determines whether the device has been jailbroken. Static property with boolean data				✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IOS	AGENT	CLIENT EXTENSION							
type. Persists as `REMOTE_IOS_JAILBROKEN` for the remote device.									
Passcode									
Determines whether a passcode is required to unlock the iOS device. Static prope				✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IOS	AGENT	CLIENT EXTENSION							
rty with boolean data type. Persists as `REMOTE_IOS_PASSCODE` for the remote device.									

Location Properties

LOCATION	AGENT	CLIENT EXTENSION							
Describes the geographical location of	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
the endpoint.									
Accuracy									
The accuracy of the latitude and longitude values. Static property with number data type. Persists as `LOCAL_LOCATION_ACCURACY` for the	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_LOCATION_ACCURACY` for the remote device.									
Building									
The building where the device is located. Static property with text data type. Persists	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
as `LOCAL_LOCATION_BUILDING` for the local agent and `REMOTE_LOCATION_BUILDING` for the remote device.									
Country									
The country code where the device is locat	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
ed. Static property with text data type. Persists as `LOCAL_LOCATION_COUNTRY` for the local agent and `REMOTE_LOCATION_COUNTRY` for the remote device.									
County									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
The county where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_COUNTY` for the local agent and `REMOTE_LOCATION_COUNTY` for	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
the remote device.									
Position									
The geographical position as determined by the latitude and longitude of the device. Static property with position data type. Persists as	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
`LOCAL_LOCATION_POSITION` for the local agent and `REMOTE_LOCATION_POSITION` for the remote device.									
Postcode									
The postcode where the device is located. Static	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `LOCAL_LOCATION_POSTCODE` for the local agent and `REMOTE_LOCATION_POSTCODE` for the remote device.									
Provider									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
The provider that was used to determine the position. Static property with enum data type with options Third Party, Operating System. Persists as `LOCAL_LOCATION_PROVIDER`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_LOCATION_PROVIDER` for the remote device.									
Source									
The source used by the provider to determine the position. Static property	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION
with enum data type with options Cellular, Satellite, Wi-Fi, IP Address. Persists as `LOCAL_LOCATION_SOURCE` for the local agent and `REMOTE_LOCATION_SOURCE` for the		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
remote device.									
State									
The state where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_STATE` for the local agent and `REMOTE_`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
`LOCATION_STATE` for the remote device.									
Street									
The street where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_STRE`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
`ET` for the local agent and `REMOTE_LOCATION_STREET` for the remote device.									
Town									
The town where the device is located. Static property with text data type. Persi	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
sts as `LOCAL_LOCATION_TOWN` for the local agent and `REMOTE_LOCATION_TOWN` for the remote device.									
Url									
A URL displaying the location of the device. Static	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOCATION	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `LOCAL_LOCATION_URL` for the local agent and `REMOTE_LOCATION_URL` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logical Disk Properties

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Describes the logical disks available to the user.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Bus Type									
Set to the name of the bus that the device is connected, e.g., SATA, SCSI, USB, NVMe, etc. Realti	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
me property with enum data type with options SCSI, ATAPI, ATA, IEEE 1394, SSA, Fibre Channel, USB, RAID, iSCSI, SAS, SATA, Secure Digital, Multimedia Card,									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Virtual, File Backed Virtual, Storage Spaces, NVMe, PCI, Bluetooth, IP, Unspecified. Persists as `LOCAL_LOGICALDISK_X_BUSTYPE` for the local agent and `REMOTE_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
`LOGICALDISK_X_BUSTYPE` for the remote device.									
Count									
The number of logical disks. Realtime property with number data type. Persists as `LOCAL_LOGIC`	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
`ALDISK_COUNT` for the local agent and `REMOTE_LOGICALDISK_COUNT` for the remote device.									
Drive									
The drive where the logical disk is mounted. Realtime property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_LOGICALDISK_X_DRIVE` for the local agent and `REMOTE_LOGICALDISK_X_DRIVE` for the remote device.									
Encrypted									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Determines whether the disk is encrypted with Microsoft BitLocker Drive Encryption. Realtime property with boolean data type. Persists as `LOCAL_LOGICALDISK_X_ENCRYPT`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
`ED` for the local agent and `REMOTE_LOGICALDISK_X_ENCRYPTED` for the remote device.									
Filesystem									
The underlying filesystem. Realtime property with text data	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_LOGICALDISK_X_FILESYSTEM` for the local agent and `REMOTE_LOGICALDISK_X_FILESYSTEM` for the remote device.									
Free									
The free spac	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
e as a percentage of the total space. This is only available on mounted volumes. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_X_FREE` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_LOGICALDISK_X_FREE` for the remote device.									
Total MB									
The total size in MB of the logical disk. This is only available on mounted	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
volumes. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_X_TOTALMB` for the local agent and `REMOTE_LOGICALDISK_X_TOTALMB` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
device.									
Type									
The type of the logical disk, such as Fixed, Removable, or Portable Device. Realtime property with enum data type with options Unknown, No Root Direc	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
tory, Removable, Fixed, Remote, Cdrom, RAM Disk, Portable Device. Persists as `LOCAL_LOGICALDISK_X_TYPE` for the local agent and `REMOTE_LOGICALDISK_X_TYPE`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOGICAL DISK	AGENT	CLIENT EXTENSION							
for the remote device.									

macOS Properties

MAC OS	AGENT	CLIENT EXTENSION							
Describes properties unique to an Apple macOS endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Gatekeeper									
Determines the Gatekeep			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION							
er setting which defines the trust level of software that can run on the Mac. Static property with enum data type with options Anywhere, App Store and Identified Developers									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION							
, App Store . Persists as `REMOTE_MACOS_GATEKEEPER` for the remote device.									
iCloud Account									
The iCloud account associated with the logged-in user.			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION							
Static property with text data type. Persists as `REMOTE_MACOS_ICLOUD_ACCOUNT` for the remote device.									
Secure Virtual Memory									
Determines whether the			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION							
swap file is encrypted. Static property with boolean data type. Persists as `REMOTE_MACOS_SECURE VIRTUALMEMORY` for the remote device.									
System Integrity Protection									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION						
Determines whether System Integrity Protection is enabled, which helps protect Mac users from malicious software. Static property with boolean data type. Persists as `REM`			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS	AGENT	CLIENT EXTENSION							
`REMOTE_MACOS_SYSTEMINTEGRITYPROTECTION` for the remote device.									

macOS Firewall Properties

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
Provides real-time properties describing the state of the mac OS	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
Firewall.									
Allow Signed Downloaded Inbound									
Determines whether the firewall is configured to allow signed downloaded software to receive inbound connections.			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_ALLOWSIGNEDDOWNLOADINBOUND` for the remote device.									
Allow Signed Inbound									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION						
Determines whether the firewall is configured to allow built-in software to receive inbound connections. Dynamic property with boolean data type. Persists as `REMOTE_`			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
`MACOSFIREWALL_ALLOWSIGNEDINBOUND` for the remote device.									
Block All Inbound									
Determines whether the firewall is configured to block all inbound connectio			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS FIREWALL	AGENT	CLIENT EXTENSION							
ns. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_BLOCKALLINBOUND` for the remote device.									
Enabled									
Determines whether			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
the firewall is enabled. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_ENABLED` for the remote device.									
Inbound Program Rules									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
The firewall rules configured to allow programs to receive inbound connections. Dynamic property with text data type. Persists as `REMOTE_MACOSFIREWALL_INBOUNDRUL`			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS FIREWALL	AGENT	CLIENT EXTENSION						
`ES_PROGRAMS` for the remote device.								
Stealth Mode								
Determines whether the firewall is configured to ignore ICMP packets. Dynamic property with boolean data			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS FIREWALL	AGENT	CLIENT EXTENSION							
type. Persists as `REMOTE_MACOSFIREWALL_STEALTHMODE` for the remote device.									

macOS Update Properties

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Describes the status of macOS Softw	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
are Update settings and updates.								
Auto Check For Updates								
Set to true when mac OS is configured to automatically check for updates. Realtime property with			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_CHECK` for the remote device.									
Auto Download Updates									
Set to true when macOS is configured			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
to automatically download updates. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_DOWNLOAD` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Auto Install App Store Updates								
Set to true when mac OS is configured to automatically install App Store updates. Realtime property with boolean data type. Persists			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
as `REMOTE_MACOSUPDATE_AUTO_INSTALL_APPSTORE` for the remote device.								
Auto Install Data Updates								
Set to true when macOS is configured to automatic			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ally install system data files. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_INSTALL_DATA` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Auto Install macOS Updates								
Set to true when macOS is configured to automatically install macOS updates. Realtime property with boolean data type. Persi			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
sts as `REMOTE_MACOSUPDATE_AUTO_INSTALL_MACOS` for the remote device.									
Auto Install Security Updates									
Set to true when macOS is configured to			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
automatically install security updates. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_INSTALL_SECURITY` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Enabled									
Determines whether the Software Update service is running and the last attempt to update was successful. Realtime property with			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
boolean data type. Persists as `REMOTE_MACOSUPDATE_ENABLED` for the remote device.									
Ignore Update									
The name of any updates that are not to be			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
installed. Realtime property with text data type. Persists as `REMOTE_MACOSUPDATE_IGNOREUPDATE` for the remote device.									
Last Search									
The time that the			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Software Update service last checked for updates. Realtime property with datetime data type. Persists as `REMOTE_MACOSUPDATE_LASTSEARCH` for the remot									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
e device.									
Update Count									
The number of updates that are waiting to be installed. Realtime property with number data type. Persists as `REMOTE_MACO`			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`SUPDATE_UPDATE_COUNT` for the remote device.									
Update Name									
The name of the update that is waiting to be installed. Realtime property with text data type.			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Persists as `REMOTE_MACOSUPDATE_UPDATE_X_NAME` for the remote device.								
Update Product Key								
The product key of the update that is waiting to be install			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ed. Realtime property with text data type. Persists as `REMOTE_MACOSUPDATE_UPDATE_X_PRODUCTKEY` for the remote device.									
Update Version									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
The version of the update that is waiting to be installed. Realtime property with version data type. Persists as `REMOTE_MACOSUPDATE_UPDATE_X_VERSION` for the			✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
remote device.								
Version								
The version number of the Software Update service that last checked for updates. Realtime property with version data type.			✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Persists as `REMOTE_MACOSUPDATE_VERSION` for the remote device.									

Mapped Drive Properties

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
Describes the mapped drives available within	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
a user session.									
Count									
The number of mapped drives available. Dynamic property with number data type. Persists as `LOCAL_MAPPEDDRIVE_COUNT` for the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_MAPPEDDRIVE_COUNT` for the remote device.									
Drive									
The drive where the mapped drive is mounted. Dynamic property with text data type. Persi	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
sts as `LOCAL_MAPPEDDRIVE_X_DRIVE` for the local agent and `REMOTE_MAPPEDDRIVE_X_DRIVE` for the remote device.									
Hidden									
Set to true if the mapped	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
drive is hidden. Dynamic property with boolean data type. Persists as `LOCAL_MAPPEDDRIVE_X_HIDDEN` for the local agent and `REMOTE_MAPPEDDRIVE_X_HIDDEN` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
remote device.									
Provider									
The provider of the mapped drive. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X_PROVIDER` for the local agent	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
and `REMOTE_MAPPEDDRIVE_X_PROVIDER` for the remote device.									
Server									
The name of the remote server. Dynamic property with text data type. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
`LOCAL_MAPPEDDRIVE_X_SERVER` for the local agent and `REMOTE_MAPPEDDRIVE_X_SERVER` for the remote device.									
Share									
The name of the share on the remote	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
server. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X_SHARE` for the local agent and `REMOTE_MAPPEDDRIVE_X_SHARE` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
device.									
User									
The name of the user authenticating the connection to the remote server. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
`_USER` for the local agent and `REMOTE_MAPPEDDRIVE_X_USER` for the remote device.									

MDM Properties

MDM	AGENT	CLIENT EXTENSION							
Provides dynamic properties describing	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
the current mobile device management (MDM) solution.									
Identifier									
Identifies the MDM provider. Static property with text data type. Persists as `LOCAL_MDM_IDENT`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
`IFIER` for the local agent and `REMOTE_MDM_IDENTIFIER` for the remote device.									
Managed									
Set to true when the device is managed by an MDM provider. Static	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
property with boolean data type. Persists as `LOCAL_MDM_MANAGED` for the local agent and `REMOTE_MDM_MANAGED` for the remote device.									
Microsoft Intune Acco									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
unt ID									
For Microsoft Intune managed devices, this uniquely identifies the Intune instance. Static property with text data type. Persists as `LOCAL_MDM_INTUNE_AC`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
`COUNTID` for the local agent and `REMOTE_MDM_INTUNE_ACCOUNTID` for the remote device.									
Microsoft Intune Device ID									
For Microsoft Intune managed devices,	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
this uniquely identifies the device. Static property with text data type. Persists as `LOCAL_MDM_INTUNE_DEVICEID` for the local agent and `REMOTE_MDM_INTUNE_DEVICEID`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM	AGENT	CLIENT EXTENSION							
for the remote device.									

Name Properties

NAME	AGENT	CLIENT EXTENSION							
Identifies the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
DN									
The Distinguished Name of the device within Active Direc	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
tory. Static property with text data type. Persists as `LOCAL_NAME_DN` for the local agent and `REMOTE_NAME_DN` for the remote device.									
DNS									
The DNS name of the	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
device. Static property with text data type. Persists as `LOCAL_NAME_DNS` for the local agent and `REMOTE_NAME_DNS` for the remote device.									
ID									
An arbitrary	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
identifier that uniquely identifies the endpoint. Static property with text data type. Persists as `LOCAL_ID` for the local agent and `REMOTE_ID` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
Name									
The name of the device. Static property with text data type. Persists as `LOCAL_NAME` for the local agent and `REMOTE_NAME` for the remote device.	✓	✓	✓	✓	✓	✓	✓	✓	✓
SID									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
The SID of the device within Active Directory. Static property with text data type. Persists as `LOCAL_NAME_SID` for the local agent and `REMOTE_NAME_SID` for the remote	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	AGENT	CLIENT EXTENSION							
device.									

Network Properties

NETWORK	AGENT	CLIENT EXTENSION							
Describes the network adapters and their bound network addresses.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Category									
Set to Public, Private, or Dom	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION
ain depending upon the OS categorization of the network. Dynamic property with enum data type with options Public, Private, Domain. Persists as `LOCAL_NETWORK_X_CAT`		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
`EGORY` for the local agent and `REMOTE_NETWORK_X_CATEGORY` for the remote device.									
Count									
The number of network adapters. Dynamic property with numb	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
er data type. Persists as `LOCAL_NETWORK_COUNT` for the local agent and `REMOTE_NETWORK_COUNT` for the remote device.									
Description									
The description of the netw	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
ork adapter. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_DESCRIPTION` for the local agent and `REMOTE_NETWORK_X_DESCRIPTION` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
device.									
DHCP Enabled									
Set to true when the network adapter is configured to use DHCP. Dynamic property with boolean data type. Persists as `LOCAL_NETWO`	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
`RK_X_DHCP_ENABLED` for the local agent and `REMOTE_NETWORK_X_DHCP_ENABLED` for the remote device.									
IPv4 Address									
The IPv4 address of the network adapt	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
er. Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_X_IPV4` for the local agent and `REMOTE_NETWORK_X_IPV4` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
MAC Address									
The physical MAC address of the network adapter. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_MAC` for the local agent and `REM`	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
`OTE_NETWORK_X_MAC` for the remote device.									
Wi-Fi SSID									
For Wi-Fi network adapters, the SSID of any connected networks. Dynamic property with text data type. Persi	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
sts as `LOCAL_NETWORK_X_WIFI_SSID` for the local agent and `REMOTE_NETWORK_X_WIFI_SSID` for the remote device.									
Status									
The status of the network	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
adapter. Dynamic property with enum data type with options Up, Down, Unknown. Persists as `LOCAL_NETWORK_X_STATUS` for the local agent and `REMOTE_NETWORK_X_ST`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	AGENT	CLIENT EXTENSION							
`ATUS` for the remote device.									

NoTouch Properties

NOTOUCH	AGENT	CLIENT EXTENSION							
Provides properties unique to a Stratodesk NoTouch device.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Environment Variable									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
Count									
The number of NoTouch Center environment variables. Static property with number data type. Persists as `REMOTE_NOTOUCH_ENVIRONMENT_COUNT` for the remot								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
e device.									
Environment Variable Name									
The name of the NoTouch Center environment variable. Static property with text data type. Persists as `REMOTE_NOTOUCH_`								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
`ENVIRONMENT_X_NAME` for the remote device.									
Environment Variable Value									
The value of the NoTouch Center environment variable. Static property with text, number,								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
boolean, datetime, ip data types. Persists as `REMOTE_NOTOUCH_ENVIRONMENT_X_VALUE` for the remote device.									
NoTouch Center Cert Serial									
The serial numb								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
er of the certificate used to connect to the NoTouch Center. Static property with text data type. Persists as `REMOTE_NOTOUCH_CERTIFICATE_SERIALNUMBER` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
device.									
NoTouch Center Cert Subject									
The subject of the certificate used to connect to the NoTouch Center. Static property with text data type. Persists as `REMOTE_`								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
`NOTOUCH_CERTIFICATE_SUBJECT` for the remote device.									
NoTouch Center Cert Thumbprint SHA256									
The SHA256 thumbprint of the certificate used to connect to the								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
NoTouch Center. Static property with text data type. Persists as `REMOTE_NOTOUCH_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									
NoTouch Center URL									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTOUCH	AGENT	CLIENT EXTENSION							
The Management URL of the NoTouch Center. Static property with text data type. Persists as `REMOTE_NOTOUCH_URL` for the remote device.								✓	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS Properties

OS	AGENT	CLIENT EXTENSION							
Provides information about the operating system installed on the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Description									
A textual description of the OS. Static property with text data type.	✓	✓		✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_OS_DESCRIPTION` for the local agent and `REMOTE_OS_DESCRIPTION` for the remote device.									
ID									
An arbitrary identifier that uniquely identi	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
fies the installation of the OS. Static property with text data type. Persists as `LOCAL_OS_ID` for the local agent and `REMOTE_OS_ID` for the remote device.									
Name									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
The name of the OS. Static property with enum data type with options Windows, macOS, iOS, IGEL, eLux®, Rangee, Linux, ChromeOS, NoTouch. Persists as `LOCAL_OS_NA`	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
`ME` for the local agent and `REMOTE_OS_NAME` for the remote device.									
Platform									
The platform of the OS, such as x64. Static property with enum data type with options	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
x86, x64, ARM, ARM 64, MIPS, MIPS 64. Persists as `LOCAL_OS_PLATFORM` for the local agent and `REMOTE_OS_PLATFORM` for the remote device.									
Release									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
The release version of the OS. Static property with text, number data types. Persists as `LOCAL_OS_RELEASE` for the local agent and `REMOTE_OS_RELEASE` for the remot	✓	✓			✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
e device.									
Start up Time									
The time that the OS started. Static property with datetime data type. Persists as `LOCAL_OS_STARTUPTIME` for the local agent and `REM`	✓	✓			✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
`OTE_OS_STARTUPTIME` for the remote device.									
Type									
The type of the OS, such as Client or Server. Static property with enum data type with options Client, Server.	✓	✓			✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_OS_TYPE` for the local agent and `REMOTE_OS_TYPE` for the remote device.									
Version									
The version number of the OS. Static property with	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS	AGENT	CLIENT EXTENSION							
version data type. Persists as `LOCAL_OS_VERSION` for the local agent and `REMOTE_OS_VERSION` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Password Policy Properties

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
Describes the password policy of the logged in user.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Force Logoff									
The amount of time in days between the end of the valid logon time and the time when the user	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
is forced to log off the network. Dynamic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_FORCELOGOFF` for the local agent and `REMOTE_POLICY_P`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
`PASSWORD_FOR CELOGOFF` for the remote device.									
Maximum Password Age									
The maximum period of time in days before the system requires the user to change it. Dyna	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
mic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_MAXAGE` for the local agent and `REMOTE_POLICY_PASSWORD_MAXAGE` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
Minimum Password Age									
The minimum period of time in days before the system can require the user to change it. Dynamic property with number data type. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
`LOCAL_POLICY_PASSWORD_MINAGE` for the local agent and `REMOTE_POLICY_PASSWORD_MINAGE` for the remote device.									
Minimum Password Length									
The minimum	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
number of characters required. Dynamic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_MINLENGTH` for the local agent and `REMOTE_POLICY_PASSWORD_MINL`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
`LENGTH` for the remote device.									
Password History									
The number of unique passwords associated with the user before an old password can be reused. Dyna	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
mic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_HISTORY` for the local agent and `REMOTE_POLICY_PASSWORD_HISTORY` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance Properties

PERFORMANCE	AGENT	CLIENT EXTENSION							
Describes the performance of the remoting protocol.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Bandwidth									
The bandwidth status of the remoting protocol. Dynamic property with enum data type with optio	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	AGENT	CLIENT EXTENSION							
ns Unavailable, Loading, Excellent, Good, Moderate, Poor. Persists as `LOCAL_PERFORMANCE_BANDWIDTH` for the local agent.									
Bandwidth Speed									
The bandwidth	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	AGENT	CLIENT EXTENSION							
of the remoting protocol in kBps. Dynamic property with number data type. Persists as `LOCAL_PERFORMANCE_BANDWIDTH_SPEED` for the local agent.									
Latency									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	AGENT	CLIENT EXTENSION							
The latency status of the remoting protocol. Dynamic property with enum data type with options Unavailable, Loading, Excellent, Good, Moderate, Poor. Persists as `LOC`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	AGENT	CLIENT EXTENSION							
`AL_PERFORMANCE_LATENCY` for the local agent.									
Latency Speed									
The latency of the remoting protocol in milliseconds. Dynamic property with number data type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_PERFORMANCE_LATENCY_SPEED` for the local agent.									

Power Properties

POWER	AGENT	CLIENT EXTENSION							
Describes the power profile of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POWER	AGENT	CLIENT EXTENSION							
AC									
Set to Online whenever the remote device is plugged in, otherwise Offline. Dynamic property with enum data type with options Offline, Online. Persists as	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POWER	AGENT	CLIENT EXTENSION							
`LOCAL_POWER_AC` for the local agent and `REMOTE_POWER_AC` for the remote device.									
Battery									
Set to High, Medium, Low or Critical depending upon the avail	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POWER	AGENT	CLIENT EXTENSION							
able battery. Dynamic property with enum data type with options High, Low, Critical, None, Medium. Persists as `LOCAL_POWER_BATTERY` for the local agent and `REMOTE_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POWER	AGENT	CLIENT EXTENSION							
`POWER_BATTERY` for the remote device.									
Scheme									
The current power scheme. Dynamic property with text data type. Persists as `LOCAL_POWER_SCHEME`	✓	✓		✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POWER	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_POWER_SCHEME` for the remote device.									

Printer Properties

PRINTER	AGENT	CLIENT EXTENSION							
Describes the printers available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
Count									
The number of printers available. Realtime property with number data type. Persists as `LOCAL_PRINTER_COUNT` for the local agent and `REMOTE_PRINTER_COUN`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`T` for the remote device.									
Default									
Set to true if this printer is the default printer. Realtime property with boolean data type. Persists as `LOCAL_PRINTER_X`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`_DEFAULT` for the local agent and `REMOTE_PRINTER_X_DEFAULT` for the remote device.									
Directory Published									
Set to true if this printer has been published by Active	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
Directory. Realtime property with boolean data type. Persists as `LOCAL_PRINTER_X_DIRECTORY_PUBLISHED` for the local agent and `REMOTE_PRINTER_X_DIRECTORY_PUBLISHE`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`D` for the remote device.									
Driver									
The name of the printer driver. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_DRIVER` for the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_PRINTER_X_DRIVER` for the remote device.									
Driver File									
The filename of the printer driver. Realtime property with text data type. Persists	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
as `LOCAL_PRINTER_X_DRIVER_FILE` for the local agent and `REMOTE_PRINTER_X_DRIVER_FILE` for the remote device.									
Driver Manufacturer									
The manufacturer of	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
the printer driver. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_DRIVER_MANUFACTURER` for the local agent and `REMOTE_PRINTER_X_DRIVER_MAN`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`UFACTURER` for the remote device.									
Driver Version									
The version of the printer driver. Realtime property with version data type. Persists as `LOCAL_P`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`RINTER_X_DRIVER_VERSION` for the local agent and `REMOTE_PRINTER_X_DRIVER_VERSION` for the remote device.									
Errors									
Lists any errors currently reported	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
by the printer. Realtime property with flags data type with options Paused, Error, Pending Deletion, Paper Jam, Paper Out, Paper Problem, Offline, Output Bin Full, Not									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION
Available, Toner Low, No Toner, Cannot Print Page, User Intervention, Out Of Memory, Door Open, Server Unknown, Server Offline, Driver Update Needed.		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_PRINTER_X_ERRORS` for the local agent and `REMOTE_PRINTER_X_ERRORS` for the remote device.									
Keep Print Jobs									
Set to true when print jobs	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
are stored by the printer. Realtime property with boolean data type. Persists as `LOCAL_PRINTER_X_KEEP_PRINT_JOBS` for the local agent and `REMOTE_PRINTER_X_KEEP_P`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`RINT_JOBS` for the remote device.									
Local									
Set to true if the printer is a local printer. Realtime property with boolean data type. Persists as `LOCAL_PRINTER_X`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`_LOCAL` for the local agent and `REMOTE_PRINTER_X_LOCAL` for the remote device.									
Location									
The location of the printer. Realtime property with text data type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_PRINTER_X_LOCATION` for the local agent and `REMOTE_PRINTER_X_LOCATION` for the remote device.									
Name									
The name of the printer. Realti	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
me property with text data type. Persists as `LOCAL_PRINTER_X_NAME` for the local agent and `REMOTE_PRINTER_X_NAME` for the remote device.									
Port									
The port	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
used by the printer. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_PORT` for the local agent and `REMOTE_PRINTER_X_PORT` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
device.									
Server									
The name of the server hosting the printer. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_SERVER` for the local agent	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
and `REMOTE_PRINTER_X_SERVER` for the remote device.									
Share									
The share that the printer is connected to. Realtime property with text data type. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRINTER	AGENT	CLIENT EXTENSION							
`LOCAL_PRINTER_X_SHARE` for the local agent and `REMOTE_PRINTER_X_SHARE` for the remote device.									

Region Properties

REGION	AGENT	CLIENT EXTENSION							
Describes the regional	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION						
information of the user session.							uch OS	
Keyboard Language								
The language configured by the keyboard. Dynamic property with text data type. Persists as `LOCAL_REGION_KEYBOA`	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
`RD_LANGUAGE` for the local agent and `REMOTE_REGION_KEYBOARD_LANGUAGE` for the remote device.									
Keyboard Locale									
The locale configured by the keyboard.	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
Dynamic property with text data type. Persists as `LOCAL_REGION_KEYBOARD_LOCALE` for the local agent and `REMOTE_REGION_KEYBOARD_LOCALE` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
Language									
The language configured by the OS. Dynamic property with text data type. Persists as `LOCAL_REGION_LANGUAGE` for the local agent and `REMOTE_REGION_L`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
`LANGUAGE` for the remote device.									
Locale									
The locale configured by the OS. Dynamic property with text data type. Persists as `LOCAL_REGION_LOCALE` for	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_REGION_LOCALE` for the remote device.									
Time zone Offset									
The offset in minutes relative to UTC. Dynamic property with number data	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REGION	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_REGION_TIMEZONE_OFFSET` for the local agent and `REMOTE_REGION_TIMEZONE_OFFSET` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remote Control Properties

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
Determines whether the user session is being remote controlled and provides information about the remote controlling endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Active									
Set to true	✓	✓					✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION
when the session is remote controlled. Dynamic property with boolean data type. Persists as `LOCAL_REMOTECONTROL_ACTIVE` for the local agent and `REMOTE_REMOTECONTRO`		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
`L_ACTIVE` for the remote device.									
Gateway									
Set to true whenever a gateway was used to access the virtual session. Supported on Citrix® and VMware	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
only. Dynamic property with boolean data type. Persists as `LOCAL_REMOTECONTROL_GATEWAY` for the local agent.									
Gateway IP									
Set to the IP address of the gate	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
way used to access the virtual session. Supported on Citrix and VMware only. Dynamic property with ip, text data types. Persists as `LOCAL_REMOTECONTROL_GAT`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
`EWAY_IP` for the local agent.									
Protocol									
Determines the protocol used to remote control the device. Currently supports Console, RDP, ICA®, Nice DCV, PCoIP, Blast,	✓	✓					✓		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
and for IGEL clients, VNC. On an IGEL device, this is set to 'VNC' whilst remote shadowing is active. Dynamic property with enum data type with options Unknown, RDP, ICA,									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
PCoIP, Blast, VNC, DCV. Persists as `LOCAL_REMOTECONTROL_PROTOCOL` for the local agent and `REMOTE_REMOTECONTROL_PROTOCOL` for the remote device.									
Remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
Install Path									
The installation path of the remote client. Supported on Citrix only. Dynamic property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_INSTALLP`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
`ATH` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_INSTALLPATH` for the remote device.									
Remote IP									
The IP address of the remote user. Dynamic	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION
property with ip, text data types. Persists as `LOCAL_REMOTECONTROL_REMOTE_IP` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_IP` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
device.									
Remote Name									
The NetBIOS name of the remote device. Dynamic property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_NAME` for	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_REMOTECONTROL_REMOTE_NAME` for the remote device.									
Remote Platform									
The platform of the remote client. Dynamic property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_PLATFORM` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_PLATFORM` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
Remote Version									
The version number of the remote client. Supported on Citrix and VMware only. Dynamic property with version data type. Persists as `LOCAL_R`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
`EMOTECONTROL_REMOTE_VERSION` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_VERSION` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remoting Client Properties

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
Provides properties about the remoting client used to remote control the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Outbound Address									
The IP address of the outbound connection estab		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
lished by the remoting client. Dynamic property with ip, text data types. Persists as `REMOTE_REMOTING CLIENT_OUTBOUND_ADDRESS` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
Outbound DNS									
The DNS name established from a reverse DNS lookup, of the outbound connection of the remoting client. Dynamic property with text data type. Persi		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
sts as `REMOTE_REMOTING CLIENT_OUTBOUND_DNS` for the remote device.									
Runtime									
The runtime of the remoting client. Static property with text data type. Persi		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
sts as `REMOTE_REMOTING CLIENT_RUNTIME` for the remote device.									
Skype Plugin									
Set to true whenever the Skype plugin is detected. Dynamic prope		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
rty with boolean data type. Persists as `REMOTE_REMOTING CLIENT_PLUGINS_SKYPE` for the remote device.									
Skype Plugin Version									
Set to the version numb		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
er of the Skype plugin. Dynamic property with version data type. Persists as `REMOTE_REMOTING CLIENT_PLUGINS_SKYPE_VERSION` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMOTING CLIENT	AGENT	CLIENT EXTENSION							
Version									
The version of the remoting client. Static property with version data type. Persists as `REMOTE_REMOTING CLIENT_VERSION` for the remote device.		✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Screen Saver Properties

SCREEN SAVER	AGENT	CLIENT EXTENSION							
Describes the screen saver applied to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Enabled									
Determines if the screensaver is enabled. Realtime property with boolean data type. Persi	✓	✓	✓				✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREENSAVER	AGENT	CLIENT EXTENSION							
sts as `LOCAL_SCREENSAVER_ENABLED` for the local agent and `REMOTE_SCREENSAVER_ENABLED` for the remote device.									
Filename									
The filename of the screensav	✓	✓	✓				✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREENSAVER	AGENT	CLIENT EXTENSION							
er that is shown to the user. Realtime property with text data type. Persists as `LOCAL_SCREENSAVER_FILENAME` for the local agent and `REMOTE_SCREENSAVER_FILENAME`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREEN SAVER	AGENT	CLIENT EXTENSION							
for the remote device.									
Secure									
Determines if a password is required when the screensaver is deactivated. Realtime property with boolean data type. Persists as	✓	✓					✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREENSAVER	AGENT	CLIENT EXTENSION							
`LOCAL_SCREENSAVER_SECURE` for the local agent and `REMOTE_SCREENSAVER_SECURE` for the remote device.									
Timeout									
Determines the amount of user idle time in	✓	✓	✓				✓		✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREENSAVER	AGENT	CLIENT EXTENSION
seconds before the screensaver is displayed. Realtime property with number data type. Persists as `LOCAL_SCREENSAVER_TIMEOUT` for the local agent and `REMOTE_SCREENSA`		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCREENSAVER	AGENT	CLIENT EXTENSION							
`VER_TIMEOUT` for the remote device.									

Security Product Properties

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
Provides real-time properties describing the state of the installed Antivirus, Antispyware	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
and Firewall security products.									
Category									
The category of security product, such as Firewall or Antivirus. Realtime property with enum data type with options Firewall,	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
Antivirus, Antispyware. Persists as `LOCAL_SECURITYPRODUCT_X_CATEGORY` for the local agent and `REMOTE_SECURITYPRODUCT_X_CATEGORY` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION						
Count								
The number of security products. Realtime property with number data type. Persists as `LOCAL_SECURITYPRODUCT_COUNT` for the local agent and `REMOTE_`	✓	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
`SECURITYPRODUCT_COUNT` for the remote device.									
Name									
The name of the security product. Realtime property with text data type. Persists as `LOCAL_S`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
`ECURITY PRODUCT_X_NAME` for the local agent and `REMOTE_SECURITY PRODUCT_X_NAME` for the remote device.									
Signature Status									
Set to Up-To-Date	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
or Out-Of-Date depending upon the state of the security product signatures. Realtime property with enum data type with options Up-To-Date, Out-Of-Date. Persists as									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
`LOCAL_SECURITYPRODUCT_X_SIGNATURESTATUS` for the local agent and `REMOTE_SECURITYPRODUCT_X_SIGNATURESTATUS` for the remote device.									
Status									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION						
Set to Active or Inactive depending upon the state of the security product. Realtime property with enum data type with options Active, Inactive. Persists as `LOCAL_S`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SECURITY PRODUCT	AGENT	CLIENT EXTENSION							
`ECURITY PRODUCT_X_STATUS` for the local agent and `REMOTE_SECURITY PRODUCT_X_STATUS` for the remote device.									

NOTE:

For Windows Client OS's, Windows Defender and the Windows Firewall are detected, in addition to any product identified by Windows Security Center. For Windows Server OS's, Windows Defender and the Windows Firewall are detected. There is no support for Windows Security Center as this is unavailable on Windows Server. For macOS, the system firewall is detected. There is no support for antivirus or antispyware products, or third-party firewalls.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Properties

SESSION	AGENT	CLIENT EXTENSION							
Provides information describing the user's logon session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Connect Id									
Uniquely identifies the current connection to the user session. Static property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
text data type. Persists as `LOCAL_SESSION_CONNECT_ID` for the local agent.									
Connect Time									
The time the session connected. Static property with datetime data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_SESSION_CONNECT_TIME` for the local agent.									
Delivery Name									
Set to a semi-colon separated list of published applications when the deliv	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
ery type is Application, or the name of the published desktop when delivery type is Desktop. Static property with text data type. Persists as `LOCAL_SESSION_DELIVERY_NAME`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
for the local agent.									
Delivery Type									
Set to Application when the session contains one or more published applications, or Desktop when the session is a published	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
desktop. Static property with enum data type with options Unknown, Desktop, Application. Persists as `LOCAL_SESSION_DELIVERY_TYPE` for the local agent.									
Id									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
The session id of the user as assigned by the operating system. Static property with number data type. Persists as `LOCAL_SESSION_ID` for the local agent.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
Idle Period									
The time period in minutes that the user session has been idle. Realtime property with number data type. Persists as `LOCAL_SESSION_IDLEPERIOD` for	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_SESSION_IDLE PERIOD` for the remote device.									
Logon Id									
Uniquely identifies the logon session of the user. Static property with text data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_SESSION_LOGON_ID` for the local agent.									
Logon Time									
The time of the session logon. Static property with datetime data type. Persists	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
as `LOCAL_SESSION_LOGON_TIME` for the local agent.									
Time									
The current session time. Static property with datetime data type. Persists as `LOCAL_SESSION_TIME`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSION	AGENT	CLIENT EXTENSION							
for the local agent.									

Smartcard Reader Properties

SMARTCARD READER	AGENT	CLIENT EXTENSION							
Describes the connected smart-card readers available to the user.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Count									
The number of smart card reade	✓	✓			✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
rs connected. Dynamic property with number data type. Persists as `LOCAL_SMARTCARDREADER_COUNT` for the local agent and `REMOTE_SMARTCARDREADER_COUNT` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
remote device.									
Name									
The name of the smart card reader. Dynamic property with text data type. Persists as `LOCAL_SMARTCARDREADER_X_NAME` for the local agent	✓	✓			✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
and `REMOTE_SMARTCARDREADER_X_NAME` for the remote device.									

User Properties

USER	AGENT	CLIENTEXTENSION							
Identifies the logged in user.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Attribute Count									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION						
The number of user attributes read from Active Directory. Static property with number data type. Persists as `LOCAL_USER_ATTRIBUTE_COUNT` for the local agent and `REMOTE_`	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`USER_ATTRIBUTE_COUNT` for the remote device.									
Attribute Name									
The name of a user attribute read from Active Directory. Static property with text data type. Persi	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
sts as `LOCAL_USER_ATTRIBUTE_X_NAME` for the local agent and `REMOTE_USER_ATTRIBUTE_X_NAME` for the remote device.									
Attribute Value									
The value of a user attrib	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
ute read from Active Directory. Static property with text, number, boolean, datetime data types. Persists as `LOCAL_USER_ATTRIBUTE_X_VALUE` for the local agent and `REM`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`OTE_USER_ATTRIBUTE_X_VALUE` for the remote device.									
Auth									
The authentication used to authenticate the user. Static property with text data type. Persists as `LOC`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`AL_USER_AUTH` for the local agent and `REMOTE_USER_AUTH` for the remote device.									
Auth Principal									
The internet provider specified principal name of the user. Static prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_USER_AUTH_PRINCIPAL` for the local agent and `REMOTE_USER_AUTH_PRINCIPAL` for the remote device.									
Auth Provider									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION						
The internet provider. Static property with text data type. Persists as `LOCAL_USER_AUTH_PROVIDER` for the local agent and `REMOTE_USER_AUTH_PROVIDER` for the remote	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
device.									
Cached Credentials									
Set to true whenever the user has cached credentials. Static property with boolean data type. Persists as `LOCAL_USER_CACHEDCR`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`EDENTIALS` for the local agent and `REMOTE_USER_CACHEDCREDENTIALS` for the remote device.									
DN									
The distinguished name of the user. Static property with text	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_USER_NAME_DN` for the local agent and `REMOTE_USER_NAME_DN` for the remote device.									
DNS									
The domain DNS of the user. Static prope	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_USER_NAME_DOMAIN_DNS` for the local agent and `REMOTE_USER_NAME_DOMAIN_DNS` for the remote device.									
Domain									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
The domain of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DOMAIN` for the local agent and `REMOTE_USER_NAME_DOMAIN` for the remote	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
device.									
Domain Logon									
Set to true whenever the user belongs to a domain. Static property with boolean data type. Persists as `LOCAL_USER_DOMAINLOGON`	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_USER_DOMAINLOGON` for the remote device.									
Groups									
The security groups that the user is a member of. Only security groups	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION
referenced below will be evaluated. Static property with text data type. Persists as `LOCAL_USER_GROUPS` for the local agent and `REMOTE_USER_GROUPS` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
device.									
Local Admin									
Set to true whenever the user has admin rights. Static property with boolean data type. Persists as `LOCAL_USER_LOCALADMIN` for	✓	✓	✓		✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_USER_LOCALADMIN` for the remote device.									
Name									
The name of the user. Static property with text data type. Persists as `LOCAL_USER_`	✓	✓	✓		✓	✓	✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`NAME` for the local agent and `REMOTE_USER_NAME` for the remote device.									
Password Age									
The age of the user password in days. Available only for Active Directory	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
and work group accounts. Static property with number data type. Persists as `LOCAL_USER_PASSWORD_AGE` for the local agent and `REMOTE_USER_PASSWORD_AGE` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
device.									
Password Auto Logon									
Set to true if auto-logon is configured for the user. Static property with boolean data type. Persists as `LOCAL_USER_PASSWORD_AUT`	✓	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
`OLOGON` for the local agent and `REMOTE_USER_PASSWORD_AUTOLOGON` for the remote device.									
SID									
The Security Identifier (SID) of the user. Static property with text	✓	✓	✓			✓			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_USER_SID` for the local agent and `REMOTE_USER_SID` for the remote device.									

WHOIS Properties

WHOIS	AGENT	CLIENT EXTENSION							
Provides the result	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHO IS	AGENT	CLIENT EXTENSION							
s of a WHO IS lookup of the endpoint.	Windows	Windows						uch OS	
Adapter									
The name of the network adapter used to query the WHO IS data. Dynamic property with text data type. Persists as `LOC`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
`AL_WHOIS_ADAPTER` for the local agent and `REMOTE_WHOIS_ADAPTER` for the remote device.									
Adapter VPN									
Determines whether the WHOIS data was queried	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
using a VPN connection. Dynamic property with boolean data type. Persists as `LOCAL_WHOIS_ADAPTER_VPN` for the local agent and `REMOTE_WHOIS_ADAPTER_VPN` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
remote device.									
Country									
The country reported by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_COUNTRY` for the local	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
agent and `REMOTE_WHOIS_COUNTRY` for the remote device.									
County									
The county reported by the WHOIS provider. Dynamic property with text data type. Persi	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
sts as `LOCAL_WHOIS_COUNTY` for the local agent and `REMOTE_WHOIS_COUNTY` for the remote device.									
DNS									
The results of a DNS lookup of the IP address. Dyna	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
mic property with text data type. Persists as `LOCAL_WHOIS_DNS` for the local agent and `REMOTE_WHOIS_DNS` for the remote device.									
IP									
The public IP address of	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
the remote device. Dynamic property with ip, text data types. Persists as `LOCAL_WHOIS_IP` for the local agent and `REMOTE_WHOIS_IP` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
ISP									
The ISP reported by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_ISP` for the local agent and `REMOTE_WHOIS_ISP` for	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
the remote device.									
Provider									
The provider used to query the WHOIS results. Dynamic property with enum data type with options IP2Location, Max Mind. Persists	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
as `LOCAL_WHOIS_PROVIDER` for the local agent and `REMOTE_WHOIS_PROVIDER` for the remote device.									
Proxy									
Set to true if a proxy is reported by the WHO	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
IS provider. Dynamic property with boolean data type. Persists as `LOCAL_WHOIS_PROXY` for the local agent and `REMOTE_WHOIS_PROXY` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
Proxy Type									
The type of proxy in use as reported by the WHOIS provider. Dynamic property with enum data type with options VPN, TOR, Hosted, Public, Residential	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
. Persists as `LOCAL_WHOIS_PROXY_TYPE` for the local agent and `REMOTE_WHOIS_PROXY_TYPE` for the remote device.									
State									
The state reported by the WHO	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
IS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_STATE` for the local agent and `REMOTE_WHOIS_STATE` for the remote device.									
Town									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
The town reported by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_TOWN` for the local agent and `REMOTE_WHOIS_TOWN` for the	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
remote device.									
Usage									
A classification of the IP address as reported by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS`	✓	✓	✓	✓	✓		✓	✓	✓

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHOIS	AGENT	CLIENT EXTENSION							
`_USAGE` for the local agent and `REMOTE_WHOIS_USAGE` for the remote device.									

Windows Properties

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
Provides real-time properties unique to a Microsoft	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
Windows device.									
SmartScreen for Microsoft Edge									
The state of SmartScreen for Microsoft Edge. Requires at least Windows 10 or Windows Server 2016. Realtime property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
with enum data type with options Off, Warn, Block. Persists as `LOCAL_WINDOWS_SMARTSCREEN_EDGE` for the local agent and `REMOTE_WINDOWS_SMARTSCREEN_EDGE` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
the remote device.									
SmartScreen for Microsoft Store									
The state of SmartScreen for Microsoft Store apps. Requires at least Windows 10 or Windows Server 2016. Realtime prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
rty with enum data type with options Off, Warn. Persists as `LOCAL_WINDOWS_SMARTSCREEN_STORE` for the local agent and `REMOTE_WINDOWS_SMARTSCREEN_STORE` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
remote device.									
SmartScreen for Windows Explorer									
The state of SmartScreen for Windows Explorer. Requires at least Windows 10 or Windows Server 2016. Realtime prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
rty with enum data type with options Off, Warn, Block. Persists as `LOCAL_WINDOWS_SMARTSCREEN_EXPLORER` for the local agent and `REMOTE_WINDOWS_SMARTSCREEN_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
`EXPLORER` for the remote device.									
UAC Enabled									
Set to true if the User Access Control (UAC) consent prompt is enabled. Realtime property with boolean data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_WINDOWS_UAC_ENABLED` for the local agent and `REMOTE_WINDOWS_UAC_ENABLED` for the remote device.									
UAC Policy									
The User Acce	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
ss Control (UAC) consent prompt policy applied to administrators. Realtime property with enum data type with options Elevate without prompting, Prompt for credentials on									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
secure desktop, Prompt for consent on secure desktop, Prompt for credentials on users desktop, Prompt for consent on users desktop, Prompt for consent for non-Windows									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
binaries on secure desktop, Prompt for consent for non-Windows binaries on users desktop. Persists as `LOCAL_WINDOWS_UAC_POLICY` for the local agent and `REMOTE_WINDOWS_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
`UAC_POLICY` for the remote device.									

Windows Defender Properties

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Provides real-time properties describing the state of Microsoft Windows Defender	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Antivirus.									
Antimalware Version									
The version of the anti-malware component. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_V`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`ERSION_ANTIMALWARE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTIMALWARE` for the remote device.									
Antispyware Version									
The version of	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
the anti-spyware component. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTISPYWARE` for the local agent and `REMOTE_`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`WINDOWS_DEFENDER_VERSION_ANTISPYWARE` for the remote device.									
Antivirus Version									
The version of the anti-virus component. Realtime property with version	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTIVIRUS` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTIVIRUS` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Behavior Threats									
Determines the number of threats identified by behavioral analysis. Realtime property with number data type. Persists as `LOCAL_WINDOWSDEFENDER_B`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`BEHAVIOR_THREATS` for the local agent and `REMOTE_WINDOWSDEFENDER_BEHAVIOR_THREATS` for the remote device.									
Cloud Protection									
Defines the status of Clou	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
d Delivered Protection, which enables Windows Defender to receive the latest protection from the cloud. Realtime property with enum data type with options Disabled, Basic									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
, Advanced. Persists as `LOCAL_WINDOWSDEFENDER_CLOUDPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_CLOUDPROTECTION` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
device.									
Controlled Folder Access									
Defines the status of Windows Defender Exploit Guard's controlled folder access, which protects files, folders, and memory from	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
unauthorized changes by unfriendly applications. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_CONTROLLEDFOLDERACCESS` for the local									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
agent and `REMOTE_WINDOWSDEFENDER_CONTROLLEDFOLDERACCESS` for the remote device.									
Engine Version									
The version of the engine. Realtime property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ENGINE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ENGINE` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
device.									
Excluded Extensions									
Defines the file extensions excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOWSDEFEND`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`ER_EXCLUSIONS_EXTENSIONS` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_EXTENSIONS` for the remote device.									
Excluded Paths									
Defines the files	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
or folders excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_PATHS` for the local agent and `REM`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`OTE_WINDOWS DEFENDER_EXCLUSIONS_PATHS` for the remote device.									
Excluded Processes									
Defines the process names excluded from Windows Defender. Realti	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
me property with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_PROCESSES` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_PROCESSES`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
for the remote device.									
Last Full Scan									
The time of the last full scan. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSDEFENDER_LASTFULLS`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`CAN` for the local agent and `REMOTE_WINDOWSDEFENDER_LASTFULLSCAN` for the remote device.									
Last Quick Scan									
The time of the last quick scan. Realtime property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
datetime data type. Persists as `LOCAL_WINDOWSDEFENDER_LASTQUICKSCAN` for the local agent and `REMOTE_WINDOWSDEFENDER_LASTQUICKSCAN` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Network Definition Version									
The version of the network definitions. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKDE`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`FINITION` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION` for the remote device.									
Network Engine Version									
The version of the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
network engine. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKENGINE` for the local agent and `REMOTE_WINDOWSDEFEN`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`DEVICE_VERSION_NETWORK_ENGINE` for the remote device.									
Real-Time Protection									
Set to true when Windows Defender's real-time protection is enabled, including	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
behavior monitoring, downloaded files and attachment scanning, monitoring of file and program activity, raw volume write notifications, and process scanning. Realtime prope									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
rty with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_REALTIMEPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_REALTIMEPROTECTION` for the									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
remote device.									
Sample Submission									
Defines the status of Windows Defender sample submission, which sends sample files to Microsoft when further analy	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
sis is required. Realtime property with enum data type with options Prompt, Send Safe Samples Automatically, Never Send Samples, Send All Samples Automatically. Persists									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
as `LOCAL_WINDOWSDEFENDER_SAMPLESUBMISSION` for the local agent and `REMOTE_WINDOWSDEFENDER_SAMPLESUBMISSION` for the remote device.									
Signature Threats									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Determines the number of threats identified by their signature. Realtime property with number data type. Persists as `LOCAL_WINDOWSDEFENDER_SIGNATURE_THREATS` for the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_WINDOWSDEFENDER_SIGNATURETHREATS` for the remote device.									
Status									
The status of Windows Defender. Realtime property with enum data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
type with options Active, Pending Full Scan, Pending Reboot, Pending Manual Steps, Pending Offline Scan, Due Full Scan, Due Quick Scan, Inactive. Persists as `LOC`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`AL_WINDOWSDEFENDER_STATUS` for the local agent and `REMOTE_WINDOWSDEFENDER_STATUS` for the remote device.									
Tamper Protection									
Set to true when Wind	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
ows Defender is configured to prevent third-party processes from changing its settings. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_T`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`AMPERPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_TAMPERPROTECTION` for the remote device.									

Windows Firewall Properties

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Provides real-	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk	Unicon™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
time properties describing the state of the Microsoft Windows Firewall.	Windows	Windows						NoTouch OS	
Active Profile Block All Inbound									
Determines the active profiles which are configured to block all	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
inbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_BLOCKALLINBOUN`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`D` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_BLOCKALLINBOUND` for the remote device.									
Active Profile Disabled									
Determines the	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
active profiles where the firewall is disabled. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIV`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`EPROFILES_DISABLED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED` for the remote device.									
Active Profile Inbound Allowed									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Determines the active profiles which are configured to allow inbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
`LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_INBOUNDALLOWED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_INBOUNDALLOWED` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Active Profile Name									
Determines the names of the active profiles. Realtime property with enum data type with options Domain, Private, Public. Persi	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
sts as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_NAME` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_NAME` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Active Profile Notifications Disabled									
Determines the active profiles which do not display a notification to the user when a program is blocked from receiving inbou	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
nd connections. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFI`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`CATIONS` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFICATIONS` for the remote device.									
Active Profile Outbound Allowed									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Determines the active profiles which are configured to allow outbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
`LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Active Profile Respond to Multicast									
Determines the active profiles which respond to multicast or broadcast network traffic. Realtime property with enum	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for the local agent and `REMOTE_WINDOWSF`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`IREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for the remote device.									
Any Inbound Rules									
Determines the port numbers which are allowed to receive an incoming	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
connection from any process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_ANY` for the local agent and `REMOTE_WINDOWSF`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`IREWALL_INBOUNDRULES_ANY` for the remote device.									
Any Outbound Rules									
Determines the port numbers which are allowed to make an outgoing connection from any	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_ANY` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULE`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`S_ANY` for the remote device.									
Inbound Package Rules									
Determines the package identifier and port number of all packages allowed to receive an incoming connection.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_PACKAGES` for the local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_PAC`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`KAGES` for the remote device.									
Inbound Program Rules									
Determines the filename and port number of all programs allowed to receive an incoming connection. Realtime	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_PROGRAMS` for the local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_PROGRAMS` for									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
the remote device.									
Inbound Service Rules									
Determines the service name and port number of all packages allowed to receive an incoming connection. Realtime property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_SERVICES` for the local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_SERVICES` for the remot									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
e device.									
Inbound System Rules									
Determines the port numbers which are allowed to receive an incoming connection from system processes. Realtime property with text	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_SYSTEM` for the local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_SYSTEM` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Outbound Package Rules									
Determines the package identifier and port number of all packages allowed to make an outgoing connection. Realtime property with text	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_PACKAGES` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULES_PACKAGES` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Outbound Program Rules									
Determines the filename and port number of all programs allowed to make an outgoing connection. Realtime property with text data type.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_PROGRAMS` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULES_PROGRAMS` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Outbound Service Rules									
Determines the service name and port number of all packages allowed to make an outgoing connection. Realtime property with text data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_SERVICES` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULES_SERVICES` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									
Outbound System Rules									
Determines the port numbers which are allowed to make an outgoing connection from system processes. Realtime property with text data	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_SYSTEM` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULES_SYSTEM` for the remote		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
device.									

Windows Registry Properties

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
Provides access to Windows Registry entries.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Count									
The number of Windows Registry entries. Static property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
with number data type. Persists as `LOCAL_WINDOWSREGISTRY_COUNT` for the local agent and `REMOTE_WINDOWSREGISTRY_COUNT` for the remote device.									
Data									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION						
The Windows Registry data. Static property with text, number, boolean, datetime, ip, position data types. Persists as `LOCAL_WINDOWSREGISTRY_X_DATA` for the local agent	✓	✓						

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
and `REMOTE_WINDOWSREGISTRY_X_DATA` for the remote device.									
Path									
The Windows Registry path. Static property with text data type. Persists as `LOCAL_WINDO`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
`WSREGISTRY_X_PATH` for the local agent and `REMOTE_WINDOWSREGISTRY_X_PATH` for the remote device.									
Value									
The Windows Registry value. Static property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_WINDOWSREGISTRY_X_VALUE` for the local agent and `REMOTE_WINDOWSREGISTRY_X_VALUE` for the remote device.									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Update Properties

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Describes the status of Microsoft Windows Update.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Critical KB									
The knowledge base article IDs of any pending critical updates. Realtime property with	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
text data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICAL` for the local agent and `REMOTE_WINDOWSUPDATE_CRITICAL` for the remote device.									
Critical									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Release Date									
The deployment date of the oldest pending critical update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICA`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`L_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_CRITICAL_RELEASEDATE` for the remote device.									
Definition KB									
The knowledge base	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
article IDs of any pending definition updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_DEFINITION` for the local agent and `REM`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`OTE_WINDOWS UPDATE_DEFINITION` for the remote device.									
Definition Release Date									
The deployment date of the oldest pending definition update. Realtime prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
rty with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_DEFINITION_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_DEFINITION_RELEASE`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`DATE` for the remote device.									
Enabled									
Set to true whenever the Windows Update service is enabled. Realtime property with boolean data type. Persists	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
as `LOCAL_WINDOWSUPDATE_ENABLED` for the local agent and `REMOTE_WINDOWSUPDATE_ENABLED` for the remote device.									
Last Install									
Set to the time that	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Windows Update last installed updates. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_LASTINSTALL` for the local agent and `REM`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`OTE_WINDOWS UPDATE_LASTINSTALL` for the remote device.									
Last Search									
Set to the time that Windows Update last checked for updates. Realtime prope	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
rty with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_LASTSEARCH` for the local agent and `REMOTE_WINDOWSUPDATE_LASTSEARCH` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Notification Level									
Represents how Windows Update is configured to notify the user. Realtime property with enum data type with options Not Configured	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
, Disabled, Notify Before Download, Notify Before Install, Scheduled Install. Persists as `LOCAL_WINDOWSUPDATE_NOTIFICATIONLEVEL` for the local agent and									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`REMOTE_WINDOWSUPDATE_NOTIFICATIONLEVEL` for the remote device.									
Reboot Required									
Set to true whenever Windows Update is awaiting a reboot to finish	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
updating. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSUPDATE_REBOOTREQUIRED` for the local agent and `REMOTE_WINDOWSUPDATE_REBOOT`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`REQUIRED` for the remote device.									
Rollup KB									
The knowledge base article IDs of any pending rollup updates. Realtime property with text data type. Persists as	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`LOCAL_WINDOWSUPDATE_ROLLUP` for the local agent and `REMOTE_WINDOWSUPDATE_ROLLUP` for the remote device.									
Rollup Release Date									
The deploymen	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
t date of the oldest pending rollup update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_ROLLUP_RELEASEDATE` for the local agent									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
and `REMOTE_WINDOWSUPDATE_ROLLUP_RELEASEDATE` for the remote device.									
Security KB									
The knowledge base article IDs of any pending security updates.	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_SECURITY` for the local agent and `REMOTE_WINDOWSUPDATE_SECURITY` for the remote									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Security Release Date									
The deployment date of the oldest pending security update. Realtime property with datetime data type. Persists as `LOCAL_W`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`INDOWSUPDATE_SECURITY_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_SECURITY_RELEASEDATE` for the remote device.									
ServicePa									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ck KB									
The knowledge base article IDs of any pending service pack updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_SERVICE`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`PACK` for the local agent and `REMOTE_WINDOWSUPDATE_SERVICEPACK` for the remote device.									
ServicePack Release Date									
The deployment date of the oldest pendi	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ng service pack update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_SERVICEPACK_RELEASEDATE` for the local agent and `REM`									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`OTE_WINDOWS UPDATE_SERVICEPACK_RELEASEDATE` for the remote device.									
Update KB									
The knowledge base article IDs of any pending updates. Realtime property	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_WINDOWSUPDATE_UPDATE` for the local agent and `REMOTE_WINDOWSUPDATE_UPDATE` for the remote device.									
Update									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Release Date									
The deployment date of the oldest pending update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_UPDATE_RELE`	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`BASE DATE` for the local agent and `REMOTE_WINDOWSUPDATE_UPDATE_RELEASE DATE` for the remote device.									
Version									
Set to the version number of Windows Upda	✓	✓							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
te. Realtime property with version data type. Persists as `LOCAL_WINDOWSUPDATE_VERSION` for the local agent and `REMOTE_WINDOWSUPDATE_VERSION` for the remot									

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
e device.									

Adobe Reader DC Template

This template creates a configuration that checks if the remote device is licensed for Adobe Reader DC. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Adobe Reader DC, you can choose between two actions:

- Hides Adobe Reader DC from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Adobe Reader DC within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Adobe Reader DC Licensed Status	Defines if the remote device is licensed to use Adobe Reader DC within the session.	You must update the following context condition with data suitable for your environment	
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`	
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.	
		Example: PF1J8T36	
		`REMOTE - OS ID Any Of 3 ITEMS`	
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.	
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Adobe Reader DC License Override
Adobe Reader DC User	Defines if the session user is member of the Adobe Reader DC AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group. *Example: DEMO\Adobe Reader DC Licensed Users*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Adobe Reader DC Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Adobe Reader DC from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Adobe Reader DC Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Adobe Reader DC within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES%\Notepad++\notepad++.exe
Adobe Reader DC Licensed Device - Conditional Application Access - Reporting	Reports Adobe Reader DC licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT ADOBE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`READER DC LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE:

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Adobe Reader DC Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Visio Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Visio. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the remote device is not licensed for Microsoft Visio, you can choose between two actions:

- Hides Microsoft Visio from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Visio Licensed Status	Defines if the remote device is licensed to use Microsoft Visio within the session.	You must update the following context condition with data suitable for your environment
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`	
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.	
		Example: DEMO\Microsoft Visio License Override	
Microsoft Visio User	Defines if the session user is member of the Microsoft Visio AD application group.	You must update the following context condition with data suitable for your environment	
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`	
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.	
		Example: DEMO\Microsoft Visio Licensed Users	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft Visio Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Microsoft Visio from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Microsoft Visio Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.	
			Example: %PROGRAMFILES%	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			\Notepad++ \notepad++.exe
Microsoft Visio Licensed Device - Conditional Application Access - Reporting	Reports Microsoft Visio licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			OG_SERVER:12201 with your Graylog configuration. *Example: dtldss02.demo.devicetrust.local:12201*

NOTE:

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Visio Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Nuance PDF Template

This template creates a configuration that checks if the remote device is licensed for Nuance PDF. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Nuance PDF, you can choose between two actions:

- Hides Nuance PDF from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Nuance PDF within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Nuance PDF Licensed Status	Defines if the remote device is licensed to use Nuance PDF within the session.	You must update the following context condition with data suitable for your environment	
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`	
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.	
		Example: PF1J8T36	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Example: DEMO\Nuance PDF License Override
Nuance PDF User	Defines if the session user is member of the Nuance PDF AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF Licensed Users

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Nuance PDF Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Nuance PDF from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: notepad++.exe	
Nuance PDF Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Nuance PDF within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.	
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe	
Nuance PDF Licensed Device - Conditional Application Access - Reporting	Reports Nuance PDF licensing status.	Activated	You must update the following context condition with data suitable for your environment	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE:

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Nuance PDF Licensed Device - Conditional Application Access - Reporting` action can be deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

IP Address Template

This template creates a configuration that maps network printers and defines a default printer based on the location of the remote device using its IP address. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a remote device based on its IP address.	You must update the following context condition with data suitable for your environment
		`REMOTE - NETWORK IPV4 SUBNET IPv4`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`Range From 1.1.1.1 to 1.1.1.254,...`
		Replace the IPv4 range for Floor 1, Floor 2, Floor 3,... with the IPv4 range representing the target location.
		Example: 1.1.1.1 to 1.1.1.254

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an enforcement action that actively configures the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Printer Management - IP Address	Maps network printers and defines a default printer based on the location of the remote device using its IP address.	Activated	You must update the following context condition with data suitable for your environment
			`MAP PRINTER Unknown, MAP PRINTER Floor 1, MAP`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`PRINTER Floor 2,...` *Configure printers for each location within the target map printer task.* *Example:* `<code>\\DTLDPS01\Corporate Printer`

NOTE:

If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

NetBIOS Name Template

This template creates a configuration that maps network printers and defines a default printer based on the location of the remote device using its NetBIOS name. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a remote device based on its NetBIOS name.	You must update the following context condition with data suitable for your environment
		`REMOTE - NAME NAME Any Of 3 ITEMS,...`
		Replace DEVICE_NAME_X for Floor 1, Floor 2, Floor 3,... with the device names representing the target location.
		Example: DE-SG01

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes an enforcement action that actively configures the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Printer Management - NetBIOS name	Maps network printers and defines a default printer based on the location of the remote device using its NetBIOS name.	Activated	You must update the following context condition with data suitable for your environment
			`MAP PRINTER Unknown, MAP PRINTER Floor 1, MAP PRINTER Floor 2,...`
			Configure printers for each location within the target map printer task.
			Example: `<code>\\DTLDPS01\Corporate Printer`

NOTE:

If the action has been disabled, the context will still be created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Wi-Fi Access Point Template

This template creates a configuration that maps network printers and defines a default printer based on the location of the remote device using its NetBIOS name. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Device Location	Defines the location of a remote device based on its connected Wi-Fi access point.	You must update the following context condition with data suitable for your environment	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - NETWORK WI-FI BSSID Any Of 3 ITEMS,...`
		Replace ENTER_YOUR_WIFI_BSSID_HERE_X for Floor 1, Floor 2, Floor 3,... with the Wi-Fi BSSIDs representing the target location.
		Example: 00:01:02:03:04:EE

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an enforcement action that actively configures the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Printer Management - Wi-Fi access point	Maps network printers and defines a default printer based on the location of the remote device using its connected Wi-Fi access point.	Activated	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`MAP PRINTER Unknown, MAP PRINTER Floor 1, MAP PRINTER Floor 2,...` *Configure printers for each location within the target map printer task.* *Example:* `\\DTLDPS01\Corporate Printer`

NOTE:

If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Teams Template

This template creates a configuration that controls access to Microsoft Teams inside the virtual session if Microsoft Teams is running based on custom values on the remote device. It can be found in the `PROCESS MONITORING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Process Monitoring - Microsoft Teams	Defines if Microsoft Teams is running on the remote device. Uses a custom property for evaluation.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Process Monitoring - Microsoft Teams - Conditional Application Access - Enforcement - FSLogix App Masking	Hides Microsoft Teams with FSLogix App Masking within the session if Microsoft Teams is running on the remote device.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.* *Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa*
Process Monitoring - Microsoft Teams - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to Microsoft Teams with Microsoft AppLocker within the session if Microsoft Teams is running on the remote device.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Snipping Tool Template

This template creates a configuration that denies access to the session if Snipping Tool is running on the remote device. It can be found in the `PROCESS MONITORING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Process Monitoring - SnippingTool	Evaluates if Snipping Tool is running on the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	Uses a custom property for evaluation.	

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Process Monitoring - Snipping Tool - Conditional Access - Enforcement	Denies access to the session if Snipping Tool is running on the remote device.	Activated	None

NOTE:

If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Access Mode Template

This template creates a configuration that checks if the remote device is connected externally. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is connected externally, you can choose between two actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hides applications with FSLogix App Masking within the session if the remote device is connected externally.
- Denies access to applications with Microsoft AppLocker within the session if the remote device is connected externally.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	You must update the following context condition with data suitable for your environment
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Equals *.REMOTING_HOST_DNS_HERE\:3389`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389 with your remoting hosts dns suffix.*
		*Example: *.demo.devicetrust.local:3389*
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Not Equals *.REMOTING_HOST_DNS_HERE\:3389`
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389 with your remoting hosts dns suffix.*
		*Example: *.demo.devicetrust.local:3389*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Access Mode - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is connected externally.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			process name on all Terminate App tasks.
			Example: notepad++.exe
Access Mode - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote device is connected externally.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Adobe Acrobat DC Template

This template creates a configuration that checks if the remote device is licensed for Adobe Reader DC. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Adobe Reader DC, you can choose between two actions:

- Hides Adobe Reader DC from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Adobe Reader DC within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Adobe Reader DC Licensed Status	Defines if the remote device is licensed to use Adobe Reader DC within the session.	You must update the following context condition with data suitable for your environment	
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`	
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.	
		Example: PF1J8T36	
		`REMOTE - OS ID Any Of 3 ITEMS`	
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.	
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73	
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Adobe Reader DC License Override
Adobe Reader DC User	Defines if the session user is member of the Adobe Reader DC AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		DOMAIN\GROUP with a security group. *Example: DEMO\Adobe Reader DC Licensed Users*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Adobe Reader DC Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Adobe Reader DC from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			path on all FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Adobe Reader DC Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Adobe Reader DC within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			configuration on all Microsoft AppLocker tasks.	
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe	
Adobe Reader DC Licensed Device - Conditional Application Access - Reporting	Reports Adobe Reader DC licensing status.	Activated	You must update the following context condition with data suitable for your environment	
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO SPLUNK`	
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO GRAYLOG`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE:

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Adobe Reader DC Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Corporate Device Template

This template creates a configuration that checks if the remote device is a corporate managed device. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not a corporate managed device, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the remote device is not a corporate managed device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Denies access to applications with Microsoft AppLocker within the session if the remote device is not a corporate managed device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Corporate Device	Defines if the remote device is a corporate managed device.	You must update the following context condition with data suitable for your environment
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Microsoft Entra ID domain joined devices, replace DOMAIN_SID and AZURE_TENANT_I

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		D with your corporate values.
		Example: S-1-5-21-1397108472-4176295369-1616608269 for a domain SID.
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your corporate devices.
		Example: PF1J8T36
		`REMOTE - IGEL UMS SERVER Equals UMS_SERVER_IP:30001`
		When using IGEL OS devices, replace UMS_SERVER_IP:30001 with the IP address of your IGEL UMS Server.
		Example: 192.168.0.22:30001

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - IGEL UMS CERT THUMPRINT SHA256 Equals UMS_CERTIFICATE_THUMBPRINT_SHA256`
		When using IGEL OS devices, replace UMS_CERTIFICATE_THUMBPRINT_SHA256 with your IGEL UMS Server certificate thumprint.
		Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56
		`REMOTE - ELUX® SCOUT NAME Equals SCOUT_NAME`
		When using eLux devices, replace SCOUT_NAME with the name of your eLux Scout Server.
		Example: DTLDES01
		`REMOTE - ELUX SCOUT CERT THUMPRINT SHA256 Equals SCOUT_CERTIFICATE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.* *Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Corporate Device - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is not a corporate	Deactivated	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	managed device.		
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Corporate Device - Conditional Application Access - Enforcement -	Denies access to applications with Microsoft AppLocker within the session if the	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft AppLocker	remote device is not a corporate managed device.		your environment `MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.* *Example: %PROGRAMFILES%\Notepad++\notepad++.exe*

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Country Template

This template creates a configuration that checks the country of the remote device. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not located within an authorized country, you can choose between two actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hides applications with FSLogix App Masking within the session based on the country of the remote device.
- Denies access to applications with Microsoft AppLocker within the session based on the country of the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Country - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the country of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code.
			Example: US
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Country - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the country of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			with your authorized countries using the ISO 3166-1 Alpha-2 code. *Example: US* `MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.* *Example: %PROGRAMFILES%\Notepad++\notepad++.exe*

NOTE:

If both actions have been disabled, the contexts will still be created.

Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Visio Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Visio. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Visio, you can choose between two actions:

- Hides Microsoft Visio from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Visio Licensed Status	Defines if the remote device is licensed to use Microsoft Visio within the session.	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Microsoft Visio License Override
Microsoft Visio User	Defines if the session user is member of the Microsoft Visio AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Example: DEMO\Microsoft Visio Licensed Users

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft Visio Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Microsoft Visio from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles% \FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Microsoft Visio Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe
Microsoft Visio Licensed Device - Conditional Application Access - Reporting	Reports Microsoft Visio licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: dtldss02.demo.devicetrust.local:8088	
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO ELK STACK`	
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.	
			Example: dtldss02.demo.devicetrust.local:9200	
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO GRAYLOG`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE:

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Visio Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Nuance PDF Template

This template creates a configuration that checks if the remote device is licensed for Nuance PDF. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Nuance PDF, you can choose between two actions:

- Hides Nuance PDF from the session with FSLogix App Masking if the remote device is not licensed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Denies Nuance PDF within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Nuance PDF Licensed Status	Defines if the remote device is licensed to use Nuance PDF within the session.	You must update the following context condition with data suitable for your environment
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF License Override
Nuance PDF User	Defines if the session user is member of the Nuance PDF AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF Licensed Users

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Nuance PDF Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Nuance PDF from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCES

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			S_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Nuance PDF Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Nuance PDF within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe
Nuance PDF Licensed Device - Conditional Application	Reports Nuance PDF licensing status.	Activated	You must update the following context condition with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
Access - Reporting			data suitable for your environment	
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO SPLUNK`	
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.	
			Example: dtldss02.demo.devicetrust.local:8088	
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO ELK STACK`	
			When using ELK Stack for license compliance	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE:

If all actions have been disabled, the contexts will still be created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unnecessary reporting options within the `Nuance PDF Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Proximity Template

This template creates a configuration that checks the proximity of the remote device to a given position. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not in proximity to a given position, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session based on the proximity of the remote device to a given position.
- Denies access to applications with Microsoft AppLocker within the session based on the proximity of the remote device to a given position.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Proximity	Defines the proximity of the remote device to a given position.	You must update the following context condition with data suitable for your environment
		`REMOTE - LOCATION POSITION In Range 500 METERS FROM 0,0,...`
		Replace 0,0 with your target position and define the range to the given position on all conditions.
		Example: 49.8971,8.9258

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Proximity - Conditional Application Access -	Hides applications with FSLogix App Masking	Deactivated	You must update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - FSLogix App Masking	within the session based on the proximity of the remote device to a given position.		condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Proximity - Conditional Application	Denies access to applications with Microsoft	Deactivated	You must update the following

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Access - Enforcement - Microsoft AppLocker	AppLocker within the session based on the proximity of the remote device to a given position.		context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Security State Template

This template creates a configuration that checks the security state of the remote device. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the security state of the remote device is unprotected, you can choose between two actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hides applications with FSLogix App Masking based on the security state of the remote device.
- Denies access to applications with Microsoft AppLocker based on the security state of the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Security State	Defines the security status of the remote device.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Security State - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the Security State of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ENTER_PROCESS_NAME_HERE with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: notepad++.exe
Security State - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the security state of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Country codes are based on ISO 3166-1 Alpha-2 code.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Wi-Fi Security Mode Template

This template creates a configuration that checks if the remote device is connected to an insecure Wi-Fi network. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is connected to an insecure Wi-Fi network, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the remote device is connected to an insecure Wi-Fi network.
- Denies access to applications with Microsoft AppLocker within the session if the remote device is connected to an insecure Wi-Fi network.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Wi-Fi Security Mode - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Wi-Fi Security Mode - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Working Time Template

This template creates a configuration that checks if the session is accessed outside of working hours. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the session is accessed outside of working hours, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session when accessed outside of working time.
- Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00`
		Adjust your work hours to fit your requirements.

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: notepad++.exe
Working Time - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application Log Template

This template creates a configuration that reports the status of the remote device to the Windows application log. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Application Log	Reports the status of the remote device to the Windows application log.	Deactivated	None

NOTE:

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

ELK Stack Template

This template creates a configuration that reports the status of the remote device to ELK Stack. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - ELK Stack	Reports the status of the remote device to ELK Stack.	Deactivated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST STATUS REPORT`
			When using ELK Stack for status reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Email Template

This template creates a configuration that reports the status of the remote device by email. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Email	Send the status of the remote device by email.	Deactivated	None

NOTE:

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Log File Template

This template creates a configuration that reports the status of the remote device to a log file. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Log File	Records the status of the remote device to a log file.	Deactivated	None

NOTE:

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Splunk Template

This template creates a configuration that reports the status of the remote device to Splunk. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Splunk	Reports the status of the remote device to Splunk.	Deactivated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST STATUS REPORT`
			When using Splunk for status reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088

NOTE:

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conditional Access Template

This template creates a configuration that checks if the session is accessed outside of working hours. It can be found in the `TIME-BASED ACCESS` category when filtered for `REMOTE` platform.

If the session is accessed outside of working hours, you can choose between two actions:

- Denies access to the session when accessed outside working time.
- Displays a message in the session when accessed outside working time.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`EVERYDAY BETWEEN 08:00 AND 18:00` *Adjust your work hours to fit your requirements.*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes a notifying action that displays a message to the user about a context status and an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Access - Enforcement	Denies access to the session if the remote BYOD is not compliant.	Deactivated	None
Working Time - Conditional Access - Notification	Displays a message in the session when accessed outside working time.	Activated	None

NOTE:

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Conditional Application Access Template

This template creates a configuration that checks if the session is accessed outside of working hours. It can be found in the `TIME-BASED ACCESS` category when filtered for `REMOTE` platform.

If the session is accessed outside of working hours, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session when accessed outside of working time.
- Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment `LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00` *Adjust your work hours to fit your requirements.*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Working Time - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			%\Notepad++\notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Unauthorized USB Device Template

This template creates a configuration that checks if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device. It can be found in the `UNAUTHORIZED USB DEVICE` category when filtered for `REMOTE` platform.

If an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device, you can choose between two actions:

- Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.
- Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Unauthorized USB Device	Defines if an unauthorized USB device, such as a Stick, Camera or Mobile Phone, is plugged into the remote device.	You must update the following context condition with data suitable for your environment `REMOTE - LOGICAL DISK IDENTITY Not Equals 0x000,0x000,ABC123456` *When checking for unauthorized USB devices, add all of your authorized USB devices by Vendor ID (VID), Product ID (PID) and / or Serial Number.* *Example: 0x0781,0x5567,4C530000110526106001 SanDisk Cruzer Blade USB Device.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes a notifying action that displays a message to the user about a context status and an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Unauthorized USB Device Enforcement	Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.	Deactivated	None
Unauthorized USB Device Notification	Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.	Activated	None

NOTE:

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Conditional Access Template

This template creates a configuration that checks if the remote device is compliant with work from home policies. It can be found in the `WORK FROM HOME` category when filtered for `REMOTE` platform.

If the remote device is not compliant with work from home policies, you can choose between two actions:

- Denies access to the session if the external remoting device is not compliant.
- Displays a message in the session if the external remoting device is not compliant.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Access Mode	Defines if the remote device is internal or external to the corporate network.	You must update the following context condition with data suitable for your environment	
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Equals *.REMOTING_HOST_DNS_HERE\:3389`	
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389 with your remoting hosts dns suffix.*	
		*Example: *.demo.devicetrust.local:3389*	
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Not Equals *.REMOTING_HOST_DNS_HERE\:3389`	
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389*	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		with your remoting hosts dns suffix. *Example: *.demo.devicetrust.local:3389*
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Detected Home Office	Defines the detected home office of the users remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Remote Controlled	Defines if the remote device is remote controlled.	None
Security State	Defines the security status of the remote device.	You must update the following context condition with data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		suitable for your environment	
		`REMOTE - IGEL UMS SERVER Equals UMS_SERVER_IP:30001`	
		When using IGEL OS devices, replace UMS_SERVER_IP:30001 with the IP address of your IGEL UMS Server.	
		Example: 192.168.0.22:30001	
		`REMOTE - IGEL UMS CERT THUMPRINT SHA256 Equals UMS_CERTIFICATE_THUMBPRINT_SHA256`	
		When using IGEL OS devices, replace UMS_CERTIFICATE_THUMBPRINT_SHA256 with your IGEL UMS Server certificate thumprint.	
		Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - ELUX® SCOUT NAME Equals SCOUT_NAME`
		When using eLux devices, replace SCOUT_NAME with the name of your eLux Scout Server.
		Example: DTLDES01
		`REMOTE - ELUX SCOUT CERT THUMPRINT SHA256 Equals SCOUT_CERTIFICATE_THUMBPRINT_SHA256`
		When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.
		Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56
Validated Home Office	Defines the validated home office of the users remote device.	None
Virtualized	Defines if the remote device is virtualized.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes a notifying action that displays a message to the user about a context status and two enforcement actions that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Compliance Check - Conditional Access - Enforcement	Denies access to the session if the external remoting device is not compliant.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X with your authorized countries using

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			the ISO 3166-1 Alpha-2 code. *Example: US*
Compliance Check - Conditional Access - Notification	Displays a message in the session if the external remoting device is not compliant.	Activated	You must update the following context condition with data suitable for your environment `COUNTRY None Of AUTHORIZED_COUNTRY_1,...` *Replace AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code.* *Example: US*
Home Office Validation - Conditional Access - Enforcement	Validates the home office context and controls session access for external remoting devices.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.
Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.