deviceTRUST® 2503 CR

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

Contents

Welcome 40
- Quick setup 40
- More information 40

Architecture 41
- Local Scenario 41
  - deviceTRUST® Agent 41
  - Architecture - Microsoft Windows local devices 41
- Remote Scenario 42
  - deviceTRUST Agent 42
  - deviceTRUST Client Extension 42
  - Architecture - Windows, macOS, Ubuntu, eLux® or IGEL OS device 43
- Operating System Compatibility 43
  - Apple iOS and iPadOS 44
  - Apple macOS 44
  - IGEL OS 10 and 11 44
  - IGEL OS 12 45
  - Microsoft Windows 45
  - Stratodesk NoTouch 45
  - Ubuntu Desktop 46
  - eLux® 46
- Platform Compatibility 46
  - Citrix Systems 46
  - Microsoft 47

Getting Started 49
- Scenario: Remote 49
- Scenario: Local 49

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

Getting Started for Local 49
Step 1: Download the deviceTRUST setup binaries 50
Step 2: Install the deviceTRUST Agent 50
Step 3: Install the deviceTRUST Console 50
Step 4: Enter your deviceTRUST License 51
Step 5: Create and apply a file based configuration 54
Step 6: Test the Unauthorized USB Device use case 56
Troubleshooting 57
Getting Started for Remote 57
Prerequisites 59
Option 1: Citrix installation packages 60
1.1: Download the Citrix product software 60
Step 1.2: Install Citrix deviceTRUST 60
Step 1.3: Install the deviceTRUST Console 60
Step 1.4: Enter your deviceTRUST License 61
Step 1.5: Install the deviceTRUST Client Extension on a Microsoft Windows device 62
Option 2: Manual installation 62
Step 2.1: Download the deviceTRUST setup binaries 62
Step 2.2: Install the deviceTRUST Agent 62
Step 2.3: Install the deviceTRUST Console 62
Step 2.4: Enter your deviceTRUST License 63
Step 2.5: Install the deviceTRUST Client Extension on a Microsoft Windows device 66
Set up a simple use case 66
Step 1: Create and apply a file based configuration 66
Step 2: Check the access to your VDA when the deviceTRUST Client Extension is not installed 67
Step 3: Test the Compliance Check use case from a Microsoft Windows device 68
Troubleshooting 68

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

Downloads 69

Download deviceTRUST® Client Extension 2503 CR for Microsoft Windows, Apple macOS and Ubuntu 69

Download deviceTRUST Client Extension 2503 CR for eLux® 7 69

Download deviceTRUST Agent and Console 2503 CR 69

Installation 70

TABLE OF CONTENTS 70

Installing the deviceTRUST Agent 70

Option 1: Install Citrix VDA 2503 or later 70

Option 2: Manual Installation 70

Option 3: Unattended Installation 73

Installing the deviceTRUST Console 74

Unattended Installation 76

Installing the deviceTRUST Client Extension 77

Templates 78

TABLE OF CONTENTS 79

Local Templates 79

TABLE OF CONTENTS 80

Remote Templates 80

TABLE OF CONTENTS 81

SaaS Templates 82

TABLE OF CONTENTS 82

Reference 83

TABLE OF CONTENTS 83

Property Reference 83

Table of contents 83

Agent Reference 85

TABLE OF CONTENTS 85

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

Client Extension Reference 85
TABLE OF CONTENTS 85
Console Reference 85
TABLE OF CONTENTS 85
Troubleshooting 86
Scenario: Remote 86
Scenario: Local 86
Open a support ticket with us 87
Knowledge Base 88
TABLE OF CONTENTS 88
General 88
TABLE OF CONTENTS 88
Configuration 88
TABLE OF CONTENTS 88
Connectivity 89
Table of Contents 89
Diagnostics 89
TABLE OF CONTENTS 89
Installation 89
TABLE OF CONTENTS 89
Licensing 89
TABLE OF CONTENTS 89
Support 89
TABLE OF CONTENTS 89
Compatibility 90
TABLE OF CONTENTS 90
Properties 90
TABLE OF CONTENTS 90

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

Reporting 90

TABLE OF CONTENTS 90

Features 90

TABLE OF CONTENTS 90

Releases 91

TABLE OF CONTENTS 91

deviceTRUST Client Extension for macOS 2503 CR 91

Supported platforms 91

Compatibility with previous releases 91

Custom Properties and Custom Process Task 91

deviceTRUST® Client Extension for eLux 2503 CR 92

Supported platforms 92

Compatibility with previous releases 92

Custom Properties and Custom Process Task 92

deviceTRUST Client Extension for Ubuntu 2503 CR 92

Supported platforms 92

Compatibility with previous releases 92

Custom Properties and Custom Process Task 93

deviceTRUST 2503 CR 93

Supported platforms 93

Licensing 93

Citrix Virtual Channel Allow List 93

Custom Properties and Custom Process Task 93

Compatibility with previous clients 94

Compatibility 94

Releases 94

TABLE OF CONTENTS 94

index 95

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

Client Extension installation on eLux® 7 104
Client Extension installation on iOS and iPadOS devices 105
Registering with the deviceTRUST Portal 106
Assigning roles to Entra ID users 106
Generating an API Key for use by the deviceTRUST Agent 106
Generating an App Registration code to register iOS and iPadOS devices 107
Registering an iOS or iPadOS device using a QR code 108
Registering an iOS or iPad device using an MDM managed app configuration 108
Naming the iOS device for compatibility with iOS 16 and deviceTRUST Agent 23.1.120 or earlier 109
Using passcodes with deviceTRUST Agent 23.1.200 or later 109
Installing the deviceTRUST Client Extension for macOS 109
Installing the deviceTRUST® Client Extension for Ubuntu 109
Installing the deviceTRUST® Client Extension for Microsoft Windows 110
Option 1: Install the latest Citrix Workspace app 110
Option 2: Install the deviceTRUST Client Extension on Microsoft Windows 110
Client Extension Installation Command Line Options 111
Option 3: Unattended Installation 112
Active Setup Components 112
deviceTRUST Channel Registration 64-bit component 112
deviceTRUST Channel Registration 32-bit component 112
deviceTRUST Citrix Cleanup 32-bit component 113
Azure Enterprise Application for AAD Conditional Access integration 113
Check that your contexts are correctly defined 118
The Security State Context 119
Virtual session properties and contexts 119
Context change audit event 120
Session properties and contexts 121

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

Multi-Hop with deviceTRUST 121
Managed Hops 121
Unmanaged Hops 122
Managed Hops with Properties 124
Process monitoring 125
deviceTRUST® + Apple Silicon support 130
Native support for Apple Silicon 130
Remoting clients that do not support Apple Silicon 130
Rosetta 2 131
deviceTRUST® + CVE-2021-44228 “Log4Shell” 131
Check that your contextual security policy has been saved and deployed 132
The deployed policies 132
Save the policy 132
Local Policy 133
Group Policy Object (GPO) 133
File-based 133
Check that the user is managed by deviceTRUST 133
An unmanaged user signed in 134
Unmanaged Users 135
Administrative Users 135
Custom Process + PowerShell Cert signing 136
The situation 136
The issue 136
The second issue 137
The solution 138
Deny Access, Logout or Disconnect? 139
Exclude specific users from the deviceTRUST policy 141

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

GPO name is not updated in deviceTRUST policy when copying a GPO within group policy editor 142
Configuring Citrix Virtual Channel Security 143
Check that the deviceTRUST Client Extension is installed on the remote device 144
Configuring Citrix Virtual Channel Security 145
Configuration 146
Allowing all Citrix virtual channels plus the deviceTRUST virtual channel 147
Allowing all virtual channels 149
Virtual Channel Compatibility 149
deviceTRUST debug log locations 150
Microsoft Windows logs 150
Windows component installer logs 150
For the deviceTRUST Client Extension 150
For the deviceTRUST Agent and Console 151
deviceTRUST Windows Event Logs 151
For the deviceTRUST Agent 151
Linux logs 151
For the deviceTRUST Client Extension 151
Apple macOS logs 152
For the deviceTRUST Client Extension 152
Apple iOS logs 152
For the deviceTRUST Client Extension 152
Export of deviceTRUST policy configuration 152
For the deviceTRUST Console 152
Amazon WorkSpaces logging 153
Check that the deviceTRUST Agent service is running 153
Check that you are using the latest deviceTRUST version 154
Configuration of the deviceTRUST Client Extension virtual channel for ICA® 155

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

Microsoft Windows (All Users) 155
Microsoft Windows (Per User) 156
Apple macOS 156
Ubuntu 157
deviceTRUST Client Extension & Active Setup 157
Active Setup Components 157
deviceTRUST Channel Registration 64-bit component 158
deviceTRUST Channel Registration 32-bit component 158
deviceTRUST Citrix Cleanup 32-bit component 158
Enabling DCV extensions on Amazon WorkSpaces WSP 159
Installing the Administrative Templates 159
Configuring DCV Extensions 159
Additional Requirements 161
Silent removal of the deviceTRUST® Client Extension for Apple macOS 162
Make sure that you have a valid license 162
Valid deviceTRUST License 163
Check deviceTRUST License 164
Group Policy Object (GPO) deployed configuration 164
IGEL OS 12 - No IGEL Properties 165
Device Location 166
Location Information 166
Operating System Location Provider 167
Third-Party Location Provider 167
WHOIS Location Provider 167
Cellular Location Provider 168
GPS Location Providers 168
deviceTRUST Policy 168
Location and Network improvements in Windows 11 24H2 169

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

SD Card detection for Logical Disk properties 170
Updating the deviceTRUST Client Extension in IGEL OS 11 171
Azure Virtual Desktop 171
VMware Horizon View 172
Log data to Microsoft Teams 172
Policy Loading 176
Active Directory GPOs 176
File-Based Policies 176
Merging Policy Items 177
Product Events 177
Application Channel 177
deviceTRUST/Admin Channel 178
deviceTRUST/Usage Channel 209
iOS Managed App Configuration 210
deviceTRUST Portal MDM Templates 212
iOS Passcodes 213
Passcode complexity and expiry 213
Simplifying passcode entry with notifications 214
Redirecting back to the remoting client 214
Actions 214
TABLE OF CONTENTS 214
Audit Event Task 214
Citrix Policy Task 215
Custom Process Task 216
Deny Access Task 217
Microsoft Entra ID Task 218
FSLogix App Masking Task 219
Task Reference 220

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

TABLE OF CONTENTS 220
Logon Abort Task 221
Map Drive Task 221
Map Printer Task 222
Microsoft AppLocker Task 223
Popup Message Task 224
Screen Saver Task 226
Send Mail Task 226
Shortcut Task 227
Terminate App Task 228
User Session Task 229
Web Request Task 230
Windows Firewall Task 231
Windows Policy Task 232
Windows Registry Task 233
Advanced Settings 234
General Settings 235
Action Settings 235
Amazon Settings 236
Connection Settings 237
Property Settings 239
Auditing Settings 240
Licensing 240
Operational 240
Remote Device 241
Tasks 242
Triggers 242
Custom Properties Settings 243

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

Local Agent Custom Properties 243
Remote Windows Device Custom Properties 245
Remote Linux, IGEL or NoTouch Device Custom Properties 246
Creating Custom Properties 247
Microsoft Entra ID Settings 247
File-Based Policy Settings 248
Importing 249
Settings 250
TABLE OF CONTENTS 250
Licensing Settings 251
Mail Server Settings 252
Map Drive Settings 253
Microsoft AppLocker Settings 254
Mobile Settings 254
Printer Settings 255
Property Settings 256
Property Filters 257
Property Queries 258
Access Point Queries 260
Certificate Queries 260
Display Queries 261
Firewall Queries 261
Logical Disk Queries 262
Mapped Drive Queries 262
Network Queries 263
Printer Queries 263
Security Product Queries 264
Text Constraints 264

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

Enumeration (Enum) Constraints 265
Number Constraints 265
Date Constraints 266
Boolean Constraints 266
IpAddress Constraints 267
Version Constraints 267
Security Settings 267
System Messages Settings 268
Access Point Properties 269
Browser Properties 280
Cellular Properties 287
Certificate Properties 306
ChromeOS Properties 338
Custom Properties 341
deviceTRUST Properties 344
Display Properties 355
Domain Properties 372
eLux® Properties 378
Hardware Properties 393
IGEL Properties 412
Input Properties 437
iOS Properties 442
Location Properties 446
Logical Disk Properties 463
macOS Properties 496
macOS Firewall Properties 503
macOS Update 512
Mapped Drive Properties 532

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

MDM Properties 542
Multihop Properties 548
Name Properties 550
Network Properties 556
NoTouch Properties 594
OS Properties 603
Password Policy Properties 614
Performance Properties 624
Power Properties 629
Printer Properties 634
Region Properties 656
Remote Control Properties 664
Remoting Client Properties 680
Screen Saver Properties 688
Security Product Properties 694
Session Properties 704
Smartcard Reader Properties 715
User Properties 719
WHOIS Properties 742
Windows Properties 760
Windows Defender Properties 771
Windows Firewall Properties 808
Windows Registry Properties 844
Windows Update Properties 850
Access Mode Template 881
Step 1: Prerequisites 882
Step 2: Context 882
Troubleshooting 882

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

Conditional Application Access Template 882
Step 1: Prerequisites 882
Step 2: Actions 883
Troubleshooting 884
Country Template 884
Step 1: Prerequisites 884
Step 2: Context 885
Troubleshooting 885
Country Provider Template 885
Step 1: Prerequisites 885
Step 2: Context 885
Troubleshooting 886
Device Location IP Address Template 886
Step 1: Prerequisites 886
Step 2: Context 886
Troubleshooting 887
Device Location NetBIOS Name Template 887
Step 1: Prerequisites 887
Step 2: Context 888
Troubleshooting 888
Device Location Wi-Fi Access Point Template 888
Step 1: Prerequisites 888
Step 2: Context 889
Troubleshooting 889
Building Blocks Templates 889
TABLE OF CONTENTS 890
Operating System Update Template 891
Step 1: Prerequisites 891

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

Step 2: Context 891
Troubleshooting 892
Override Template 892
Step 1: Prerequisites 892
Step 2: Context 892
Troubleshooting 893
Policy Mode from AD Group Template 893
Step 1: Prerequisites 893
Step 2: Context 893
Troubleshooting 894
Policy Mode from Date Template 894
Step 1: Prerequisites 894
Step 2: Context 894
Troubleshooting 895
Process Monitoring Template 895
Step 1: Prerequisites 895
Step 2: Context 895
Step 3: Settings 896
Troubleshooting 896
Proximity Template 897
Step 1: Prerequisites 897
Step 2: Context 897
Troubleshooting 898
Session Idle Template 898
Step 1: Prerequisites 898
Step 2: Context 898
Troubleshooting 899
Unauthorized USB Device Template 899

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

Step 1: Prerequisites 899
Step 2: Context 899
Troubleshooting 900
VPN Connected Template 900
Step 1: Prerequisites 901
Step 2: Context 901
Troubleshooting 901
Wi-Fi Security Mode Template 901
Step 1: Prerequisites 901
Step 2: Context 902
Troubleshooting 902
Working Time Template 902
Step 1: Prerequisites 902
Step 2: Context 902
Troubleshooting 903
Country Template 903
Step 1: Prerequisites 904
Step 2: Contexts 904
Step 3: Actions 904
Troubleshooting 906
Compliant Application Access Templates 906
TABLE OF CONTENTS 907
Proximity Template 907
Step 1: Prerequisites 908
Step 2: Contexts 908
Step 3: Actions 909
Troubleshooting 910
Security State Template 910

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

Step 1: Prerequisites 911
Step 2: Contexts 911
Step 3: Actions 911
Troubleshooting 913
Wi-Fi Security Mode Template 913
Step 1: Prerequisites 913
Step 2: Contexts 913
Step 3: Actions 914
Troubleshooting 915
Working Time Template 915
Step 1: Prerequisites 916
Step 2: Contexts 916
Step 3: Actions 917
Troubleshooting 918
Dynamic Policy Templates 918
TABLE OF CONTENTS 919
Session Lock based on Network Type Template 919
Step 1: Prerequisites 920
Step 2: Contexts 920
Step 3: Actions 920
Troubleshooting 921
Session Lock based on VPN Connection Template 921
Step 1: Prerequisites 921
Step 2: Contexts 921
Step 3: Actions 922
Troubleshooting 922
Session Lock based on Wi-Fi Security Mode Template 922
Step 1: Prerequisites 922

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

Step 2: Contexts 923
Step 3: Actions 923
Troubleshooting 923
Conditional Application Access for Country Template 923
Step 1: Prerequisites 924
Step 2: Contexts 924
Step 3: Actions 925
Troubleshooting 927
Conditional Application Access for Proximity Template 927
Step 1: Prerequisites 927
Step 2: Contexts 927
Step 3: Actions 928
Troubleshooting 929
Geolocation Templates 930
TABLE OF CONTENTS 930
Location Aware Printing Templates 930
TABLE OF CONTENTS 931
IP Address Template 931
Step 1: Prerequisites 932
Step 2: Contexts 932
Step 3: Actions 932
Troubleshooting 933
NetBIOS Name Template 933
Step 1: Prerequisites 934
Step 2: Contexts 934
Step 3: Actions 934
Troubleshooting 935
Wi-Fi Access Point Template 935

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

Step 1: Prerequisites 936
Step 2: Contexts 936
Step 3: Actions 936
Troubleshooting 937
Application Log Template 937
Step 1: Prerequisites 938
Step 2: Contexts 938
Step 3: Actions 942
Troubleshooting 943
ELK Stack Template 943
Step 1: Prerequisites 943
Step 2: Contexts 943
Step 3: Actions 948
Troubleshooting 949
Email Template 949
Step 1: Prerequisites 949
Step 2: Contexts 949
Step 3: Actions 954
Troubleshooting 954
Status Report Templates 954
TABLE OF CONTENTS 955
Log File Template 955
Step 1: Prerequisites 956
Step 2: Contexts 956
Step 3: Actions 960
Troubleshooting 961
Splunk Template 961
Step 1: Prerequisites 961

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

Step 2: Contexts 961
Step 3: Actions 966
Troubleshooting 967
Conditional Application Access Template 967
Step 1: Prerequisites 967
Step 2: Contexts 967
Step 3: Actions 968
Troubleshooting 970
Time-based Access Templates 970
TABLE OF CONTENTS 970
Unauthorized USB Drives Templates 971
Access Mode Template 971
Step 1: Prerequisites 972
Step 2: Context 972
Troubleshooting 973
Citrix Workspace App Template 973
Step 1: Prerequisites 973
Step 2: Context 973
Troubleshooting 974
Computer Certificate Template 974
Step 1: Prerequisites 974
Step 2: Context 974
Troubleshooting 975
Conditional Application Access Template 975
Step 1: Prerequisites 976
Step 2: Actions 976
Troubleshooting 977
Corporate Device Template 977

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

Step 1: Prerequisites 978
Step 2: Context 978
Troubleshooting 980
Country Template 980
Step 1: Prerequisites 980
Step 2: Context 980
Troubleshooting 980
Country Provider Template 981
Step 1: Prerequisites 981
Step 2: Context 981
Troubleshooting 981
Device Location IP Address Template 982
Step 1: Prerequisites 982
Step 2: Context 982
Troubleshooting 983
Device Location NetBIOS Name Template 983
Step 1: Prerequisites 983
Step 2: Context 983
Troubleshooting 984
Device Type Contractor Template 984
Step 1: Prerequisites 984
Step 2: Context 984
Troubleshooting 986
Device Type Corporate Template 986
Step 1: Prerequisites 987
Step 2: Context 987
Troubleshooting 989
deviceTRUST Client Extension Availability Template 989

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

Step 1: Prerequisites 989
Step 2: Context 989
Troubleshooting 990
Building Blocks Templates 990
TABLE OF CONTENTS 990
Operating System Template 992
Step 1: Prerequisites 992
Step 2: Context 992
Troubleshooting 993
Operating System Update Template 993
Step 1: Prerequisites 993
Step 2: Context 993
Troubleshooting 994
Override Template 994
Step 1: Prerequisites 994
Step 2: Context 994
Troubleshooting 995
Policy Mode from AD Group Template 995
Step 1: Prerequisites 995
Step 2: Context 995
Troubleshooting 996
Policy Mode from Date Template 996
Step 1: Prerequisites 996
Step 2: Context 996
Troubleshooting 997
Process Monitoring Template 997
Step 1: Prerequisites 997
Step 2: Context 997

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

Step 3: Settings 998
Troubleshooting 998
Proximity Template 999
Step 1: Prerequisites 999
Step 2: Context 999
Troubleshooting 1000
Remote Controlled Template 1000
Step 1: Prerequisites 1000
Step 2: Context 1000
Troubleshooting 1000
Security State Template 1001
Step 1: Prerequisites 1001
Step 2: Context 1001
Troubleshooting 1002
Session Idle Template 1003
Step 1: Prerequisites 1003
Step 2: Context 1003
Troubleshooting 1004
Threat Detection Template 1004
Step 1: Prerequisites 1004
Step 2: Context 1004
Troubleshooting 1004
Unauthorized USB Device Template 1005
Step 1: Prerequisites 1005
Step 2: Context 1005
Troubleshooting 1006
User Privileges Template 1006
Step 1: Prerequisites 1006

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

Step 2: Context 1006
Troubleshooting 1007
Virtualized Template 1007
Step 1: Prerequisites 1007
Step 2: Context 1007
Troubleshooting 1008
VPN Connected Template 1008
Step 1: Prerequisites 1008
Step 2: Context 1008
Troubleshooting 1008
Wi-Fi Security Mode Template 1009
Step 1: Prerequisites 1009
Step 2: Context 1009
Troubleshooting 1009
Working Time Template 1009
Step 1: Prerequisites 1010
Step 2: Context 1010
Troubleshooting 1010
Conditional Access Template 1011
Step 1: Prerequisites 1011
Step 2: Contexts 1011
Step 3: Actions 1015
Troubleshooting 1016
Conditional Application Access Template 1017
Step 1: Prerequisites 1017
Step 2: Contexts 1017
Step 3: Actions 1021
Troubleshooting 1023

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

BYOD (Bring Your Own Device) Templates 1023

TABLE OF CONTENTS 1024

Compliance Check Template 1024

Step 1: Prerequisites 1025

Step 2: Contexts 1025

Step 3: Actions 1027

Troubleshooting 1028

Computer Certificate Template 1028

Step 1: Prerequisites 1029

Step 2: Contexts 1029

Step 3: Actions 1030

Troubleshooting 1031

Corporate Device Template 1031

Step 1: Prerequisites 1031

Step 2: Contexts 1032

Step 3: Actions 1034

Troubleshooting 1034

Country Template 1034

Step 1: Prerequisites 1035

Step 2: Contexts 1035

Step 3: Actions 1035

Troubleshooting 1037

deviceTRUST Client Extension Availability Template 1037

Step 1: Prerequisites 1038

Step 2: Contexts 1038

Step 3: Actions 1038

Troubleshooting 1039

Compliance Check 1039

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

Table of contents 1040
Operating System Template 1040
Step 1: Prerequisites 1041
Step 2: Contexts 1041
Step 3: Actions 1042
Troubleshooting 1042
Remote Controlled Template 1042
Step 1: Prerequisites 1043
Step 2: Contexts 1043
Step 3: Actions 1043
Troubleshooting 1044
Security State Template 1044
Step 1: Prerequisites 1045
Step 2: Contexts 1045
Step 3: Actions 1046
Troubleshooting 1047
Threat Detection Template 1047
Step 1: Prerequisites 1048
Step 2: Contexts 1048
Step 3: Actions 1048
Troubleshooting 1049
User Privileges Template 1049
Step 1: Prerequisites 1050
Step 2: Contexts 1050
Step 3: Actions 1050
Troubleshooting 1051
Virtualized Template 1051
Step 1: Prerequisites 1052

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

Step 2: Contexts 1052
Step 3: Actions 1052
Troubleshooting 1053
Wi-Fi Security Mode Template 1053
Step 1: Prerequisites 1054
Step 2: Contexts 1054
Step 3: Actions 1054
Troubleshooting 1055
Access Mode Template 1055
Step 1: Prerequisites 1056
Step 2: Contexts 1056
Step 3: Actions 1057
Troubleshooting 1058
Corporate Device Template 1058
Step 1: Prerequisites 1059
Step 2: Contexts 1059
Step 3: Actions 1061
Troubleshooting 1063
Country Template 1063
Step 1: Prerequisites 1063
Step 2: Contexts 1063
Step 3: Actions 1064
Troubleshooting 1066
Compliant Application Access Templates 1066
TABLE OF CONTENTS 1067
Proximity Template 1067
Step 1: Prerequisites 1068
Step 2: Contexts 1068

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

Step 3: Actions 1068

Troubleshooting 1070

Security State Template 1070

Step 1: Prerequisites 1071

Step 2: Contexts 1071

Step 3: Actions 1071

Troubleshooting 1073

Wi-Fi Security Mode Template 1073

Step 1: Prerequisites 1073

Step 2: Contexts 1073

Step 3: Actions 1074

Troubleshooting 1075

Working Time Template 1075

Step 1: Prerequisites 1076

Step 2: Contexts 1076

Step 3: Actions 1077

Troubleshooting 1078

Conditional Access Template 1078

Step 1: Prerequisites 1079

Step 2: Contexts 1079

Step 3: Actions 1083

Troubleshooting 1084

Compliant Backend Access Templates 1084

TABLE OF CONTENTS 1085

Amazon DCV Clipboard Security State Template 1085

Step 1: Prerequisites 1086

Step 2: Contexts 1086

Step 3: Actions 1086

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

Troubleshooting 1087
Citrix Policy Access Mode Template 1087
Step 1: Prerequisites 1087
Step 2: Contexts 1087
Step 3: Actions 1088
Troubleshooting 1088
Citrix Policy Corporate Device Template 1088
Step 1: Prerequisites 1089
Step 2: Contexts 1089
Step 3: Actions 1091
Troubleshooting 1092
Citrix Policy Wi-Fi Security Mode Template 1092
Step 1: Prerequisites 1092
Step 2: Contexts 1092
Step 3: Actions 1093
Troubleshooting 1093
Dynamic Policy Templates 1094
TABLE OF CONTENTS 1094
Secure Screen Saver Template 1094
Step 1: Prerequisites 1095
Step 2: Contexts 1095
Step 3: Actions 1095
Troubleshooting 1096
Conditional Access Template 1096
Step 1: Prerequisites 1097
Step 2: Contexts 1097
Step 3: Actions 1101
Troubleshooting 1102

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

Conditional Application Access Template 1102
Step 1: Prerequisites 1103
Step 2: Contexts 1103
Step 3: Actions 1107
Troubleshooting 1109
External Partners Templates 1109
TABLE OF CONTENTS 1109
Conditional Access for Country Template 1110
Step 1: Prerequisites 1110
Step 2: Contexts 1110
Step 3: Actions 1111
Troubleshooting 1112
Conditional Application Access for Country Template 1112
Step 1: Prerequisites 1113
Step 2: Contexts 1113
Step 3: Actions 1113
Troubleshooting 1115
Conditional Application Access for Proximity Template 1115
Step 1: Prerequisites 1116
Step 2: Contexts 1116
Step 3: Actions 1117
Troubleshooting 1118
Geolocation Templates 1118
TABLE OF CONTENTS 1119
License Compliance Templates 1119
TABLE OF CONTENTS 1120
Microsoft Visio Template 1120
Step 1: Prerequisites 1121

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

Step 2: Contexts 1121
Step 3: Actions 1122
Troubleshooting 1125
Nuance PDF Template 1125
Step 1: Prerequisites 1126
Step 2: Contexts 1126
Step 3: Actions 1128
Troubleshooting 1131
Location Aware Printing Templates 1131
TABLE OF CONTENTS 1131
IP Address Template 1132
Step 1: Prerequisites 1132
Step 2: Contexts 1132
Step 3: Actions 1133
Troubleshooting 1133
NetBIOS Name Template 1134
Step 1: Prerequisites 1134
Step 2: Contexts 1134
Step 3: Actions 1135
Troubleshooting 1135
Wi-Fi Access Point Template 1135
Step 1: Prerequisites 1136
Step 2: Contexts 1136
Step 3: Actions 1136
Troubleshooting 1137
Process Monitoring Templates 1137
TABLE OF CONTENTS 1138
Microsoft Teams Template 1138

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

Step 1: Prerequisites 1138
Step 2: Contexts 1139
Step 3: Actions 1139
Troubleshooting 1140
Snipping Tool Template 1140
Step 1: Prerequisites 1140
Step 2: Contexts 1141
Step 3: Actions 1141
Troubleshooting 1141
Access Mode Template 1142
Step 1: Prerequisites 1142
Step 2: Contexts 1142
Step 3: Actions 1143
Troubleshooting 1145
Adobe Acrobat DC Template 1145
Step 1: Prerequisites 1146
Step 2: Contexts 1146
Step 3: Actions 1147
Troubleshooting 1150
Corporate Device Template 1150
Step 1: Prerequisites 1151
Step 2: Contexts 1151
Step 3: Actions 1153
Troubleshooting 1155
Country Template 1155
Step 1: Prerequisites 1155
Step 2: Contexts 1155
Step 3: Actions 1156

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

Troubleshooting 1158
Silo Optimization Templates 1158
TABLE OF CONTENTS 1159
Microsoft Visio Template 1159
Step 1: Prerequisites 1160
Step 2: Contexts 1160
Step 3: Actions 1162
Troubleshooting 1164
Nuance PDF Template 1165
Step 1: Prerequisites 1165
Step 2: Contexts 1165
Step 3: Actions 1167
Troubleshooting 1170
Proximity Template 1170
Step 1: Prerequisites 1170
Step 2: Contexts 1171
Step 3: Actions 1171
Troubleshooting 1173
Security State Template 1173
Step 1: Prerequisites 1173
Step 2: Contexts 1173
Step 3: Actions 1174
Troubleshooting 1175
Wi-Fi Security Mode Template 1175
Step 1: Prerequisites 1176
Step 2: Contexts 1176
Step 3: Actions 1176
Troubleshooting 1178

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

Working Time Template 1178
Step 1: Prerequisites 1179
Step 2: Contexts 1179
Step 3: Actions 1179
Troubleshooting 1181
Application Log Template 1181
Step 1: Prerequisites 1181
Step 2: Contexts 1181
Step 3: Actions 1186
Troubleshooting 1187
ELK Stack Template 1187
Step 1: Prerequisites 1187
Step 2: Contexts 1187
Step 3: Actions 1192
Troubleshooting 1193
Email Template 1193
Step 1: Prerequisites 1193
Step 2: Contexts 1193
Step 3: Actions 1198
Troubleshooting 1198
Status Report Templates 1198
TABLE OF CONTENTS 1199
Log File Template 1199
Step 1: Prerequisites 1200
Step 2: Contexts 1200
Step 3: Actions 1204
Troubleshooting 1205
Splunk Template 1205

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

Step 1: Prerequisites 1205

Step 2: Contexts 1205

Step 3: Actions 1210

Troubleshooting 1211

Conditional Access Template 1211

Step 1: Prerequisites 1212

Step 2: Contexts 1212

Step 3: Actions 1212

Troubleshooting 1213

Conditional Application Access Template 1213

Step 1: Prerequisites 1214

Step 2: Contexts 1214

Step 3: Actions 1214

Troubleshooting 1216

Time-based Access Templates 1216

TABLE OF CONTENTS 1216

Unauthorized USB Device Templates 1217

TABLE OF CONTENTS 1217

Unauthorized USB Device Template 1217

Step 1: Prerequisites 1218

Step 2: Contexts 1218

Step 3: Actions 1219

Troubleshooting 1220

Conditional Access Template 1220

Step 1: Prerequisites 1220

Step 2: Contexts 1221

Step 3: Actions 1224

Troubleshooting 1225

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

Work From Home Templates 1225

TABLE OF CONTENTS 1226

Country Template 1226

Step 1: Prerequisites 1227

Step 2: Contexts 1227

Step 3: Actions 1227

Troubleshooting 1229

Compliance Check 1229

TABLE OF CONTENTS 1230

Operating System Update State Template 1230

Step 1: Prerequisites 1231

Step 2: Contexts 1231

Step 3: Actions 1231

Troubleshooting 1232

Remote Controlled Template 1232

Step 1: Prerequisites 1233

Step 2: Contexts 1233

Step 3: Actions 1233

Troubleshooting 1234

Security State Template 1234

Step 1: Prerequisites 1235

Step 2: Contexts 1235

Step 3: Actions 1235

Troubleshooting 1236

Threat Detection Template 1236

Step 1: Prerequisites 1237

Step 2: Contexts 1237

Step 3: Actions 1237

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

Troubleshooting 1238
User Privileges Template 1238
Step 1: Prerequisites 1239
Step 2: Contexts 1239
Step 3: Actions 1239
Troubleshooting 1240
Wi-Fi Security Mode Template 1240
Step 1: Prerequisites 1241
Step 2: Contexts 1241
Step 3: Actions 1242
Troubleshooting 1242

© 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.
- Reference provides a set of reference material describing the more advanced features of deviceTRUST.
- Knowledge Base provides a useful resource for common problems and resolutions.
- Troubleshooting important steps are described to help troubleshoot the deviceTRUST installation and configuration.
- 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

TABLE OF CONTENTS

- 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.

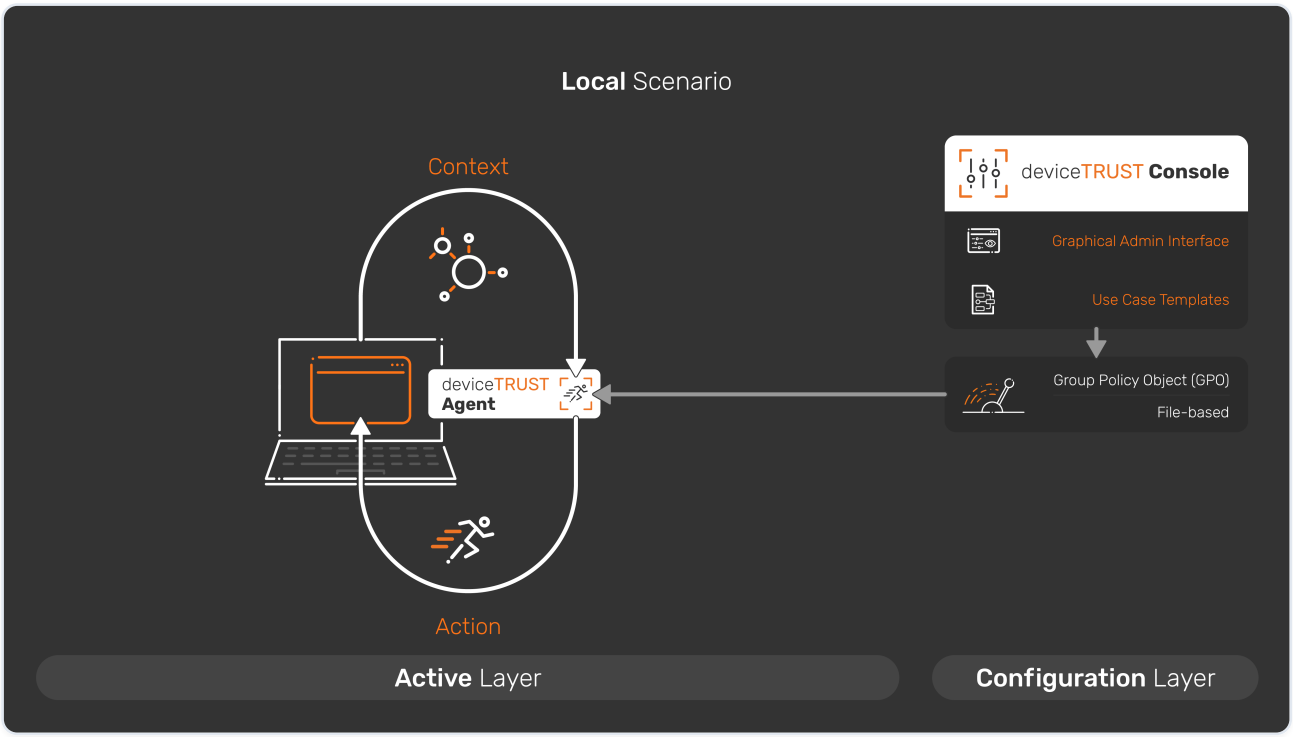
deviceTRUST® Agent

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.

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

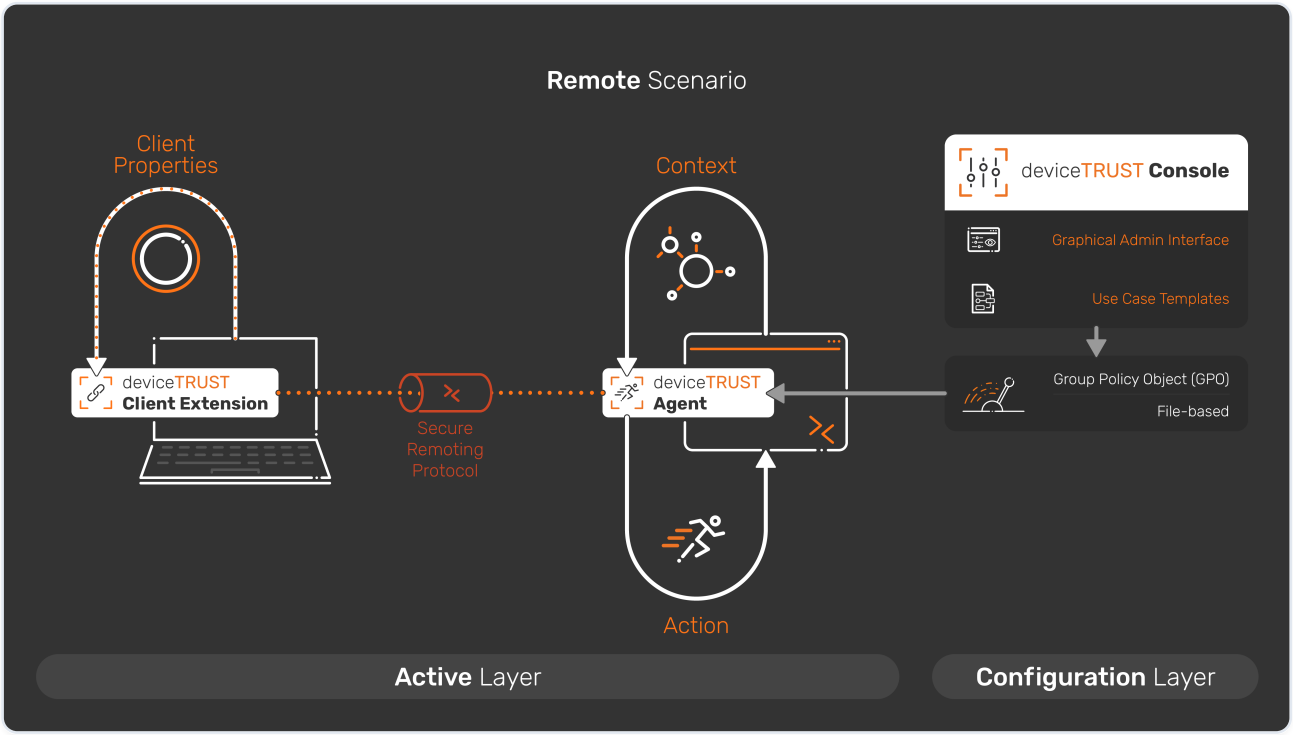
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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® or IGEL OS device

The following diagram details the deviceTRUST architecture when the remote client is installed on a Windows, macOS, Ubuntu, eLux 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
- Apple macOS
- IGEL OS 10 and 11
- IGEL OS 12
- Microsoft Windows

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

- 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:

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

IGEL OS 10 and 11

Compatible technologies (deviceTRUST Client Extension):

- 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

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

- Microsoft Remote Desktop natively integrated in IGEL OS 10.03.500 and later

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.

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:

- Azure Virtual Desktop
- Azure Active Directory
- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services

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

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

- Microsoft Remote Desktop 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:

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

eLux®

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops natively integrated in eLux 7
- Citrix Cloud natively integrated in eLux 7

Platform Compatibility

- Citrix Systems
- Microsoft

Citrix Systems

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

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

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

- Microsoft Windows Server 2012 R2 and later
- Stratodesk NoTouch OS 3.4.516 and later
- Ubuntu Desktop 18.04 LTS and later
- eLux® 7

NOTE:

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

Microsoft

Compatible technologies:

- Microsoft Remote Desktop Services
- Azure Virtual Desktop
- Azure Active Directory

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
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS and later (via FreeRDP 2)

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

NOTE:

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

© 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.

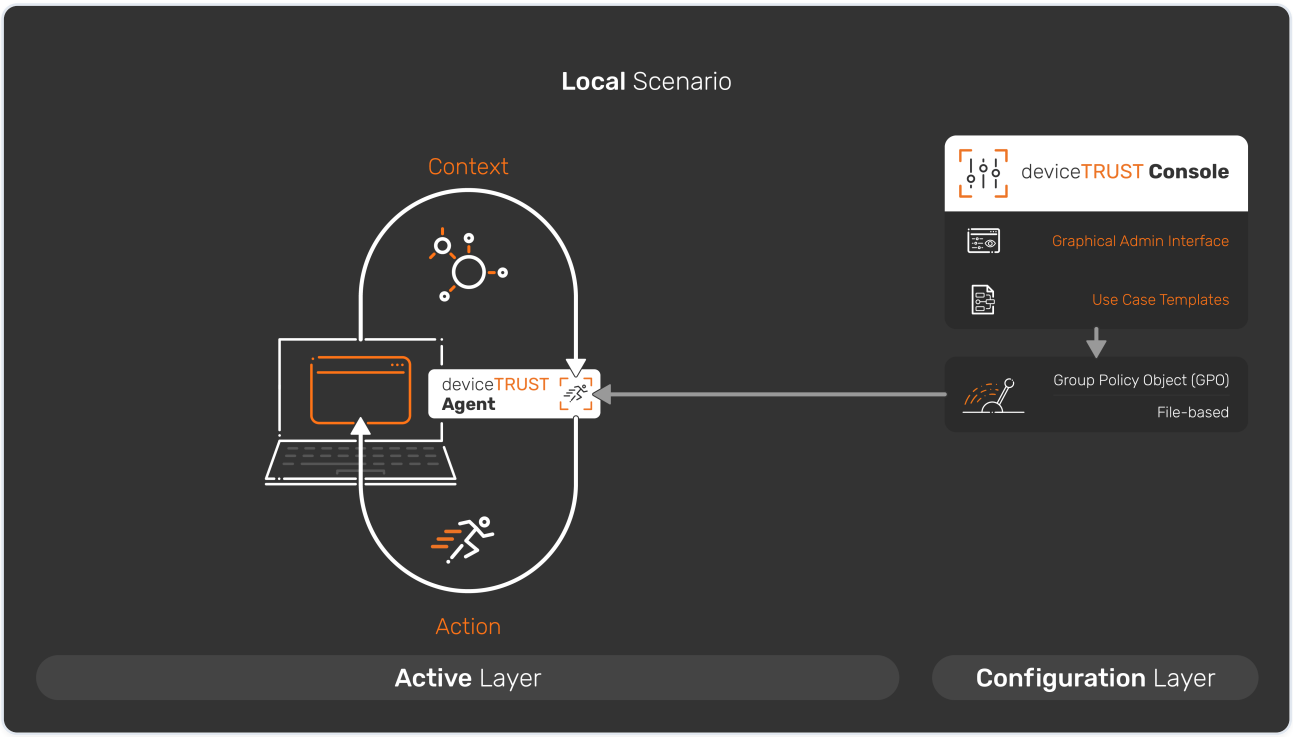
Scenario: Local

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: Create and apply a file based configuration
- 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

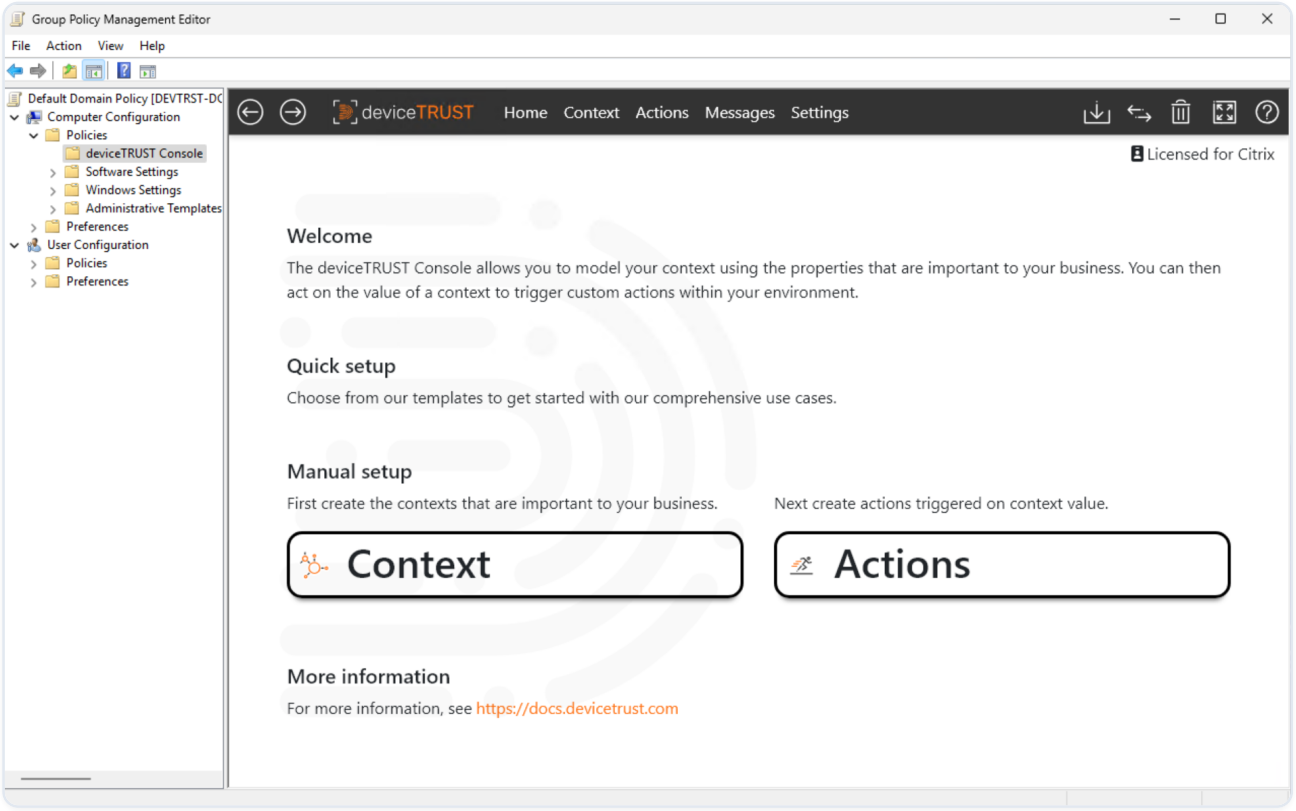
To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the

© 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.

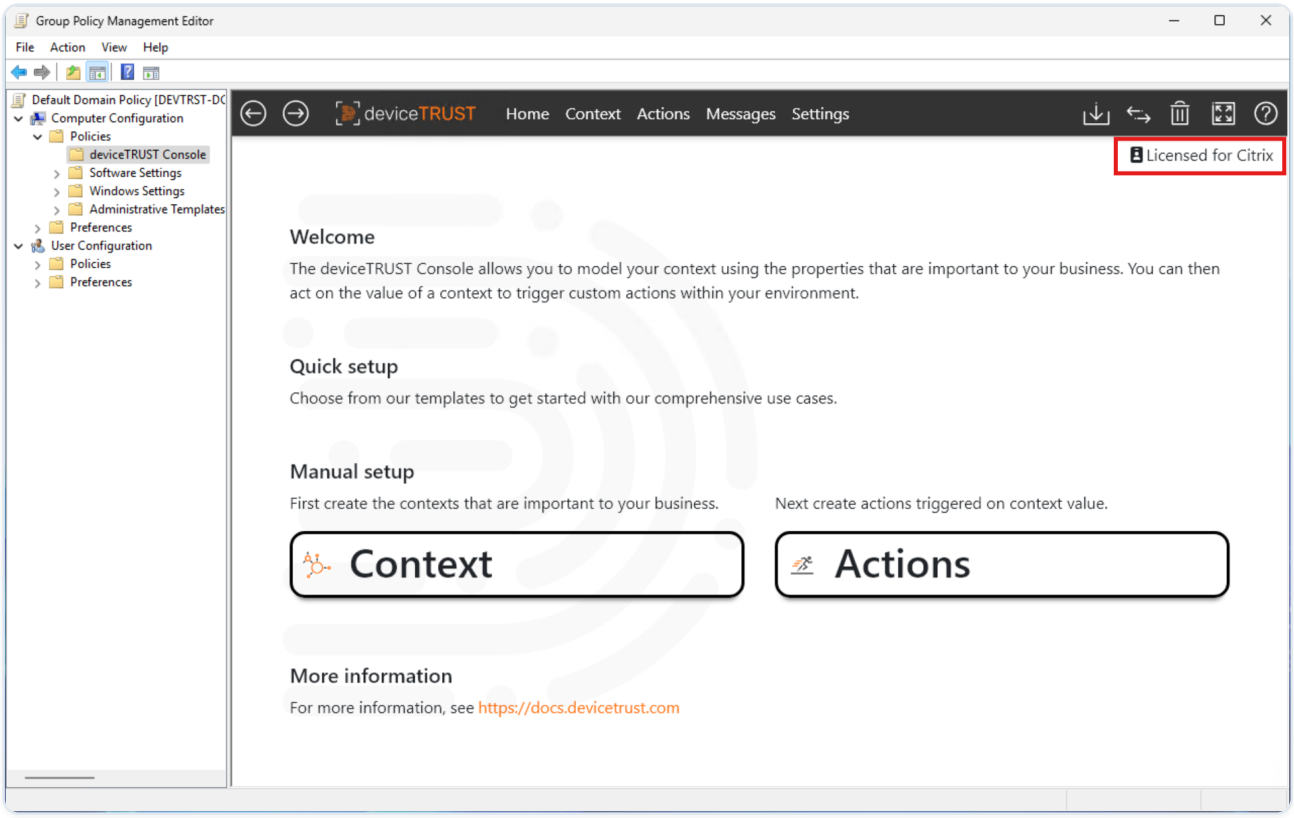


Step 4: Enter your deviceTRUST License

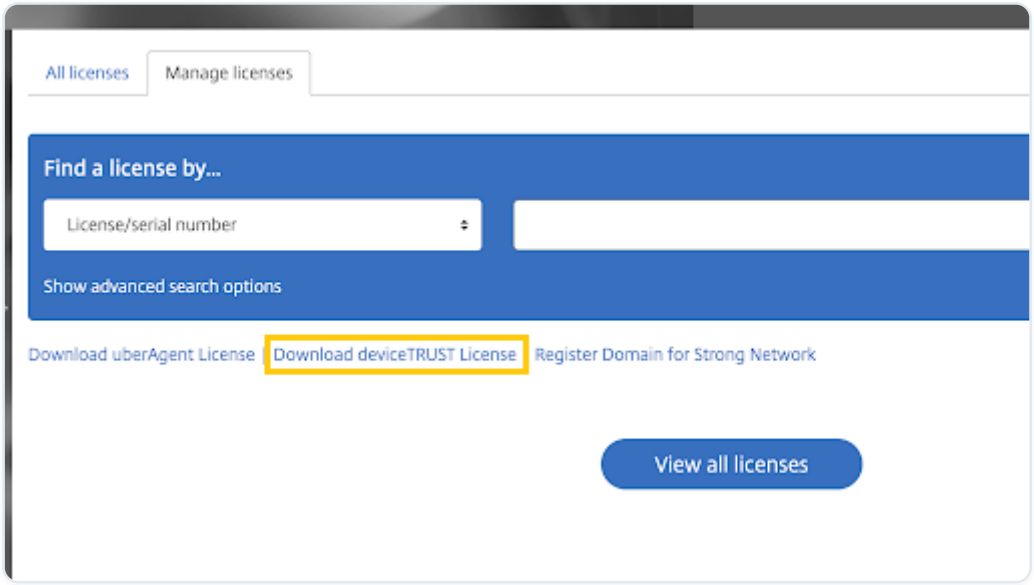
Adding a deviceTRUST license is only necessary in a non CVAD environment.

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

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

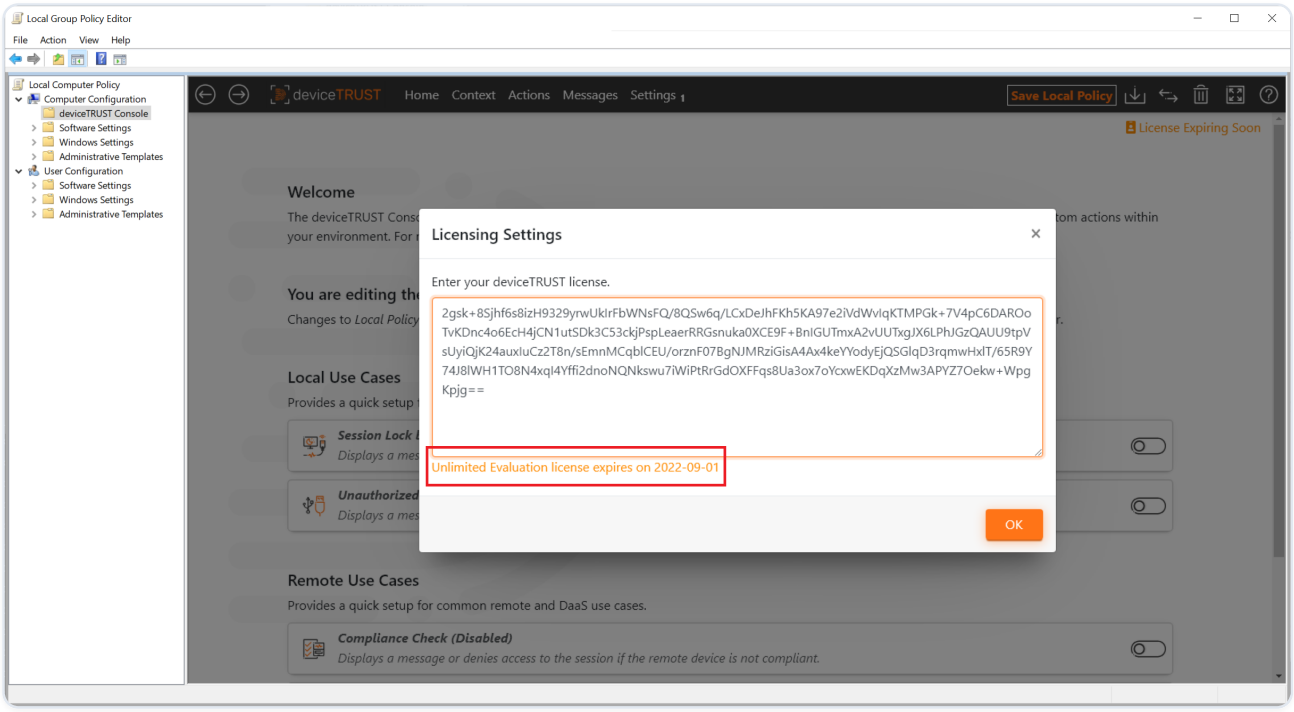


Dependent on your license, your individual deviceTRUST license can be found in your MyCitrix Portal.

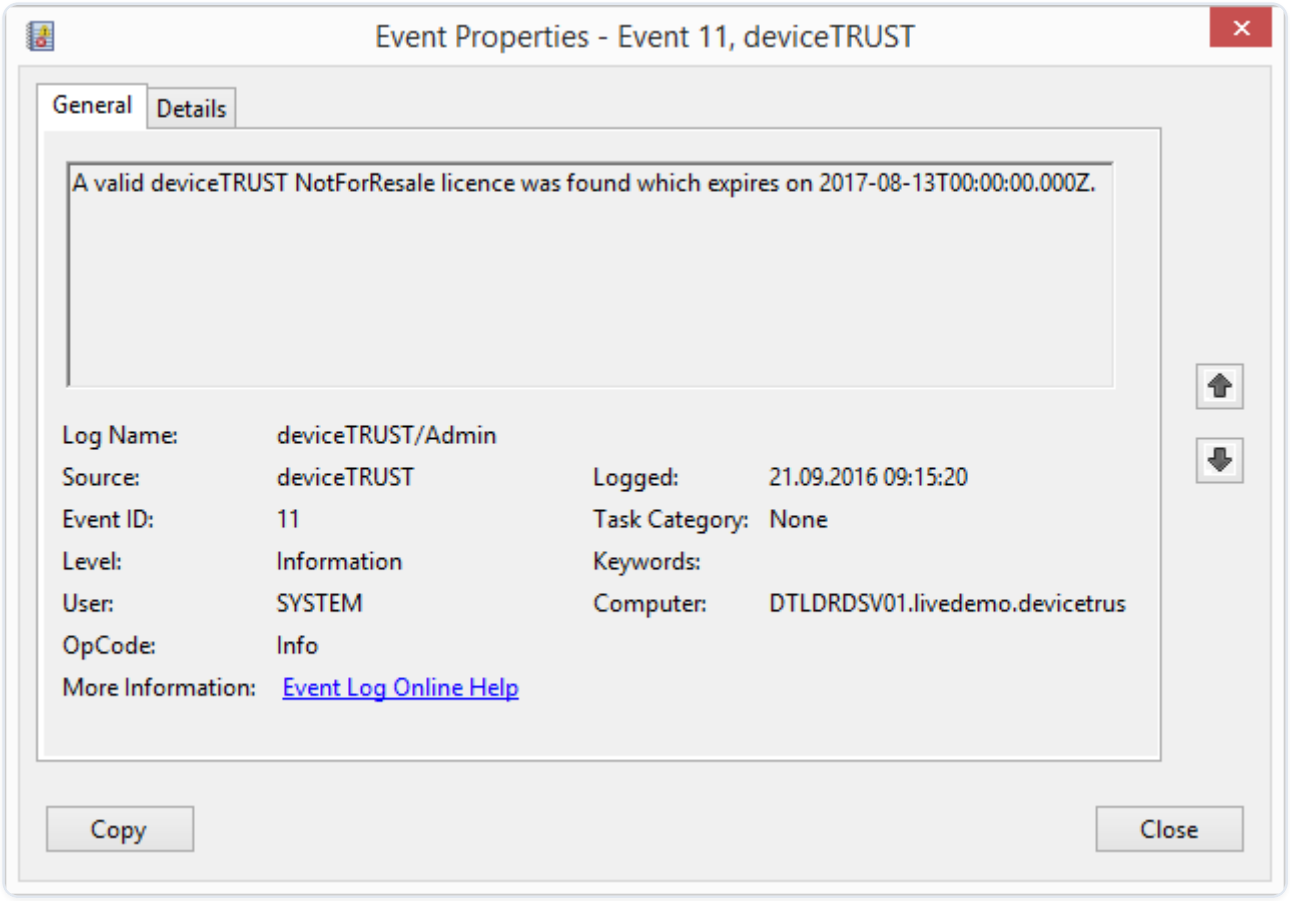


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.

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



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.

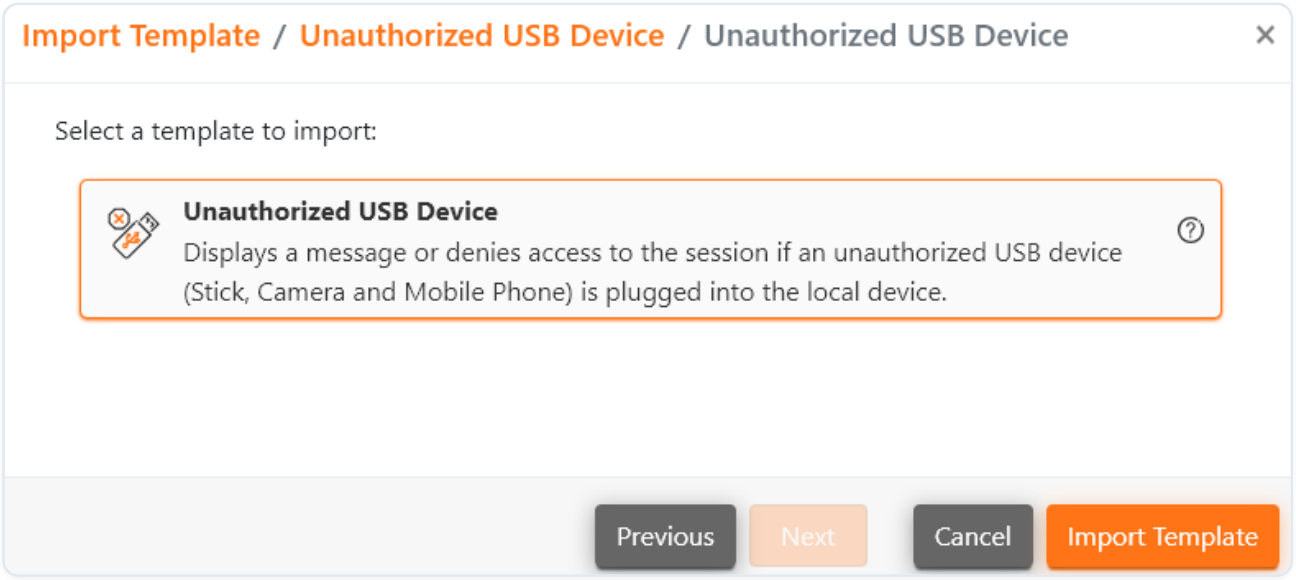


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5: Create and apply a file based configuration

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 create a New Policy.

Select `Sharing` top right and click `Import Template`, `Local`, `Unauthorized USB Device`, `Unauthorized USB Device` and confirm with `Import Template` at the bottom.

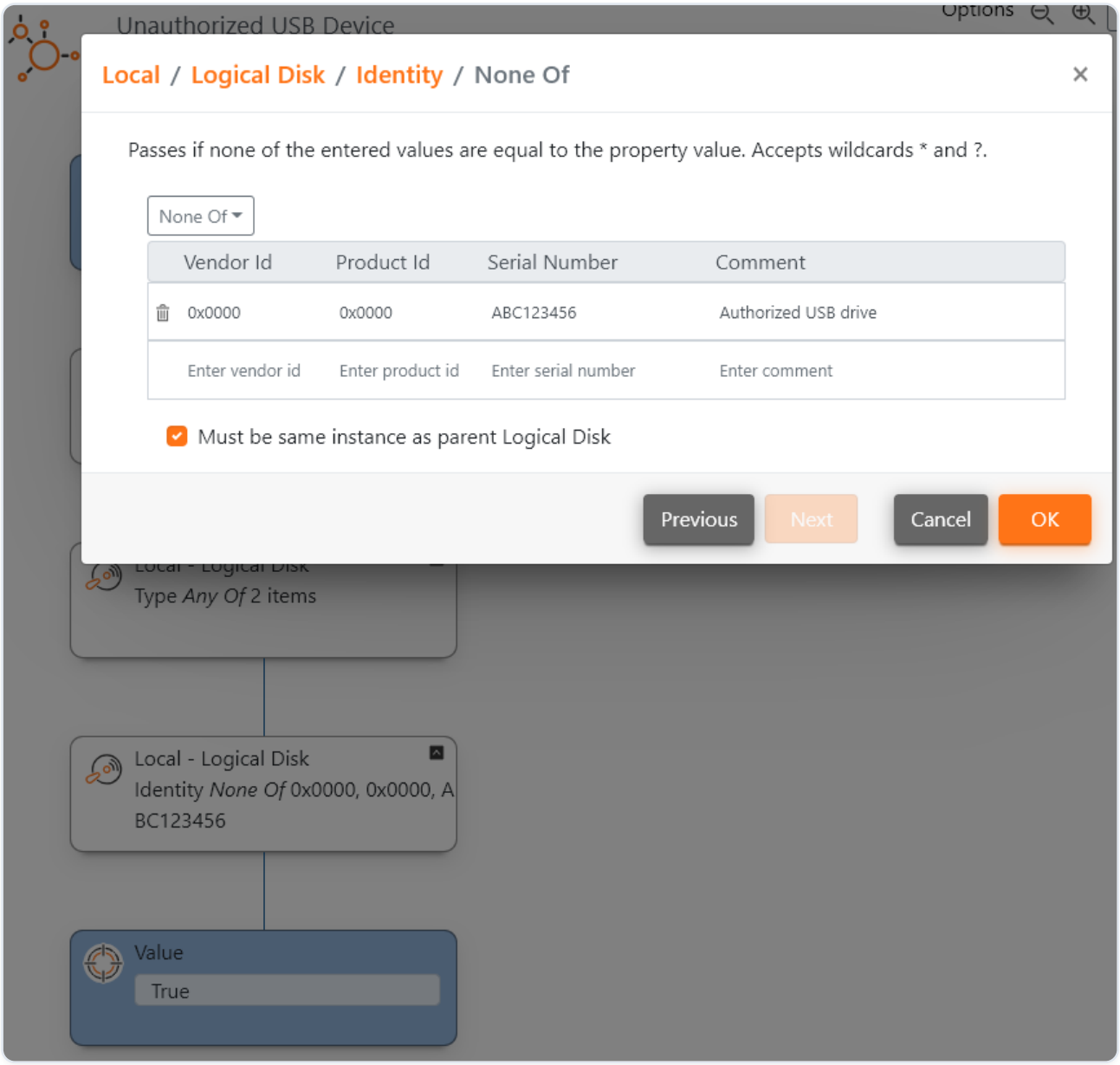


A confirmation of the successful import apears, confirm with `OK`.

At the top of the console you´ll find the count of configured Context, Actions, Messages, Settings.

Select `Context`, `Unauthorized USB Device` and click on the 3rd white property box `Local / Logical Disk / Identity / None of`.

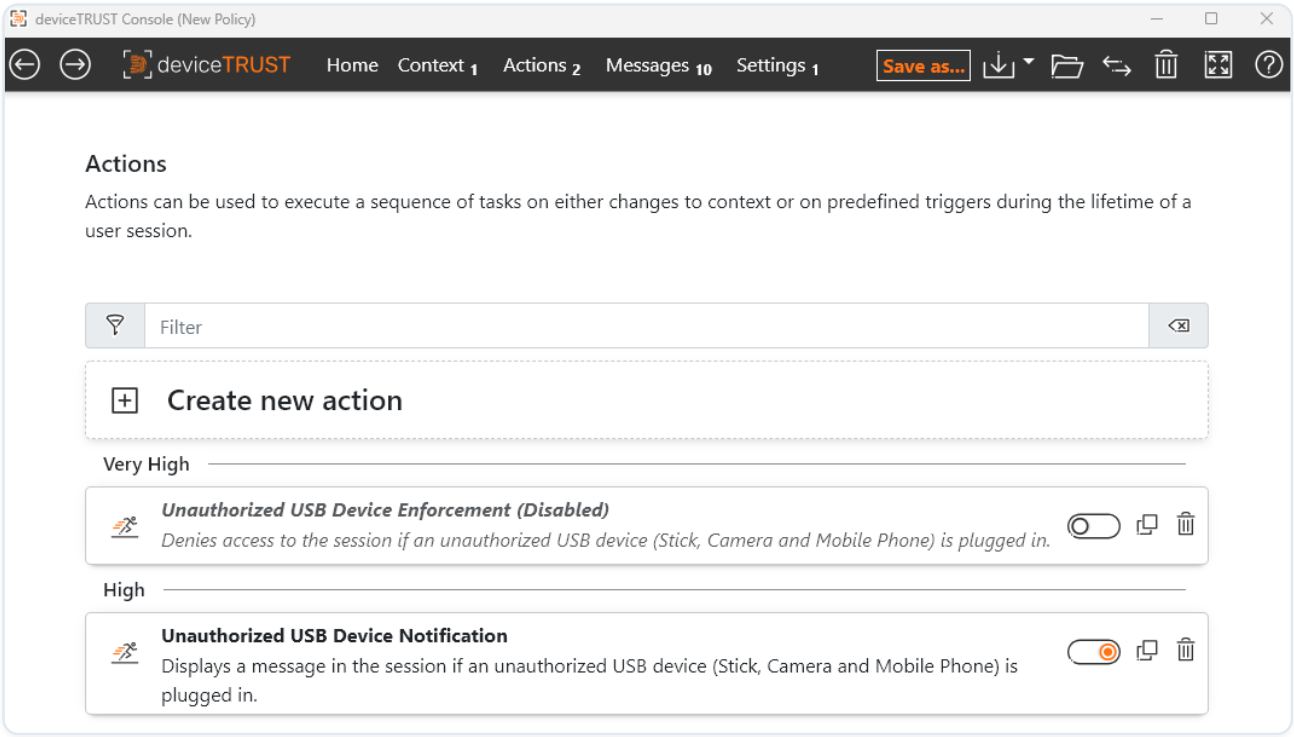
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Add allowed USB drives line by line, other USB drives will be seen as unauthorized, and confirm with `OK`.

Select `Actions` and see one active (Unauthorized USB Device Notification) and one disabled (Unauthorized USB Device - Enforcement) action. Depending on whether you only want to inform about the execution of the policy or block access, select what should be active using the Enable/Disable toggle on the right side of the respective action.

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

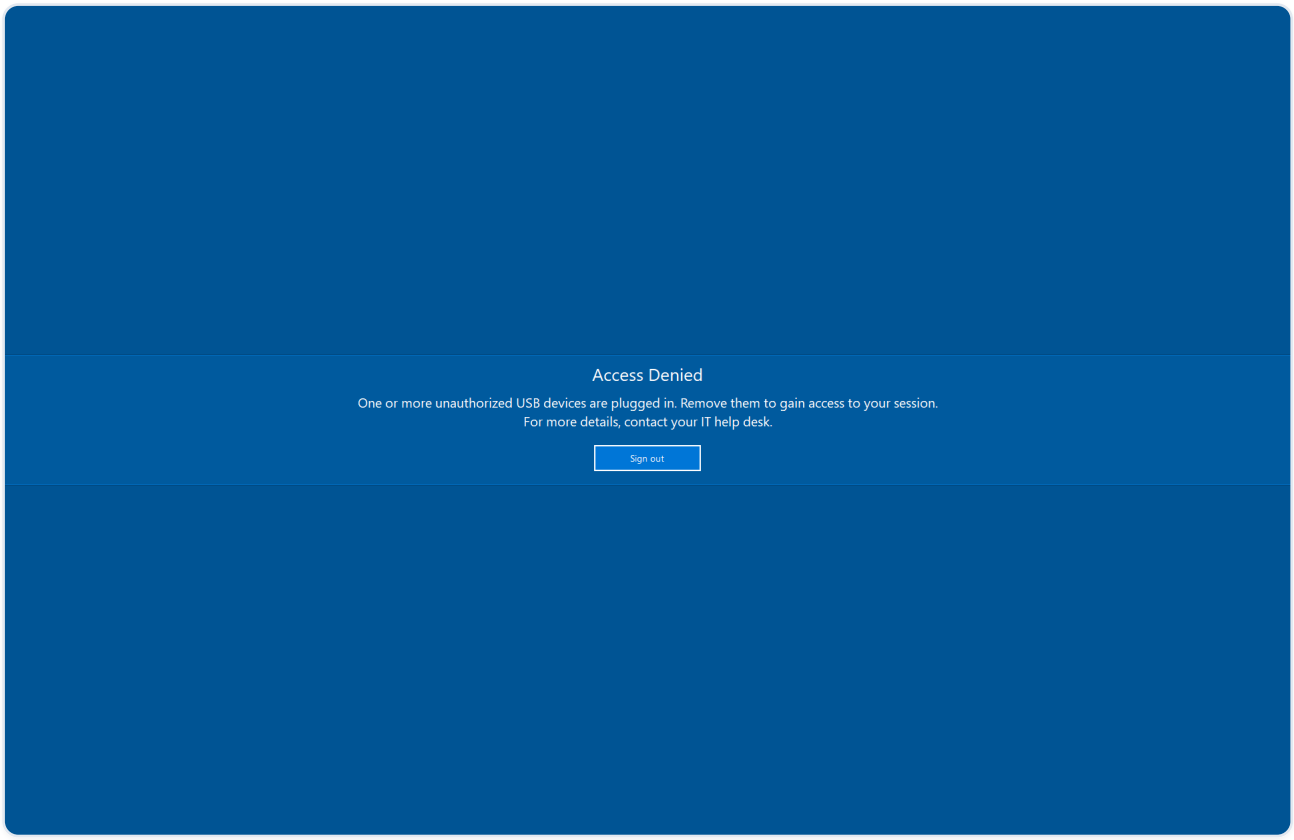


Save the policy whether as `Local Policy` or `File-Based Policy`. Check Policy Loading to find the correct folder to save file-based policies.

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.



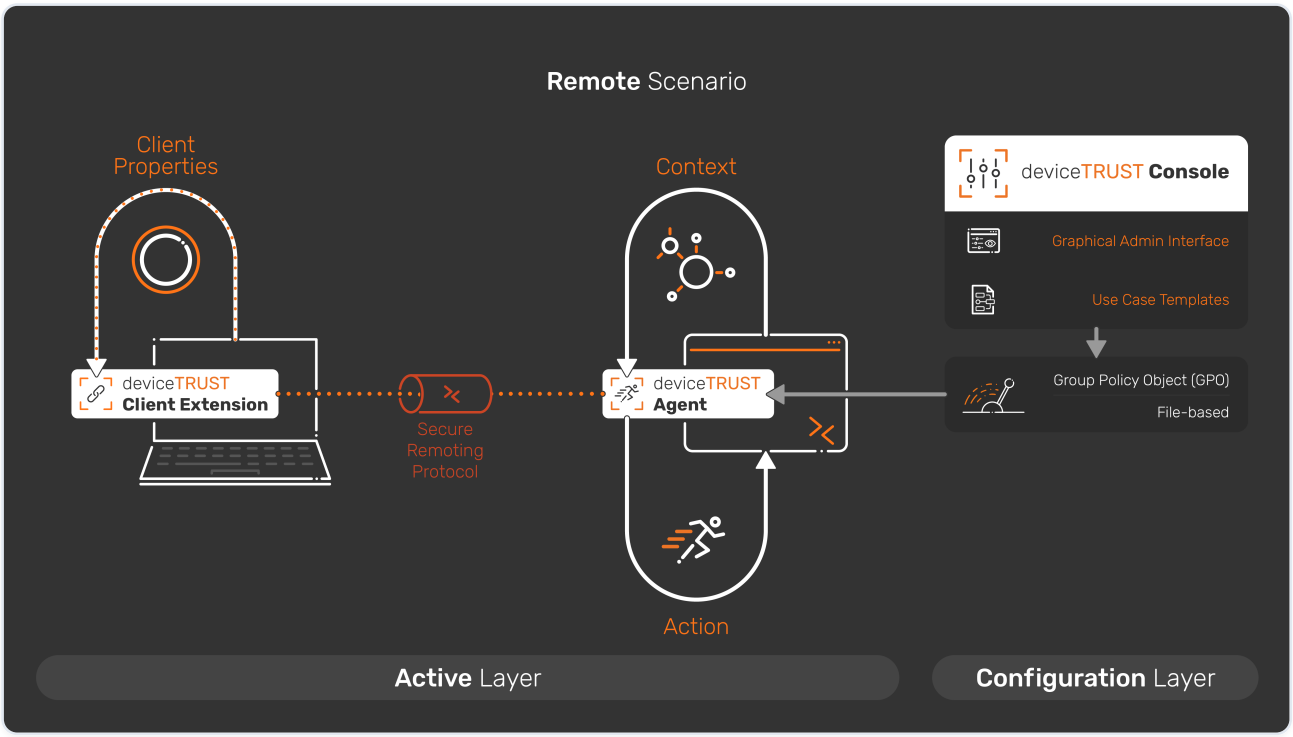
Troubleshooting

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 simple use case within your remote environment.

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



We will perform the following steps:

- Prerequisites
- Option 1: Citrix® installation packages
  - 1.1: Download the Citrix product software
  - Step 1.2: Install Citrix deviceTRUST
  - Step 1.3: Install the deviceTRUST Console
  - Step 1.4: Enter your deviceTRUST License
  - Step 1.5: Install the xdeviceTRUST Client Extension on a Microsoft Windows device
- Option 2: Manual installation
  - Step 2.1: Download the deviceTRUST setup binaries
  - Step 2.2: Install the deviceTRUST Agent
  - Step 2.3: Install the deviceTRUST Console
  - Step 2.4: Enter your deviceTRUST License
  - Step 2.5: Install the deviceTRUST Client Extension on a Microsoft Windows device
- Set up a simple use case
  - Step 1: Create and apply a file based configuration

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

- Step 2: Check the access to your VDA when the deviceTRUST Client Extension is not installed
- Step 3: Test the Compliance Check use case from a Microsoft Windows device

Prerequisites

Before getting started with deviceTRUST in a remote access environment, make sure the following components are available:

- **Windows session host (VDA):**

  At least one Windows session host with the deviceTRUST Agent installed. (Included in Citrix Virtual Apps and Desktops™ 2503 or later)

- **Endpoint device:**

  At least one endpoint (e.g., Windows 11) with the deviceTRUST Client Extension installed. (Included in Citrix Workspace™ App 2503 or later)

- **Policy management device:**

  A Windows device used to install the deviceTRUST Console and provide the deviceTRUST policy. Choose one of the following options to deploy the policy:

  - **Option 1 – Group Policy (GPO):** The Windows device must have permission to create and edit a GPO for the session host.
  - **Option 2 – File-based policy deployment:** An administrative user must transfer the deviceTRUST policy from the Windows device to the session host at: C:\ProgramData\deviceTRUST\Policy (The deviceTRUST Console is available on the Citrix Virtual Apps and Desktops 2503 or later Product ISO within the ‘x64\deviceTRUST’ folder)

- **Citrix Policy Management:**

  An administrative user must be available to create and edit Citrix Policies using Citrix Studio or Web Studio.

- **Test user account:**

  A non-administrative user for testing access from the endpoint to the session host.

If you plan to use deviceTRUST in combination with other tools (e.g. Microsoft AppLocker or FSLogix App Masking), ensure that these components are installed and working properly. If deviceTRUST is intended to take over functionality previously managed by other tools (e.g.

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

clipboard redirection via Citrix Policy), make sure those features are disabled or unconfigured to avoid conflicts.

Option 1: Citrix installation packages

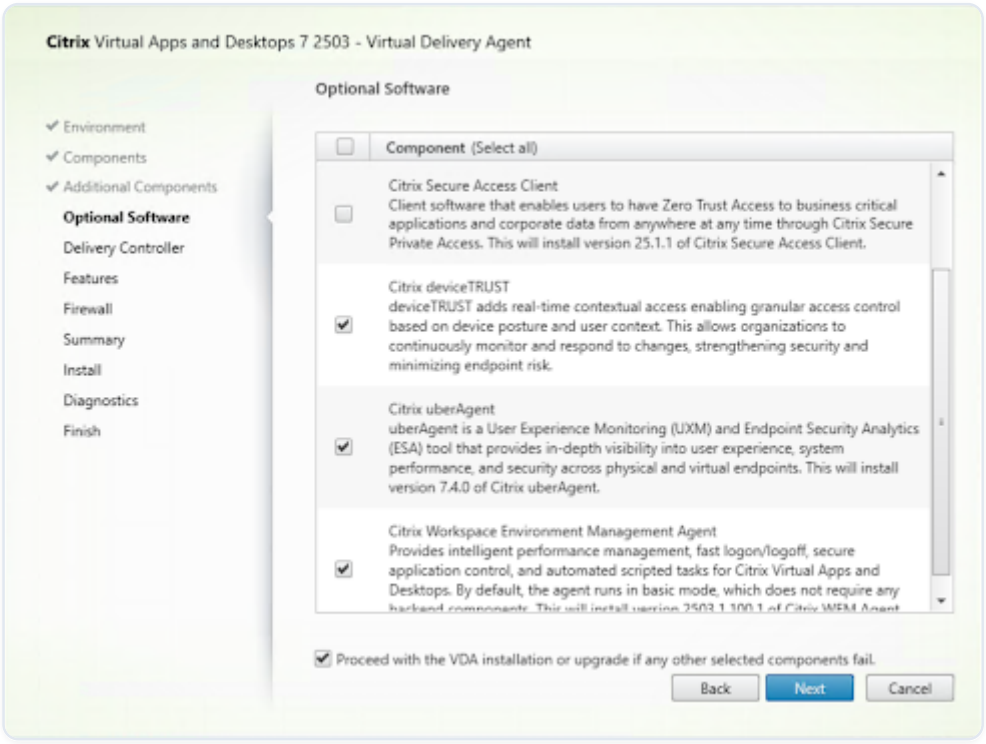
1.1: Download the Citrix product software

The deviceTRUST software is included from Citrix Virtual Apps™ and Desktop 7 2503.

Follow the VDA installation guide to get the right version.

Step 1.2: Install Citrix deviceTRUST

In the VDA Setup Wizard, Citrix deviceTRUST is part of the Optional Software:



Check the box and proceed with the installation.

Step 1.3: Install the deviceTRUST Console

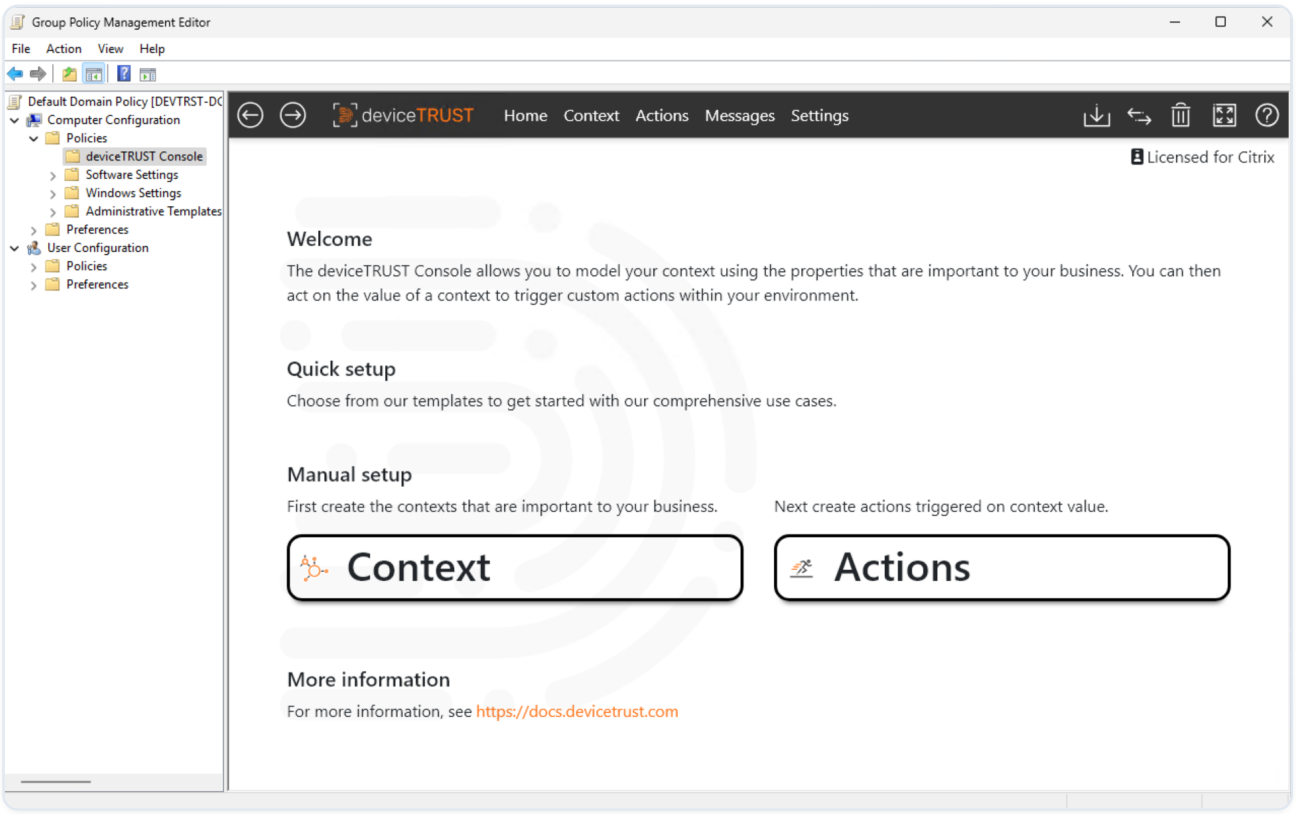
To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the contextual security policies to the deviceTRUST Agent. Those options are using the Local Policy Editor, a Group Policy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

The latest deviceTRUST console can be found on our Download page. Download the full binaries and just use the console installation file.

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

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.

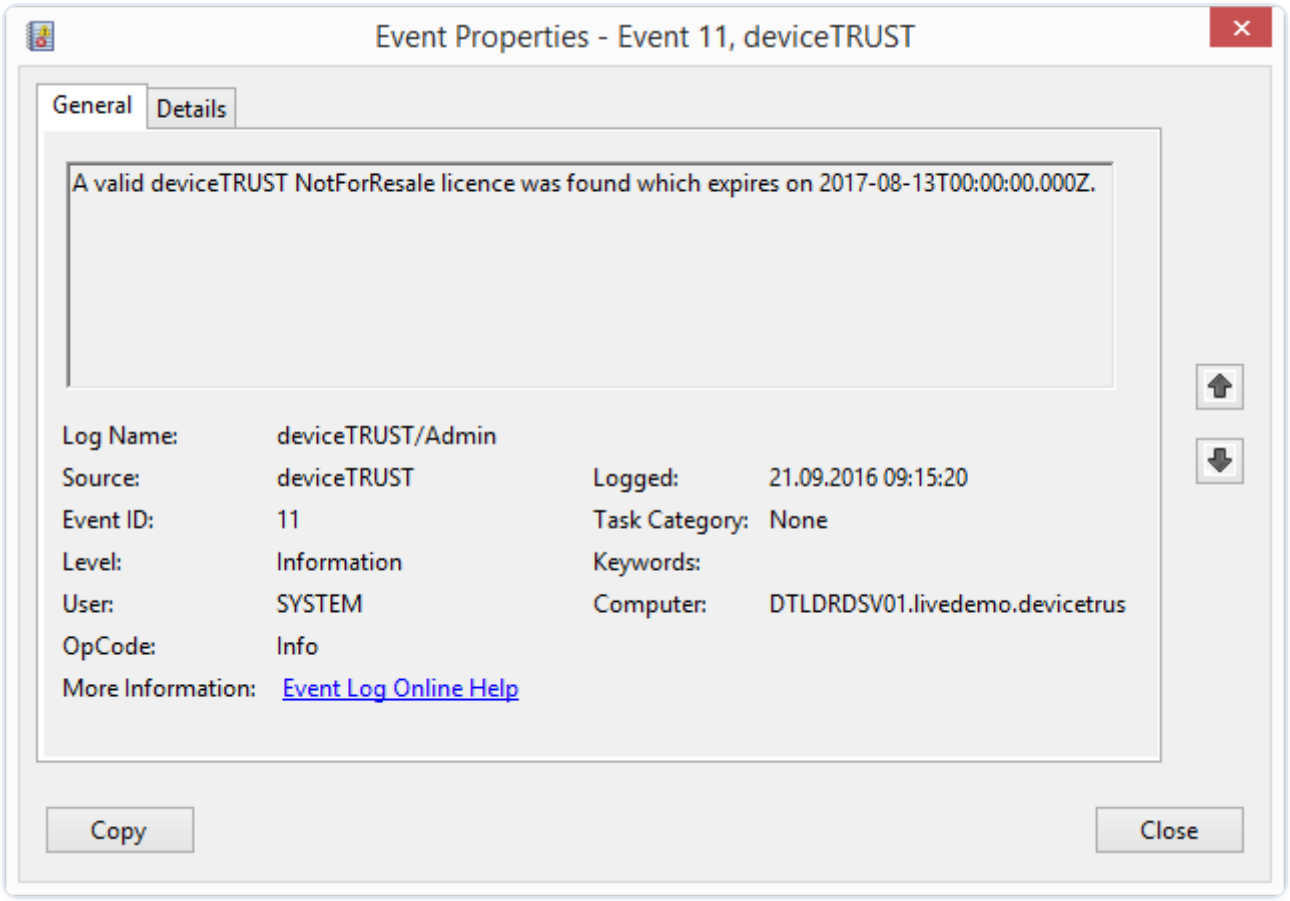


Step 1.4: Enter your deviceTRUST License

Adding a deviceTRUST license is only necessary in a non CVAD environment.

For a CVAD environment, Citrix deviceTRUST is now enabled and will work for all users except local administrators connecting to that remoting or DaaS host system with Citrix deviceTRUST Agent installed. To check if a valid deviceTRUST license is applied, 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 1.5: Install the deviceTRUST Client Extension on a Microsoft Windows device

Follow the information on Installation Client Extension page.

Option 2: Manual installation

Step 2.1: Download the deviceTRUST setup binaries

The latest deviceTRUST software can be found on our Download page.

Step 2.2: Install the deviceTRUST Agent

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

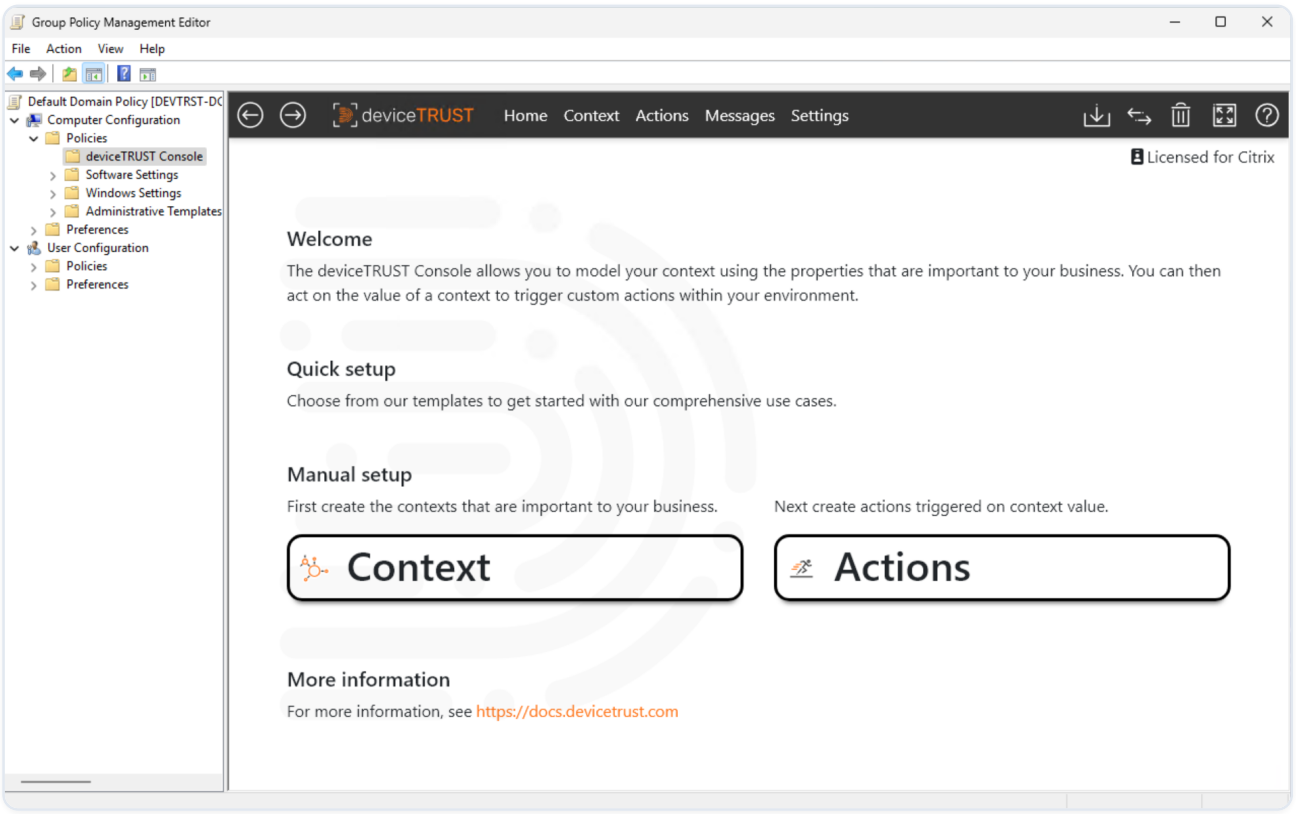
Step 2.3: Install the deviceTRUST Console

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.

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

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.

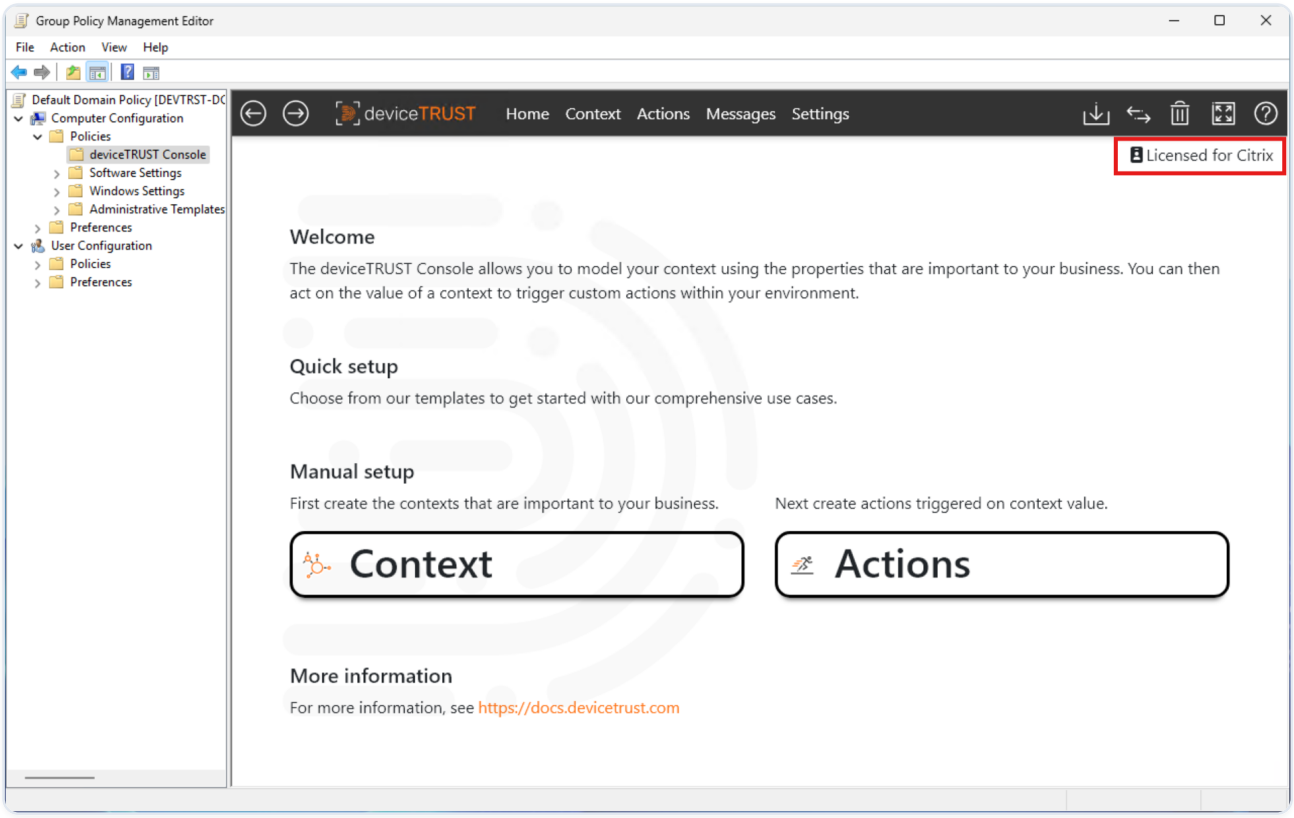


Step 2.4: Enter your deviceTRUST License

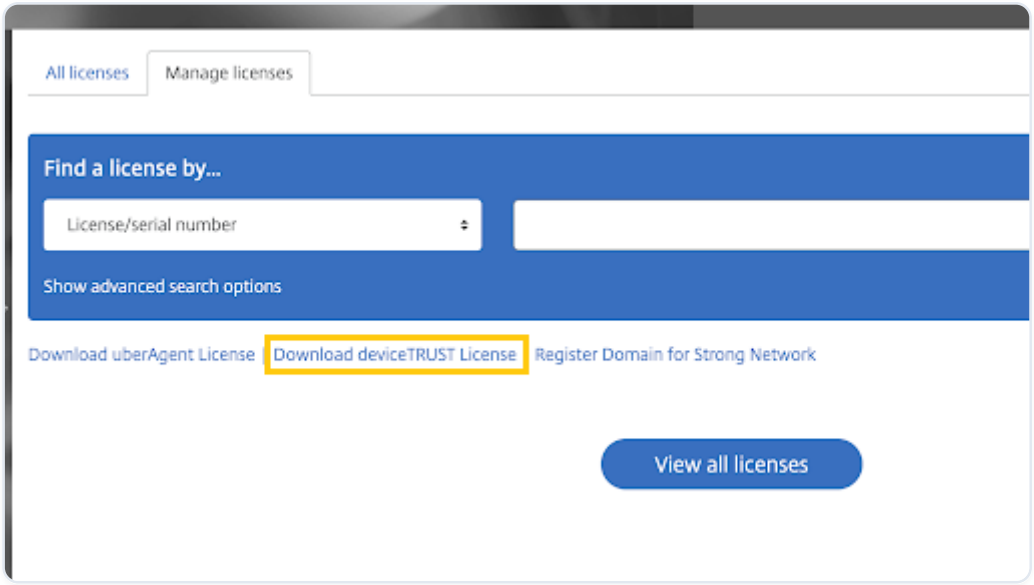
Adding a deviceTRUST license is only necessary in a non CVAD environment.

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.

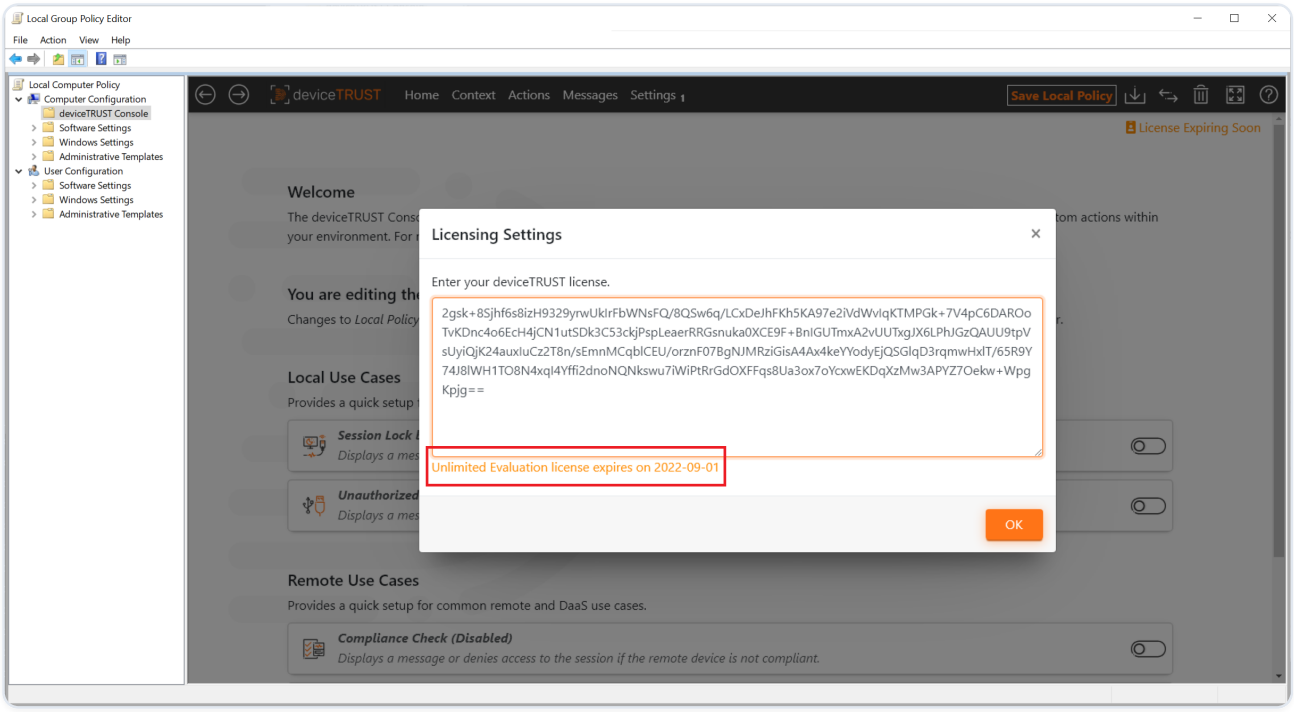


Dependent on your license, your individual deviceTRUST license can be found in your MyCitrix Portal.

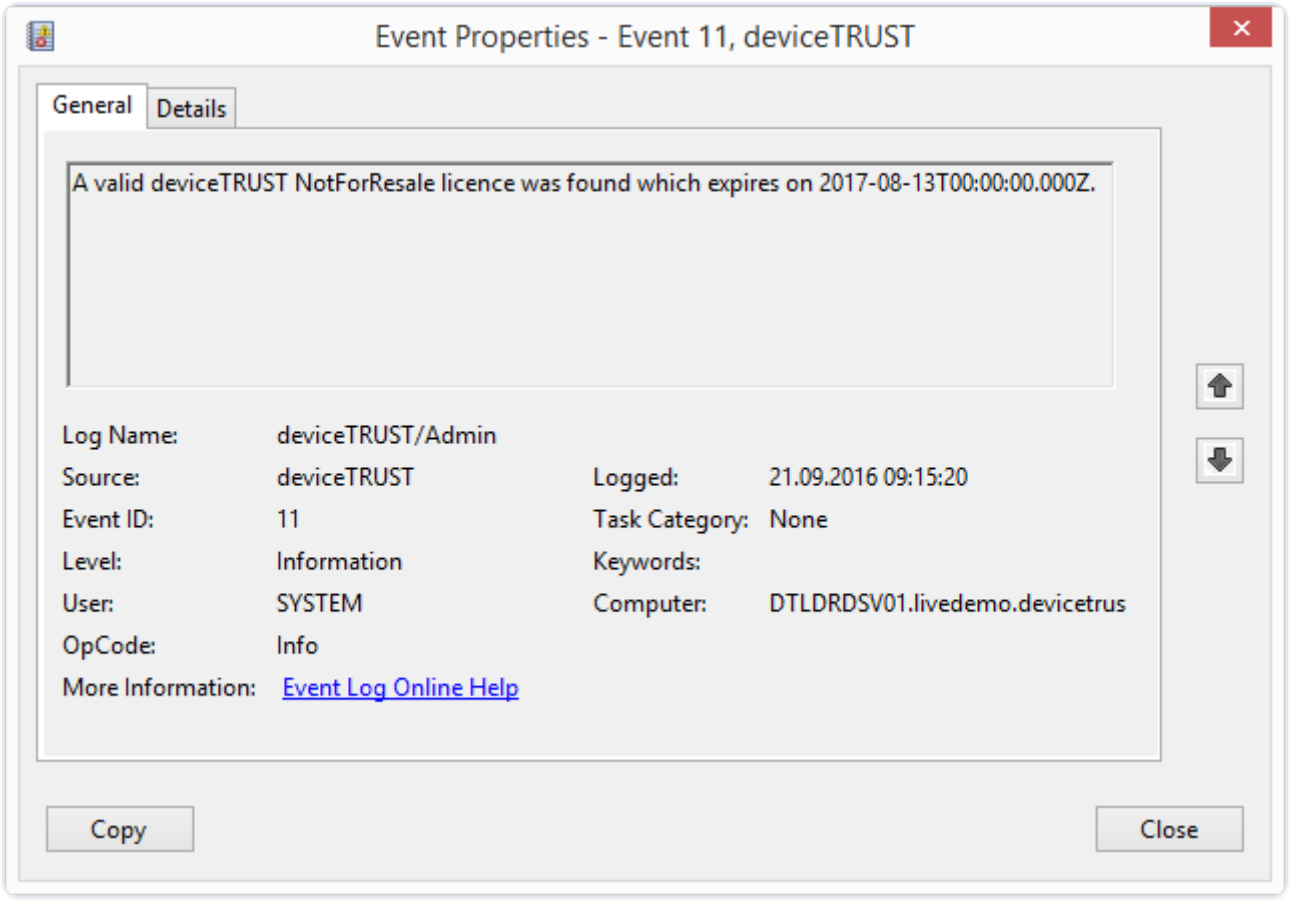


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.

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



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 2.5: Install the deviceTRUST Client Extension on a Microsoft Windows device

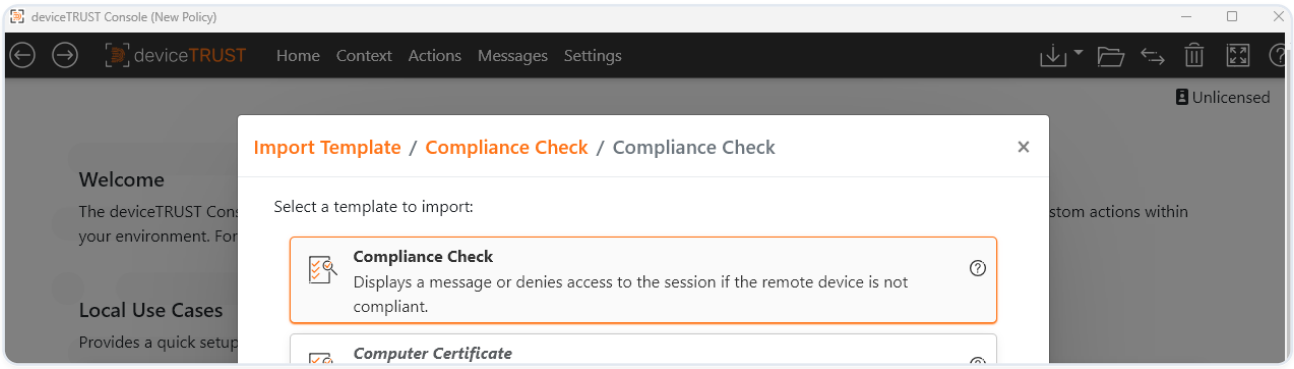
Within the Getting Started Guide, for simplicity, we will only install the deviceTRUST Client Extension on a Microsoft Windows device. Other device operating systems are also supported and an overview of how to install the deviceTRUST Client Extension on the particular operating system can be found on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

Set up a simple use case

Step 1: Create and apply a file based configuration

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 create a New Policy.

Select `Sharing` top right and click `Import Template`, `Compliance Check`, `Compliance Check` and confirm with `Import Template` at the bottom.

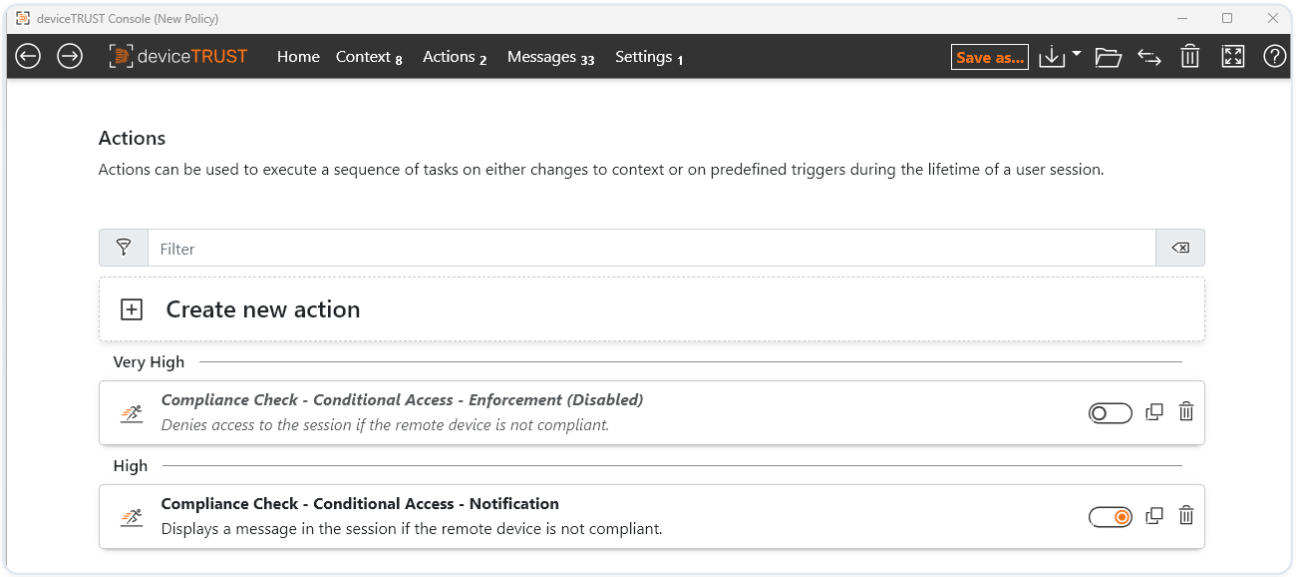


A confirmation of the successful import apears, confirm with `OK`.

At the top of the console you´ll find the count of configured Context, Actions, Messages, Settings.

Select `Actions` and see one active (Compliance Check - Conditional Access - Notification) and one disabled (Compliance Check - Conditional Access - Enforcement) action. Depending on whether you only want to inform about the execution of the policy or block access, select what should be active using the Enable/Disable toggle on the right side of the respective action.

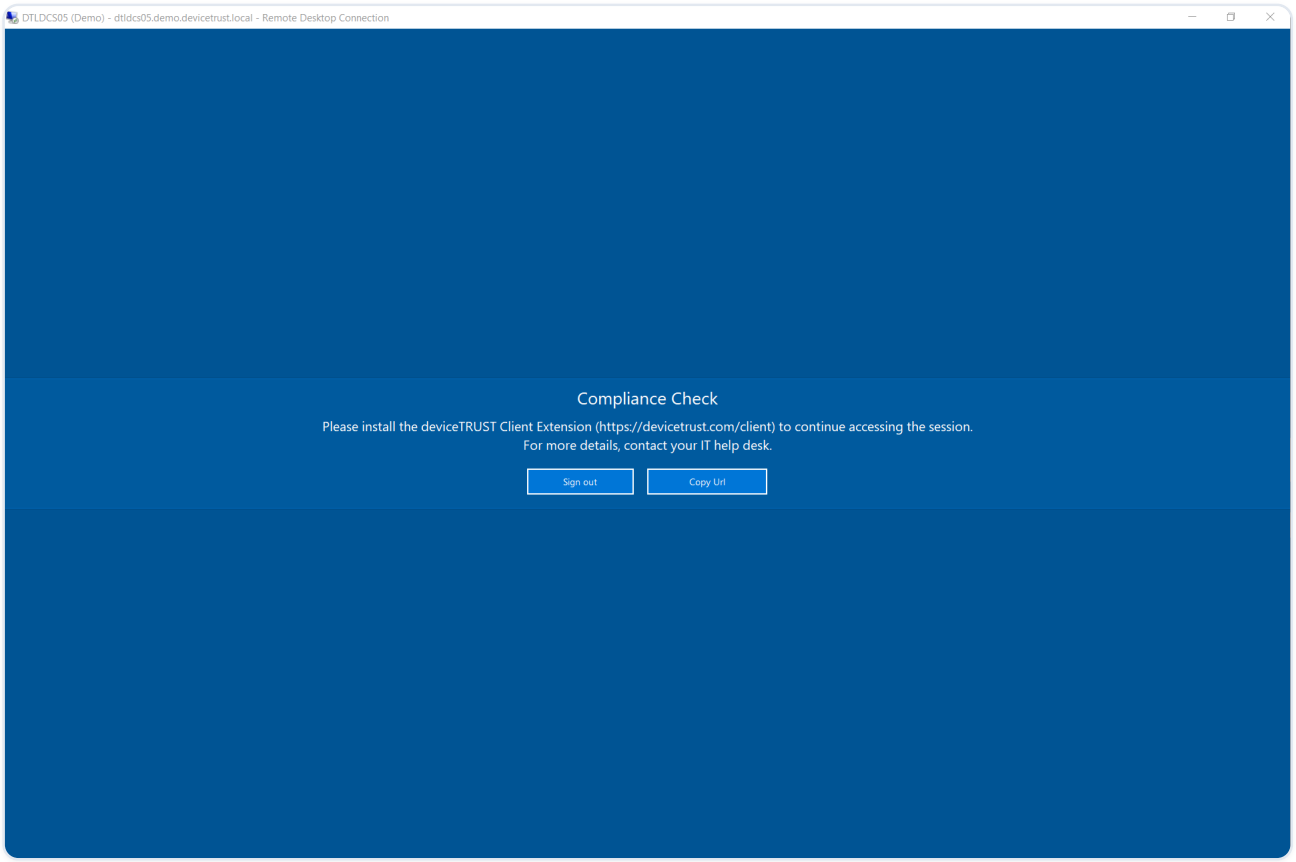
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Save the policy whether as `Local Policy` or `File-Based Policy`. Check Policy Loading to find the correct folder to save file-based policies.

Step 2: Check the access to your VDA when the deviceTRUST Client Extension is not installed

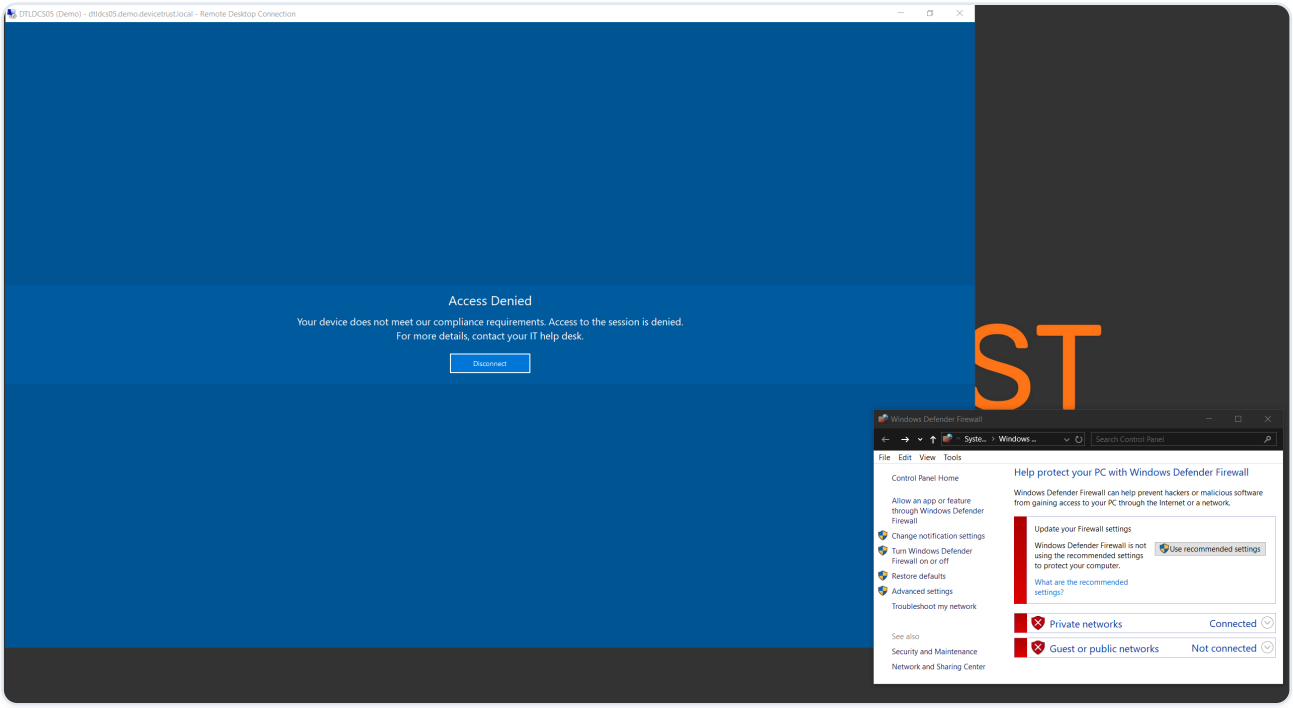
From a device without the deviceTRUST Client Extension installed, connect to your VDA. Because the remote device does not have an active deviceTRUST Client Extension, you´ll get a response according to your active Action, like the access will be denied with the following message:



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

Step 3: 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 VDA. 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.



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.

Downloads

Download deviceTRUST® Client Extension 2503 CR for Microsoft Windows, Apple macOS and Ubuntu

The deviceTRUST Client Extension for Microsoft Windows, Apple macOS and Ubuntu is now installed by default as part of Citrix Workspace app when using release 2503 or later. This can be downloaded from Citrix Downloads.

Download deviceTRUST Client Extension 2503 CR for eLux® 7

The deviceTRUST Client Extension is available for eLux 7 as part of the Citrix Workspace app 2503 or later and is available to download on the myelux portal.

Download deviceTRUST Agent and Console 2503 CR

The deviceTRUST Agent is installed by default as part of the Citrix Virtual Apps and Desktops VDA installation when using release 2503 or later. The deviceTRUST Console can be found within the Product ISO of Citrix Virtual Apps and Desktops 2503 or later, within the ‘x64\deviceTRUST’ folder. These can be downloaded from Citrix Downloads.

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

Installation

TABLE OF CONTENTS

- Agent
- Console
- Client Extension
- Compatibility between components

Installing the deviceTRUST Agent

- Option 1: Install Citrix VDA 2503 or later
- Option 2: Manual Installation
- Option 3: Unattended Installation

Option 1: Install Citrix VDA 2503 or later

The deviceTRUST Agent is now installed by default as part of the Citrix Virtual Apps and Desktops VDA installation when using release 2503 or later. This can be downloaded from Citrix Downloads.

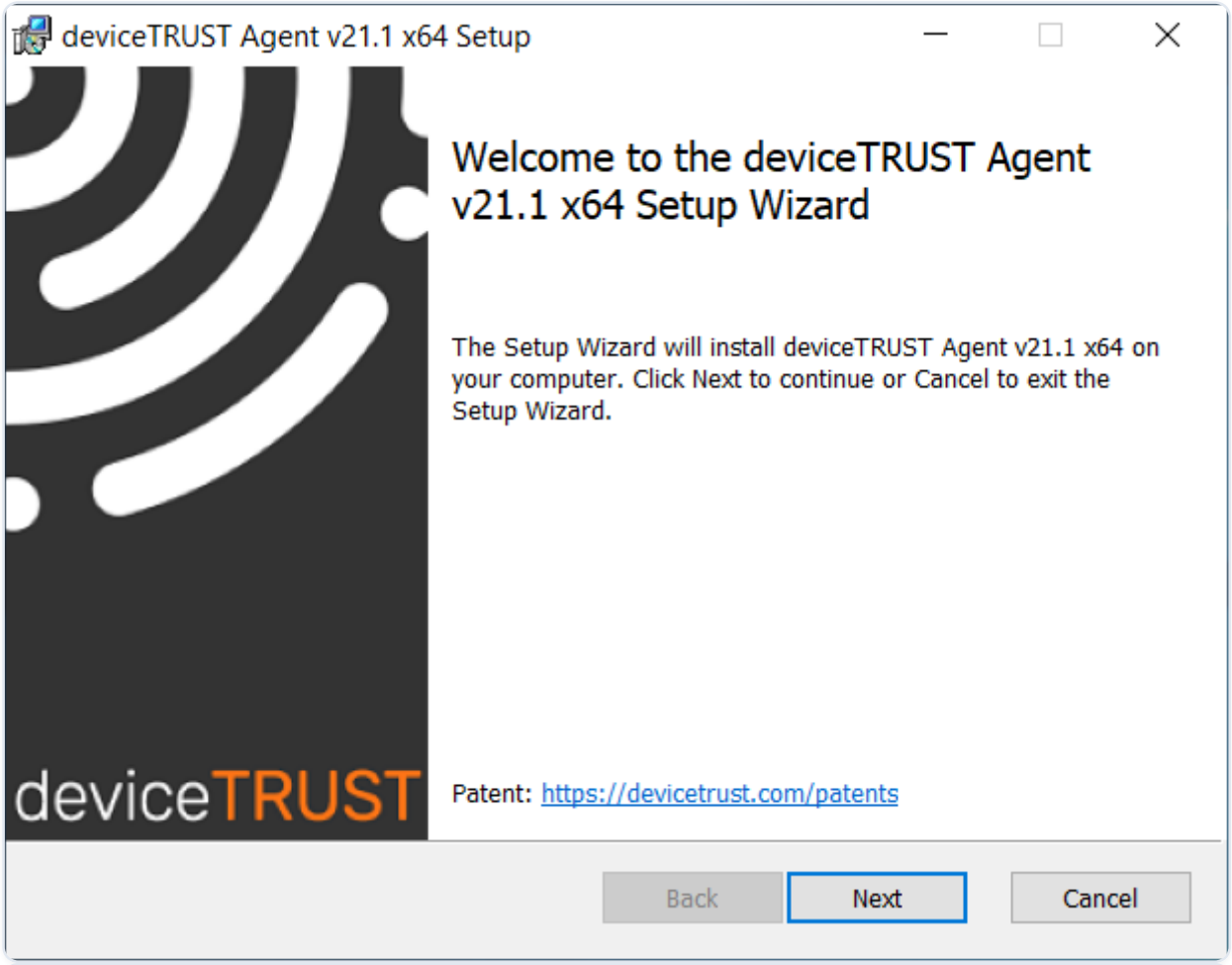
IMPORTANT:

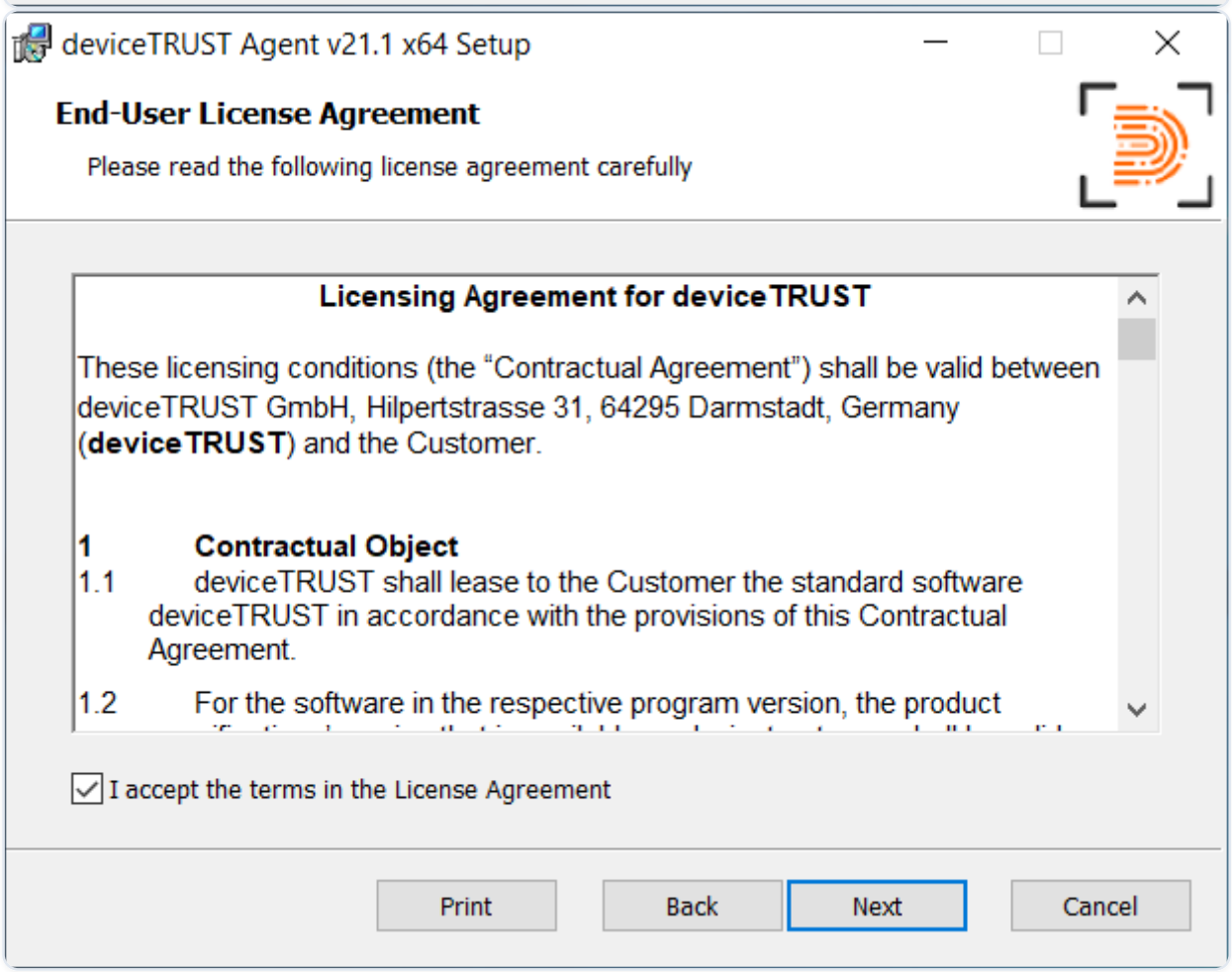
When using Citrix Virtual Apps and Desktops™, you may need to edit the Virtual channel allow list policy to allow the deviceTRUST Agent to open a virtual channel to the deviceTRUST Client Extension.

Option 2: Manual Installation

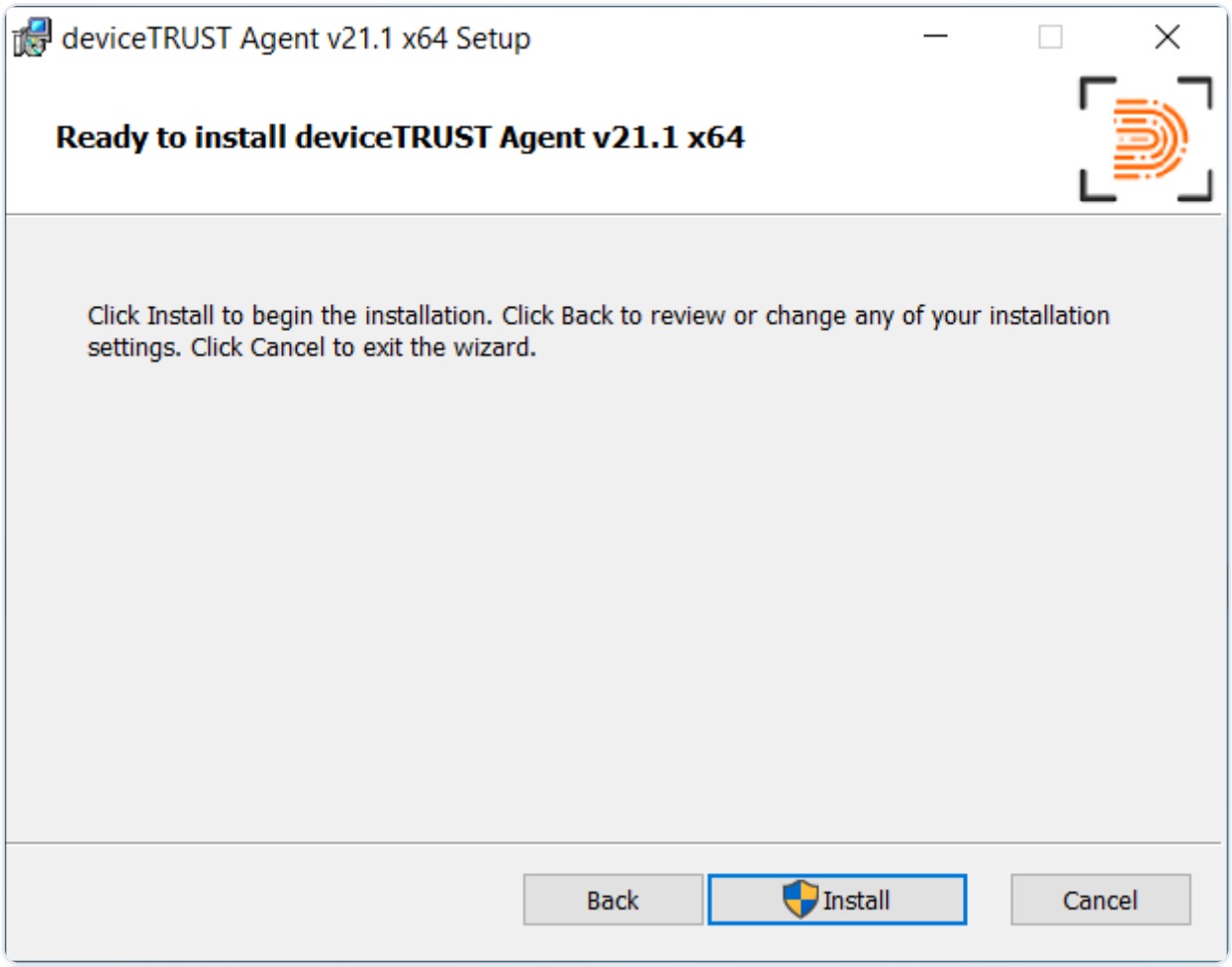
The deviceTRUST Agent requires a user account with local administrative privileges to install the deviceTRUST Agent on the target system. The installation can be performed by following the steps of the deviceTRUST Agent installer.

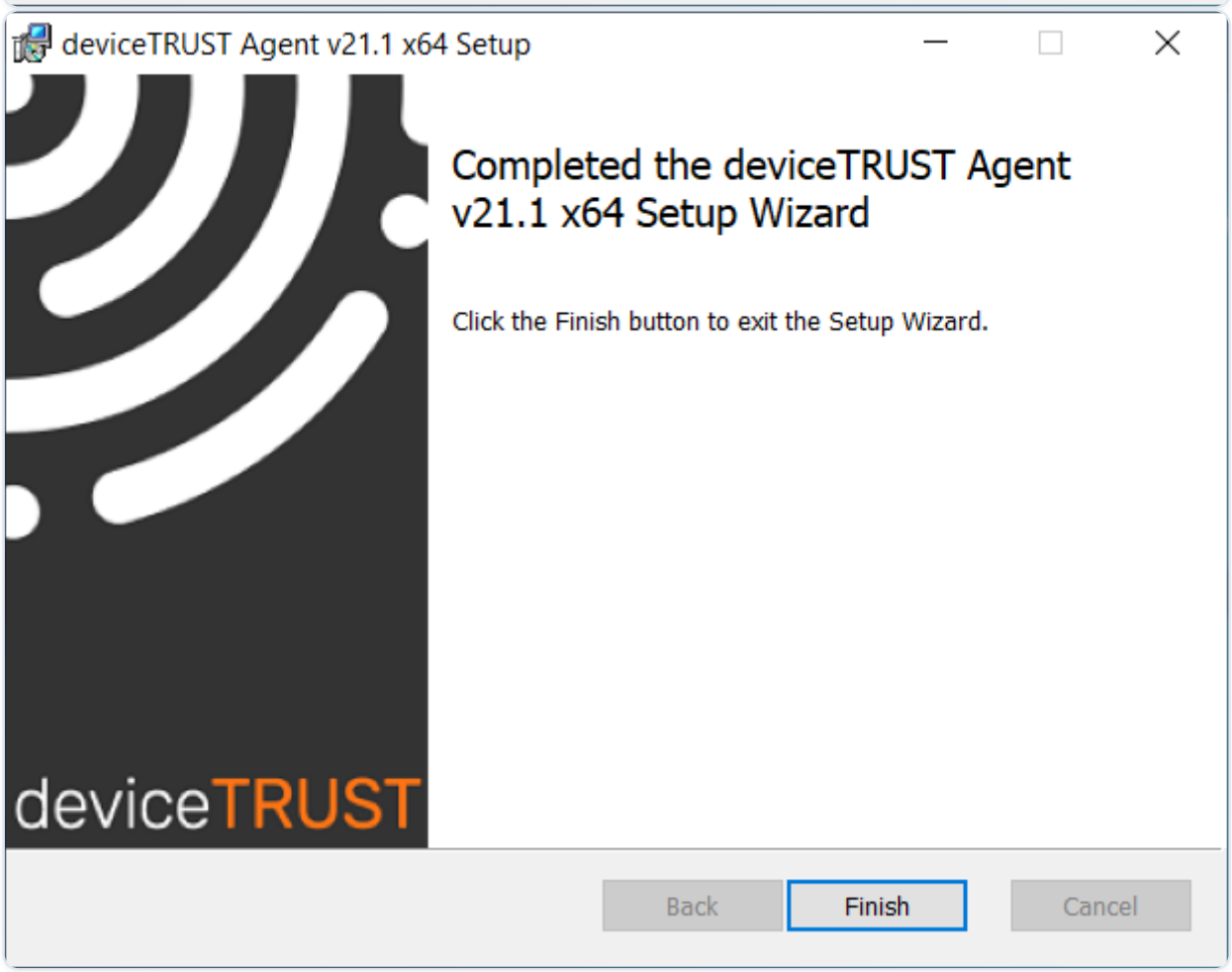
© 1997–2026 Citrix Systems, Inc. All rights reserved.



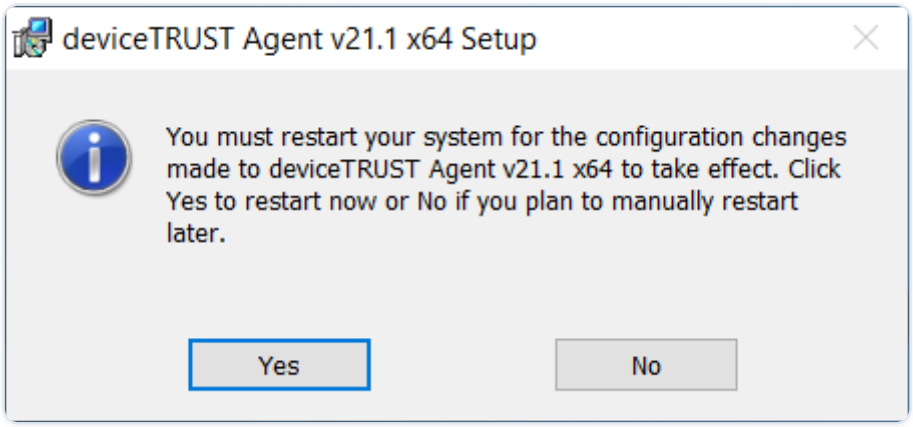


© 1997–2026 Citrix Systems, Inc. All rights reserved.





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



IMPORTANT:

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 Extension.

Note:

- Installation path: %PROGRAMFILES%\Citrix\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

Option 3: 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`

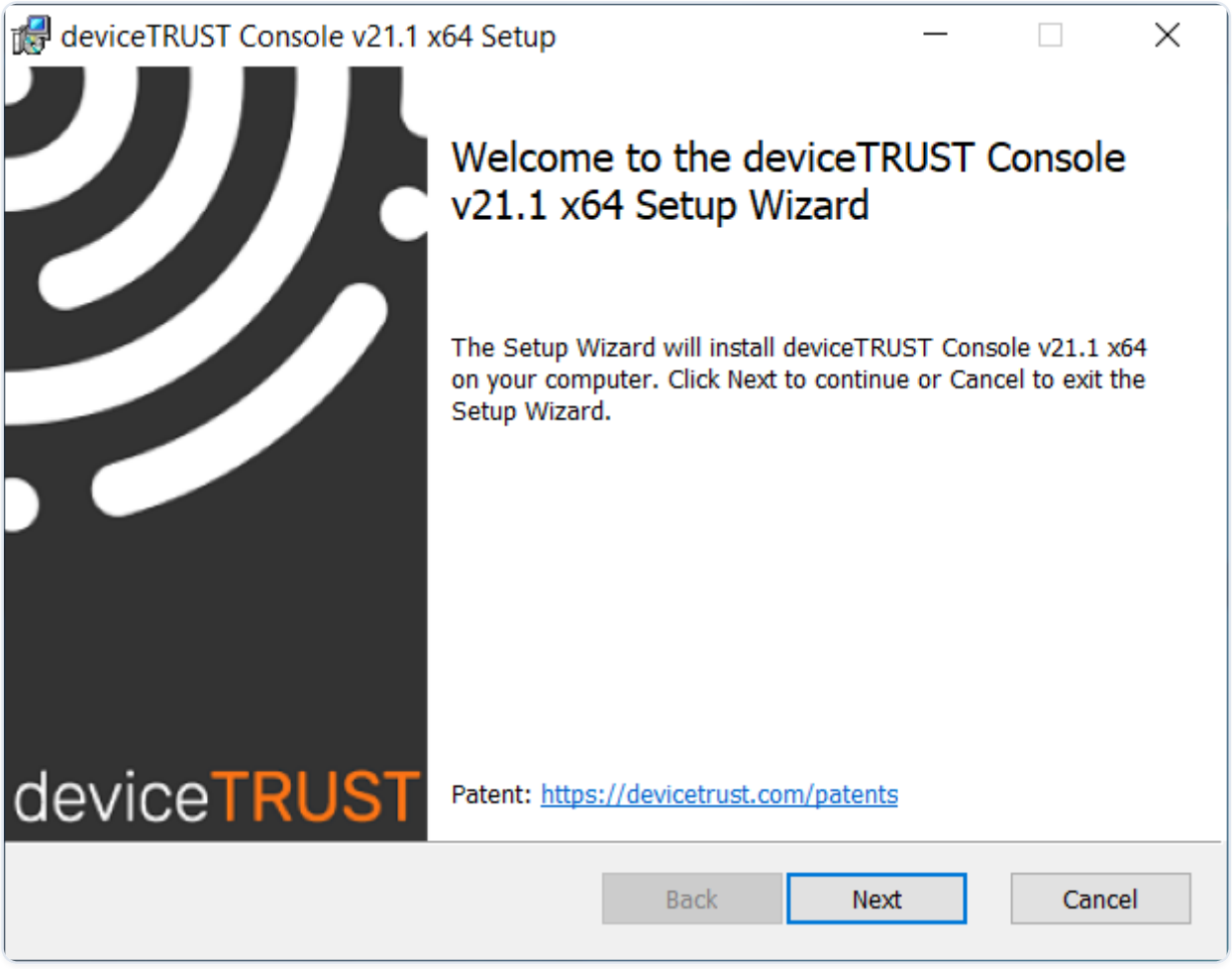
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

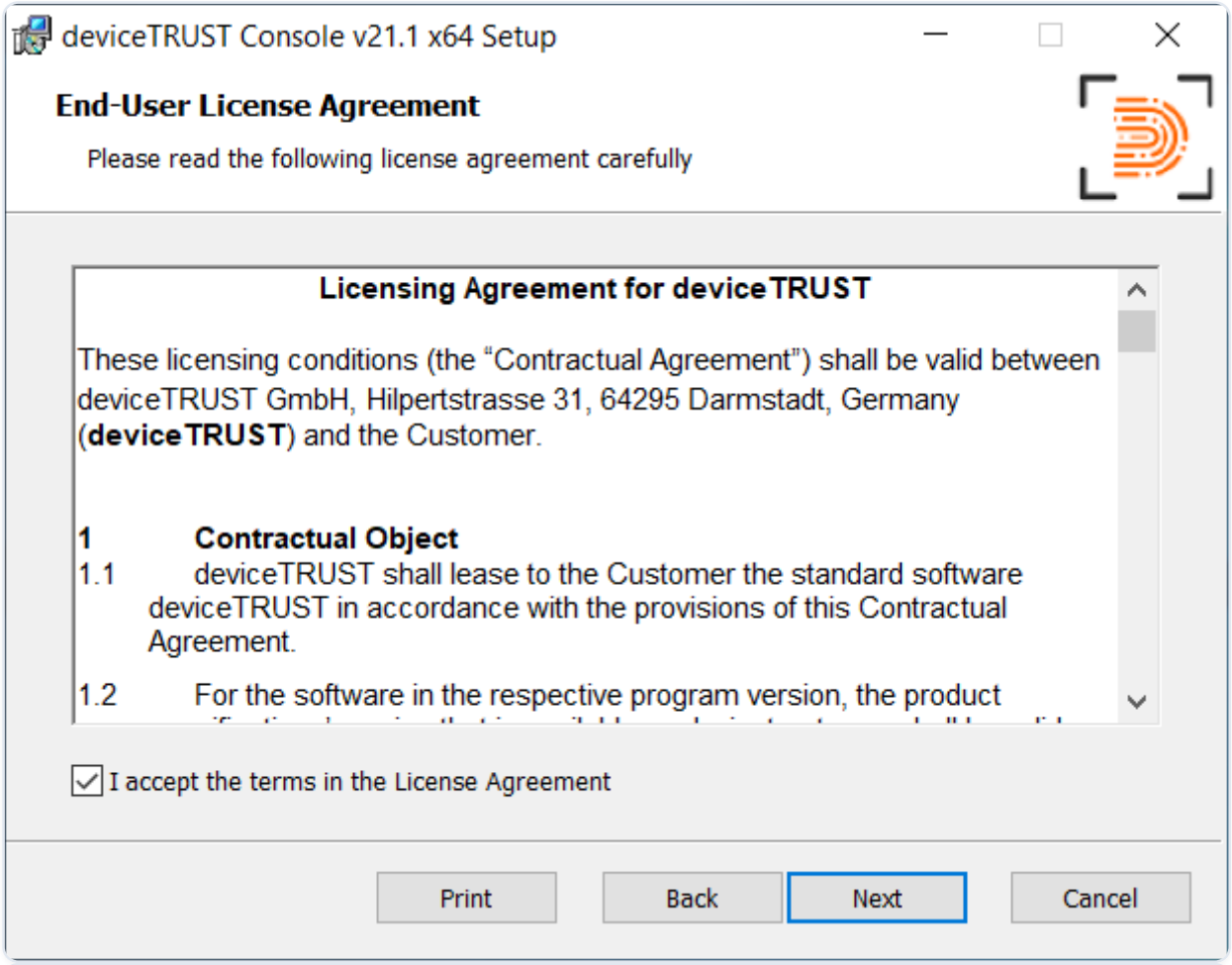
When using Citrix Virtual Apps and Desktops, you may need to edit the Virtual channel allow list policy to allow the deviceTRUST Agent to open a virtual channel to the deviceTRUST Client Extension.

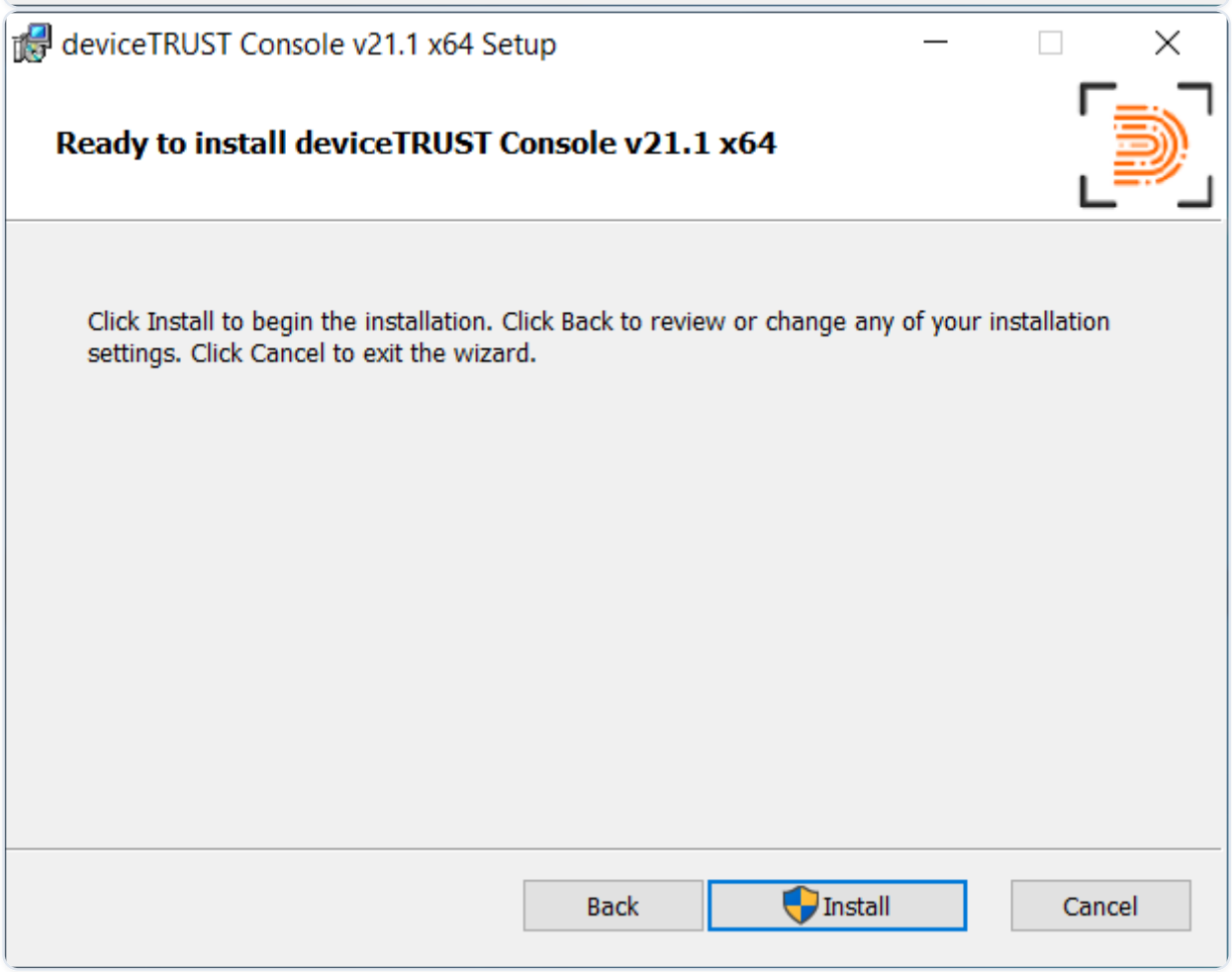
Installing the deviceTRUST Console

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.

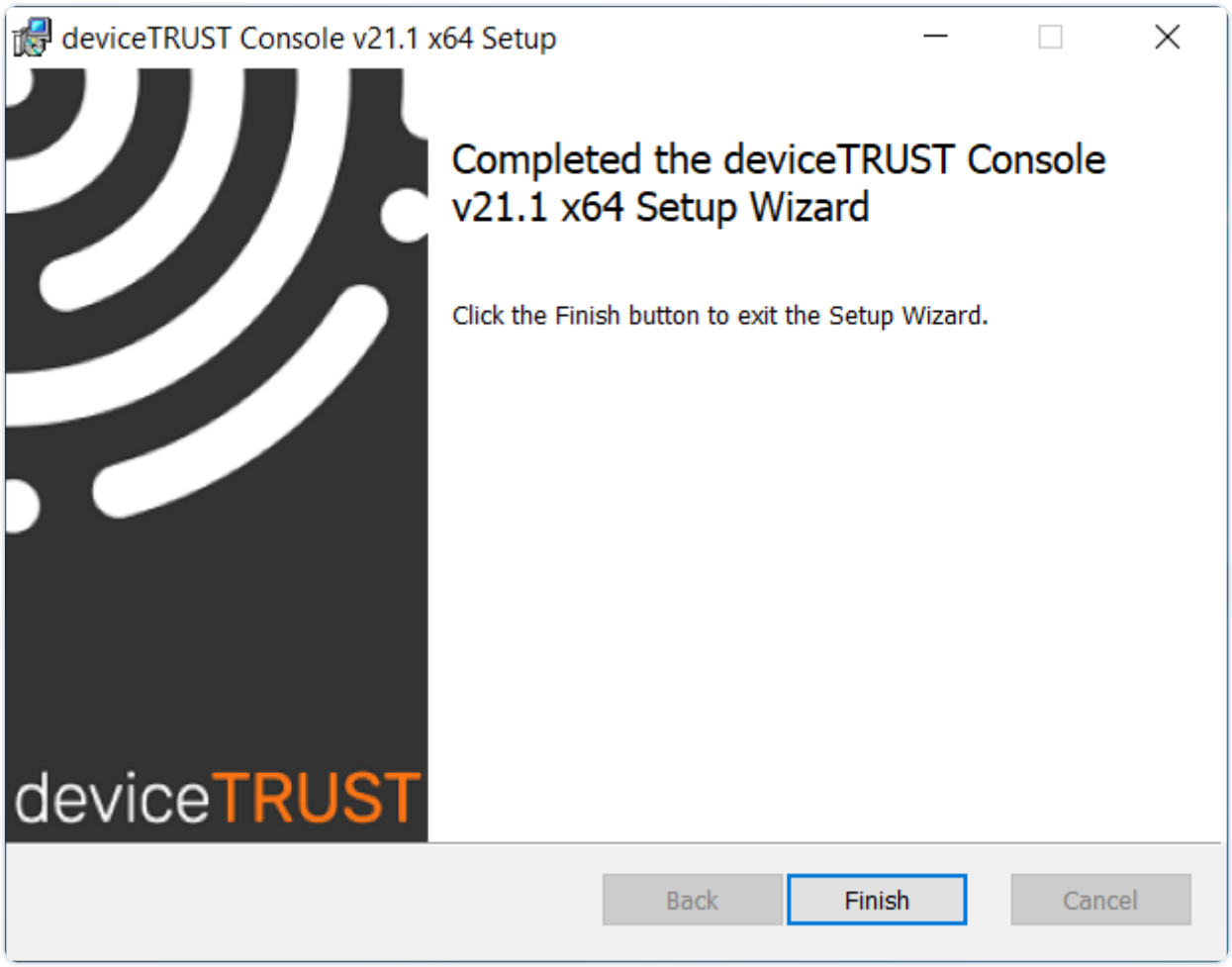


© 1997–2026 Citrix Systems, Inc. All rights reserved.





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



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`

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

Installing the deviceTRUST Client Extension

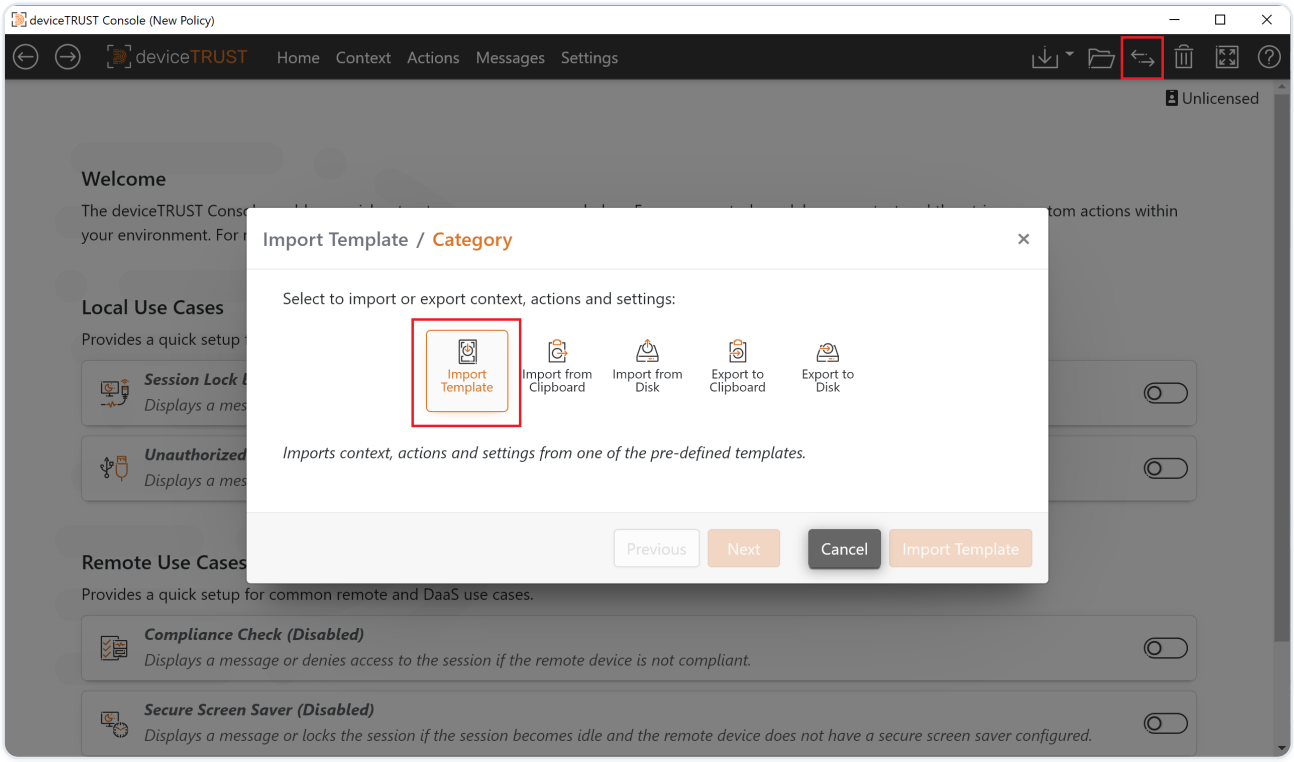
TABLE OF CONTENTS

- Microsoft Windows
- Apple macOS
- Apple iOS and iPadOS
- Ubuntu
- eLux 7

© 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 and then `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.

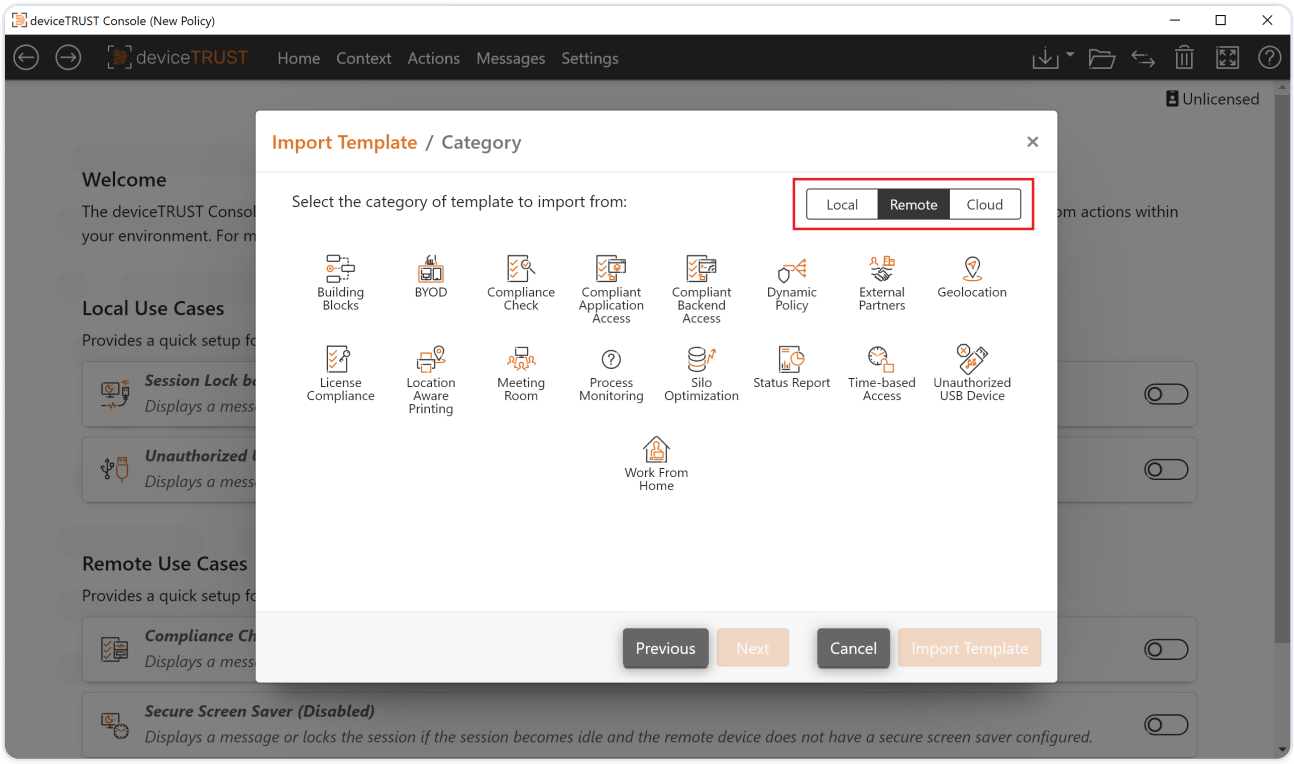


TABLE OF CONTENTS

- 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.

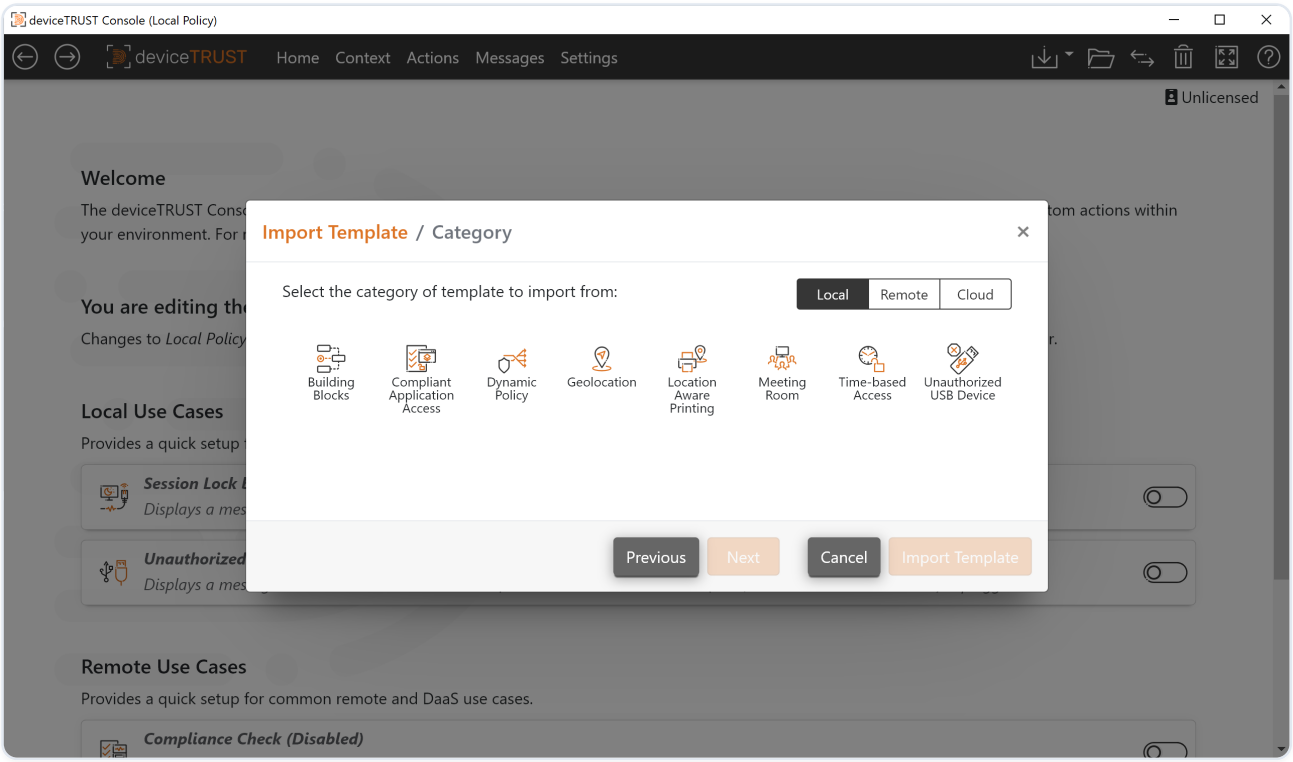


TABLE OF CONTENTS

- 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.

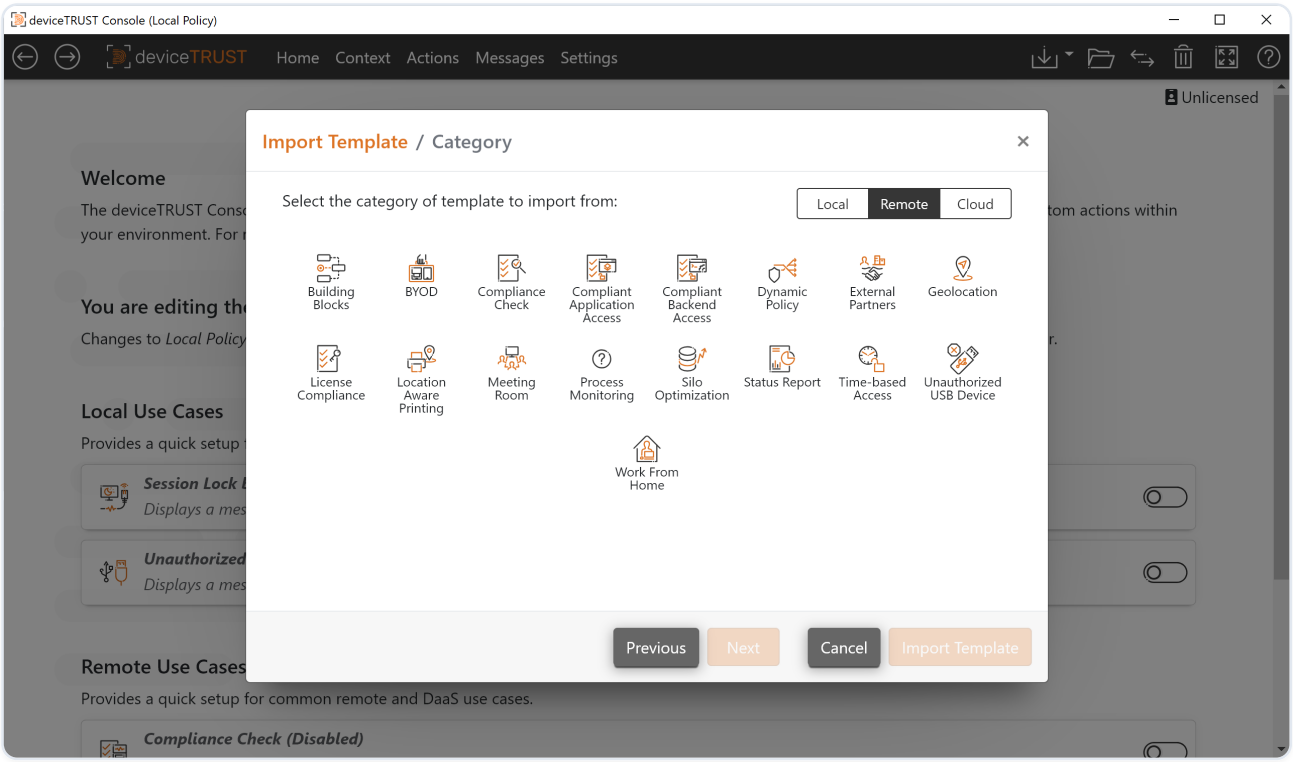


TABLE OF CONTENTS

- 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 remote 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 remote 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.

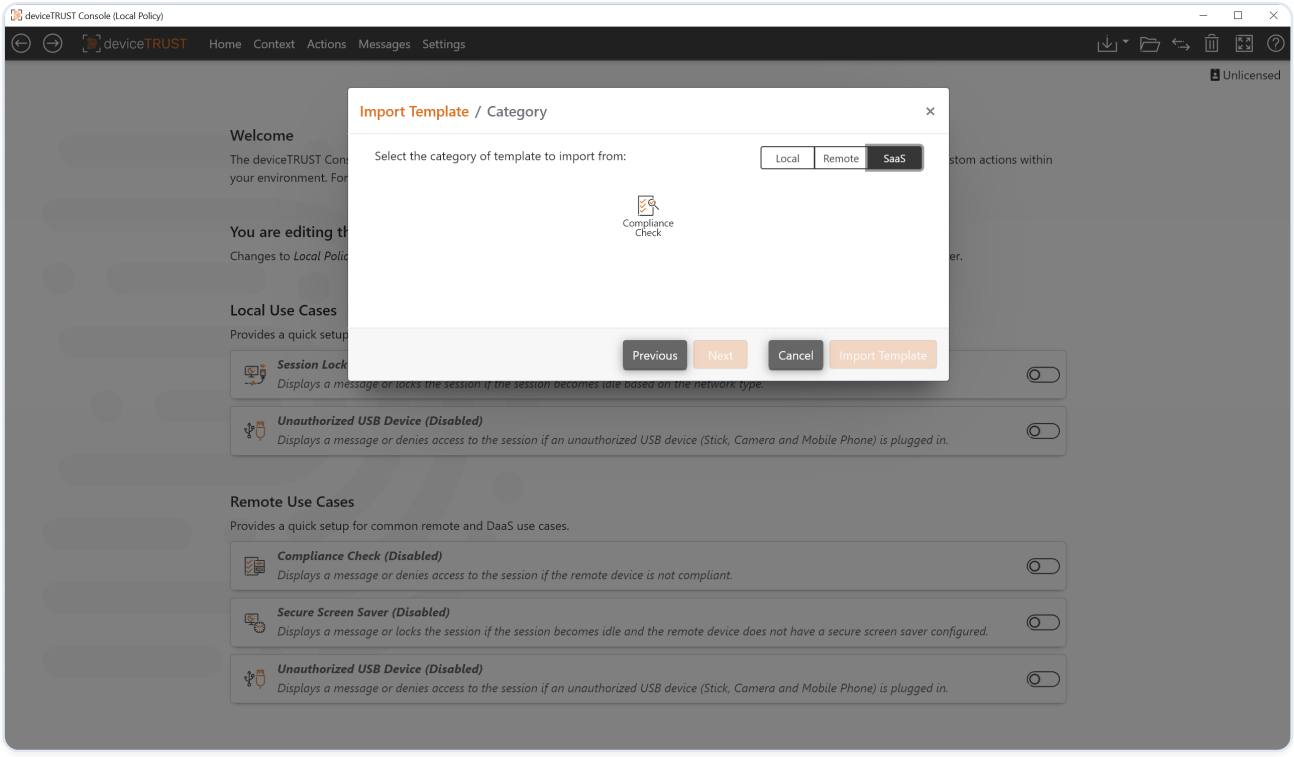


TABLE OF CONTENTS

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

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

Reference

TABLE OF CONTENTS

- Properties
- Agent
- Client Extension
- Console

Property Reference

Table of contents

- 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.

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

- iOS Properties - Provides properties unique to an Apple iOS endpoint.
- Location Properties - Describes the geographical location of the endpoint.
- 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.

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

- Smartcard Reader Properties - Describes the connected smart-card readers available to the user.
- User Properties - Identifies the logged in user.
- 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 Windows Update.

Agent Reference

TABLE OF CONTENTS

- Policy Loading - Policy Loading
- Product Events - 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{:target="_"blank}.

© 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
- Enabling Custom Scripts on Remote Devices
- Exclude specific users from the deviceTRUST policy

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

- GPO name is not updated in deviceTRUST policy when copying a GPO within group policy editor

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
- Virtual Channel Compatibility

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

- (windows/2503 CR/index)
- (macos/2503 CR/index)
- (elux/2503 CR/index)
- (ubuntu/2503 CR/index)
- Previous Release (23.1)

deviceTRUST Client Extension for macOS 2503 CR

The deviceTRUST Client Extension is available for macOS as part of the Citrix Workspace app 2503 or later.

Details on the installation of the deviceTRUST Client Extension for macOS can be found within our Installation guide.

Supported platforms

The supported platforms have been updated. Please refer to the OS Compatibility guide for more information.

Compatibility with previous releases

The deviceTRUST Client Extension v2503 CR is not compatible with the previous deviceTRUST Agent v23.1 due to a change of the virtual channel name. More details can be found in the Virtual Channel Compatibility Knowledge Base article.

Custom Properties and Custom Process Task

Custom Property Scripts and Custom Process Tasks of remote device are now disabled by default and can be enabled via an environment variable on Ubuntu. More details can be found in the Enabling Custom Scripts on Remote Devices Knowledge Base article.

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

deviceTRUST® Client Extension for eLux 2503 CR

The deviceTRUST Client Extension is available for eLux 7 as part of the Citrix Workspace app 2503 or later and is available to download on the myelux portal.

Details on the installation of the deviceTRUST Client Extension for eLux 7 can be found within our Installation guide.

Supported platforms

For supported platforms, please refer to the OS Compatibility guide for more information.

Compatibility with previous releases

The deviceTRUST Client Extension v2503 CR is not compatible with the previous deviceTRUST Agent v23.1 due to a change of the virtual channel name. More details can be found in the Virtual Channel Compatibility Knowledge Base article.

Custom Properties and Custom Process Task

Custom Property Scripts and Custom Process Tasks of remote device are now disabled by default and can be enabled via an environment variable on eLux 7. More details can be found in the Enabling Custom Scripts on Remote Devices Knowledge Base article.

deviceTRUST Client Extension for Ubuntu 2503 CR

The deviceTRUST Client Extension is available for Ubuntu as part of the Citrix Workspace app 2503 or later.

Details on the installation of the deviceTRUST Client Extension for Ubuntu can be found within our Installation guide.

Supported platforms

The supported platforms have been updated. Please refer to the OS Compatibility guide for more information.

Compatibility with previous releases

The deviceTRUST Client Extension v2503 CR is not compatible with the previous deviceTRUST Agent v23.1 due to a change of the virtual channel name. More details can be found in the Virtual Channel Compatibility Knowledge Base article.

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

Custom Properties and Custom Process Task

Custom Property Scripts and Custom Process Tasks of remote device are now disabled by default and can be enabled via an environment variable on Ubuntu. More details can be found in the Enabling Custom Scripts on Remote Devices Knowledge Base article.

deviceTRUST 2503 CR

deviceTRUST 2503 CR is now built into the Citrix Virtual Apps and Desktops™ and the Citrix Workspace™ app.

- Supported platforms
- Licensing
- Citrix Virtual Channel Allow List
- Custom Properties and Custom Process Task
- Compatibility with previous clients
- Compatibility

Supported platforms

The supported platforms have been updated. Please refer to the Platform Compatibility for more information.

Licensing

A deviceTRUST license is no longer required when using the Citrix ICA/HDX protocol and a deviceTRUST Policy is applied. A license is still required when using an RDP protocol.

Citrix Virtual Channel Allow List

The Citrix virtual channel allow list must be updated to support deviceTRUST Agent 2503, due to a rename of the virtual channel to `CTXDT`, and a new installation path. More details can be found in the Configuring Citrix Virtual Channel Security Knowledge Base article.

Custom Properties and Custom Process Task

Custom Property Scripts and Custom Process Tasks of the remote device are now disabled by default and can be enabled via a Windows Registry entry, or an environment variable on non-Windows platforms. More details can be found in the Enabling Custom Scripts on Remote Devices Knowledge Base article.

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

Compatibility with previous clients

The deviceTRUST Client Extension v2503 CR is not compatible with the previous deviceTRUST Agent v23.1 due to a change of the virtual channel name. More details can be found in the Virtual Channel Compatibility Knowledge Base article.

Compatibility

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

If upgrading from a previous release, be sure to check out the deviceTRUST 23.1.410 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 2503 CR is deployed before applying policy that has been written by the deviceTRUST Console 2503 CR.

Releases

TABLE OF CONTENTS

- Next Release (2503 CR)
- 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)

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

index

- Client Extension installation on eLux® 7
- Client Extension installation on iOS and iPadOS devices
- Installing the deviceTRUST Client Extension for macOS
- Installing the deviceTRUST® Client Extension for Ubuntu
- Installing the deviceTRUST® Client Extension for Microsoft Windows
- Azure Enterprise Application for AAD Conditional Access integration
- Check that your contexts are correctly defined
- Multi-Hop with deviceTRUST
- Process monitoring
- deviceTRUST® + Apple Silicon support
- deviceTRUST® + CVE-2021-44228 “Log4Shell”
- Check that your contextual security policy has been saved and deployed
- Check that the user is managed by deviceTRUST
- 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
- Configuring Citrix Virtual Channel Security
- Check that the deviceTRUST Client Extension is installed on the remote device
- Configuring Citrix Virtual Channel Security
- Virtual Channel Compatibility
- deviceTRUST debug log locations
- Check that the deviceTRUST Agent service is running
- Check that you are using the latest deviceTRUST version

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

- 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
- 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

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

- 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
- 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

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

- Domain Properties
- eLux® Properties
- Hardware Properties
- IGEL Properties
- Input Properties
- iOS Properties
- Location Properties
- Logical Disk Properties
- macOS Properties
- macOS Firewall Properties
- macOS Update
- Mapped Drive Properties
- MDM Properties
- Multihop Properties
- Name Properties
- Network Properties
- NoTouch Properties
- 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

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

- WHOIS Properties
- Windows Properties
- Windows Defender Properties
- Windows Firewall Properties
- Windows Registry Properties
- Windows Update Properties
- Access Mode Template
- Conditional Application Access Template
- Country Template
- Country Provider Template
- Device Location IP Address Template
- Device Location NetBIOS Name Template
- Device Location Wi-Fi Access Point Template
- Building Blocks Templates
- Operating System Update Template
- Override Template
- Policy Mode from AD Group Template
- Policy Mode from Date Template
- Process Monitoring Template
- Proximity Template
- Session Idle Template
- Unauthorized USB Device Template
- VPN Connected Template
- Wi-Fi Security Mode Template
- Working Time Template
- Country Template
- Compliant Application Access Templates
- Proximity Template
- Security State Template
- Wi-Fi Security Mode Template

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

- Working Time Template
- Dynamic Policy Templates
- Session Lock based on Network Type Template
- Session Lock based on VPN Connection Template
- Session Lock based on Wi-Fi Security Mode Template
- Conditional Application Access for Country Template
- Conditional Application Access for Proximity Template
- Geolocation Templates
- Location Aware Printing Templates
- IP Address Template
- NetBIOS Name Template
- Wi-Fi Access Point Template
- Application Log Template
- ELK Stack Template
- Email Template
- Status Report Templates
- Log File Template
- Splunk Template
- Conditional Application Access Template
- Time-based Access Templates
- Unauthorized USB Drives Templates
- Access Mode Template
- Citrix Workspace App Template
- Computer Certificate Template
- Conditional Application Access Template
- Corporate Device Template
- Country Template
- Country Provider Template
- Device Location IP Address Template
- Device Location NetBIOS Name Template

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

- Device Type Contractor Template
- Device Type Corporate Template
- deviceTRUST Client Extension Availability Template
- Building Blocks Templates
- Operating System Template
- Operating System Update Template
- Override Template
- Policy Mode from AD Group Template
- Policy Mode from Date Template
- Process Monitoring Template
- Proximity Template
- Remote Controlled Template
- Security State Template
- Session Idle Template
- Threat Detection Template
- Unauthorized USB Device Template
- User Privileges Template
- Virtualized Template
- VPN Connected Template
- Wi-Fi Security Mode Template
- Working Time Template
- Conditional Access Template
- Conditional Application Access Template
- BYOD (Bring Your Own Device) Templates
- Compliance Check Template
- Computer Certificate Template
- Corporate Device Template
- Country Template
- deviceTRUST Client Extension Availability Template
- Compliance Check

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

- Operating System Template
- Remote Controlled Template
- Security State Template
- Threat Detection Template
- User Privileges Template
- Virtualized Template
- Wi-Fi Security Mode Template
- Access Mode Template
- Corporate Device Template
- Country Template
- Compliant Application Access Templates
- Proximity Template
- Security State Template
- Wi-Fi Security Mode Template
- Working Time Template
- Conditional Access Template
- Compliant Backend Access Templates
- Amazon DCV Clipboard Security State Template
- Citrix Policy Access Mode Template
- Citrix Policy Corporate Device Template
- Citrix Policy Wi-Fi Security Mode Template
- Dynamic Policy Templates
- Secure Screen Saver Template
- Conditional Access Template
- Conditional Application Access Template
- External Partners Templates
- Conditional Access for Country Template
- Conditional Application Access for Country Template
- Conditional Application Access for Proximity Template
- Geolocation Templates

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

- License Compliance Templates
- Microsoft Visio Template
- Nuance PDF Template
- Location Aware Printing Templates
- IP Address Template
- NetBIOS Name Template
- Wi-Fi Access Point Template
- Process Monitoring Templates
- Microsoft Teams Template
- Snipping Tool Template
- Access Mode Template
- Adobe Acrobat DC Template
- Corporate Device Template
- Country Template
- Silo Optimization Templates
- 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
- Status Report Templates
- Log File Template
- Splunk Template
- Conditional Access Template
- Conditional Application Access Template
- Time-based Access Templates

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

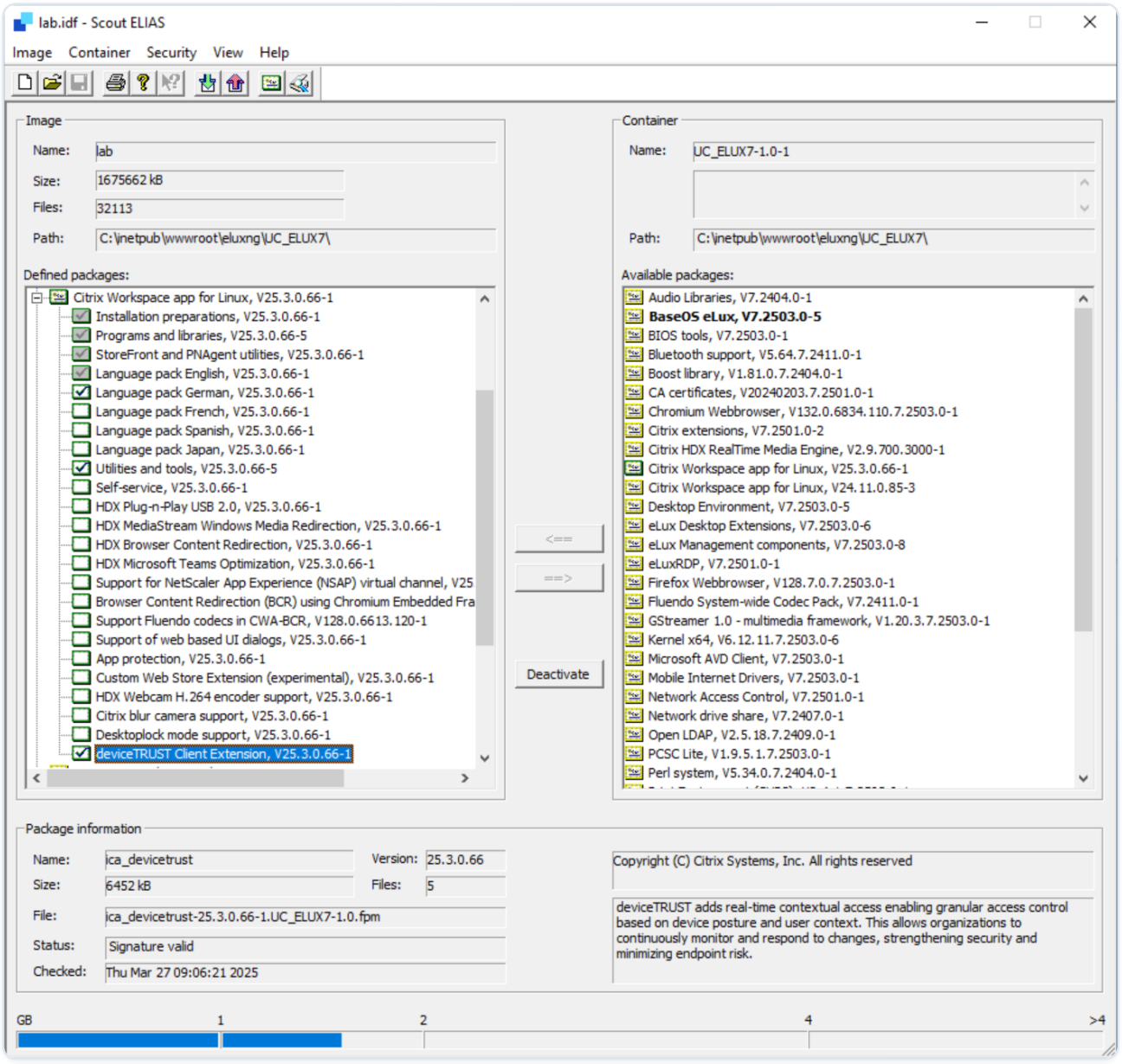
- Unauthorized USB Device Templates
- Unauthorized USB Device Template
- Conditional Access Template
- Work From Home Templates
- Country Template
- Compliance Check
- Operating System Update State Template
- Remote Controlled Template
- Security State Template
- Threat Detection Template
- User Privileges Template
- Wi-Fi Security Mode Template

Client Extension installation on eLux® 7

The deviceTRUST Client Extension is built into the Citrix Workspace™ app 2503 or later.

To install, activate the package `Citrix Workspace app for Linux` -> `deviceTRUST Client Extension` within Scout ELIAS as shown below. Additionally, the `PCSC Lite` -> `PCSC Lite SmartCard Library` package must also be activated. Save the image and update your devices.

© 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.

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

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.

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.

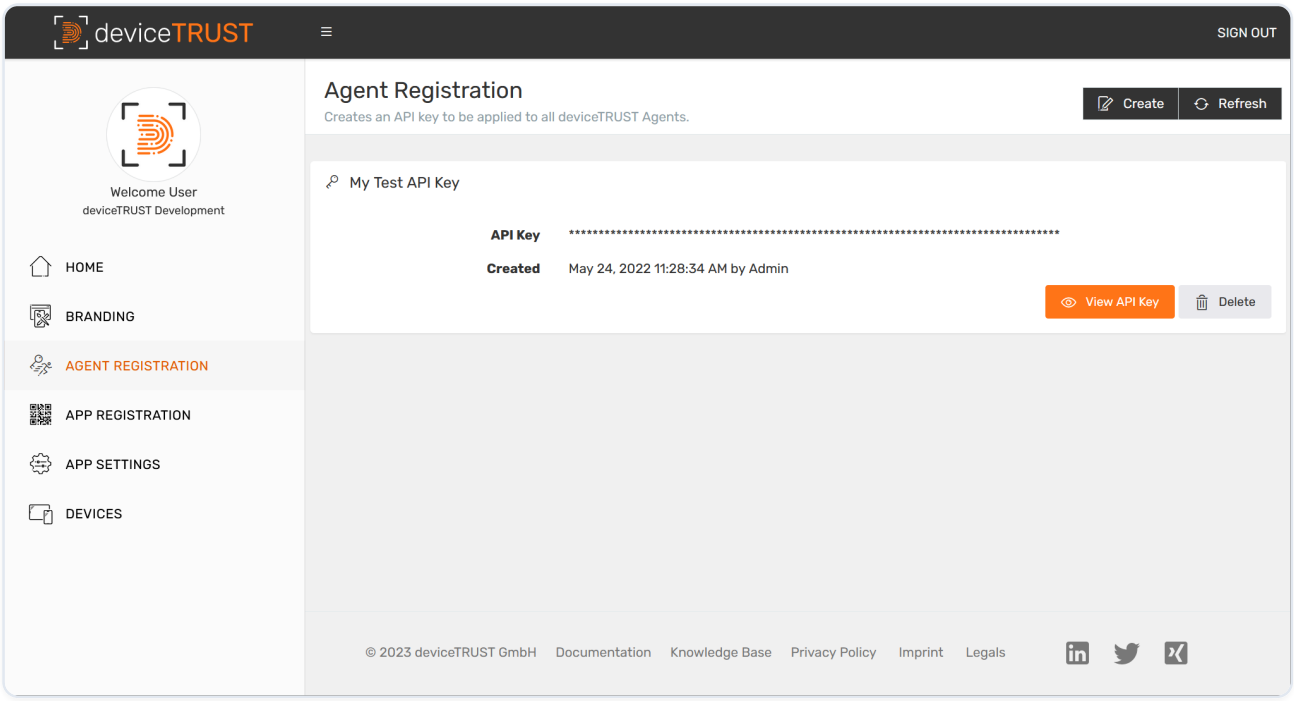
When signed into the Azure portal:

- 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.

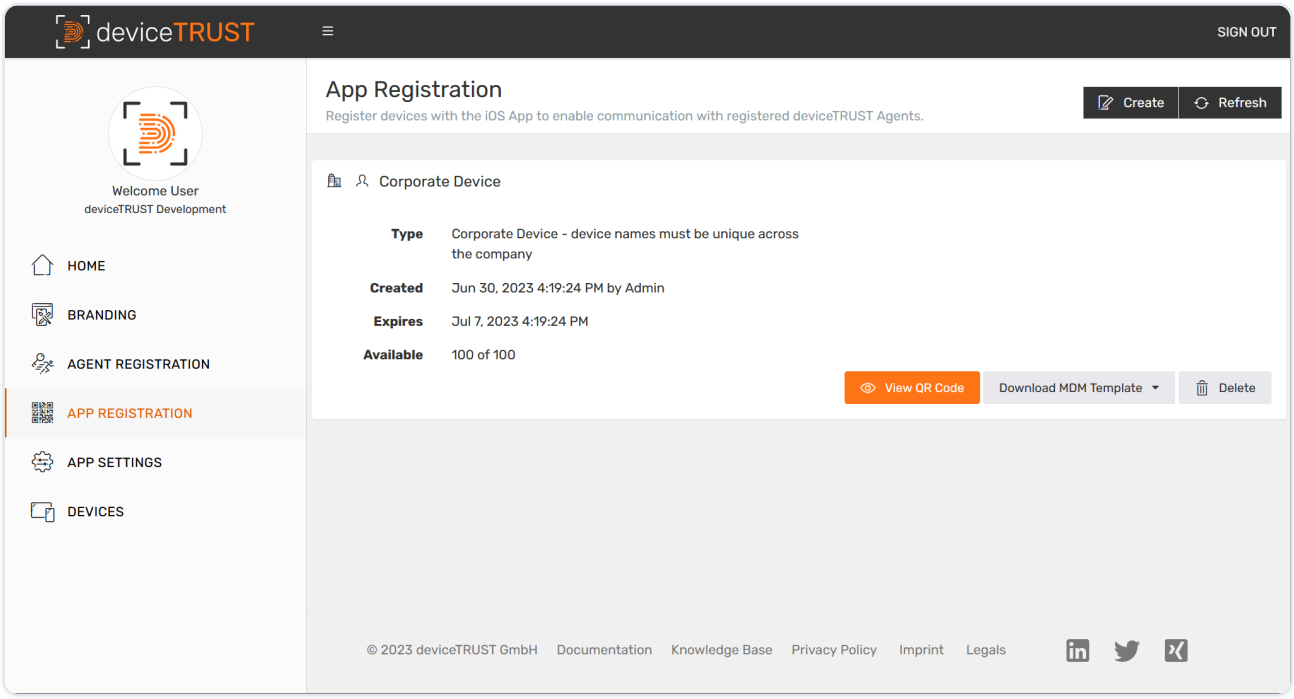
Generating an App Registration code to register iOS and iPadOS devices

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.

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

- *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.



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.

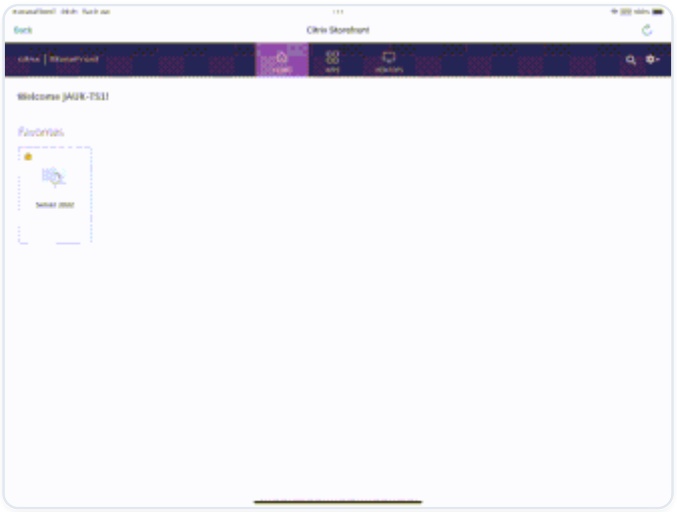
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Installing the deviceTRUST Client Extension for macOS

The deviceTRUST Client Extension for macOS is now installed by default as part of Citrix Workspace app when using release 2503 or later. This can be downloaded from Citrix Downloads.

Installing the deviceTRUST® Client Extension for Ubuntu

The deviceTRUST Client Extension for Ubuntu is now installed by default as part of Citrix Workspace app when using release 2503 or later. This can be downloaded from Citrix Downloads.

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

Installing the deviceTRUST® Client Extension for Microsoft Windows

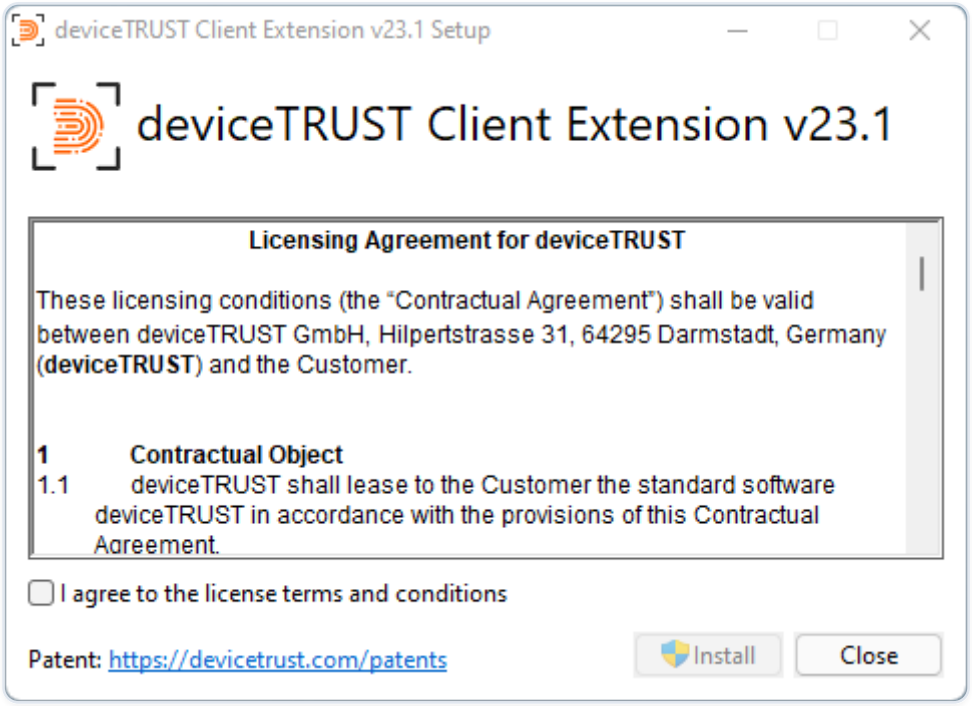
- Option 1: Install the latest Citrix Workspace™ app
- Option 2: Install the deviceTRUST Client Extension on Microsoft Windows
- Client Extension Installation Command Line Options
- Option 3: Unattended Installation
- Active Setup Components
- deviceTRUST Channel Registration 64-bit component
- deviceTRUST Channel Registration 32-bit component
- deviceTRUST Citrix Cleanup 32-bit component

Option 1: Install the latest Citrix Workspace app

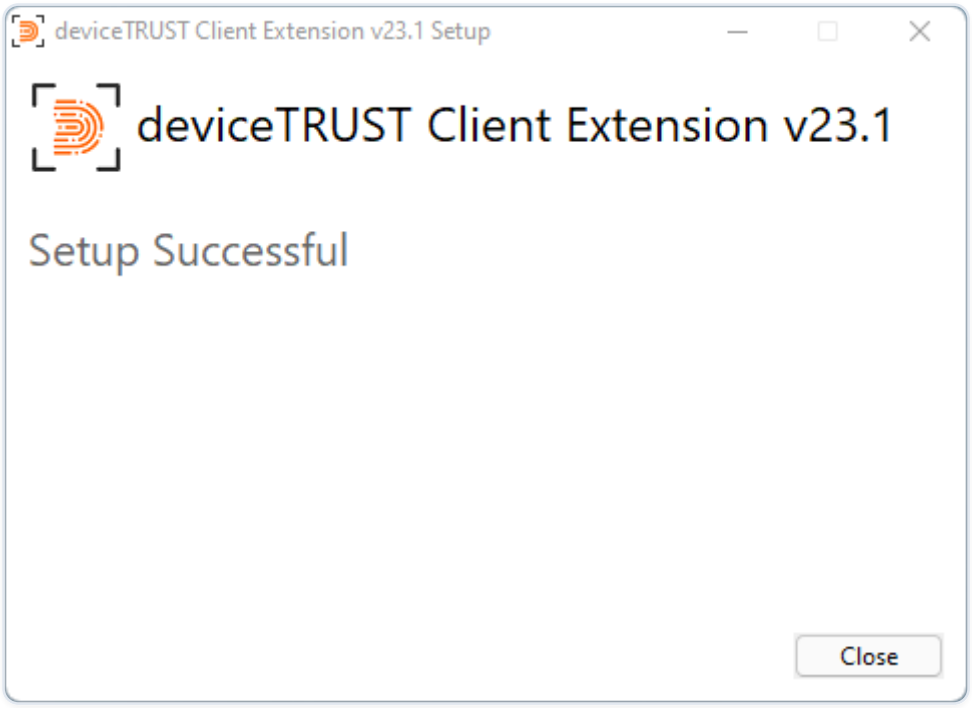
The deviceTRUST Client Extension for Microsoft Windows is now installed by default as part of Citrix Workspace app when using release 2503 or later. This can be downloaded from Citrix Downloads.

Option 2: Install the deviceTRUST Client Extension on Microsoft Windows

The deviceTRUST Client Extension for Microsoft Windows devices can be installed by following the steps of the installation.



© 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.
- The deviceTRUST Client Extension installer installs both the 32-bit and 64-bit deviceTRUST Client Extension components depending on the Windows operating system platform.

Option 3: 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 `HKLM\Software\Microsoft\Active Setup\Installed Components\{8a4445d6-867e-4e60-8cc5-05bc2e3a2512}` on a 32-bit OS)

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

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.

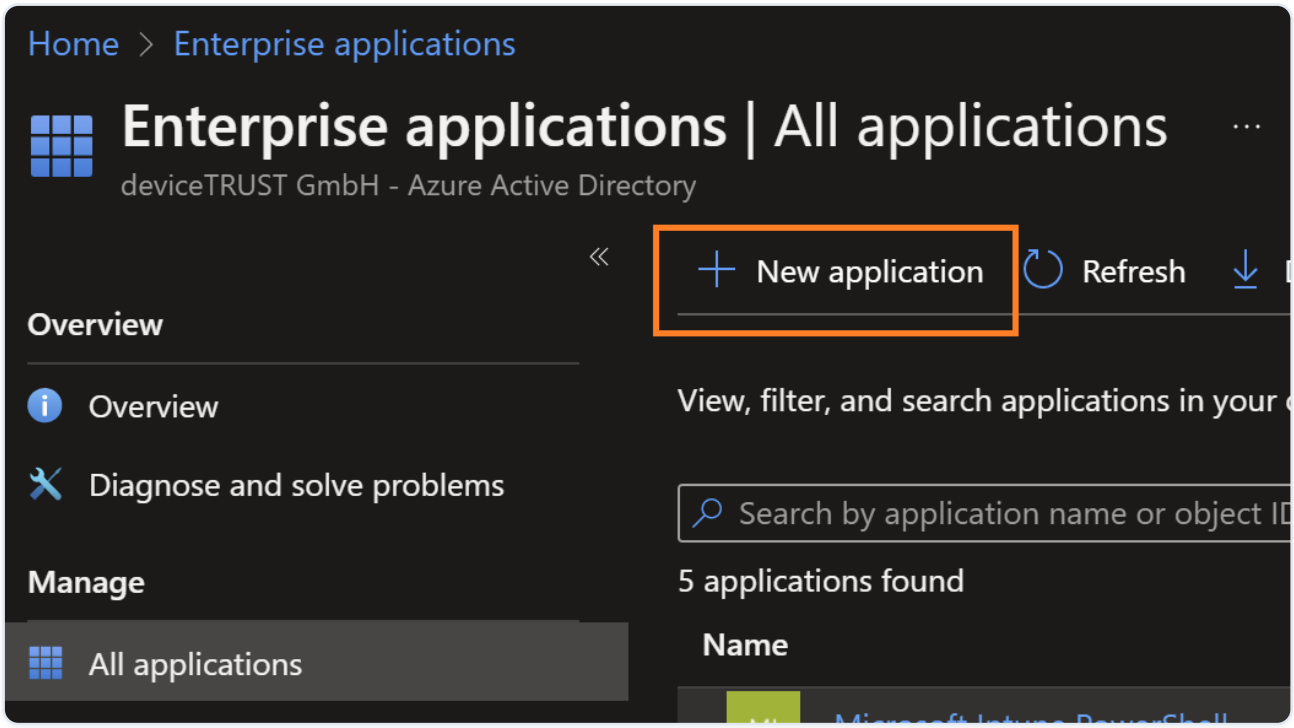
Azure Enterprise Application for AAD Conditional Access integration

This article describes how to set up and configure an Enterprise Application in Microsoft Azure to be used with the deviceTRUST Azure Conditional Access Integration.

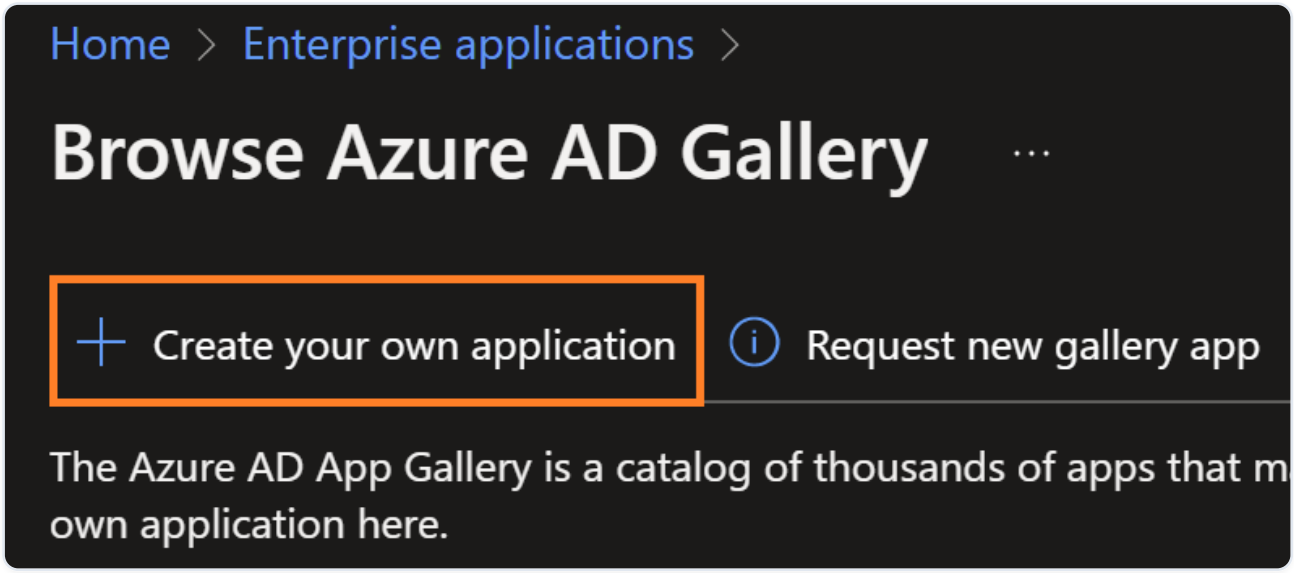
Integrating deviceTRUST with Azure Conditional Access requires the dT Agent being able to send data to the Azure control plane. Therefor, an Enterprise Application is utilized.

The first step is to log on to you Azure subscription with an appropriate account and head over to "Enterprise Applications". There you click "New application"

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

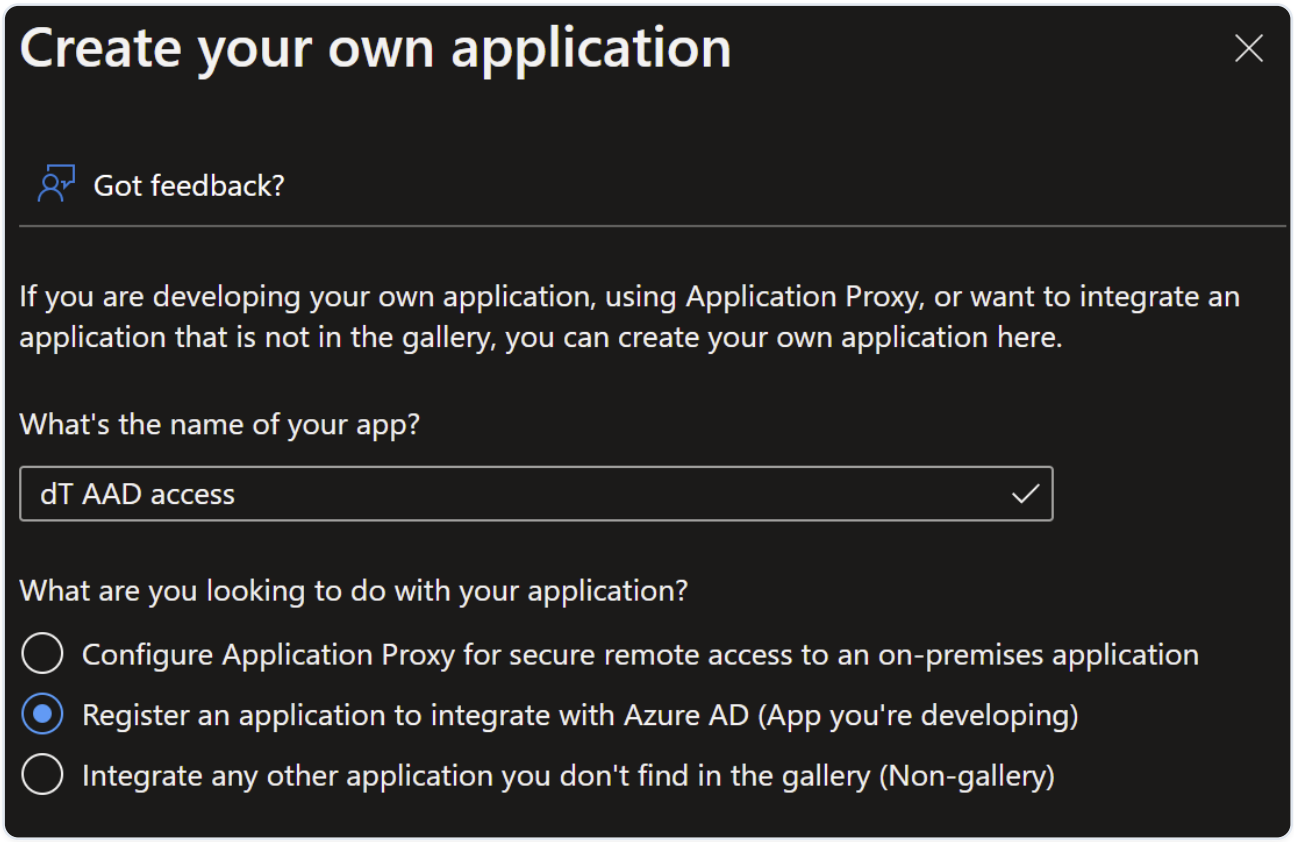


Choose "Create your own application"

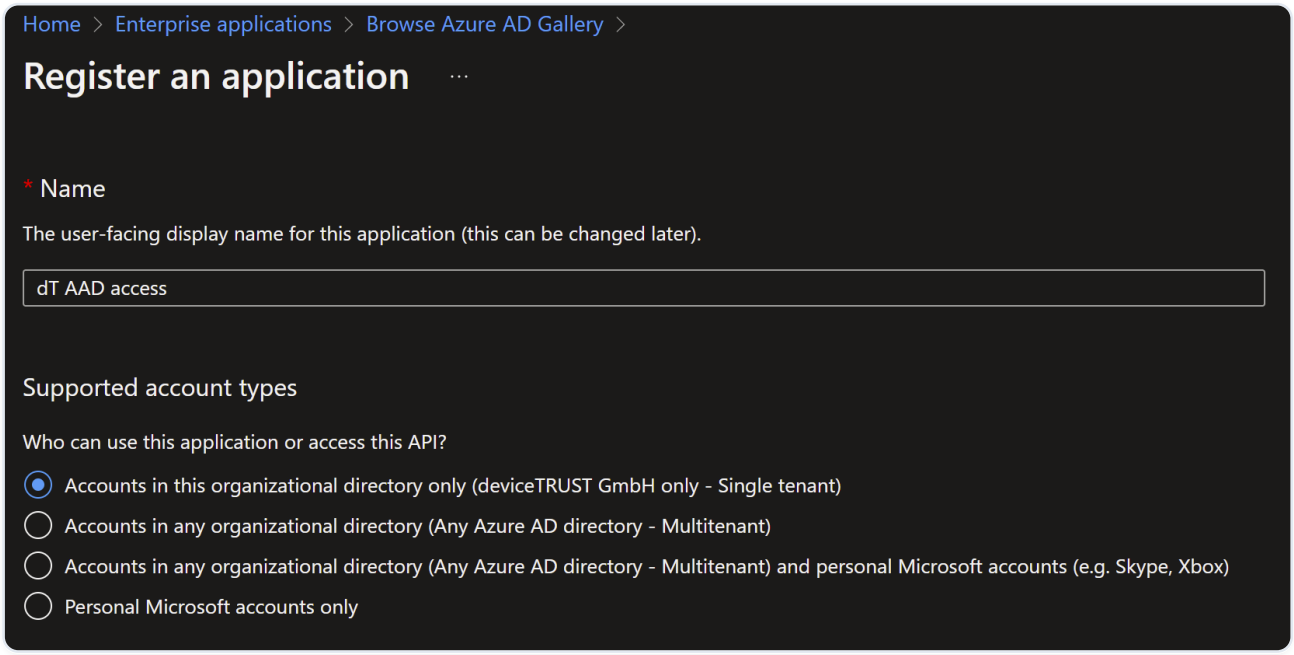


Give the application an name of your choice and select "Register an application to integrate with Azure AD (App you're deploying)"

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

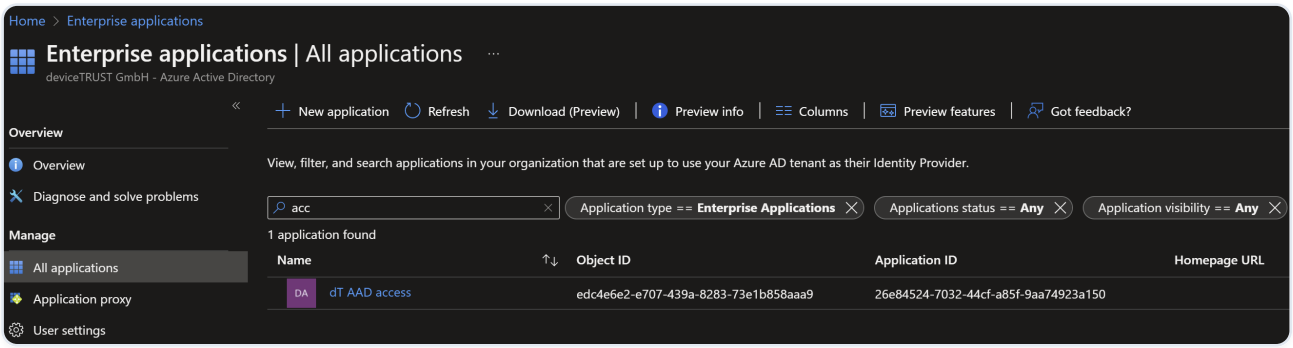


Stick to the name and select "Accounts in this organizational directory only"

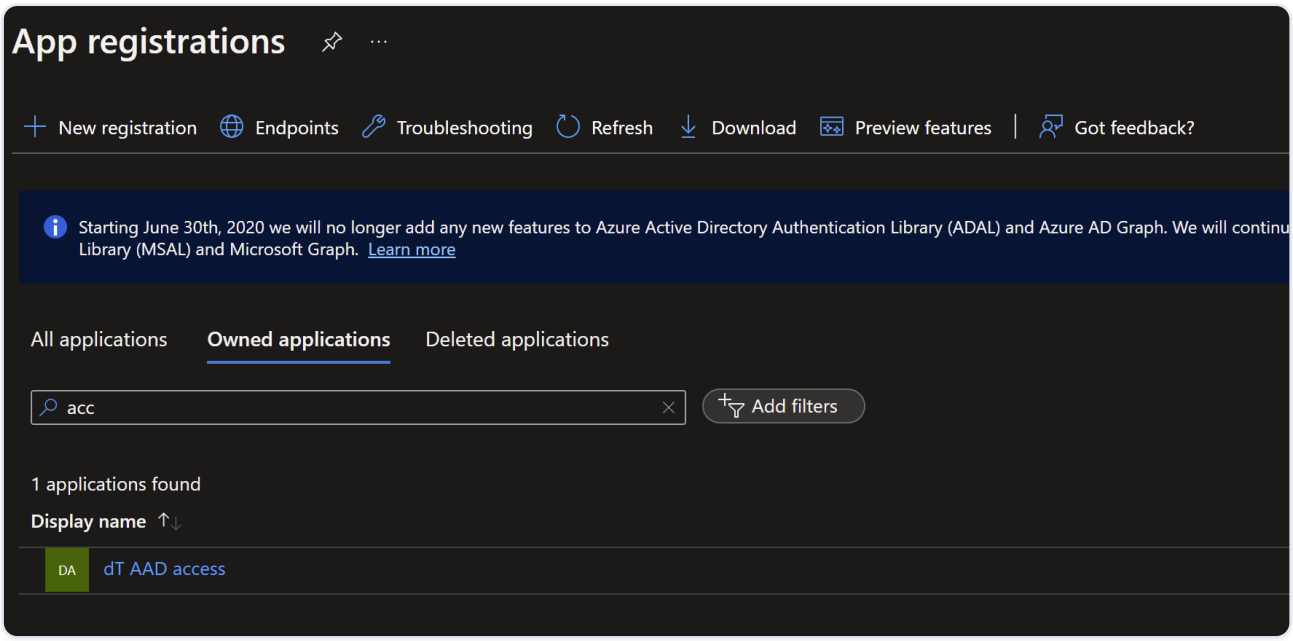


You'll find your application listed in the Enterprise Application menu

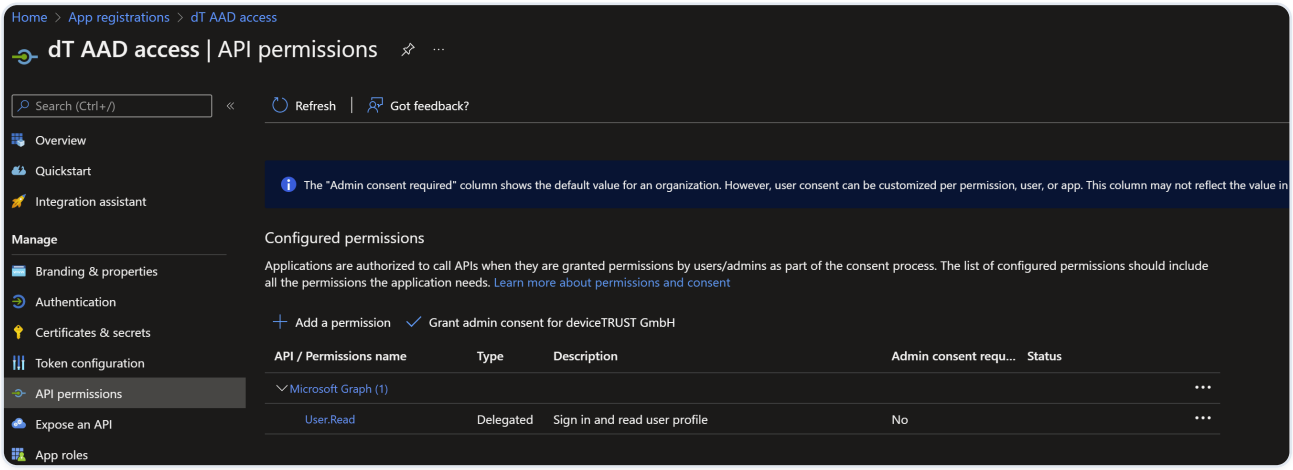
© 1997–2026 Citrix Systems, Inc. All rights reserved.



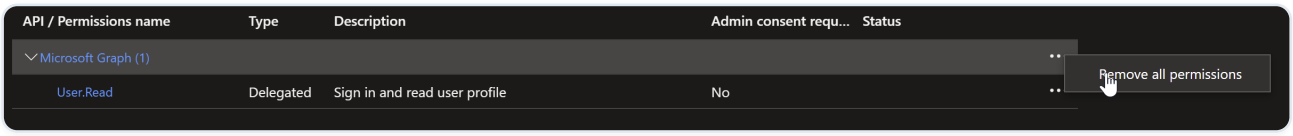
Now head over to "App registrations". There you'll find the created app:



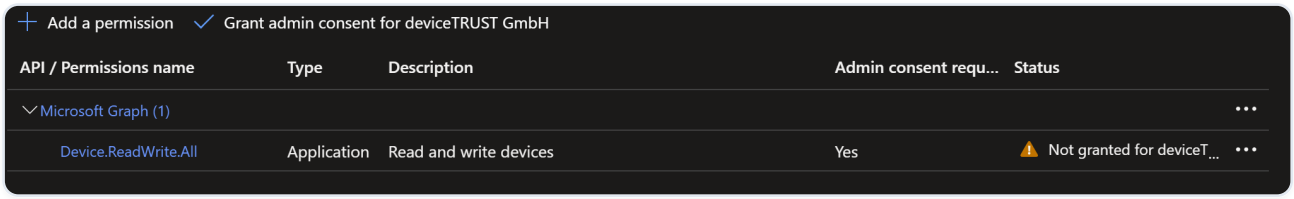
Edit the app and select "API permission" from the menu on the left.



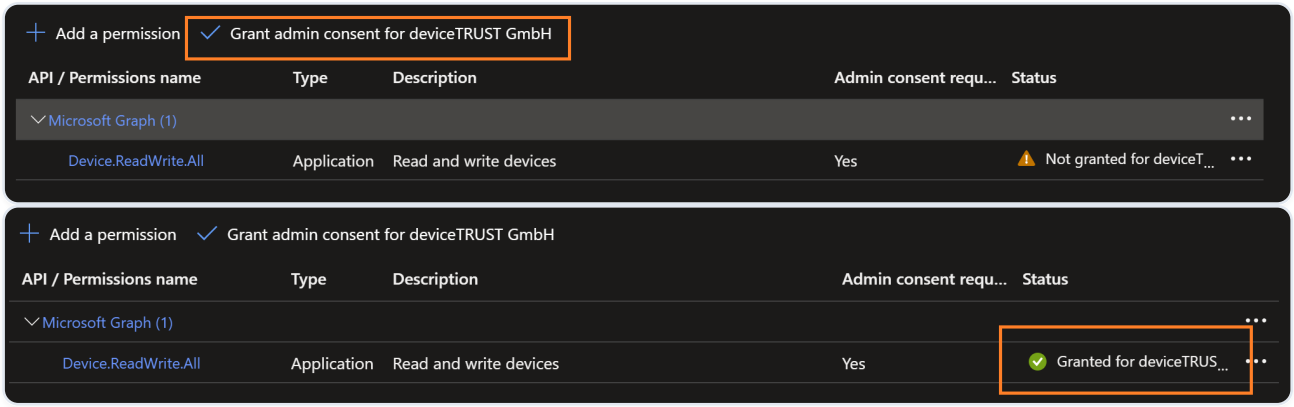
Eliminate "User.Read" here and add "Device.ReadWrite.All"



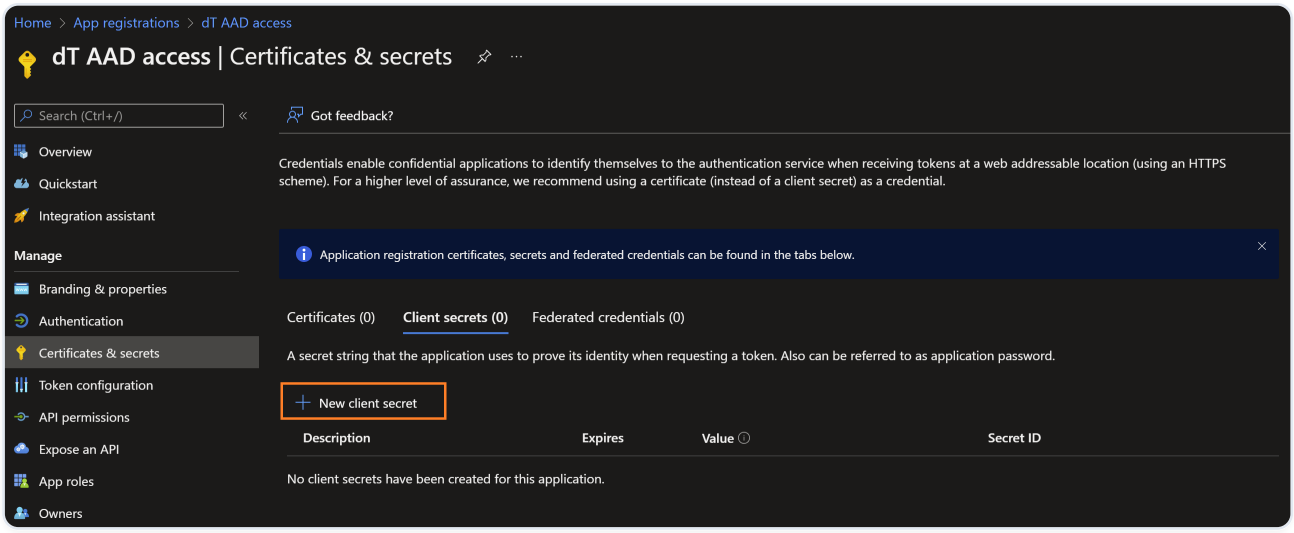
© 1997–2026 Citrix Systems, Inc. All rights reserved.



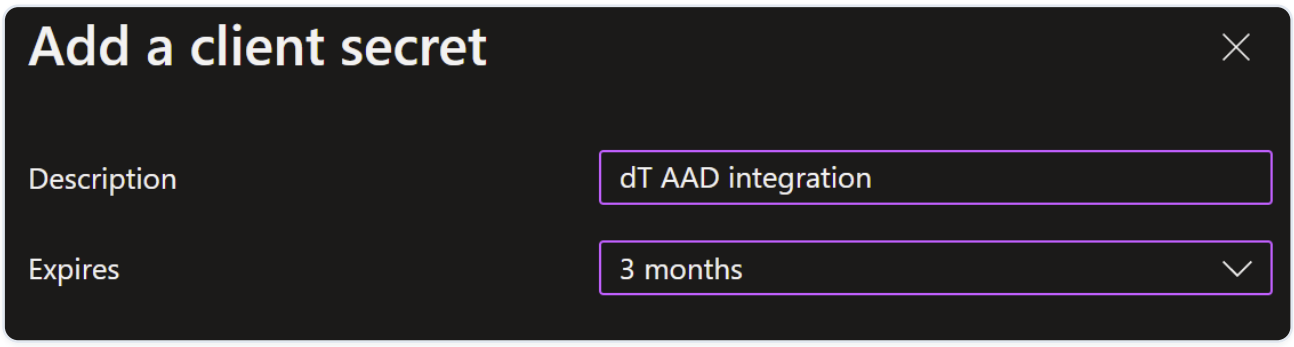
The newly added API permissions need to be consented.



Your app is now fully configured. Next, you'll have to create a secret which will let you use the apps remotely. In your app's menu, you'll find "Certificates and secrets". Click "New client secret" here.

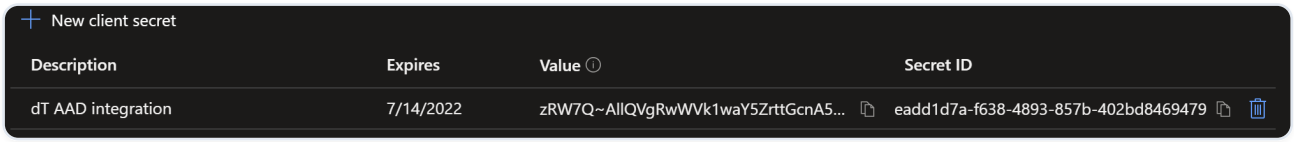


Set name and expiry to your likes. Be sure to remember the expiry date!



Copy the created "Value". It will only be displayed once!

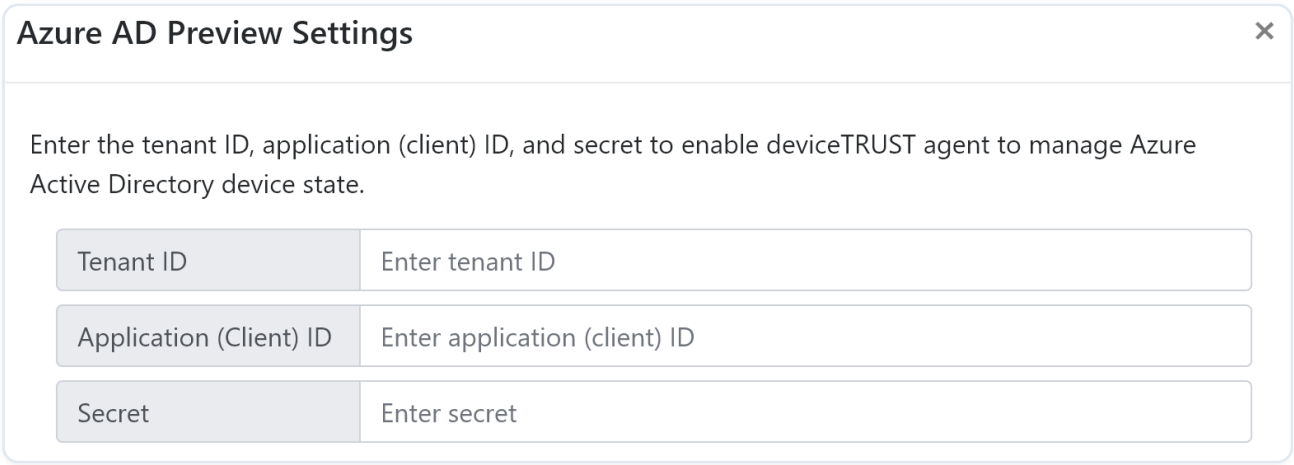
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You should no be able to provide the following information:

- Tenant ID: Your AAD tenant's ID
- Enterprise Application (client) ID: The ID of the newly created Enterprise Application
- Secret: the "Value" from the generated client secret

Finally, the details of the created Enterprise Application can be entered in the deviceTRUST Console (Settings\Azure AD Preview Settings):



Check that your contexts are correctly defined

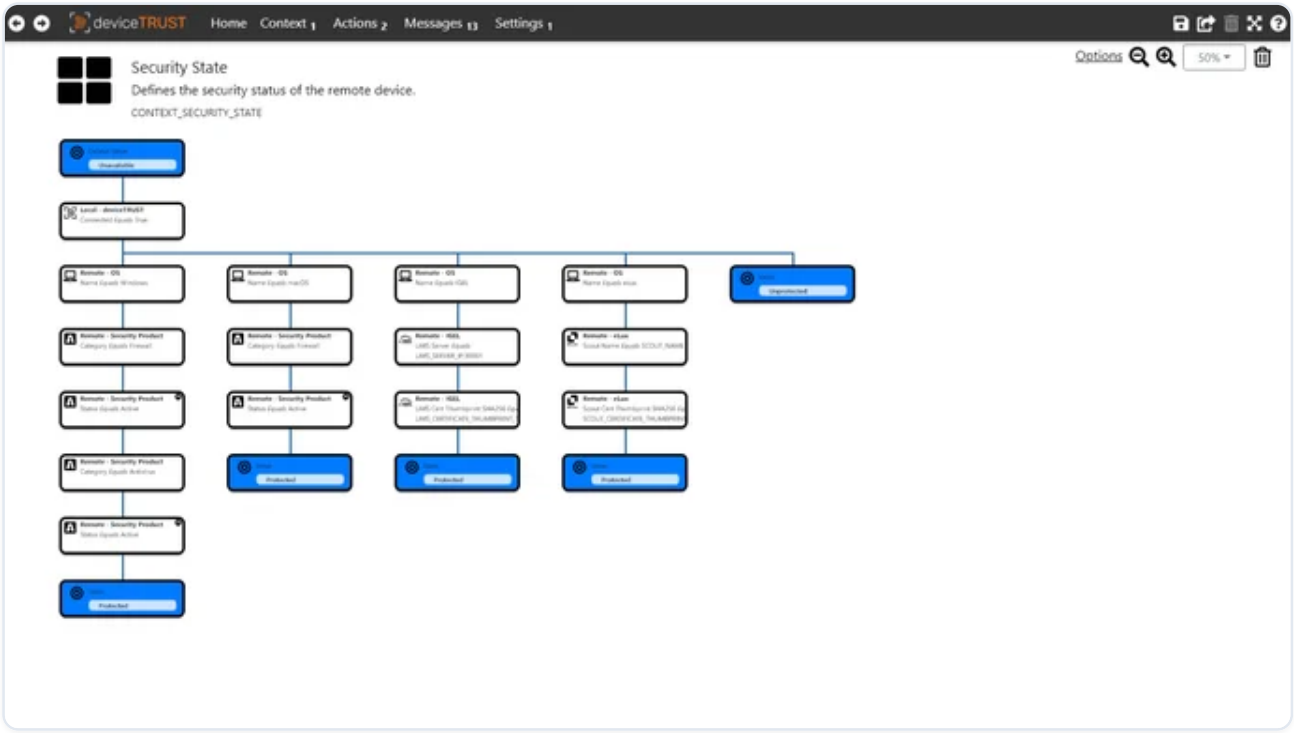
The contexts and their logical status must be correctly defined. Inaccuracies in the logic can have an undesirable impact on the user.

To analyze what exactly led to the undesired action, it is necessary to check the status of the respective context for its correctness.

In the following example, the context SECURITY STATE was defined, which indicates the security state of the remote device the user uses to access the virtual session. Based on the logical configuration of the context SECURITY STATE, the values UNAVAILABLE, PROTECTED, and UNPROTECTED can be reported back.

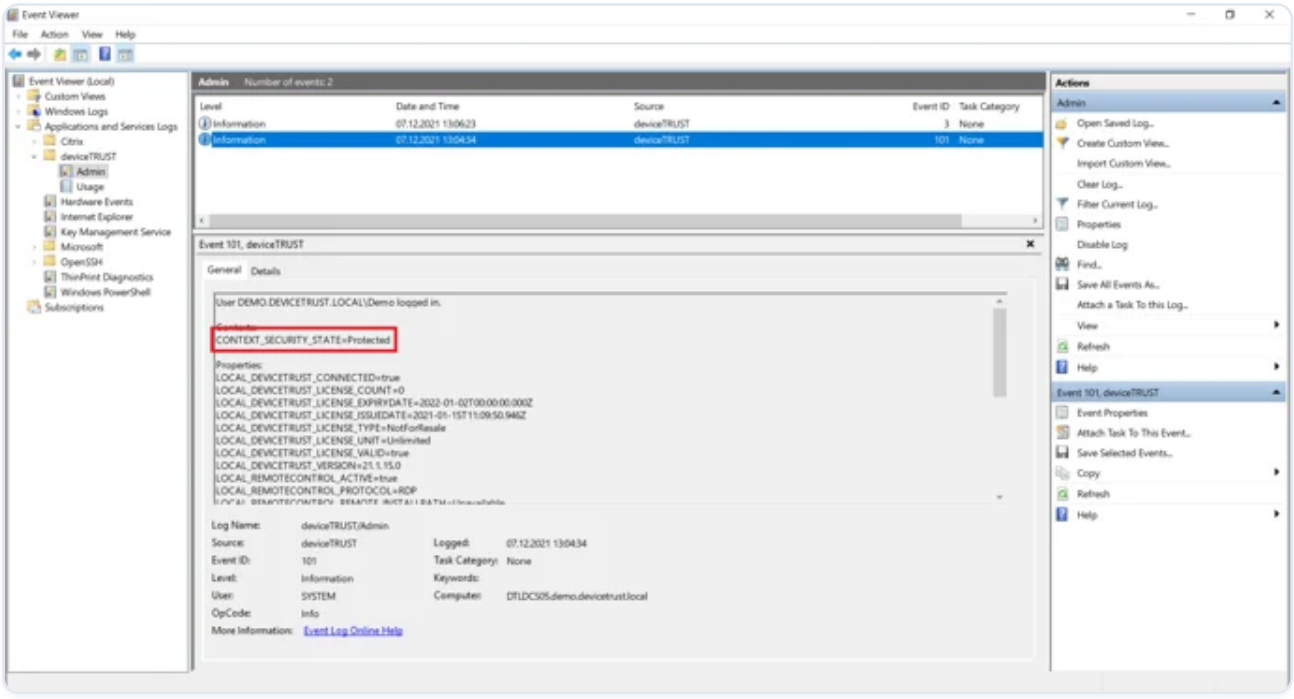
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Security State Context



The context value evaluated for a user session can be seen by opening the Windows Event Log on the host system and navigating to APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN. Event ID 101 is raised during logon and details the properties and context of the users' virtual session.

Virtual session properties and contexts

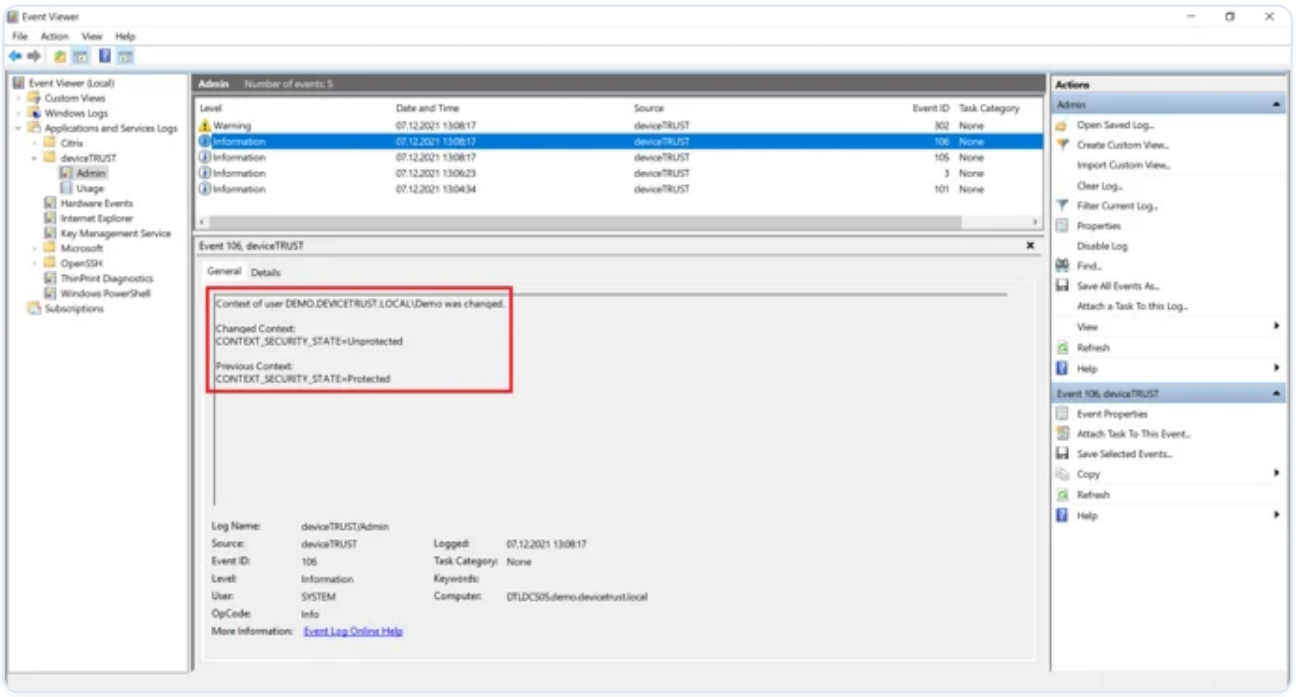


In the above example, we can force a context change on the remote device by, for example, disabling Microsoft Defender Firewall and looking at how the corresponding context updates. To

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

check this, open the Windows Event Log on the host system, navigate to APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN, and check for Event ID 106, which is raised whenever a context changes value within the users' session.

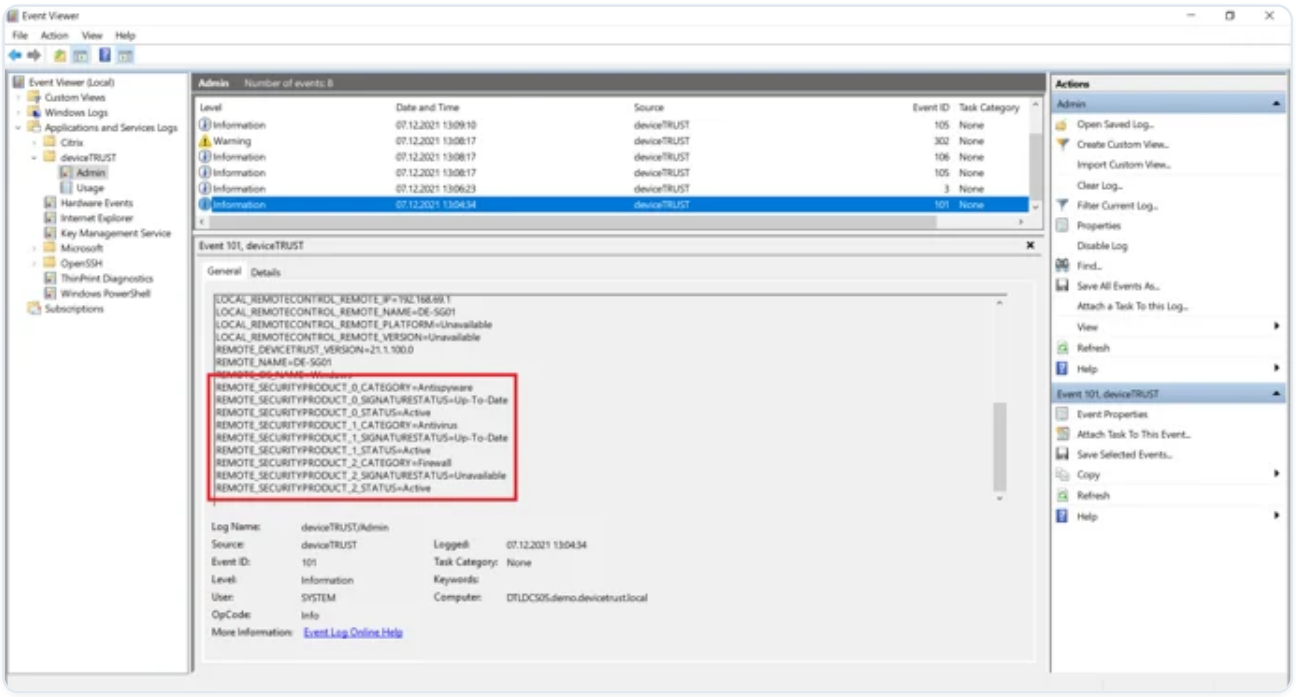
Context change audit event



If the context takes the correct value, the logic for the context definition is correct. If not, the individual properties used within the context definition should also be checked. Check within your context definition which properties are used for the logic and check the accuracy of the logic based on the submitted properties and adjust them if necessary. To do this, open the Windows Event Log on the host system, navigate to APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN, and check for Event ID 101, which details the properties and context of the users' virtual session.

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

Session properties and contexts



Multi-Hop with deviceTRUST

deviceTRUST supports different Multi-Hop scenarios. Read how they work and how they can be implemented.

Imagine you have clients, be they from inside your organization or outside, which access a server or workstation inside your network. To reach this target, they must pass through one or multiple hops, for example in a multiple DMZ structure. You could now either want information from the initial client or even from any hop in between to be available in the target or another hop.

There are three different approaches regarding such scenarios. These are explained here.

All three approaches can be used as mixed scenarios, of course.

Managed Hops

The "Managed Hops" scenario brings information from a client machine to a target machine, passing over one or multiple hops. On the target, Context will be evaluated and actions will be executed.

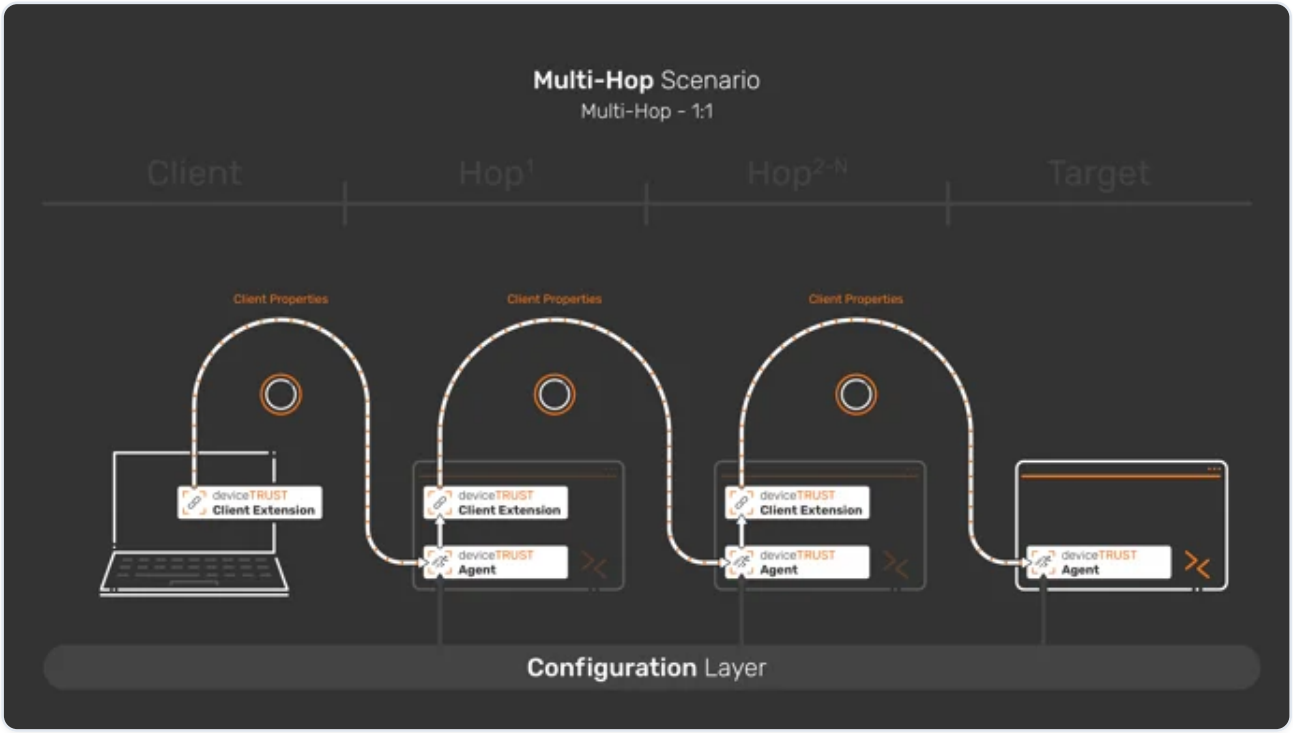
In this scenario, all hops as well as the target require a licensed deviceTRUST Agent to be installed and configured.

The following configuration elements are required:

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

Machine	Software	Configuration
Client	deviceTRUST Client Extension	None
Hop1	deviceTRUST Client Extension deviceTRUST Agent	Evaluate Properties
Hop2 - HopN	deviceTRUST Client Extension deviceTRUST Agent	Forward Properties
Target	deviceTRUST Agent	Build Context Run Actions

This is how the implementation looks from an architectural view.



Unmanaged Hops

The "Unmanaged Hops" scenario brings information from a client machine directly to a target machine, passing over one or multiple hops. On the target, Context will be evaluated and actions will be executed.

In this scenario, only the target requires a licensed deviceTRUST Agent to be installed and configured. The hops use a special function of the deviceTRUST Client Extension (available from Version 21.1.314) to forward the properties.

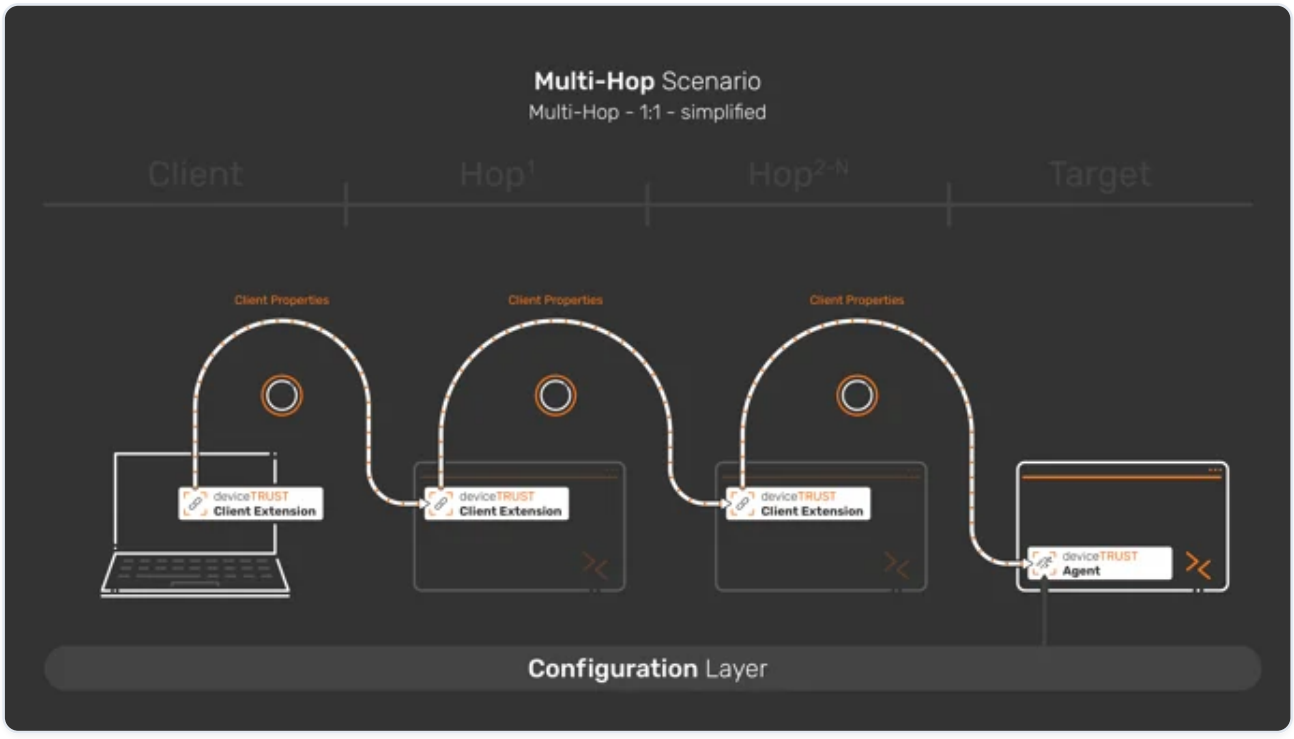
© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the deviceTRUST Client Extension discovers an upstream connection (e.g. Client to Hop1) and does not recognize a deviceTRUST Agent, but a deviceTRUST Client Extension on Hop1, it will attempt to communicate further. This will happen on every hop until a deviceTRUST Agent is found. Then, a secure channel will be established between the deviceTRUST Agent and the deviceTRUST Client Extension on the user's device. The secure channel is then used to fetch properties from the user's device.

The following configuration elements are required:

Machine	Software	Configuration
Client	deviceTRUST Client Extension	None
Hop1 - HopN	deviceTRUST Client Extension	None
Target	deviceTRUST Agent	Evaluate Properties Build Context based on Properties Run Actions

This is how the implementation looks from an architectural view.



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

Managed Hops with Properties

This scenario collects additional properties from the intermediate hops. deviceTRUST can gather data from any hop in a multi-hop scenario and use the information on any subsequent hop and the target.

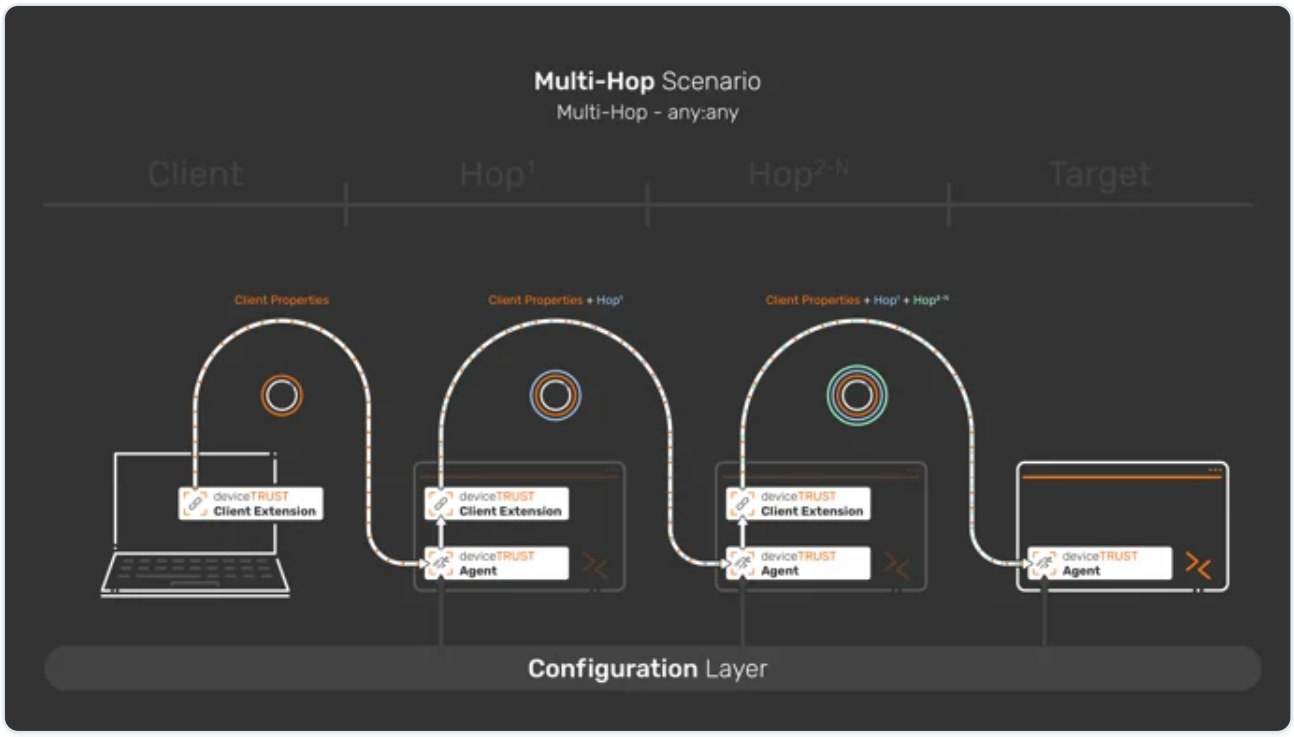
You might, for example, want to know that a user only hopped over machines that are joined to your domain and thus controlled and secured by your organization, when accessing the target session. Or you could make sure the user took a pre-defined path, hopping through your DMZ structure. These scenarios would require evaluating information not only on the user's device but also on the hops along the chain.

The following configuration elements are required:

Machine	Software	Configuration
Client	deviceTRUST Client Extension	None
Hop1 - HopN	deviceTRUST Client Extension deviceTRUST Agent	Evaluate Remote Properties Evaluate Local Properties Evaluate Multi-Hop Properties Build Context Run Actions Push Properties forward
Target	deviceTRUST Agent	Evaluate Remote Properties Evaluate Multi-Hop Properties Build Context Run Actions

This is how the implementation looks from an architectural view.

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



Process monitoring

Use deviceTRUST to check for running processes and react with appropriate controls. In this example, we check for sharing tools and block the access to a remote session, if such is running.

With release 21.1.200 and later , we added a method for checking for running processes on Windows devices. This can be either local devices (Fat Clients) or remote devices (e.g. in a Citrix or AVD environment).

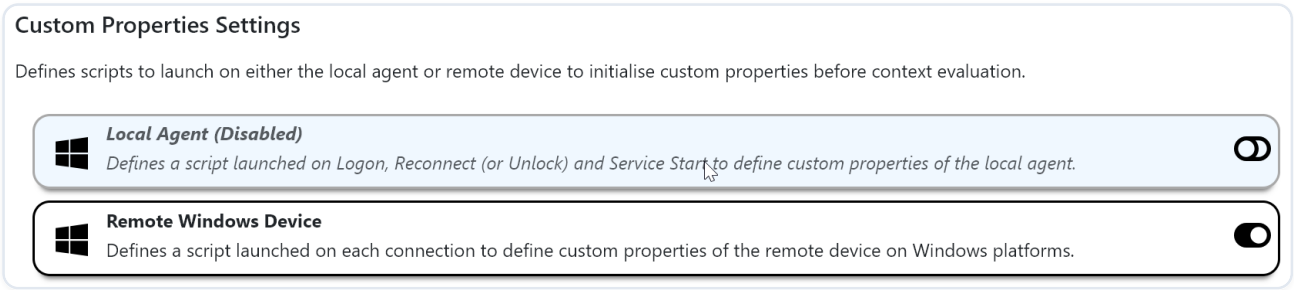
This article describes how you can use deviceTRUST to check for running processes on a remote device in a remoting scenario and apply controls inside the remoting session.

As processes, we will use "Snipping Tool" and "Zoom", the control will be to block the remote session, so no data can be shared.

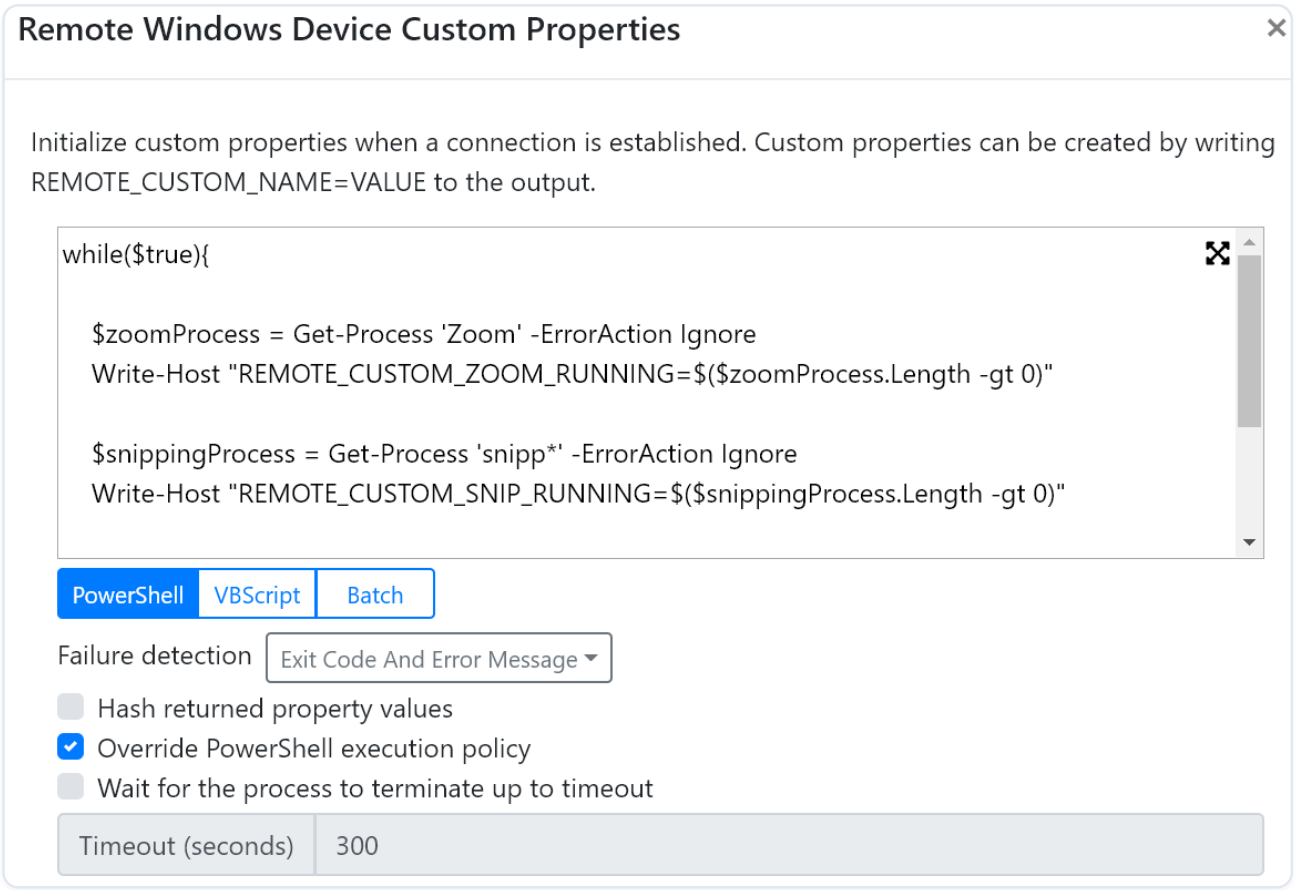
Script based process monitoring: The current release allows you to control all running processes based on script execution. This gives you the freedom to configure any process of your needs and also use script logic to configure more detailed evaluation.

deviceTRUST uses so called "custom properties" to evaluate individual information. These custom properties are the base for the process evaluation configuration. Head over to "Settings\Custom Properties" in the deviceTRUST console to create your config. We'll use "Remote Windows Device" here, as this example uses a remoting scenario.

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



You'll find a field that will contain your evaluation script here.



The following code can be used as example for your process checking configuration.

```
while($true){

    $zoomProcess = Get-Process 'Zoom' -ErrorAction Ignore

    Write-Host "REMOTE_CUSTOM_ZOOM_RUNNING=$($zoomProcess.Length -gt 0)"

    $snippingProcess = Get-Process 'snipp*' -ErrorAction Ignore

    Write-Host "REMOTE_CUSTOM_SNIP_RUNNING=$($snippingProcess.Length -gt
0)"

    Write-Host "CONTINUE"
```

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

```
    Sleep -Seconds 1

}
```

First: Create a non-exiting loop that is continuously runs on the device:

```
while($true){

}
```

Second: Add code to find your running process (Get-Process 'name') and create a custom deviceTRUST variable based on that information.

```
$zoomProcess = Get-Process 'Zoom' -ErrorAction Ignore

Write-Host "REMOTE_CUSTOM_ZOOM_RUNNING=$($zoomProcess.Length -gt 0)"



$snippingProcess = Get-Process 'snipp*' -ErrorAction Ignore

Write-Host "REMOTE_CUSTOM_SNIP_RUNNING=$($snippingProcess.Length -gt 0)"
```

Third: Adding "Write-Host CONTINUE" to the script will make deviceTRUST run the script in background.

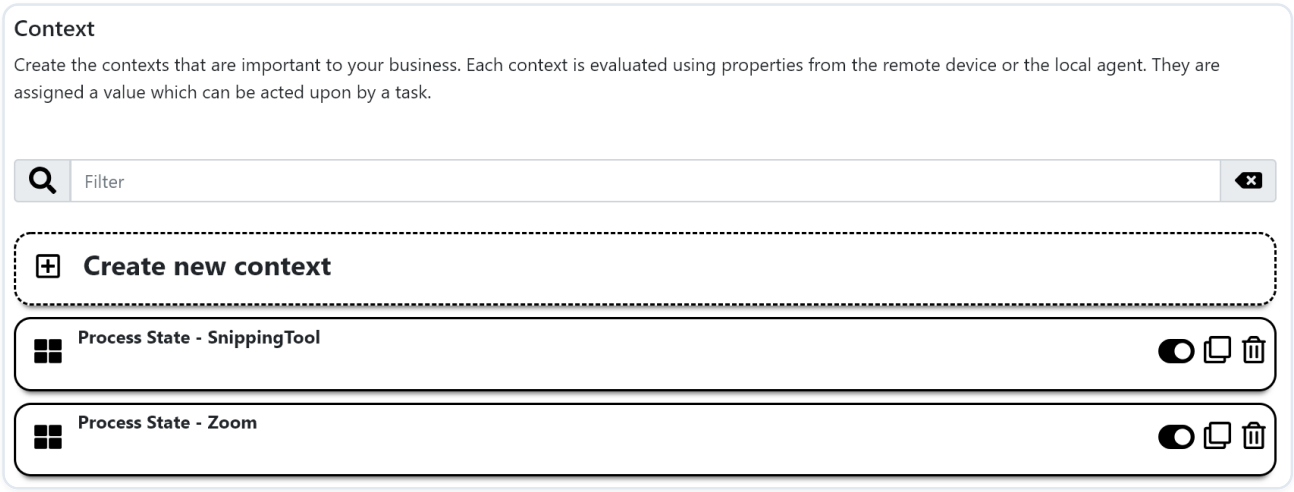
```
Write-Host "CONTINUE"
```

Fourth: Add a timeout of your choice. A 1 second loop should do fine in most cases.

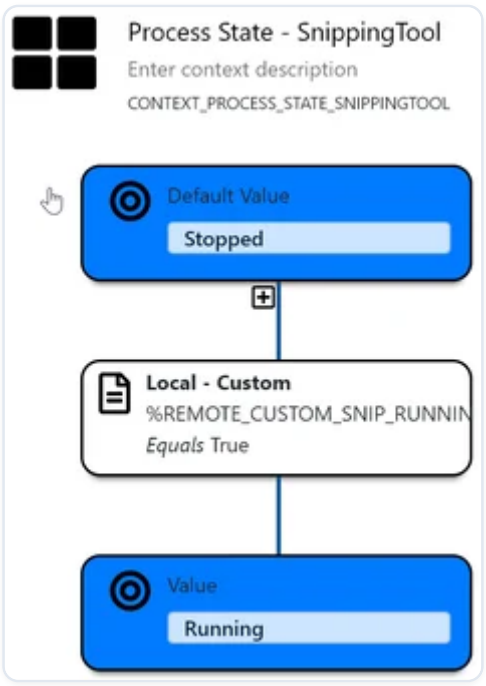
```
Sleep -Seconds 1
```

Create Contexts to use the evaluated data: The "Custom Properties" script creates internal variables. Those need to be made available internally by creating matching contexts.

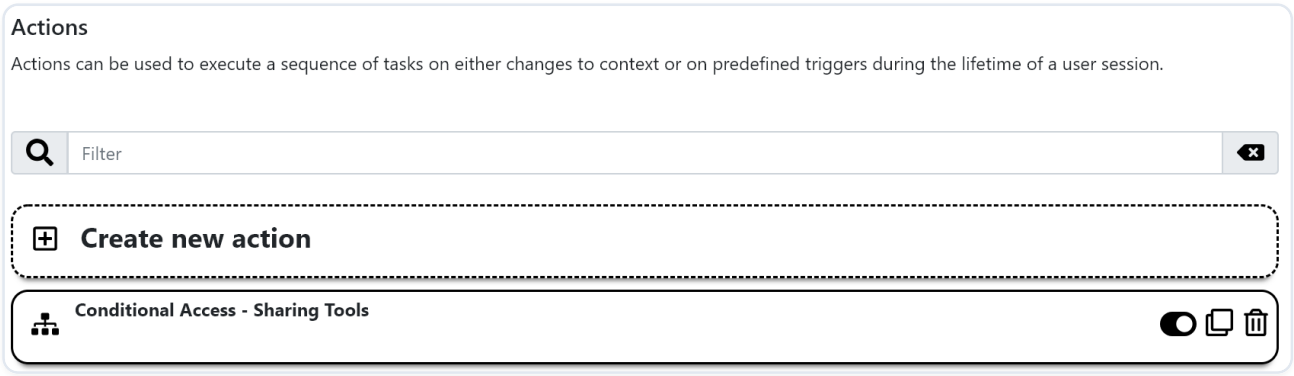
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Default value will be "Stopped" (or similar). The context will report "Running", if a "Local Custom" check is matched.

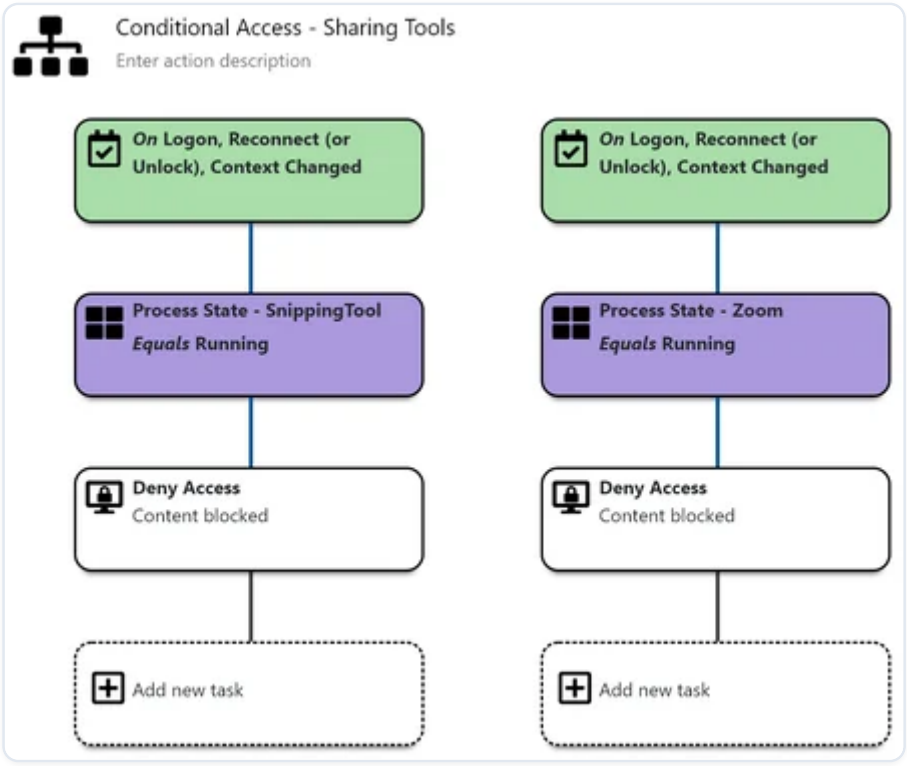


The "Local custom" check evaluates the variable that you set in the "Custom Properties" script. If the variable's value is "True", The Context will report "Running".



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

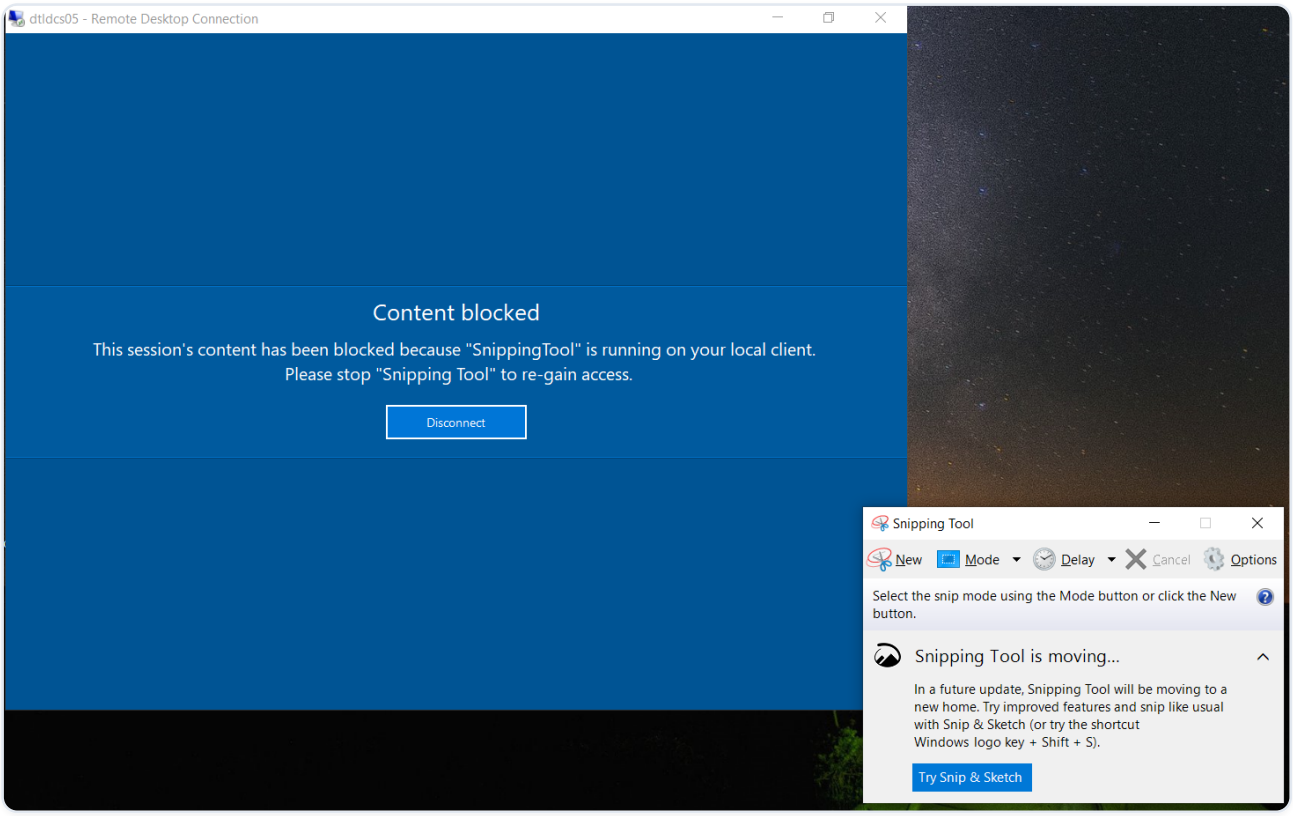
Create an action that blocks access: If you find on of the configured processes running, you might want to block access to you remote session. This way, a user cannot share the content. You'll need to create an action to do so.



Configure the action to react on your configured processes. In this example, both "Zoom" and "Snipping tool" will trigger a "Deny Access" Task.

Outcome: Having the configuration in place, your remote sessions will deny access as soon as a user starts one of the configured processes / applications on her local device. This way, deviceTRUST will help protecting your sensitive data and information.

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



deviceTRUST® + Apple Silicon support

Apple Silicon, the most powerful chip designed specifically for the Mac. Amongst all of the powerful features there are a couple of things to note when using the intel based remoting clients alongside deviceTRUST on an M1/M2 capable Mac.

Native support for Apple Silicon

This has been added in the latest release of the deviceTRUST Client Extension version 21.1.300.

This requires a remoting client that is also built with native Apple silicon support. and is therefore currently supported with the following clients:

- Citrix Workspace App for macOS v22.11.0.12 or later.
- FreeRDP v2.8.2 or later.
- VMware Horizon View v8.7.0 or later.

Remoting clients that do not support Apple Silicon

Earlier versions of the above technologies may still require Rosetta translation. For example, Citrix added support for the Apple silicon M1 chip in Workspace version 2101. In order to use 3rd party virtual channels with Workspace there is a dependency on Rosetta 2 being installed. Without

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

Rosetta these virtual channels may not work in Citrix Workspace app on macOS Big Sur 11.0 and later. More information on this can be found here.

Other remoting technologies that do not currently support Apple Silicon will also require Rosetta 2 to be installed. The latest deviceTRUST Client Extension is compatible with this configuration.

Rosetta 2

Rosetta is Apple's tool for translating code intended for Intel processors so that the M1 chip understands it. Rosetta 2 should mean that most existing Mac apps will run on the new M1 Macs. More information on how to install Rosetta on your Mac can be found here.

If you are intending to run deviceTRUST Client Extension 21.1.300 on an M1 mac with a remoting technology that does not support Apple Silicon

- Install remoting client
- Install Rosetta 2
- Install deviceTRUST Client Extension 21.1.300

deviceTRUST® + CVE-2021-44228 "Log4Shell"

If you have opened Twitter, LinkedIn or basically anything with Internet access since last Thursday, you will have heard of "log4j" or "Log4Shell". There are already heaps of very good sources on the details of this security issue. Please refer to those if you wish to get more insight:

- CVE – CVE-2021-44228 (mitre.org)
- Log4j – Apache Log4j Security Vulnerabilities
- Zero-Day Exploit Targeting Popular Java Library Log4j (admin.ch)
- Zero-day in ubiquitous Log4j tool poses a grave threat to the Internet (Ars Technica)

You might be wanting to take a look at the list of affected software to make sure you can take the right measures authomize/log4j-log4shell-affected (github.com).

That being said: deviceTRUST does not use any Apache JAVA components at all. Though we use a server-client-concept in some situations, none of our components include JAVA code in general or the affected libraries in special. deviceTRUST is, thus, not affected by CVE-2021-44228.

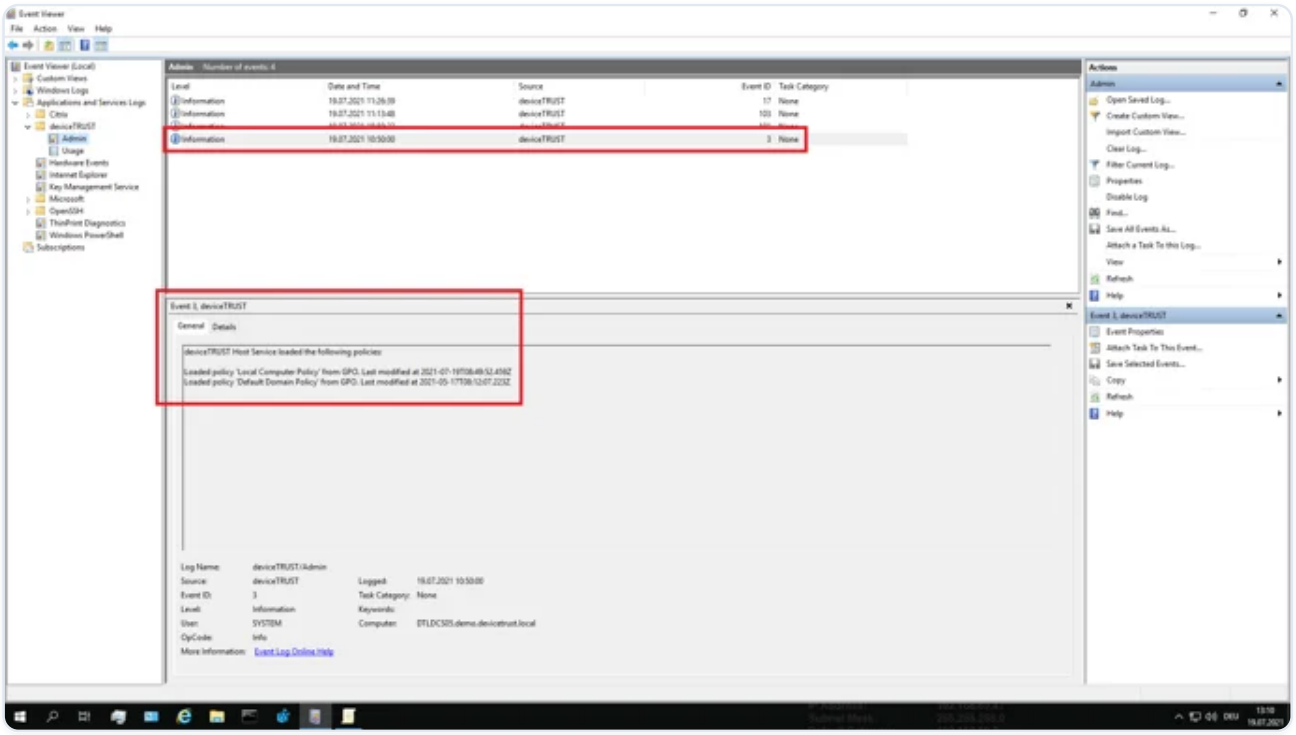
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Check that your contextual security policy has been saved and deployed

Ensure that your deviceTRUST contextual security policy has been saved within the deviceTRUST Console and successfully deployed to the host system.

To check which policies are effective, open the Windows Event Log on the remoting or DaaS host system, navigate to APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN, and look for Event ID 3, which details the name of each policy and the timestamp that it was last modified.

The deployed policies



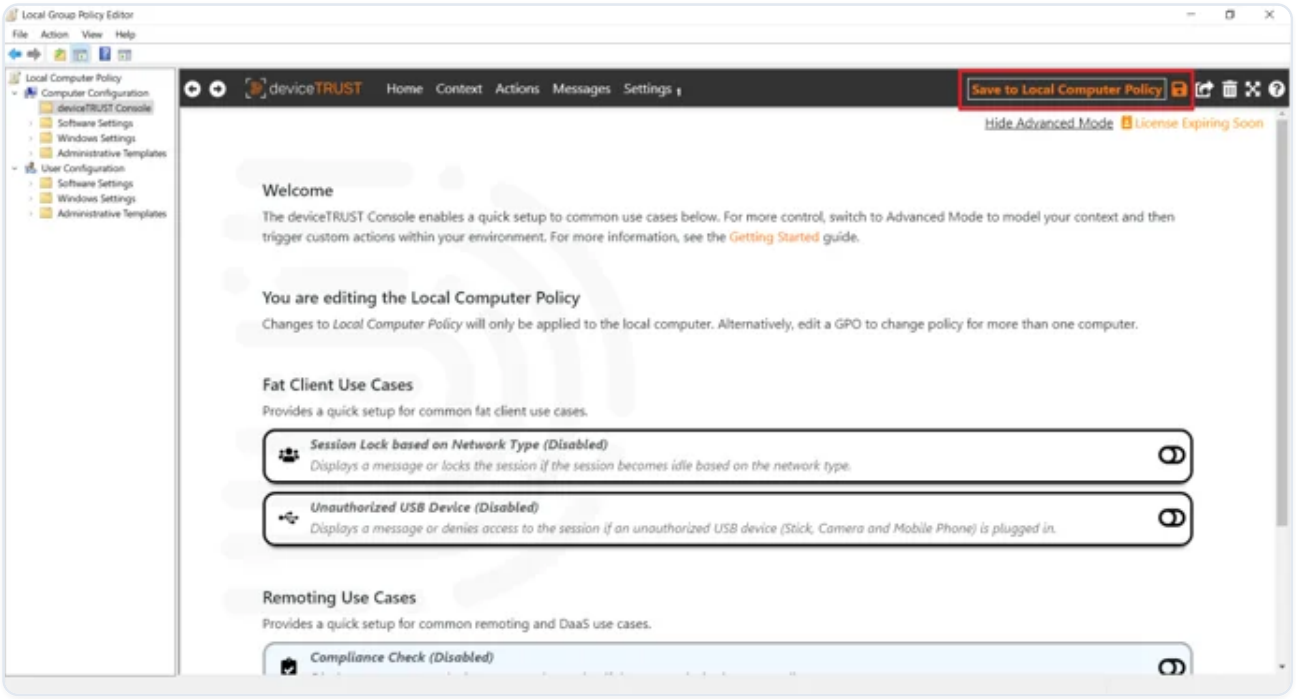
NOTE:

User sessions get their deviceTRUST policies during login and are active until the session is logged out. If newer contextual security policies are deployed on the remoting or DaaS host during this time, they will not affect running user sessions, only new logins.

Save the policy

If the policy is not listed or does not have the expected timestamp, ensure that you have successfully saved the policy from within the deviceTRUST Console.

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



Next, the policy must be successfully deployed to the remoting or DaaS host system. The method used to deploy the policy depends on where the changes were saved.

Local Policy

When using local policy, no additional steps need to be taken to enable the updated contextual security policy for the deviceTRUST Agent.

Group Policy Object (GPO)

When using group policy, a Group Policy update should be forced on the remoting or DaaS host system to propagate an update of the contextual security policy. Of course, waiting for the next group policy refresh is possible, but for testing purposes, this can be forced directly with a call to GPUPDATE /TARGET:COMPUTER. After the updated contextual security policy is successfully deployed to the remoting or DaaS host system, the deviceTRUST Agent will use it immediately.

File-based

When using a file-based policy, the updated contextual security policy is copied to the appropriate target directory as a file-based policy on the remoting or DaaS host system. After the updated file-based contextual security policy is copied to the target directory, the deviceTRUST Agent will use it immediately.

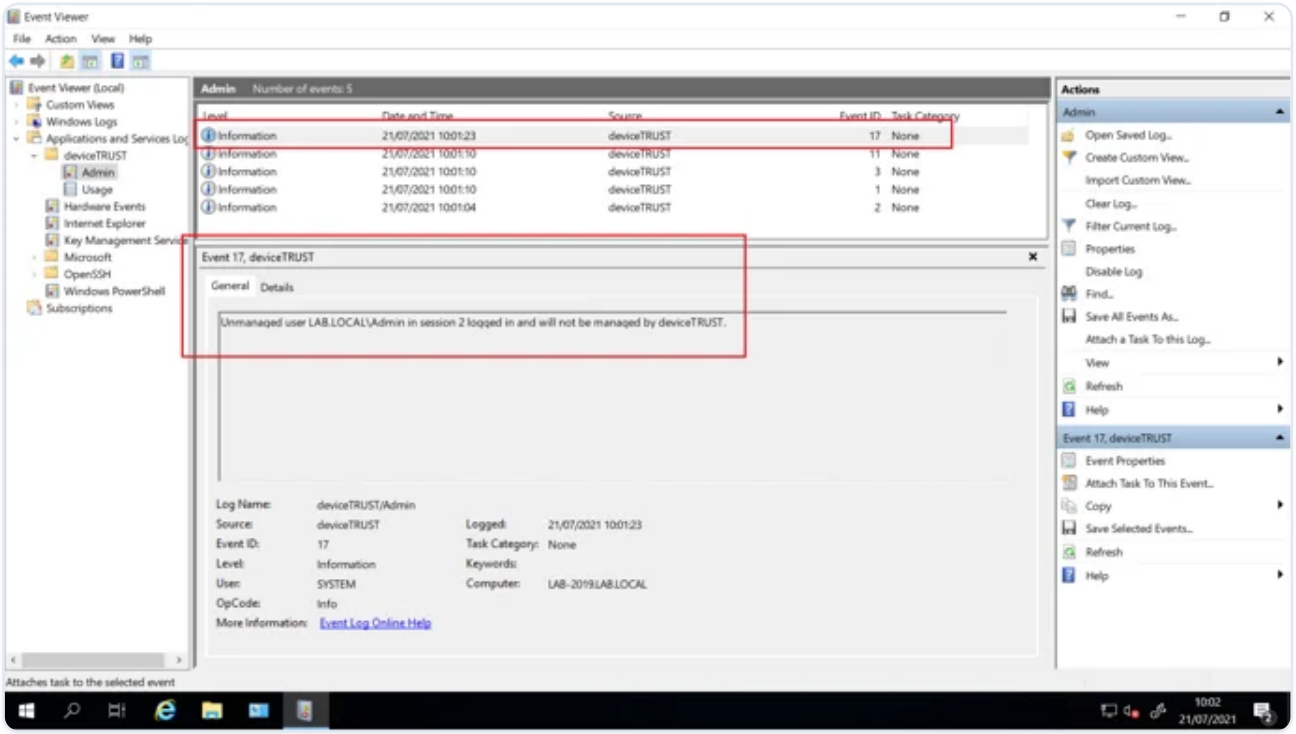
Check that the user is managed by deviceTRUST

The deviceTRUST contextual security policy defines the users that will be managed by deviceTRUST. By default, this does not include members of the local administrators group.

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

To check if an unmanaged user has signed in, open the Windows Event Log on the remoting or DaaS host system, navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN`, and look for Event ID 17.

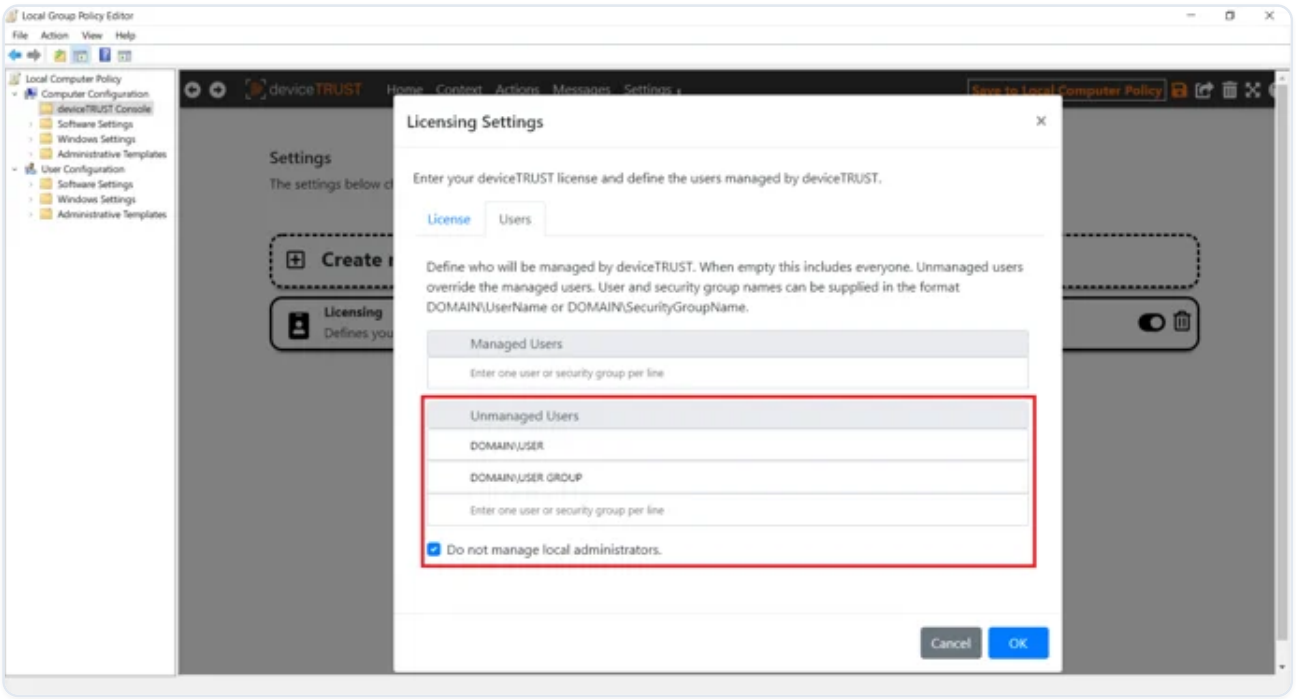
An unmanaged user signed in



To change the list of managed users, open your active deviceTRUST contextual security policy, navigate to DEVICETRUST CONSOLE, and click the SETTINGS tab. Select LICENSING, navigate to the USERS tab, and check that the user account is not configured in the UNMANAGED USERS directly or via group membership.

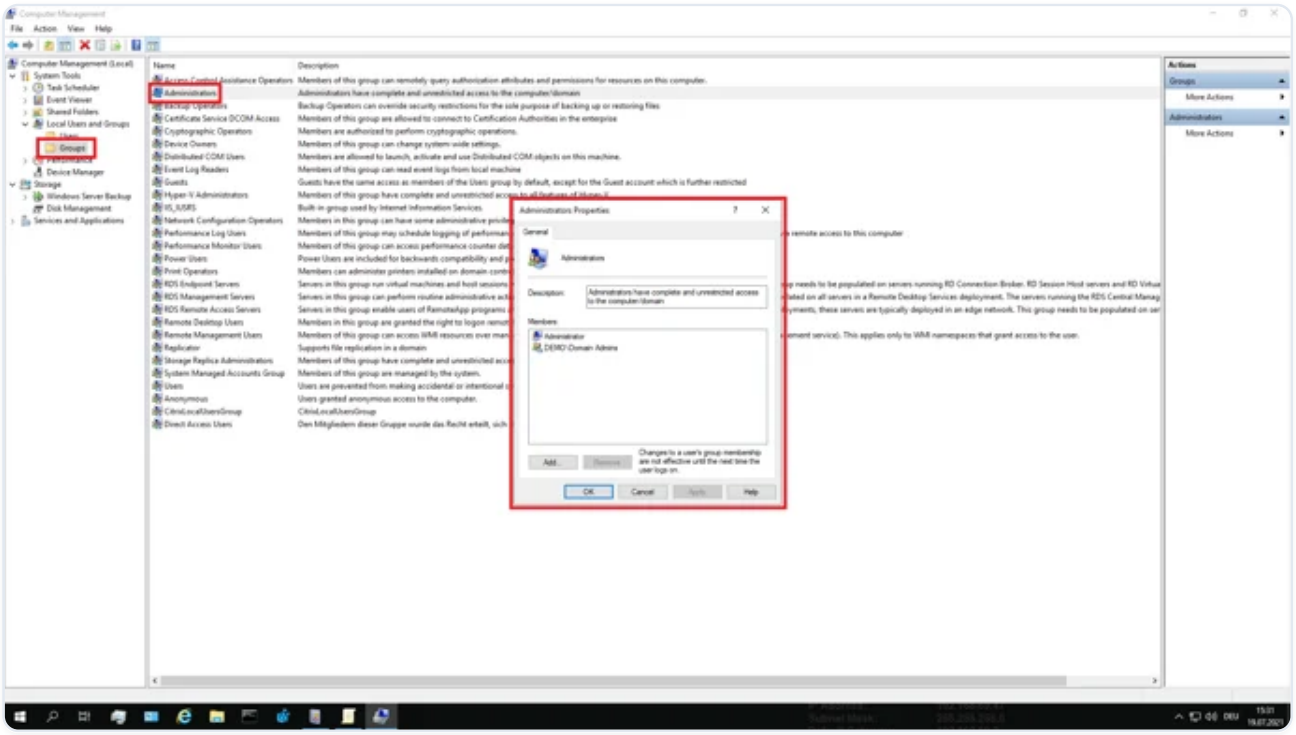
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unmanaged Users



If deviceTRUST policies are still not applied to the user, check if the user account is a member of the local administrators group. To do this, start COMPUTER MANAGEMENT on the remoting or DaaS host system, navigate to SYSTEM TOOLS, select LOCAL USERS AND GROUPS, and check that the user is not a member of the ADMINISTRATORS group.

Administrative Users



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

Custom Process + PowerShell Cert signing

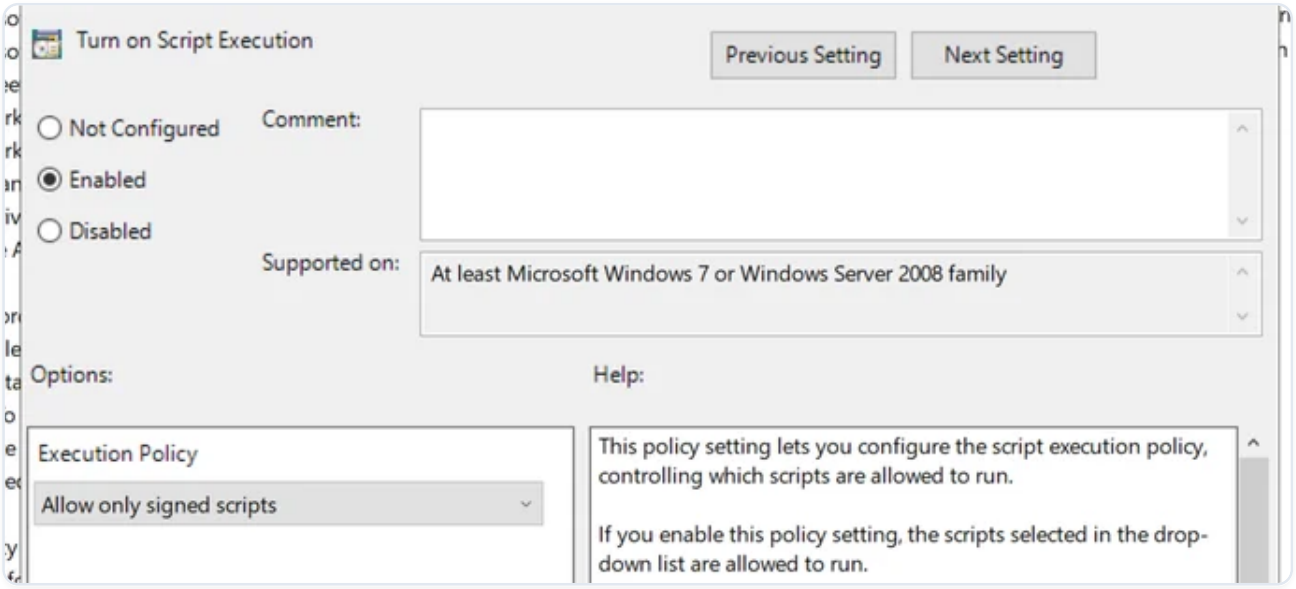
You may need to sign PowerShell scripts you use for your deviceTRUST Custom Processes. File format can be a challenge with script signing. Read here how to format the signed PowerShell scrips properly.

Script signing signs the given script with all details, including content, name, file properties, and format. A change in the file format can be a cog in the machine if unrecognized.

We use a PowerShell script here to guide you through the signing process.

The situation

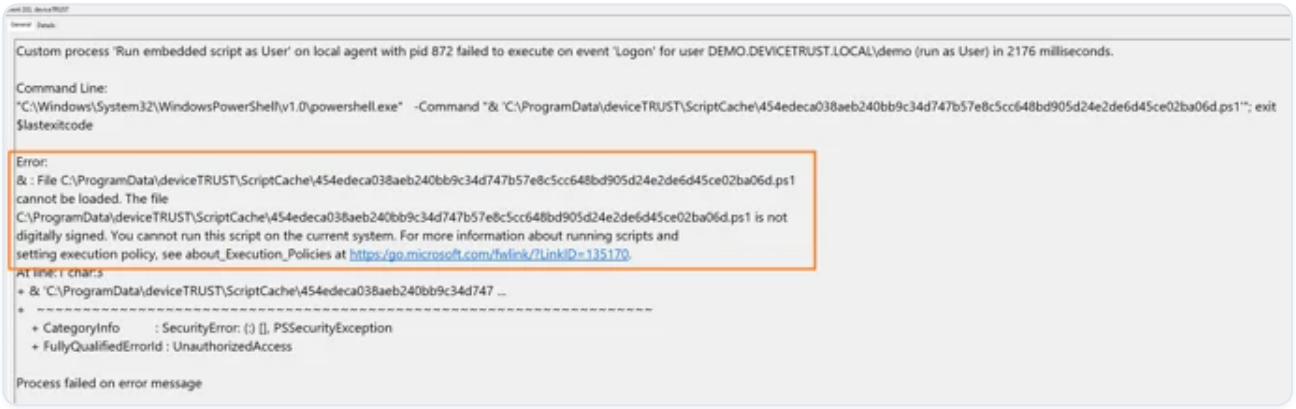
Your PowerShell Execution Policy might be set to "Signed Scripts only". This way, the execution of any PowerShell script that has not been signed with a trusted code signing certificate will be denied from running.



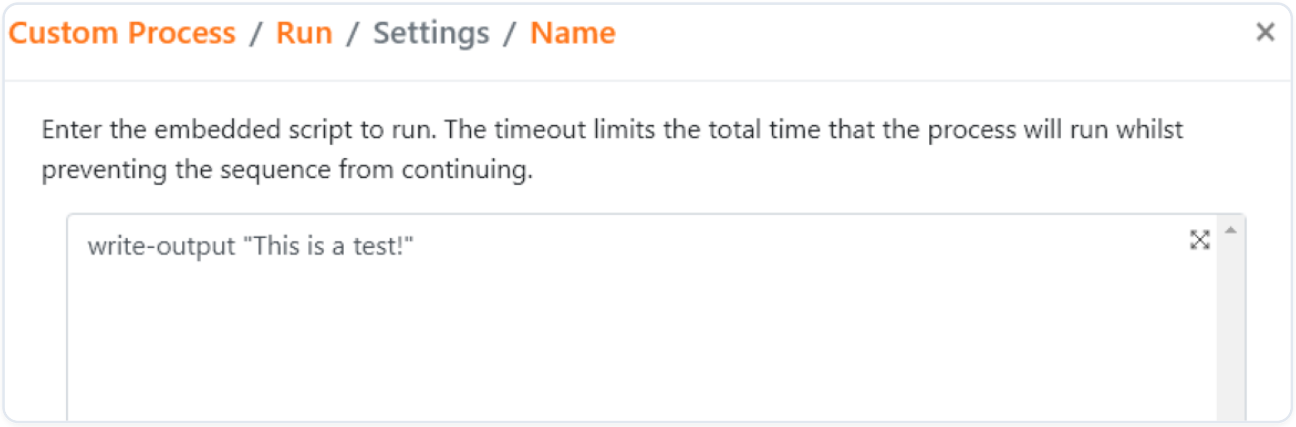
The issue

Codesigning being enforced will affect PowerShell based Custom Processes in deviceTRUST Actions. Unsigned scripts will be triggered, but not executed.

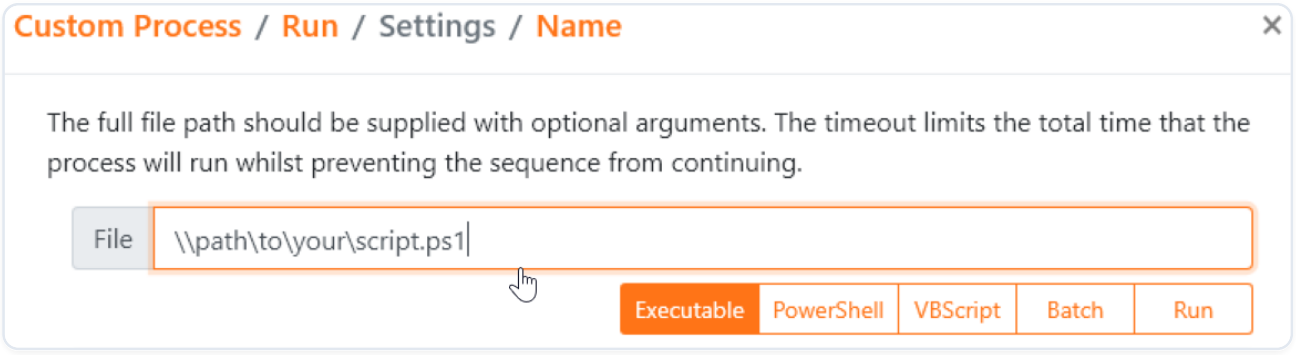
© 1997–2026 Citrix Systems, Inc. All rights reserved.



This is valid for embedded scripts.



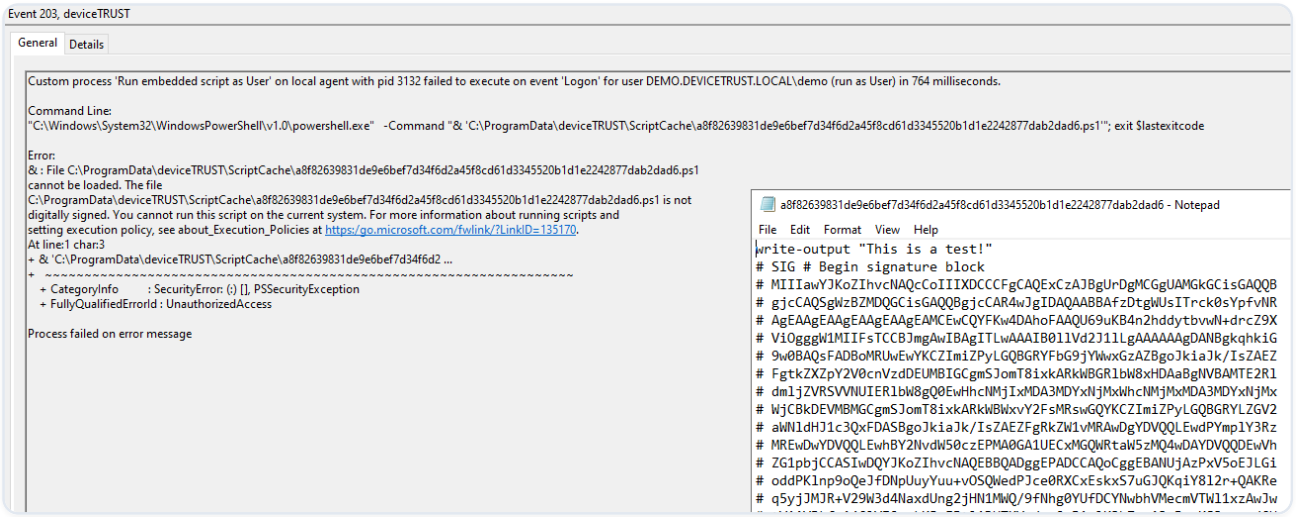
... as well as for externally triggered scripts.



The second issue

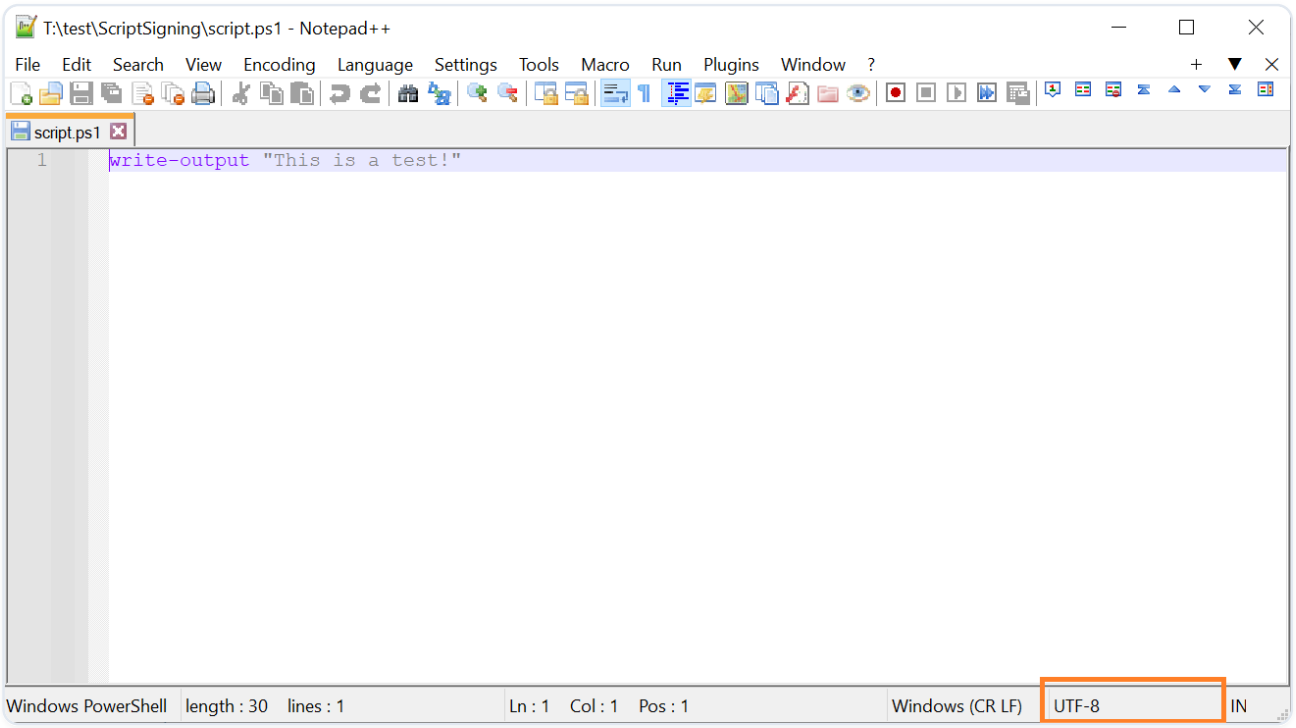
Now, even if you signed the cert with your certificate, you might see the same issue: The script is being blocked from execution. The signing is not accepted.

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



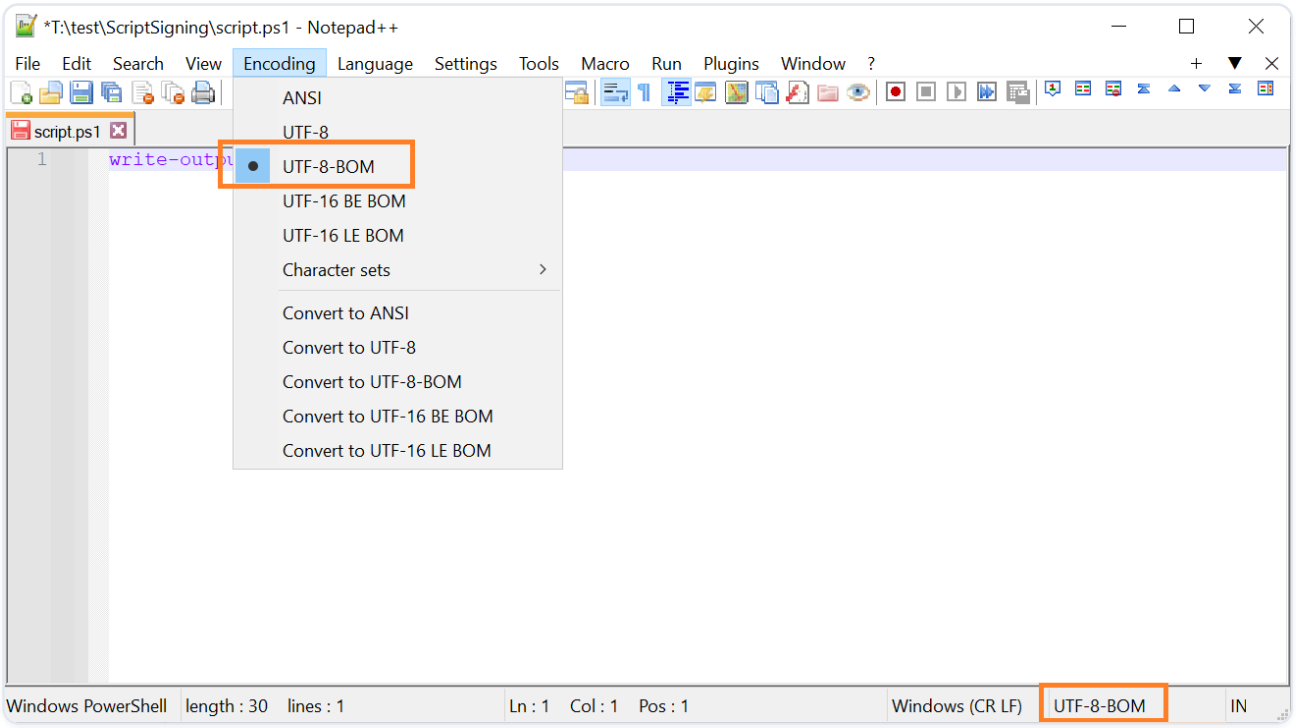
The solution

Opening the script in your favourite text editor before signing, you'll notice the file format being (for example and most likely) "UTF-8".

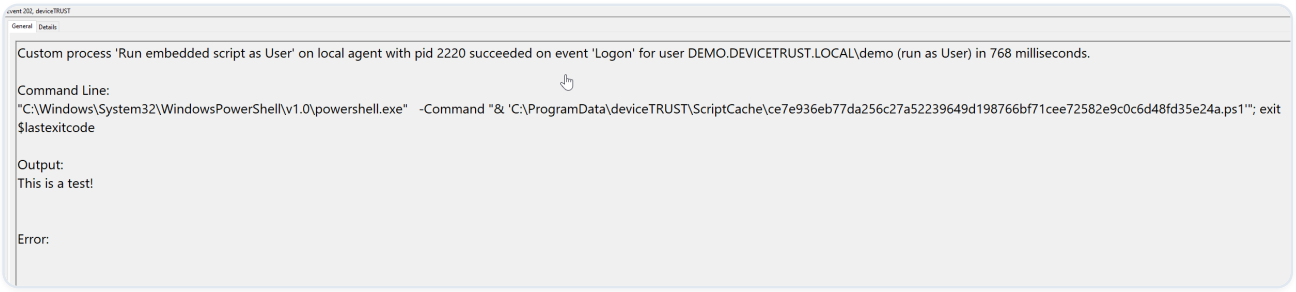


Set the file format to "UTF-8 with BOM" and save. Then sign again.

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



This will result in a sucessfully executed script.



Anything shown is valid for PowerShell scripts, be the embedded or referenced as file.

Deny Access, Logout or Disconnect?

When access to a session is controlled with a Deny Access task, users will be presented with either a Disconnect or Sign out button. This article describes, when and why either will be used.

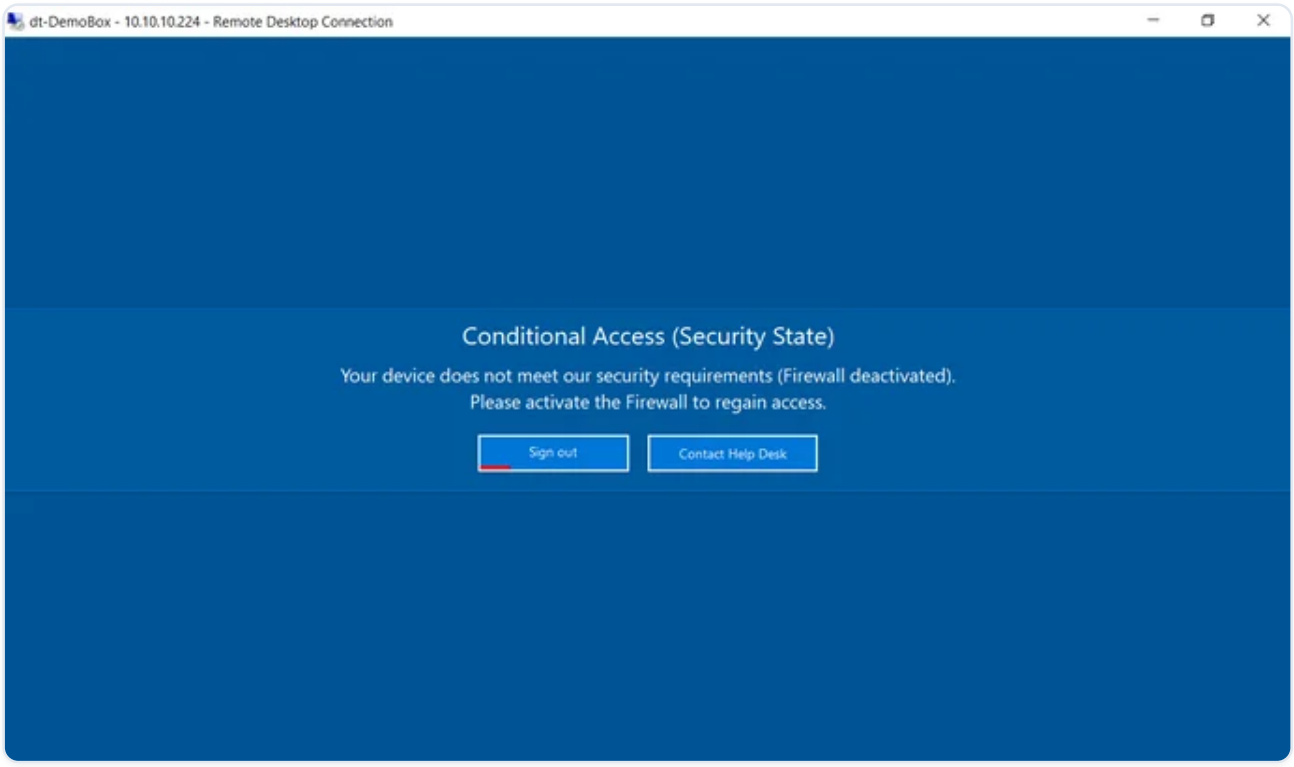
Inarguably deviceTRUST's most straightforward use case is conditional access, or - more specifically - conditional workspace access: The user's access to a remote session will be denied based on the individual Context.

Without further configuration, deviceTRUST will display a "Sign out" button or a "Disconnect" button when denying access. The distinction is made to adjust to the type of session the user has on the system.

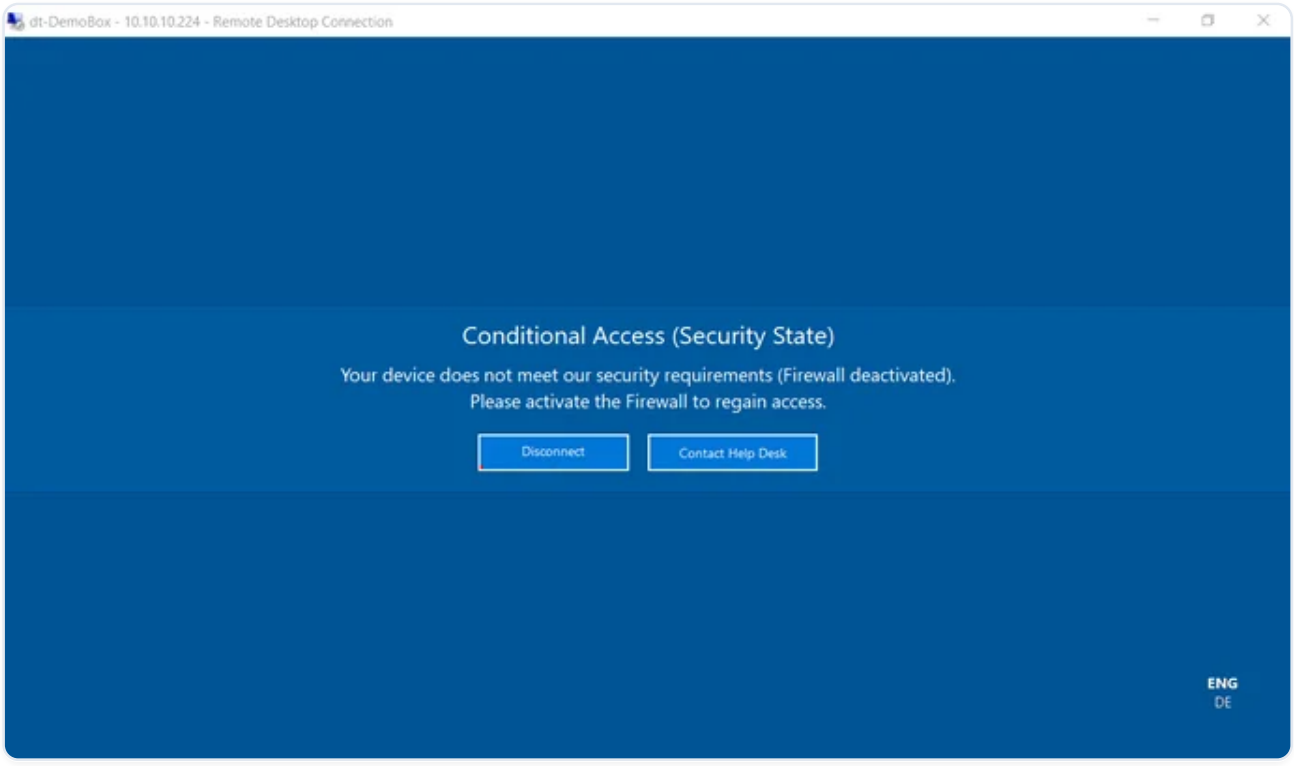
If the user is just about to log on to a remote system and thus has not started any resources or software, deviceTRUST will present the "Sign out" button. In this case, we can be sure no unsaved

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

data is lost when logging out the user. It is the most straightforward action to log out the user and - thus - save resources on the (remote) system.

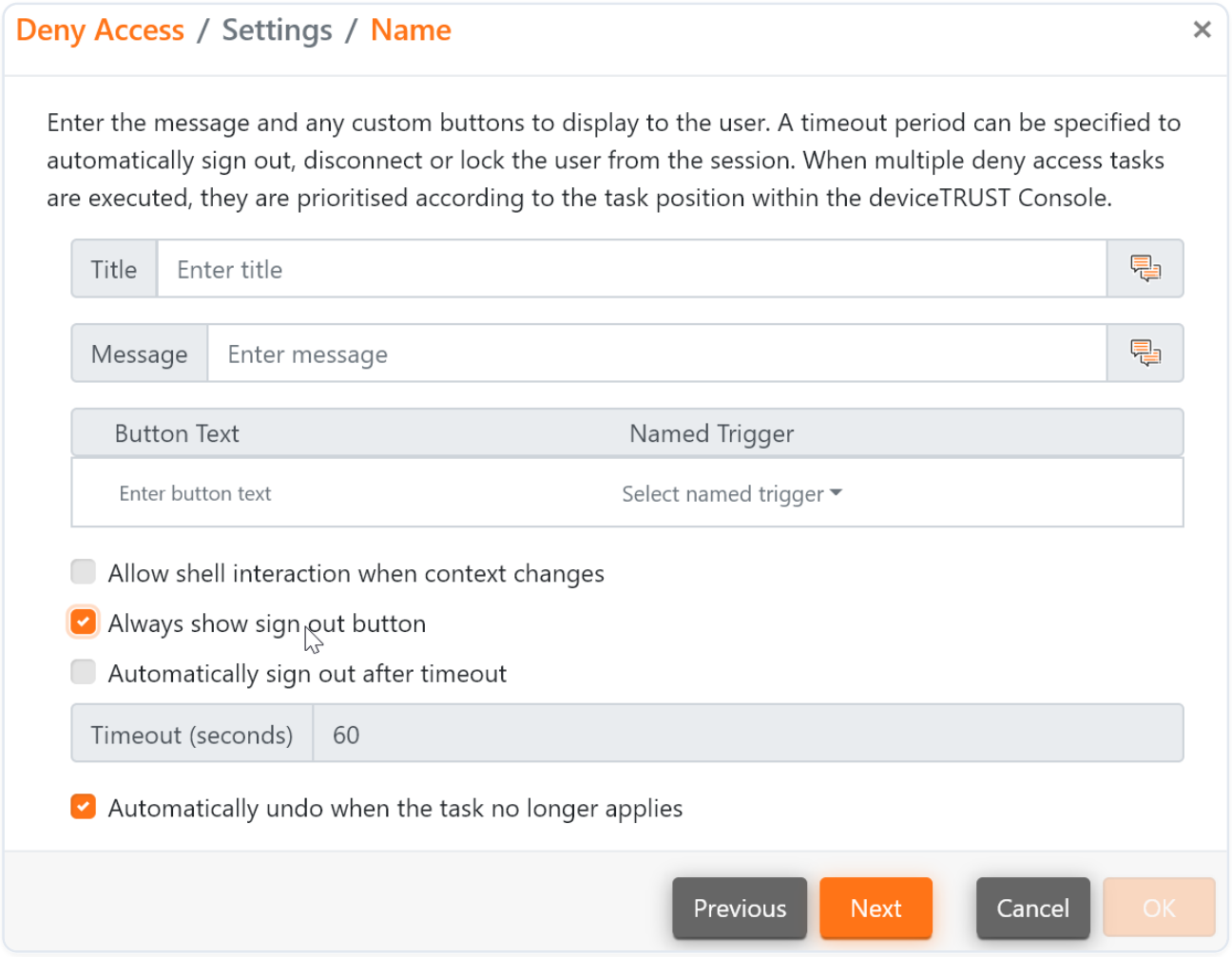


If the user has already started a session on the remote system, deviceTRUST will present a "Disconnect" button by default. This way, the session will be kept alive in the background, and the user can re-access it once the Context fits the requirements again. This way, we make sure unsaved work will not be lost. The disconnected session might be logged off automatically based on your configured policies.



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

You'll find a switch to alter this behavior in the "Deny Access" task of your deviceTRUST Actions. The "Always show sign out button" check box will ensure users are only presented with the "Sign out" button, whether they have already launched a session and started applications or not.

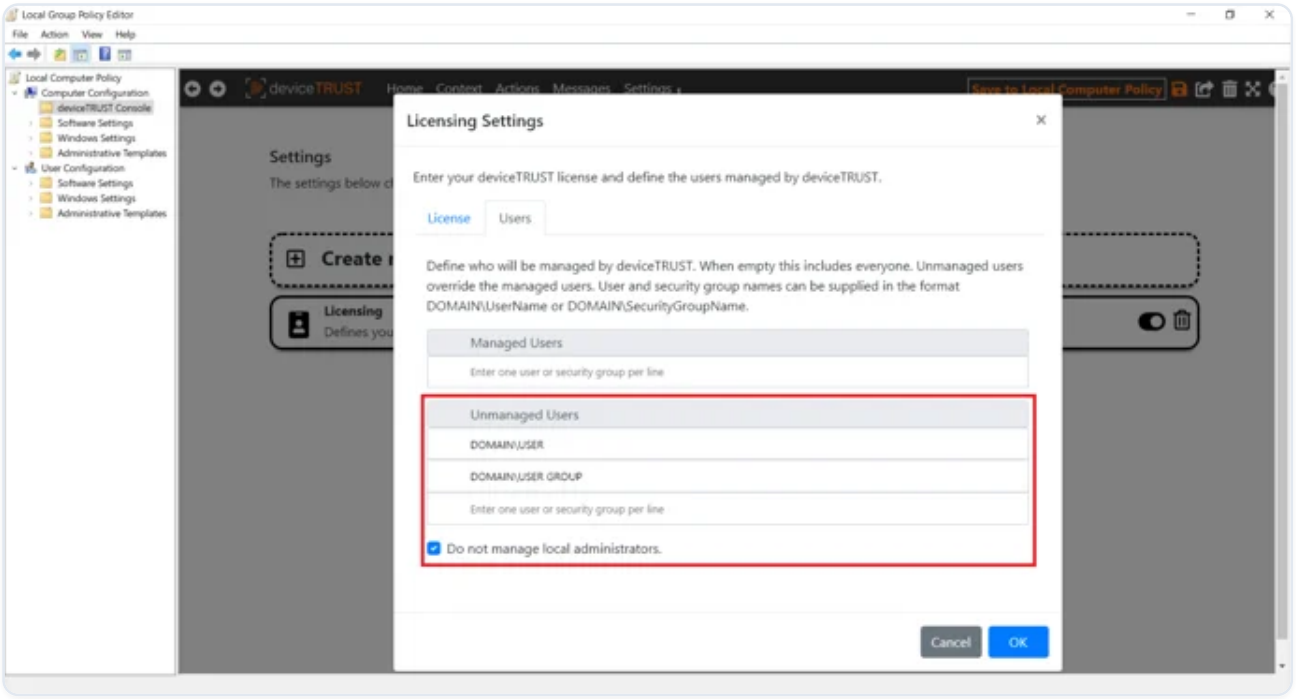


Exclude specific users from the deviceTRUST policy

It may be necessary to exclude a user or user group from the deviceTRUST contextual security policy, for example, to quickly grant access independently of deviceTRUST on the host system.

To exclude a user, open your active deviceTRUST contextual security policy and navigate to DEVICETRUST CONSOLE and click on the SETTINGS tab. Select LICENSING, navigate to the USERS tab and add the user or the user group to the UNMANAGED USERS to exclude them completely from deviceTRUST.

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

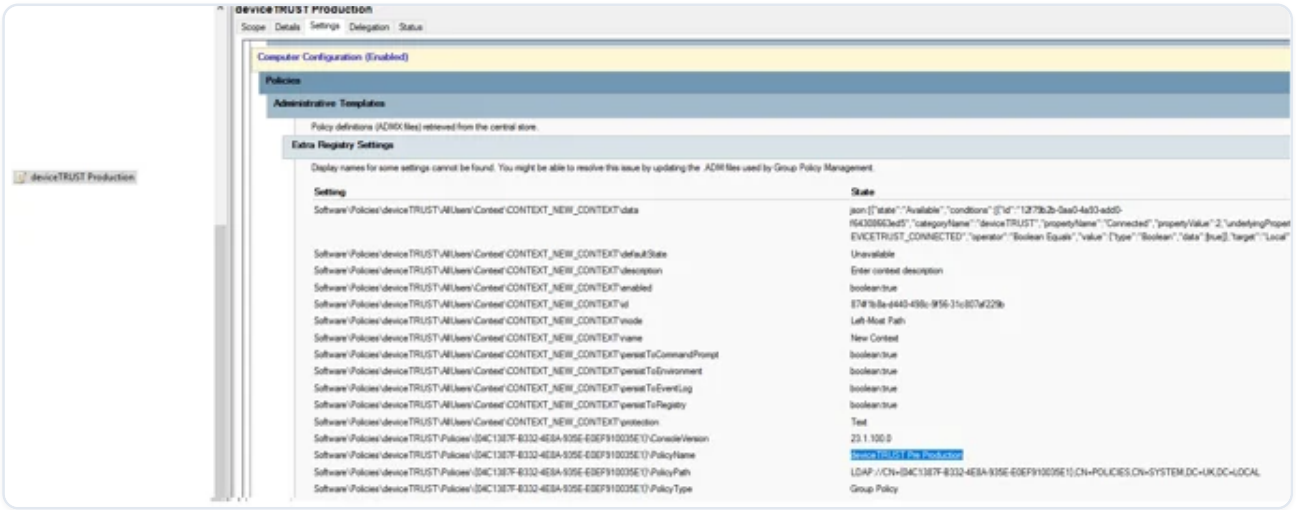


GPO name is not updated in deviceTRUST policy when copying a GPO within group policy editor

The name of the GPO is saved into the deviceTRUST configuration at the time our console saves to the GPO. If you copy a GPO that contains deviceTRUST policy within a group policy editor, then the previous policy name is still persisted.

This is a common scenario when migrating a deviceTRUST policy from test to production.

The example below demonstrates a GPO that has been copied but contains the original policy name



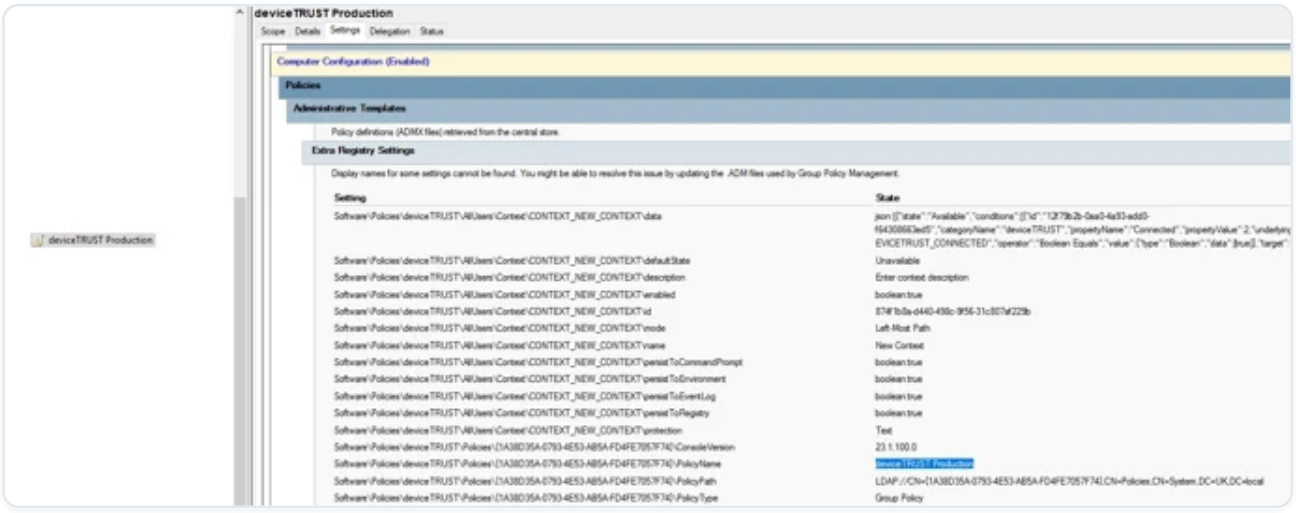
If you have copied a policy within a group policy editor, such as GPMC, that contains deviceTRUST policy the name can be updated in the copied GPO using the steps below.

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

- Open deviceTRUST Console
- In the Open Policy dialogue select 'Open Group Policy'
- In the GPO browser windows select the GPO that was copied
- This will open the copied policy in the deviceTRUST Console
- In the deviceTRUST Console click the down arrow next to the save icon in the top right corner and select 'Save As'
- In the 'Save As' Policy dialogue select 'Save Group Policy'
- Browse and select the policy that was copied
- Click OK to update the policy

If you check the 'Settings' of the copied GPO it should contain the updated name.

The name set in the policy settings has been updated to reflect the name of the GPO



Configuring Citrix Virtual Channel Security

In iOS 16 or later, Apple requires an com.apple.developer.device-information.user-assigned-device-name entitlement for an application to be able to read the device name. Currently, the deviceTRUST iOS Client Extension does not include this entitlement, and therefore the operating system always returns 'iPhone' or 'iPad' as the device name. Consequently, when the deviceTRUST Client Extension for iOS running on iOS 16 or later registers with the deviceTRUST Portal, it is registered against the wrong device name.

The deviceTRUST Agent identifies the remote iOS device name using the LOCAL_REMOTECONTROL_REMOTE_NAME property within the virtual session. This remote iOS device name is compared against the name of the iOS devices registered within the deviceTRUST Portal at https://portal.devicetrust.com/#/app/admin/devices to determine which iOS

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

device to connect to. If the devices are registered against the wrong device name, then a successful connection cannot be made.

Establishing the `com.apple.developer.device-information.user-assigned-device-name` entitlement from Apple is work in progress. It may be necessary for us to make changes to the deviceTRUST iOS app before this entitlement can be granted.

Whilst we work to establish the entitlement, we've made the following changes to the deviceTRUST Portal to mitigate the problem.

- We've added the ability to manually rename the iOS devices. By renaming the devices to the value that appears within the iOS Settings app under General > About > Name, a successful connection can once again be established.
- When the deviceTRUST Portal determines that an iOS device has been upgraded to iOS 16 or later, the previous device name is captured and the device is automatically renamed.

An updated deviceTRUST Client Extension for iOS will soon be released which allows the user to better identify their iOS device within the deviceTRUST Portal, allowing multiple iOS devices all with the name 'iPhone' or 'iPad' to be better identified.

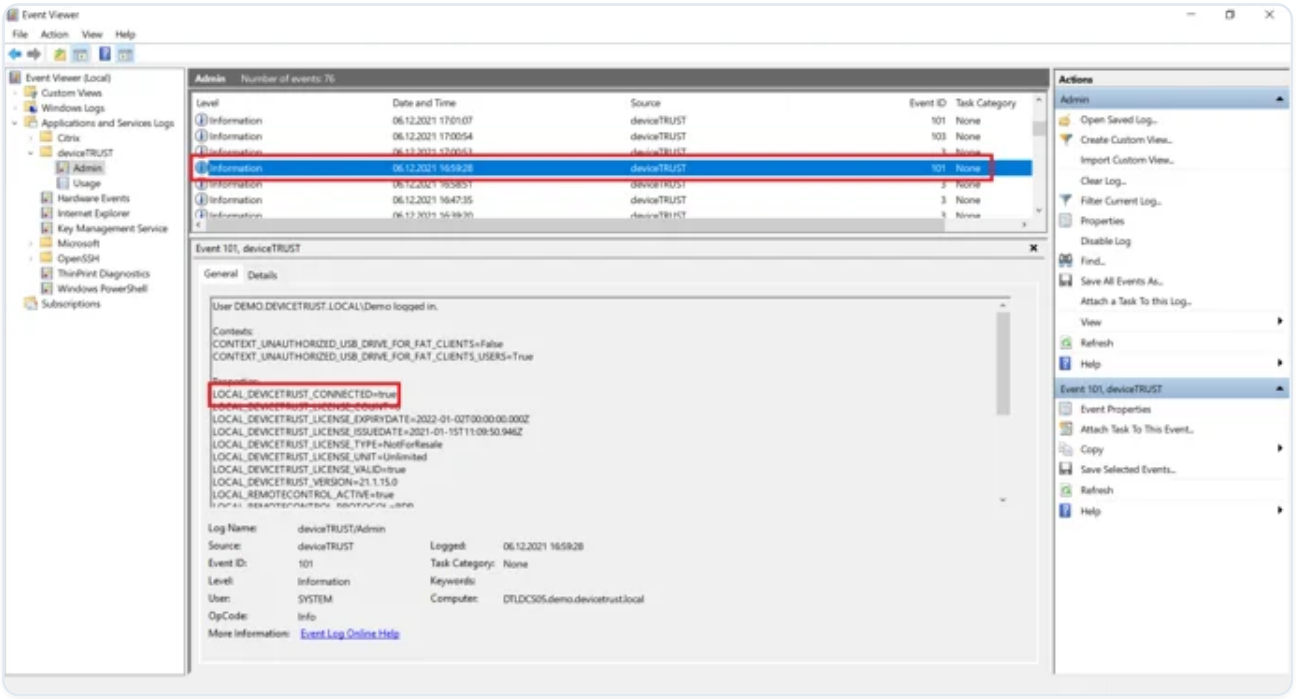
Check that the deviceTRUST Client Extension is installed on the remote device

Within the user session, a deviceTRUST property can detect whether a deviceTRUST Client Extension has been detected on the remote device.

To check whether a deviceTRUST Client Extension has been identified on the remote device, open the Windows Event Log on the remoting or DaaS system, navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN`, and check for Event ID 101. This event is raised during logon and details the properties and context of the users' virtual session.

Virtual session properties and contexts

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



The LOCAL_DEVICETRUST_CONNECTED property can have the following states:

- LOCAL_DEVICETRUST_CONNECTED = FALSE - No deviceTRUST Client Extension is installed on the remote device.
- LOCAL_DEVICETRUST_CONNECTED = TRUE - A deviceTRUST Client Extension is installed on the remote device.

If no deviceTRUST Client Extension is installed on the remote device, install the deviceTRUST Client Extension on the respective operating system Installation Client Extension from the Client Extension installation page.

Configuring Citrix Virtual Channel Security

With Citrix Virtual Apps™ and Desktops, the Virtual Channel Allow List must be configured to allow the deviceTRUST virtual channel.

Citrix Virtual Apps and Desktops contains a policy titled Virtual channel allow list which controls the processes which are able to open a virtual channel. When enabled, all processes except the Citrix internal virtual channels must be declared. Additional entries are required for the deviceTRUST® Agent to be able to connect to the deviceTRUST Client Extension.

- With Citrix Virtual Apps and Desktops 2109 or later, the Virtual channel allow list is enabled by default. These default settings will deny access to the deviceTRUST virtual channel as the allow list does not include the deviceTRUST process names.

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

- With Citrix Virtual Apps and Desktops 1912 LTSR to 2106, the Virtual channel allow list is disabled by default. These default settings will allow access to the deviceTRUST virtual channel.
- With previous releases of Citrix Virtual Apps and Desktops, the Virtual channel allow list is unavailable.

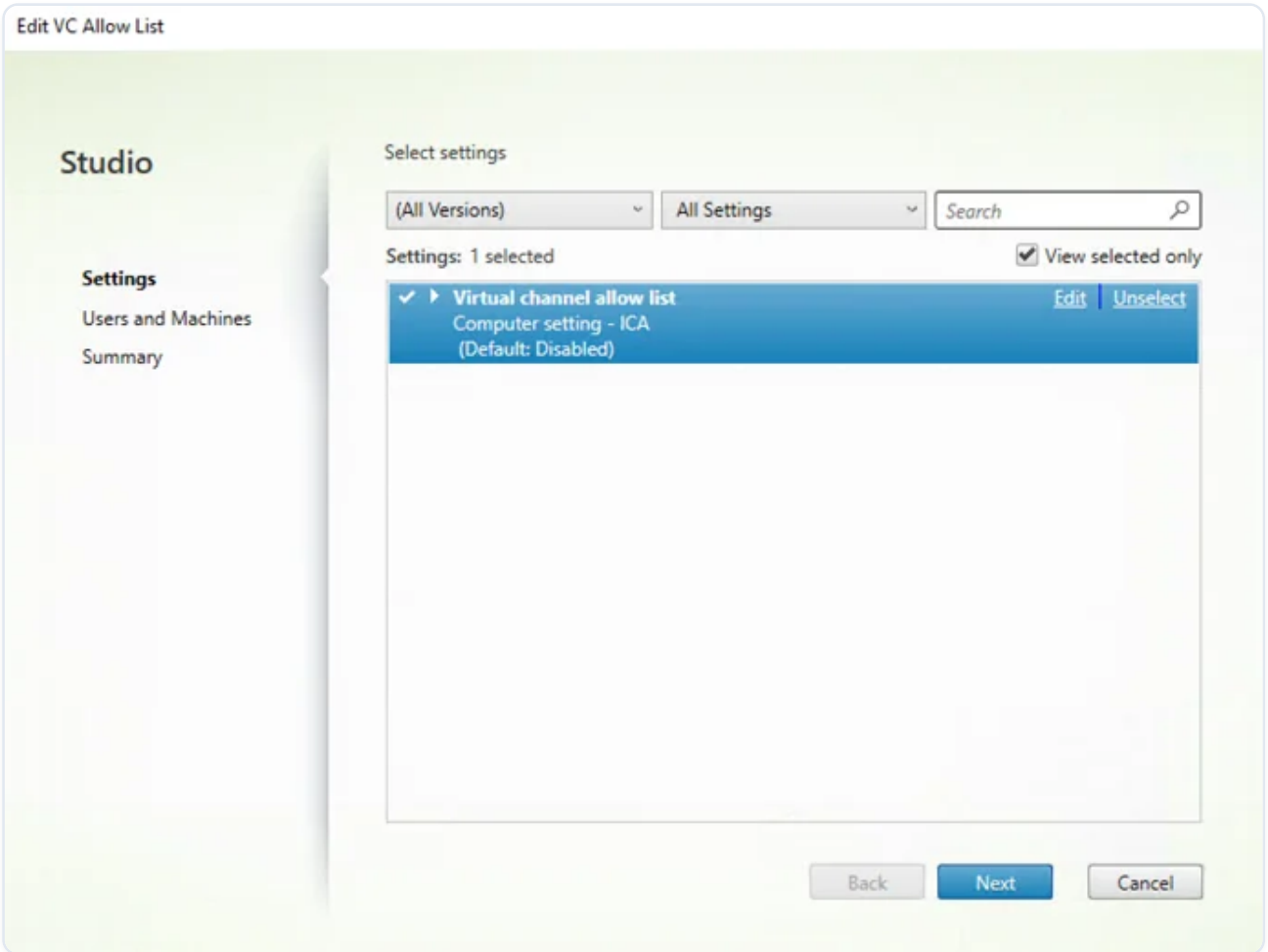
Configuration

There are two options to configure the virtual channel allow list for enabling deviceTRUST in a Citrix Virtual Apps and Desktops environment:

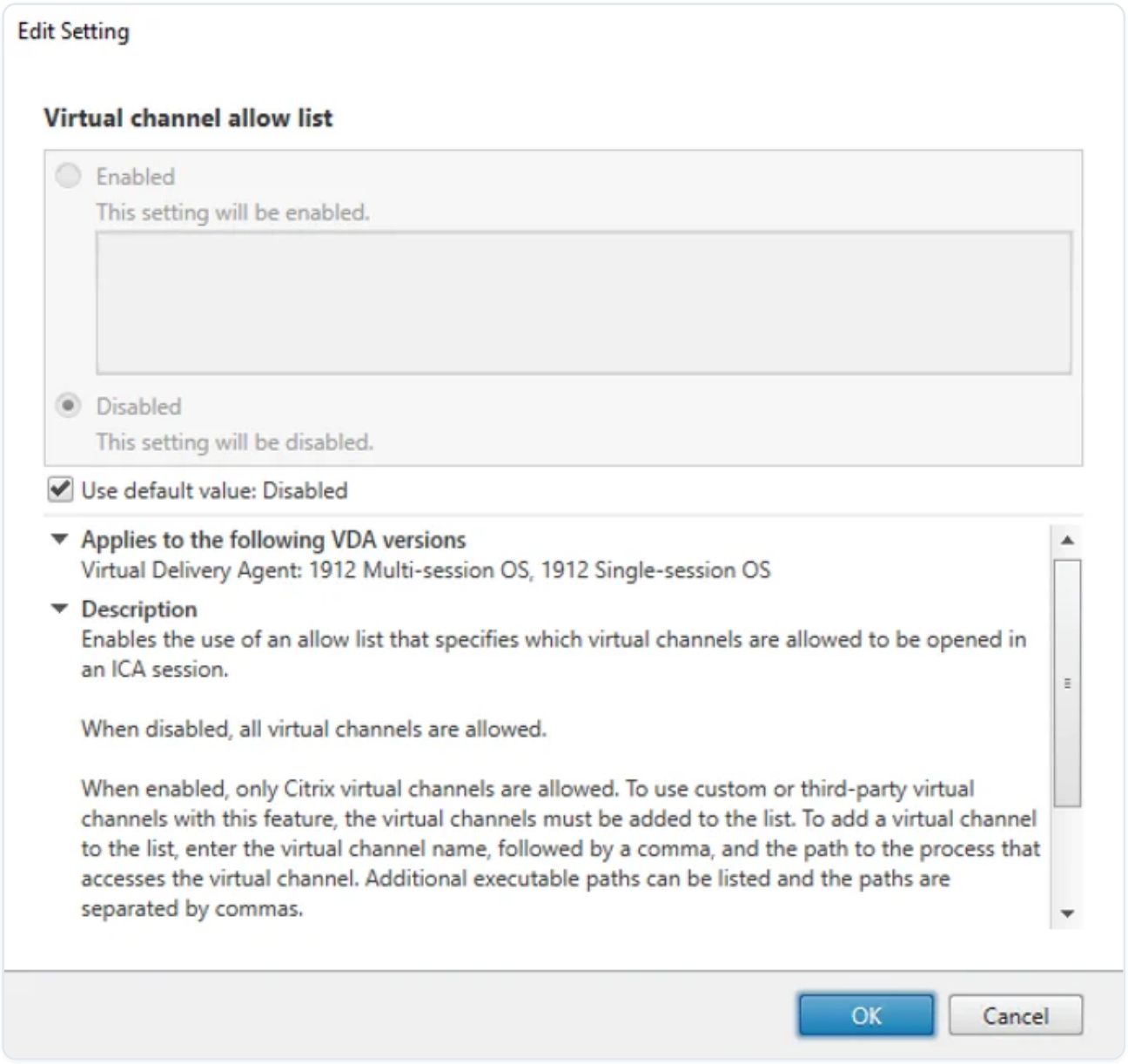
- Allowing all Citrix virtual channels plus the deviceTRUST
- Allowing all virtual channels

The first is the recommended solution, as it complies with Citrix's idea of virtual channel security. However both approaches are described here.

Both settings need to be set on the VDA level. The required configuration can be found in the Citrix farm policies. The setting's name is Virtual channel allow list.



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

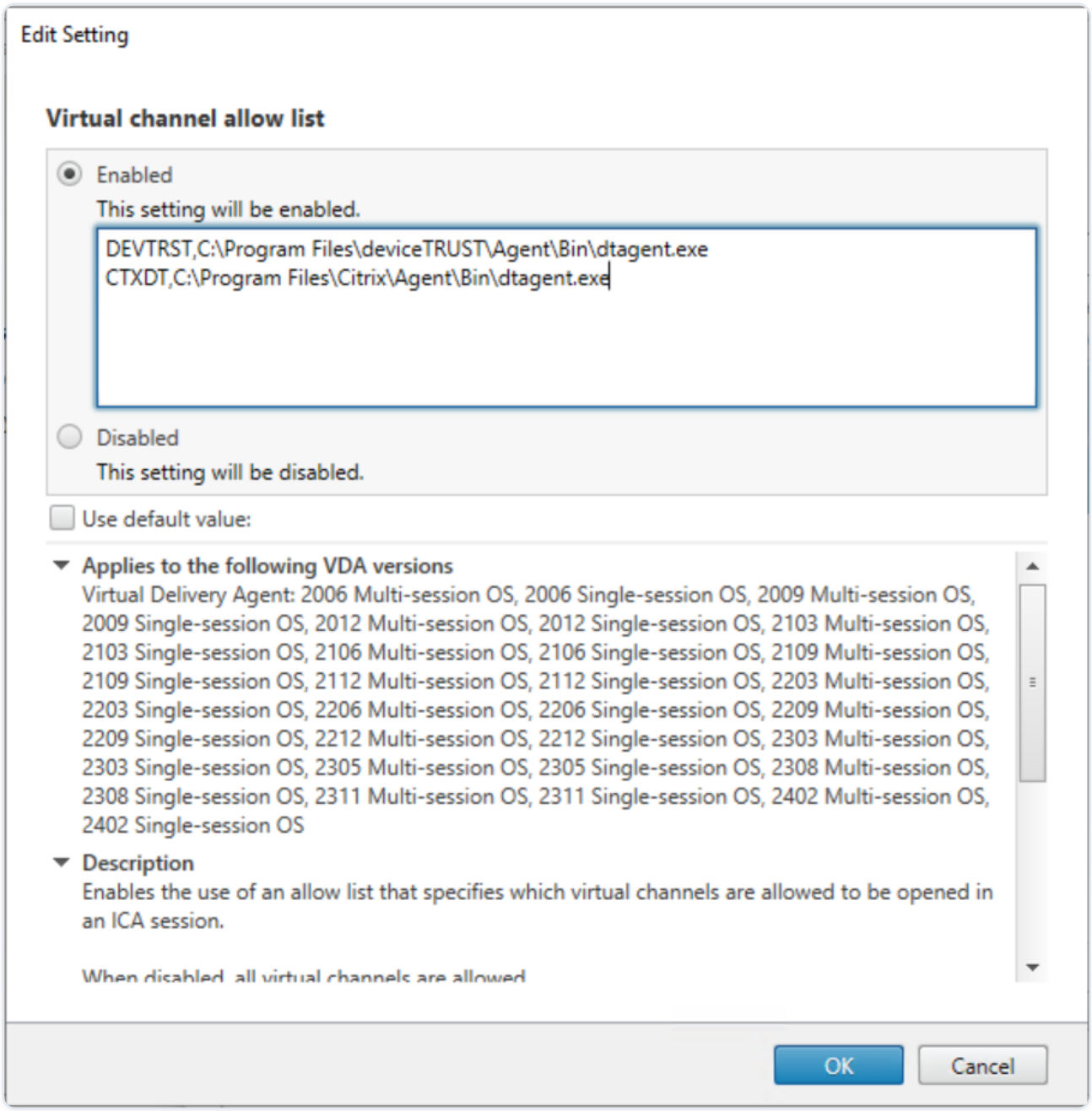


Allowing all Citrix virtual channels plus the deviceTRUST virtual channel

We recommend configuring the deviceTRUST virtual channel explicitly. Doing so will comply with Citrix's concept of securing the virtual channel feature whilst allowing deviceTRUST to establish its connection between the deviceTRUST Agent and Client. Doing so requires the following steps:

- Explicitly enable the Virtual channel allow list policy setting
- Add the following deviceTRUST virtual channel and process names to the allow list
  - DEVTRST,C:\Program Files\deviceTRUST\Agent\Bin\dtagent.exe
  - CTXDT,C:\Program Files\Citrix\Agent\Bin\dtagent.exe

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



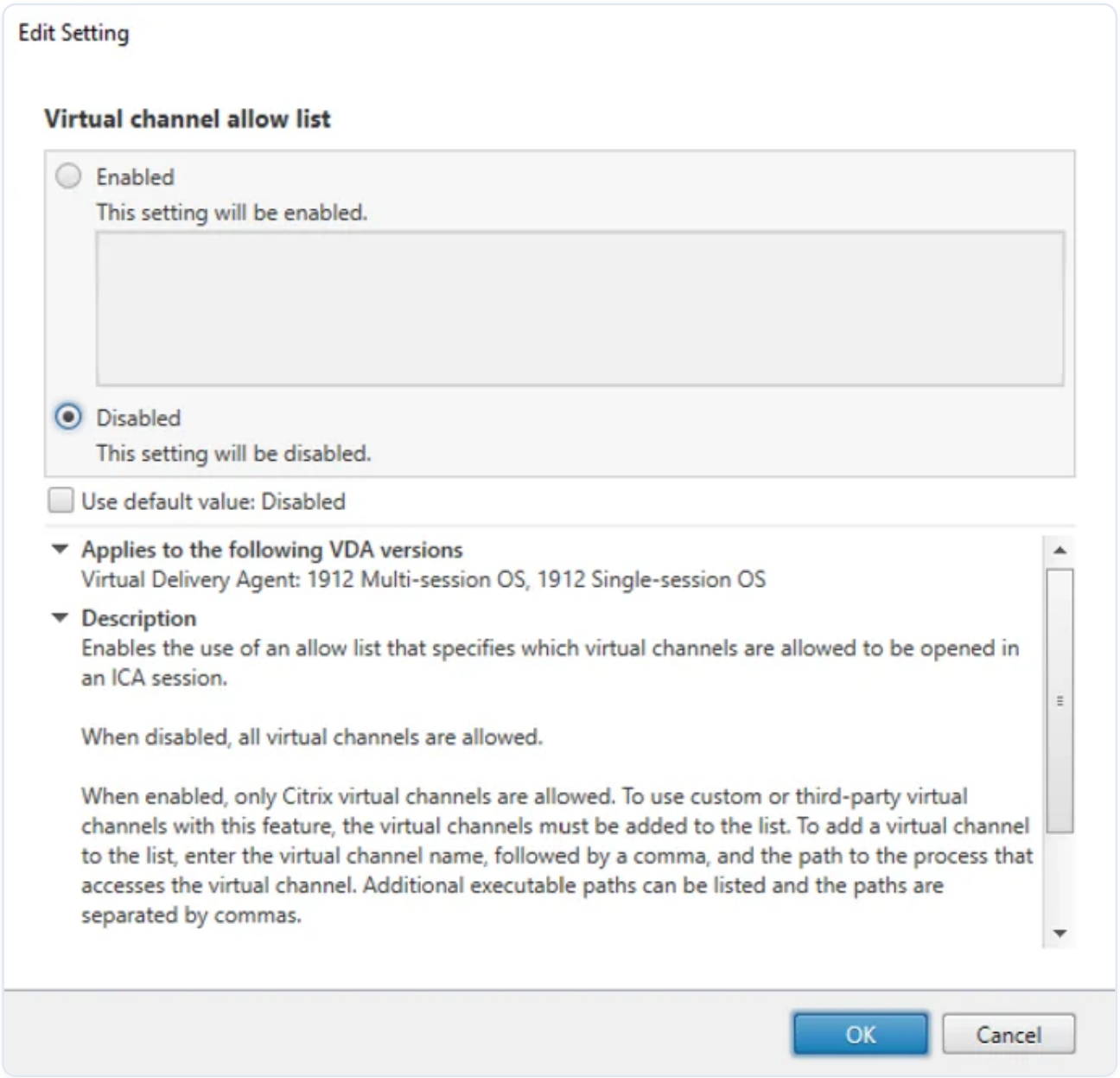
NOTE:

- If you use additional virtual channels for other functions, these need to be added explicitly as well.
- If you are using only deviceTRUST 2503 CR or later then you can remove the entry 'DEVTRST,C:\Program Files\deviceTRUST\Agent\Bin\dtagent.exe'.

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

Allowing all virtual channels

A fallback option would be to simply allow all virtual channels to be established. This will work from a technical perspective. It will however work around the security measures Citrix introduced with the 2109 release.



Virtual Channel Compatibility

The deviceTRUST Client Extension v2503 CR as part of Citrix Workspace app can be installed along-side the deviceTRUST Client Extension v23.1.

To support this side by side installation, it was necessary to rename the virtual channel. This results in the following compatibility scenarios:

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

- **When using the deviceTRUST Agent 23.1 or earlier**, communication will occur with the deviceTRUST Client Extension 23.1 or earlier. The deviceTRUST Client Extension 2503 CR is not supported.
- **When using the deviceTRUST Agent 2503 CR or later**, communication will be preferred with the deviceTRUST Client Extension 2503 CR or later. However when unavailable, communication will fall back to the deviceTRUST Client Extension 23.1 or earlier.

deviceTRUST debug log locations

To assist us in troubleshooting deviceTRUST related issues you may be required by support to collect debug log information from your environment. Below is a list of deviceTRUST log file locations for each component.

Microsoft Windows logs

For the deviceTRUST Client Extension, Agent and Console:

On Microsoft Windows, the deviceTRUST components log to an Event Tracing for Windows (.etl) file in the following location:

- C:\ProgramData\deviceTRUST\Diagnostics\Logs\deviceTRUST-Log-xx.etl

NOTE:

This file can be copied and provided to Support

Logging is enabled by default. Log files are cyclic and will overwrite when their max size is reached. It is therefore important that the log file is captured shortly after reproduction of an issue. The default etl log file size is 1GB.

Windows component installer logs

For the deviceTRUST Client Extension

The deviceTRUST Client Extension installer executable logs installation activity to `%AppData%\Local\Temp`:

- deviceTRUST_Client_Extension_v2503 CR_20250113094950.log
- deviceTRUST_Client_Extension_v2503 CR_20250113094950_dtclient_extension_x64.msi.log
- deviceTRUST_Client_Extension_v2503 CR_20250113094950_dtclient_extension_x86.msi.log

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

NOTE:

This file can be copied and provided to Support

For the deviceTRUST Agent and Console

When troubleshooting installation issues for the deviceTRUST Agent or Console, MSI logs can be generated with msiexec.

For example, from an elevated CMD prompt run the commands below to create an MSI log file capturing the install activity. The MSI and location information should be customised to your environment.

- `msiexec /i "dtagent-x64-release-2503 CR.410.0.msi" /l*v "C:\Temp\Agent.log"`
- `msiexec /i "dtconsole-x64-release-2503 CR.410.0.msi" /l*v "C:\Temp\Console.log"`

NOTE:

This file can be copied and provided to Support

deviceTRUST Windows Event Logs

For the deviceTRUST Agent

The Event logs are available on any computer where the Agent is installed. The event logs can be exported from Event Viewer.

Open Event Viewer as an admin user and browse

- Application and Services Logs > deviceTRUST > Admin
- Right Click on Admin and `Save All Events As`
- This will export the deviceTRUST Events to an .evtx file which can be provided to Support

Linux logs

For the deviceTRUST Client Extension

On Linux, the deviceTRUST client components log activity to the following location.

- /tmp/ctxdt.log

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

NOTE:

- This file can be copied and provided to Support
- On IGEL OS 12 deviceTRUST Client logging is disabled by default as requested by IGEL. If required logging can be enabled via the local Setup application or within the UMS.

Apple macOS logs

For the deviceTRUST Client Extension

On Apple macOS, the deviceTRUST client components log activity to the following location.

- /tmp/ctxdt.log

NOTE:

This file can be copied and provided to Support

Apple iOS logs

For the deviceTRUST Client Extension

On Apple iOS, the deviceTRUST client component logs can be shared from within the deviceTRUST App under `Settings > Diagnostics`:

- Share log files option - Allows the user to transmit deviceTRUST logs using Apple tools e.g Mail, Air Drop
- Send a support email option - If a Mail profile is configured on the iOS device, this option will auto construct an email for the user with the deviceTRUST log files attached. The user can fill out the email with their issue statement prior to sending.

Export of deviceTRUST policy configuration

For the deviceTRUST Console

The Policy configuration can exported from the 'Sharing' menu in deviceTRUST Console.

- Open the deviceTRUST Console > Sharing > Export to Disk.
- A save dialogue box will allow the user to save the .dtpol policy file to their preferred location.

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

- Example policy file '2025-01-17_10-33_deviceTRUST_Policy.dtpol'

NOTE:

The policy can be copied and provided to Support

Amazon WorkSpaces logging

When troubleshooting deviceTRUST Virtual Channel issues on Amazon WorkSpace, in conjunction with deviceTRUST debug log information we also require Level 3 logs to be enabled on the Amazon WorkSpace and for the connecting Amazon WorkSpace client.

The verbosity level of these logs are required to assist deviceTRUST in troubleshooting issues, this is the minimum log level expected by Amazon Support if an issue is referred.

To enable these logging options please see refer to the Amazon Documentation using the links below.

- Amazon Workspace Client Advanced options
- Amazon Workspace Advanced options

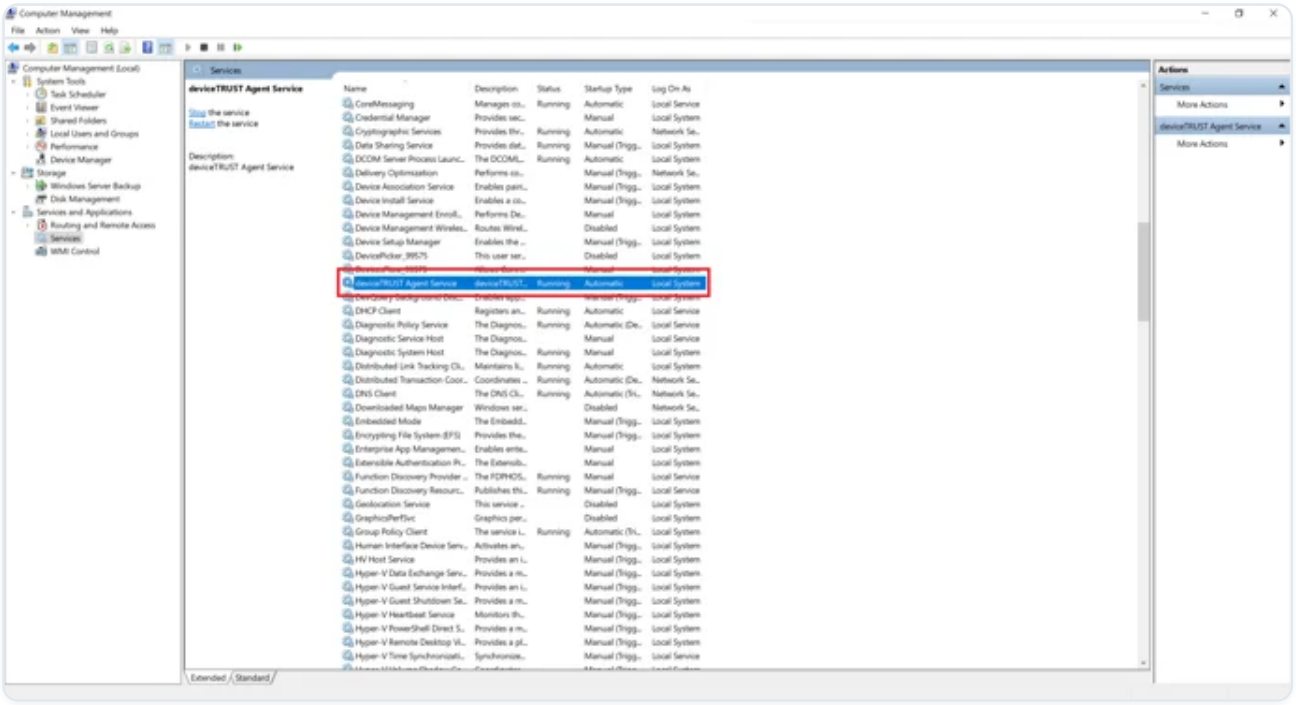
Check that the deviceTRUST Agent service is running

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.

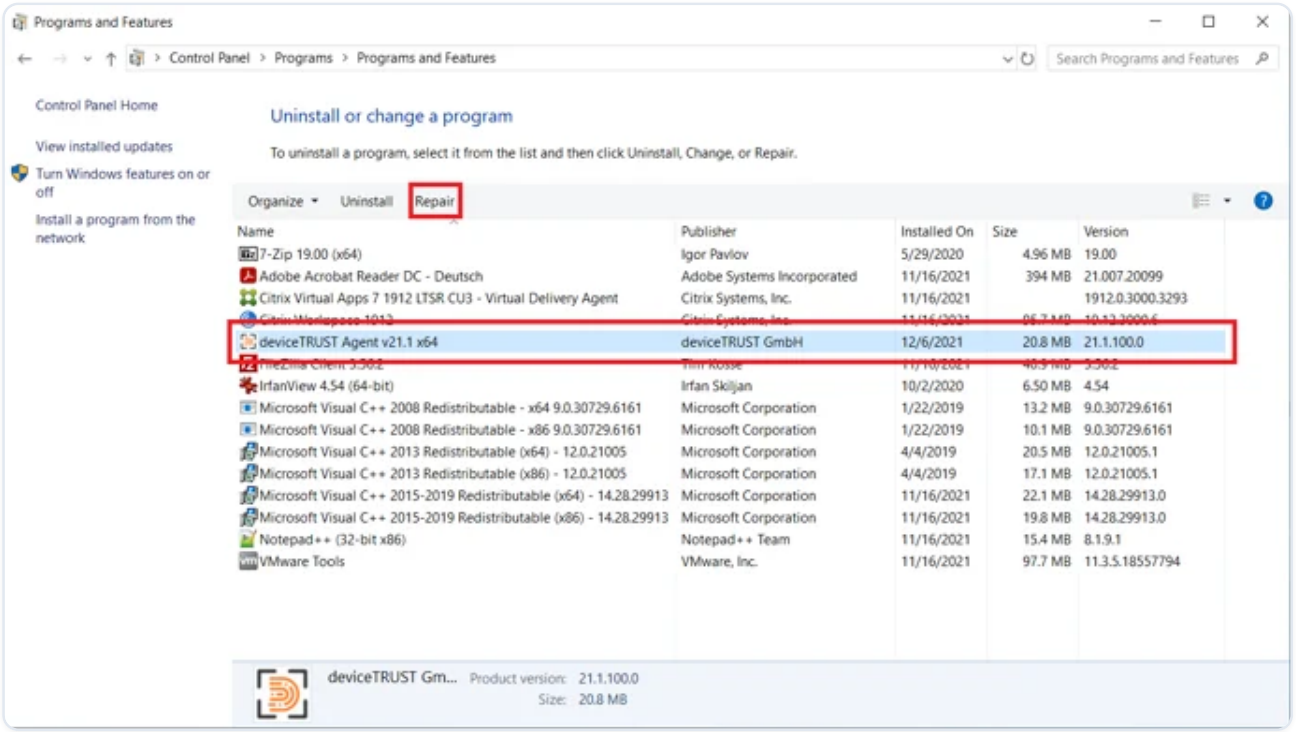
The deviceTRUST Agent service is monitored by standard operating system functions and recovered if necessary.

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.



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".

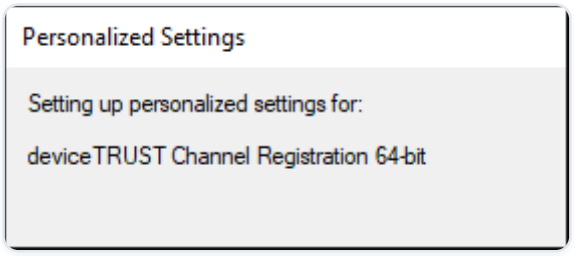
Neither the module.ini or the files on disk are monitored for incorrect values. To repair, perform an uninstall and reinstall of the installation.

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\
{f758f573-8e78-4539-97f8-5d5cc3537d7b}
```

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\{72971d25-6eb7-4b21-bfc0-a716f89f3765} (on a 64-bit OS)

HKLM\Software\Microsoft\Active Setup\Installed
Components\{72971d25-6eb7-4b21-bfc0-a716f89f3765} (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.

deviceTRUST Citrix Cleanup 32-bit component

Registry Key:

```
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\
{f3252a49-fd7e-4067-96e1-02987531fb41}
```

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

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`

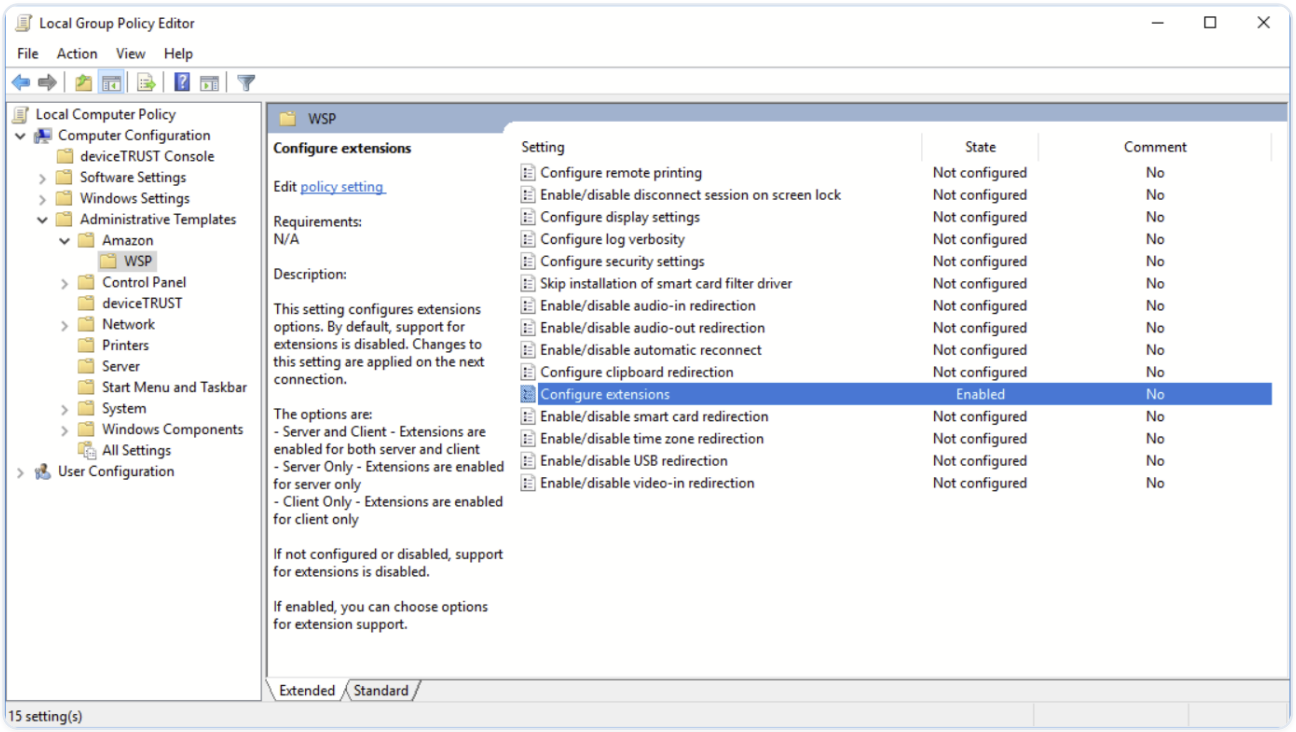
If however you are using a Central Store, then the following files need to be copied to the Central Store:

- 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`

Configuring DCV Extensions

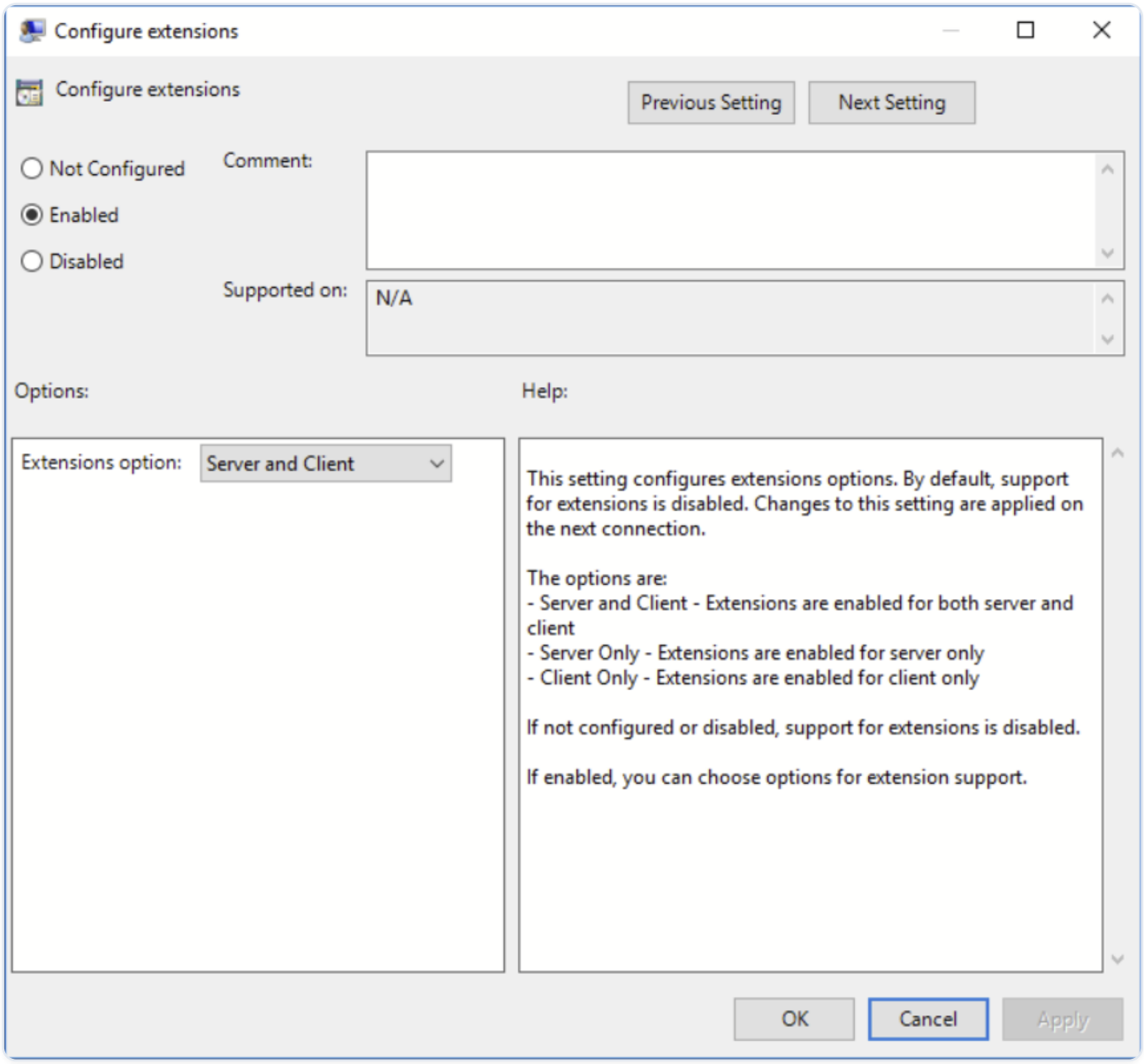
Within the policy editor of your choice, navigate to Administrative Templates -> Amazon -> WSP and enable the Configure extensions setting:

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



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

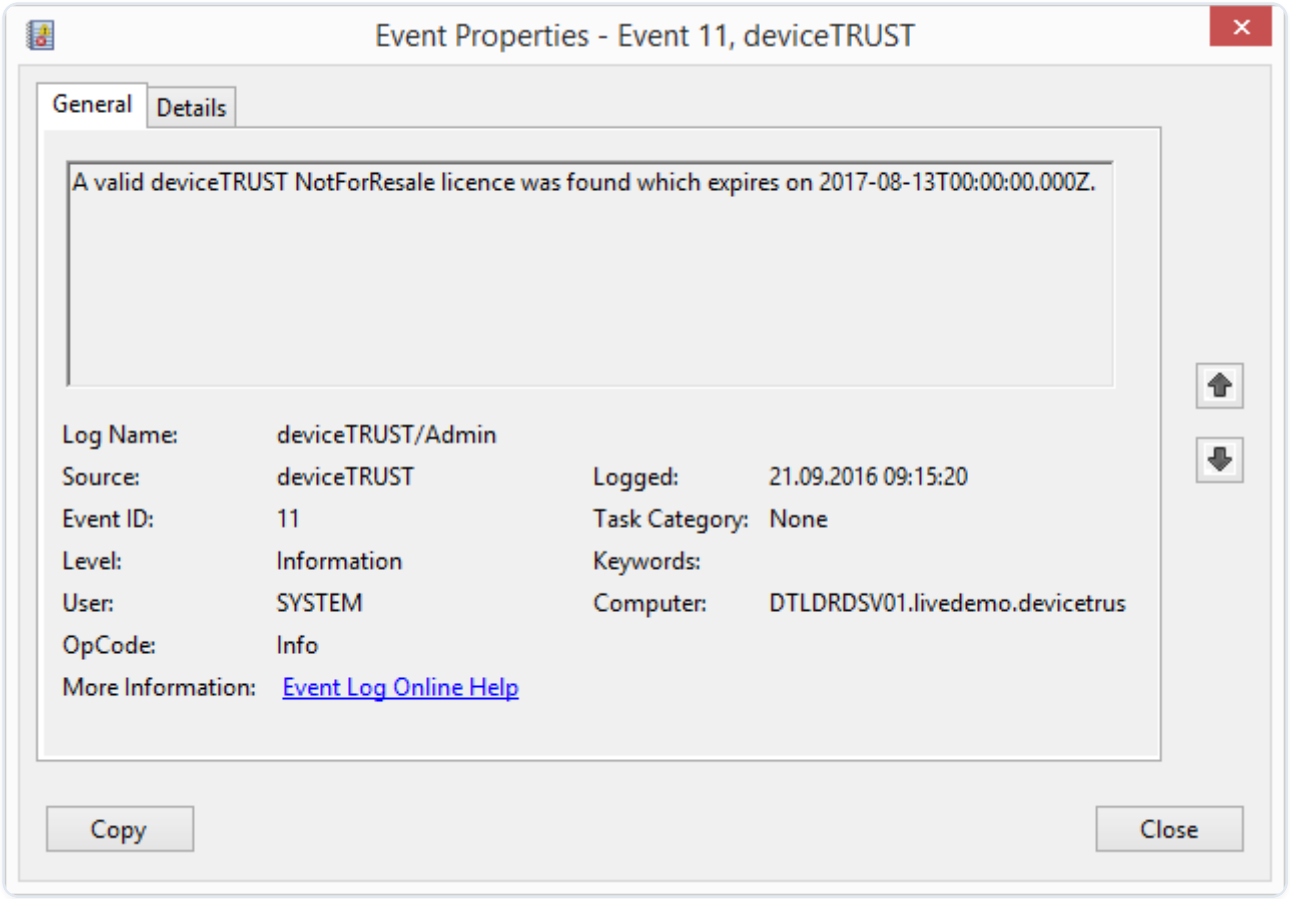
If your deviceTRUST License has not been configured, or has expired, then you may find that the deviceTRUST functionality is disabled.

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

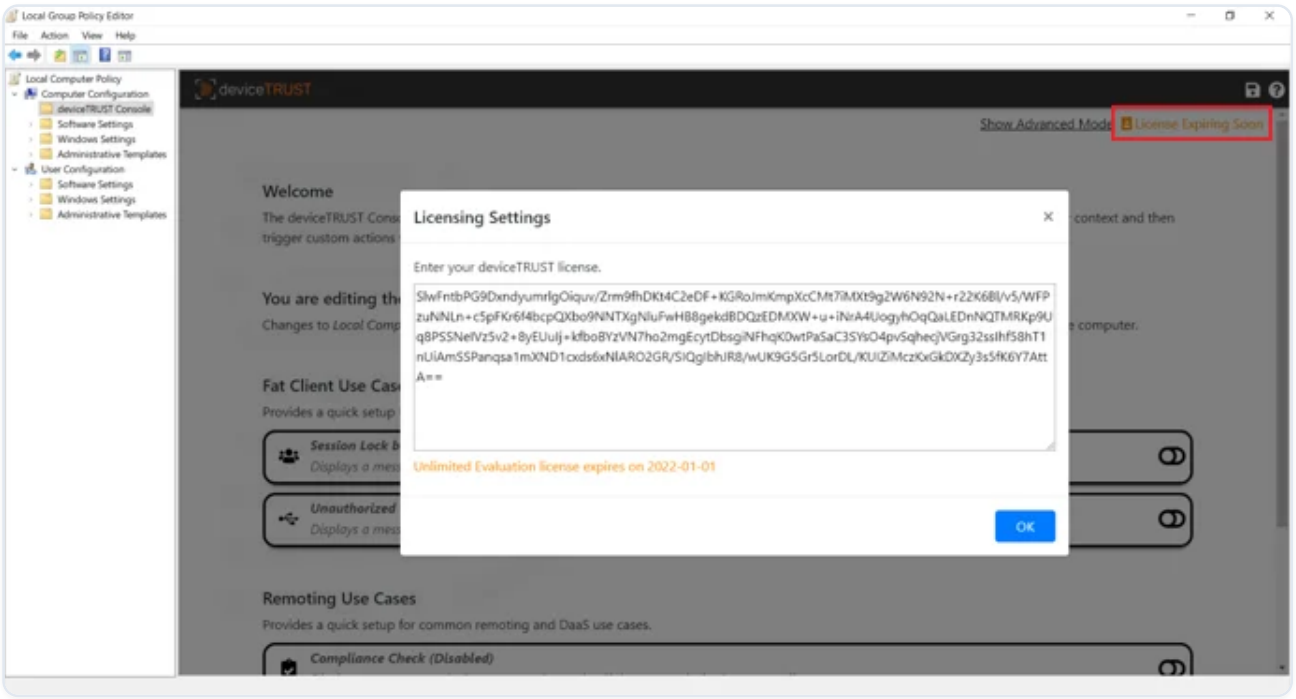


If your Windows Event Log reports a licensing event other that Event ID 11, then you should check your license.

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

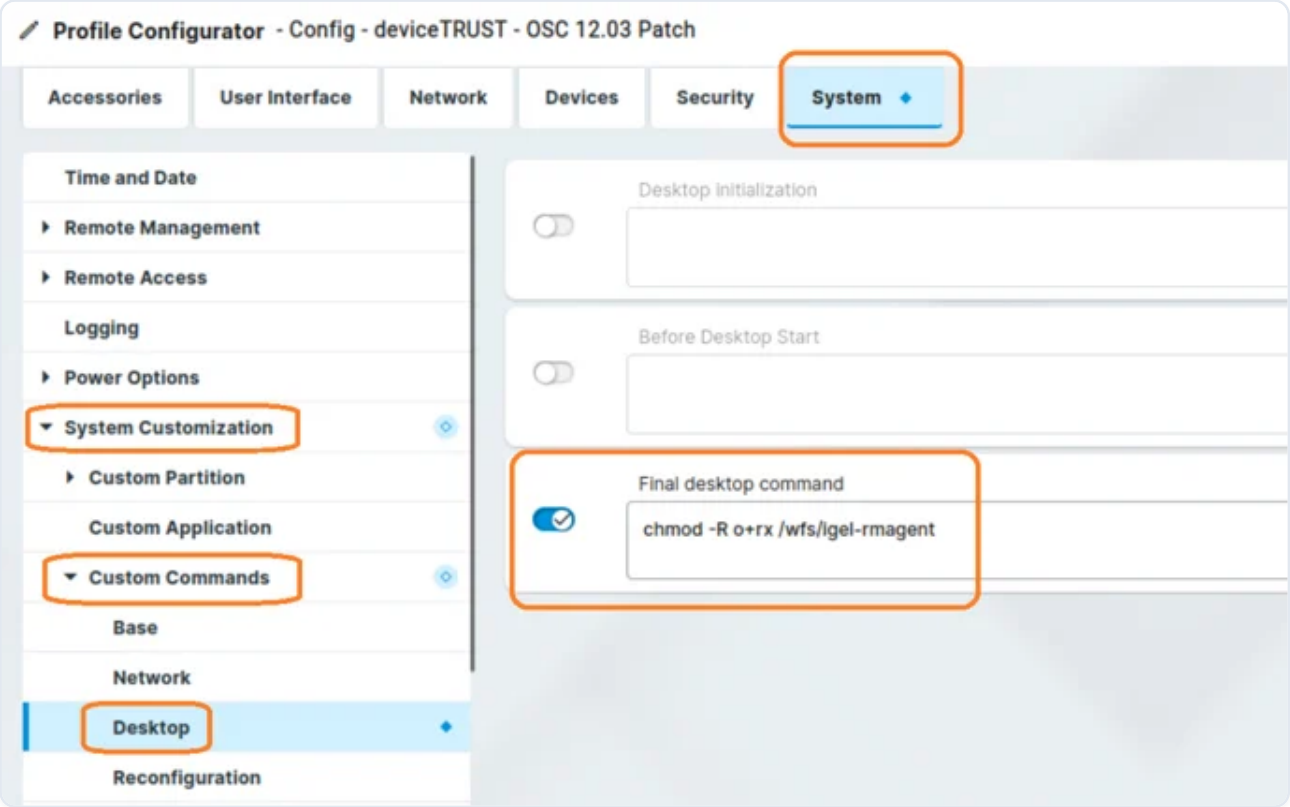
IGEL OS 12, created with OSC 12.03 and younger, does not provide IGEL-specific properties in deviceTRUST. Here's why and how to fix.

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.

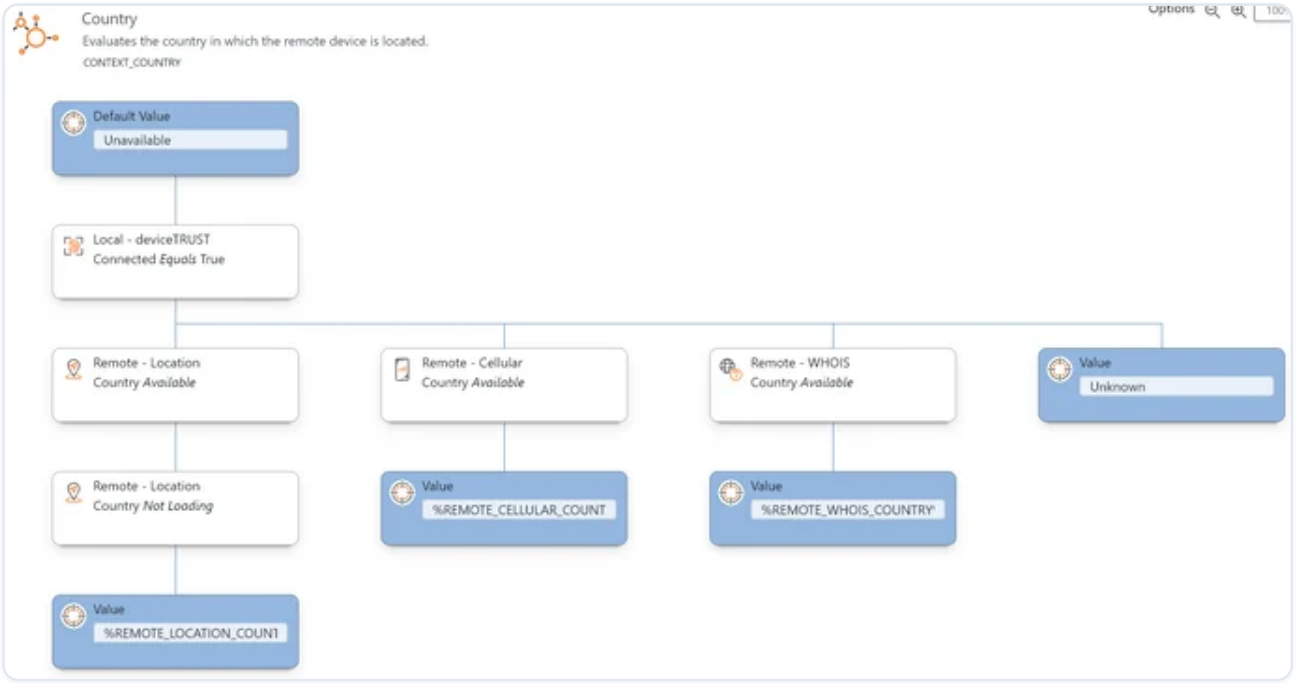
deviceTRUST Policy

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.

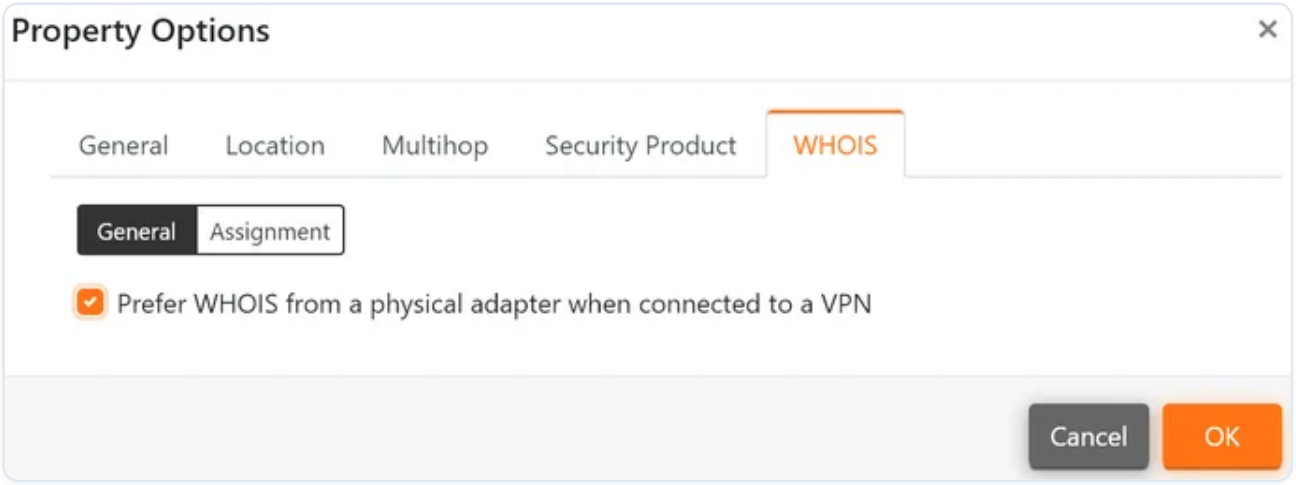
This example configuration is designed to

- 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 at.

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.

- 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

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

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

System > Registry sessions > wvd0 > plugins >deviceTRUST

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 at `https://docs.devicetrust.com/docs/21.1/architecture/supported_technologies` for more information.

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!

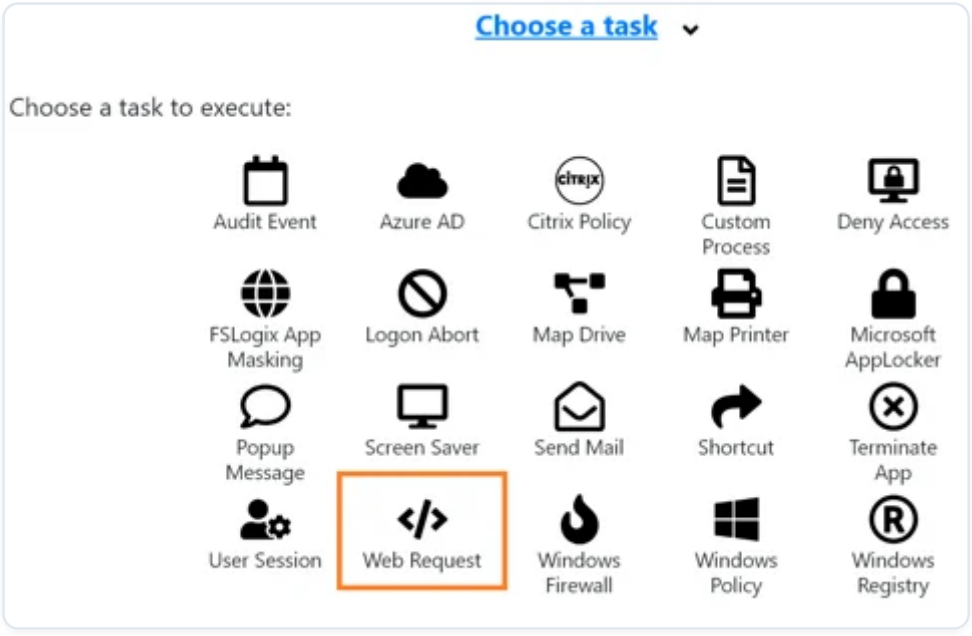
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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!

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.

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",
```

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

```
    "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%"

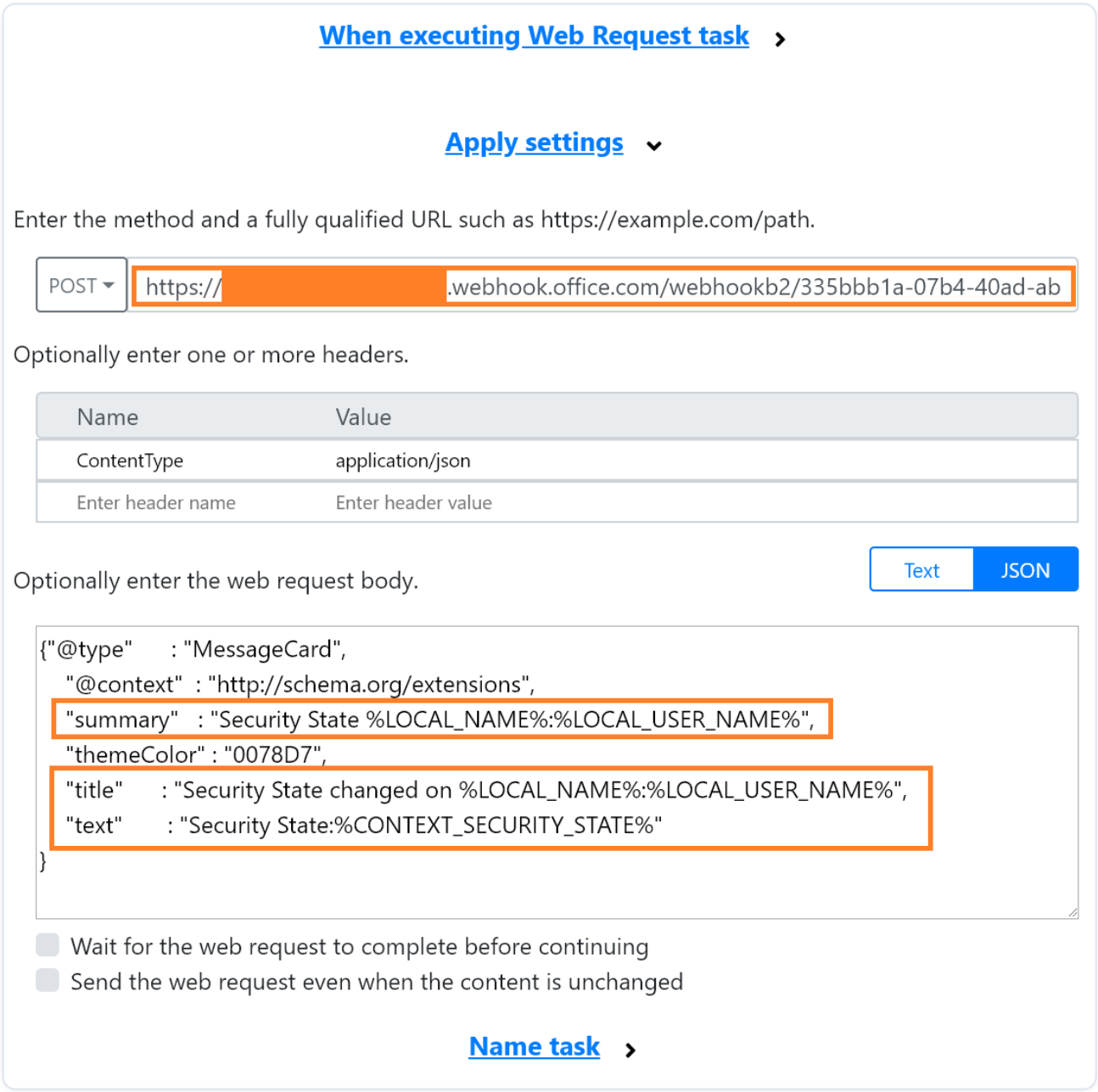
}
```

NOTE:

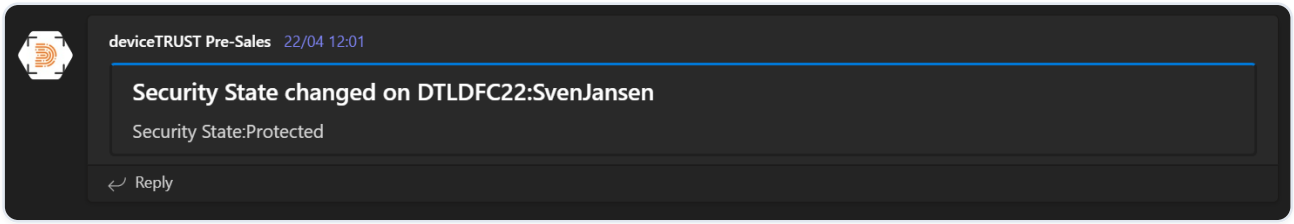
This configuration uses the variable %LOCAL_NAME%, %LOCAL_USER_NAME% and %CONTEXT_SECURITY_STATE%, which are to be seen exemplarily. Edit as required.

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

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



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.

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

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.

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

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

- 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.

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				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.

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				Agent Service loaded new policies.
4	Policy Load Failed	Error	Policy Loaded)	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 (30 days). The license is read on service startup, and any time a new license is deployed by Group Policy.
12	License Expires Soon	Warning	License)	The license is valid, but it expires within the expiry threshold (30 days). The software will stop functioning once the expiry date is reached.
14	License Expired	Error	License)	The license is valid, but has expired. The

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				software will no longer function.
16	License Invalid	Error	License Invalid)	The license contains invalid data.
17	Unmanaged User Logon	Information	Unmanaged User Logon)	An unmanaged user logged on.
18	License Not Found	Information	License)	The license could not be found. Citrix virtual sessions will be automatically licensed when deviceTRUST policy is applied.
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.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
104	Disconnect	Information	Session)	A user which previously successfully logged onto a session was 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.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
112	Trusted Device Blocked	Warning	Trusted Device)	A trusted device, i.e. a device with the deviceTRUST Client Extension installed, was 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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				the process either timed out or reported an error.
301	Access Allowed	Information	Access Allowed)	Access to the shell was allowed after a 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

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

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				in one or more errors.
325	AppLocker PowerShell Allowed	Information	AppLocker PowerShell)	A PowerShell Script or Cmdlet was allowed to execute.
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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				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.
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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				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.
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.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
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.
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.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
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.
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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	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.
	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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			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 the policy was saved.
Policy Load Failed (extends Policy Loaded)	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	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.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	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.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			CONTEXT1=VALUE 1\nCONTEXT2=VAL UE2\n
	Errors (14)	TEXT	A description of any errors that occurred whilst obtaining properties.
	Timings (15)	TEXT	Lists the five local and remote property 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 (extends Session)	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=VALU E1\nPROPERTY2=V ALUE2\n
	RemovedProperties (10)	TEXT	A textual representation of all properties that were

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			removed. The properties are formatted with the name of each property, with multiple properties separated by a newline (\n) character. E.g. 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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
Context Changed (extends Session)	ChangedContexts (9)	TEXT	A textual representation of all 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\n

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			CONTEXT_TWO=PREVIOUSVALUE2\n
	TriggeredBy (11)	TEXT	The name of the property that changed that ultimately caused the context to change.
	Trigger (12)	TEXT	The name of the trigger that generated the context change event.
Untrusted Device Blocked (extends Session)	ClientName (9)	TEXT	The Operating System reported name of the connecting device.
Trusted Device (extends Session)	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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			the underlying protocol.
Trusted Device Auto Update (extends Trusted Device)	AutoUpdateUrls (13)	TEXT	The auto-update URLS that were used to upgrade the deviceTRUST Client Extension.
Trusted Device Auto Update Failed (extends Trusted Device Auto Update)	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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			Custom Process task is located.
	TaskName (14)	TEXT	The name of the Custom Process task.
	CommandLine (15)	TEXT	The command line that was executed.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
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 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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Timeout (11)	INT	The timeout period that the user would have had before being disconnected from the session, if the call to dtcmd.exe 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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	ReportDeviceName (13)	TEXT	The name of the remote device that the user was connecting from.
	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,

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			Dll, Installer, Script or Package.
	Duration (12)	INT	The time taken for the AppLocker rule to become effective.
	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'.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Message (2)	TEXT	A description of the changes that were made.
	Duration (3)	INT	The time taken for the AppLocker Policy 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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Applications (11)	TEXT	A comma separated list of all processes and their PID’s that were terminated.
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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Registry Warning (extends Registry Updated)	Warnings (12)	TEXT	The warning messages generated by the update.
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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Subject (11)	TEXT	The subject of the mail message.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Duration (12)	INT	The time in milliseconds taken to perform the web request.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	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.
	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.

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

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 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.

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

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 to populate the REMOTE_HARDWARE_BIOS_SERIAL property.	`$DEVICE_SN$`
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.

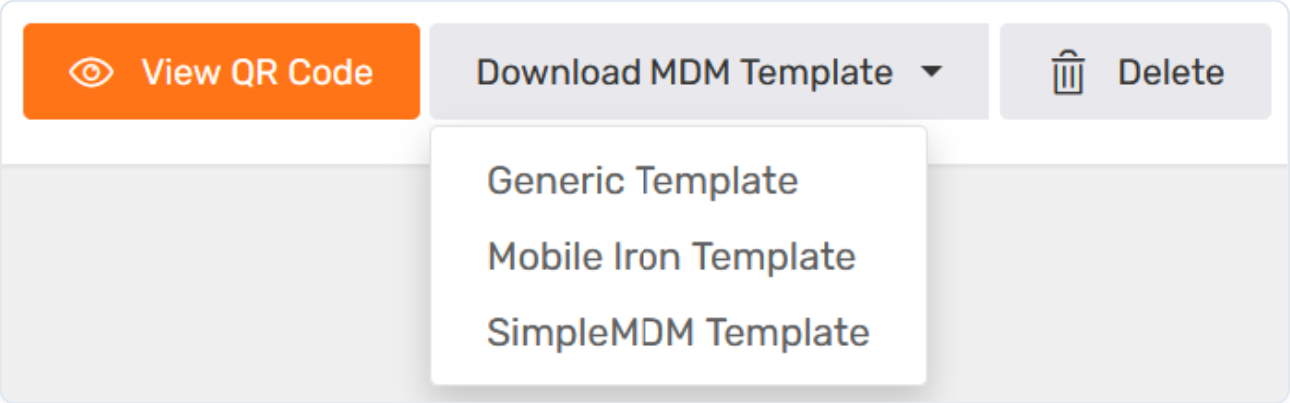
NOTE:

- Each MDM provider includes it's 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

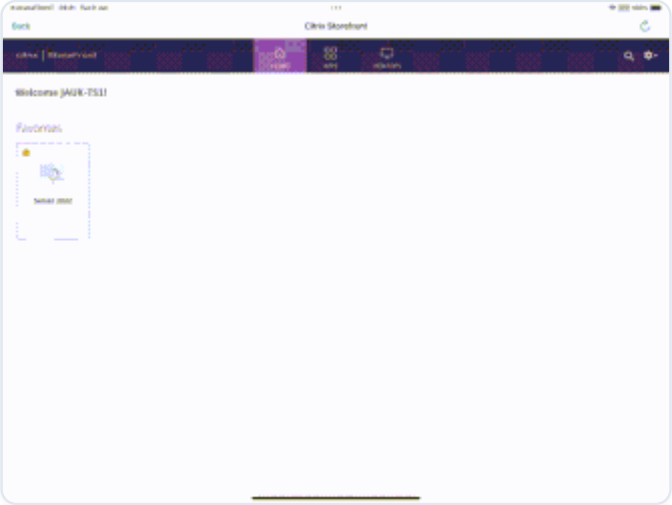
An MDM Template *plist* file can be downloaded from the deviceTRUST Portal within the *App Registration* section. This file contains all of the fields above, and can be edited with values suitable for your environment before uploading to your MDM provider.

© 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

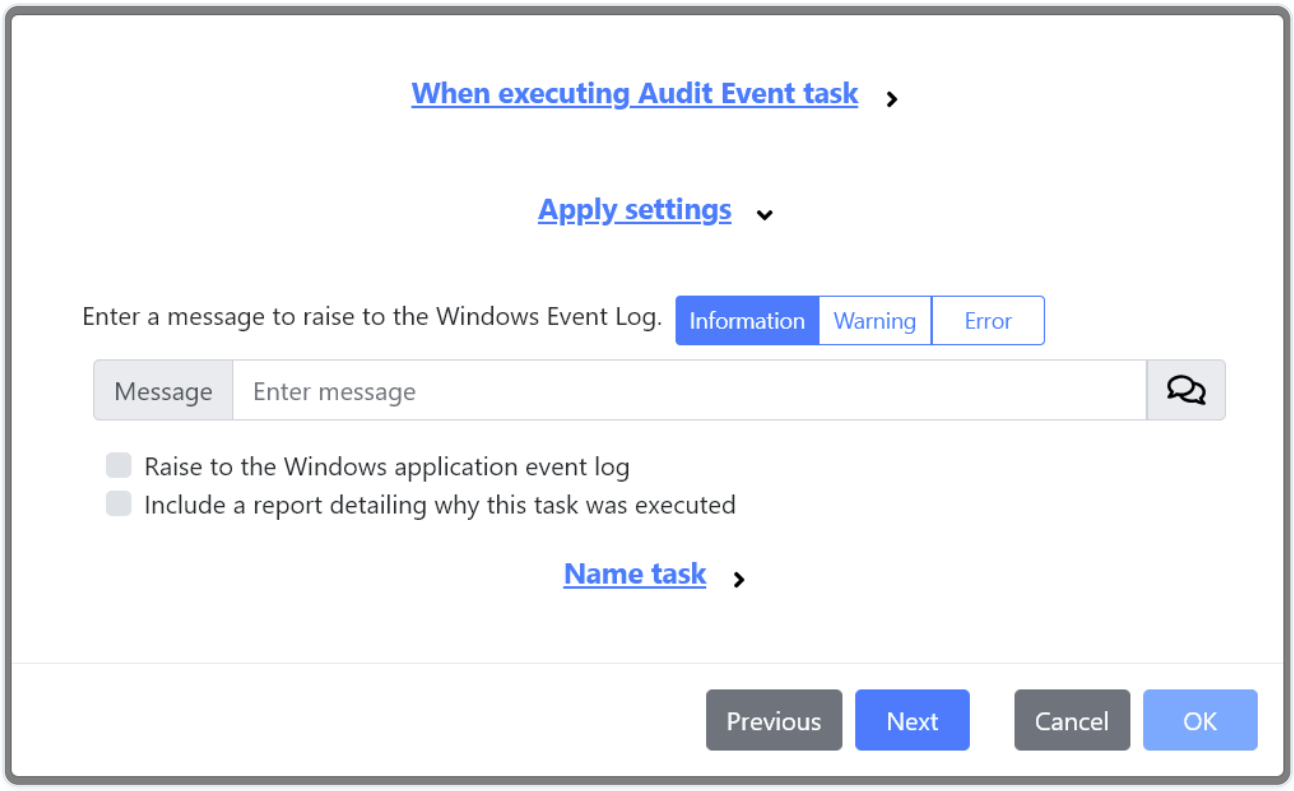
TABLE OF CONTENTS

- Tasks - Task Reference

Audit Event Task

The `Audit Event` task raises an Information, Warning or Error event to the Windows Event Log.

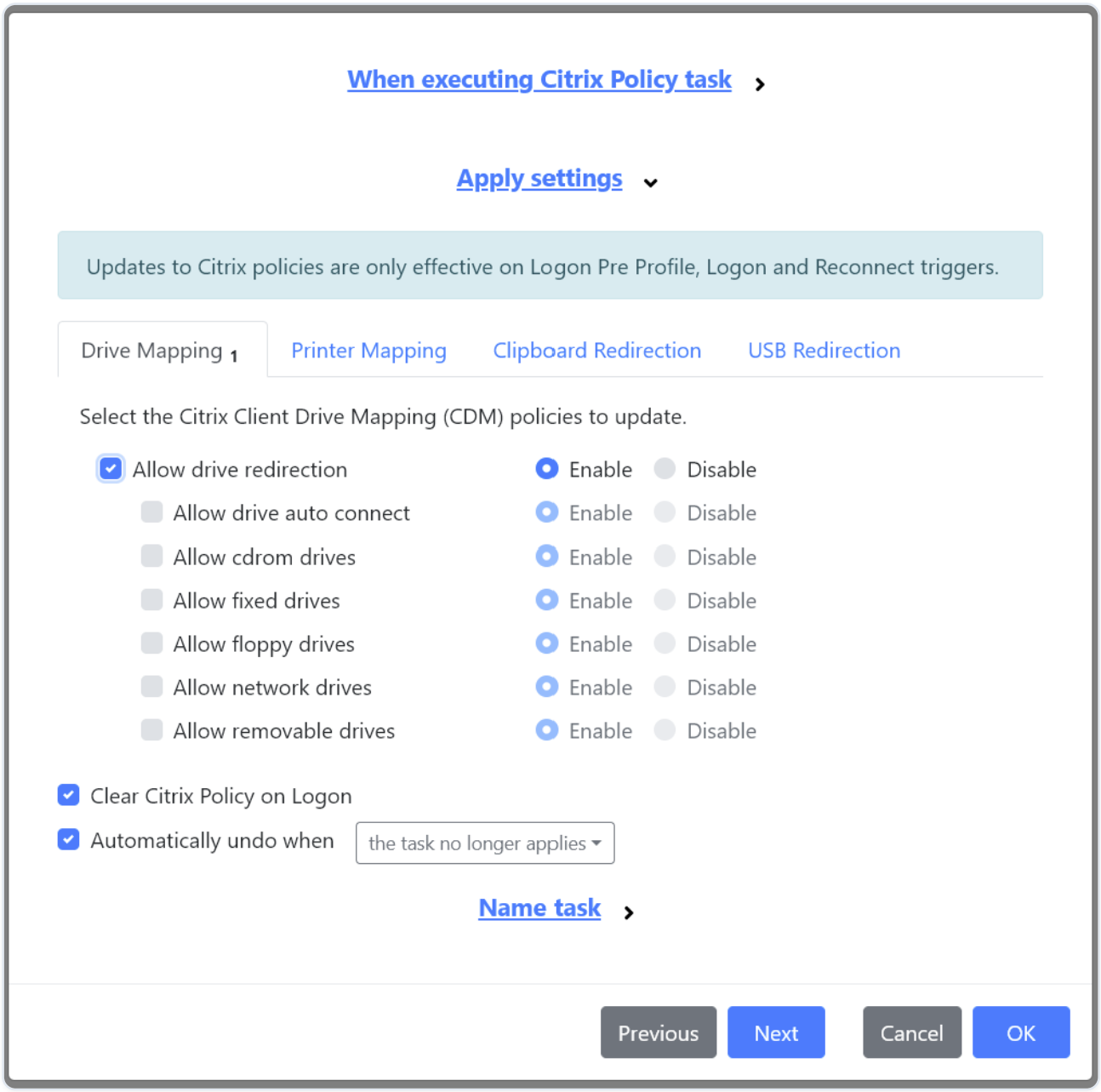
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



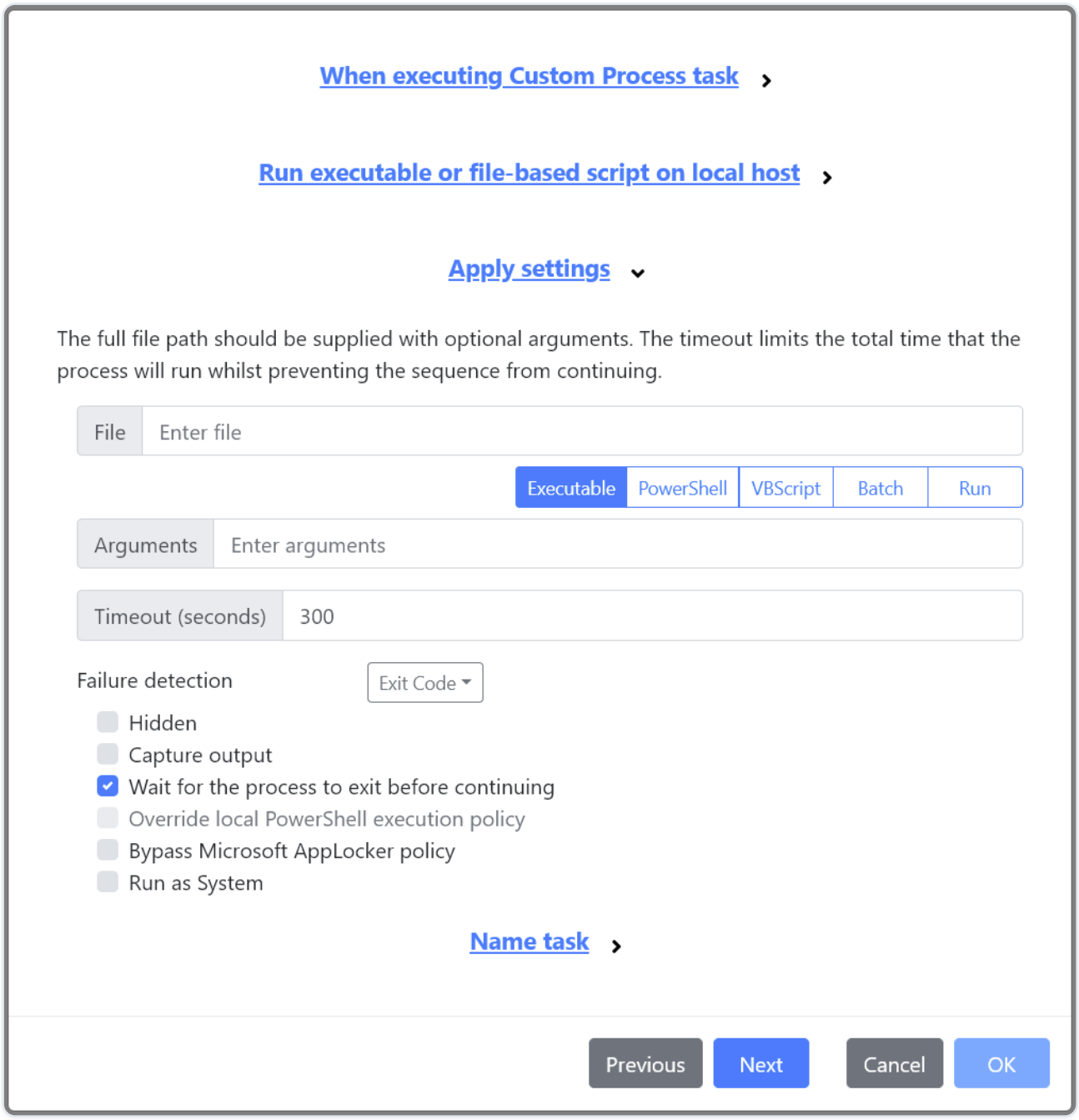
The following controls are available:

- *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.

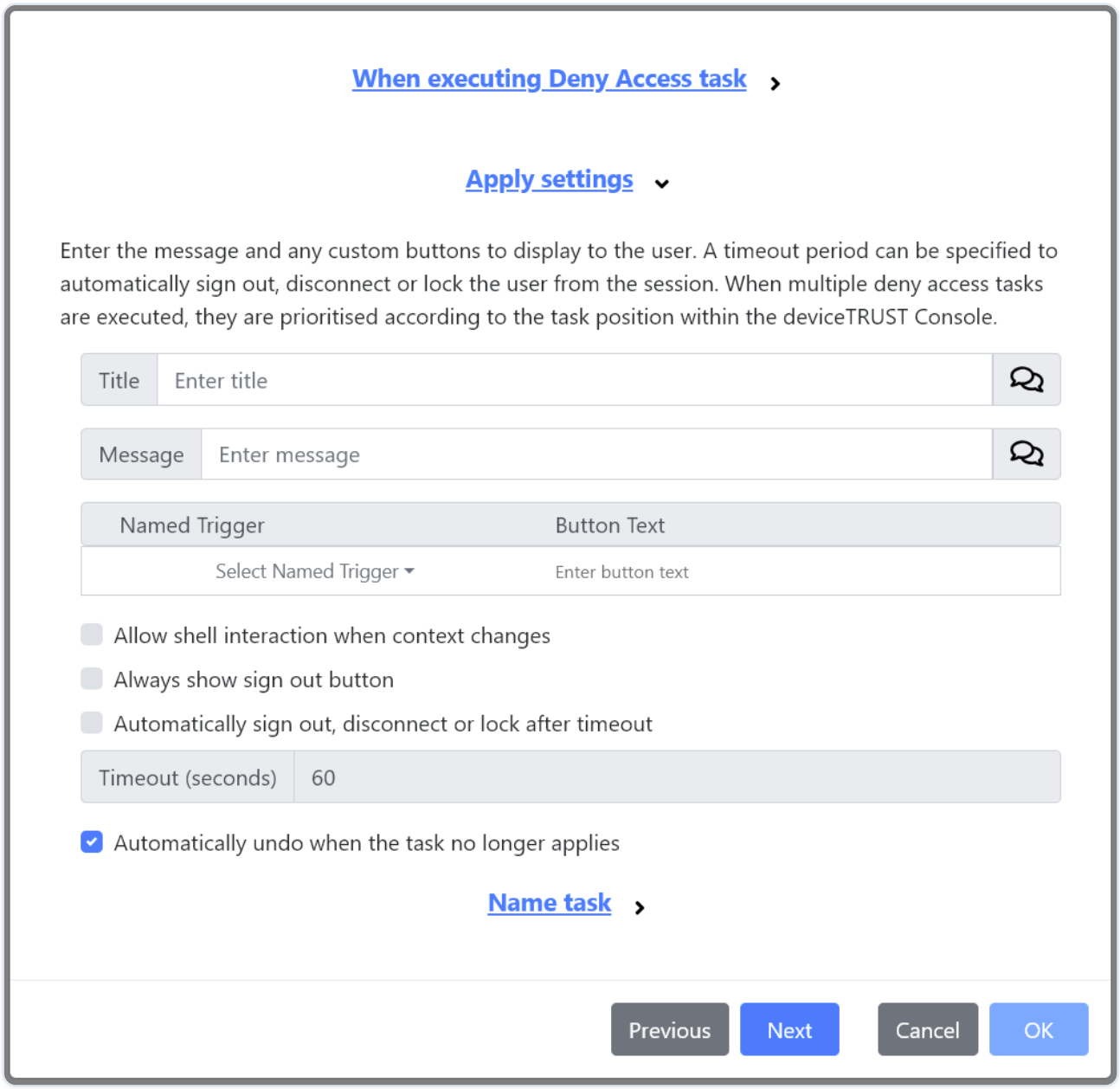
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

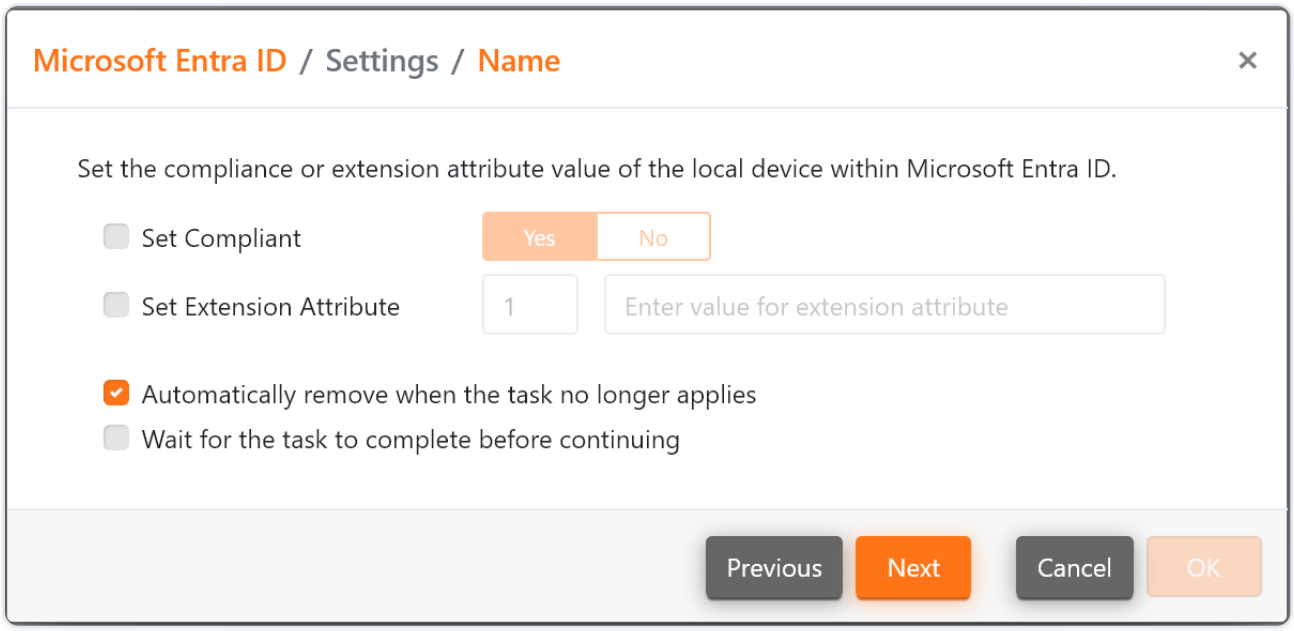
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Entra ID Task

The `Microsoft Entra ID` task updates domain joined device compliance or extension attribute value within Microsoft Entra ID.

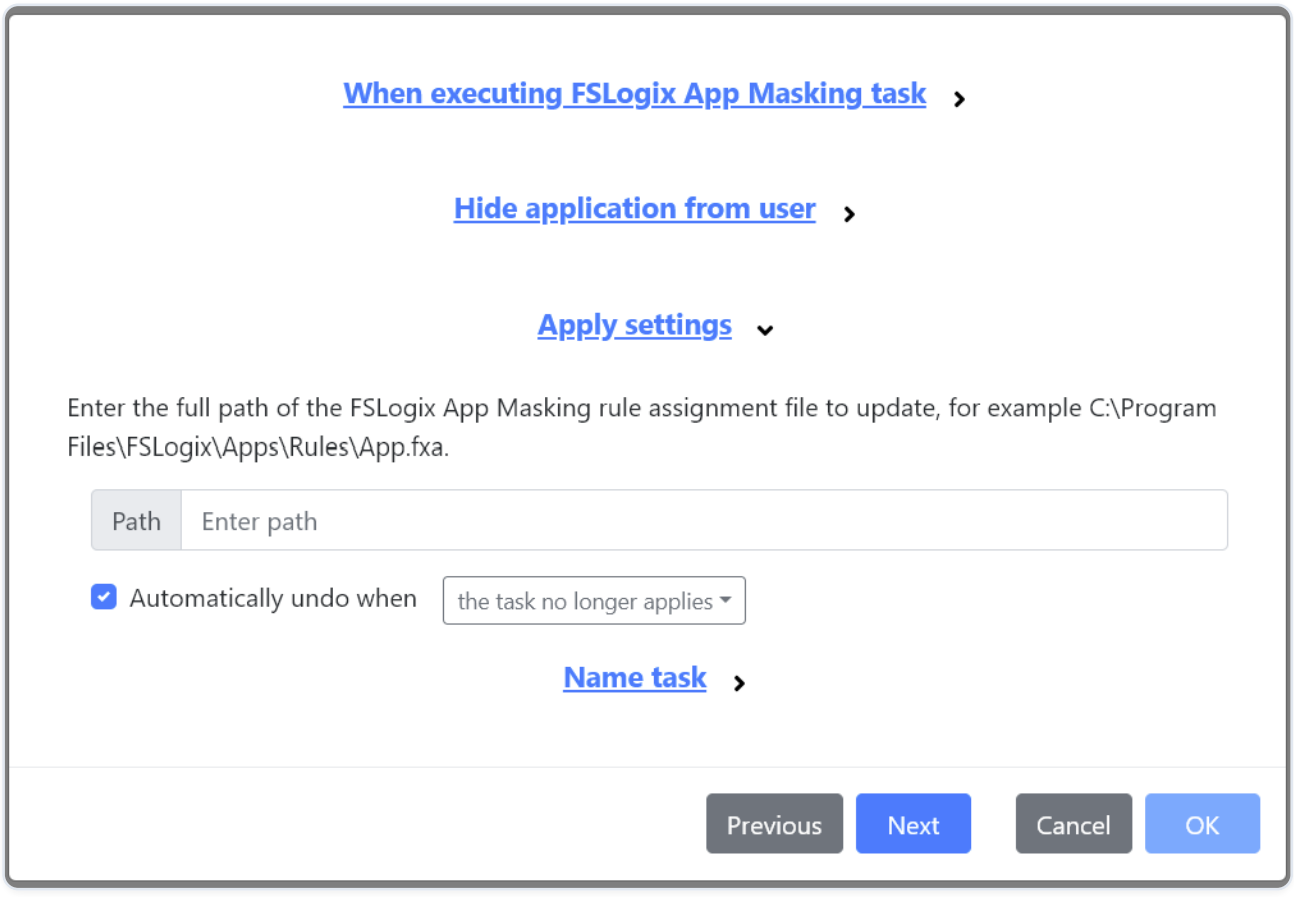
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

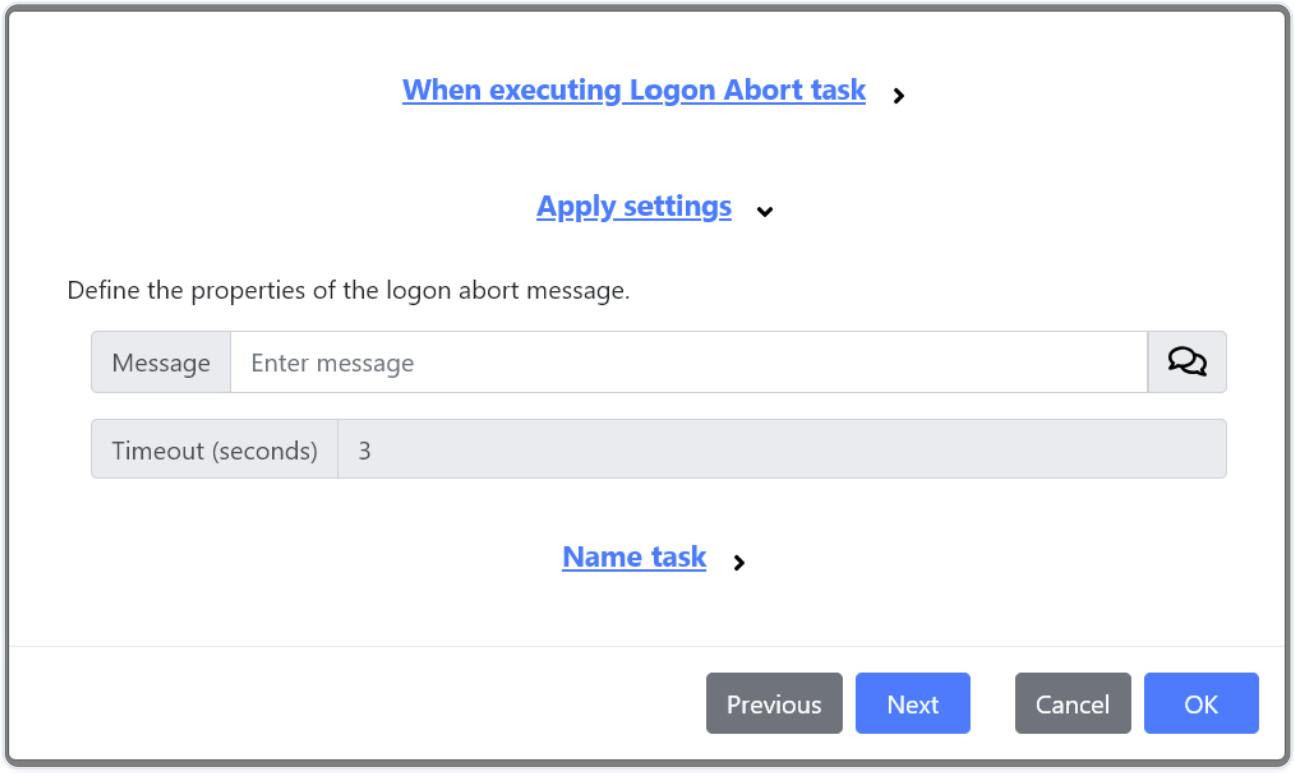
TABLE OF CONTENTS

- 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

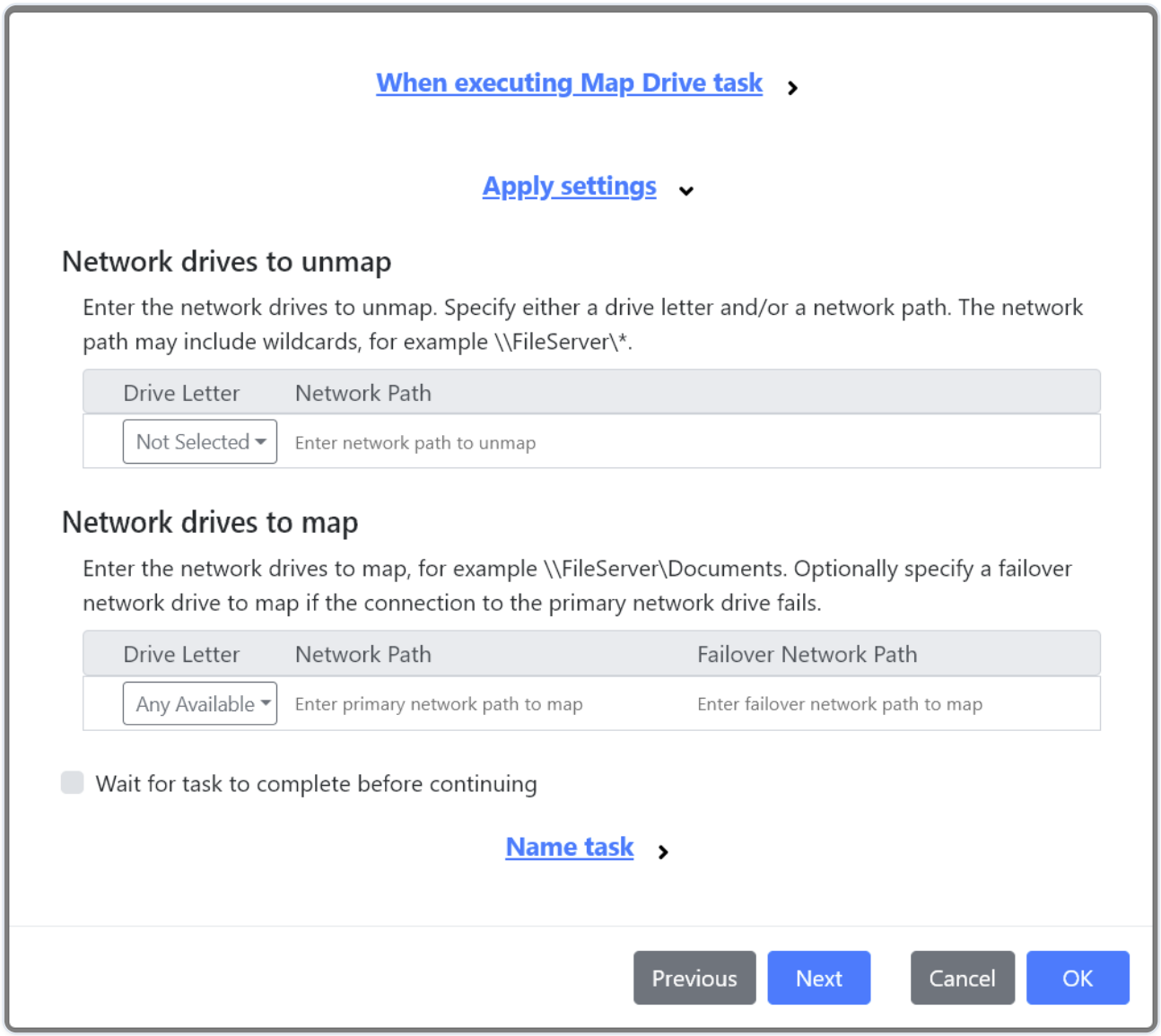
The `Logon Abort` task aborts the logon process, preventing the creation of the user session. When run as part of a Logon Pre Profile trigger, ensures that the user policy is not created. A message is displayed to the user briefly before reverting to an Operating System dependent access denied screen.



Map Drive Task

The `Map Drive` task maps and unmaps network drives within the user session.

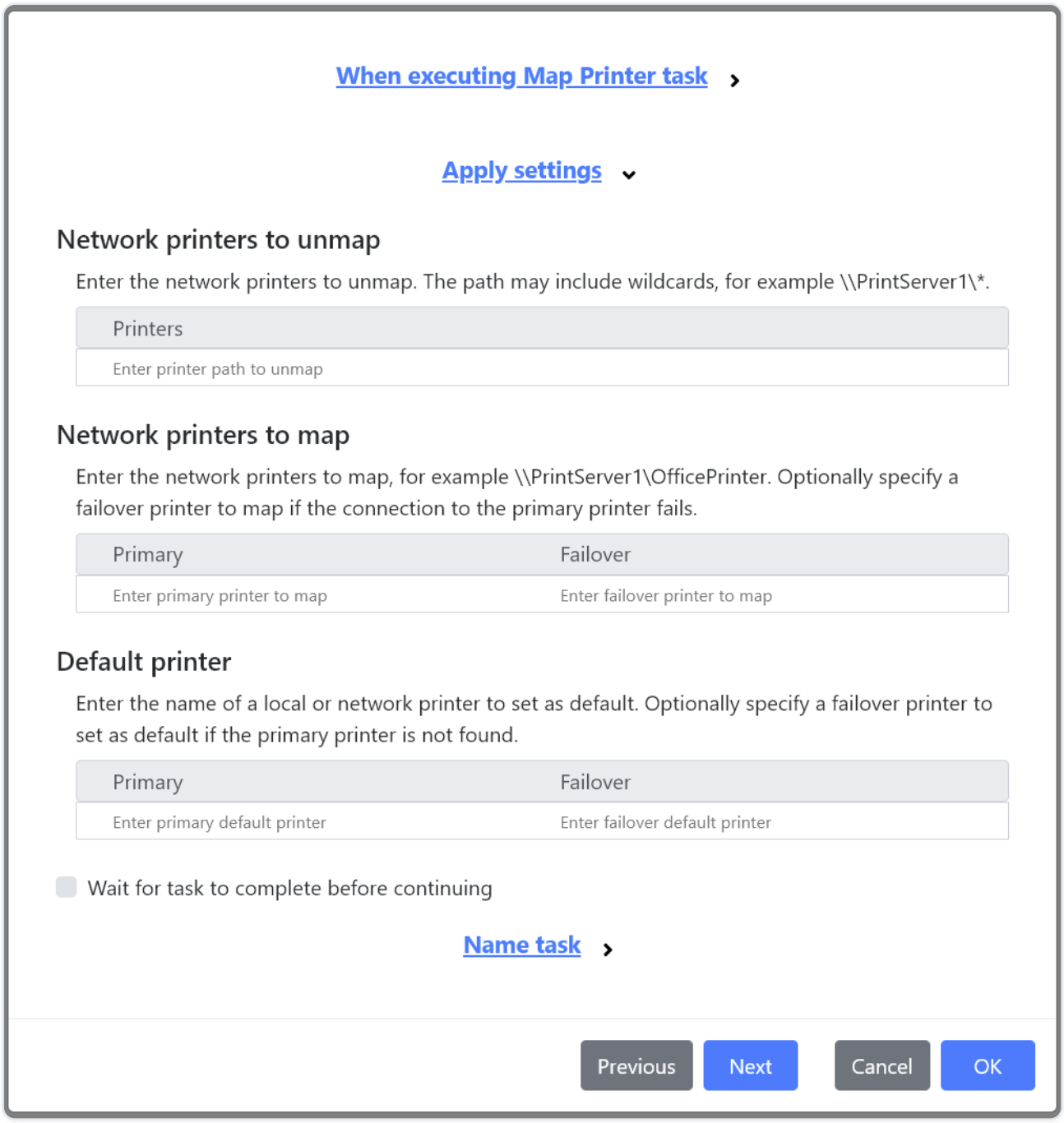
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Printer Task

The `Map Printer` task maps and unmaps network printers within the user session, and sets the default printer.

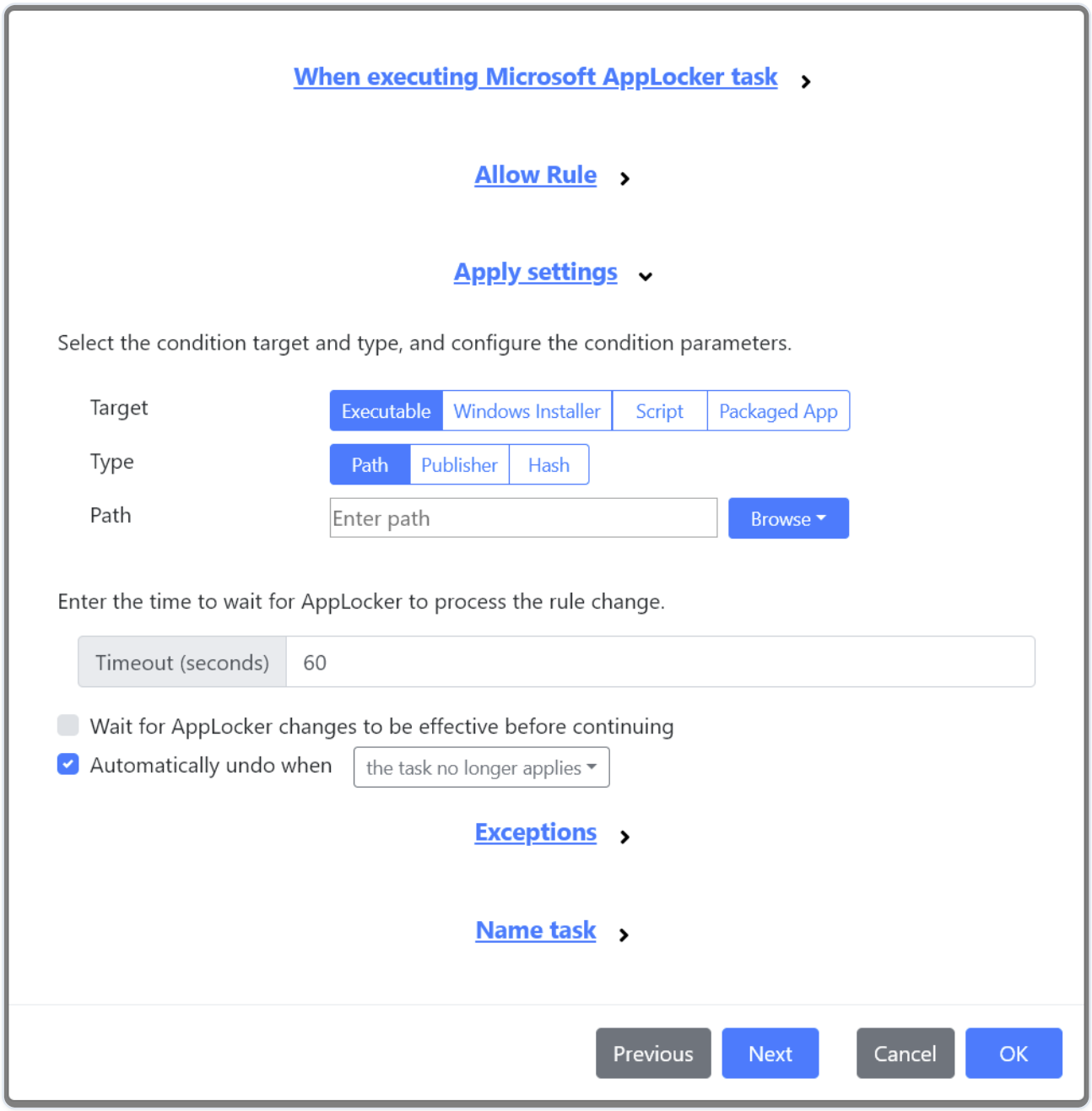
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

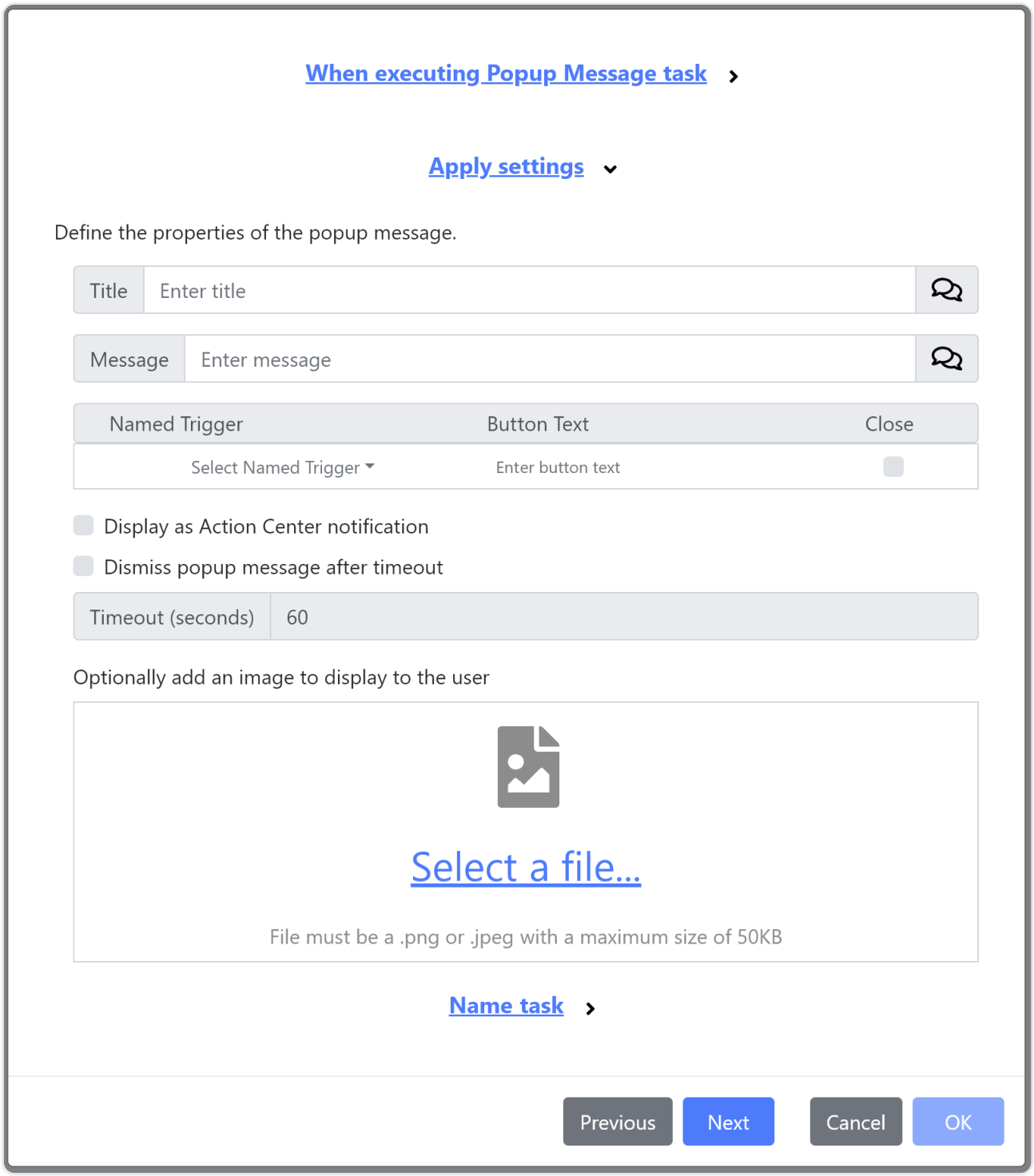
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

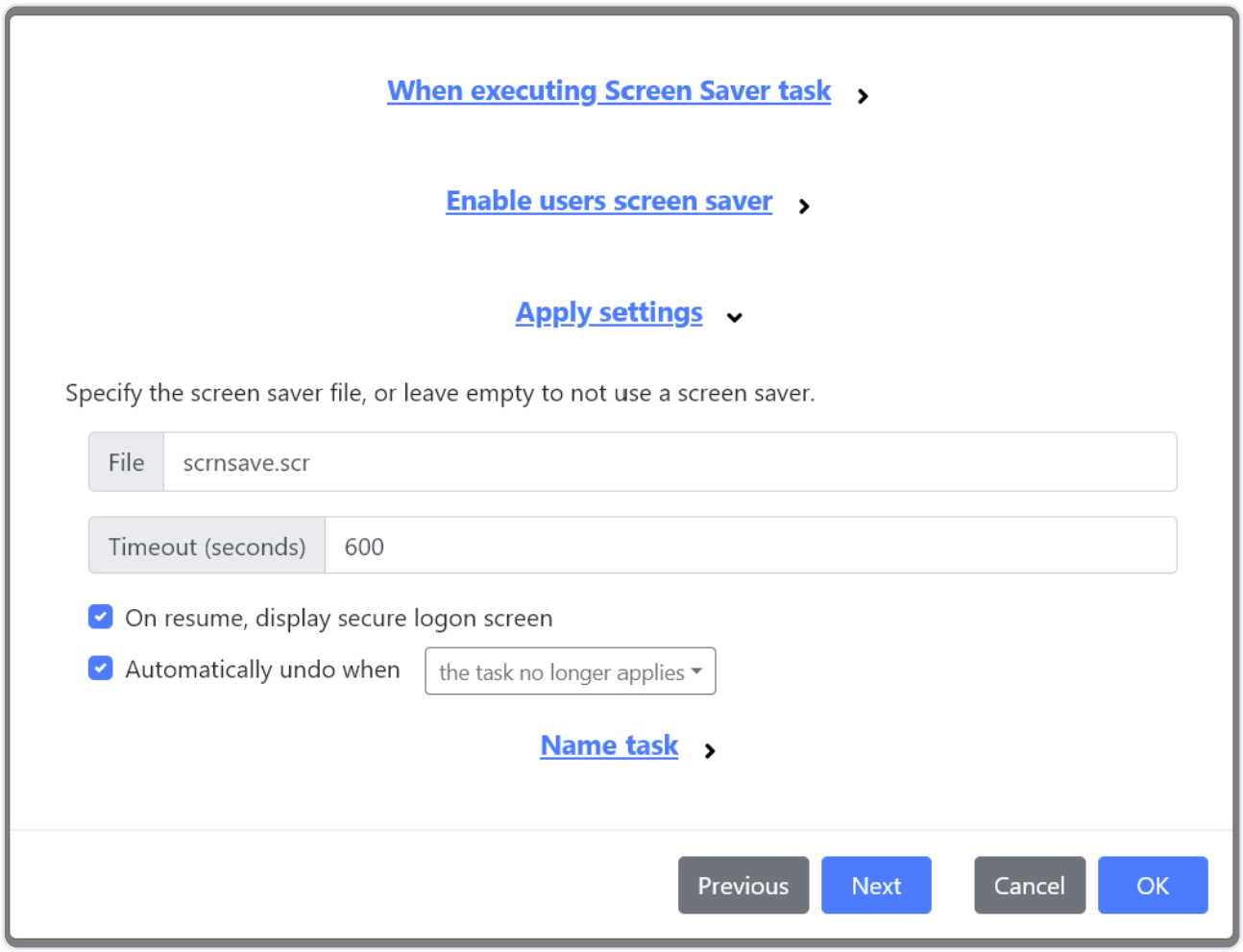
- *Title* - The title of the message displayed to the user.
- *Message* - The message displayed to the user.
- *Buttons* - Optionally, one or more additional buttons to add to the popup:
  - *Named Trigger* - The name of a named trigger to execute when the user clicks the button.
  - *Button Text* - 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

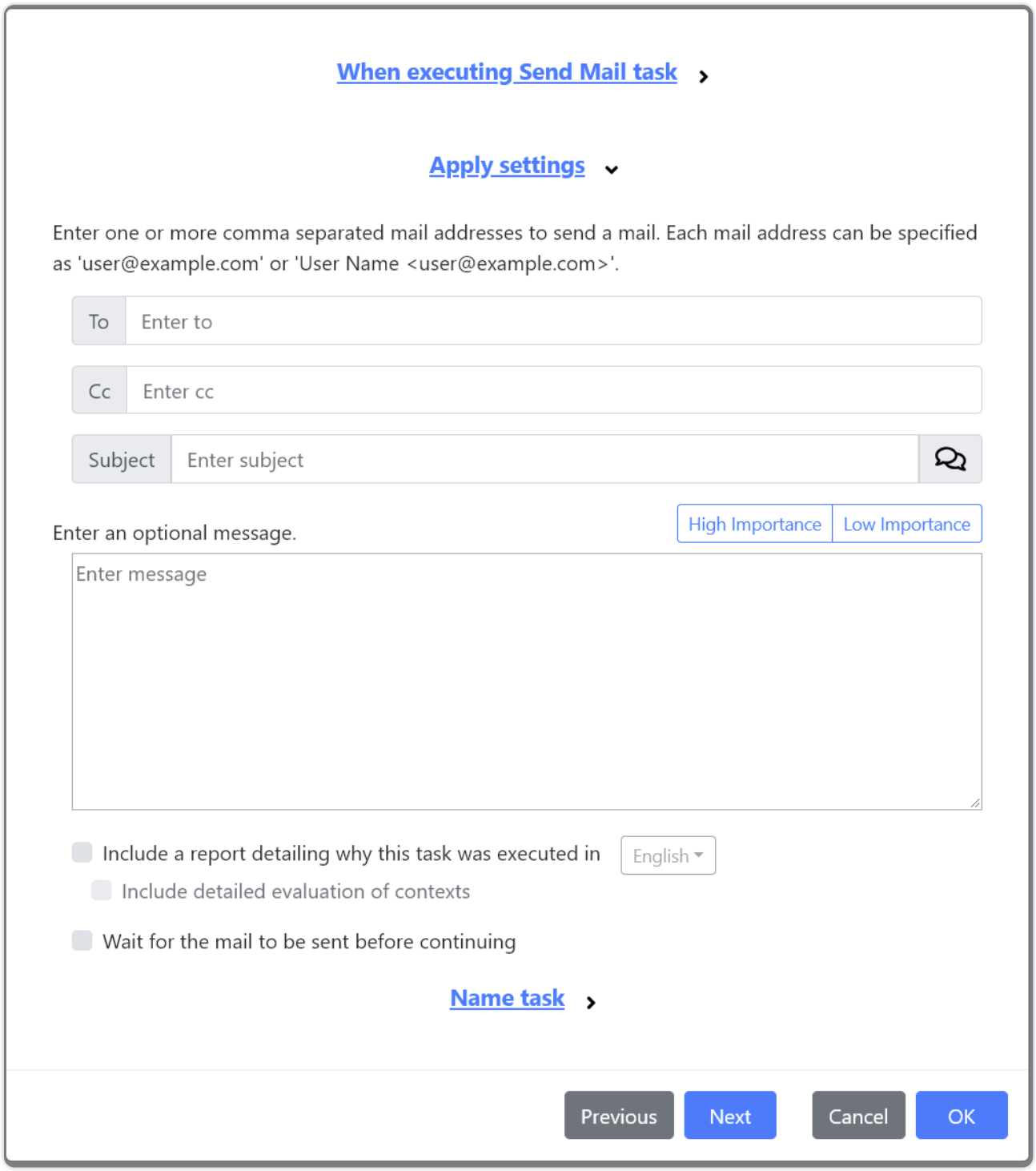
The `Screen Saver` task updates the screen saver settings within the session.



Send Mail Task

The `Send Mail` task sends an email with the defined content. Mail Server Settings must be configured.

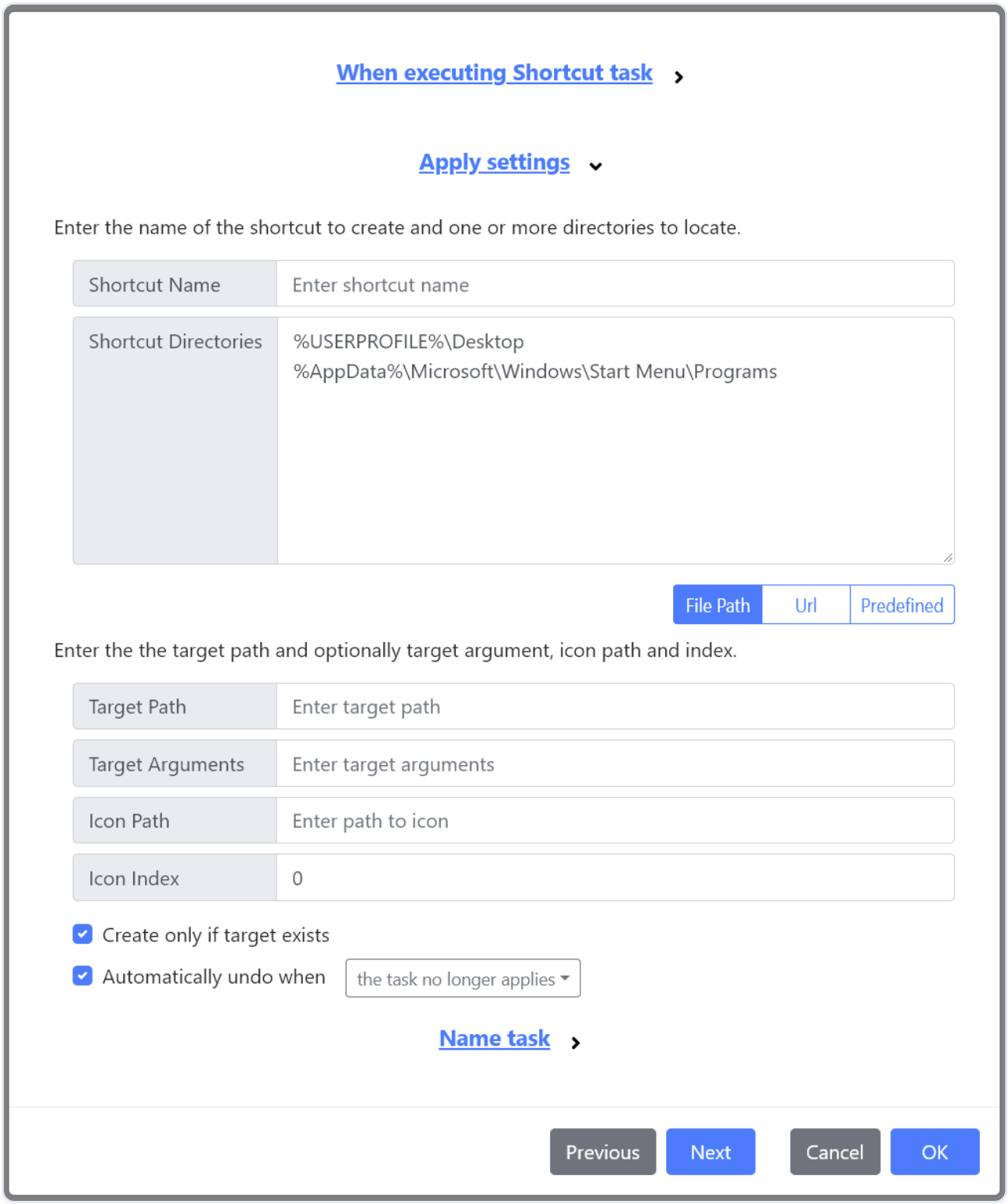
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Shortcut Task

The `Shortcut` task creates a shortcut within the user session.

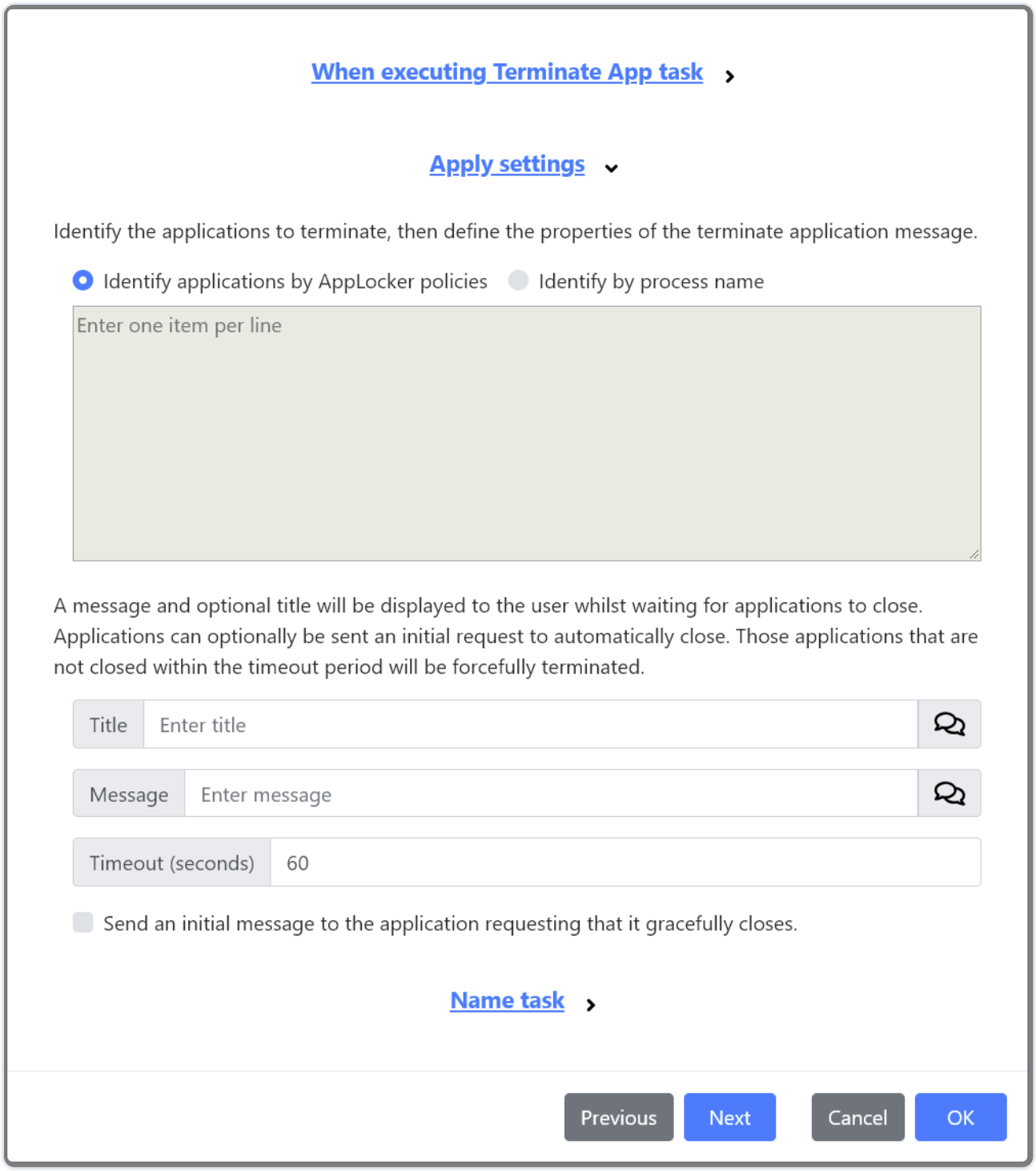
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

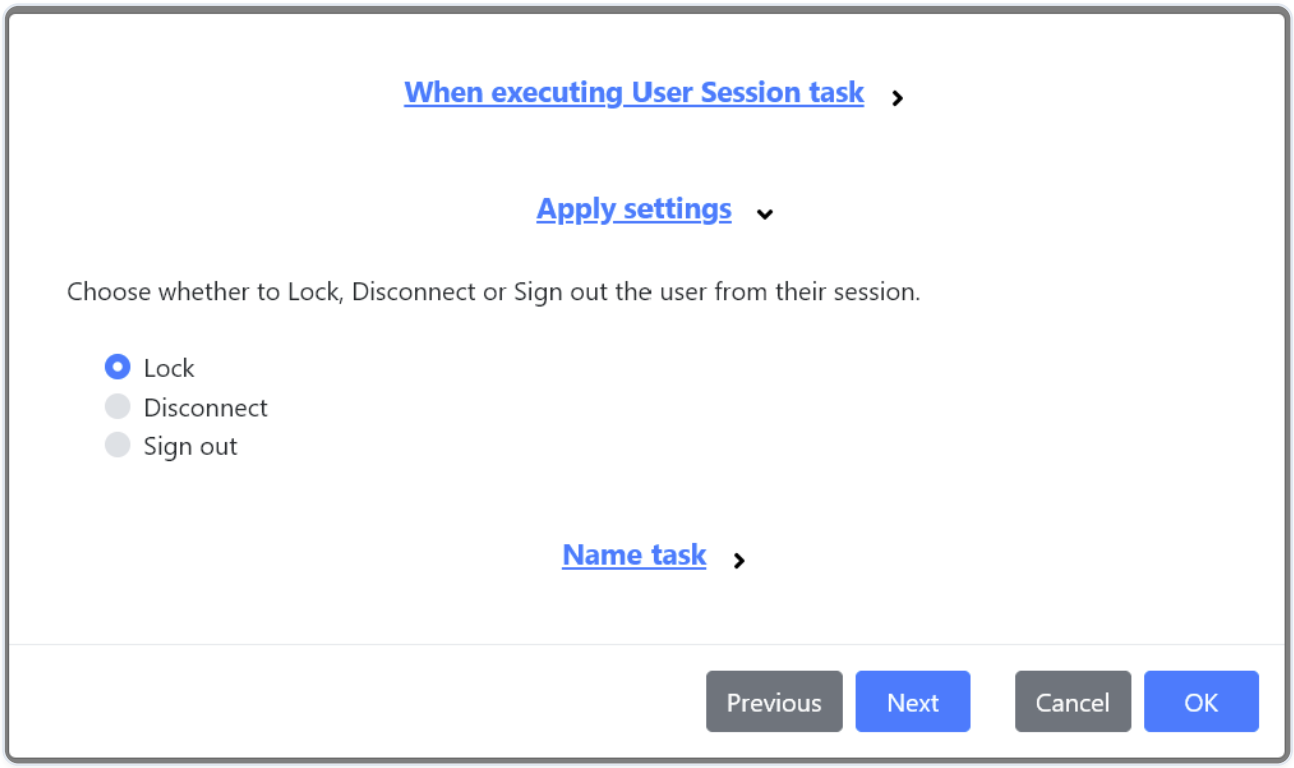
© 1997–2026 Citrix Systems, Inc. All rights reserved.



User Session Task

The `User Session` task locks, disconnects, or signs out the user session.

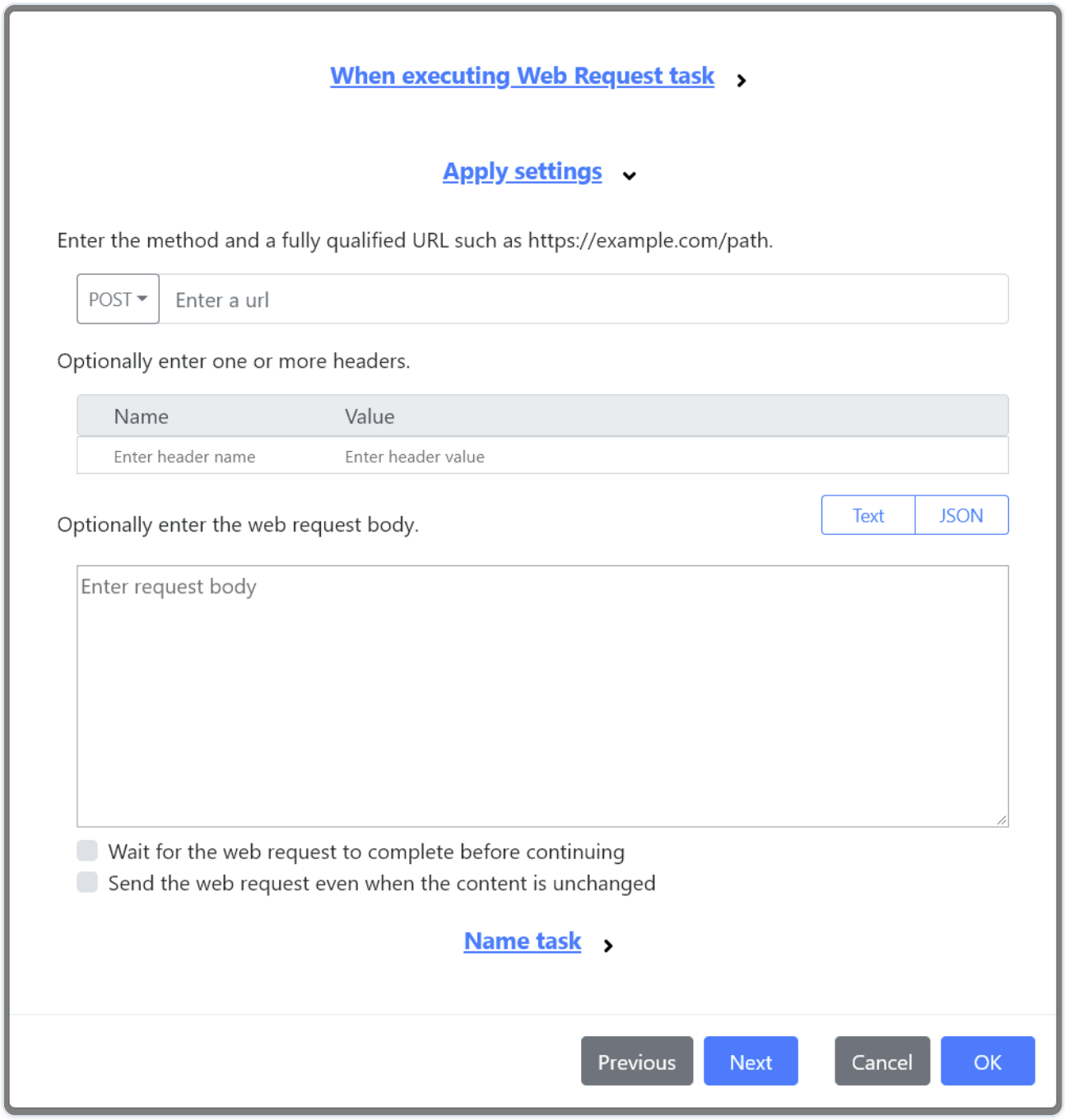
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

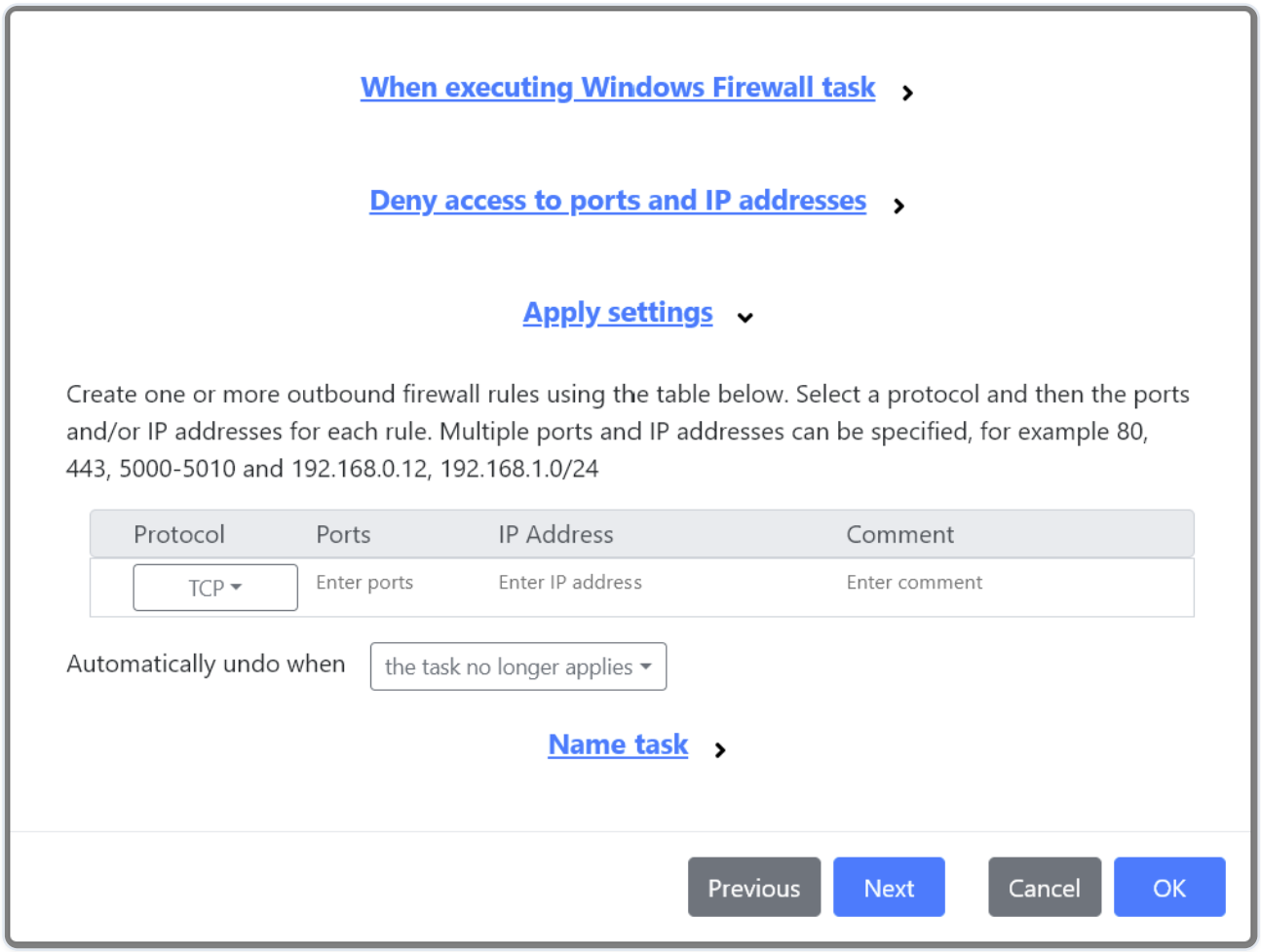
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

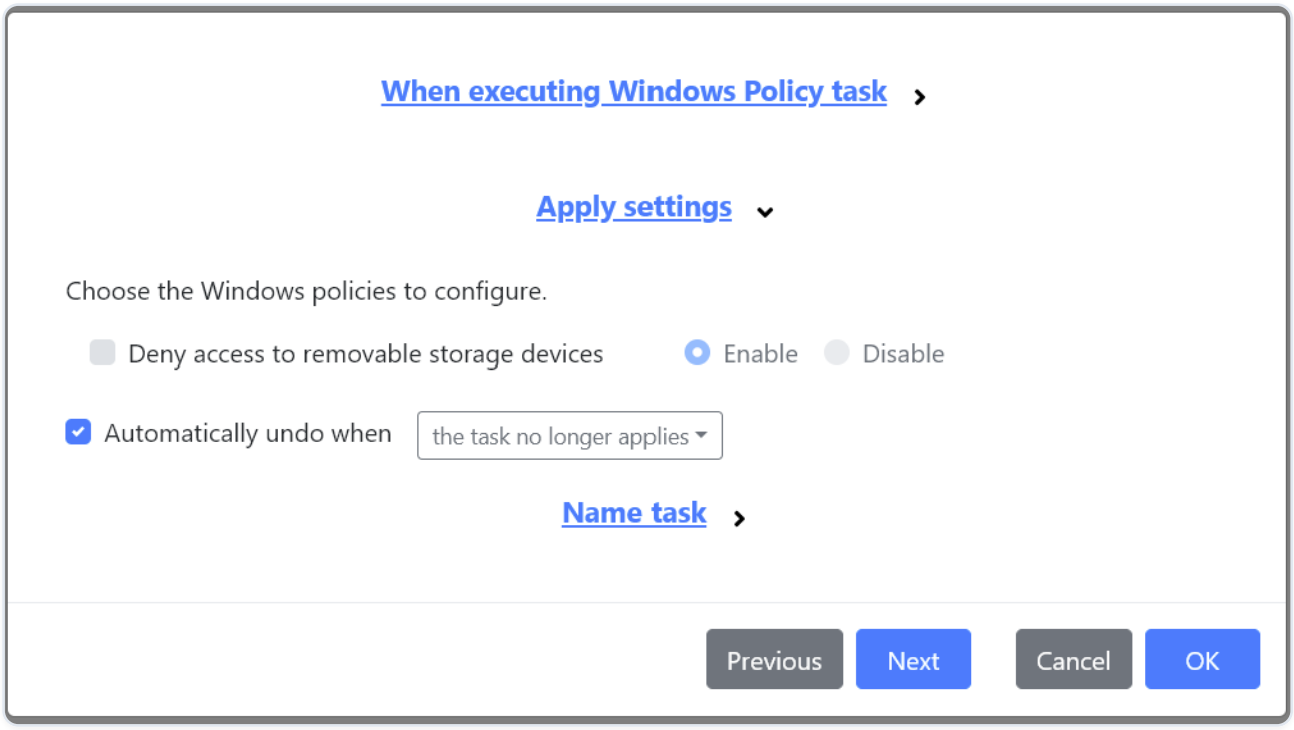
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Policy Task

The `Windows Policy` task updates Windows policies allowing control of removable storage devices on the local device.

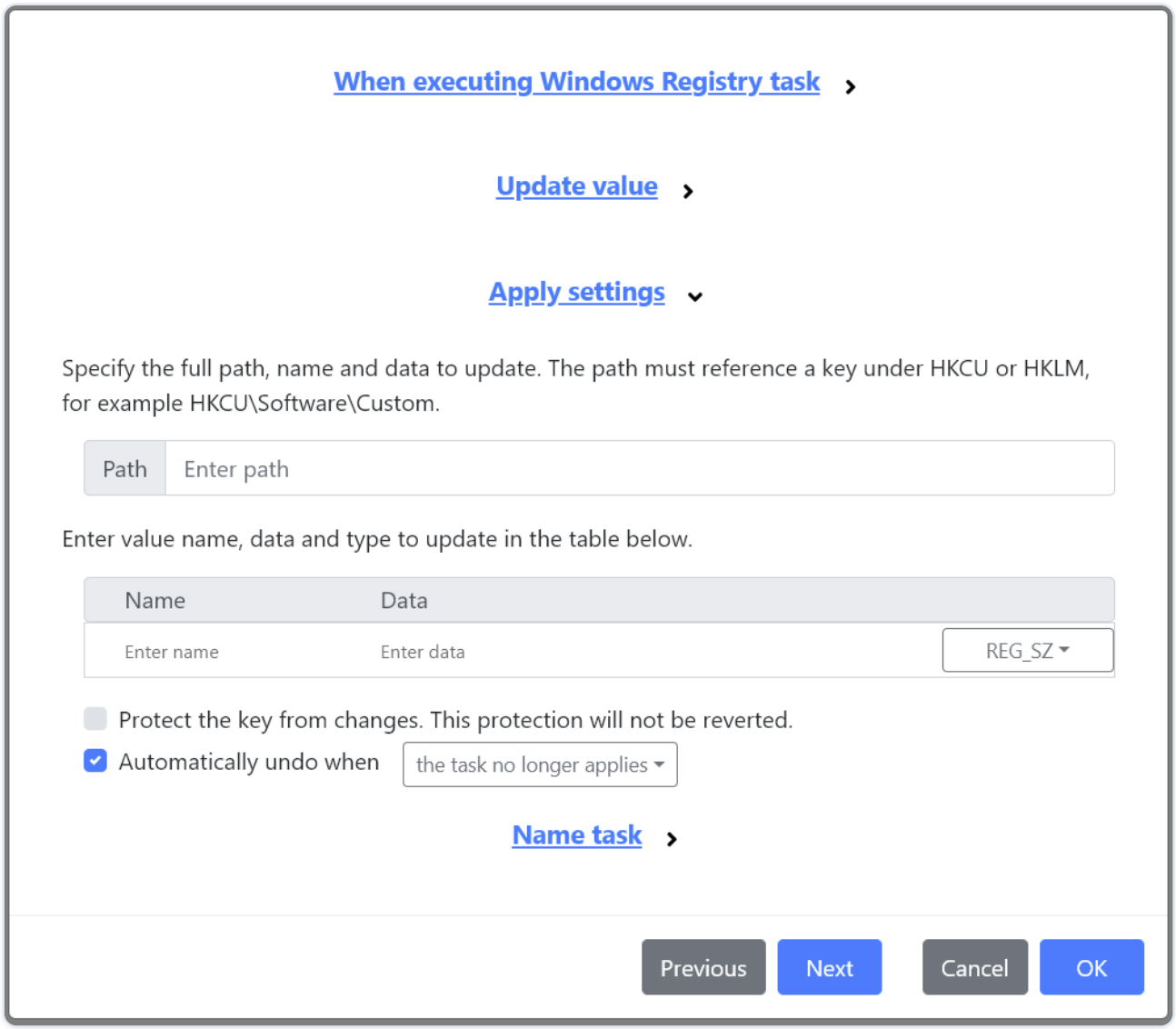
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Registry Task

The `Windows Registry` task updates or deletes values from the Windows Registry.

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

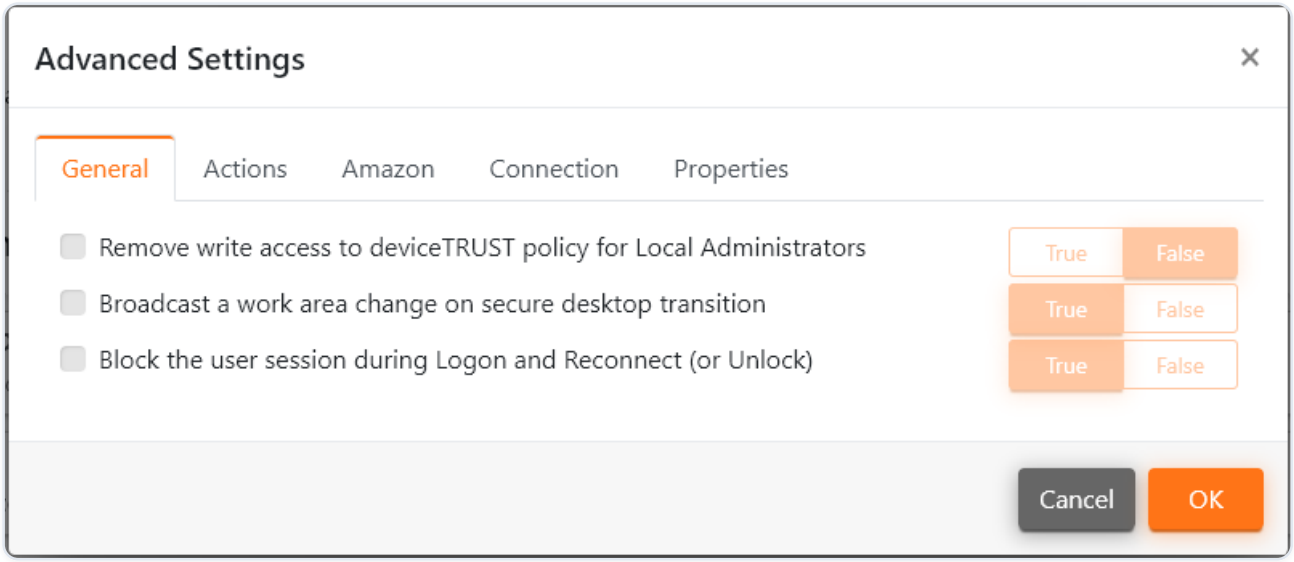


Advanced Settings

The `Advanced Settings` defines the advanced settings for configuring deviceTRUST behavior. These settings are described below.

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

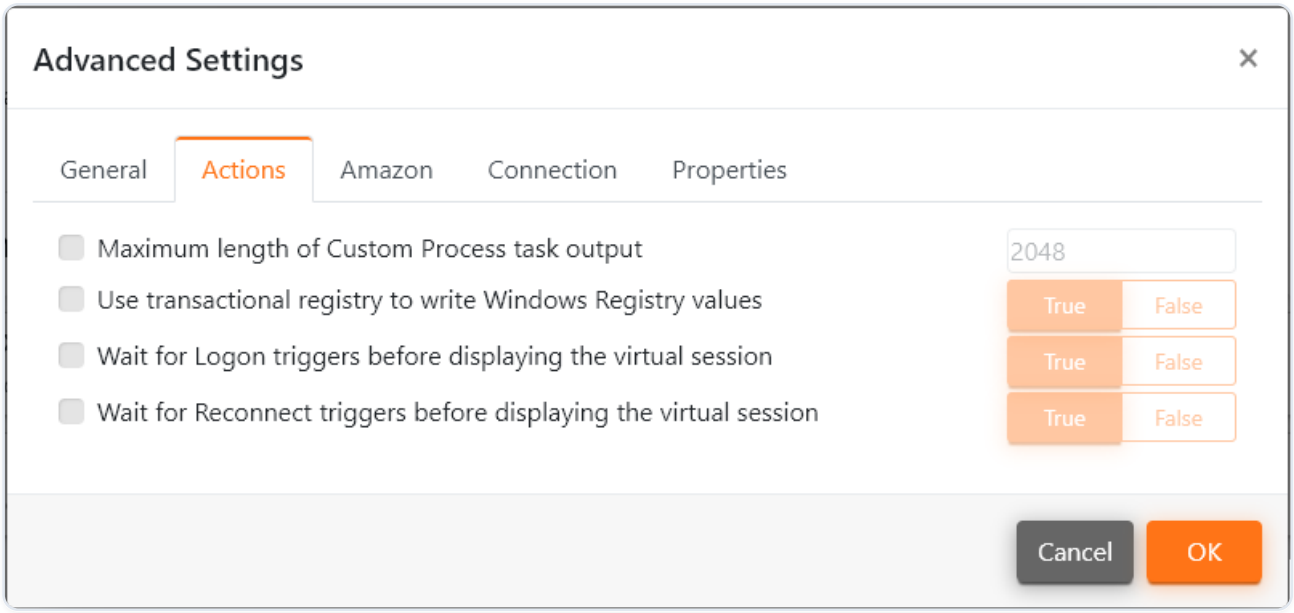
General Settings



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

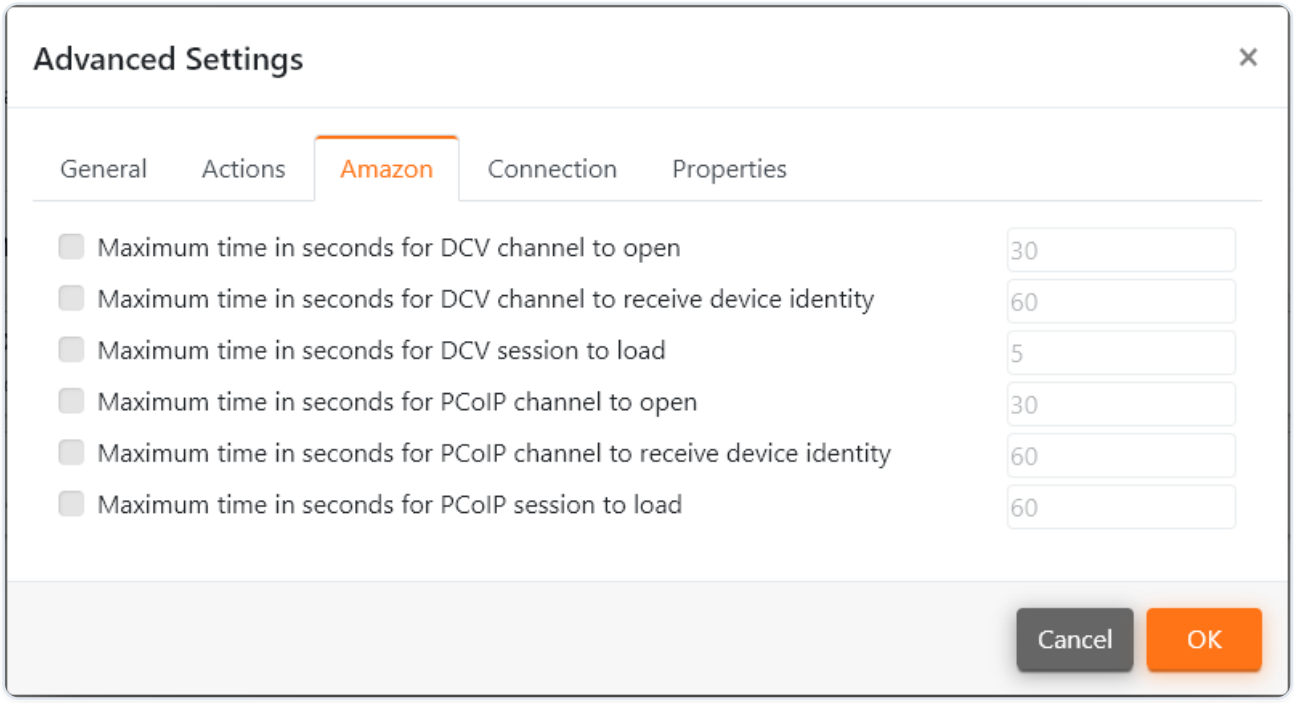


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



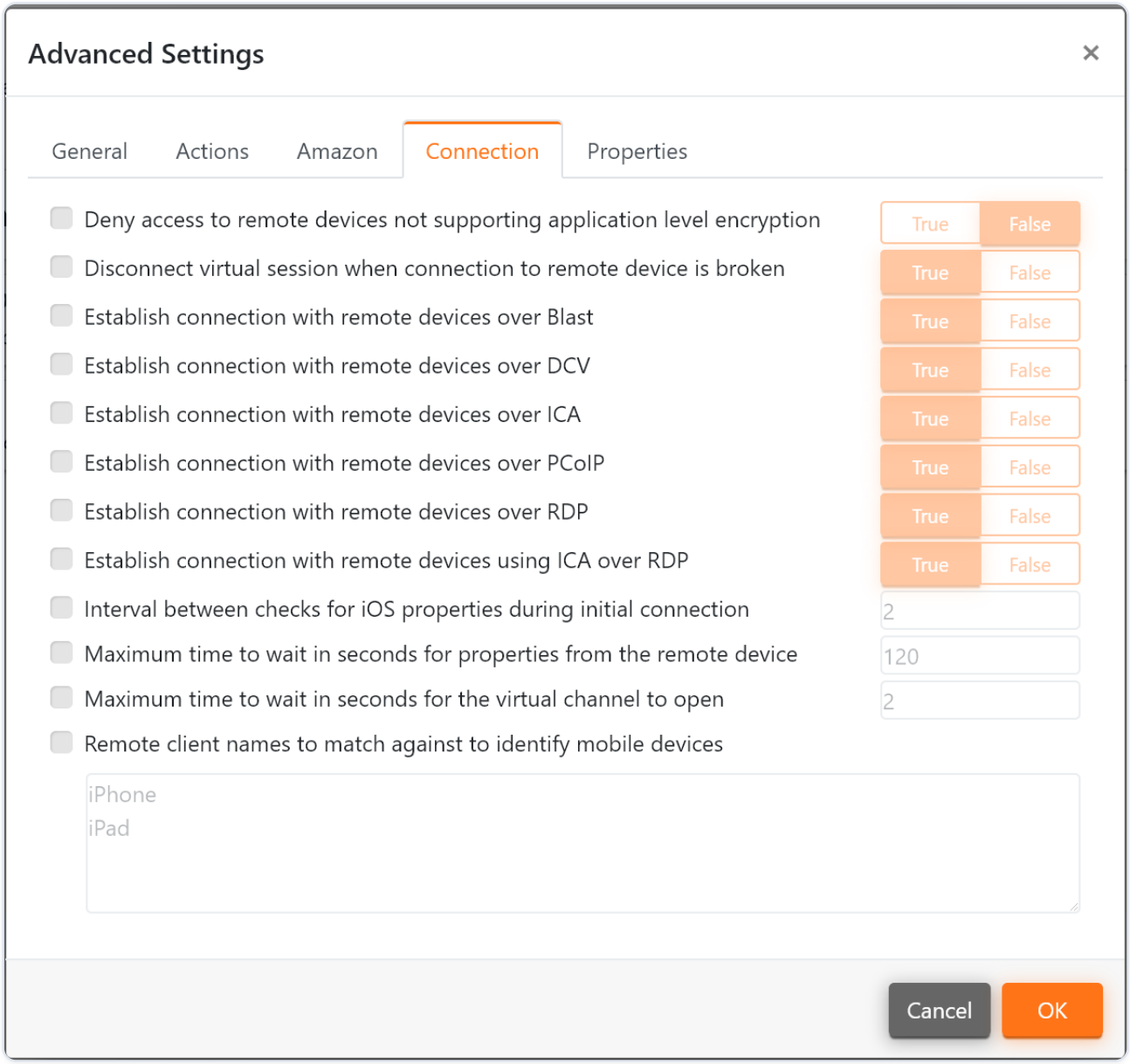
The following controls are available:

- `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



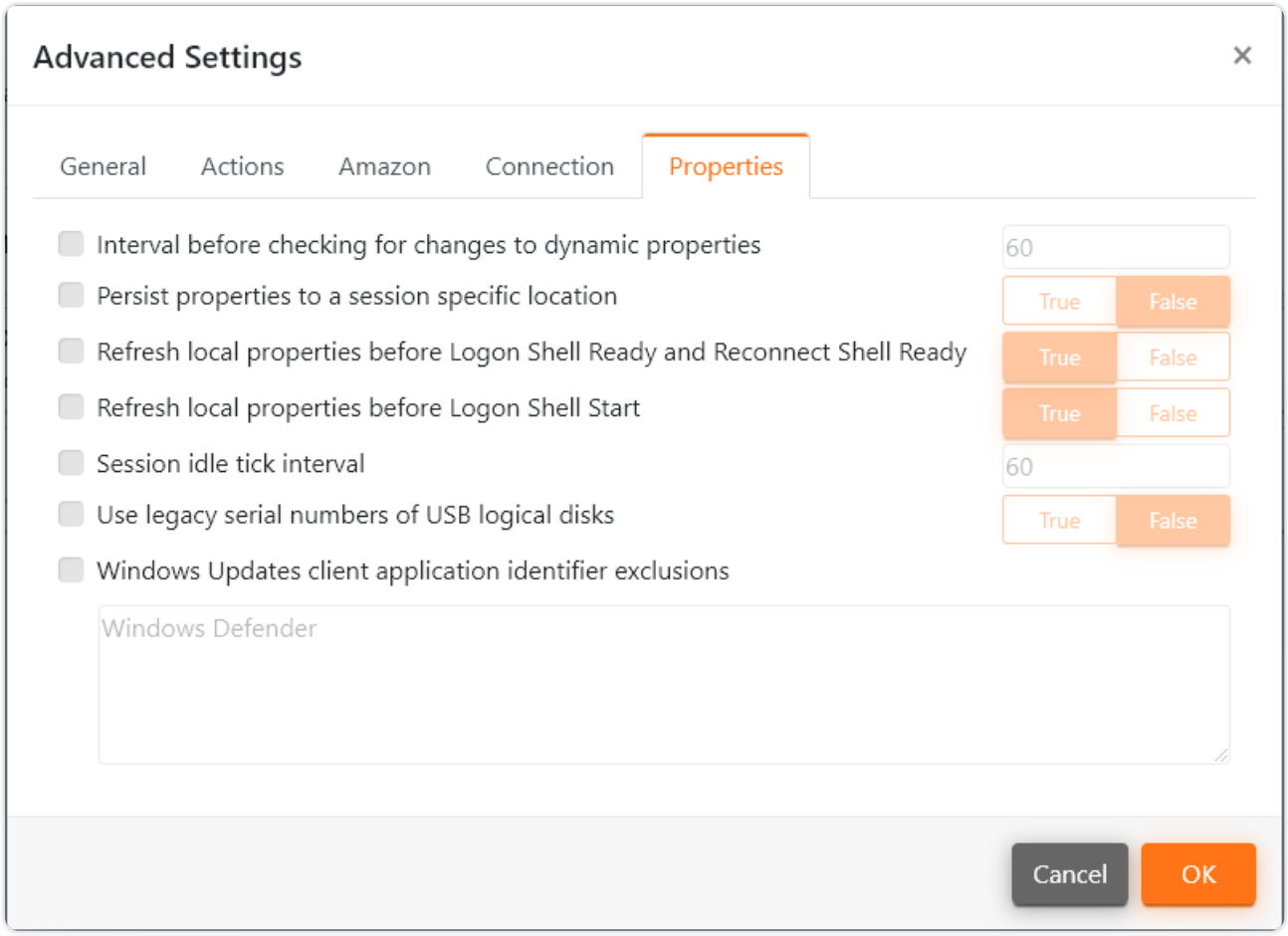
The following controls are available:

© 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.

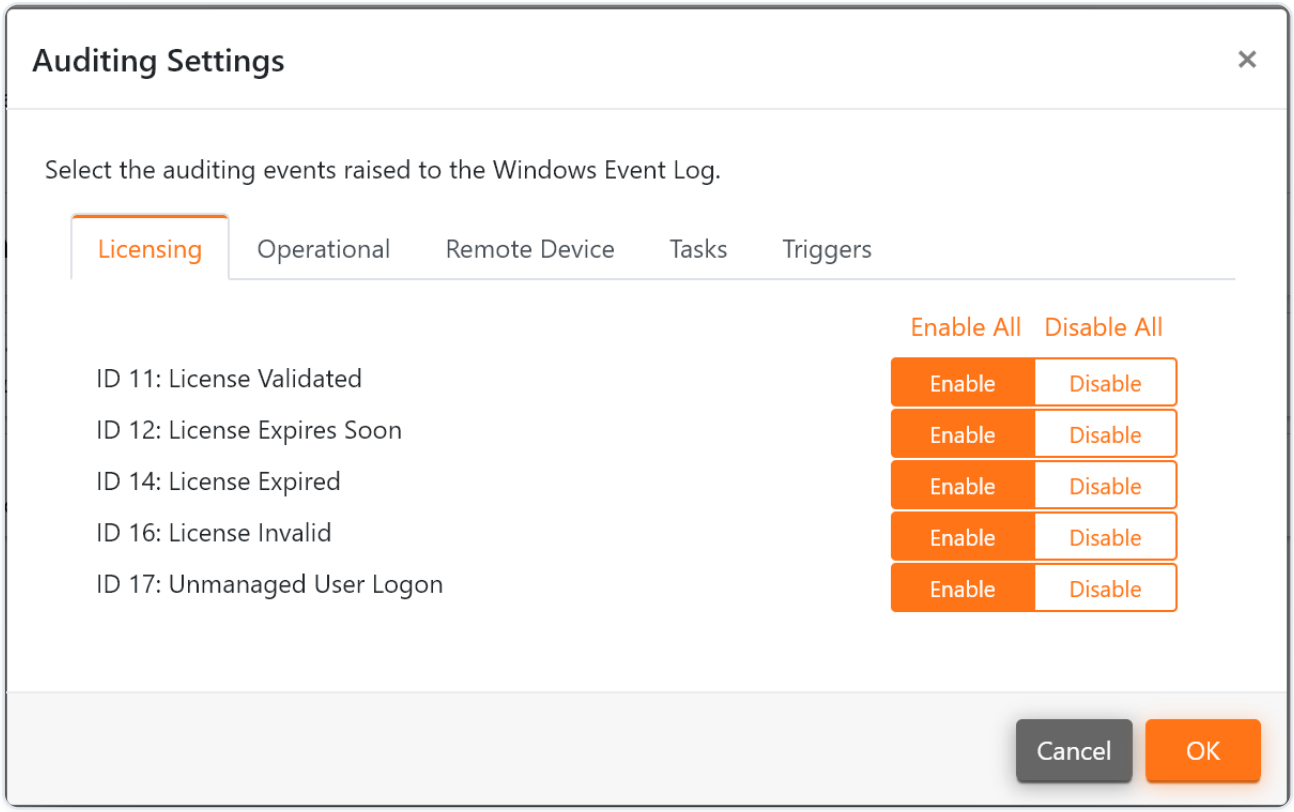
- `Windows Updates client application identifier exclusions` - List of client application identifiers of Windows Updates to ignore when calculating the last install time.

Auditing Settings

The `Auditing Settings` defines the audit events that are raised to the Windows Event Log.

Licensing

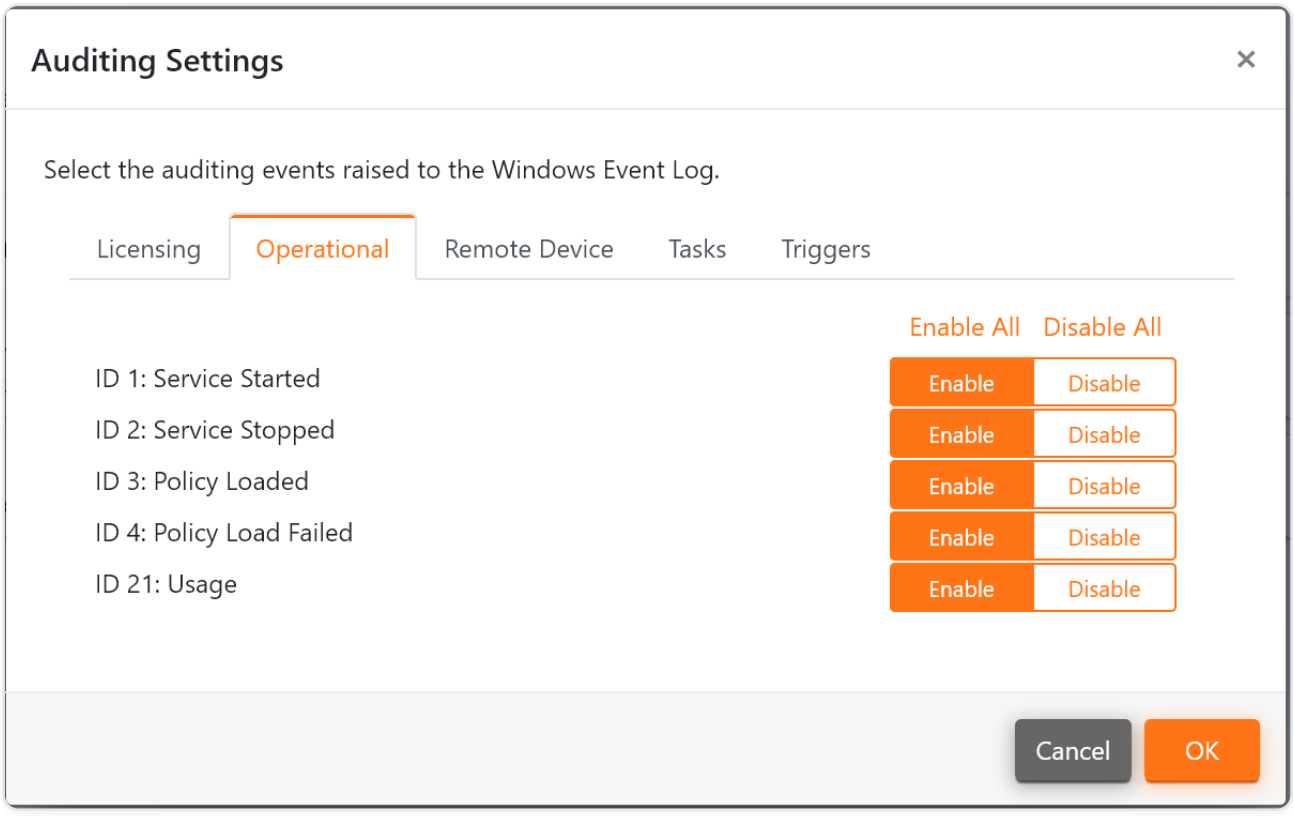
This section allows the control of events relating to the licensing of the deviceTRUST® product. All events are turned on by default but this can be customized by changing which events are enabled.



Operational

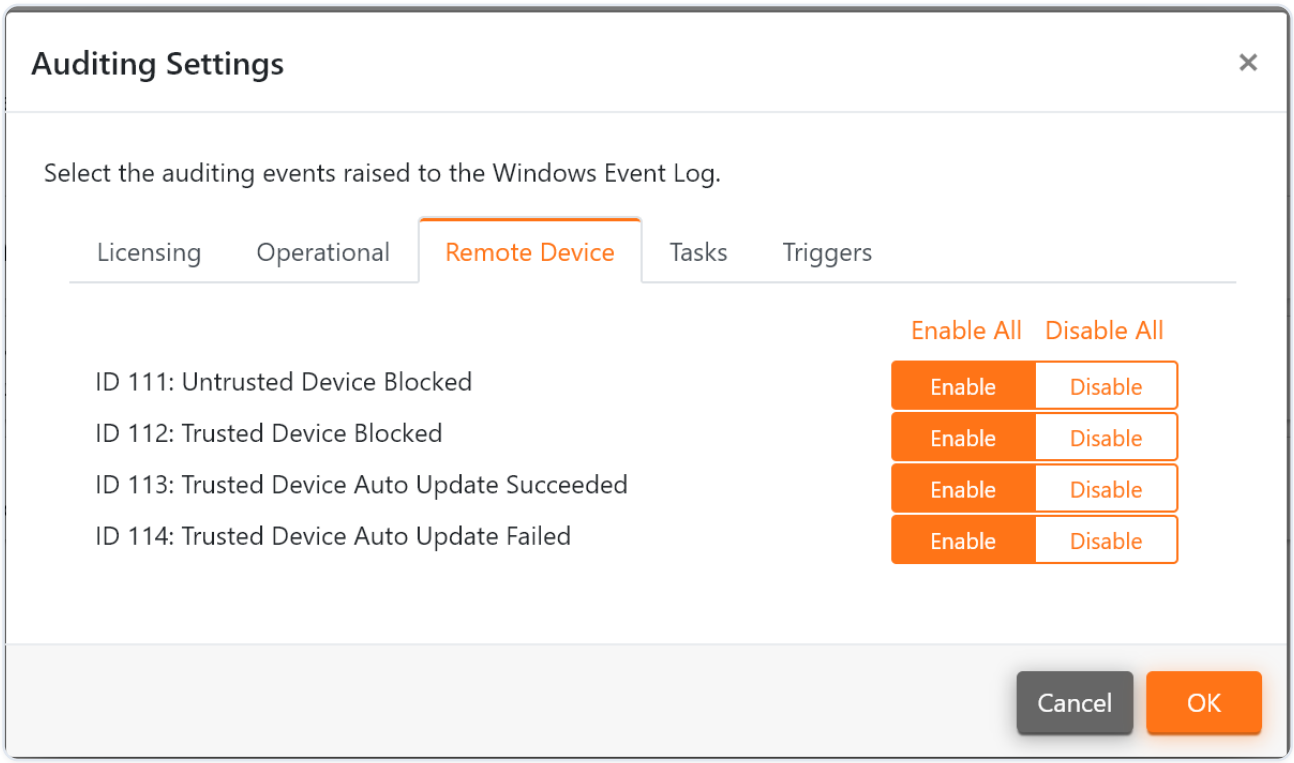
This section allows the control of events relating to the operation of the deviceTRUST product. All events are turned on by default but this can be customized by changing which events are enabled.

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



Remote Device

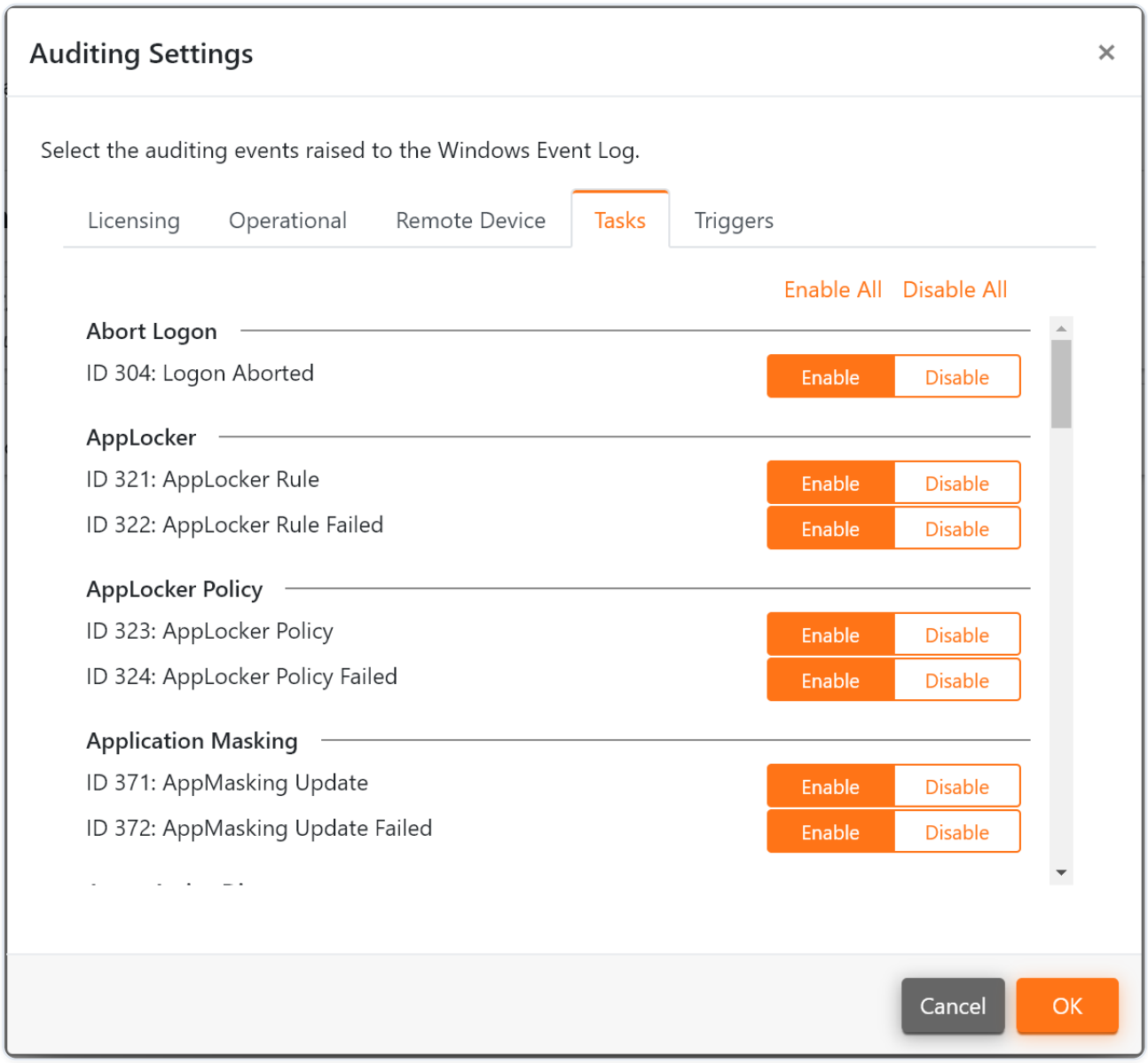
This section allows the control of events relating to the trust of a remote device attempting to establish a connection and also the status of the auto-update. All events are turned on by default but this can be customized by changing which events are enabled.



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

Tasks

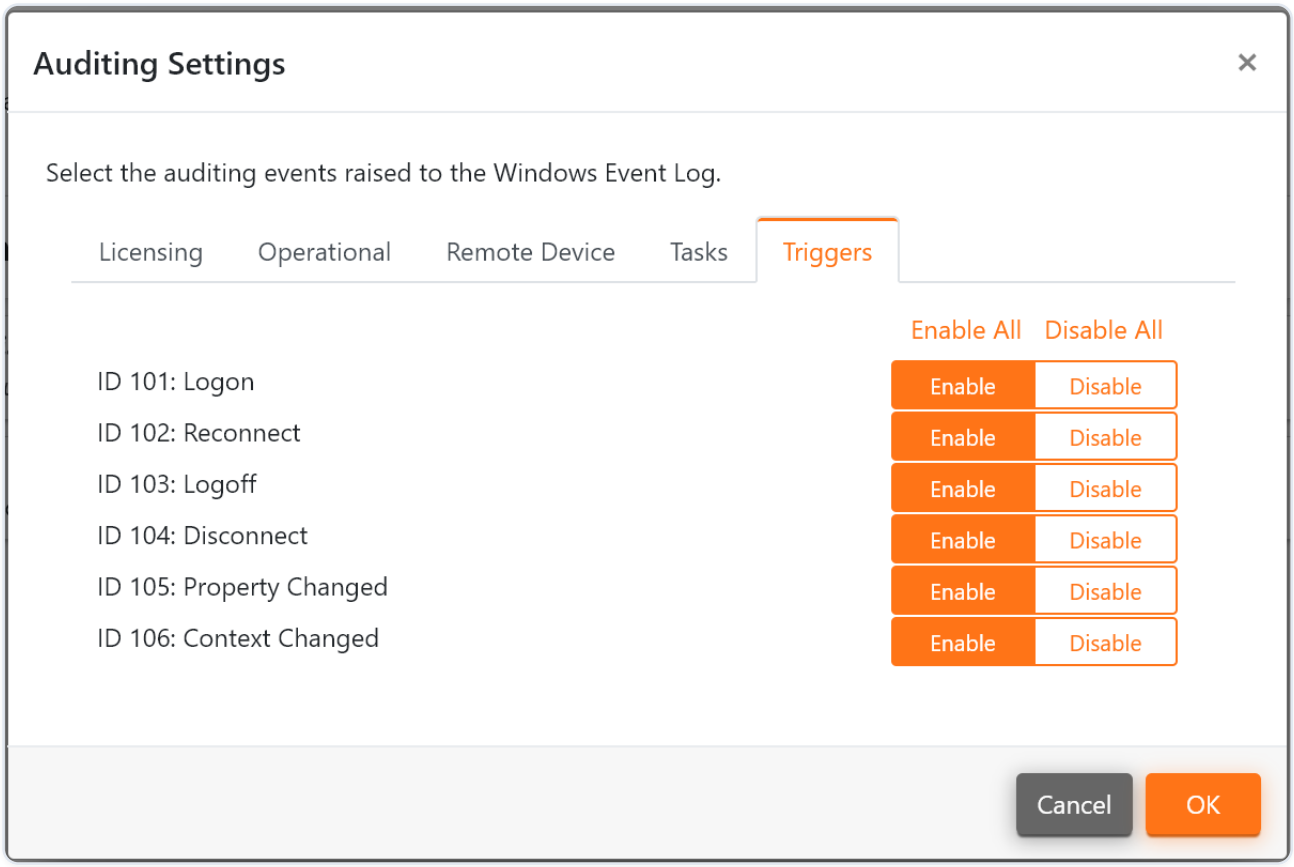
This section allows the control of events relating to the execution of tasks by the deviceTRUST product. This section groups the events per-task as described by each header. All events are turned on by default but this can be customized by changing which events are enabled.



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

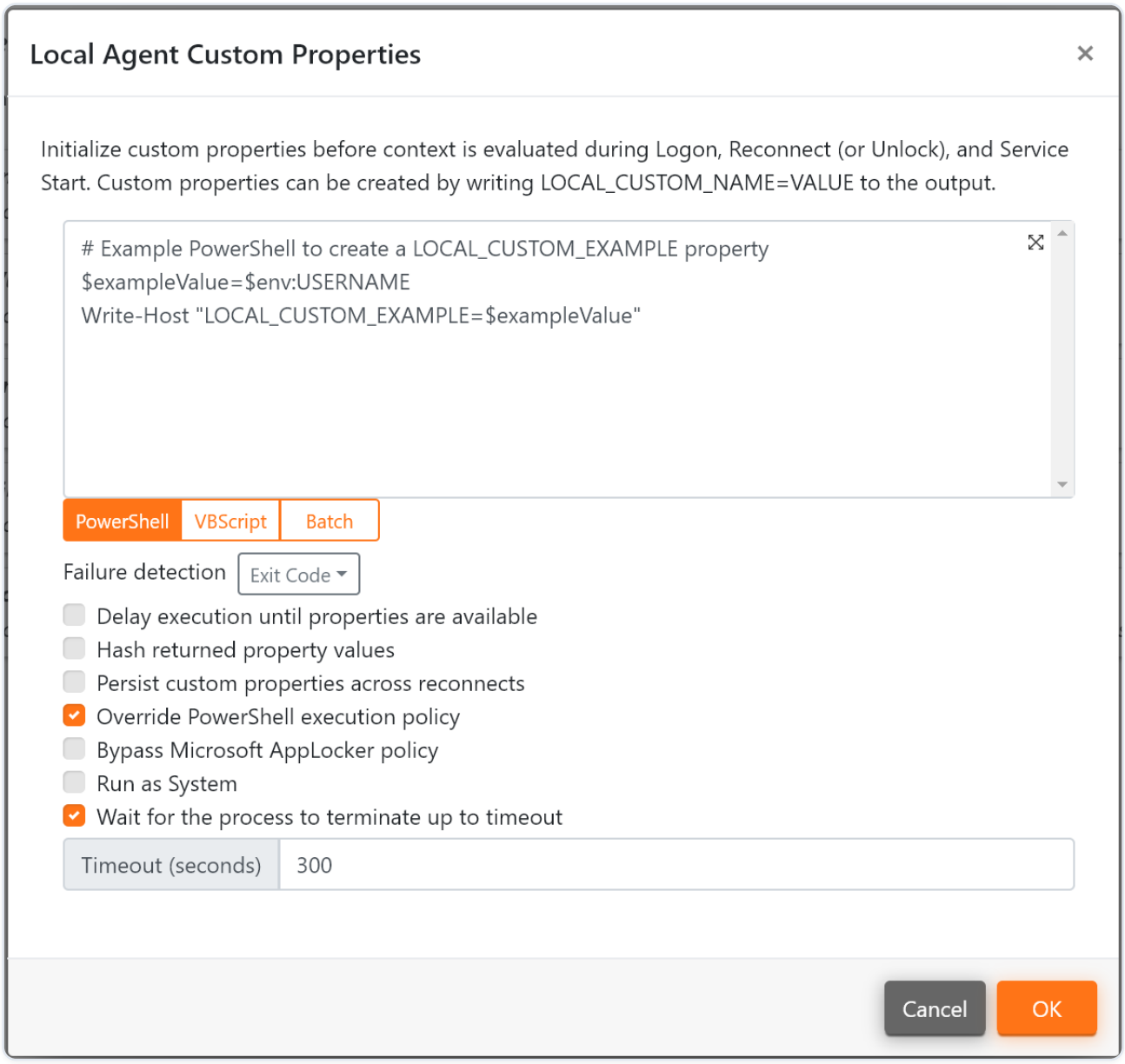
The `Custom Properties Settings` defines scripts that can be launched during a session to determine additional properties of the local agent or remote device before the context is first evaluated.

- 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

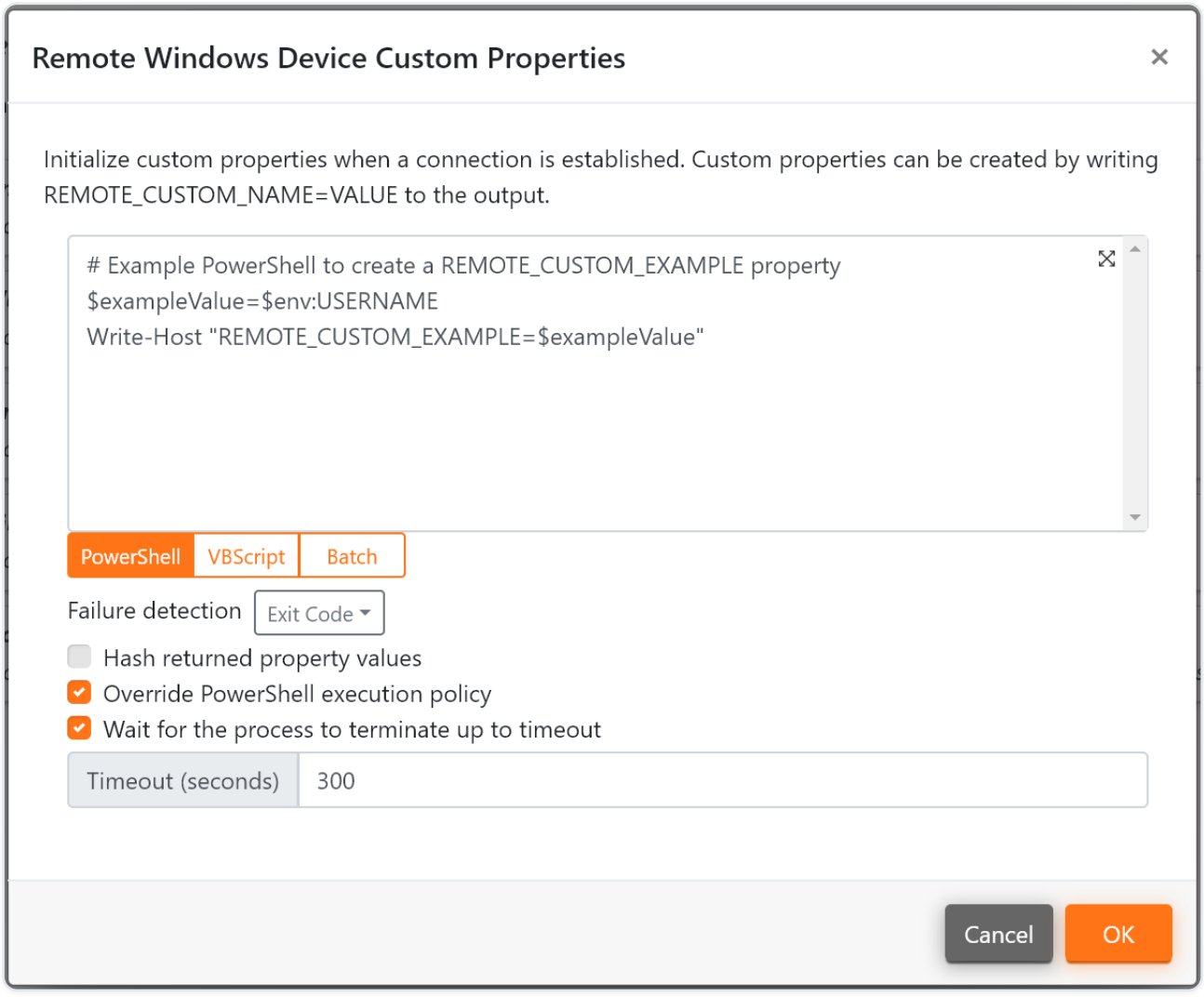
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



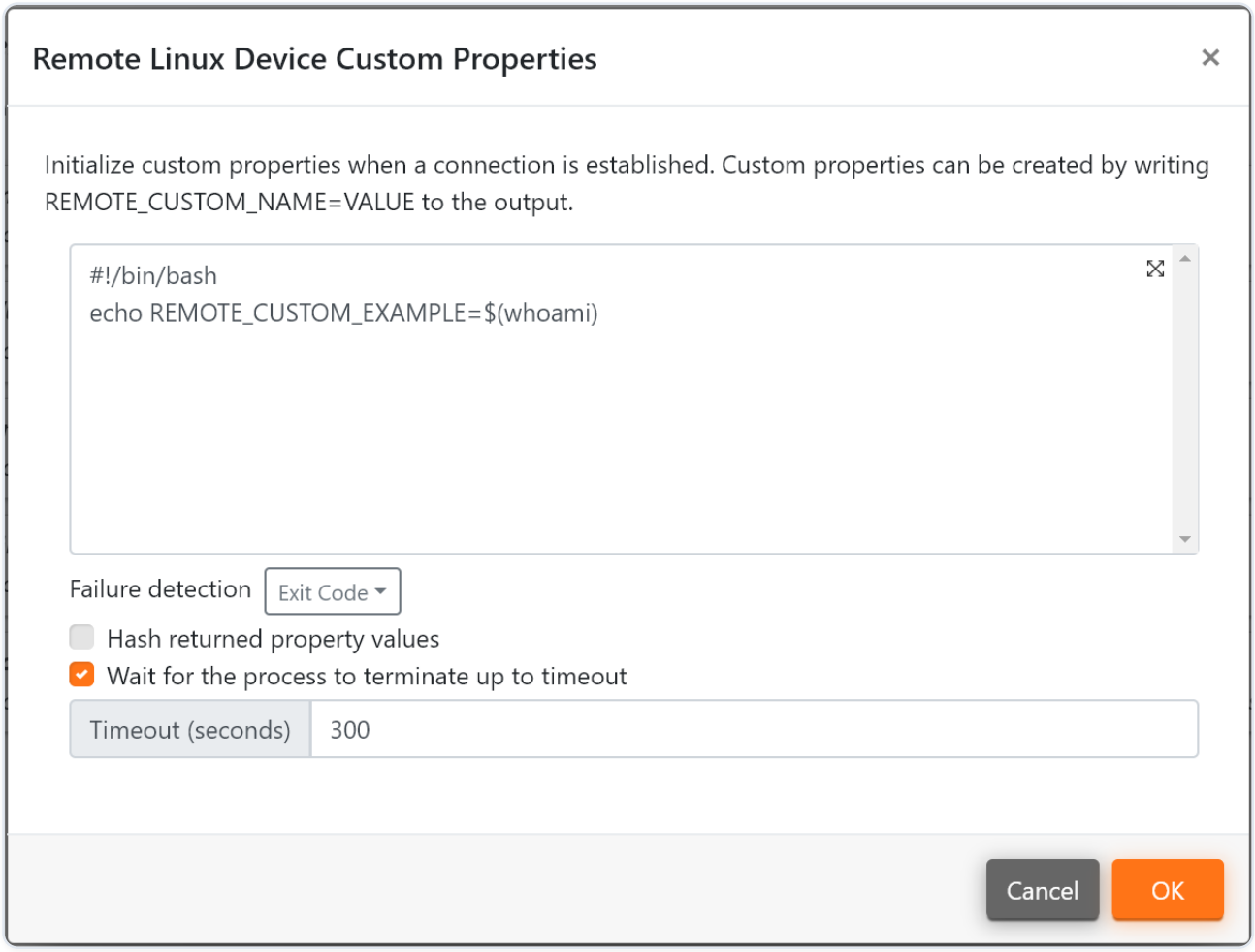
The following controls are available for the Remote Windows Device:

© 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.

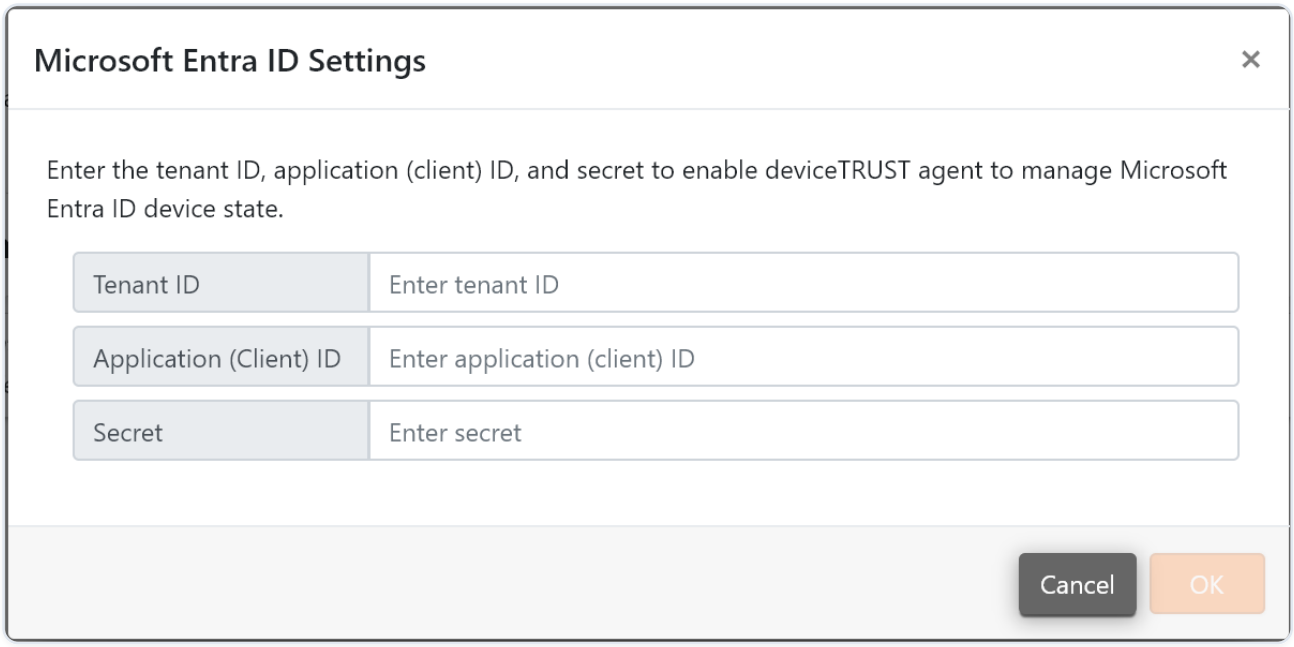
The `Wait for the process to terminate up to timeout` option should be unchecked for resident scripts. Any custom properties scripts that are still executing will be terminated when it is no longer needed.

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:

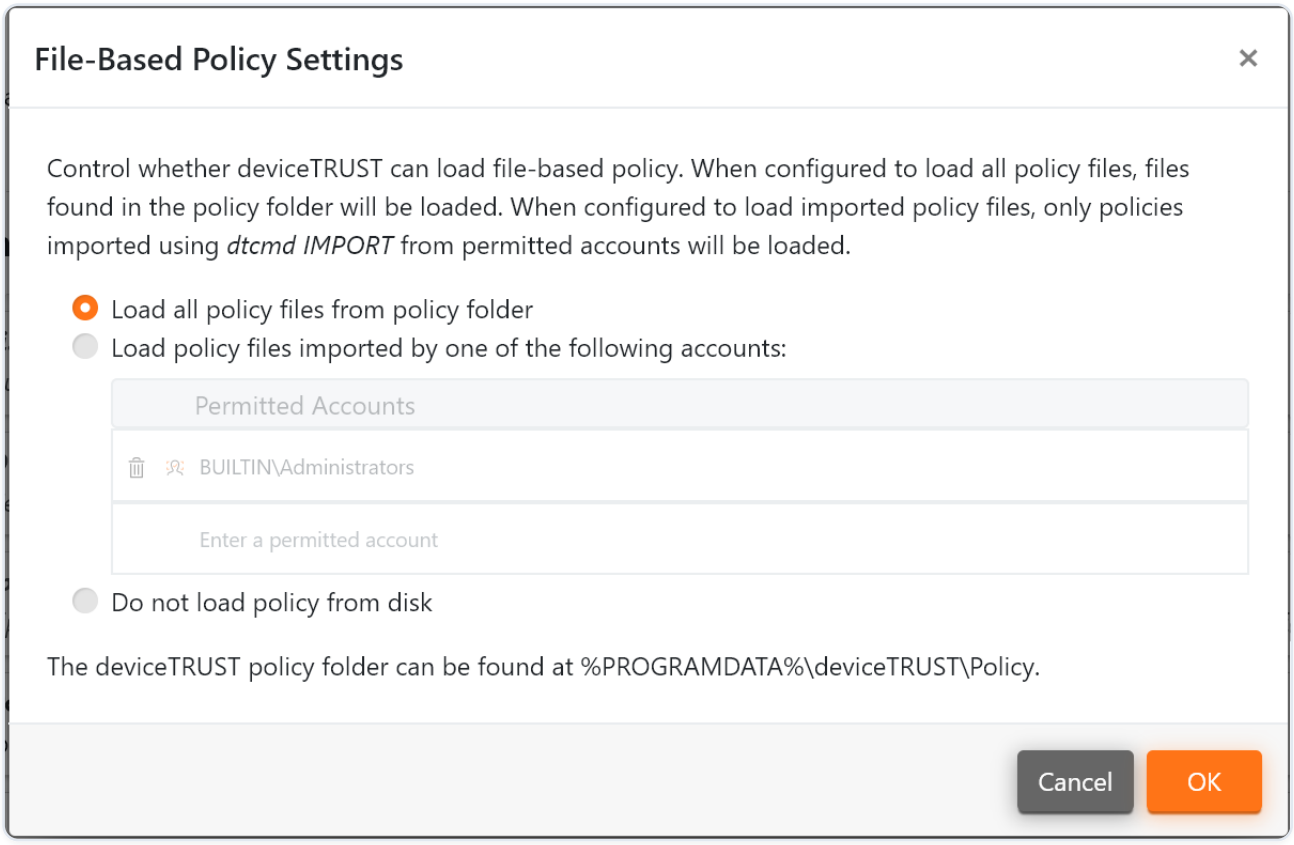
- `Tenant ID` - The Tenant ID of the Microsoft Entra ID tenant. This can be copied from the App Registrations `Overview` page.
- `Application (Client) ID` - The Application (client) ID field from the App Registrations `Overview` page.
- `Secret` - The `Value` field of the client secret.

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

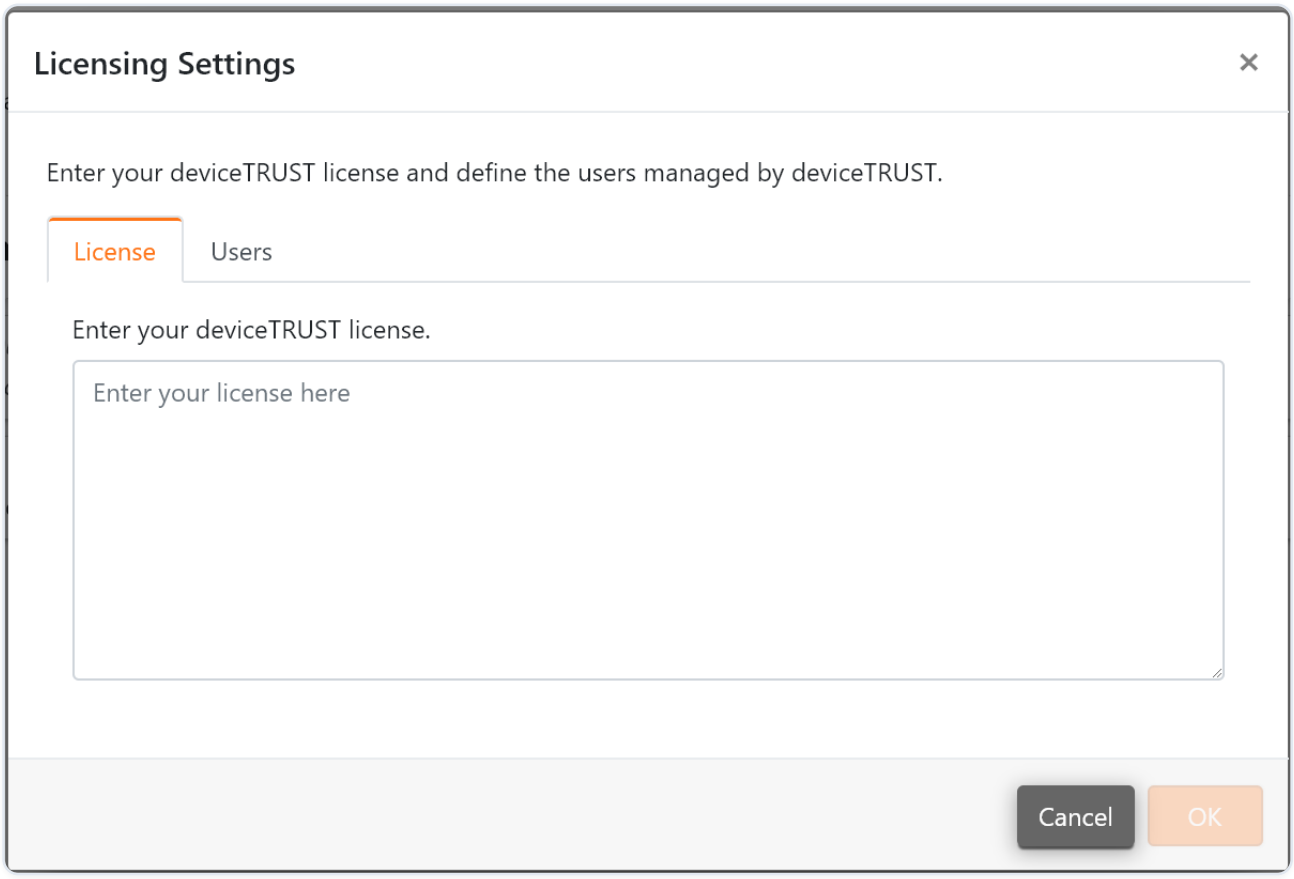
TABLE OF CONTENTS

- 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.

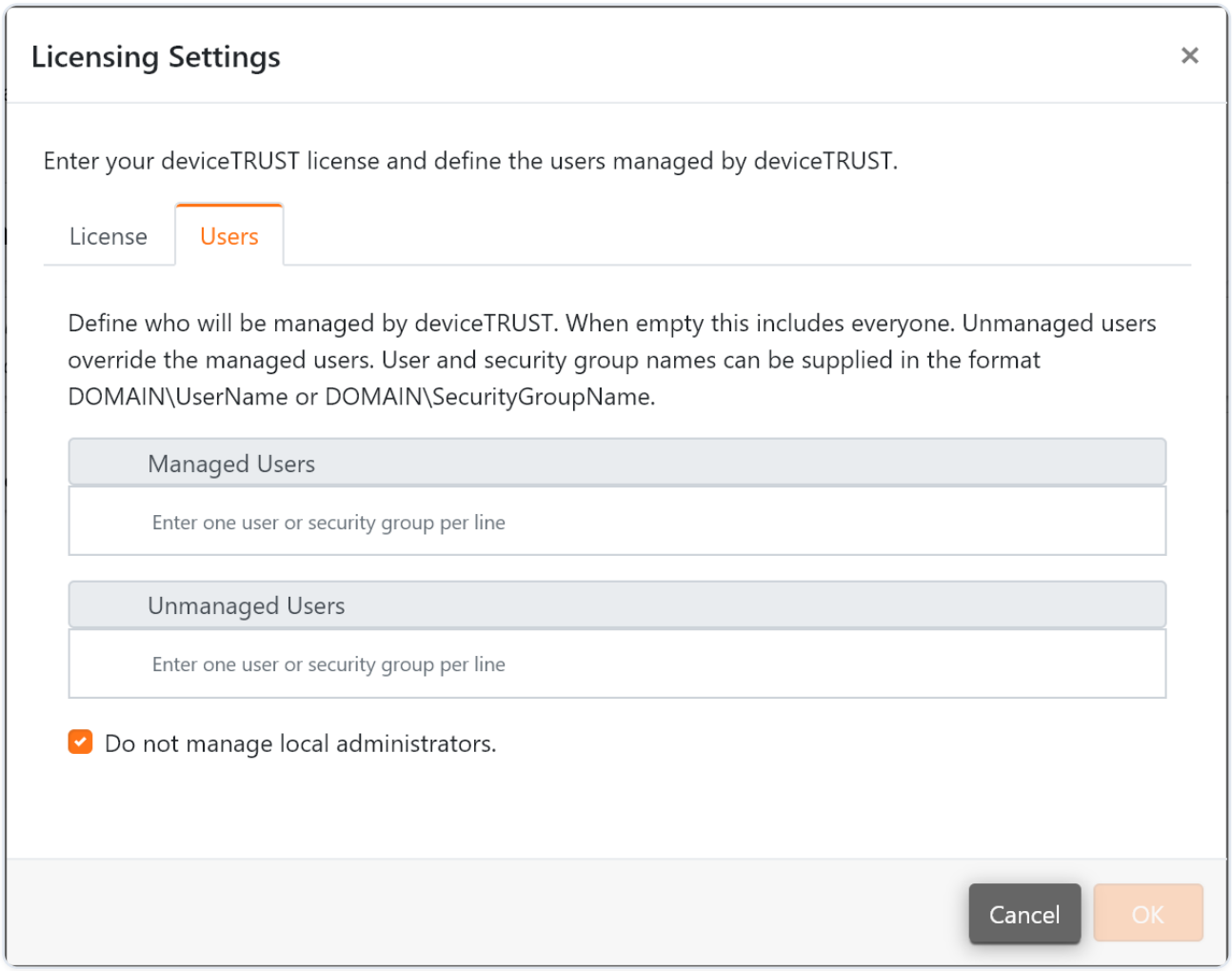
Licensing Settings

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.

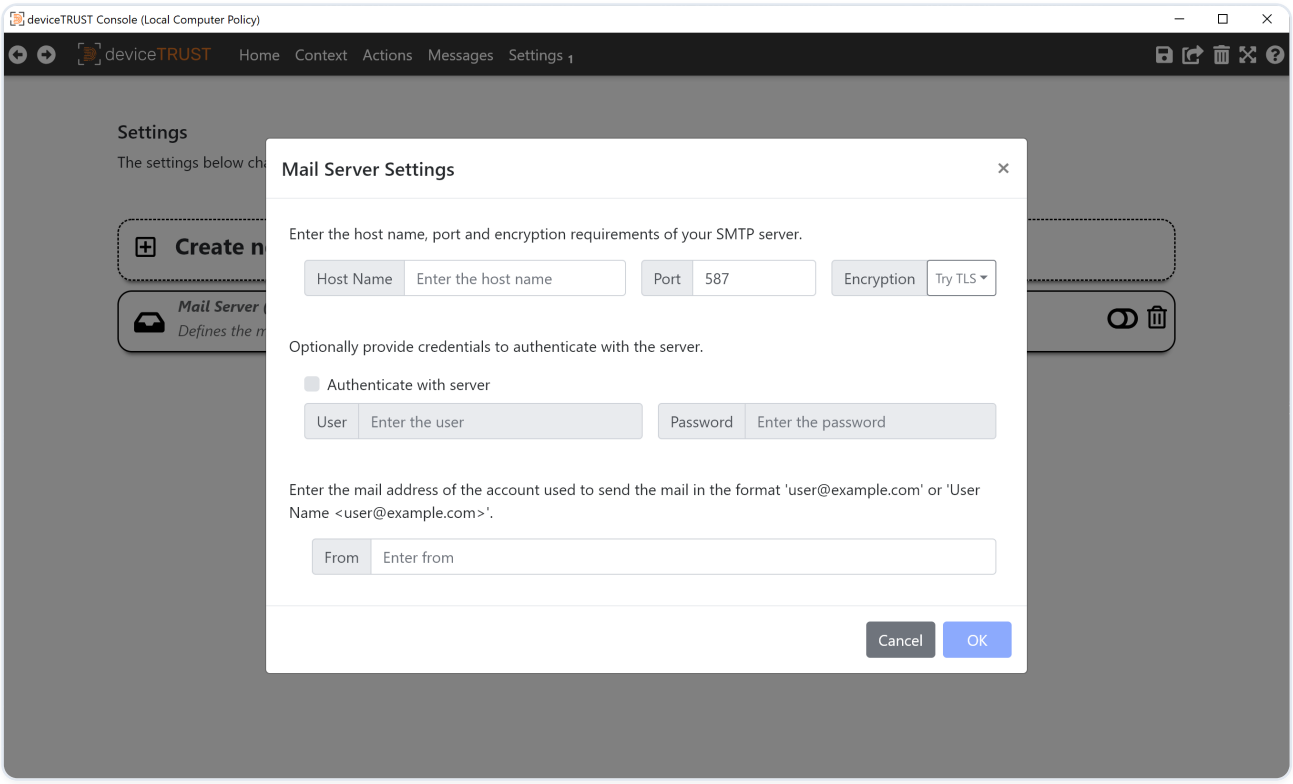
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Mail Server Settings

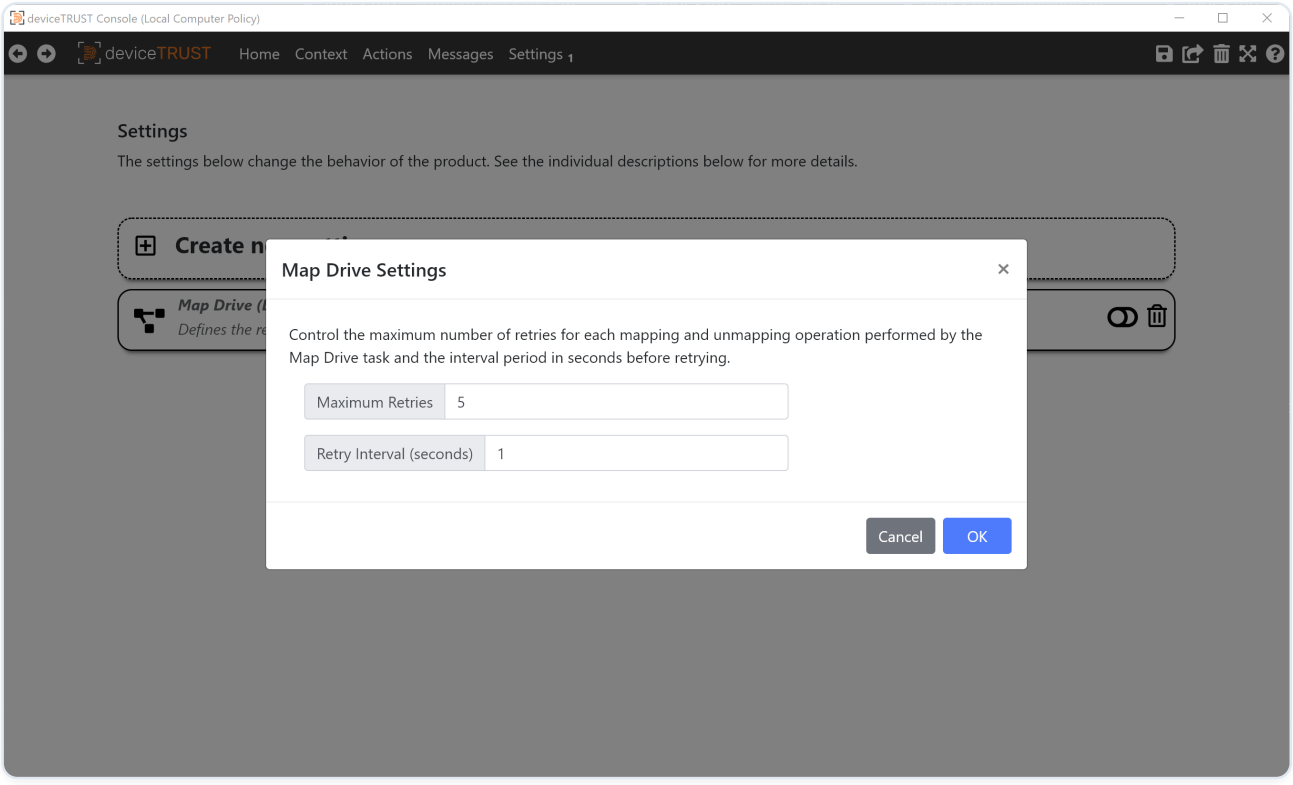
The `Mail Server Settings` defines the mail server used by the Send Mail task.

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



Map Drive Settings

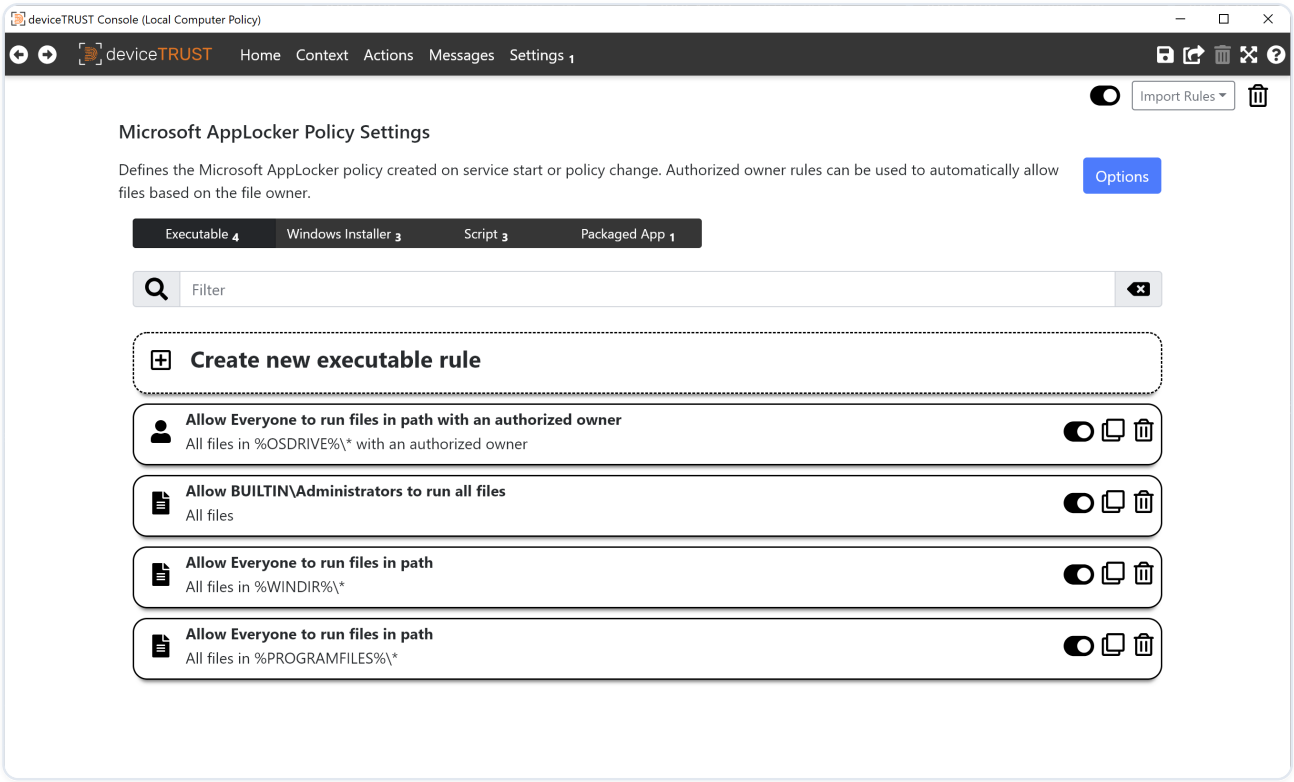
The `Map Drive Settings` define the retry and timeout settings for the Map Drive task.



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

Microsoft AppLocker Settings

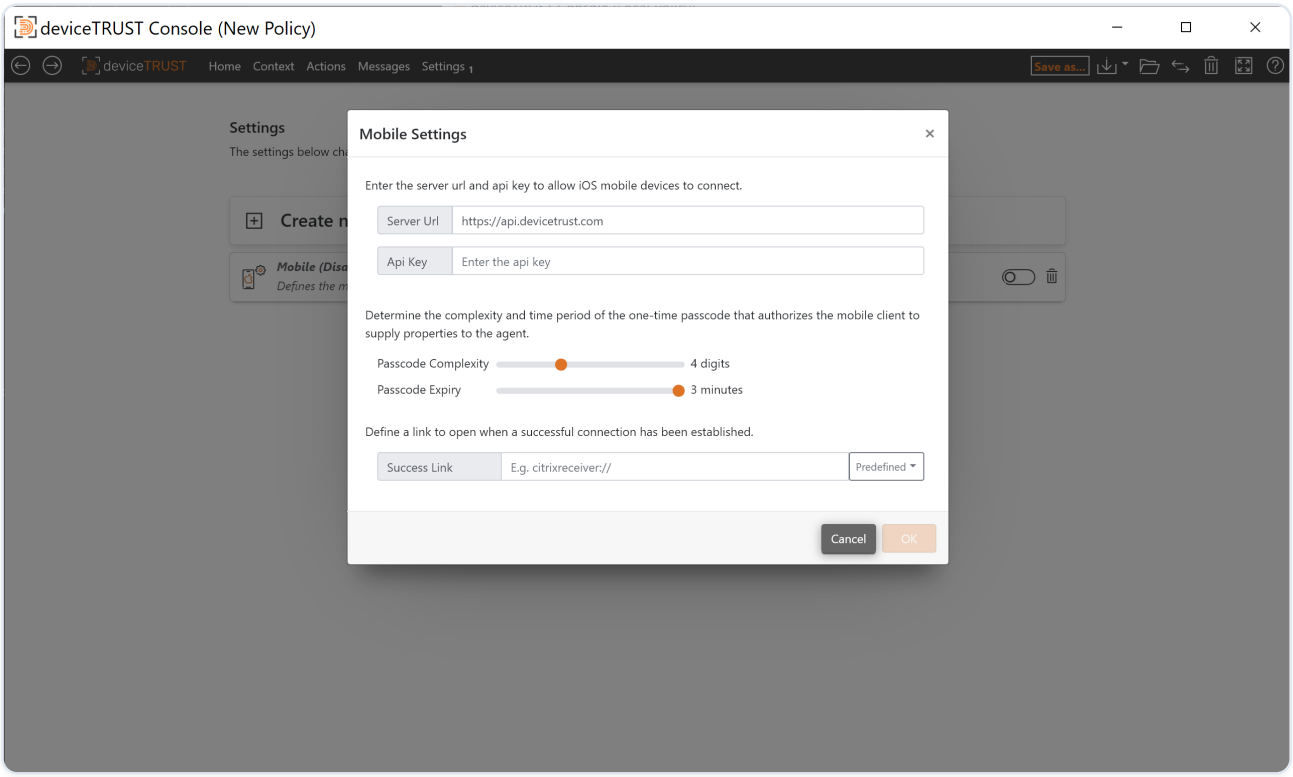
The `Microsoft AppLocker Settings` define the Microsoft AppLocker policy to control the applications, installers and scripts that can be launched.



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:

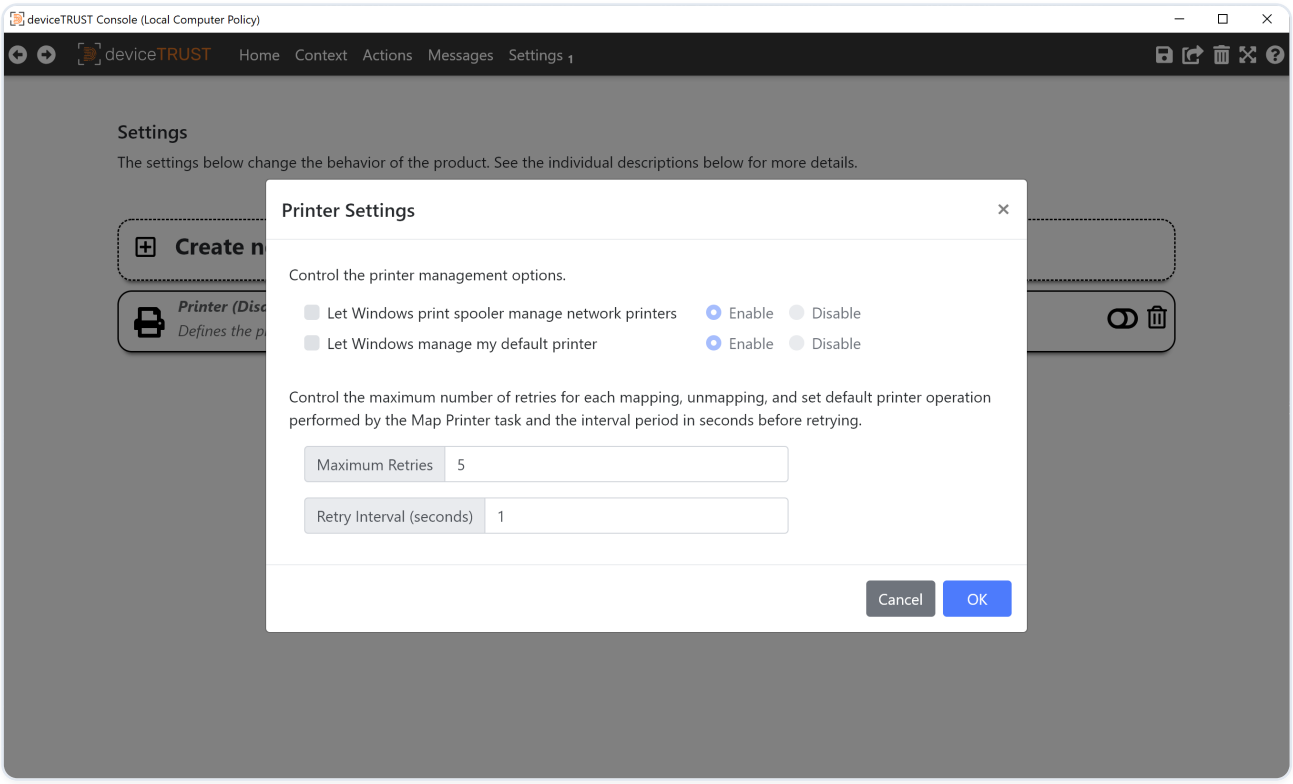
- *Server Url* - This is the URL used by the deviceTRUST® Agent to facilitate a connection to a remote iOS device. The default value should remain unchanged.
- *Api Key* - This is an API Key generated from the *App Registration* section of the deviceTRUST Portal.
- *Passcode Complexity* - Determines 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

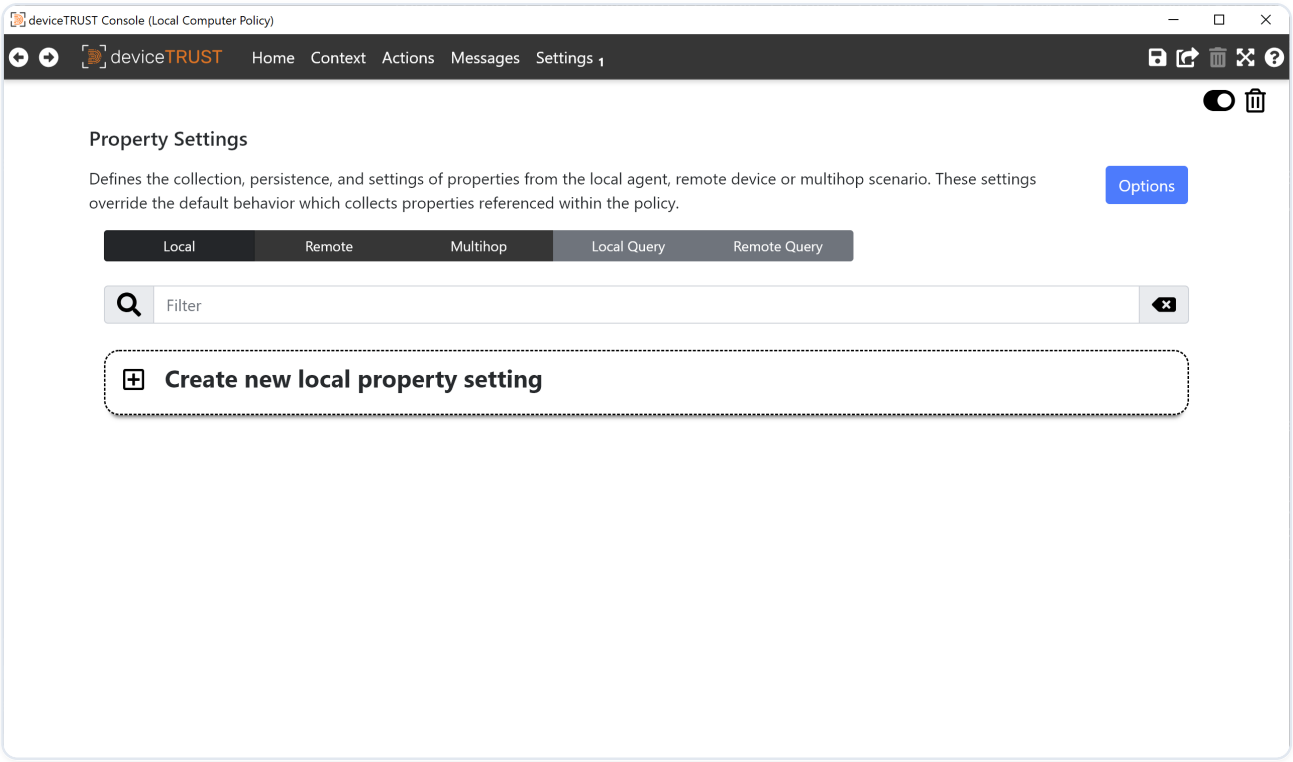
The `Printer Settings` define the printer management options and the retry and timeout settings for the Map Printer task.

© 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.

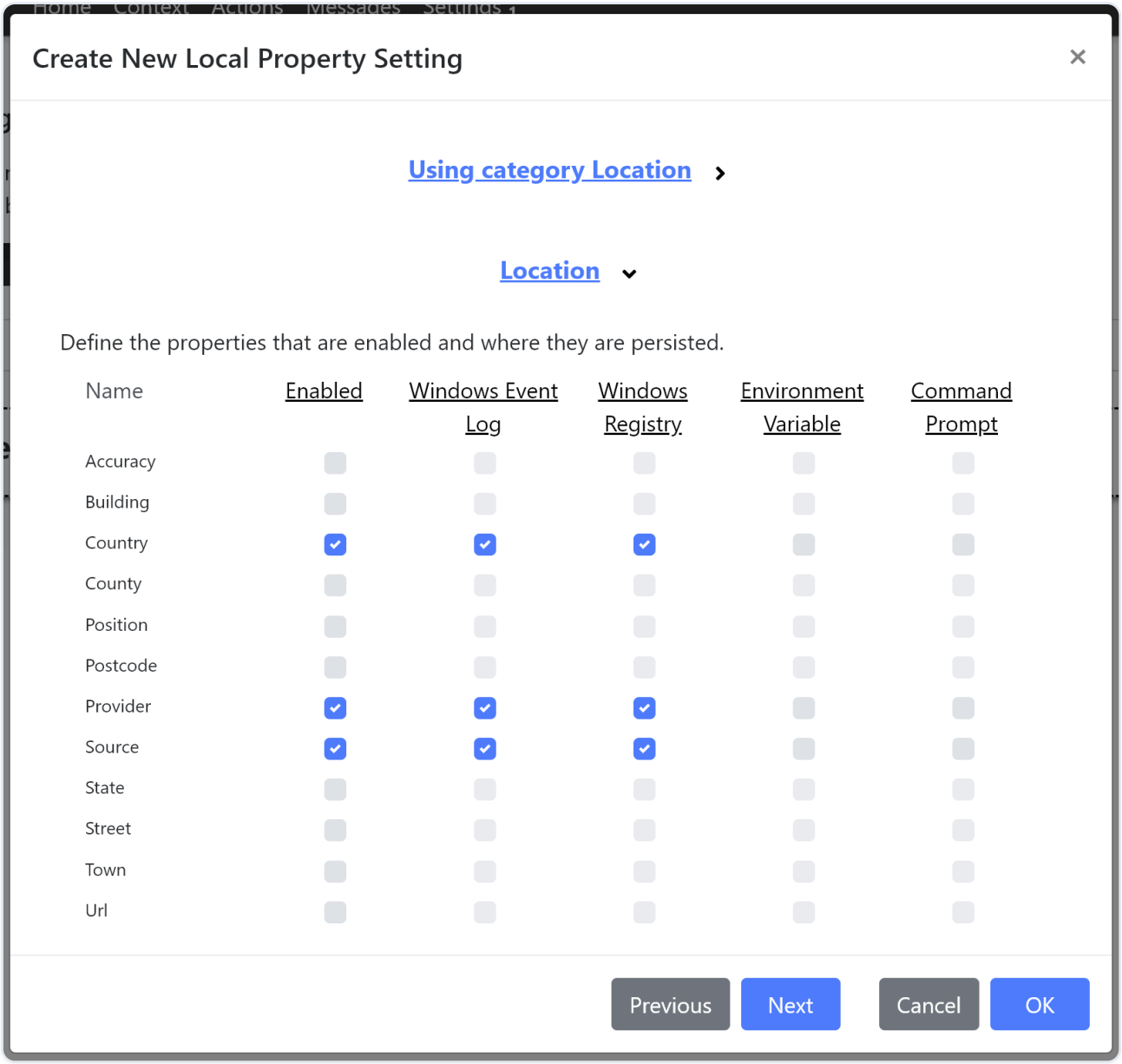


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

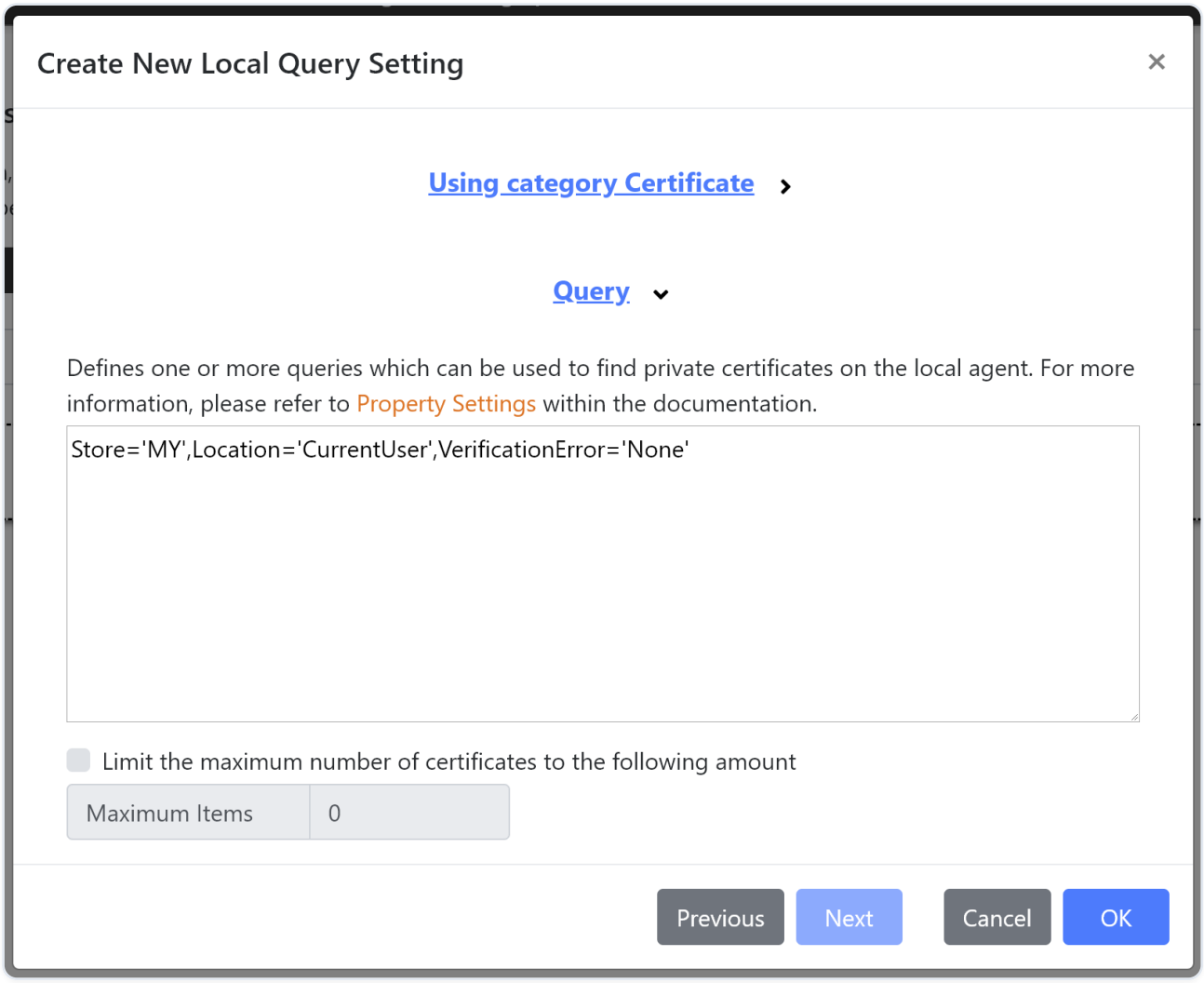
- `Enabled` - determines whether the property is collected from the device.
- `Windows Event Log` - determines whether the property is written to the Windows Event Log.
- `Windows Registry` - determines whether the property is written to the Windows Registry at `HKCU/Software/deviceTRUST/Properties`.
- `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 `http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml`.
- 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.

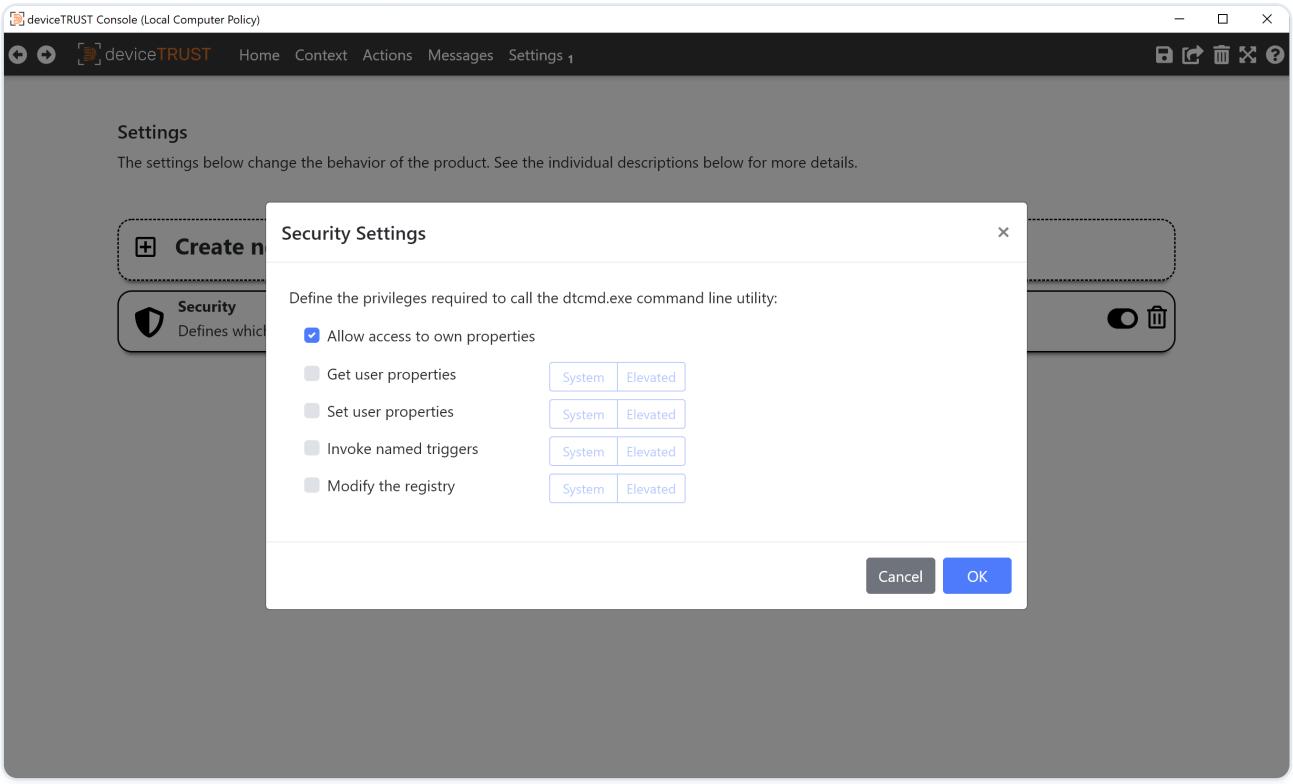
For example:

- 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

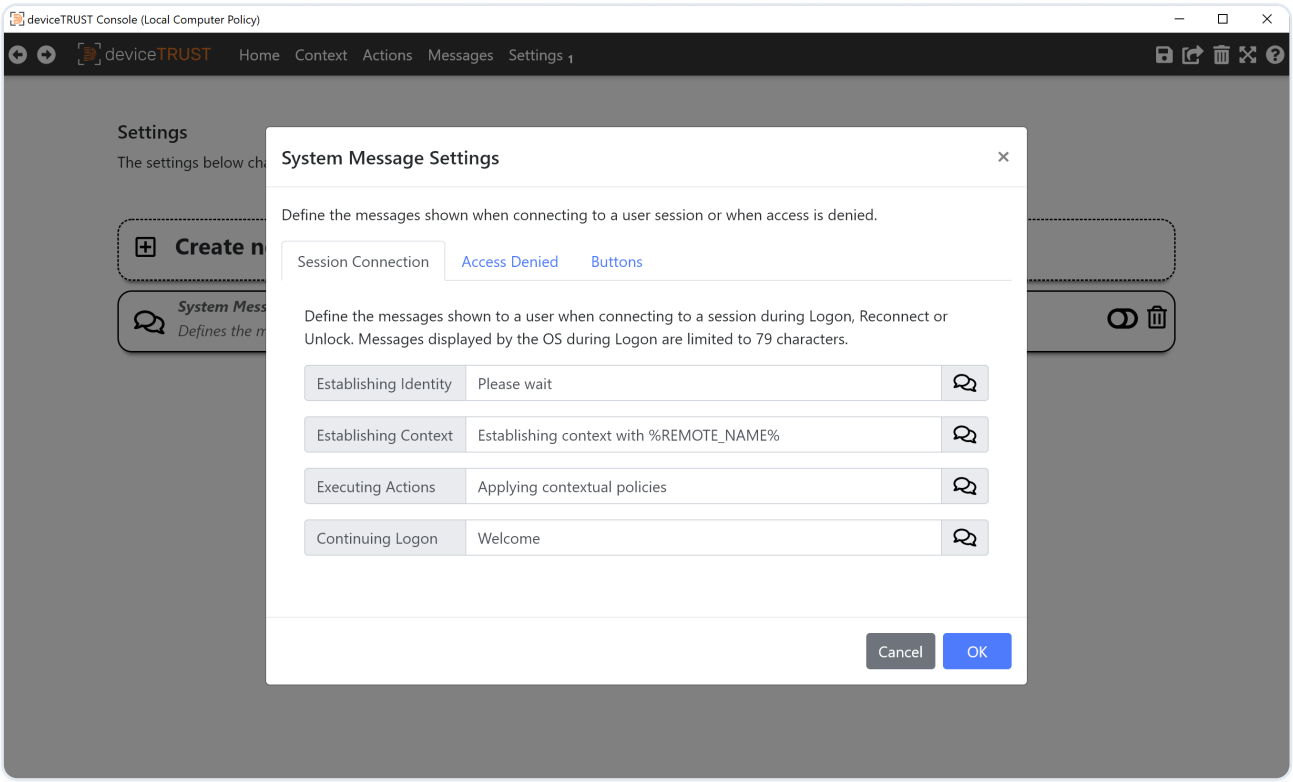
The `Security Settings` defines which external processes have permission to get or set properties, modify the registry, and invoke triggers.

© 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 PROPERTY	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	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
type. Persists as LOCAL_ACCESSPOINT_X_BSSID for the local agent and REMOTE_ACCESSPOINT_X_BSSID for the remote device.									
Count									
The number of	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
available access points. Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_COUNT for the local agent and REMOTE_ACCESSPOINT_									

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
COUNT for the remote device.									
Frequency									
The frequency of the response received from the access point, measured in kilohertz (kHz). Dynamic prope	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
rty with number data type. Persists as LOCAL_ACCESSPOINT_X_FREQUENCY for the local agent and REMOTE_ACCESSPOINT_X_FREQUENCY for the remote									

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Quality									
The link quality measured as a percentage, with 100 being the highest link quality. Dynamic property with number data type. Persists as LOC	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
AL_ACCESSPOINT_X_QUALITY for the local agent and REMOTE_ACCESSPOINT_X_QUALITY for the remote device.									
Secure									
Set to true if the access	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
point is secured. Dynamic property with boolean data type. Persists as LOCAL_ACCESSPOINT_X_SECURE for the local agent and REMOTE_ACCESSPOINT_X_SE									

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
CURE for the remote device.									
SSID									
The Service Set Identifier (SSID) of the access point. Dynamic property with text data type. Persists as LOCAL_ACCE	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
SSPOINT_X_SSID for the local agent and REMOTE_ACCESSPOINT_X_SSID for the remote device.									
Strength									
The Received Signal Strength Indicator (RSS	✓	✓							

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
I) value measured in units of decibels referenced to 1.0 milliwatts (dBm). Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_X_STRE									

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION							
NGTH for the local agent and REMOTE_ACCESSPOINT_X_STRENGTH for the remote device.									

Browser Properties

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
Describes installed	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.

BROWSER PROPERTY	AGENT	CLIENT EXTENSION						
internet browsers.							uch OS	
Count								
The number of internet browsers. Realtime property with number data type. Persists as `LOCAL_BROWSER_COUNT` for the local agent and	✓	✓						

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
`REMOTE_BROWSER_COUNT` for the remote device.									
Default									
Determines whether the browser is the default. Realtime property with boolean data type. Persists	✓	✓							

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
as `LOCAL_BROWSER_X_DEFAULT` for the local agent and `REMOTE_BROWSER_X_DEFAULT` for the remote device.									
File Path									
The file path of the internet browser	✓	✓							

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
executable. Realtime property with text data type. Persists as `LOCAL_BROWSER_X_FILEPATH` for the local agent and `REMOTE_BROWSER_X_FILEPATH` for the remote									

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Name									
The name of the internet browser. Realtime property with text data type. Persists as `LOCAL_BROWSER_X_NAME` for the local agent and `REMOTE_`	✓	✓							

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
`BROWSER_X_NAME` for the remote device.									
Version									
The version of the internet browser executable. Realtime property with text data type. Persists as `LOC`	✓	✓							

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

BROWSER PROPERTY	AGENT	CLIENT EXTENSION							
`AL_BROWSER_X_VERSION` for the local agent and `REMOTE_BROWSER_X_VERSION` for the remote device.									

Cellular Properties

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
Describes the activ	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon™ eLux

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION						
e cellular capabilities of an endpoint.	Windows	Windows					uch OS	
Class								
The cellular data class of the active connection to the network provider. Realtime property with enum, text data types	✓	✓		✓				

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
with options GPRS, EDGE, UTMS, HSDPA, HSUPA, HSPA, HSPA+, LTE, WCDMA, 1xRTT, 1xEVDO, 1xEVDV, 3xRTT, UMB, HRPD, NRNSA, NRSA. Persi									

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
sts as `LOCAL_CELLULAR_CLASS` for the local agent and `REMOTE_CELLULAR_CLASS` for the remote device.									
Country									

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
The ISO-3166 country name of the country where the connected network provider resides. This value is only available for GSM devices. Realtime property with text data	✓	✓		✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
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 PROPERTY	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	✓	✓		✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
as `LOCAL_CELLULAR_COUNTRY_CODE` for the local agent and `REMOTE_CELLULAR_COUNTRY_CODE` for the remote device.									
ID									

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION						
For GSM devices, this is the 15 digit IMEI number. For CDMA devices, this is the 11 digit ESN or the 17 digit MEID. Realtime property with text data type. Persists	✓	✓						

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
as `LOCAL_CELLULAR_ID` for the local agent and `REMOTE_CELLULAR_ID` for the remote device.									
Network Code									

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
The mobile network code (MNC) of the connected network provider. This value is only available for GSM devices. Realtime property with number data type. Persists	✓	✓		✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
as `LOCAL_CELLULAR_NETWORK_CODE` for the local agent and `REMOTE_CELLULAR_NETWORK_CODE` for the remote device.									
Network Name									
The name of the conn	✓	✓		✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
ected network provider. Realtime property with text data type. Persists as `LOCAL_CELLULAR_NETWORK` for the local agent and `REMOTE_CELLULAR_NETWORK` for the remot									

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
e device.									
Product									
The product name of the device providing the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLULAR_PROD`	✓	✓							

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
`UCT` for the local agent and `REMOTE_CELLULAR_PRODUCT` for the remote device.									
Roaming									
Determines whether the connected network provider is different to the	✓	✓							

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION
home provider defined by the SIM. Realtime property with boolean data type. Persists as `LOCAL_CELLULAR_ROAMING` for the local agent and `REMOTE_CELLULAR_ROAMING`		

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
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 PROPERTY	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_CELLULAR_TYPE` for the local agent and `REMOTE_CELLULAR_TYPE` for the remote device.									
Vendor									
The vendor name of the device provi	✓	✓							

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION
ding the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLULAR_VENDOR` for the local agent and `REMOTE_CELLULAR_VENDOR` for the		

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION							
remote device.									

Certificate Properties

CERTIFICATE	AGENT	CLIENT EXTENSION							
Describes the private certificates available within the users certificate store.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Count									
The number of install	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
ed certificates. Dynamic property with number data type. Persists as `LOCAL_CERTIFICATE_COUNT` for the local agent and `REMOTE_CERTIFICATE_COUNT` for the remote									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
device.									
Extended Usage									
The valid extended usages of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_EXTENDEDUSAGE`	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_CERTIFICATE_X_EXTENDEDUSAGE` for the remote device.									
Issuer									
The name of the certificate authority that issued the certificate. Dyna	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
mic property with text data type. Persists as `LOCAL_CERTIFICATE_X_ISSUER` for the local agent and `REMOTE_CERTIFICATE_X_ISSUER` for the remote device.									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
Location									
The location of the certificate, such as 'CurrentUser'. Dynamic property with enum data type with options Current User, Local Machine. Persists as `LOCAL_CERTI`	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`FICATE_X_LOCATION` for the local agent and `REMOTE_CERTIFICATE_X_LOCATION` for the remote device.									
Name									
The name of the certificate. Dynamic property	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_CERTIFICATE_X_NAME` for the local agent and `REMOTE_CERTIFICATE_X_NAME` for the remote device.									
Not After									
The date	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
after which the certificate expires. Dynamic property with datetime data type. Persists as `LOCAL_CERTIFICATE_X_NOTAFTER` for the local agent and `REMOTE_CERTIFICATE_X_NO`									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`TAFTER` for the remote device.									
Not Before									
The date after which the certificate becomes valid. Dynamic property with datetime data type. Persists as `LOCAL_C`	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`CERTIFICATE_X_NOTBEFORE` for the local agent and `REMOTE_CERTIFICATE_X_NOTBEFORE` for the remote device.									
Policies									
The certificate policies identifying the	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
intended purpose of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_POLICIES` for the local agent and `REMOTE_CERTIFICATE_X_POLICI`									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`ES` for the remote device.									
Root Name									
The root name of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_ROOT_NAME`	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_CERTIFICATE_X_ROOT_NAME` for the remote device.									
Root Thumbprint SHA 256									
The SHA 256 Thumbprint of the root certificate. Dynamic	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION
property with text data type. Persists as `LOCAL_CERTIFICATE_X_ROOT_THUMBPRINT_SHA256` for the local agent and `REMOTE_CERTIFICATE_X_ROOT_THUMBPRINT_SHA256` for		

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
the remote device.									
Serial Number									
The serial number of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_SERIALNUMBER` for	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_CERTIFICATE_X_SERIALNUMBER` for the remote device.									
Signature Algorithm									
The algorithm used to create the certificate. Dynamic prope	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_CERTIFICATE_X_SIGNATUREALGORITHM` for the local agent and `REMOTE_CERTIFICATE_X_SIGNATUREALGORITHM` for the remote									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
device.									
Store									
The name of the store which contains the certificate, such as 'My'. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_STORE` for	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_CERTIFICATE_X_STORE` for the remote device.									
Subject									
The subject distinguished name of the certificate. Dynamic property with text	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_CERTIFICATE_X_SUBJECT` for the local agent and `REMOTE_CERTIFICATE_X_SUBJECT` for the remote device.									
Template									
The name of the	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
template which was used to generate the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_TEMPLATE` for the local agent and `REMOTE_CERT`									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`IFICATE_X_TEMPLATE` for the remote device.									
Thumbprint SHA256									
The SHA256 Thumbprint 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_THUMBPRINT_SHA256` for the local agent and `REMOTE_CERTIFICATE_X_THUMBPRINT_SHA256` for the remote device.									
TPM Key Attestation									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
Detects the key attestation issuance policies which prove to a CA that the certificate is protected by a trusted TPM. Dynamic property with enum data type with options None	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
, User Credentials, Hardware Certificate, Hardware Key. Persists as `LOCAL_CERTIFICATE_X_TPM_KEY_ATTESTATION` for the local agent and `REMOTE_CERTIFICATE_X_TPM_KE`									

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`Y_ATTESTATION` for the remote device.									
Usage									
The valid usages of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X`	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`_USAGE` for the local agent and `REMOTE_CERTIFICATE_X_USAGE` for the remote device.									
Verification Error									
Describes why the certificate failed verification. Dyna	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
mic property with enum data type with options None, Cannot Be Verified, Revoked, Untrusted Root, Untrusted Test Root, Chaining, Wrong Usage, Expired, Invalid Name,									

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

CERTIFICATE	AGENT	CLIENT EXTENSION
Invalid Policy, Basic Constraints, Critical, Validity Period Nesting, No Revocation Check, Revocation Offline. Persists as `LOCAL_CERTIFICATE_X_VERIFIC`		

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`ATIONERROR` for the local agent and `REMOTE_CERTIFICATE_X_VERIFICATIONERROR` for the remote device.									
Version									
The x509 format version of the certificate.	✓	✓	✓						

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

CERTIFICATE	AGENT	CLIENT EXTENSION
Dynamic property 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_`		

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

CERTIFICATE	AGENT	CLIENT EXTENSION							
`X_VERSION` for the remote device.									

ChromeOS Properties

CHROMEOS	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 admi						✓			

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

CHROME OS	AGENT	CLIENT EXTENSION							
nistrator-annotated Asset Id. Static property with text data type. Persists as `REMOTE_CHROMEOS_ASSETID` for the remote device.									
Directory Device ID									
The directory						✓			

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

CHROME OS	AGENT	CLIENT EXTENSION							
device ID. Static property with text data type. Persists as `REMOTE_CHROMEOS_DIRECTORYDEVICEID` for the remote device.									
Location									
The administrator-annotated						✓			

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

CHROMEOS	AGENT	CLIENT EXTENSION							
Location. Static property with text data type. Persists as `REMOTE_CHROMEOS_LOCATION` for the remote device.									

Custom Properties

CUSTOM	AGENT	CLIENT EXTENSION							
Provides a condition	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon eLux

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

CUSTOM	AGENT	CLIENT EXTENSION							
that can operate on any property, including custom properties created using 'dtcmd.exe'.	Windows	Windows						uch OS	
Condition									
This is a placeholder custom property to allow the creation of a custo	✓	✓			✓		✓	✓	

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

CUSTOM	AGENT	CLIENT EXTENSION
m condition. This text does not appear within the console. Realtime property with text, number, boolean, datetime, ip, position data types. Persists as `LOCAL_CUSTO`		

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

CUSTOM	AGENT	CLIENT EXTENSION							
`M_CONDITION` for the local agent and `REMOTE_CUSTOM_CONDITION` for the remote device.									

deviceTRUST Properties

DEVICETRUST	AGENT	CLIENT EXTENSION							
Provides information about whether a	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							
connection to a deviceTRUST Client Extension has been established, the version of the deviceTRUST software and the status of the deviceTRUST license.									
Connected									

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

DEVICETRUST	AGENT	CLIENT EXTENSION
Determines whether the deviceTRUST Agent has established a connection with the deviceTRUST Client Extension. Static property with boolean data type. Persists as `LOC`	✓	✓

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
`AL_DEVICETRUST_CONNECTED` for the local agent.									
License Count									
Determines the number of deviceTRUST licensed units. Static property with number data type. Persi	✓	✓							

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
sts as `LOCAL_DEVICETRUST_LICENSE_COUNT` for the local agent.									
License Expiry Date									
Determines the date that the deviceTRUST license expires. Static prope	✓	✓							

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
rty with datetime data type. Persists as `LOCAL_DEVICETRUST_LICENSE_EXPIRYDATE` for the local agent.									
License Issue Date									
Determines the date that the deviceTR	✓	✓							

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
UST license was issued. Static property with datetime data type. Persists as `LOCAL_DEVICETRUST_LICENSE_ISSUEDATE` for the local agent.									
License Type									

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
Determines the deviceTRUST license type. Static property with text data type. Persists as `LOCAL_DEVICETRUST_LICENSE_TYPE` for the local agent.	✓	✓							
License Unit									

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
Determines the deviceTRUST licensable unit, e.g. a User or Device. Static property with enum data type with options User, Device, Unlimited. Persists as `LOCAL_DEVICETRUST_L`	✓	✓							

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
`LICENSE_UNIT` for the local agent.									
License Valid									
Determines whether the deviceTRUST license is valid. Static property with boolean data type. Persists as `LOCAL_D`	✓	✓							

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
`EVICETRUST_LICENSE_VALID` for the local agent.									
Version									
The version of the deviceTRUST software. Static property with version data type. Persists as `LOCAL_D`	✓	✓	✓	✓	✓		✓	✓	✓

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

DEVICETRUST	AGENT	CLIENT EXTENSION							
`EVICETRUST_VERSION` for the local agent and `REMOTE_DEVICETRUST_VERSION` for the remote device.									

Display Properties

DISPLAY	AGENT	CLIENT EXTENSION							
Describes the displays	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.

DISPLAY	AGENT	CLIENT EXTENSION						
available to the user session.							uch OS	
Adapter Product								
The product name of the display adapter. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_ADA`	✓	✓	✓					

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

DISPLAY	AGENT	CLIENT EXTENSION							
`PTER_PRODUCT` for the local agent and `REMOTE_DISPLAY_X_ADAPTER_PRODUCT` for the remote device.									
Adapter Vendor									
The vendor of the display adapter. Realti	✓	✓	✓						

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

DISPLAY	AGENT	CLIENT EXTENSION							
me property with text data type. Persists as `LOCAL_DISPLAY_X_ADAPTER_VENDOR` for the local agent and `REMOTE_DISPLAY_X_ADAPTER_VENDOR` for the remote device.									

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

DISPLAY	AGENT	CLIENT EXTENSION							
BPP									
The number of bits 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	✓	✓	✓	✓	✓		✓	✓	✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
remote device.									
Count									
The number of displays. Realtime property with number data type. Persists as `LOCAL_DISPLAY_COUNT` for the local agent and `REMOTE_`	✓	✓	✓	✓	✓		✓	✓	✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
`DISPLAY_COUNT` for the remote device.									
DPI									
The number of dots per inch. Realtime property with number data type. Persists as `LOCAL_DISPLAY_X_DPI` for	✓	✓	✓		✓		✓		✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_DISPLAY_X_DPI` for the remote device.									
Height									
The height of the screen in pixels. Realtime property with number data type. Persi	✓	✓	✓	✓	✓		✓	✓	✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
sts as `LOCAL_DISPLAY_X_HEIGHT` for the local agent and `REMOTE_DISPLAY_X_HEIGHT` for the remote device.									
Monitor External									
Set to true when the monit	✓	✓	✓						

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

DISPLAY	AGENT	CLIENT EXTENSION
or is external to the device. Realtime property with boolean data type. Persists as `LOCAL_DISPLAY_X_MONITOR_EXTERNAL` for the local agent and `REMOTE_DISPLAY_X_MONITO`		

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

DISPLAY	AGENT	CLIENT EXTENSION							
`R_EXTERNAL` for the remote device.									
Monitor Product									
The monitors product name. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X`	✓	✓	✓						

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

DISPLAY	AGENT	CLIENT EXTENSION							
`_MONITOR_PRODUCT` for the local agent and `REMOTE_DISPLAY_X_MONITOR_PRODUCT` for the remote device.									
Monitor Serial Number									
The serial number of the monitor.	✓	✓	✓						

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

DISPLAY	AGENT	CLIENT EXTENSION
Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_SERIALNUMBER` for the local agent and `REMOTE_DISPLAY_X_MONITOR_SERIALNUMBER` for the		

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

DISPLAY	AGENT	CLIENT EXTENSION							
remote device.									
Monitor Vendor									
The vendor of the monitor. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_VENDOR` for the	✓	✓	✓						

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

DISPLAY	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_DISPLAY_X_MONITOR_VENDOR` for the remote device.									
Name									
The name of the display adapter. Realtime property with text data type. Persi	✓				✓		✓	✓	✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
sts as `LOCAL_DISPLAY_X_NAME` for the local agent and `REMOTE_DISPLAY_X_NAME` for the remote device.									
Width									
The width of the screen in pixels. Realtime prope	✓	✓	✓	✓	✓		✓	✓	✓

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

DISPLAY	AGENT	CLIENT EXTENSION							
rty with number 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							
	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 number data type. Persists									✓

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

ELUX	AGENT	CLIENT EXTENSION							
as `REMOTE_ELUX_ENVIRONMENT_COUNT` for the remote device.									
Environment Variable Name									
The name of the ELUX environment variable. Static property									✓

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

ELUX	AGENT	CLIENT EXTENSION							
with text data type. Persists as `REMOTE_ELUX_ENVIRONMENT_X_NAME` for the remote device.									
Environment Variable Value									
The value of the ELUX environment									✓

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

ELUX	AGENT	CLIENT EXTENSION							
variable. Static property with text, number, boolean, datetime, ip data types. Persists as `REMOTE_ELUX_ENVIRONMENT_X_VALUE` for the remote device.									
Host ID									

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

ELUX	AGENT	CLIENT EXTENSION							
The Host ID assigned to the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_HOSTID` for the remote device.									✓
Info1									
The Info1 property of									✓

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

ELUX	AGENT	CLIENT EXTENSION							
the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_INFO1` for the remote device.									
Info2									
The Info2 property of the eLux device. Static prope									✓

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

ELUX	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `REMOTE_ELUX_INFO2` for the remote device.									
Info3									
The Info3 property of the eLux device. Static property with text data type. Persi									✓

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

ELUX	AGENT	CLIENT EXTENSION							
sts as `REMOTE_ELUX_INFO3` for the remote device.									
Organization Unit ID									
The ID property of the Organization Unit containing the eLux device. Static property									✓

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

ELUX	AGENT	CLIENT EXTENSION							
with number data type. Persists as `REMOTE_ELUX_OU_ID` for the remote device.									
Scout Cert Serial									
The serial number of the certificate used to connect to the eLux Scout									✓

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

ELUX	AGENT	CLIENT EXTENSION							
server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_SERIALNUMBER` for the remote device.									
Scout Cert Subject									
The subje									✓

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

ELUX	AGENT	CLIENT EXTENSION							
ct of the certificate used to connect to the eLux Scout server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_SUBJECT` for the remote									

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

ELUX	AGENT	CLIENT EXTENSION							
device.									
Scout Cert Thumbprint SHA 256									
The SHA 256 thumbprint of the certificate used to connect to the eLux Scout server. Static property with text data type. Persists as `REM`									✓

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

ELUX	AGENT	CLIENT EXTENSION							
`OTE_ELUX_SCOUT_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									
Scout IP									
The IP address of the eLux Scout server. Static property with text data type.									✓

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

ELUX	AGENT	CLIENT EXTENSION							
Persists as `REMOTE_ELUX_SCOUT_IP` for the remote device.									
Scout Name									
The name of the eLux Scout server. Static property with text data type. Persists as `REM`									✓

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

ELUX	AGENT	CLIENT EXTENSION							
`OTE_ELUX_SCOUT_NAME` for the remote device.									
Scout Version									
The version number of the eLux Scout server. Static property with version data type. Persists as									✓

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

ELUX	AGENT	CLIENT EXTENSION							
`REMOTE_ELUX_SCOUT_VERSION` for the remote device.									

Hardware Properties

HARDWARE	AGENT	CLIENT EXTENSION							
Describes the hardware and its capabilities.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
BIOS Rele									

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

HARDWARE	AGENT	CLIENT EXTENSION							
ase Date									
The date of release of the BIOS. Static property with datetime data type. Persists as `LOCAL_HARDWARE_BIOS_RELEASEDATE` for the local agent and `REMOTE_`	✓	✓			✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
`HARDWARE_BIOS_RELEASEDATE` for the remote device.									
BIOS Serial Number									
The serial number of the BIOS of the device. Static property with text data type. Persists	✓	✓	✓		✓	✓	✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
as `LOCAL_HARDWARE_BIOS_SERIAL` for the local agent and `REMOTE_HARDWARE_BIOS_SERIAL` for the remote device.									
BIOS Version									
The version number of the	✓	✓	✓		✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
BIOS. Static property with version data type. Persists as `LOCAL_HARDWARE_BIOS_VERSION` for the local agent and `REMOTE_HARDWARE_BIOS_VERSION` for the remote									

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

HARDWARE	AGENT	CLIENT EXTENSION							
device.									
CPU									
The CPU available on the device. Static property with text data type. Persists as `LOCAL_HARDWARE_CPU` for the local agent and `REMOTE_HARDWARE`	✓	✓	✓		✓	✓	✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
`_CPU` for the remote device.									
CPU Count									
The number of CPUs. Static property with number data type. Persists as `LOCAL_HARDWARE_CPU_COUNT` for the local	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
agent and `REMOTE_HARDWARE_CPU_COUNT` for the remote device.									
CPU Speed									
The speed of the CPU in Mhz. Static property with number data type. Persists	✓	✓	✓		✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
as `LOCAL_HARDWARE_CPU_SPEED` for the local agent and `REMOTE_HARDWARE_CPU_SPEED` for the remote device.									
Lid									
This real-time property determines if the	✓	✓	✓		✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION
lid of 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 `REM`		

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

HARDWARE	AGENT	CLIENT EXTENSION							
`OTE_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	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
local 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	✓	✓	✓		✓		✓		✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
type with options Server, Desktop, Laptop, Tablet, Virtual. Persists as `LOCAL_HARDWARE_ROLE` for the local agent and `REMOTE_HARDWARE_ROLE` for the remote									

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

HARDWARE	AGENT	CLIENT EXTENSION							
device.									
Secure Boot									
Determines if the device was booted using secure boot. Static property with boolean data type. Persists as `LOCAL_HARDWARE_SECUREBO`	✓	✓		✓	✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
`OT` for the local agent and `REMOTE_HARDWARE_SECUREBOOT` for the remote device.									
System Memory									
The amount of physical memory in MB. Static property with	✓	✓	✓	✓	✓		✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
number data type. Persists as `LOCAL_HARDWARE_SYSTEMMEMORY` for the local agent and `REMOTE_HARDWARE_SYSTEMMEMORY` for the remote device.									
Vendor									

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

HARDWARE	AGENT	CLIENT EXTENSION							
The vendor of the device. Static property with text data type. Persists as `LOCAL_HARDWARE_VENDOR` for the local agent and `REMOTE_HARDWARE_VENDOR` for the remote	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
device.									
Virtualization									
The type of virtualization used to host the device. Static property with enum data type with options None, VMware, Xen®, VirtualPC, Parall	✓	✓	✓		✓		✓		✓

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

HARDWARE	AGENT	CLIENT EXTENSION							
els, VirtualBox, 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	IGEL OS
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 COSMOS 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 COS MOS 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.									
Flags									
Flags associate	✓	✓							

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
d with the logical disk. Realtime property with flags data type with options Not Ready, Preserved Name, Case Sensitive Search, Dax Volume, Supports Compression,									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Named Streams, Persistent Acls, Read Only, Sequential Write Once, Supports Encryption, Extended Attributes, Hard Links, Object Ids, Open By File Id, Reparse Points, Spar									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
se Files, Transactions, Usn Journal, Unicode Filenames, Is Compressed, Supports Quotas. Persists as `LOCAL_LOGICALDISK_X_FLAGS` for the local agent and `REMOTE_`									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
`LOGICAL DISK _X_FLAGS` for the remote device.									
Free									
The free space as a percentage of the total space. This is only available on mounted volumes. Realtime prope	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
rty with number data type. Persists as `LOCAL_LOGICALDISK_X_FREE` for the local agent and `REMOTE_LOGICALDISK_X_FREE` for the remote device.									
Free MB									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
The free / available size in MB. This is only available on mounted volumes. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_X_FREEMB` for	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_LOGICALDISK_X_FREEMB` for the remote device.									
Hidden									
Set to true if the logical disk is hidden. Realtime property with boole	✓	✓							

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
an data type. Persists as `LOCAL_LOGICALDISK_X_HIDDEN` for the local agent and `REMOTE_LOGICALDISK_X_HIDDEN` for the remote device.									
Identity									
Enter one	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
or more vendor id, product id or serial number to identify each disk. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_IDENTITY` for the local agent and									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
`REMOTE_LOGICALDISK_X_IDENTITY` for the remote device.									
Label									
The volume label associated with the logical disk. Realtime property with text data type.	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_LOGICALDISK_X_LABEL` for the local agent and `REMOTE_LOGICALDISK_X_LABEL` for the remote device.									
Name									
The name of the logical	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION
disk as seen within Device Manager. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_NAME` for the local agent and `REMOTE_LOGICALDISK_X_NAME`		

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
for the remote device.									
Path									
The path where the disk is mounted. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_PATH` for the local	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
agent and `REMOTE_LOGICALDISK_X_PATH` for the remote device.									
Product Id									
For USB connected disks, this is the USB product id. For PCI connected disks, this is the devic	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION
e id. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_PRODUCT_ID` for the local agent and `REMOTE_LOGICALDISK_X_PRODUCT_ID` for the remote		

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
device.									
Serial Number									
The serial number of the physical disk. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_SERIALNUMBER` for the local	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
agent and `REMOTE_LOGICALDISK_X_SERIALNUMBER` for the remote device.									
System									
Determines whether the disk is the system drive, i.e. if it contains the	✓	✓	✓						

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

LOGICAL DISK	AGENT	CLIENT EXTENSION
Operating System installation. Realtime property with boolean data type. Persists as `LOCAL_LOGICALDISK_X_SYSTEM` for the local agent and `REMOTE_LOGICALDISK_X_SYSTEM`		

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
for the remote device.									
Total MB									
The total size in MB of the logical disk. This is only available on mounted volumes. Realtime property with number data type. Persi	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
sts as `LOCAL_LOGICALDISK_X_TOTALMB` for the local agent and `REMOTE_LOGICALDISK_X_TOTALMB` for the remote device.									
Type									
The type of the logical disk, such	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
as Fixed, Removable, or Portable Device. Realtime property with enum data type with options Unknown, No Root Directory, Removable, Fixed, Remote, Cdrom, RAM									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
Disk, Portable Device. Persists as `LOCAL_LOGICALDISK_X_TYPE` for the local agent and `REMOTE_LOGICALDISK_X_TYPE` for the remote device.									
Vendor Id									

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
The vendor id of the logical disk for USB or PCI connected disks. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_VENDOR_ID` for the local agent	✓	✓	✓		✓		✓	✓	✓

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

LOGICAL DISK	AGENT	CLIENT EXTENSION							
and `REMOTE_LOGICALDISK_X_VENDOR_ID` for the remote device.									
Volume Id									
The id of the volume. Realtime property with text data type. Persists as `LOCAL_L`	✓	✓			✓		✓		

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

LOGICAL DISK	AGENT	CLIENT EXTENSION
`OGICALDISK_X_VOLUME_ID` for the local agent and `REMOTE_LOGICALDISK_X_VOLUME_ID` for the remote device.		

macOS Properties

MAC OS	AGENT	CLIENT EXTENSION							
Describes prope	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk	Unicon™ eLux

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

MAC OS	AGENT	CLIENT EXTENSION							
rties unique to an Apple mac OS endpoint	Windows	Windows						NoTouch OS	
Gatekeeper									
Determines the Gatekeeper setting which defines the trust level of software that can run on the Mac. Static			✓						

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

MAC OS	AGENT	CLIENT EXTENSION							
property with enum data type with options Anywhere, App Store and Identified Developers, App Store. Persists as `REMOTE_MACOS_GATEKEEPER` for the remote device.									

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

MAC OS	AGENT	CLIENT EXTENSION							
iCloud Account									
The iCloud account associated with the logged in user. Static property with text data type. Persists as `REMOTE_MACOS_ICLOUD_ACCOUNT` for the			✓						

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

MAC OS	AGENT	CLIENT EXTENSION						
remote device.								
Secure Virtual Memory								
Determines whether the swap file is encrypted. Static property with boolean data type. Persists as `REMOTE_MACOS_SECURE`			✓					

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

MAC OS	AGENT	CLIENT EXTENSION							
`VIRTUAL MEMORY` for the remote device.									
System Integrity Protection									
Determines whether System Integrity Protection is enabled, which helps protect Mac users			✓						

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

MAC OS	AGENT	CLIENT EXTENSION							
from malicious software. Static property with boolean data type. Persists as `REMOTE_MACOS_SYSTEM INTEGRITYPROTECTION` for the remote device.									

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

macOS Firewall Properties

MACOS FIREWALL	AGENT	CLIENT EXTENSION							
Provides real-time properties describing the state of the macOS Firewall	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Allow Signed Downloaded Inbound									
Determines whether the firewall is configured			✓						

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
to allow signed downloaded software to receive inbound connections. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_ALLOWSIGNEDDOW`									

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
`NLOADINBOUND` for the remote device.									
Allow Signed Inbound									
Determines whether the firewall is configured to allow built in software to receive inbound connectio			✓						

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
ns. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_ALLOWSIGNEDINBOUND` for the remote device.									
Block All Inbound									
Determine			✓						

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
s whether the firewall is configured to block all inbound connection. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_BLOCKALLINBOUN`									

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION						
`D` for the remote device.								
Enabled								
Determines whether the firewall is enabled. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIR`			✓					

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
`EWALL_ENABLED` for the remote device.									
Inbound Program Rules									
The firewall rules configured to allow programs to receive inbound connections. Dynamic prope			✓						

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `REMOTE_MACOSFIREWALL_INBOUNDRULES_PROGRAMS` for the remote device.									
Stealth Mode			✓						
Determines whether the firew			✓						

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

MAC OS FIREWALL	AGENT	CLIENT EXTENSION							
all is configured to ignore ICMP packets. Dynamic property with boolean data type. Persists as `REMOTE_MACOSFIREWALL_STEALTHMODE` for the remote device.									

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

macOS Update

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Describes the status of macOS Software Update settings and updates.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Auto Check For 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 check for updates. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_CHECK` for the remote device.									
Auto Download									

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

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Updates								
Set to true when mac OS is configured to automatically download updates. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_`			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
`AUTO_DOWNLOAD` for the remote device.								
Auto Install App Store Updates								
Set to true when macOS is configured to automatically install App Store updates. Realti			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
me property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_INSTALL_APPSTORE` for the remote device.									
Auto Install Data Updates									

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

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Set to true when mac OS is configured to automatically install system data files. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO`			✓						

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

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`_INSTALL_DATA` for the remote device.									
Auto Install macOS Updates									
Set to true when macOS is configured to automatically install macOS updates.			✓						

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_AUTO_INSTALL_MACOS` for the remote device.									
Auto Install Security									

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

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Updates								
Set to true when mac OS is configured to automatically install security updates. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPD`			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
`ATE_AUTO_INSTALL_SECURITY` for the remote device.								
Enabled								
Determines whether the Software Update service is running and the last attempt to			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
update was successful. Realtime property with boolean data type. Persists as `REMOTE_MACOSUPDATE_ENABLED` for the remote device.									
Ignore									

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
Update								
The name of any updates that are not to be installed. Realtime property with text data type. Persists as `REMOTE_MACOSUPDATE_IGNOREUPDATE` for the			✓					

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

MAC OS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
remote device.								
Last Search								
The time that the Software Update service last checked for updates. Realtime property with datetime data type. Persists			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
as `REMOTE_MACOSUPDATE_LASTSEARCH` for the remote device.								
Update Count								
The number of updates that are waiting to be installed. Realtime prope			✓					

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
rty with number data type. Persists as `REMOTE_MACOSUPDATE_UPDATE_COUNT` for the remote device.									
Update Name									
The name of the update that is waitin			✓						

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
g to be installed. Realtime property with text data type. Persists as `REMOTE_MACOSUPDATE_UPDATE_X_NAME` for the remote device.									
Update Product Key									

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION						
The product key of the update that is waiting to be installed. Realtime property with text data type. Persists as `REMOTE_MACOSUPDATE_UPDATE_X_PRODUCTKEY` for			✓						

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
the remote device.									
Update Version									
The version of the update that is waiting to be installed. Realtime property with version data type. Persists as `REM`			✓						

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`OTE_MACOSUPDATE_UPDATE_X_VERSION` for the remote device.									
Version									
The version number of the Software Update service that last checked for updat			✓						

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

MACOS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
es. Realtime property with version data type. Persists as `REMOTE_MACOSUPDATE_VERSION` for the remote device.									

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

Mapped Drive Properties

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
Describes the mapped drives available within a user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Count									
The number of mapped drives available. Dynamic property with number data	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_MAPPEDDRIVE_COUNT` for the local agent and `REMOTE_MAPPEDDRIVE_COUNT` for the remote device.									
Drive									
The drive where the mapped drive	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
is mounted. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X_DRIVE` for the local agent and `REMOTE_MAPPEDDRIVE_X_DRIVE` for the remote									

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
device.									
Hidden									
Set to true if the mapped drive is hidden. Dynamic property with boolean data type. Persists as `LOCAL_MAPPEDDRIVE_X_HIDDEN` for the	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_MAPPEDDRIVE_X_HIDDEN` for the remote device.									
Provider									
The provider of the mapped drive. Dynamic property with text data type. Persists	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
as `LOCAL_MAPPEDDRIVE_X_PROVIDER` for the local agent and `REMOTE_MAPPEDDRIVE_X_PROVIDER` for the remote device.									
Server									
The name of the remote serve	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
r. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X_SERVER` for the local agent and `REMOTE_MAPPEDDRIVE_X_SERVER` for the remote device.									

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
Share									
The name of the share on the remote server. Dynamic property with text data type. Persists as `LOCAL_MAPPEDDRIVE_X_SHARE` for the local agent and `REM`	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
`OTE_MAPPEDDRIVE_X_SHARE` for the remote device.									
User									
The name of the user authenticating the connection to the remote server. Dynamic property with text	✓	✓							

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

MAPPED DRIVE	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_MAPPEDDRIVE_X_USER` for the local agent and `REMOTE_MAPPEDDRIVE_X_USER` for the remote device.									

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

MDM Properties

MDM	AGENT	CLIENT EXTENSION							
Provides dynamic properties describing the current mobile device management (MDM) solution.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Identifier									
Identifies the MDM provider. Static property	✓	✓	✓						

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

MDM	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_MDM_IDENTIFIER` for the local agent and `REMOTE_MDM_IDENTIFIER` for the remote device.									
Managed									
Set to true when	✓	✓	✓						

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

MDM	AGENT	CLIENT EXTENSION							
the device is managed by an MDM provider. Static property with boolean data type. Persists as `LOCAL_MDM_MANAGED` for the local agent and `REMOTE_MDM_MANAGED` for the									

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

MDM	AGENT	CLIENT EXTENSION							
remote device.									
Microsoft Intune Account ID									
For Microsoft Intune managed devices, this uniquely identifies the Intune instance. Static property with text data	✓	✓	✓						

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

MDM	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_MDM_INTUNE_ACCOUNTID` for the local agent and `REMOTE_MDM_INTUNE_ACCOUNTID` for the remote device.									
Microsoft Intune Device ID									

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

MDM	AGENT	CLIENT EXTENSION							
For Microsoft Intune managed devices, this uniquely identifies the device. Static property with text data type. Persists as `LOCAL_MDM_INTUNE_DEVICEID` for the local	✓	✓	✓						

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

MDM	AGENT	CLIENT EXTENSION							
agent and `REMOTE_MDM_INTUNE_DEVICEID` for the remote device.									

Multihop Properties

MULTIHOP	AGENT	CLIENT EXTENSION							
Describes the number of hops taken by the user over 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.

MULTIHOP	AGENT	CLIENT EXTENSION							
UST connected sessions..									
Count									
The number of multihop properties. Static property with number data type. Persists as undefined.		✓							

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

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 Directory. Static property with text data type. Persists as `LOCAL_N`	✓	✓	✓						

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

NAME	AGENT	CLIENT EXTENSION							
`AME_DN` for the local agent and `REMOTE_NAME_DN` for the remote device.									
DNS									
The DNS name of the device. Static property with text data type. Persists as `LOC`	✓	✓	✓		✓		✓	✓	✓

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

NAME	AGENT	CLIENT EXTENSION							
`AL_NAME_DNS` for the local agent and `REMOTE_NAME_DNS` for the remote device.									
ID									
An arbitrary identifier that uniquely identifies the endpoint. Static property	✓	✓	✓	✓	✓		✓	✓	✓

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

NAME	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_ID` for the local agent and `REMOTE_ID` for the remote device.									
Name									
The name of the device. Static property with text	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

NAME	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_NAME` for the local agent and `REMOTE_NAME` for the remote device.									
SID									
The SID of the device within Active Directory. Static prope	✓	✓	✓						

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

NAME	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_NAME_SID` for the local agent and `REMOTE_NAME_SID` for the remote device.									

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

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 Domain depending upon the OS categorisation of	✓	✓							

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

NETWORK	AGENT	CLIENT EXTENSION							
the network. Dynamic property with enum data type with options Public, Private, Domain. Persists as `LOCAL_NETWORK_X_CATEGORY` for the local agent and `REMOTE_NETW`									

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

NETWORK	AGENT	CLIENT EXTENSION							
`ORK_X_CATEGORY` for the remote device.									
Count									
The number of network adapters. Dynamic property with number data type. Persists as `LOCAL_NETWORK_C`	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`COUNT` for the local agent and `REMOTE_NETWORK_COUNT` for the remote device.									
Description									
The description of the network adapter. Dynamic property with text data	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_NETWORK_X_DESCRIPTION` for the local agent and `REMOTE_NETWORK_X_DESCRIPTION` for the remote device.									
DHCP Enabled									
Set to	✓	✓	✓		✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
true when the network adapter is configured to use DHCP. Dynamic property with boolean data type. Persists as `LOCAL_NETWORK_X_DHCP_ENABLED` for the local agent and									

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

NETWORK	AGENT	CLIENT EXTENSION							
`REMOTE_NETWORK_X_DHCP_ENABLED` for the remote device.									
DHCP Expires									
The time that the IP address expires. Dynamic property with datetime data	✓	✓			✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_NETWORK_X_DHCP_EXPIRES` for the local agent and `REMOTE_NETWORK_X_DHCP_EXPIRES` for the remote device.									
DHCP Lease									

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

NETWORK	AGENT	CLIENT EXTENSION							
The lease time of the IP address. Dynamic property with datetime data type. Persists as `LOCAL_NETWORK_X_DHCP_LEASE` for the local agent and `REMOTE_NETWORK_X_DHCP_L`	✓	✓			✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`EASE` for the remote device.									
DHCP Server									
The IP address of the DHCP server. Dynamic property with ip, text data types. Persists as `LOCAL_NETWO`	✓	✓	✓		✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`RK_X_DHCP_SERVER` for the local agent and `REMOTE_NETWORK_X_DHCP_SERVER` for the remote device.									
DNS									
The IP address of the DNS server. Dynamic property	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
with ip, text data types. Persists as `LOCAL_NETWORK_X_DNS` for the local agent and `REMOTE_NETWORK_X_DNS` for the remote device.									
DNS Suffix									
The DNS suffix	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
es. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_DNS_SUFFIX` for the local agent and `REMOTE_NETWORK_X_DNS_SUFFIX` for the remote device.									

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

NETWORK	AGENT	CLIENT EXTENSION							
Gateway									
The IP address of the gateway. Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_X_GATEWAY` for the local agent and `REMOTE_NETW`	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`ORK_X_GATEWAY` for the remote device.									
Gateway MAC									
The MAC address of the gateway. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X`	✓	✓	✓		✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`_GATEWAY_MAC` for the local agent and `REMOTE_NETWORK_X_GATEWAY_MAC` for the remote device.									
IPv4 Address									
The IPv4 address of the network adapter. Dynamic	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
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.									
IPv4 Subnet									

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

NETWORK	AGENT	CLIENT EXTENSION							
The IPv4 subnet of the network adapter. Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_X_IPV4_SUBNET` for the local agent and `REMOTE_NETW`	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`ORK_X_IPV4_SUBNET` for the remote device.									
IPv6 Address									
The IPv6 address of the network adapter. Dynamic property with ip, text data types. Persists as	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`LOCAL_NETWORK_X_IPV6` for the local agent and `REMOTE_NETWORK_X_IPV6` for the remote device.									
IPv6 Subnet									
The IPv6 subnet of the network adapter. Dyna	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
mic property with ip, text data types. Persists as `LOCAL_NETWORK_X_IPV6_SUBNET` for the local agent and `REMOTE_NETWORK_X_IPV6_SUBNET` 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.									
Name									
The name of the network adapter. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X`	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
`_NAME` for the local agent and `REMOTE_NETWORK_X_NAME` for the remote device.									
Speed									
The speed of the network adapter. Dynamic property with numb	✓	✓			✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
er data type. Persists as `LOCAL_NETWORK_X_SPEED` for the local agent and `REMOTE_NETWORK_X_SPEED` for the remote device.									
Status									
The status of the	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
network adapter. Dynamic property with enum data type with options Up, Down, Unknown. Persists as `LOCAL_NETWORK_X_STATUS` for the local agent and `REMOTE_NETW`									

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

NETWORK	AGENT	CLIENT EXTENSION							
`ORK_X_STATUS` for the remote device.									
Type									
The type of network adapter, such as Ethernet or Wi-Fi. Dynamic property with enum data type with options Other,	✓	✓	✓	✓	✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
Ethernet, PPP, ATM, Wi-Fi, Tunnel, Firewire, Cellular. Persists as `LOCAL_NETWORK_X_TYPE` for the local agent and `REMOTE_NETWORK_X_TYPE` for the remote device.									

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

NETWORK	AGENT	CLIENT EXTENSION							
Virtual									
Set to true when the network adapter is not supported by a physical device. Dynamic property with boolean data type. Persists as `LOCAL_NETWORK_X_VIR`	✓	✓	✓		✓		✓		

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

NETWORK	AGENT	CLIENT EXTENSION							
`TUAL` for the local agent and `REMOTE_NETWORK_X_VIRTUAL` for the remote device.									
Wi-Fi BSSID									
For Wi-Fi network adapters, the BSSID of the connected access	✓	✓	✓		✓		✓		✓

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

NETWORK	AGENT	CLIENT EXTENSION							
point. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_WIFI_BSSID` for the local agent and `REMOTE_NETWORK_X_WIFI_BSSID` for the remote device.									

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

NETWORK	AGENT	CLIENT EXTENSION							
Wi-Fi Security									
The security used to authenticate and encrypt the data over the Wi-Fi network adapter. Dynamic property with enum, text data types with options Open, Enha	✓	✓	✓		✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION
nced Open, WEP, WPA Personal, WPA Enterprise, WPA 2 Personal, WPA 2 Enterprise, WPA 3 Personal, WPA 3 Enterprise. Persists as `LOCAL_NETWORK_X_WIFI_SECURITY`		

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

NETWORK	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_NETWORK_X_WIFI_SECURITY` for the remote device.									
Wi-Fi SSID									
For Wi-Fi network adapters, the SSID of any connected networks.	✓	✓	✓		✓		✓		✓

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

NETWORK	AGENT	CLIENT EXTENSION							
Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_WIFI_SSID` for the local agent and `REMOTE_NETWORK_X_WIFI_SSID` for the remote device.									

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

NETWORK	AGENT	CLIENT EXTENSION							
Wi-Fi Strength									
The signal strength of the Wi-Fi network adapter. Dynamic property with number data type. Persists as `LOCAL_NETWORK_X_WIFI_STRENGTH` for the	✓	✓	✓		✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_NETWORK_WIFI_STRENGTH` for the remote device.									
WINS									
The IP address of the WINS server. Dynamic property with ip, text	✓	✓			✓		✓	✓	✓

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

NETWORK	AGENT	CLIENT EXTENSION							
data types. Persists as `LOCAL_NETWORK_X_WINS` for the local agent and `REMOTE_NETWORK_X_WINS` for the remote device.									

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

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 Count									
The number of NoTouch Center environment variables. Static								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
property with number data type. Persists as `REMOTE_NOTOUCH_ENVIRONMENT_COUNT` for the remote device.									
Environment Variable Name									
The name of the NoTo								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION
uch Center environment variable. Static property with text data type. Persists as `REMOTE_NOTOUCH_ENVIRONMENT_X_NAME` for the remote device.		
Environment		

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

NOTOUCH	AGENT	CLIENT EXTENSION							
Variable Value									
The value of the NoTouch Center environment variable. Static property with text, number, boolean, datetime, ip data types. Persists as `REMOTE_NOTO`								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
`UCH_ENVIRONMENT_X_VALUE` for the remote device.									
NoTouch Center Cert Serial									
The serial number of the certificate used to connect to the NoTouch Center. Static								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `REMOTE_NOTOUCH_CERTIFICATE_SERIALNUMBER` for the remote device.									
NoTouch Center Cert Subject									
The subject of								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
the certificate used to connect to the NoTouch Center. Static property with text data type. Persists as `REMOTE_NOTOUCH_CERTIFICATE_SUBJECT` for the remote device.									

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

NOTOUCH	AGENT	CLIENT EXTENSION							
NoTouch Center Cert Thumbprint SHA 256									
The SHA 256 thumbprint of the certificate used to connect to the NoTouch Center. Static property with text data type. Persists as								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
`REMOTE_NOTOUCH_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.									
NoTouch Center URL									
The Management URL of the NoTouch Center. Static property								✓	

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

NOTOUCH	AGENT	CLIENT EXTENSION							
with text data type. Persists as `REMOTE_NOTOUCH_URL` for the remote device.									

OS Properties

OS	AGENT	CLIENT EXTENSION							
Provides information about the operating syste	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.

OS	AGENT	CLIENT EXTENSION							
m installed on the endpoint.									
Description									
A textual description of the OS. Static property with text data type. Persists as `LOCAL_OS_DESCRIPTION` for the local agent	✓	✓		✓	✓		✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
and `REMOTE_OS_DESCRIPTION` for the remote device.									
Id									
An arbitrary identifier that uniquely identifies the installation of the OS. Static property with text data	✓	✓	✓		✓		✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_OS_ID` for the local agent and `REMOTE_OS_ID` for the remote device.									
Name									
The name of the OS. Static property with enum data type with	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION
options Windows, macOS, iOS, IGEL, eLux®, Rangee, Linux, ChromeOS, NoTouch. Persists as `LOCAL_OS_NAME` for the local agent and `REMOTE_OS_NAME` for the		

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

OS	AGENT	CLIENT EXTENSION							
remote device.									
Platform									
The platform of the OS, such as x64. Static property with enum data type with options x86, x64, ARM, ARM64, MIPS, MIPS64. Persists as	✓	✓	✓	✓	✓		✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
`LOCAL_OS_PLATFORM` for the local agent and `REMOTE_OS_PLATFORM` for the remote device.									
Release									
The release version of the OS. Static property with text,	✓	✓			✓		✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
number data types. Persists as `LOCAL_OS_RELEASE` for the local agent and `REMOTE_OS_RELEASE` for the remote device.									
Start up Time									
The time that the	✓	✓			✓		✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
OS started. Static property with datetime data type. Persists as `LOCAL_OS_STARTUPTIME` for the local agent and `REMOTE_OS_STARTUPTIME` for the remote device.									

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

OS	AGENT	CLIENT EXTENSION							
Type									
The type of the OS, such as Client or Server. Static property with enum data type with options Client, Server. Persists as `LOCAL_OS_TYPE` for the local agent	✓	✓			✓	✓	✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
and `REMOTE_OS_TYPE` for the remote device.									
Version									
The version number of the OS. Static property with version data type. Persists as `LOCAL_OS_VERSIO`	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

OS	AGENT	CLIENT EXTENSION							
`N` for the local agent and `REMOTE_OS_VERSION` for the remote device.									

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

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
Force Logoff									
The amount of time in days between the end of the valid logon time and the time when the user is forced to log off the network. Dynamic property with	✓	✓							

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
text data type. Persists as `LOCAL_POLICY_PASSWORD_FORCELOGOFF` for the local agent and `REMOTE_POLICY_PASSWORD_FORCELOGOFF` for the remote device.									

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
Maximum Password Age									
The maximum period of time in days before the system requires the user to change it. Dynamic property with text data type. Persists as `LOC`	✓	✓							

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
`AL_POLICY_PASSWORD_MAXAGE` for the local agent and `REMOTE_POLICY_PASSWORD_MAXAGE` for the remote device.									
Minimum Password Age									
The minimum perio	✓	✓							

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
d of time in days before the system can require the user to change it. Dynamic property with number data type. Persists as `LOCAL_POLICY_PASSWORD_MINAGE` for the local									

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
agent and `REMOTE_POLICY_PASSWORD_MINAGE` for the remote device.									
Minimum Password Length									
The minimum number of characters required. Dynamic property	✓	✓							

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_POLICY_PASSWORD_MINLENGTH` for the local agent and `REMOTE_POLICY_PASSWORD_MINLENGTH` for the remote device.									
Password									

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
History									
The number of unique passwords associated with the user before an old password can be reused. Dynamic property with text data type. Persists as	✓	✓							

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

PASSWORD POLICY	AGENT	CLIENT EXTENSION							
`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 support Console, RDP, ICA®, Nice DCV, PCoIP, Blast	✓	✓					✓		

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
and for IGEL clients we also support VNC. On an IGEL device, this is set to 'VNC' whilst remote shadowing is active. Dynamic property with enum data type with options Unkn									

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
own, RDP, ICA, PCoIP, Blast, VNC, DCV. Persists as `LOCAL_REMOTECONTROL_PROTOCOL` for the local agent and `REMOTE_REMOTECONTROL_PROTOCOL` for the remote device.									

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
Remote Install Path									
The installation path of the remote client. Supported on Citrix only. Dynamic property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_`	✓	✓							

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
`INSTALLPATH` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_INSTALLPATH` for the remote device.									
Remote IP									
The IP address of the remote user.	✓	✓							

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
Dynamic property with ip, text data types. Persists as `LOCAL_REMOTECONTROL_REMOTE_IP` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_IP` for the remot									

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
e device.									
Remote Name									
The NetBIOS name of the remote device. Dynamic property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_NAME`	✓	✓							

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_REMOTECONTROL_REMOTE_NAME` for the remote device.									
Remote Platform									
The platform of the remote client. Dynamic property	✓	✓							

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

REMOTE CONTROL	AGENT	CLIENT EXTENSION							
with 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	CLIENTEXTENSION							
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.									

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

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.

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	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
the current connection to the user session. Static property with text data type. Persists as `LOCAL_SESSION_CONNECT_ID` for the local agent.									
Connect Time									

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

SESSION	AGENT	CLIENT EXTENSION							
The time the session connected. Static property with datetime data type. Persists as `LOCAL_SESSION_CONNECT_TIME` for the local agent.	✓	✓							
Delivery Name									

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

SESSION	AGENT	CLIENT EXTENSION							
Set to a semi-colon separated list of published applications when the delivery type is Application, or the name of the published desktop when delivery type is Desktop. Static prope	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_SESSION_DELIVERY_NAME` for the local agent.									
Delivery Type									
Set to Application when the session contains one	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
or more published application, or Desktop when the session is a published desktop. Static property with enum data type with options Unknown, Desktop, Application. Persists									

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

SESSION	AGENT	CLIENT EXTENSION							
as `LOCAL_SESSION_DELIVERY_TYPE` for the local agent.									
Id									
The session id of the user as assigned by the operating system. Static property with number data	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_SESSION_ID` for the local agent.									
Idle Period									
The time period in minutes that the user session has been idle. Realtime property with numb	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
er data type. Persists as `LOCAL_SESSION_IDLEPERIOD` for the local agent and `REMOTE_SESSION_IDLEPERIOD` for the remote device.									
Logon Id									
Uniquely identi	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
fies the logon session of the user. Static property with text data type. Persists as `LOCAL_SESSION_LOGON_ID` for the local agent.									
Logon Time									
The time of the sessi	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
on logon. Static property with datetime data type. Persists as `LOCAL_SESSION_LOGON_TIME` for the local agent.									
Time									
The current session time. Static property	✓	✓							

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

SESSION	AGENT	CLIENT EXTENSION							
with datetime data type. Persists as `LOCAL_SESSION_TIME` for the local agent.									

Smartcard Reader Properties

SMARTCARD READER	AGENT	CLIENT EXTENSION							
Describes the connected smart-card readers avail	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.

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
able to the user.									
Count									
The number of smart card readers connected. Dynamic property with number data type. Persists as `LOCAL_SMARTCARDREADER_COUNT` for	✓	✓			✓		✓	✓	✓

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

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
the local agent and `REMOTE_SMARTCARDREADER_COUNT` for the remote device.									
Name									
The name of the smart card reader. Dynamic property with text data type. Persi	✓	✓			✓		✓	✓	✓

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

SMARTCARDREADER	AGENT	CLIENTEXTENSION							
sts as `LOCAL_SMARTCARDREADER_X_NAME` for the local agent and `REMOTE_SMARTCARDREADER_X_NAME` for the remote device.									

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

User Properties

USER	AGENT	CLIENT EXTENSION							
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									
The number of user attributes read from Active Directory. Static property with number data type. Persists as	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
`LOCAL_USER_ATTRIBUTE_COUNT` for the local agent and `REMOTE_USER_ATTRIBUTE_COUNT` for the remote device.									
Attribute Name									
The name of a user attribute	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
read from Active Directory. Static property with text data type. Persists as `LOCAL_USER_ATTRIBUTE_X_NAME` for the local agent and `REMOTE_USER_ATTRIBUTE_X_NAME` for the									

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

USER	AGENT	CLIENT EXTENSION							
remote device.									
Attribute Value									
The value of a user attribute read from Active Directory. Static property with text, number, boolean, datetime data types. Persists as	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
`LOCAL_USER_ATTRIBUTE_X_VALUE` for the local agent and `REMOTE_USER_ATTRIBUTE_X_VALUE` for the remote device.									
Auth									
The authentication used to authenticat	✓	✓	✓						

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

USER	AGENT	CLIENT EXTENSION							
e the user. Static property with text data type. Persists as `LOCAL_USER_AUTH` for the local agent and `REMOTE_USER_AUTH` for the remote device.									
Auth Principal									

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

USER	AGENT	CLIENT EXTENSION						
The internet provider specified principal name of the user. Static property with text data type. Persists as `LOCAL_USER_AUTH_PRINCIPAL` for the local agent and `REMOTE_USER`	✓	✓						

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

USER	AGENT	CLIENT EXTENSION							
`_AUTH_PRINCIPAL` for the remote device.									
Auth Provider									
The internet provider. Static property with text data type. Persists as `LOCAL_USER_AUTH_PROVIDER` for	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_USER_AUTH_PROVIDER` for the remote device.									
Cached Credentials									
Set to true whenever the user has cached credentials.	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
Static property with boolean data type. Persists as `LOCAL_USER_CACHEDCREDENTIALS` for the local agent and `REMOTE_USER_CACHEDCREDENTIALS` for the remote device.									

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

USER	AGENT	CLIENT EXTENSION							
DN									
The distinguished name of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DN` for the local agent and `REMOTE_USER_NAME_DN` for the remot	✓	✓	✓						

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

USER	AGENT	CLIENT EXTENSION							
e device.									
DNS									
The domain DNS of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DOMAIN_DNS` for the local agent and `REMOTE_USER`	✓	✓	✓		✓		✓	✓	✓

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

USER	AGENT	CLIENT EXTENSION							
`_NAME_DOMAIN_DNS` for the remote device.									
Domain									
The domain of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DOMAIN` for the	✓	✓	✓		✓		✓	✓	✓

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

USER	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_USER_NAME_DOMAIN` for the remote device.									
Domain Logon									
Set to true whenever the user belongs to a domain. Static property with	✓	✓	✓		✓		✓	✓	✓

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

USER	AGENT	CLIENT EXTENSION							
boolean data type. Persists as `LOCAL_USER_DOMAINLOGON` for the local agent and `REMOTE_USER_DOMAINLOGON` for the remote device.									
Groups									
The security	✓	✓							

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

USER	AGENT	CLIENT EXTENSION							
groups that the user is a member of. Only security groups referenced below will be evaluated. Static property with text data type. Persists as `LOCAL_USER_GROUPS` for									

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

USER	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_USER_GROUPS` for the remote device.									
Local Admin									
Set to true whenever the user has admin rights. Static property with boolean	✓	✓	✓		✓		✓	✓	✓

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

USER	AGENT	CLIENT EXTENSION							
data type. Persists as `LOCAL_USER_LOCALADMIN` for the local agent and `REMOTE_USER_LOCALADMIN` for the remote device.									
Name									
The name of the user. Static	✓	✓	✓		✓	✓	✓	✓	✓

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

USER	AGENT	CLIENT EXTENSION							
property with text data type. Persists as `LOCAL_USER_NAME` for the local agent and `REMOTE_USER_NAME` for the remote device.									
Password Age									
The age of the user	✓	✓	✓						

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

USER	AGENT	CLIENT EXTENSION							
password in days. Available only for Active Directory and work group accounts. Static property with number data type. Persists as `LOCAL_USER_PASSWORD_AGE` for the local									

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

USER	AGENT	CLIENT EXTENSION							
agent and `REMOTE_USER_PASSWORD_AGE` for the remote device.									
Password Auto Logon									
Set to true if auto-logon is configured for the user. Static property with boole	✓	✓	✓						

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

USER	AGENT	CLIENT EXTENSION							
an data type. Persists as `LOCAL_USER_PASSWORD_AUTOLOGON` for the local agent and `REMOTE_USER_PASSWORD_AUTOLOGON` for the remote device.									
SID									

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

USER	AGENT	CLIENT EXTENSION						
The Security Identifier (SID) of the user. Static property with text data type. Persists as `LOCAL_USER_SID` for the local agent and `REMOTE_USER_SID` for the remote	✓	✓	✓			✓			

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

USER	AGENT	CLIENT EXTENSION							
device.									

WHOIS Properties

WHOIS	AGENT	CLIENT EXTENSION							
Provides the results of a WHOIS lookup of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Adapter									
The name of the network adapter used to query	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
the whois data. Dynamic property with text data type. Persists as `LOCAL_WHOIS_ADAPTER` for the local agent and `REMOTE_WHOIS_ADAPTER` for the remote device.									

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

WHOIS	AGENT	CLIENT EXTENSION							
Adapter VPN									
Determines whether the whois data was queried using a VPN connection. Dynamic property with boolean data type. Persists as `LOCAL_WHOIS_ADA`	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
`PTER_VPN` for the local agent and `REMOTE_WHOIS_ADAPTER_VPN` for the remote device.									
Country									
The country reported by the WHOIS provider. Dynamic prope	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_WHOIS_COUNTRY` for the local agent and `REMOTE_WHOIS_COUNTRY` for the remote device.									
County									
The county repor	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
ted by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_COUNTY` for the local agent and `REMOTE_WHOIS_COUNTY` for the remote									

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

WHOIS	AGENT	CLIENT EXTENSION							
device.									
DNS									
The results of a DNS lookup of the IP address. Dynamic property with text data type. Persists as `LOCAL_WHOIS_DNS` for the local agent and `REMOTE_`	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
`WHOIS_DNS` for the remote device.									
IP									
The public IP address of the remote device. Dynamic property with ip, text data types. Persists as `LOCAL_W`	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
`HOIS_IP` for the local agent and `REMOTE_WHOIS_IP` for the remote device.									
ISP									
The ISP reported by the WHOIS provider. Dynamic property with text data	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_WHOIS_ISP` for the local agent and `REMOTE_WHOIS_ISP` for the remote device.									
Provider									
The provider used to query the WHOIS result	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION
s. Dynamic property with enum data type with options IP2Location, Max Mind. Persists as `LOCAL_WHOIS_PROVIDER` for the local agent and `REMOTE_WHOIS_PROVIDER` for		

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

WHOIS	AGENT	CLIENT EXTENSION							
the remote device.									
Proxy									
Set to true if a proxy is reported by the WHOIS provider. Dynamic property with boolean data type. Persists as `LOCAL_WHOIS_PRO`	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
`XY` for the local agent and `REMOTE_WHOIS_PROXY` for the remote device.									
Proxy Type									
The type of proxy in use as reported by the WHOIS provider. Dyna	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
mic property with enum data type with options VPN, TOR, Hosted, Public, Residential. Persists as `LOCAL_WHOIS_PROXY_TYPE` for the local agent and `REMOTE_WHOIS_PR`									

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

WHOIS	AGENT	CLIENT EXTENSION							
`OXY_TYPE` for the remote device.									
State									
The state reported by the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_STATE`	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_WHOIS_STATE` for the remote device.									
Town									
The town 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_TOWN` for the local agent and `REMOTE_WHOIS_TOWN` for the remote device.									
Usage									
A classification of the IP address as reported by	✓	✓	✓	✓	✓		✓	✓	✓

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

WHOIS	AGENT	CLIENT EXTENSION							
the WHOIS provider. Dynamic property with text data type. Persists as `LOCAL_WHOIS_USAGE` for the local agent and `REMOTE_WHOIS_USAGE` for the remote device.									

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

Windows Properties

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
Provides real-time properties unique to a Microsoft Windows device.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
SmartScreen for Microsoft Edge									
The state of SmartScreen for Microsoft Edge. Requires at	✓	✓							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
least Windows 10 or Windows Server 2016. Realtime property with enum data type with options Off, Warn, Block. Persists as `LOCAL_WINDOWS_SMARTSCREEN_EDGE` for									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_WINDOWS_SMARTSCREEN_EDGE` for the remote device.									
SmartScreen for Microsoft Store									
The state of SmartScreen for Microsoft Store apps. Requ	✓	✓							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
ires at least Windows 10 or Windows Server 2016. Realtime property with enum data type with options Off, Warn. Persists as `LOCAL_WINDOWS_SMARTSCREEN_STORE` for									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_WINDOWS_SMARTSCREEN_STORE` for the remote device.									
SmartScreen for Windows Explorer									
The state of SmartScreen for Windows Explorer.	✓	✓							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
Requires at least Windows 10 or Windows Server 2016. Realtime property with enum data type with options Off, Warn, Block. Persists as `LOCAL_WINDOWS_SMARTSCRE`									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
`EN_EXPLORER` for the local agent and `REMOTE_WINDOWS_SMARTSCREEN_EXPLORER` for the remote device.									
UAC Enabled									
Set to true if the User Access Control	✓	✓							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
(UAC) consent prompt is enabled. Realtime property with boolean data type. Persists as `LOCAL_WINDOWS_UAC_ENABLED` for the local agent and `REMOTE_WINDOWS_UAC_`									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
`ENABLED` for the remote device.									
UAC Policy									
The User Access Control (UAC) consent prompt policy applied to administrators. Realtime property with enum data	✓	✓							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
type with options Elevate without prompting, Prompt for credentials on secure desktop, Prompt for consent on secure desktop, Prompt for credentials on users desktop, Prom									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
pt for consent on users desktop, Prompt for consent for non-Windows binaries on secure desktop, Prompt for consent for non-Windows binaries on users desktop. Persists as									

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION							
`LOCAL_WINDOWS_UAC_POLICY` for the local agent and `REMOTE_WINDOWS_UAC_POLICY` for the remote device.									

Windows Defender Properties

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Provides real-time	Microsoft	Microsoft	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTo	Unicon™ eLux

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
properties describing the state of Microsoft Windows Defender Antivirus.	Windows	Windows						uch OS	
Antimalware Version									
The version of the anti-malware component. Realtime property with versi	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
on data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTIMALWARE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTIMALWARE` for the remote									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
device.									
Antispyware Version									
The version of the anti-spyware 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							
`VERSION_ANTISPYWARE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTISPYWARE` for the remote device.									
Antivirus Version									
The version of the	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION
anti-virus component. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTIVIRUS` for the local agent and `REMOTE_WINDOWSDEFEN`		

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`DEVICE_VERSION_ANTIVIRUS` for the remote device.									
Behavior Threats									
Determines the number of threats identified by behavioral analysis. Realtime property with	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION
number data type. Persists as `LOCAL_WINDOWSDEFENDER_BEHAVIORTHREATS` for the local agent and `REMOTE_WINDOWSDEFENDER_BEHAVIORTHREATS` for the remote		

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
device.									
Cloud Protection									
Defines the status of Cloud Delivered Protection, which enables Windows Defender to receive the latest protection from the cloud. Realti	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
me property with enum data type with options Disabled, Basic, Advanced. Persists as `LOCAL_WINDOWSDEFENDER_CLOUDPROTECTION` for the local agent and `REMOTE_WIND`									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`OWS DEFE NDER _CLO UDPR OTEC TION` for the remote device.									
Controlled Folder Access									
Defines the status of Windows Defender Exploit Guard's controlled folder	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
access, which protects files, folders and memory from unauthorized changes by unfriendly applications. Realtime property with boolean data type. Persists as `LOCAL_WINDO`									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`WSDEFENDER_CONTROLLEDFOLDERACCESS` for the local agent and `REMOTE_WINDOWSDEFENDER_CONTROLLEDFOLDERACCESS` for the remote device.									
Engine									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Version									
The version of the engine. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ENGINE` for the local agent and `REMOTE_`	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`WINDOWS DEFENDER_VERSION_ENGINE` for the remote device.									
Excluded Extensions									
Defines the file extensions excluded from Windows Defender. Realtime property	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_EXTENSIONS` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_EXTENSIONS` for the remot									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
e device.									
Excluded Paths									
Defines the files or folders 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_PATHS` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_PATHS` for the remote device.									
Excluded Processes									
Defines the proce	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
ss names excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_PROCESSES` for the local agent and									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`REMOTE_WINDOWSDEFENDER_EXCLUSIONS_PROCESSES` for the remote device.									
Last Full Scan									
The time of the last full scan. Realtime property with datetime data type.	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_WINDOWSDEFENDER_LASTFULLSCAN` for the local agent and `REMOTE_WINDOWSDEFENDER_LASTFULLSCAN` for the remote device.									
Last Quick Scan									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
The time of the last quick scan. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSDEFENDER_LASTQUICKSCAN` for the local agent and `REMOTE_WINDOWSDEFEN`	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`DER_LASTQUICKSCAN` for the remote device.									
Network Definition Version									
The version of the network definitions. Realtime property with version data type. Persists	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION` for the remote device.									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Network Engine Version									
The version of the network engine. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKEN`	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`GINE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_NETWORKENGINE` for the remote device.									
Real-Time Protection									
Set to true when Windows Defender'	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
s real time protection is enabled, including behavior monitoring, downloaded files and attachment scanning, monitoring of file and program activity, raw volume write notificatio									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
ns, and process scanning. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_REALTIMEPROTECTION` for the local agent and `REMOTE_WINDOWSD`									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`EFENDER_REALTIMEPROTECTION` for the remote device.									
Sample Submission									
Defines the status of Windows Defender sample submission, which sends	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
sample files to Microsoft when further analysis is required. Realtime property with enum data type with options Prompt, Send Safe Samples Automatically, Never Send Sam									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
ples, Send All Samples Automatically. Persists as `LOCAL_WINDOWSDEFENDER_SAMPLESUBMISSION` for the local agent and `REMOTE_WINDOWSDEFENDER_SAMPLESUBMISSION` for									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
the remote device.									
Signature Threats									
Determines the number of threats identified by their signature. Realtime property with number data type. Persists as `LOCAL_W`	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
`INDOWSDEFENDER_SIGNATURETHREATS` for the local agent and `REMOTE_WINDOWSDEFENDER_SIGNATURETHREATS` for the remote device.									
Status									
The status of Wind	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
ows Defender. Realtime property with enum data type with options Active, Pending Full Scan, Pending Reboot, Pending Manual Steps, Pending Offline Scan, Due Full									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Scan, Due Quick Scan, Inactive. Persists as `LOCAL_WINDOWSDEFENDER_STATUS` for the local agent and `REMOTE_WINDOWSDEFENDER_STATUS` for the remote device.									

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
Tamper Protection									
Set to true when Windows Defender is configured to prevent third party processes from changing its settings. Realtime property with boolean data	✓	✓							

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

WINDOWS DEFENDER	AGENT	CLIENT EXTENSION							
type. Persists as `LOCAL_WINDOWSDEFENDER_TAMPERPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_TAMPERPROTECTION` for the remote device.									

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

Windows Firewall Properties

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Provides real-time properties describing the state of the Microsoft Windows Firewall.	Microsoft Windows	Microsoft Windows	Apple macOS	Apple iOS	Ubuntu	Chrome OS	IGEL OS	Stratodesk NoTouch OS	Unicon™ eLux
Active Profile Block All Inbound									
Determines the active profiles which	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
are configured to block all inbound traffic. 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_BLOCKALLINBOUND` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_BLOCKALLINBOUND` for the remote device.									
Active Profile									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Disabled									
Determines the active profiles where the firewall is disabled. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOC`	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`AL_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED` for the remote device.									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Active Profile Inbound Allowed									
Determines the active profiles which are cofigured to allow inbound traffic. Realtime property with enum data type with options	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_INBOUNDALLOWED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_I`		

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`NBOUNDALLOWED` for the remote device.									
Active Profile Name									
Determines the names of the active profiles. Realtime property with enum data type with optio	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
ns Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_NAME` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_NAME`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
for the remote device.									
Active Profile Notifications Disabled									
Determines the active profiles which do not display a notification to the user when a program is	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
blocked from receiving inbound connections. 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_DISABLEDNOTIFICATIONS` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFICATIONS` for the remote device.									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
Active Profile Outbound Allowed									
Determines the active profiles which are configured to allow outbound traffic. Realtime property with enum data type with options	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_O`		

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`UTBOUNDALLOWED` for the remote device.									
Active Profile Respond to Multicast									
Determines the active profiles which respond to multicast or broadcast network	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for the remote device.									
Any Inbound Rules									
Determines the port numbers which	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
are allowed to receive an incoming connection from any process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_ANY` for the									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_ANY` for the remote device.									
Any Outbound Rules									
Determines the port numbers which are allowed to make an	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
outgoing connection from any process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_ANY` for the local agent and `REMOTE_`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`WINDOWSFIREWALL_OUTBOUNDRULES_ANY` for the remote device.									
Inbound Package Rules									
Determines the package identifier and port number of all packages allow	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
ed to receive an incoming connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_PACKAGES` for the local agent and `REMOTE_`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`WINDOWS FIREWALL_INBOUND RULES_PACKAGES` for the remote device.									
Inbound Program Rules									
Determines the filename and port number of all programs allowed to	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
receive an incoming connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_PROGRAMS` for the local agent and `REMOTE_WIND`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`OWS FIREWALL_INBOUND RULES_PROGRAMS` for the remote device.									
Inbound Service Rules									
Determines the service name and port number of all packages allowed to	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
receive an incoming connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_SERVICES` for the local agent and `REMOTE_WIND`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`OWS FIREWALL_INBOUND RULES_SERVICES` for the remote device.									
Inbound System Rules									
Determines the port numbers which are allowed to receive an incoming conn	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
ection from system processes. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_INBOUNDRULES_SYSTEM` for the local agent and `REMOTE_WIND`		

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`OWS FIREWALL_INBOUND RULES_SYSTEM` for the remote device.									
Outbound Package Rules									
Determines the package identifier and port number of all packages allowed to	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
make an outgoing connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_PACKAGES` for the local agent and `REMOTE_WIND`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`OWS FIREWALL_OUTBOUNDRULES_PACKAGES` for the remote device.									
Outbound Program Rules									
Determines the filename and port number of all programs allowed to make	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
an outgoing connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_PROGRAMS` for the local agent and `REMOTE_WINDOWSF`									

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`IREWALL_OUTBOUNDRULES_PROGRAMS` for the remote device.									
Outbound Service Rules									
Determines the service name and port number of all packages allowed to make	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
an outgoing connection. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_SERVICES` for the local agent and `REMOTE_WINDOWSF`		

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`IREWALL_OUTBOUNDRULES_SERVICES` for the remote device.									
Outbound System Rules									
Determines the port numbers which are allowed to make an outgoing connectio	✓	✓							

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION
n from system processes. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_SYSTEM` for the local agent and `REMOTE_WINDOWSF`		

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

WINDOWS FIREWALL	AGENT	CLIENT EXTENSION							
`IREWALL_OUTBOUNDRULES_SYSTEM` for the remote 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									

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION						
The number of Windows Registry entries. Static property with number data type. Persists as `LOCAL_WINDOWSREGISTRY_COUNT` for the local agent and `REMOTE_WINDOWSREGIS`	✓	✓						

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
`TRY_COUNT` for the remote device.									
Data									
The Windows Registry data. Static property with text, number, boolean, datetime, ip, position data types. Persists as	✓	✓							

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
`LOCAL_WINDOWSREGISTRY_X_DATA` for the local agent and `REMOTE_WINDOWSREGISTRY_X_DATA` for the remote device.									
Path									
The Windows Registry path. Static prope	✓	✓							

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
rty with text data type. Persists as `LOCAL_WINDOWSREGISTRY_X_PATH` for the local agent and `REMOTE_WINDOWSREGISTRY_X_PATH` for the remote device.									
Value									

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
The Windows Registry value. Static property with text data type. Persists as `LOCAL_WINDOWSREGISTRY_X_VALUE` for the local agent and `REMOTE_WINDOWSREGISTRY_X_VA`	✓	✓							

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

WINDOWS REGISTRY	AGENT	CLIENT EXTENSION							
`LUE` for the remote device.									

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	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
article IDs of any pending critical updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICAL` for the local agent and `REMOTE_`		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`WINDOWS_UPDATE_CRITICAL` for the remote device.									
Critical Release Date									
The deployment date of the oldest pending critical update. Realtime property	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICAL_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_CRITICAL_RELEASEDATE` for

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
the remote device.									
Definition KB									
The knowledge base article IDs of any pending definition updates. Realtime property with text data type. Persists as `LOC`	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`AL_WINDOWSUPDATE_DEFINITION` for the local agent and `REMOTE_WINDOWSUPDATE_DEFINITION` for the remote device.									
Definition Release Date									
The deplo	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
yment date of the oldest pending definition update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_DEFINITION_RELEASEDATE` for		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
the local agent and `REMOTE_WINDOWSUPDATE_DEFINITION_RELEASE DATE` for the remote device.									
Enabled									
Set to true whenever the Windows Update servi	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ce is enabled. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSUPDATE_ENABLED` for the local agent and `REMOTE_WINDOWSUPDATE_ENABLED` for									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
the remote device.									
Last Install									
Set to the time that Windows Update last installed updates. Realtime property with datetime data type. Persists as `LOC`	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`AL_WINDOWSUPDATE_LASTINSTALL` for the local agent and `REMOTE_WINDOWSUPDATE_LASTINSTALL` for the remote device.									
Last Search									
Set to the time that	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
Windows Update last checked for updates. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_LASTSEARCH` for the local agent and		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`REMOTE_WINDOWSUPDATE_LASTSEARCH` for the remote device.									
Notification Level									
Represents how Windows Update is configured to notify the user. Realtime	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
property with enum data type with options Not Configured, Disabled, Notify Before Download, Notify Before Install, Scheduled Install. Persists as `LOCAL_WINDOWSUP`									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`DATE_NOTIFICATIONLEVEL` for the local agent and `REMOTE_WINDOWSUPDATE_NOTIFICATIONLEVEL` for the remote device.									
Reboot Required									
Set to	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
true whenever Windows Update is awaiting a reboot to finish updating. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSUPDATE_REBOOTREQUIRED`									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
for the local agent and `REMOTE_WINDOWSUPDATE_REBOOTREQUIRED` for the remote device.									
Rollup KB									
The knowledge base article IDs of any pending rollup updat	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
es. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_ROLLUP` for the local agent and `REMOTE_WINDOWSUPDATE_ROLLUP` for the remote		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
device.									
Rollup Release Date									
The deployment date of the oldest pending rollup update. Realtime property with datetime data type. Persists as `LOCAL_WINDO`	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`WSUPDATE_ROLLUP_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_ROLLUP_RELEASEDATE` for the remote device.									
Security KB									
The knowl	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
edge base article IDs of any pending security updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_SECURITY` for the local agent and		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`REMOTE_WINDOWSUPDATE_SECURITY` for the remote device.									
Security Release Date	✓	✓							
The deployment date of the oldest pending security update. Realtime	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_SECURITY_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_SECURITY_RELEASEDA`									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
TE for the remote device.									
ServicePack KB									
The knowledge base article IDs of any pending service pack updates. Realtime property with text data type.	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Persists as `LOCAL_WINDOWSUPDATE_SERVICEPACK` for the local agent and `REMOTE_WINDOWSUPDATE_SERVICEPACK` for the remote device.									
ServicePack Rele									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
ase Date									
The deployment date of the oldest pending service pack update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_SERVICE`	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`PACK_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_SERVICEPACK_RELEASEDATE` for the remote device.									
Update KB									
The knowledge base articl	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION
e IDs of any pending updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_UPDATE` for the local agent and `REMOTE_WINDOWSUPDAT`		

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
`E_UPDATE` for the remote device.									
Update Release Date									
The deployment date of the oldest pending update. Realtime property with datetime data type. Persi	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
sts as `LOCAL_WINDOWSUPDATE_UPDATE_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_UPDATE_RELEASE_DATE` for the remote device.									

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
Version									
Set to the version number of Windows Update. Realtime property with version data type. Persists as `LOCAL_WINDOWSUPDATE_VERSION` for the local	✓	✓							

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

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION							
agent and `REMOTE_WINDOWSUPDATE_VERSION` for the remote device.									

Access Mode Template

This template imports a predefined context that defines whether the local device is internal or external to the corporate network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the local device is internal or external to the corporate network.	None

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 imports a predefined action that hides or denies access to applications in the session, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

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

Step 2: 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
Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session.	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. Example: notepad++.exe
Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session.	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

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 imports a predefined context that defines the country in which the local device is located, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

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

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the local device is located.	None

Troubleshooting

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

Country Provider Template

This template imports a predefined context that defines the the country provider that reports the country in which the local device is located, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country in which the local device is located.	None

Troubleshooting

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

Device Location IP Address Template

This template imports a predefined context that defines the location of a local device based on its IP address, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a local device based on its IP address.	You must update the following context condition with data suitable for your environment: `LOCAL - NETWORK IPV4 SUBNET IPv4 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*

Troubleshooting

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

Device Location NetBIOS Name Template

This template imports a predefined context that defines the location of a local device based on its NetBIOS name, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

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

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a local device based on its NetBIOS name.	You must update the following context condition with data suitable for your environment: LOCAL - 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

Troubleshooting

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

Device Location Wi-Fi Access Point Template

This template imports a predefined context that defines the location of a local device based on its connected Wi-Fi access point, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

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

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a local device based on its connected Wi-Fi access point.	You must update the following context condition with data suitable for your environment: LOCAL - 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

Troubleshooting

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

Building Blocks Templates

Individual contexts and actions that can be used as building blocks within your configuration.

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

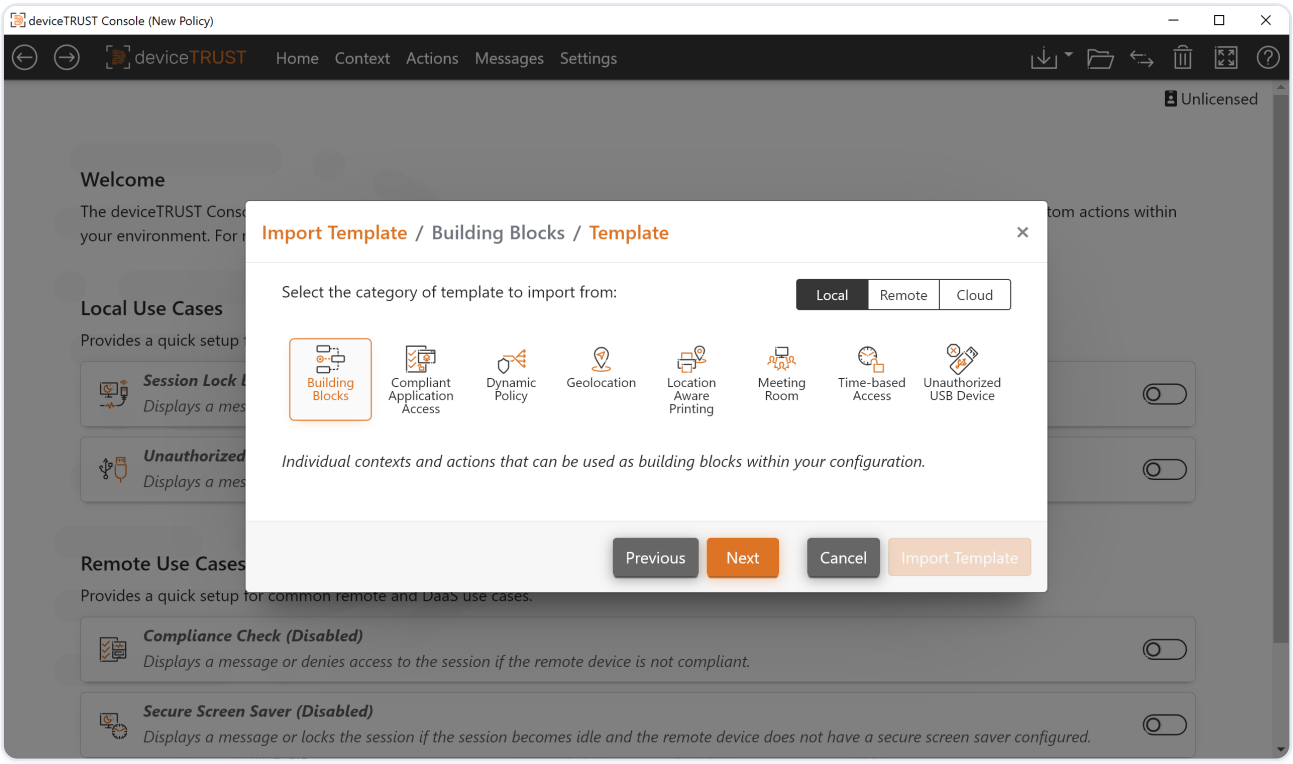


TABLE OF CONTENTS

- Access Mode - Defines if the local device is internal or external to the corporate network.
- Conditional Application Access - Hides or denies applications within the session.
- Country - Defines the country in which the local device is located.
- Country Provider - Defines the country provider that reports the country in which the local device is located.
- Device Location IP Address - Defines the location of a local device based on its IP address.
- Device Location NetBIOS Name - Defines the location of a local device based on its NetBIOS name.
- Device Location Wi-Fi Access Point - Defines the location of a local device based on its connected Wi-Fi access point.
- Operating System Update - Defines if a recent update search has been performed and that critical updates have been installed.
- Override - Defines if the session user is a member of the override AD group.
- Policy Mode from AD Group - Defines if the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group.
- Policy Mode from Date - Defines if the deviceTRUST policy runs in active or passive mode based upon a fixed date.

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

- Process Monitoring - Evaluates if an application is running on the local device. Uses a custom property for evaluation.
- Proximity - Defines the proximity of the local device to a given position.
- Session Idle - Defines if the session is idle.
- Unauthorized USB Device - Defines if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the local device.
- VPN Connected - Defines if a network adapter of the local device is connected to a VPN network.
- Wi-Fi Security Mode - Defines if the local device is connected to a secure Wi-Fi network.
- Working Time - Defines if the current time is within work hours.

Operating System Update Template

This template imports a predefined context that defines if a recent update search has been performed and that critical updates have been installed on the local device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Update	Defines if a recent update search has been performed and that all updates have been installed.	None

Troubleshooting

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

Override Template

This template imports a predefined context that defines whether the session user is a member of the override AD group, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

Troubleshooting

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

Policy Mode from AD Group Template

This template imports a predefined context that defines whether the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Policy Mode	Defines if the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to activate the deviceTRUST policy for those users.

Troubleshooting

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

Policy Mode from Date Template

This template imports a predefined context that defines whether the deviceTRUST policy runs in active or passive mode based upon a fixed date, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Policy Mode	Defines if the deviceTRUST policy runs in active or passive mode based upon a date.	You must set a date to run the deviceTRUST policy in active or passive mode.

Troubleshooting

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

Process Monitoring Template

This template imports a predefined context that evaluates if an application is running on the local device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Settings

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Process State - Your App	Evaluates if Your App is running on the local device. Uses a custom property for evaluation.	You must update the following context condition with data suitable for your environment
		`LOCAL - CUSTOM`
		Ensure %LOCAL_CUSTOM_YOURAPP_RUNNING% reflects the custom property created by the Custom Properties on the Local Agent.

Step 3: Settings

The template has imported the following settings:

SETTINGS	DESCRIPTION	CUSTOMIZATIONS
Custom Properties	The Local Agent section of Custom Properties has been customised to monitor the running processes.	You must update the following setting with data suitable for your environment
		`CUSTOM PROPERTIES - LOCAL AGENT`
		Ensure the call to Get-Process is monitoring the process of interest, and that the LOCAL_CUSTOM_YOURAPP_RUNNING property name is reflected in the Process State - Your App context.

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.

Proximity Template

This template imports a predefined context that defines the proximity of the local device to a given position, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Proximity	Defines the proximity of the local device to a given position.	You must update the following context condition with data suitable for your environment: LOCAL - 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

© 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.

Session Idle Template

This template imports a predefined context that defines if the session is idle, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines if the session is idle.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION IDLE PERIODE Greater Than 10`

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Configure a maximum idle time in minutes for your environment.
		Example: 10

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 imports a predefined context that defines whether an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the local device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Unauthorized USB Device	Defines if an unauthorized USB device such as a Stick, Camera or Mobile Phone, plugged into the local device.	You must update the following context condition with data suitable for your environment
		`LOCAL - 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.

Troubleshooting

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

VPN Connected Template

This template imports a predefined context that defines whether a network adapter of the local device is connected to a VPN network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Defines if a network adapter on the local device is connected to a VPN network.	None

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 imports a predefined context that defines whether the local device is connected to a secure Wi-Fi network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

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

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the local device is connected to a secure Wi-Fi network.	None

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 imports a predefined context that defines whether the current time is within work hours, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

© 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.

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 hides or denies access to applications in the session based on the country of the local device. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `LOCAL` platform.

If the local device is not located within an authorized country, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the country.
- Denies access to applications with Microsoft AppLocker based on the country.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 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.	None
Country Provider	Defines the provider that reports the country information.	None

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
Country - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking based on the country.	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

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Alpha-2 code. Example: US
			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
Country - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker based on the country.	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

© 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

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.

Compliant Application Access Templates

Controls access to applications within the session.

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

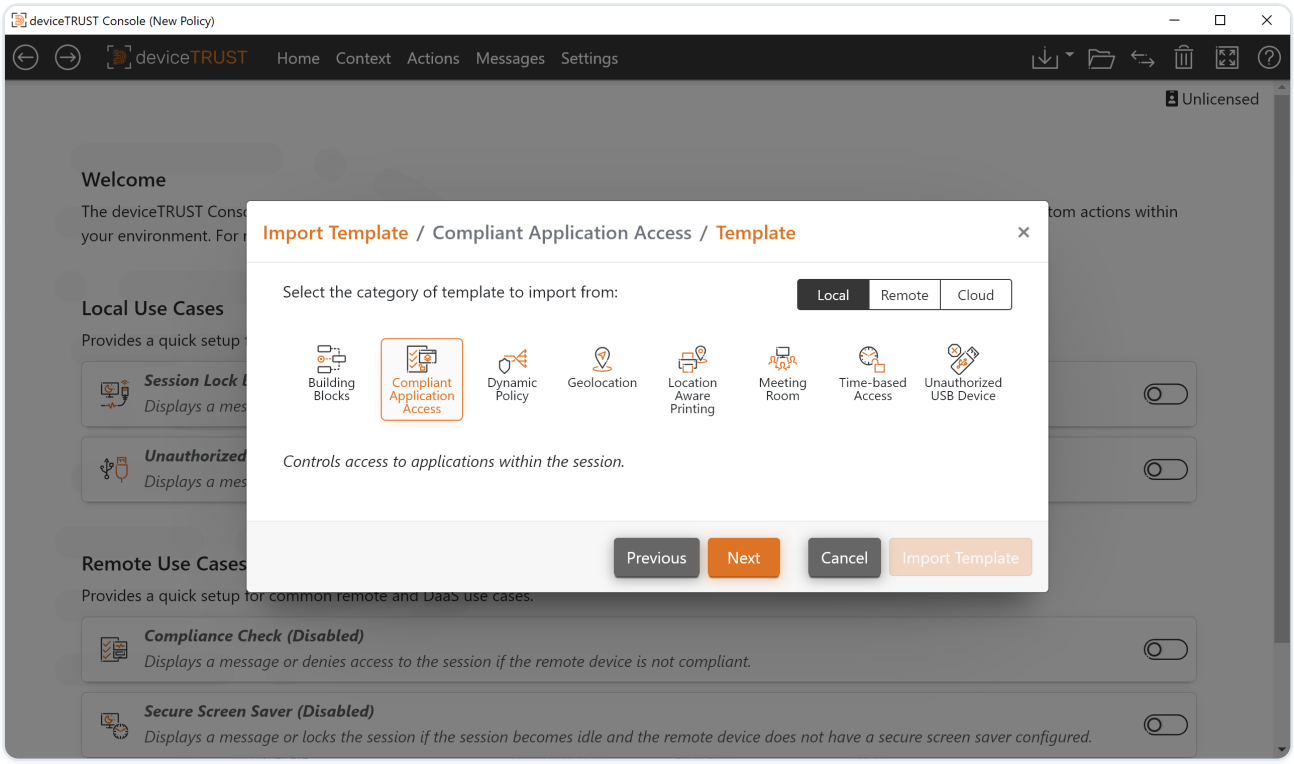


TABLE OF CONTENTS

- Country - Hides or denies access to applications in the session based on the country of the local device.
- Proximity - Hides or denies access to applications in the session based on the proximity of the local device to a given position.
- Security State - Hides or denies access to applications in the session based on the Security State of the local device.
- Wi-Fi Security Mode - Hides or denies access to applications in the session when the local device is connected to an insecure Wi-Fi network.
- Working Time - Hides or denies access to applications in the session outside of working hours.

Proximity Template

This template creates a configuration that hides or denies access to applications in the session based on the proximity of the local device to a given position. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `LOCAL` platform.

If the local device is not in proximity to a given position, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the proximity to a given position.

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

- Denies access to applications with Microsoft AppLocker based on the proximity to a given position.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Proximity	Defines the proximity to a given position.	You must update the following context condition with data suitable for your environment: `LOCAL - 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.

© 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
Proximity - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking based on the proximity to a given position.	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. Example: notepad++.exe*
Proximity - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker based on the proximity to a given position.	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*

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 hides or denies access to applications in the session based on the security state of the local device. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `LOCAL` platform.

If the security state of the local device is unprotected, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the security state.
- Denies access to applications with Microsoft AppLocker based on the security state.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites

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

- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 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 local 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.

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 local 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*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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. 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 local 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*

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

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.

Wi-Fi Security Mode Template

This template creates a configuration that hides or denies access to applications in the session when the local device is connected to an insecure Wi-Fi network. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `LOCAL` platform.

If the local device is using an insecure Wi-Fi network, you can choose between two actions:

- Hides applications with FSLogix App Masking for insecure Wi-Fi networks.
- Denies access to applications with Microsoft AppLocker for insecure Wi-Fi networks.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines the Wi-Fi network security mode.	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 for insecure Wi-Fi networks.	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 Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			TERMINATE APP Replace ADD_PROCESS_NAME_X with your

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 for insecure Wi-Fi networks.	Deactivated	You must update the following context condition with data suitable for your environment
			MICROSOFT APPLOCKERReplace 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.

Working Time Template

This template creates a configuration that hides or denies access to applications in the session outside of working hours. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `LOCAL` platform.

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

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 local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

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.

© 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.

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. Example: notepad++.exe*
Working Time - Conditional Application Access -	Denies access to applications with Microsoft AppLocker within the session	Deactivated	You must update the following context condition with data suitable for your

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - Microsoft AppLocker	when accessed outside of working time.		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.

Dynamic Policy Templates

Applies a dynamic policy within the session.

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

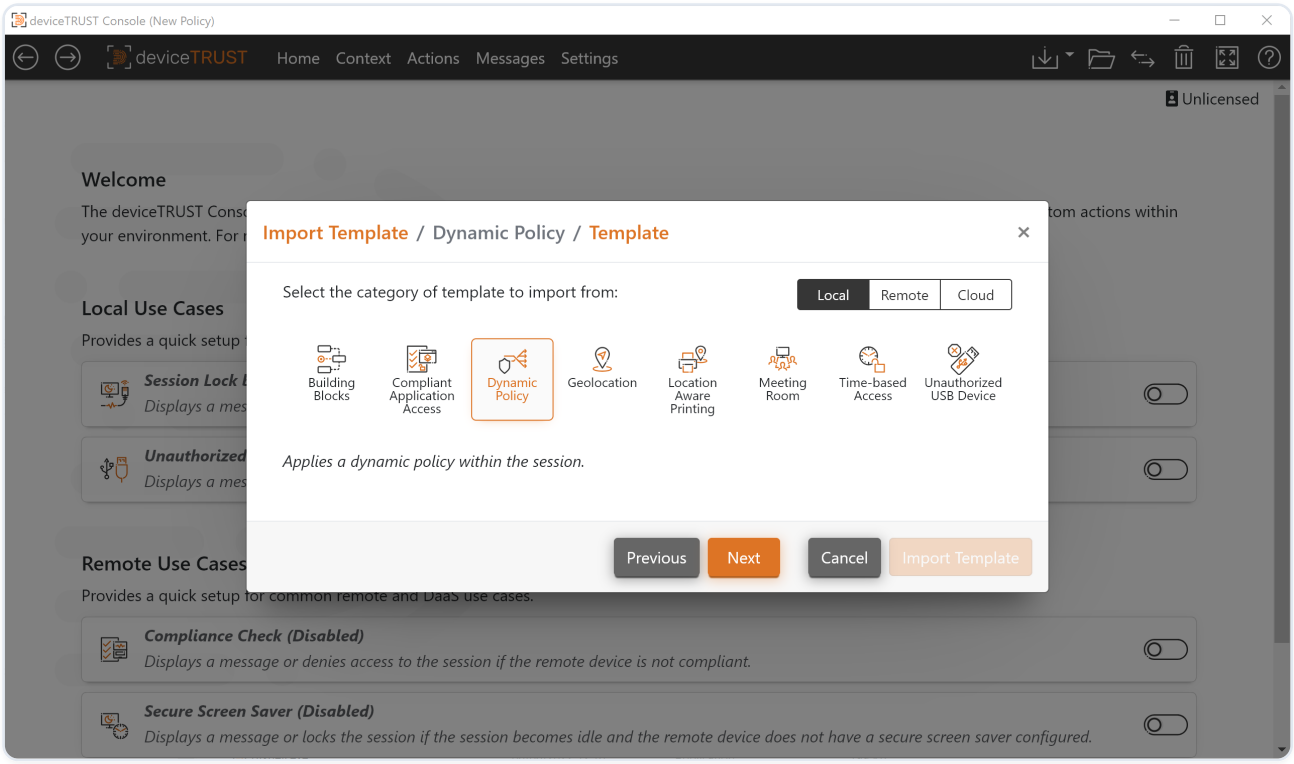


TABLE OF CONTENTS

- Session Lock based on Network Type - Locks the session if the session becomes idle based on the network type.
- Session Lock based on VPN Connection - Locks the session if the session becomes idle based on the VPN connected state.
- Session Lock based on Wi-Fi Security Mode - Locks the session if the session becomes idle based on the Wi-Fi security mode.

Session Lock based on Network Type Template

This template creates a configuration that locks the session if the session becomes idle based on the network type. It can be found in the `DYNAMIC POLICY` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts

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

- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines the session idle state of a corporate network connected 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 enforcement action that actively controls access to the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Session Idle - Conditional Access - Enforcement	Locks the session if the session becomes idle.	Activated	None

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.

Session Lock based on VPN Connection Template

This template creates a configuration that locks the session if the session becomes idle based on the VPN connected state. It can be found in the `DYNAMIC POLICY` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines the session idle state of a VPN connected 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 enforcement action that actively controls access to the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Session Idle - Conditional Access - Enforcement	Locks the session if the session becomes idle.	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.

Session Lock based on Wi-Fi Security Mode Template

This template creates a configuration that locks the session if the session becomes idle based on the Wi-Fi security mode. It can be found in the `DYNAMIC POLICY` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 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 context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines the session idle state of a device connected to a 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 enforcement action that actively controls access to the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Session Idle - Conditional Access - Enforcement	Locks the session if the session becomes idle.	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.

Conditional Application Access for Country Template

This template creates a configuration that hides or denies access to applications in the session based on the country of the local device. It can be found in the `GEOLOCATION` category when filtered for `LOCAL` platform.

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

If the local device is not located within an authorized country, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the country.
- Denies access to applications with Microsoft AppLocker based on the country.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 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.	None
Country Provider	Defines the provider that reports the country information.	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 based on the country.	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 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*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			tasks. Example: notepad++.exe
Country - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker based on the country.	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*
			`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.

Conditional Application Access for Proximity Template

This template creates a configuration that hides or denies access to applications in the session based on the proximity of the local device to a given position. It can be found in the `GEOLOCATION` category when filtered for `LOCAL` platform.

If the local device is not in proximity to a given position, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the proximity to a given position.
- Denies access to applications with Microsoft AppLocker based on the proximity to a given position.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Proximity	Defines the proximity to a given position.	You must update the following context condition with data suitable for your

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		environment: `LOCAL - 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 - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking based on the proximity to a given position.	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*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			\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 Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker based on the proximity to a given position.	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.

Geolocation Templates

Validates and controls access based on geolocation information of the local device.

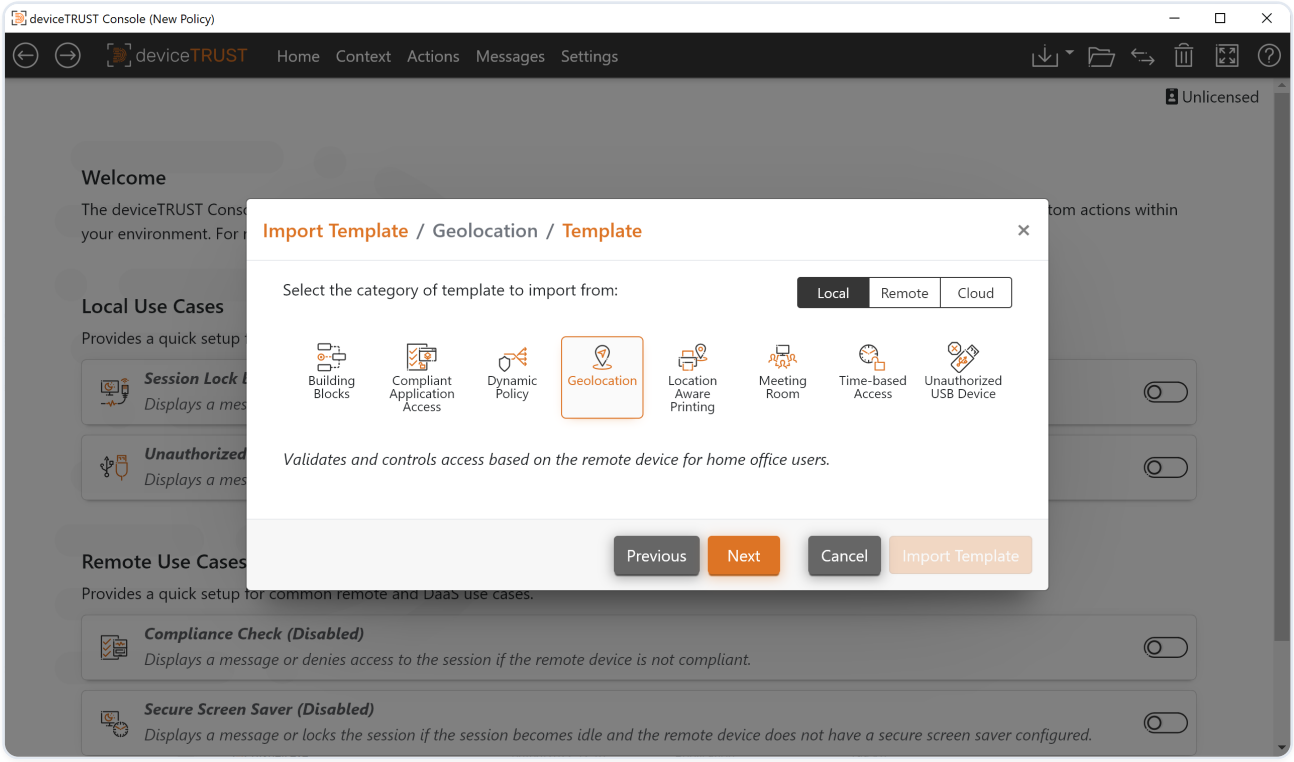


TABLE OF CONTENTS

- Conditional Application Access for Country - Hides or denies access to applications in the session based on the country of the local device.
- Conditional Application Access for Proximity - Hides or denies access to applications in the session based on the proximity of the local device to a given position.

Location Aware Printing Templates

Maps network printers and defines a default printer based on the device placement within a building.

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

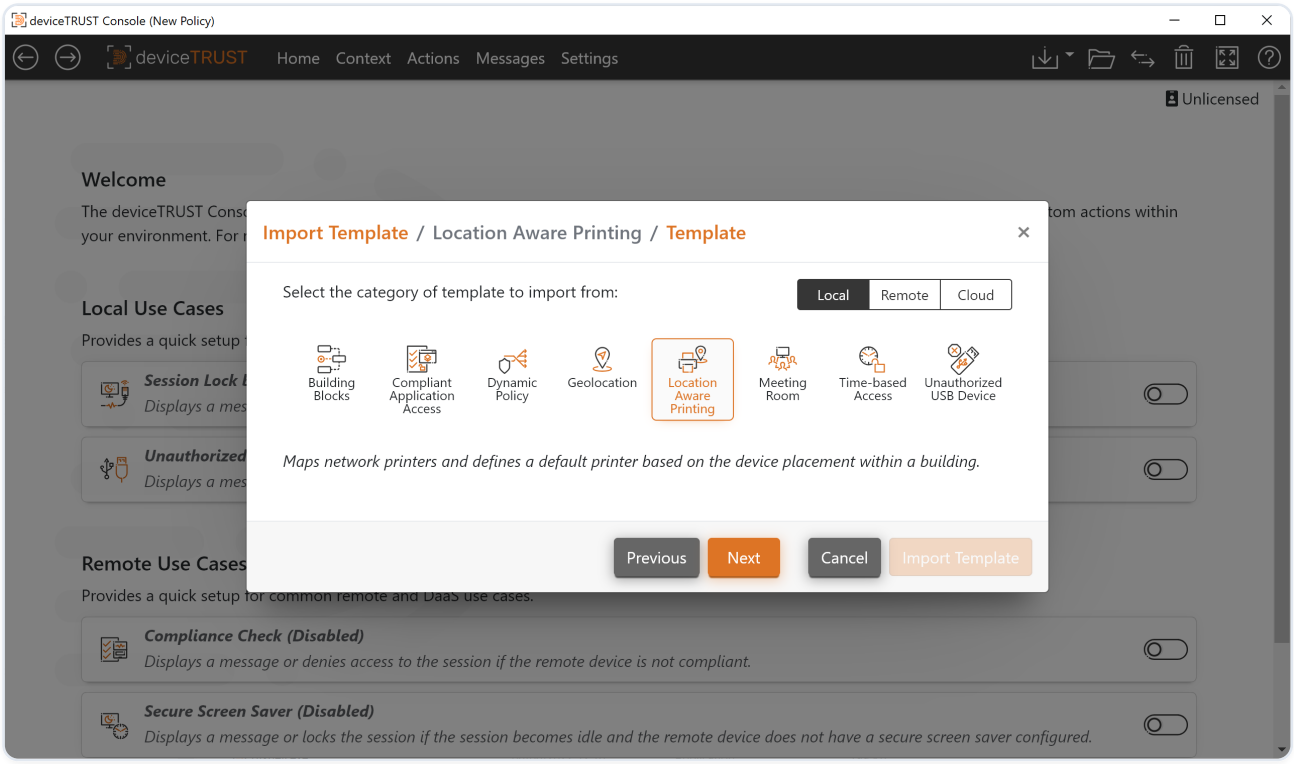


TABLE OF CONTENTS

- IP Address - Maps network printers and defines a default printer based on the location of the local device using its IP address.
- NetBIOS Name - Maps network printers and defines a default printer based on the location of the local device using its NetBIOS name.
- Wi-Fi Access Point - Maps network printers and defines a default printer based on the location of the local device using its connected Wi-Fi access point.

IP Address Template

This template creates a configuration that maps network printers and defines a default printer based on the location of the local device using its IP address. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts

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

- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a device based on its IP address.	You must update the following context condition with data suitable for your environment: `LOCAL - NETWORK IPV4 SUBNET IPv4 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 -	Maps network printers and defines	Activated	You must update the following context

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Printer Management - IP Address	a default printer based on the location of the device using its IP address.		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: \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 local device using its NetBIOS name. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts

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

- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a device based on its NetBIOS name.	You must update the following context condition with data suitable for your environment: `LOCAL - 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.

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 device	Activated	You must update the following context condition with data suitable for your environment: `MAP`

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	using its NetBIOS name.		`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.

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 local device using its connected Wi-Fi access point. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a device based on its connected Wi-Fi access point.	You must update the following context condition with data suitable for your environment: `LOCAL - 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 device	Activated	You must update the following context condition with data suitable for your environment: `MAP`

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	using its connected Wi-Fi access point.		`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.

Application Log Template

This template creates a configuration that reports the status of the local device to the Windows application log. It can be found in the `STATUS REPORT` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Evaluates the active antivirus product used on the local device.	None
Antivirus Signature Status	Evaluates the signature status of the active antivirus product used on the local device.	None
Antivirus Status	Evaluates the status of the active antivirus product used on the local device.	None
Country	Evaluates the country in which the local device is located.	None
Country Provider	Evaluates the country provider that reports the country of the local device.	None
Device Identifier	Evaluates the device identifier of the local device.	None
Device Type	Evaluates the device type of the local device.	None
Economic Region	Evaluates the economic region the local device is located within.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Firewall Name	Evaluates the available firewall product used on the local device.	None
Firewall Status	Evaluates the status of the active firewall product used on the local device.	None
Hardware Bios Release Date	Evaluates the hardware BIOS release date of the local device.	None
Hardware Model	Evaluates the hardware model of the local device.	None
Hardware Role	Evaluates the hardware role of the local device.	None
Hardware Secure Boot	Evaluates the hardware secure boot settings of the local device.	None
Hardware Vendor	Evaluates the hardware vendor of the local device.	None
Network Address Assignment	Evaluates the network address assignment type of the local device.	None
Network DHCP Server	Evaluates the network DHCP server of the local device.	None
Network DNS Server	Evaluates the network DNS server of the local device.	None
Network DNS Suffix	Evaluates the network DNS suffix of the local device.	None
Network Gateway	Evaluates the network gateway of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network Gateway MAC	Evaluates the network gateway mac address of the local device.	None
Network IP Address	Evaluates the network ip address of the local device.	None
Network MAC Address	Evaluates the network MAC address of the local device.	None
Network Subnet	Evaluates the network subnet of the local device.	None
Operating System Description	Evaluates the operating system description of the local device.	None
Operating System Disk Encryption	Evaluates the operating system disk encryption of the local device.	None
Operating System Name	Evaluates the operating system name of the local device.	None
Operating System Platform	Evaluates the operating system platform of the local device.	None
Operating System Release	Evaluates the operating system release of the local device.	None
Operating System Type	Evaluates the operating system type of the local device.	None
Operating System Updates	Evaluates if a recent update search has been performed and that all updates have	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	been installed on the local device.	
Operating System Version	Evaluates the operating system version of the local device.	None
Override	Evaluates 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	Evaluates the region keyboard locale of the local device.	None
Region Locale	Evaluates the region locale of the local device.	None
Region Timezone Offset	Evaluates the region timezone offset of the local device.	None
Remote Controlled	Evaluates if the local device is remote controlled.	None
Secure Screen Saver	Evaluates whether the local device is using a secure screen saver.	None
Security State	Evaluates the security status of the local device.	None
Session User Domain	Evaluates the user domain of the user account used within the session.	None
Session User Name	Evaluates the user name of the user account used within the session.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
User Authentication	Evaluates the authentication of the user account used on the local device.	None
User Privileges	Evaluates the privileges of the user logged into the local device.	None
Virtualized	Evaluates if the local device is virtualized.	None
VPN Connected	Evaluates if a network adapter of the local device is connected to a VPN network.	None
Wi-Fi Security Mode	Evaluates if the local 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 local device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Application Log	Reports the status of the local device to the Windows application log.	Activated	None

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

NOTE:

If the action has 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 local device to ELK Stack. It can be found in the `STATUS REPORT` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Evaluates the active antivirus product used on the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Signature Status	Evaluates the signature status of the active antivirus product used on the local device.	None
Antivirus Status	Evaluates the status of the active antivirus product used on the local device.	None
Country	Evaluates the country in which the local device is located.	None
Country Provider	Evaluates the country provider that reports the country of the local device.	None
Device Identifier	Evaluates the device identifier of the local device.	None
Device Type	Evaluates the device type of the local device.	None
Economic Region	Evaluates the economic region the local device is located within.	None
Firewall Name	Evaluates the available firewall product used on the local device.	None
Firewall Status	Evaluates the status of the active firewall product used on the local device.	None
Hardware Bios Release Date	Evaluates the hardware BIOS release date of the local device.	None
Hardware Model	Evaluates the hardware model of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Role	Evaluates the hardware role of the local device.	None
Hardware Secure Boot	Evaluates the hardware secure boot settings of the local device.	None
Hardware Vendor	Evaluates the hardware vendor of the local device.	None
Network Address Assignment	Evaluates the network address assignment type of the local device.	None
Network DHCP Server	Evaluates the network DHCP server of the local device.	None
Network DNS Server	Evaluates the network DNS server of the local device.	None
Network DNS Suffix	Evaluates the network DNS suffix of the local device.	None
Network Gateway	Evaluates the network gateway of the local device.	None
Network Gateway MAC	Evaluates the network gateway mac address of the local device.	None
Network IP Address	Evaluates the network ip address of the local device.	None
Network MAC Address	Evaluates the network MAC address of the local device.	None
Network Subnet	Evaluates the network subnet of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Description	Evaluates the operating system description of the local device.	None
Operating System Disk Encryption	Evaluates the operating system disk encryption of the local device.	None
Operating System Name	Evaluates the operating system name of the local device.	None
Operating System Platform	Evaluates the operating system platform of the local device.	None
Operating System Release	Evaluates the operating system release of the local device.	None
Operating System Type	Evaluates the operating system type of the local device.	None
Operating System Updates	Evaluates if a recent update search has been performed and that all updates have been installed on the local device.	None
Operating System Version	Evaluates the operating system version of the local device.	None
Override	Evaluates 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.

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Region Keyboard Locale	Evaluates the region keyboard locale of the local device.	None
Region Locale	Evaluates the region locale of the local device.	None
Region Timezone Offset	Evaluates the region timezone offset of the local device.	None
Remote Controlled	Evaluates if the local device is remote controlled.	None
Secure Screen Saver	Evaluates whether the local device is using a secure screen saver.	None
Security State	Evaluates the security status of the local device.	None
Session User Domain	Evaluates the user domain of the user account used within the session.	None
Session User Name	Evaluates the user name of the user account used within the session.	None
User Authentication	Evaluates the authentication of the user account used on the local device.	None
User Privileges	Evaluates the privileges of the user logged into the local device.	None
Virtualized	Evaluates if the local device is virtualized.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Evaluates if a network adapter of the local device is connected to a VPN network.	None
Wi-Fi Security Mode	Evaluates if the local 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 local device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - ELK Stack	Reports the status of the local 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 has 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 local device by email. It can be found in the `STATUS REPORT` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Evaluates the active antivirus product used on the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Signature Status	Evaluates the signature status of the active antivirus product used on the local device.	None
Antivirus Status	Evaluates the status of the active antivirus product used on the local device.	None
Country	Evaluates the country in which the local device is located.	None
Country Provider	Evaluates the country provider that reports the country of the local device.	None
Device Identifier	Evaluates the device identifier of the local device.	None
Device Type	Evaluates the device type of the local device.	None
Economic Region	Evaluates the economic region the local device is located within.	None
Firewall Name	Evaluates the available firewall product used on the local device.	None
Firewall Status	Evaluates the status of the active firewall product used on the local device.	None
Hardware Bios Release Date	Evaluates the hardware BIOS release date of the local device.	None
Hardware Model	Evaluates the hardware model of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Role	Evaluates the hardware role of the local device.	None
Hardware Secure Boot	Evaluates the hardware secure boot settings of the local device.	None
Hardware Vendor	Evaluates the hardware vendor of the local device.	None
Network Address Assignment	Evaluates the network address assignment type of the local device.	None
Network DHCP Server	Evaluates the network DHCP server of the local device.	None
Network DNS Server	Evaluates the network DNS server of the local device.	None
Network DNS Suffix	Evaluates the network DNS suffix of the local device.	None
Network Gateway	Evaluates the network gateway of the local device.	None
Network Gateway MAC	Evaluates the network gateway mac address of the local device.	None
Network IP Address	Evaluates the network ip address of the local device.	None
Network MAC Address	Evaluates the network MAC address of the local device.	None
Network Subnet	Evaluates the network subnet of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Description	Evaluates the operating system description of the local device.	None
Operating System Disk Encryption	Evaluates the operating system disk encryption of the local device.	None
Operating System Name	Evaluates the operating system name of the local device.	None
Operating System Platform	Evaluates the operating system platform of the local device.	None
Operating System Release	Evaluates the operating system release of the local device.	None
Operating System Type	Evaluates the operating system type of the local device.	None
Operating System Updates	Evaluates if a recent update search has been performed and that all updates have been installed on the local device.	None
Operating System Version	Evaluates the operating system version of the local device.	None
Override	Evaluates 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.

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Region Keyboard Locale	Evaluates the region keyboard locale of the local device.	None
Region Locale	Evaluates the region locale of the local device.	None
Region Timezone Offset	Evaluates the region timezone offset of the local device.	None
Remote Controlled	Evaluates if the local device is remote controlled.	None
Secure Screen Saver	Evaluates whether the local device is using a secure screen saver.	None
Security State	Evaluates the security status of the local device.	None
Session User Domain	Evaluates the user domain of the user account used within the session.	None
Session User Name	Evaluates the user name of the user account used within the session.	None
User Authentication	Evaluates the authentication of the user account used on the local device.	None
User Privileges	Evaluates the privileges of the user logged into the local device.	None
Virtualized	Evaluates if the local device is virtualized.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Evaluates if a network adapter of the local device is connected to a VPN network.	None
Wi-Fi Security Mode	Evaluates if the local 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 local device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Email	Send the status of the local 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.

Status Report Templates

Reports the status of the local device to various destinations.

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

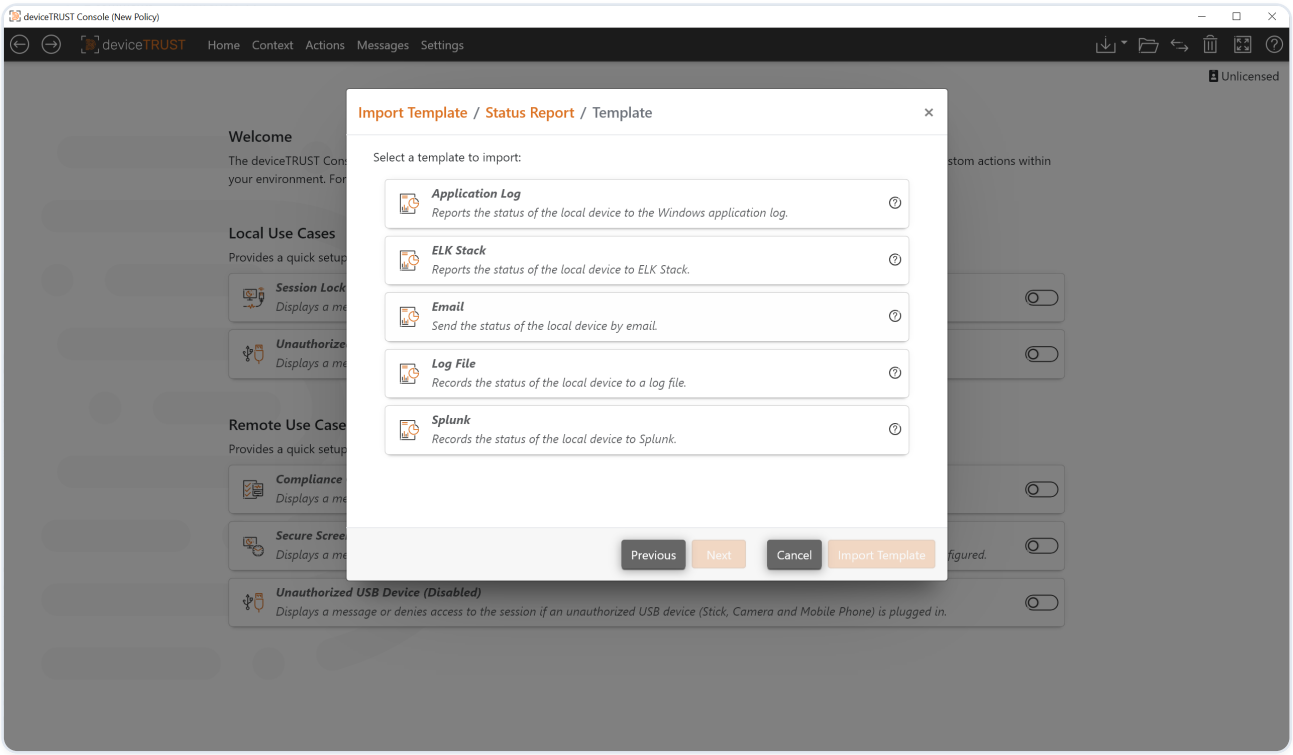


TABLE OF CONTENTS

- Application Log - Reports the status of the local device to the Windows application log.
- ELK Stack - Reports the status of the local device to ELK Stack.
- Email - Send the status of the local device by email.
- Log File - Records the status of the local device to a log file.
- Splunk - Records the status of the local device to Splunk.

Log File Template

This template creates a configuration that reports the status of the local device to a log file. It can be found in the `STATUS REPORT` category when filtered for `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

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

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Evaluates the active antivirus product used on the local device.	None
Antivirus Signature Status	Evaluates the signature status of the active antivirus product used on the local device.	None
Antivirus Status	Evaluates the status of the active antivirus product used on the local device.	None
Country	Evaluates the country in which the local device is located.	None
Country Provider	Evaluates the country provider that reports the country of the local device.	None
Device Identifier	Evaluates the device identifier of the local device.	None
Device Type	Evaluates the device type of the local device.	None
Economic Region	Evaluates the economic region the local device is located within.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Firewall Name	Evaluates the available firewall product used on the local device.	None
Firewall Status	Evaluates the status of the active firewall product used on the local device.	None
Hardware Bios Release Date	Evaluates the hardware BIOS release date of the local device.	None
Hardware Model	Evaluates the hardware model of the local device.	None
Hardware Role	Evaluates the hardware role of the local device.	None
Hardware Secure Boot	Evaluates the hardware secure boot settings of the local device.	None
Hardware Vendor	Evaluates the hardware vendor of the local device.	None
Network Address Assignment	Evaluates the network address assignment type of the local device.	None
Network DHCP Server	Evaluates the network DHCP server of the local device.	None
Network DNS Server	Evaluates the network DNS server of the local device.	None
Network DNS Suffix	Evaluates the network DNS suffix of the local device.	None
Network Gateway	Evaluates the network gateway of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network Gateway MAC	Evaluates the network gateway mac address of the local device.	None
Network IP Address	Evaluates the network ip address of the local device.	None
Network MAC Address	Evaluates the network MAC address of the local device.	None
Network Subnet	Evaluates the network subnet of the local device.	None
Operating System Description	Evaluates the operating system description of the local device.	None
Operating System Disk Encryption	Evaluates the operating system disk encryption of the local device.	None
Operating System Name	Evaluates the operating system name of the local device.	None
Operating System Platform	Evaluates the operating system platform of the local device.	None
Operating System Release	Evaluates the operating system release of the local device.	None
Operating System Type	Evaluates the operating system type of the local device.	None
Operating System Updates	Evaluates if a recent update search has been performed and that all updates have	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	been installed on the local device.	
Operating System Version	Evaluates the operating system version of the local device.	None
Override	Evaluates 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	Evaluates the region keyboard locale of the local device.	None
Region Locale	Evaluates the region locale of the local device.	None
Region Timezone Offset	Evaluates the region timezone offset of the local device.	None
Remote Controlled	Evaluates if the local device is remote controlled.	None
Secure Screen Saver	Evaluates whether the local device is using a secure screen saver.	None
Security State	Evaluates the security status of the local device.	None
Session User Domain	Evaluates the user domain of the user account used within the session.	None
Session User Name	Evaluates the user name of the user account used within the session.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
User Authentication	Evaluates the authentication of the user account used on the local device.	None
User Privileges	Evaluates the privileges of the user logged into the local device.	None
Virtualized	Evaluates if the local device is virtualized.	None
VPN Connected	Evaluates if a network adapter of the local device is connected to a VPN network.	None
Wi-Fi Security Mode	Evaluates if the local 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 local device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Log File	Records the status of the local device to a log file.	Deactivated	None

NOTE:

If the action 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.

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 `LOCAL` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Evaluates the active antivirus product used on the local device.	None
Antivirus Signature Status	Evaluates the signature status of the active antivirus product used on the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Status	Evaluates the status of the active antivirus product used on the local device.	None
Country	Evaluates the country in which the local device is located.	None
Country Provider	Evaluates the country provider that reports the country of the local device.	None
Device Identifier	Evaluates the device identifier of the local device.	None
Device Type	Evaluates the device type of the local device.	None
Economic Region	Evaluates the economic region the local device is located within.	None
Firewall Name	Evaluates the available firewall product used on the local device.	None
Firewall Status	Evaluates the status of the active firewall product used on the local device.	None
Hardware Bios Release Date	Evaluates the hardware BIOS release date of the local device.	None
Hardware Model	Evaluates the hardware model of the local device.	None
Hardware Role	Evaluates the hardware role of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Secure Boot	Evaluates the hardware secure boot settings of the local device.	None
Hardware Vendor	Evaluates the hardware vendor of the local device.	None
Network Address Assignment	Evaluates the network address assignment type of the local device.	None
Network DHCP Server	Evaluates the network DHCP server of the local device.	None
Network DNS Server	Evaluates the network DNS server of the local device.	None
Network DNS Suffix	Evaluates the network DNS suffix of the local device.	None
Network Gateway	Evaluates the network gateway of the local device.	None
Network Gateway MAC	Evaluates the network gateway mac address of the local device.	None
Network IP Address	Evaluates the network ip address of the local device.	None
Network MAC Address	Evaluates the network MAC address of the local device.	None
Network Subnet	Evaluates the network subnet of the local device.	None
Operating System Description	Evaluates the operating system description of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Disk Encryption	Evaluates the operating system disk encryption of the local device.	None
Operating System Name	Evaluates the operating system name of the local device.	None
Operating System Platform	Evaluates the operating system platform of the local device.	None
Operating System Release	Evaluates the operating system release of the local device.	None
Operating System Type	Evaluates the operating system type of the local device.	None
Operating System Updates	Evaluates if a recent update search has been performed and that all updates have been installed on the local device.	None
Operating System Version	Evaluates the operating system version of the local device.	None
Override	Evaluates 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	Evaluates the region keyboard locale of the local device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Region Locale	Evaluates the region locale of the local device.	None
Region Timezone Offset	Evaluates the region timezone offset of the local device.	None
Remote Controlled	Evaluates if the local device is remote controlled.	None
Secure Screen Saver	Evaluates whether the local device is using a secure screen saver.	None
Security State	Evaluates the security status of the local device.	None
Session User Domain	Evaluates the user domain of the user account used within the session.	None
Session User Name	Evaluates the user name of the user account used within the session.	None
User Authentication	Evaluates the authentication of the user account used on the local device.	None
User Privileges	Evaluates the privileges of the user logged into the local device.	None
Virtualized	Evaluates if the local device is virtualized.	None
VPN Connected	Evaluates if a network adapter of the local device is connected to a VPN network.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Evaluates if the local 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 local device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Splunk	Records the status of the local 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.

© 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 hides or denies access to applications in the session outside of working hours. It can be found in the `TIME-BASED ACCESS` category when filtered for `LOCAL` 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 local environment. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your local environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console and License) are not yet installed, please visit the Getting Started for Local guide and complete step 1 to 4 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following context:

© 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: `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*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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*
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: `COUNTRY None Of AUTHORIZED_COUNTRY_1,...` *Replace AUTHORIZED_COUNTRY_X 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*

© 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.

Time-based Access Templates

Controls access to the session or applications when accessed outside of working hours.

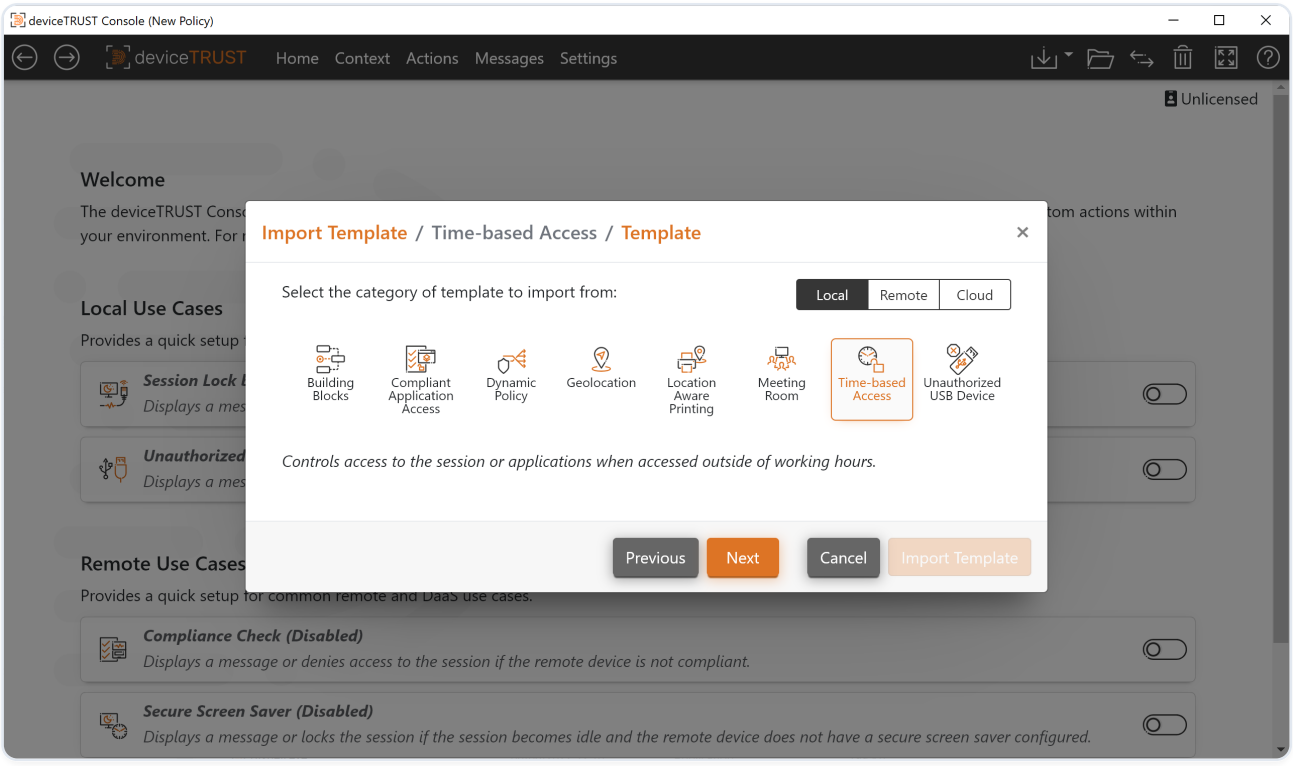


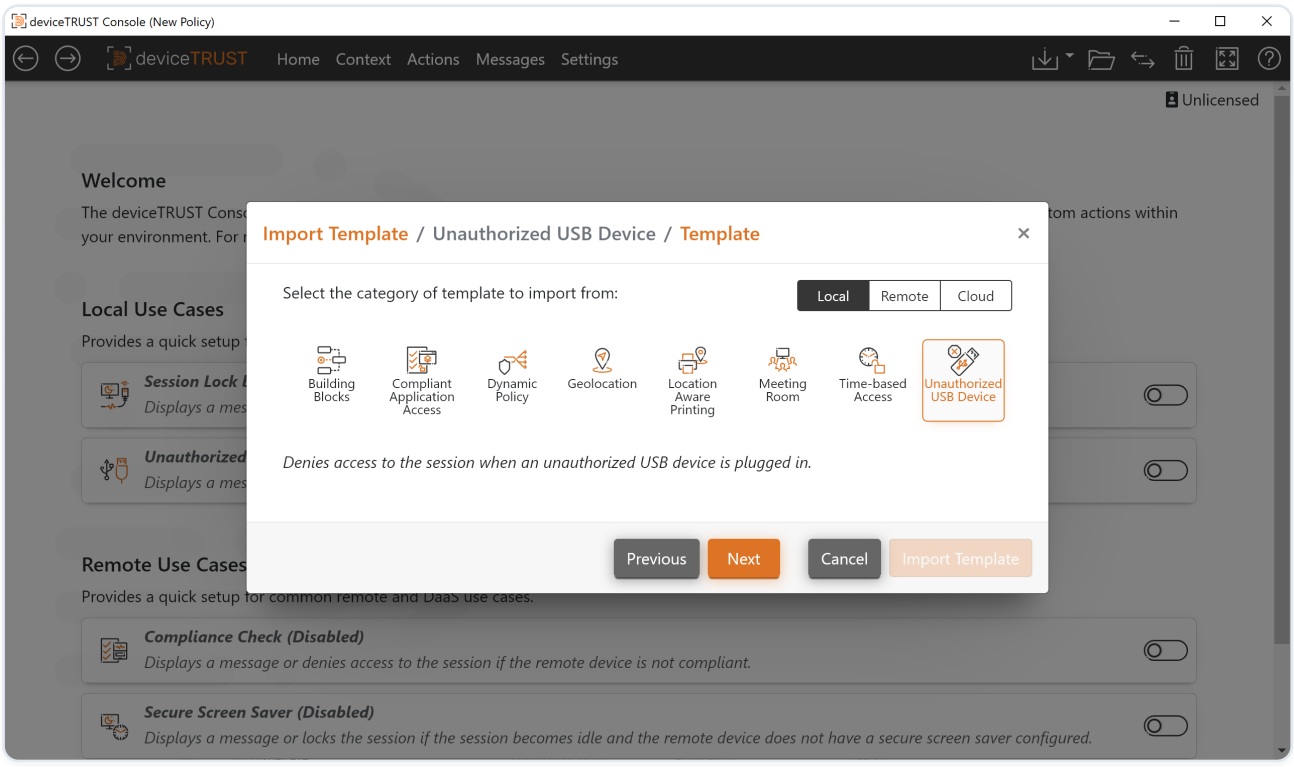
TABLE OF CONTENTS

- Conditional Application Access - Hides or denies access to applications in the session outside of working hours.

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

Unauthorized USB Drives Templates

Denies access to the session when an unauthorized USB device is plugged in.



Access Mode Template

This template imports a predefined context that defines whether the remote device is an internal or external device on the corporate network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 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: Context

The template has imported the following context:

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 with your remoting hosts dns suffix.**Example: *.demo.devicetrust.local:3389*

© 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.

Citrix Workspace App Template

This template imports a predefined context that defines whether a supported version of the Citrix Workspace app is installed on the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Citrix Workspace App Version	Defines if a supported version of the Citrix Workspace App is installed on the remote device.	You must update the following context condition with data suitable for your environment: `LOCAL - REMOTE CONTROL REMOTE VERSION Greater Than Or Equals 20.1` *Configure the minimal Citrix Workspace*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		App version for your environment. Example: 20.1

Troubleshooting

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

Computer Certificate Template

This template imports a predefined context that defines whether a valid computer certificate is available on the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Computer Certificate	Defines if a valid corporate computer certificate is available on the remote device.	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 - CERTIFICATE ROOT NAME Equals ADD_ROOT_NAME` *Replace ADD_ROOT_NAME with your root certification authority (CA) name. Example: deviceTRUST Demo CA*
		REMOTE - CERTIFICATE ROOT THUMPRINT SHA256 Equals ADD_ROOT_THUMPRINT` *Replace ADD_ROOT_THUMPRINT with your root certification authority (CA) thumprint SHA256 value. Example: deviceTRUST Demo CA*

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 imports a predefined action that hides or denies access to applications in the session, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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
Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session.	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. Example: notepad++.exe*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session.	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*

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 imports a predefined context that defines whether the remote device is a corporate managed device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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_ID 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

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
		`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*

© 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.

Country Template

This template imports a predefined context that defines the country in which the remote device is located, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None

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.

Country Provider Template

This template imports a predefined context that defines the country provider that reports the country in which the remote device is located, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country of the remote device.	None

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.

Device Location IP Address Template

This template imports a predefined context that defines the location of a remote device based on its IP address, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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 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*

© 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.

Device Location NetBIOS Name Template

This template imports a predefined context that defines the location of a remote device based on its NetBIOS name, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		the target location. Example: DE-SG01

Troubleshooting

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

Device Type Contractor Template

This template imports a predefined context that defines the device type of the remote device as Contractor or Corporate, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Type	Defines the remote device device type.	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 - DOMAIN ID Any Of 2 ITEMS` *When using AD or Microsoft Entra ID domain joined devices, replace DOMAIN_SID and AZURE_TENANT_ID 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*
		`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: 0d57fdd21474ef7806818a66*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		1a5f1d1cb3361a8bb4ccd660dae6930a6a135a56
		`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*

Troubleshooting

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

Device Type Corporate Template

This template imports a predefined context that defines the device type of the remote device as Corporate or Unknown, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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_ID 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*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
		`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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		eLux Scout Server certificate thumprint.**Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*

Troubleshooting

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

deviceTRUST Client Extension Availability Template

This template imports a predefined context that defines the availability of the deviceTRUST Client Extension on the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

© 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

Troubleshooting

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

Building Blocks Templates

Individual contexts and actions that can be used as building blocks within your configuration.

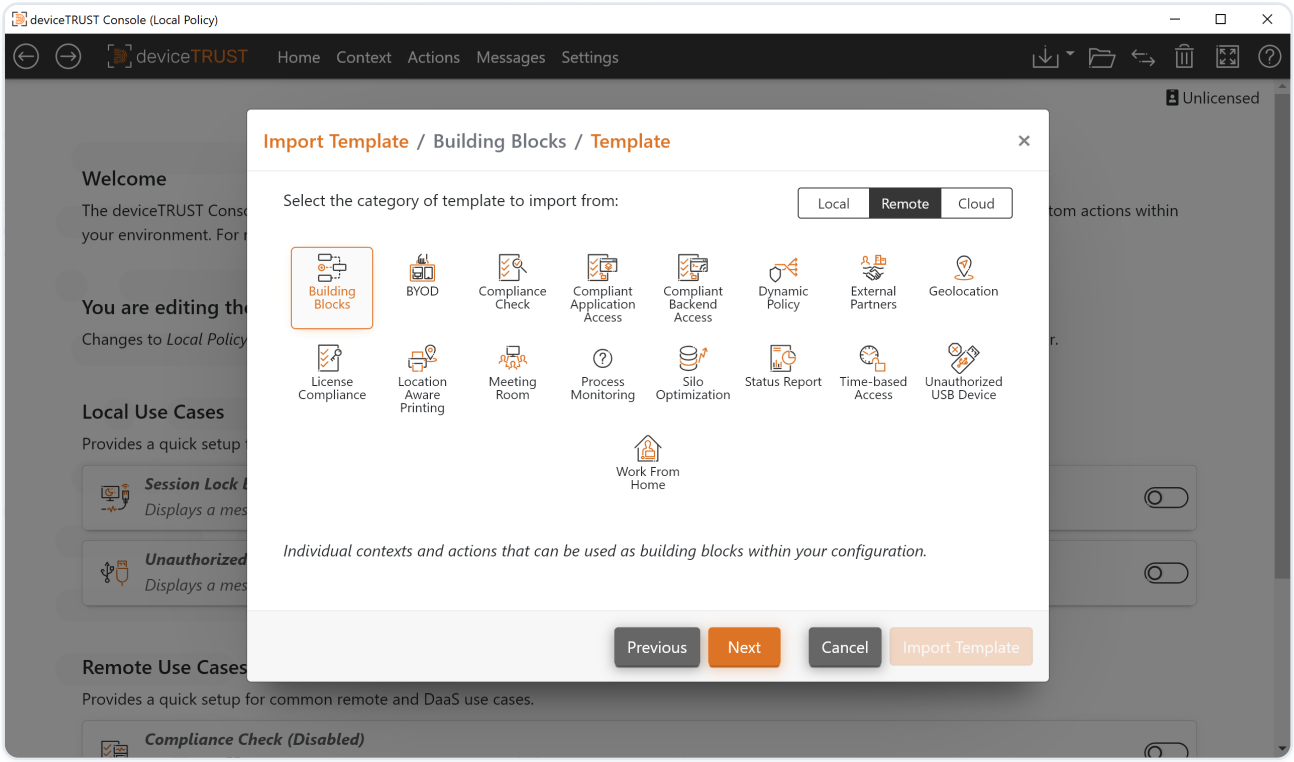


TABLE OF CONTENTS

- Access Mode - Defines if the remote device is internal or external to the corporate network.
- Citrix Workspace App - Defines if a supported version of the Citrix Workspace app is installed on the remote device.
- Computer Certificate - Defines if a valid computer certificate is available on the remote device.
- Conditional Application Access - Hides or denies applications within the session.

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

- Corporate Device - Defines if the remote device is a corporate managed device.
- Country - Defines the country in which the remote device is located.
- Country Provider - Defines the country provider that reports the country in which the remote device is located.
- Device Location IP Address - Defines the location of a remote device based on its IP address.
- Device Location NetBIOS Name - Defines the location of a remote device based on its NetBIOS name.
- Device Location Wi-Fi Access Point - Defines the location of a remote device based on its connected Wi-Fi access point.
- Device Type Contractor - Defines the device type of the remote device as Contractor or Corporate.
- Device Type Corporate - Defines the device type of the remote device as Corporate or Unknown.
- deviceTRUST Client Extension Availability - Defines the availability of the deviceTRUST Client Extension on the remote device.
- Operating System - Defines if the operating system of the remote device is supported.
- Operating System Update - Defines if a recent update search has been performed and that critical updates have been installed on the remote device.
- Override - Defines if the session user is a member of the override AD group.
- Policy Mode from AD Group - Defines if the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group.
- Policy Mode from Date - Defines if the deviceTRUST policy runs in active or passive mode based upon a fixed date.
- Process Monitoring - Evaluates if an application is running on the remote device. Uses a custom property for evaluation.
- Proximity - Defines the proximity of the remote device to a given position.
- Remote Controlled - Defines if the remote device is remote controlled.
- Security State - Defines the security state of the remote device.
- Session Idle - Defines if the session is idle.
- Threat Detection - Defines if the remote device has been recently scanned and has no current threats.

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

- Unauthorized USB Device - Defines if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.
- User Privileges - Defines the privileges of the user logged into the remote device.
- Virtualized - Defines if the remote device is virtualized.
- VPN Connected - Defines if a network adapter of the remote device is connected to a VPN network.
- Wi-Fi Security Mode - Defines if the remote device is connected to a secure Wi-Fi network.
- Working Time - Defines if the current time is within work hours.

Operating System Template

This template imports a predefined context that defines whether the operating system of the remote device is supported, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System	Defines if the operating system of the remote device is supported.	None

Troubleshooting

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

Operating System Update Template

This template imports a predefined context that defines if a recent update search has been performed and that critical updates have been installed on the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Update	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None

Troubleshooting

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

Override Template

This template imports a predefined context that defines whether the session user is a member of the override AD group, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

Troubleshooting

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

Policy Mode from AD Group Template

This template imports a predefined context that defines whether the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Policy Mode	Defines if the deviceTRUST policy runs in active or passive mode based upon the membership of an AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to activate the deviceTRUST policy for those users.

Troubleshooting

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

Policy Mode from Date Template

This template imports a predefined context that defines whether the deviceTRUST policy runs in active or passive mode based upon a fixed date, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Policy Mode	Defines if the deviceTRUST policy runs in active or passive mode based upon a date.	You must set a date to run the deviceTRUST policy in active or passive mode.

Troubleshooting

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

Process Monitoring Template

This template imports a predefined context that evaluates if an application is running on the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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: Settings

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Process State - Your App	Evaluates if Your App is running on the remote device. Uses a custom property for evaluation.	You must update the following context condition with data suitable for your environment
		`LOCAL - CUSTOM` *Ensure %REMOTE_CUSTOM_YOURAPP_RUNNING% reflects the custom property created by the Custom Properties on the Remote Windows Device.*

Step 3: Settings

The template has imported the following settings:

SETTINGS	DESCRIPTION	CUSTOMIZATIONS
Custom Properties	The Remote Windows Device section of Custom Properties has been customised to monitor the running processes.	You must update the following setting with data suitable for your environment
		`CUSTOM PROPERTIES - REMOTE WINDOWS DEVICE` *Ensure the call to Get-Process is monitoring the process of interest, and that the REMOTE_CUSTOM_YOURAPP_RUNNING property name is reflected in the Process State - Your App context.*

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.

Proximity Template

This template imports a predefined context that defines the proximity of the remote device to a given position, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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*

© 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.

Remote Controlled Template

This template imports a predefined context that defines whether the remote device is remote controlled, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remote Controlled	Defines if the remote device is remote controlled.	None

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.

Security State Template

This template imports a predefined context that defines the security state of the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Security State	Defines the security status of the remote device.	You must update the following context condition with data 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*

© 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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.**Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*

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.

Session Idle Template

This template imports a predefined context that defines if the session is idle, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines if the session is idle.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION IDLE PERIODE Greater Than 10` *Configure a maximum idle time in minutes for your environment. Example: 10*

© 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.

Threat Detection Template

This template imports a predefined context that defines whether the remote device has been recently scanned and has no current threat, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Threat Detection	Defines if the remote device has been recently scanned and has no current threats.	None

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.

Unauthorized USB Device Template

This template imports a predefined context that defines whether an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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 /*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		or Serial Number. Example: 0x0781,0x5567,4C53000011 0526106001 SanDisk Cruzer Blade USB Device.

Troubleshooting

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

User Privileges Template

This template imports a predefined context that defines the privileges of the user logged into the remote device, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
User Privileges	Defines the privileges of the user logged into the remote device.	None

Troubleshooting

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

Virtualized Template

This template imports a predefined context that defines whether the remote device is virtualized, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Virtualized	Defines if the remote device is virtualized.	None

© 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.

VPN Connected Template

This template imports a predefined context that defines whether a network adapter of the remote device is connected to a VPN network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None

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.

Wi-Fi Security Mode Template

This template imports a predefined context that defines whether the remote device is connected to a secure Wi-Fi network, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

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 imports a predefined context that defines whether the current time is within work hours, and can be used as a building block in your configuration. It can be found in the `BUILDING BLOCKS` 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 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remoteguide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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.*

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 remote device is compliant with BYOD policies. It can be found in the `BYOD (BRING YOUR OWN DEVICE)` category when filtered for `REMOTE` platform.

If the remote device is not compliant with BYOD policies, you can choose between two actions:

- Denies access to the session if the remote device is not compliant with BYOD policies.
- Displays a message within the session if the remote device is not compliant with BYOD policies.

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: Contexts
- 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 Remoteguide 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

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Type	Defines the remote device device type.	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_ID 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*
		`REMOTE - IGEL UMS CERT THUMPRINT SHA256 Equals UMS_CERTIFICATE_THUMBPRINT_SHA256` *When using IGEL OS devices, replace*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
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.

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 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*
		`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`

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`SCOUT_CERTIFICATE_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
Virtualized	Defines if the remote device is virtualized.	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 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
Compliance Check - Conditional Access - Enforcement	Denies access to the session if the remote BYOD is not compliant.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...` *Replace*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code. Example: US
Compliance Check - Conditional Access - Notification	Displays a message in the session if the remote BYOD 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*

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.

Conditional Application Access Template

This template creates a configuration that checks if the remote device is compliant with BYOD policies. It can be found in the `BYOD (BRING YOUR OWN DEVICE)` category when filtered for `REMOTE` platform.

If the remote device is not compliant with BYOD policies, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the remote BYOD is not compliant.
- Denies access to applications with Microsoft AppLocker within the session if the remote BYOD 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: Contexts
- 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 Remoteguide 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

© 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 Type	Defines the remote device device type.	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_ID 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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 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*
		`REMOTE - ELUX SCOUT NAME Equals SCOUT_NAME` *When using eLux devices, replace SCOUT_NAME with*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
Virtualized	Defines if the remote device is virtualized.	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 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
Compliance Check - Conditional Application Access -	Hides applications with FSLogix App Masking within the	Deactivated	You must update the following context condition with data

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - FSLogix App Masking	session if the remote BYOD is not compliant.		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 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*
Compliance Check - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote BYOD is not compliant.	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
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...` *Replace AUTHORIZED_COUNTRY_X 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.

BYOD (Bring Your Own Device) Templates

The BYOD templates control access to the session or applications when compliance requirements for BYOD users are not satisfied.

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

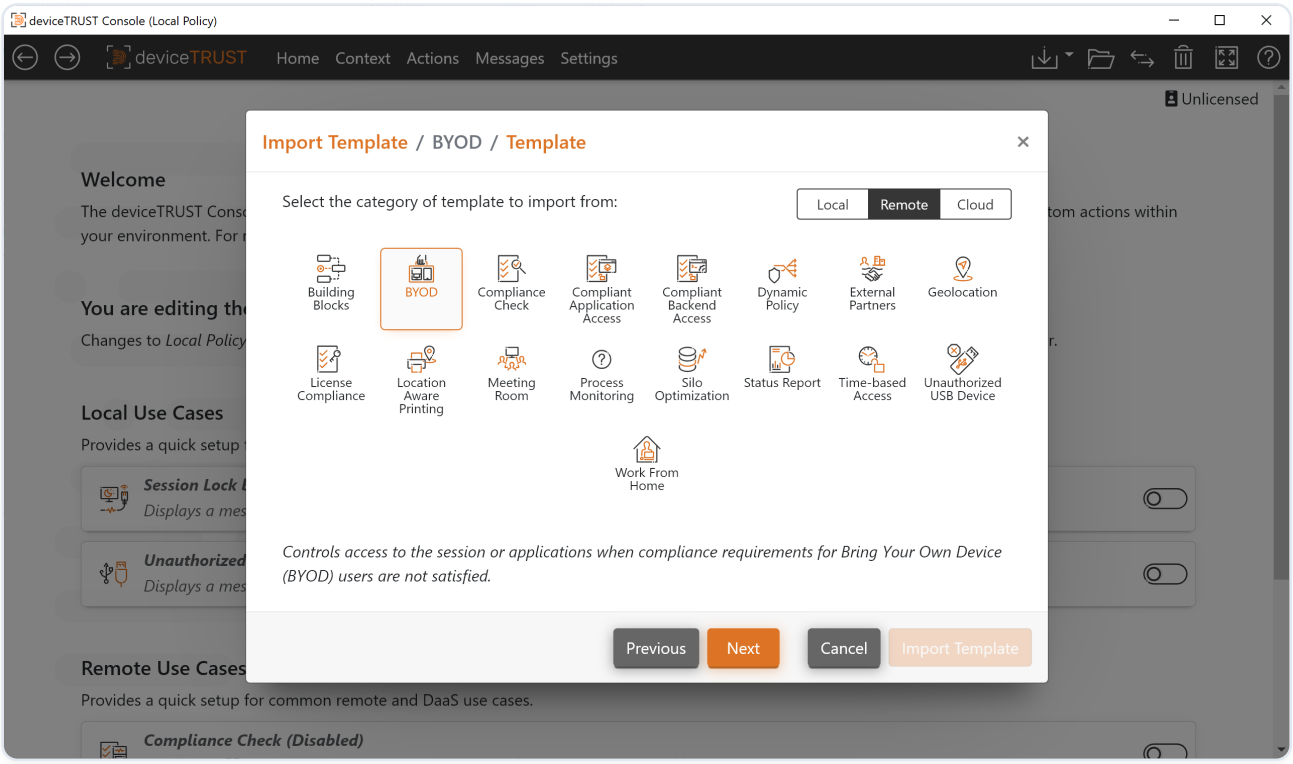


TABLE OF CONTENTS

- Conditional Access - Displays a message or denies access to the session if the remote device is not compliant with BYOD policies.
- Conditional Application Access - Hides or denies access to applications within the session if the remote device is not compliant with BYOD policies.

Compliance Check Template

This template creates a configuration that checks if the remote device is compliant. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is not compliant, you can choose between two actions:

- Denies access to the session if the remote device is not compliant.
- Displays a message in the session if the remote 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:

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

- Step 1: Prerequisites
- Step 2: Contexts
- 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 Remoteguide 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
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 suitable for your environment

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*
		`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: 0d57fdd21474ef7806818a66*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		1a5f1d1cb3361a8bb4ccd660dae6930a6a135a56
Virtualized	Defines if the remote device is virtualized.	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 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
Compliance Check - Conditional Access - Enforcement	Denies access to the session if the remote 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 the ISO 3166-1 Alpha-2 code. Example: US*

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

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Compliance Check - Conditional Access - Notification	Displays a message in the session if the remote 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*

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.

Computer Certificate Template

This template creates a configuration that checks if the remote device does provide a valid computer certificate. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device does not provide a valid computer certificate, you can choose between two actions:

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

- Denies access to the session if the remote device does not provide a valid computer certificate.
- Displays a message in the session if the remote device does not provide a valid computer certificate.

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: Contexts
- 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 Remoteguide 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
Computer Certificate	Defines if a valid corporate computer certificate is available on the remote device.	You must update the following context condition with data suitable for your environment
		`REMOTE - CERTIFICATE ROOT NAME Equals ADD_ROOT_NAME` *Replace ADD_ROOT_NAME with your root certification authority (CA) name. Example: deviceTRUST Demo CA*

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

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - CERTIFICATE ROOT THUMPRINT SHA256 Equals ADD_ROOT_THUMPRINT` *Replace ADD_ROOT_THUMPRINT with your root certification authority (CA) thumprint SHA256 value. Example: deviceTRUST Demo CA*

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
Computer Certificate - Conditional Access - Enforcement	Denies access to the session if the remote device does not provide a valid computer certificate.	Deactivated	None
Computer Certificate - Conditional Access - Notification	Displays a message in the session if the remote device does not provide a valid computer certificate.	Activated	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.

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 `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is not a corporate managed device, you can choose between two actions:

- Denies access to the session if the remote device is not a corporate managed device.
- Displays a message in 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: Contexts
- 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 Remoteguide 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
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_ID 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_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.

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

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
Corporate Device - Conditional Access - Enforcement	Denies access to the session if the remote device is not a corporate managed device.	Deactivated	None
Corporate Device - Conditional Access - Notification	Displays a message in the session if the remote device is not a corporate managed 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.

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 `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is not located within an authorized country, you can choose between two actions:

- Denies access to the session based on the country of the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Displays a message in 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: Contexts
- 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 Remoteguide 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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Country - Conditional Access - Enforcement	Denies access to 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*
Country - Conditional Access - Notification	Displays a message in the session based on the country of the remote device.	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*

© 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.

deviceTRUST Client Extension Availability Template

This template creates a configuration that checks if the remote device does have the deviceTRUST Client Extension installed. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device does not have the deviceTRUST Client Extension installed, you can choose between two actions:

- Denies access to the session if the deviceTRUST Client Extension is not installed on the remote device.
- Displays a message in the session if the deviceTRUST Client Extension is not installed on 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: Contexts
- 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 Remoteguide 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
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on 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 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
deviceTRUST Client Availability - Conditional Access - Enforcement	Denies access to the session if the deviceTRUST Client Extension is not installed on the remote device.	Deactivated	None
deviceTRUST Client Availability - Conditional Access - Notification	Displays a message in the session if the deviceTRUST Client Extension is not	Activated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	installed on the remote device.		

NOTE:

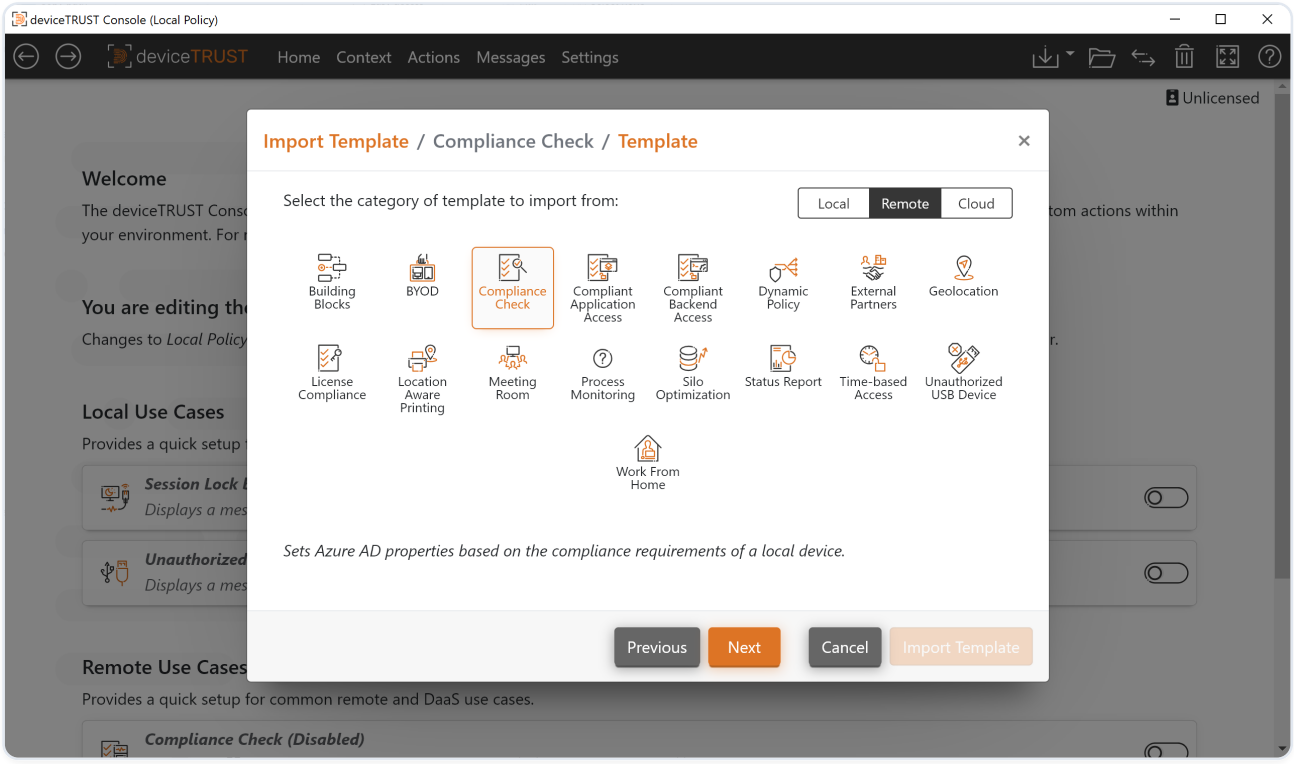
- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Compliance Check

Display a message or denies access to the session when compliance requirements on a remote device are not satisfied.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table of contents

- Compliance Check - Displays a message or denies access to the session if the remote device is not compliant.
- Computer Certificate - Displays a message or denies access to the session if the remote device does not provide a valid computer certificate.
- Corporate Device - Displays a message or denies access to the session if the remote device is not a corporate managed device.
- Country - Displays a message or denies access to the session based on the country of the remote device.
- deviceTRUST Client Extension Availability - Displays a message or denies access to the session if the remote device does not have the deviceTRUST Client Extension installed.
- Operating System - Displays a message or denies access to the session if the operating system of the remote device is not supported.
- Operating System Update - Displays a message or denies access to the session if the operating system of the remote device has not performed a recent update search or has outstanding critical updates.
- Remote Controlled - Displays a message or denies access to the session if the remote device is remote controlled.
- Security State - Displays a message or denies access to the session based on the security state of the remote device.
- Threat Detection - Displays a message or denies access to the session if a threat is detected or the remote device has not been scanned recently.
- User Privileges - Displays a message or denies access to the session based on the privileges of the user logged into the remote device.
- Virtualized - Displays a message or denies access to the session if the remote device is virtualized.
- Wi-Fi Security Mode - Displays a message or denies access to the session if the remote device is connected to an insecure Wi-Fi network.

Operating System Template

This template creates a configuration that checks if the operating system of the remote device is supported. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the operating system of the remote device is not supported, you can choose between two actions:

- Denies access to the session if the operating system of the remote device is not supported.
- Displays a message in the session if the operating system of the remote device is not supported.

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: Contexts
- 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 Remoteguide 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
Operating System	Defines if the operating system of the remote device is supported.	None

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 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
Operating System - Conditional Access - Enforcement	Denies access to the session if the operating system of the remote device is not supported.	Deactivated	None
Operating System - Conditional Access - Notification	Displays a message in the session if the operating system of the remote device is not supported.	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.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Remote Controlled Template

This template creates a configuration that checks if the remote device is remote controlled. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is remote controlled, you can choose between two actions:

- Denies access to the session if the device is remote controlled.
- Displays a message in the session if the device is remote controlled.

© 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: Contexts
- 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 Remoteguide 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
Remote Controlled	Defines if the remote device is remote controlled.	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 an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Remote Controlled - Conditional Access - Enforcement	Denies access to the session if the device is remote controlled.	Deactivated	None
Remote Controlled - Conditional Access - Notification	Displays a message in the session if the device is remote controlled.	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.

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 `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the security state of the remote device is unprotected, you can choose between two actions:

- Denies access to the session based on the security state of the remote device.
- Displays a message in the session 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Contexts
- 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 Remoteguide 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.	You must update the following context condition with data 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*

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
Security State - Conditional Access - Enforcement	Denies access to the session based on the	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	security state of the remote device.		
Security State - Conditional Access - Notification	Displays a message in the session based on the security state of 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.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Threat Detection Template

This template creates a configuration that checks if a threat is detected or the remote device has not been scanned recently. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If a threat is detected or the remote device has not been scanned recently, you can choose between two actions:

- Denies access if a threat is detected or the device has not been scanned recently.
- Displays a message in the session if a threat is detected or the device has not been scanned recently.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 Remoteguide 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
Threat Detection	Defines if the remote device has been recently scanned and has no current threats.	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 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
Threat Detection - Conditional Access - Enforcement	Denies access if a threat is detected or the device has not been scanned recently.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Threat Detection - Conditional Access - Notification	Displays a message in the session if a threat is detected or the device has not been scanned recently.	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.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

User Privileges Template

This template creates a configuration that checks the privileges of the user logged into the remote device. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the privileges of the user logged into the remote device are privileged without protection, you can choose between two actions:

- Denies access to the session based on the privileges of the user logged into the remote device.
- Displays a message in the session based on the privileges of the user logged 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Contexts
- 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 Remoteguide 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
User Privileges	Defines the privileges of the user logged into 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 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
User Privilege - Conditional Access - Enforcement	Denies access to the session based on the privileges of the user logged into the remote device.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
User Privilege - Conditional Access - Notification	Displays a message in the session based on the privileges of the user logged 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.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Virtualized Template

This template creates a configuration that checks if the remote device is virtualized. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is virtualized, you can choose between two actions:

- Denies access to the session if the remote device is virtualized.
- Displays a message in the session if the remote device is virtualized.

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: Contexts
- 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 Remoteguide 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
Virtualized	Defines if the remote device is virtualized.	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 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
Virtualized - Conditional Access - Enforcement	Denies access to the session if the remote device is virtualized.	Deactivated	None
Virtualized - Conditional Access - Notification	Displays a message in the session if the remote device is virtualized.	Activated	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.

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 `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the remote device is connected to an insecure Wi-Fi network, you can choose between two actions:

- Denies access to the session if the remote device is connected to an insecure Wi-Fi network.
- Displays a message in 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: Contexts
- 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
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 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
Wi-Fi Security - Conditional Access - Enforcement	Denies access to the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	None
Wi-Fi Security - Conditional Access - Notification	Displays a message in the session if the remote device is connected to an insecure Wi-Fi network.	Activated	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.

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 `COMPLIANT APPLICATION ACCESS` category when filtered for `REMOTE` platform.

If the remote device is connected externally, you can choose between two actions:

- 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: Contexts
- 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
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 with your remoting hosts dns suffix.*Example:* .demo.devicetrust.local:3389*

© 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.

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 process name on all Terminate App tasks. Example: notepad++.exe*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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.

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 `COMPLIANT APPLICATION ACCESS` 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: Contexts
- 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_ID with your corporate values. Example: S-1-5-21-1397108472-4176295369-1616608269 for a domain SID.*

© 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 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*
		`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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*

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 managed 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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*
Corporate Device - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote device is not a corporate managed 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.

© 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.

Country Template

This template creates a configuration that checks the country of the remote device. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `REMOTE` platform.

If the remote device is not located within an authorized country, you can choose between two actions:

- 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: Contexts
- 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
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.

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*

© 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*
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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks. Example: %PROGRAMFILES%\Notepad++\notepad++.exe

NOTE:

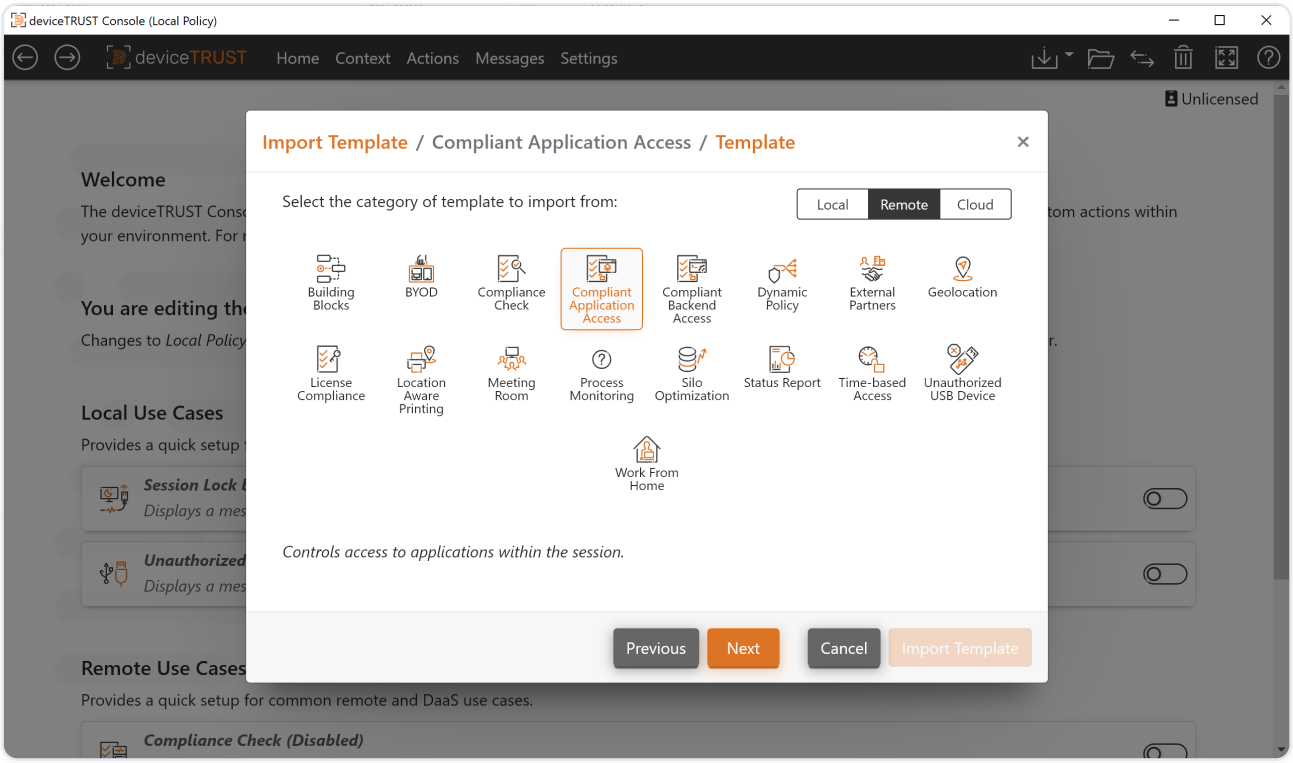
- If both actions have been disabled, the contexts will still be created.
- Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Compliant Application Access Templates

Controls access to applications within the session.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

TABLE OF CONTENTS

- Access Mode - Hides or denies access to applications in the session if the remote device is connected externally.
- Corporate Device - Hides or denies access to applications in the session if the remote device is not a corporate managed device.
- Country - Hides or denies access to applications in the session based on the country of the remote device.
- Proximity - Hides or denies access to applications in the session based on the proximity of the remote device to a given position.
- Security State - Hides or denies access to applications in the session based on the country of the remote device.
- Wi-Fi Security Mode - Hides or denies access to applications in the session when the remote device is connected to an insecure Wi-Fi network.
- Working Time - Hides or denies access to applications in the session when accessed outside of working hours.

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 `COMPLIANT APPLICATION ACCESS` 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Contexts
- 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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Proximity - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the proximity of the remote device to a given position.	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. Example: notepad++.exe*
Proximity - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the proximity of the remote device to a given position.	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.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 hides or denies access to applications in the session based on the security state of the remote device. It can be found in the `COMPLIANT APPLICATION ACCESS` category when filtered for `REMOTE` platform.

If the security state of the remote device is unprotected, you can choose between two actions:

- Hides applications with FSLogix App Masking based on the security state.
- Denies access to applications with Microsoft AppLocker based on the security state.

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: Contexts
- 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
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.

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:*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			%ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP` *Replace ENTER_PROCESS_NAME_HERE with your target process name on all Terminate App tasks. 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.

© 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 `COMPLIANT APPLICATION ACCESS` 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: Contexts
- 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. Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa* `TERMINATE APP` *Replace ADD_PROCESS_N*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AME_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 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 `COMPLIANT APPLICATION ACCESS` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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: Contexts
- 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.*

© 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.

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. Example: notepad++.exe*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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.

Conditional Access Template

This template creates a configuration that checks if the remote device is compliant for accessing backend servers. It can be found in the `COMPLIANT BACKEND ACCESS` category when filtered for `REMOTE` platform.

If the remote device is not compliant for accessing backend servers, you can choose between two actions:

- Denies access to the session if the remote device is not compliant or corporate managed.
- Displays a message in the session if the remote device is not compliant or corporate managed.

© 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: Contexts
- 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_ID with your corporate values. Example: S-1-5-21-1397108472-4176295369-1616608269 for a domain SID.*
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*
		`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`Equals` `SCOUT_CERTIFICATE_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.**Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
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 Type	Defines the remote device device type.	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 suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*
		`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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		thumprint.**Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
Virtualized	Defines if the remote device is virtualized.	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 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
Compliance Check - Conditional Access - Enforcement	Denies access to the session if the remote device is not compliant or corporate managed.	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Alpha-2 code.**Example: US*
Compliance Check - Conditional Access - Notification	Displays a message in the session if the remote device is not compliant or corporate managed.	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*

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.

Compliant Backend Access Templates

Display a message or denies access to backend servers when compliance requirements are not satisfied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

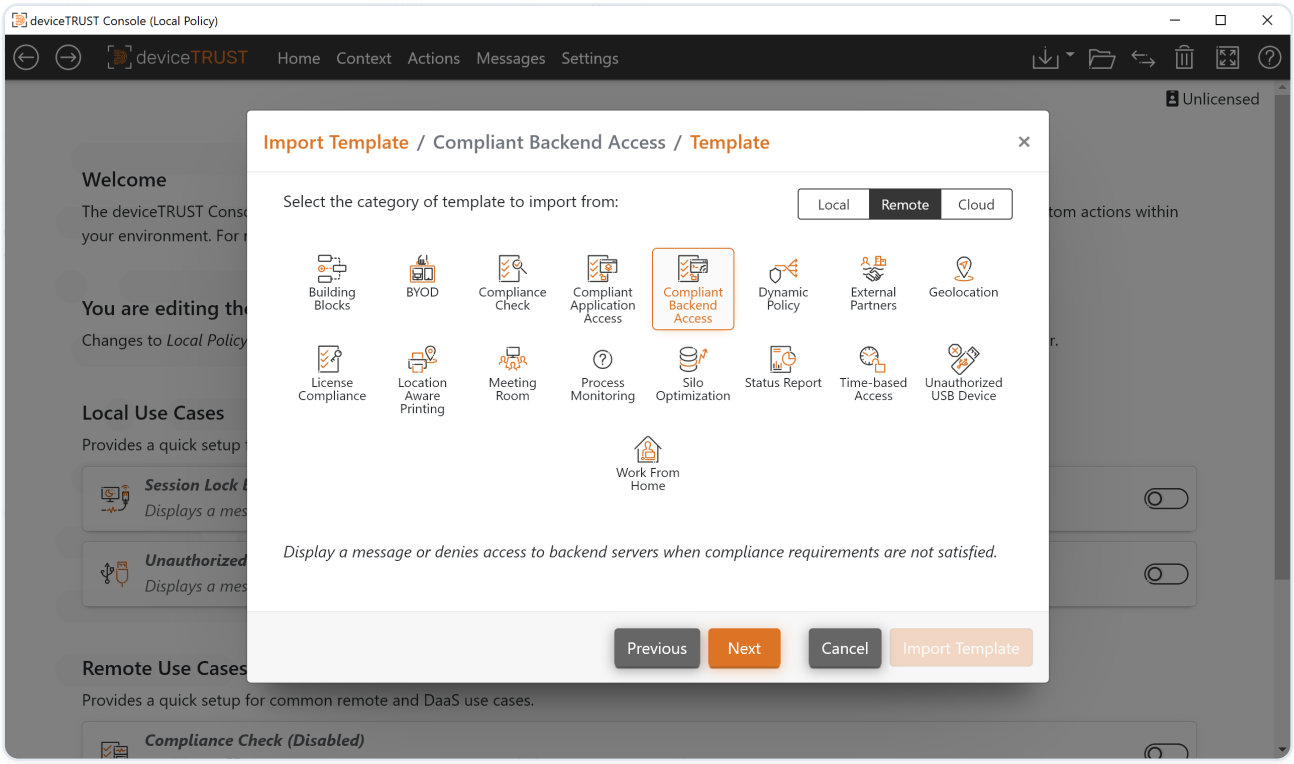


TABLE OF CONTENTS

- Conditional Access - Displays a message or denies access to the session if the remote device is not compliant for accessing backend servers.

Amazon DCV Clipboard Security State Template

This template creates a configuration that applies Amazon DCV clipboard policy within the session based on the security state of the remote device. It can be found in the `DYNAMIC POLICY` 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: Contexts
- 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
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 enforcement action that actively controls access to the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Amazon DCV Settings - Security State	Applies Amazon DCV clipboard policy within the session based on the security state of the remote device.	Activated	None

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.

Citrix Policy Access Mode Template

This template creates a configuration that applies Citrix policies within the session based on whether the remote device is accessing internally or externally. It can be found in the `DYNAMIC POLICY` 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: Contexts
- 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.

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 - Citrix Policies - Access Mode	Applies Citrix Policies within the session based on whether the remote device is accessing internally or externally.	Activated	You must update the following context condition with data suitable for your environment
		`CITRIX POLICY DISABLED` *Configure the Citrix policies to be disabled within the task.*	
		`CITRIX POLICY ENABLED` *Configure the Citrix policies to be enabled within the task.*	

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.

Citrix Policy Corporate Device Template

This template creates a configuration that applies Citrix policies within the session based on whether the remote device is a corporate managed device. It can be found in the `DYNAMIC POLICY` 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: Contexts
- 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_ID with your corporate values. Example: S-1-5-21-1397108472-4176295369-1616608269 for a domain SID.*
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*
		`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`SCOUT_CERTIFICATE_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 enforcement action that actively configures the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Citrix Policies - Corporate Device	Applies Citrix Policies within the session based on whether the remote device is a corporate managed device.	Activated	You must update the following context condition with data suitable for your environment
		`CITRIX POLICY DISABLED` *Configure the Citrix policies to be disabled within the task.*	
		`CITRIX POLICY ENABLED` *Configure the Citrix policies to be enabled within the task.*	

© 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.

Citrix Policy Wi-Fi Security Mode Template

This template creates a configuration that applies Citrix policies within the session if the remote device is connected to an insecure Wi-Fi network. It can be found in the `DYNAMIC POLICY` 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: Contexts
- 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 enforcement action that actively configures the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Conditional Configuration - Citrix Policies - Wi-Fi Security Mode	Applies Citrix Policies within the session based on the secure Wi-Fi network of the remote device.	Activated	You must update the following context condition with data suitable for your environment
		`CITRIX POLICY DISABLED` *Configure the Citrix policies to be disabled within the task.*	
		`CITRIX POLICY ENABLED` *Configure the Citrix policies to be enabled within the task.*	

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dynamic Policy Templates

Applies a dynamic policy within the session.

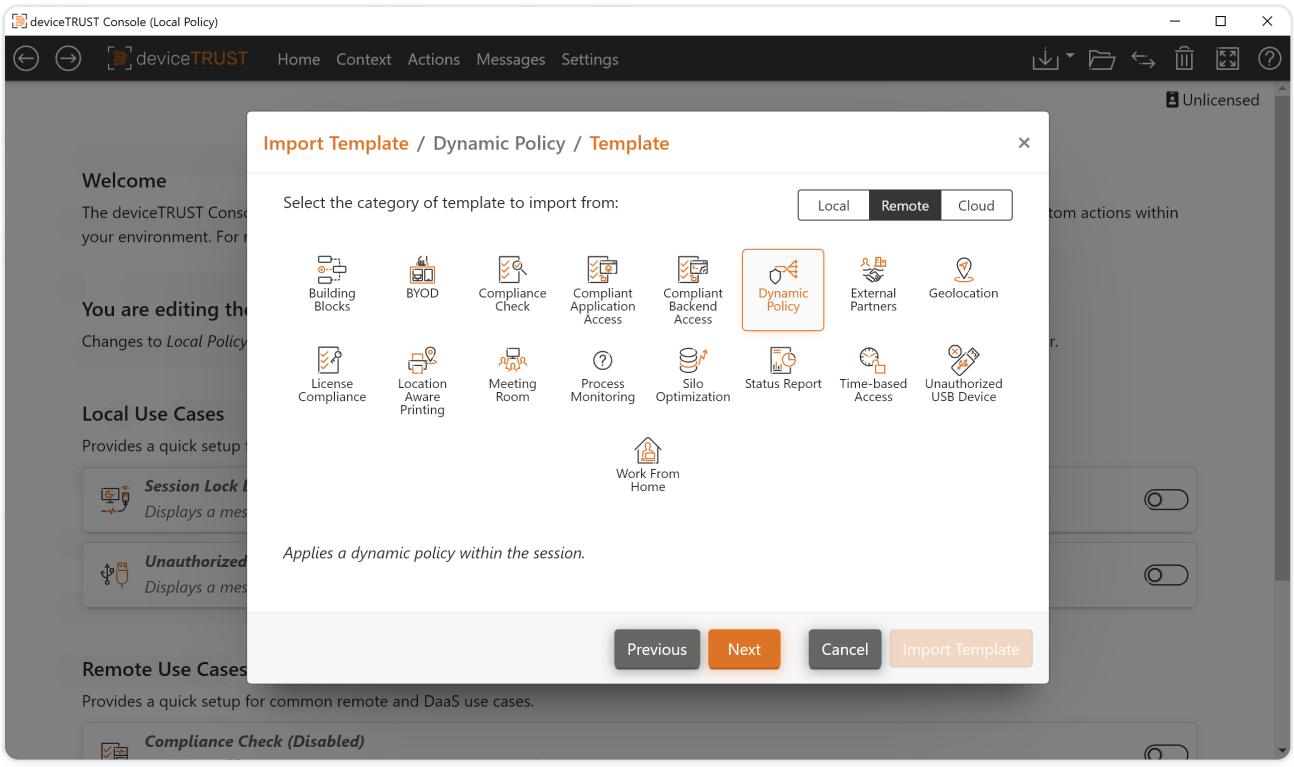


TABLE OF CONTENTS

- Amazon DCV Clipboard Security State - Applies Amazon DCV clipboard policy within the session based on the security state of the remote device.
- Citrix Policy Access Mode - Applies Citrix policies within the session based on whether the remote device is accessing internally or externally.
- Citrix Policy Corporate Device - Applies Citrix policies within the session based on whether the remote device is a corporate managed device.
- Citrix Policy Wi-Fi Security Mode - Applies Citrix policies within the session if the remote device is connected to an insecure Wi-Fi network.
- Secure Screen Saver - Locks the session if the session becomes idle and the remote devices does not have a secure screen saver configured.

Secure Screen Saver Template

This template creates a configuration that locks the session if the session becomes idle and the remote devices does not have a secure screen saver configured. It can be found in the `DYNAMIC POLICY` 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: Contexts
- 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
Session Idle	Defines the idle state of the session based on the screen saver configuration of a 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 enforcement action that actively controls access to the session. By default, the enforcement action is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Session Idle - Conditional Access - Enforcement	Locks the session if the session becomes idle.	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.

Conditional Access Template

This template creates a configuration that checks if the remote device is compliant with contractor policies. It can be found in the `EXTERNAL PARTNERS` category when filtered for `REMOTE` platform.

If the remote device is not compliant with contractor policies, you can choose between two actions:

- Denies access to the session if the contractor's device is not compliant.
- Displays a message in the session if the contractor's 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:

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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
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 Type	Defines the remote device device type.	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_ID 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
		`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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		eLux Scout Server certificate thumprint.**Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
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 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_THUM*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		BPRINT_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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
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 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
Compliance Check - Conditional Access - Enforcement	Denies access to the session if the contractor's 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 the ISO 3166-1 Alpha-2 code. Example: US*
Compliance Check - Conditional Access - Notification	Displays a message in the session if the contractor's 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Alpha-2 code. Example: US

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.

Conditional Application Access Template

This template creates a configuration that checks if the remote device is compliant with contractor policies. It can be found in the `EXTERNAL PARTNERS` category when filtered for `REMOTE` platform.

If the remote device is not compliant with contractor policies, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the contractor's device is not compliant.
- Denies access to applications with Microsoft AppLocker within the session if the contractor's 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: Contexts

© 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
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 Type	Defines the remote device device type.	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_ID 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
		`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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THU*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		MBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56
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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint. Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*
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 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
Compliance Check - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the contractor's 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 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 FSLogix App Masking tasks. Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`TERMINATE APP` *Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks. Example: notepad++.exe*
Compliance Check - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the contractor's 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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

External Partners Templates

The external partners templates controls access to the session and applications when compliance requirements for external partners are not satisfied.

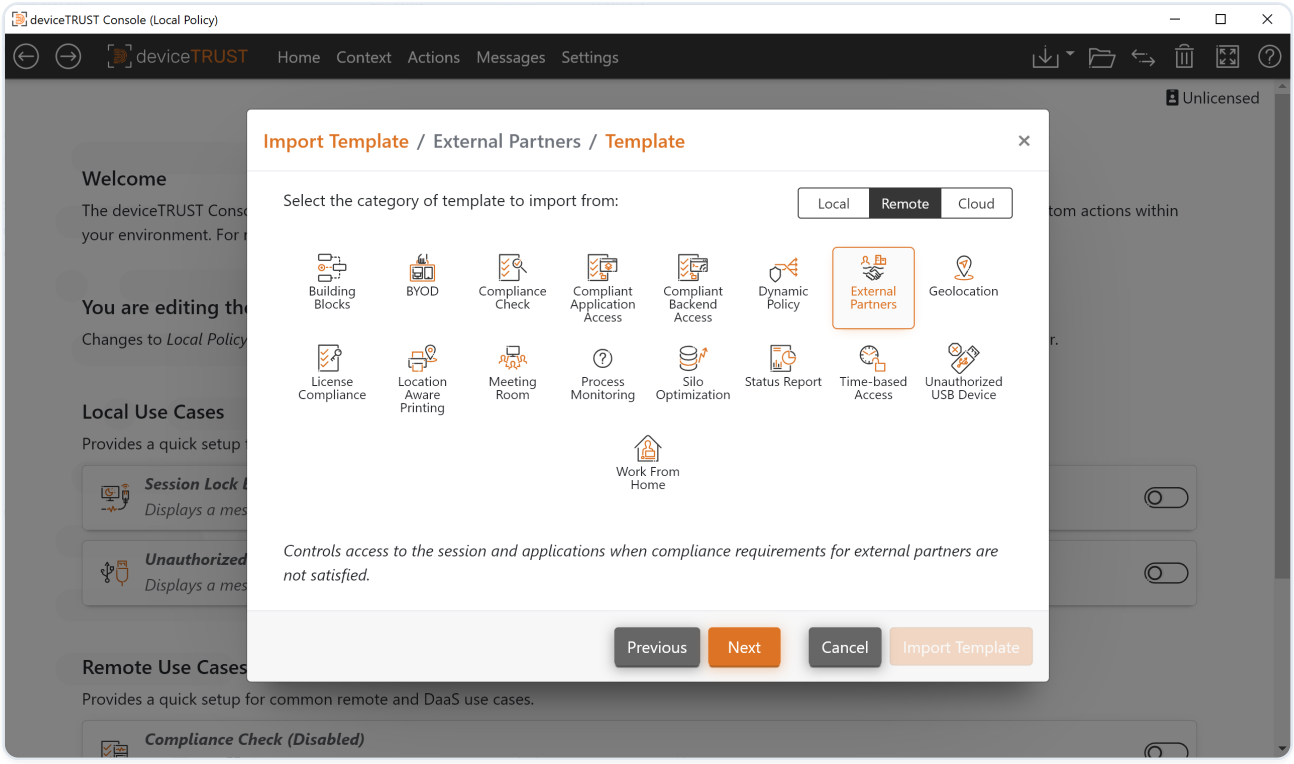


TABLE OF CONTENTS

- Conditional Access - Displays a message or denies access to the session if the remote device is not compliant with contractor policies.
- Conditional Application Access - Hides or denies access to applications within the session if the remote device is not compliant with contractor policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conditional Access for Country Template

This template creates a configuration that checks the country of the remote device. It can be found in the `GEOLOCATION` category when filtered for `REMOTE` platform.

If the remote device is not located within an authorized country, you can choose between two actions:

- Denies access to the session based on the country of the remote device.
- Displays a message in 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: Contexts
- 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

© 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
Country - Conditional Access - Enforcement	Denies access to 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*
Country - Conditional Access - Notification	Displays a message in the session based on the country of the remote device.	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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Alpha-2 code. *Example: US*

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.

Conditional Application Access for Country Template

This template creates a configuration that checks the country of the remote device. It can be found in the `GEOLOCATION` category when filtered for `REMOTE` platform.

If the remote device is not located within an authorized country, you can choose between two actions:

- 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: Contexts

© 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
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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`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 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*
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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AUTHORIZED_COUNTRY_X 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.

Conditional Application Access for 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 `GEOLOCATION` 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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: Contexts
- 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
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*

© 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.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Proximity - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the proximity of the remote device to a given position.	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. Example: notepad++.exe*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Proximity - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the proximity of the remote device to a given position.	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.

Geolocation Templates

Validates and controls access based on geolocation information of the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

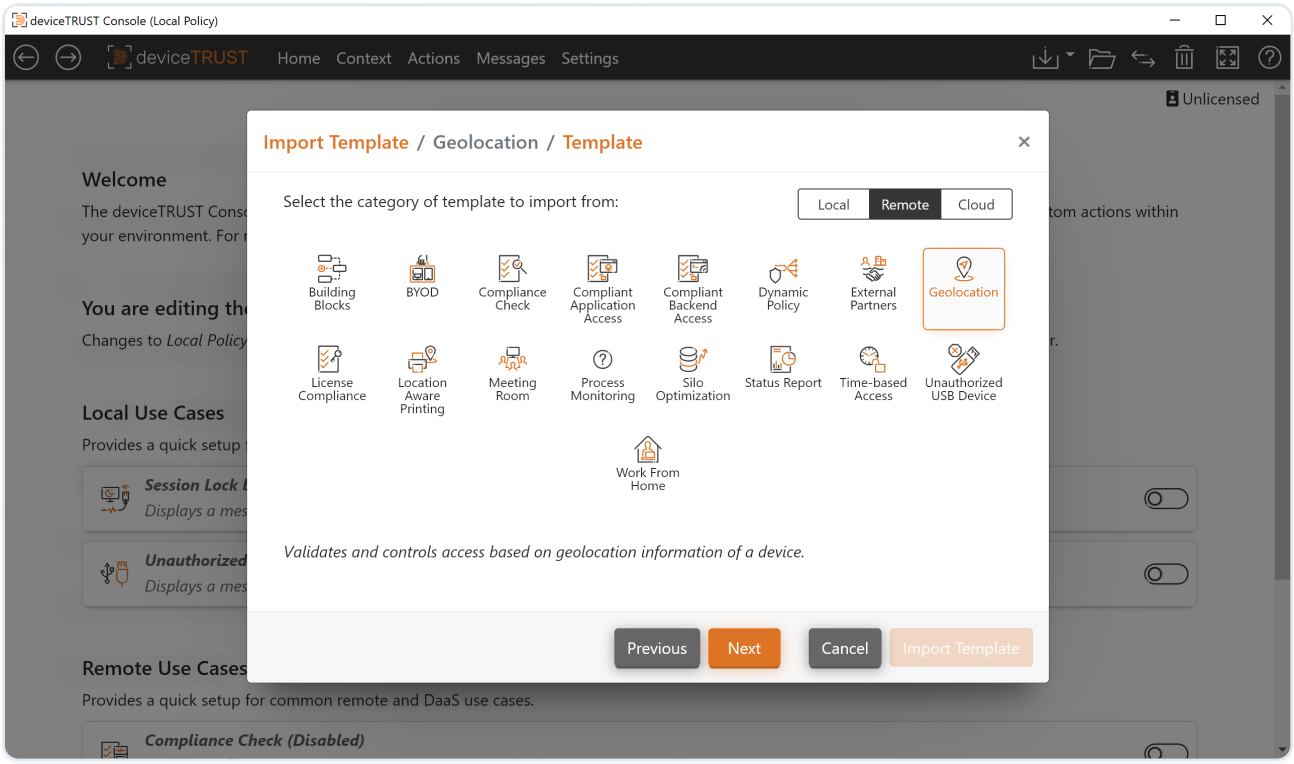


TABLE OF CONTENTS

- Conditional Access for Country - Displays a message or denies access to the session based on the country of the remote device.
- Conditional Application Access for Country - Hides or denies access to applications in the session based on the country of the remote device.
- Conditional Application Access for Proximity - Hides or denies access to applications in the session based on the proximity of the remote device to a given position.

License Compliance Templates

Controls access to applications within the session if the remote device is not licensed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

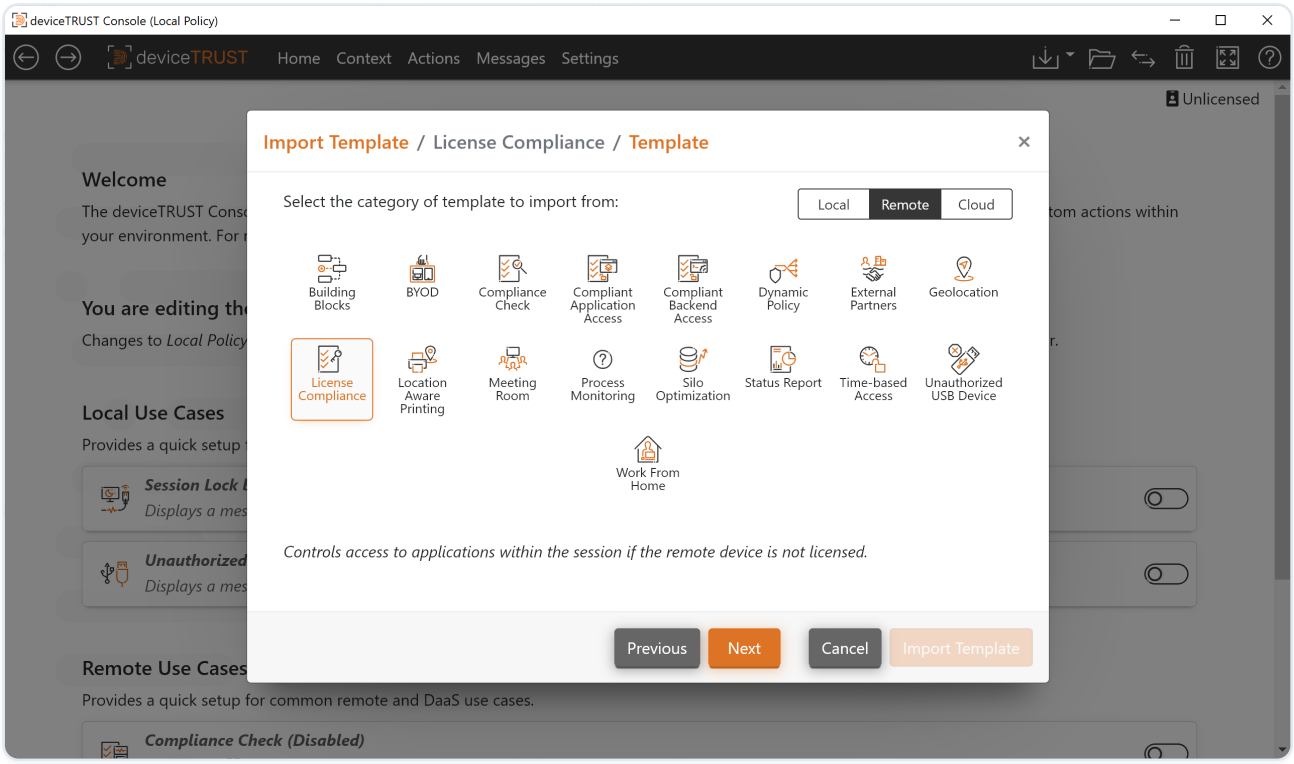


TABLE OF CONTENTS

- Adobe Reader DC - Reports, hides or denies Adobe Reader DC within the session if the remote device is not licensed.
- Microsoft Visio - Reports, hides or denies Microsoft Visio within the session if the remote device is not licensed.
- Nuance PDF - Reports, hides or denies Nuance PDF within the session if the remote device is not licensed.

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.

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

© 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: Contexts
- 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` *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\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*

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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\Rules\NotepadPlusPlus.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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			target configuration on all Microsoft 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. 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 OUR_ELKSTACK_S

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			ERVER: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_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 `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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: Contexts
- 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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` *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.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

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_N*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AME_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 Access - Reporting	Reports Nuance PDF licensing status.	Activated	You must update the following context condition with 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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: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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Location Aware Printing Templates

Maps network printers and defines a default printer based on the device placement within a building.

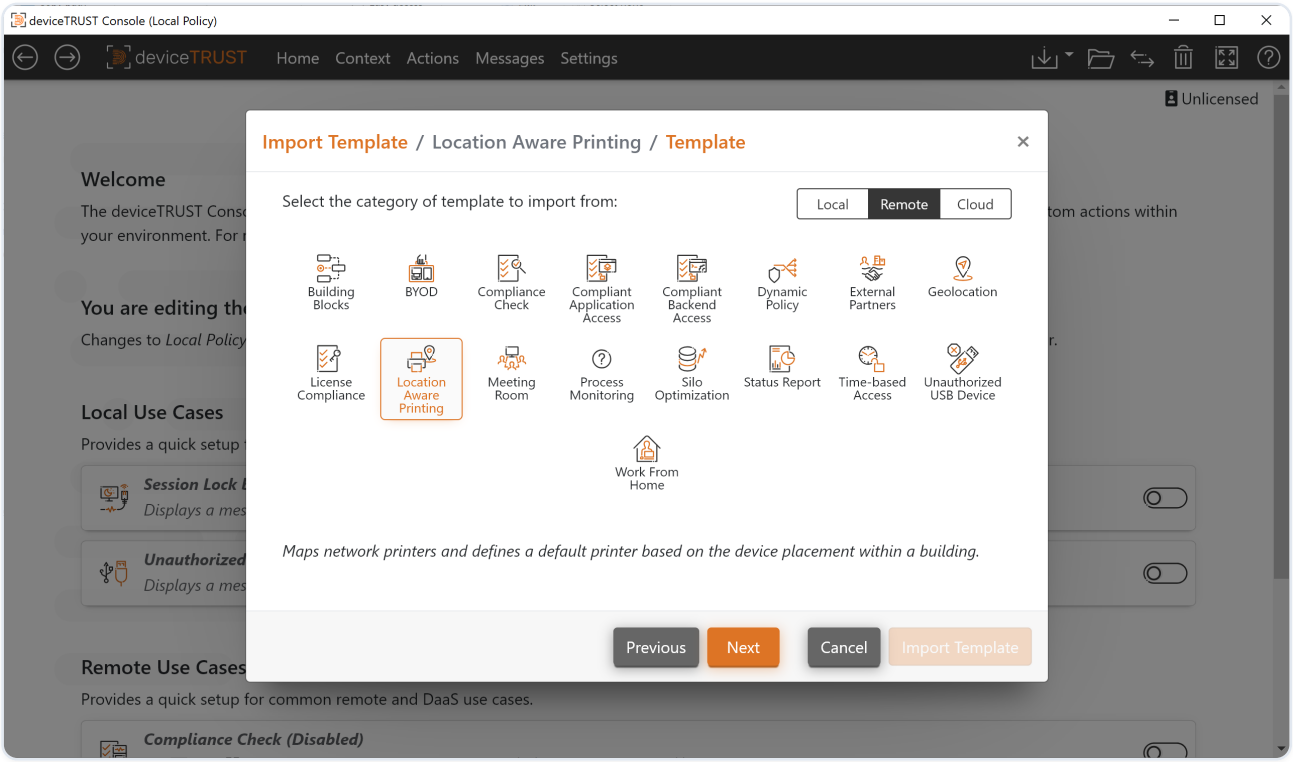


TABLE OF CONTENTS

- IP Address - Maps network printers and defines a default printer based on the location of the remote device using its IP address.
- NetBIOS Name - Maps network printers and defines a default printer based on the location of the remote device using its NetBIOS name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 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*

© 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 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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: \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.

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.

We will perform the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Contexts
- 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 `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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 `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.

Process Monitoring Templates

Controls access to applications or the session based on running processes on the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

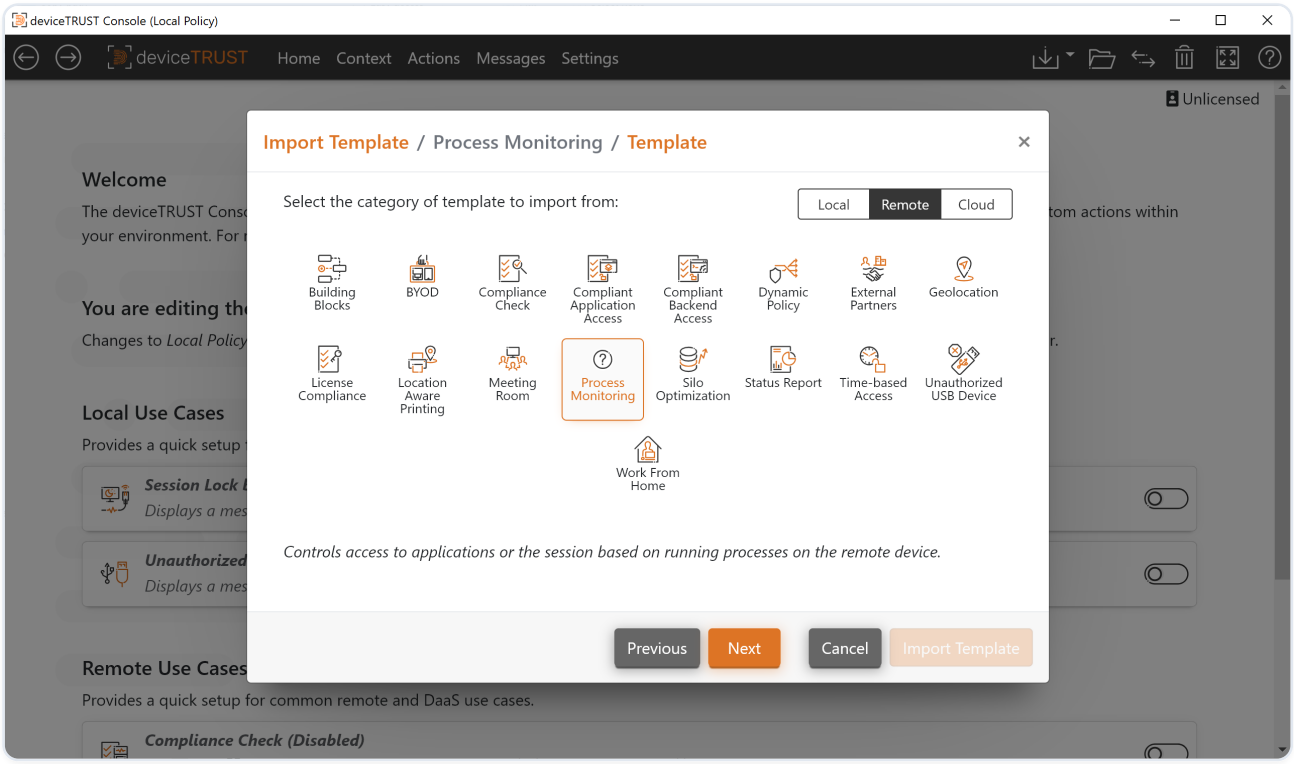


TABLE OF CONTENTS

- Microsoft Teams - Controls access to Microsoft Teams inside the virtual session if Microsoft Teams is running on the remote device.
- Snipping Tool - Denies access to the session if Snipping Tool is running on the remote device.

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.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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
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.

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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			\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

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.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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
Process Monitoring - SnippingTool	Evaluates if Snipping Tool 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

- 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: Contexts
- 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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 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.

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	Hides applications with FSLogix App	Deactivated	You must update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Application Access - Enforcement - FSLogix App Masking	Masking within the session if the remote device is connected externally.		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*
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*

© 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.

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: Contexts
- 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
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` *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\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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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
			`MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			configuration.**Example: dtldss02.demo.devicetrust.local:9200*
			`WEB REQUEST REPORT ADOBE 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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hides applications with FSLogix App Masking within the session if the remote device is not a corporate managed device.
- 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: Contexts
- 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_ID with your corporate values. Example: S-1-5-21-1397108472-41762*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		95369-1616608269 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*
		`REMOTE - IGEL UMS CERT THUMPRINT SHA256 Equals MS_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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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*

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 managed 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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*
Corporate Device - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote device is not a corporate managed 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.

© 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.

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:

- 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: Contexts
- 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
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

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
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 FSLogix*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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*
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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			%\Notepad++\notepad++.exe

NOTE:

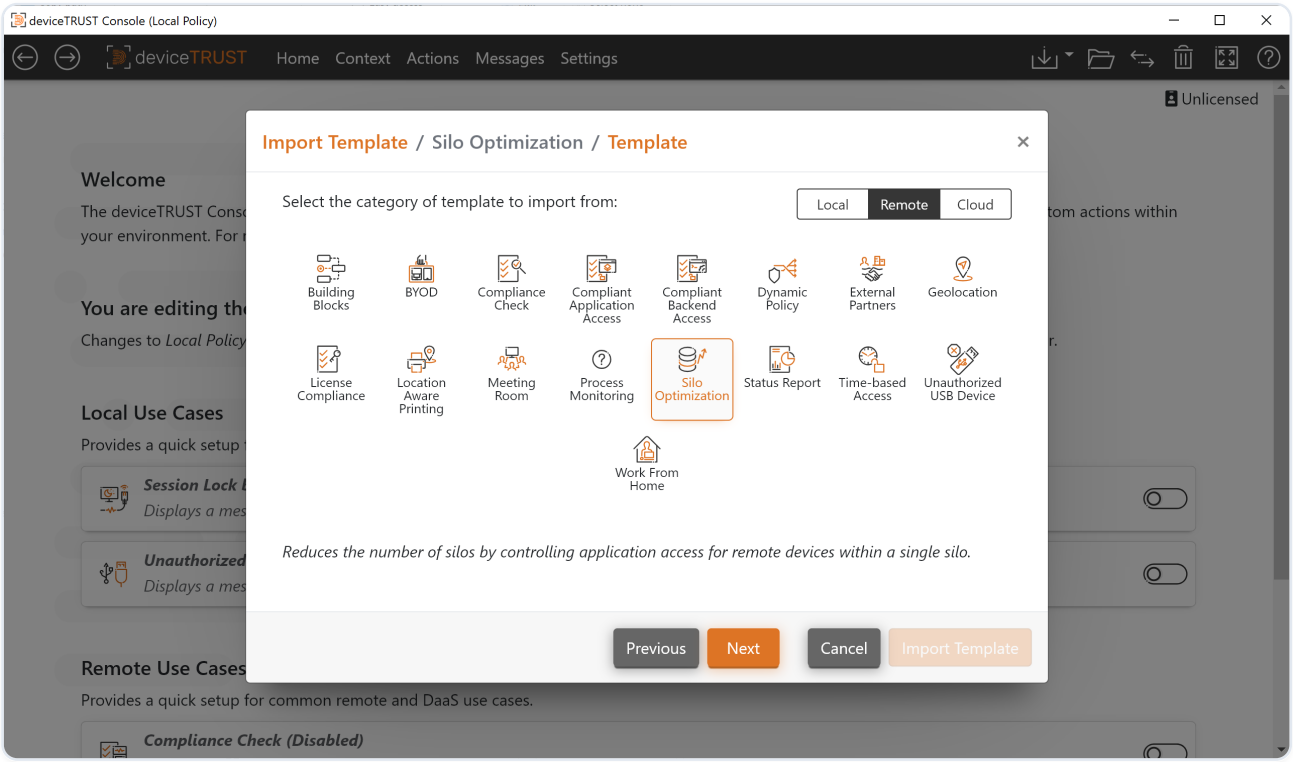
- If both actions have been disabled, the contexts will still be created.
- Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Silo Optimization Templates

Reduces the number of silos by controlling application access for remote devices within a single silo.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

TABLE OF CONTENTS

- Access Mode - Hides or denies access to applications in the session if the remote device is connected externally.
- Adobe Acrobat DC - Reports, hides or denies Adobe Acrobat DC within the session if the remote device is not licensed.
- Corporate Device - Hides or denies access to applications in the session if the remote device is not a corporate managed device.
- Country - Hides or denies access to applications in the session based on the country of the local device.
- Microsoft Visio - Reports, hides or denies Microsoft Visio within the session if the remote device is not licensed.
- Nuance PDF - Reports, hides or denies Nuance PDF within the session if the remote device is not licensed.
- Proximity - Displays a message and hides or denies applications in the session based on the proximity of the remote device to a given position.
- Security State - Displays a message and hides or denies applications in the session based on the country of the remote device.
- Wi-Fi Security Mode - Hides or denies access to applications in the session based on the proximity of the remote device to a given position.
- Working Time - Hides or denies access to applications in the session when accessed outside of working hours.

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.

© 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: Contexts
- 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` *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:*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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. 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*

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
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\Rules\NotepadPlusPlus.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

© 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*
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*
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO ELK STACK` *When using*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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_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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- 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: Contexts
- 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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 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\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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`TERMINATE APP` *Replace ADD_PROCESS_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 Access - Reporting	Reports Nuance PDF licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO SPLUNK` *When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SE*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			RVER: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: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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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: Contexts
- 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
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 - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the proximity of the remote device to a given position.	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*
Proximity - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the proximity of the remote device to a given position.	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.---

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:

- 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: Contexts
- 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

© 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.

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. Example: notepad++.exe*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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: Contexts
- 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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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*
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 AppLocker tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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
- Step 2: Contexts
- 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
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 -	Hides applications with FSLogix App Masking within the session when	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
FSLogix App Masking	accessed outside of working time.		`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*
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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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: Contexts
- 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.	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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		(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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

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.

© 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.

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 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: Contexts
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
Network Subnet	Defines the network subnet of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
Region Locale	Defines the region locale of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 - 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: Contexts
- 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.

Status Report Templates

Reports the status of the remote device to various destinations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

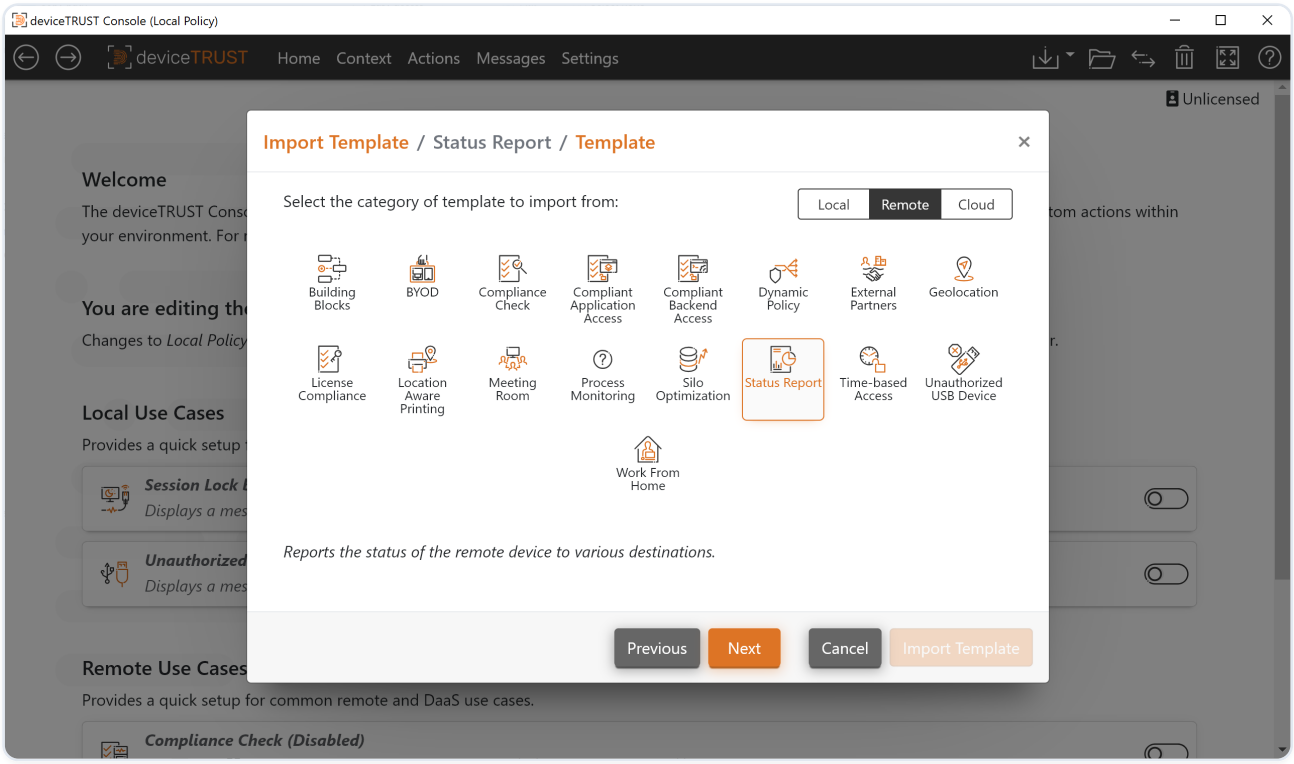


TABLE OF CONTENTS

- Application Log - Reports the status of the remote device to the Windows application log.
- ELK Stack - Reports the status of the remote device to ELK Stack.
- Email - Send the status of the remote device by email.
- Log File - Records the status of the remote device to a log file.
- Splunk - Records the status of the remote device to Splunk.

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.

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: Contexts

© 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 - 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: Contexts
- 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.	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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		(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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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: Contexts
- 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
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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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.

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: Contexts

© 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
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 -	Hides applications with FSLogix App Masking within the	Deactivated	You must update the following context condition with data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - FSLogix App Masking	session when accessed outside of working time.		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*
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.

Time-based Access Templates

Controls access to the session or applications when accessed outside of working hours.

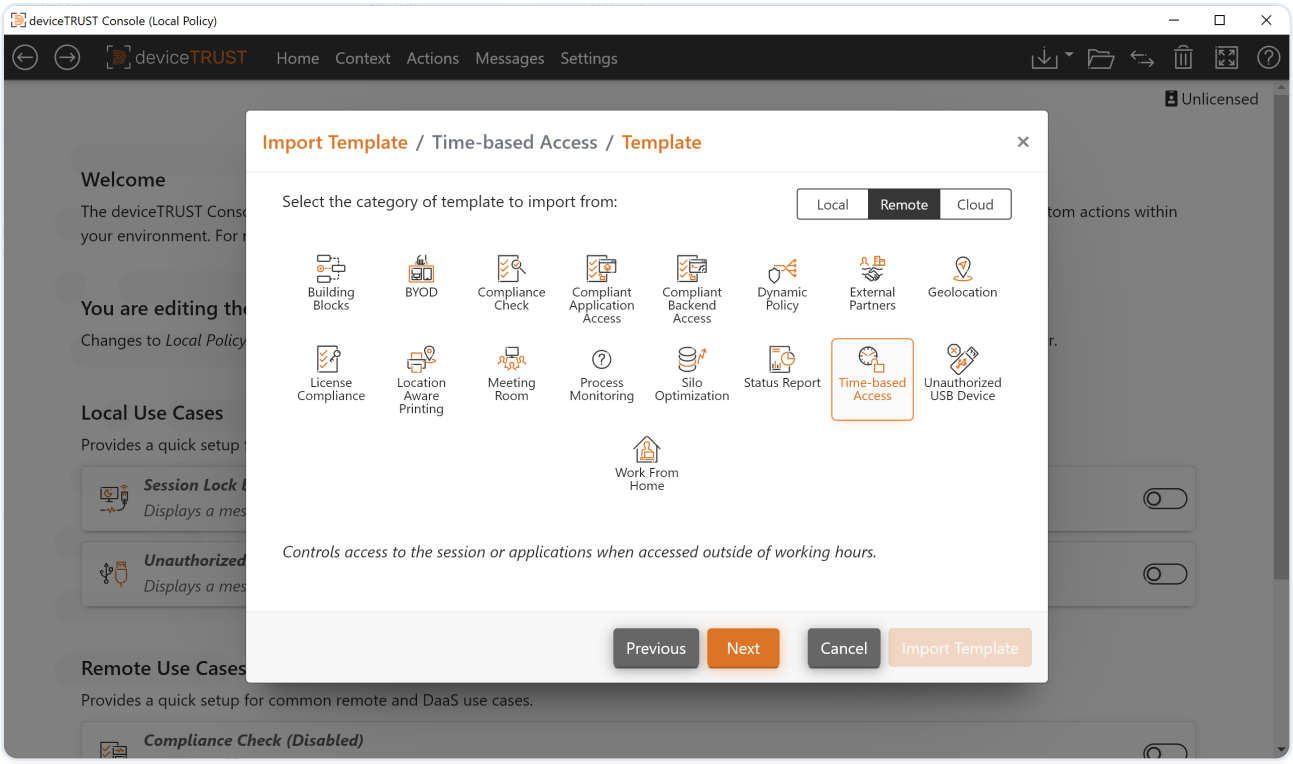


TABLE OF CONTENTS

- Conditional Access - Displays a message or denies access to the session when accessed outside of working hours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Conditional Application Access - Hides or denies access to applications in the session when accessed outside of working hours.

Unauthorized USB Device Templates

Denies access to the session when an unauthorized USB device is plugged in.

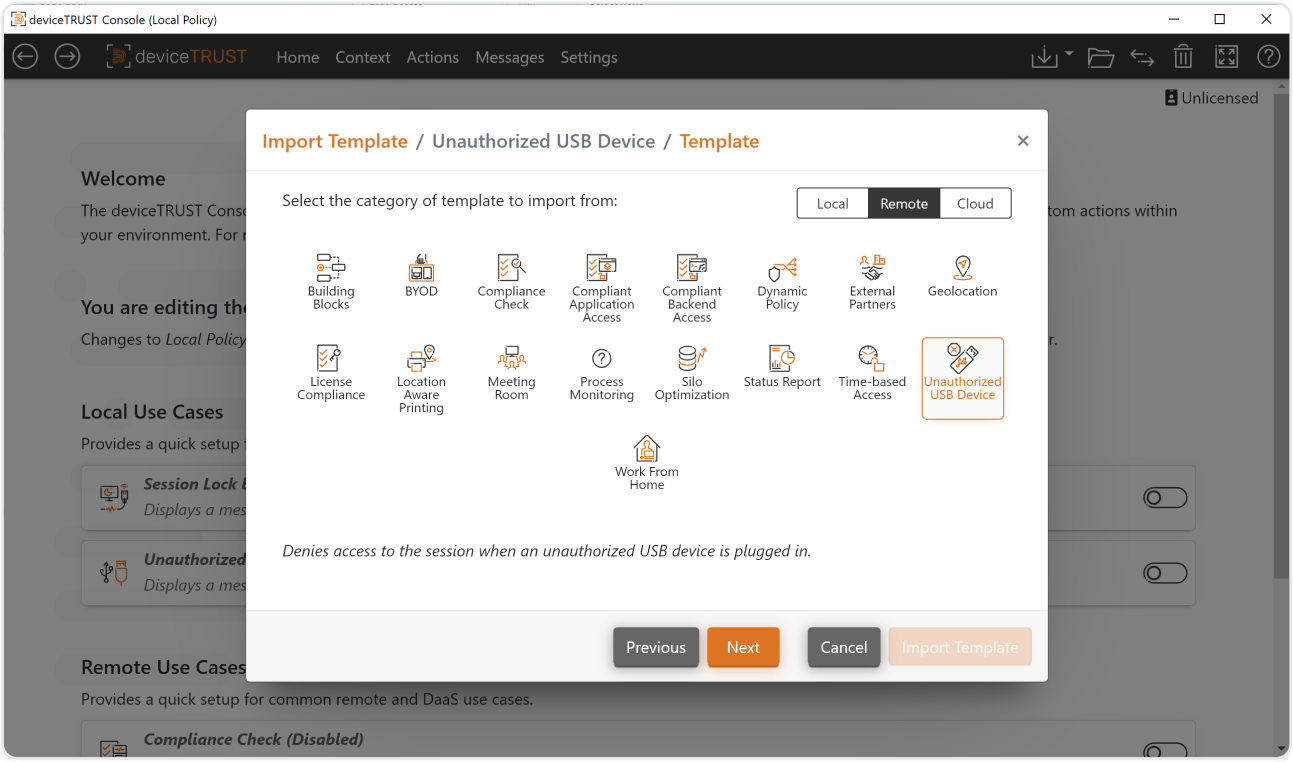


TABLE OF CONTENTS

- Unauthorized USB Device - Displays a message or denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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: Contexts
- 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
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: 0x0781,0x5567,4C53000011*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		0526106001 SanDisk Cruzer Blade USB Device.

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

© 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.

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: Contexts
- 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
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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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_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
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 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 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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

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.

Work From Home Templates

Validates and controls access based on the remote device for home office users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

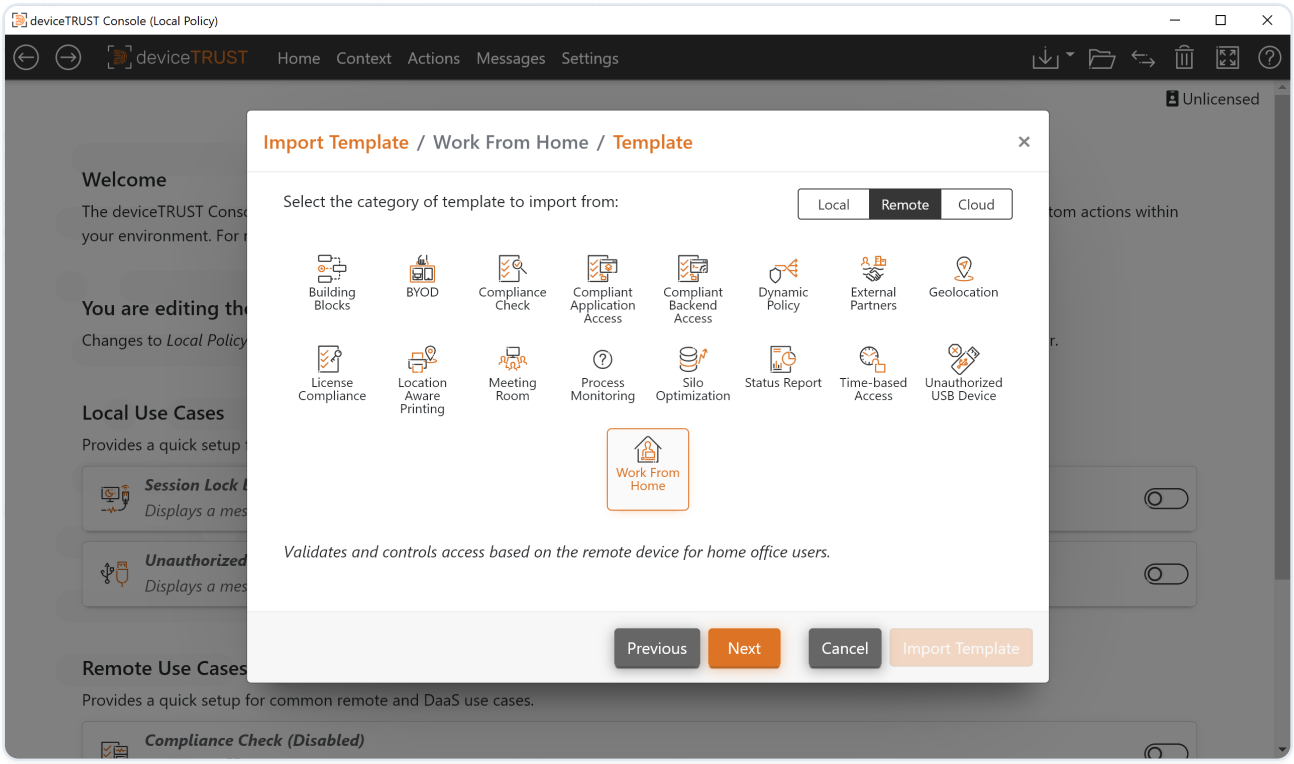


TABLE OF CONTENTS

- Conditional Access - Displays a message or denies access to the session if the remote device is not compliant with work from home policies.

Country Template

This template creates a configuration that checks the country of the local device. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If the local device is not located within an authorized country, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on the country of the local device.
- Sets an Extension Attribute in Microsoft Entra ID based on the country of the local device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the local device is located.	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 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
Country - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on the country of the local 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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Alpha-2 code. Example: US
			`COUNTRY Any Of AUTHORIZED_COUNTRY_1,...` *Replace AUTHORIZED_COUNTRY_X with the same list of authorized countries as above.*
Country - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Microsoft Entra ID based on the country of the local 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*
			`COUNTRY Any Of AUTHORIZED_COUNTRY_1,...` *Replace AUTHORIZED_COUNTRY_X with the same list of authorized countries as above.*
			`Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			may be changed to a value suitable for your organisation.

NOTE:

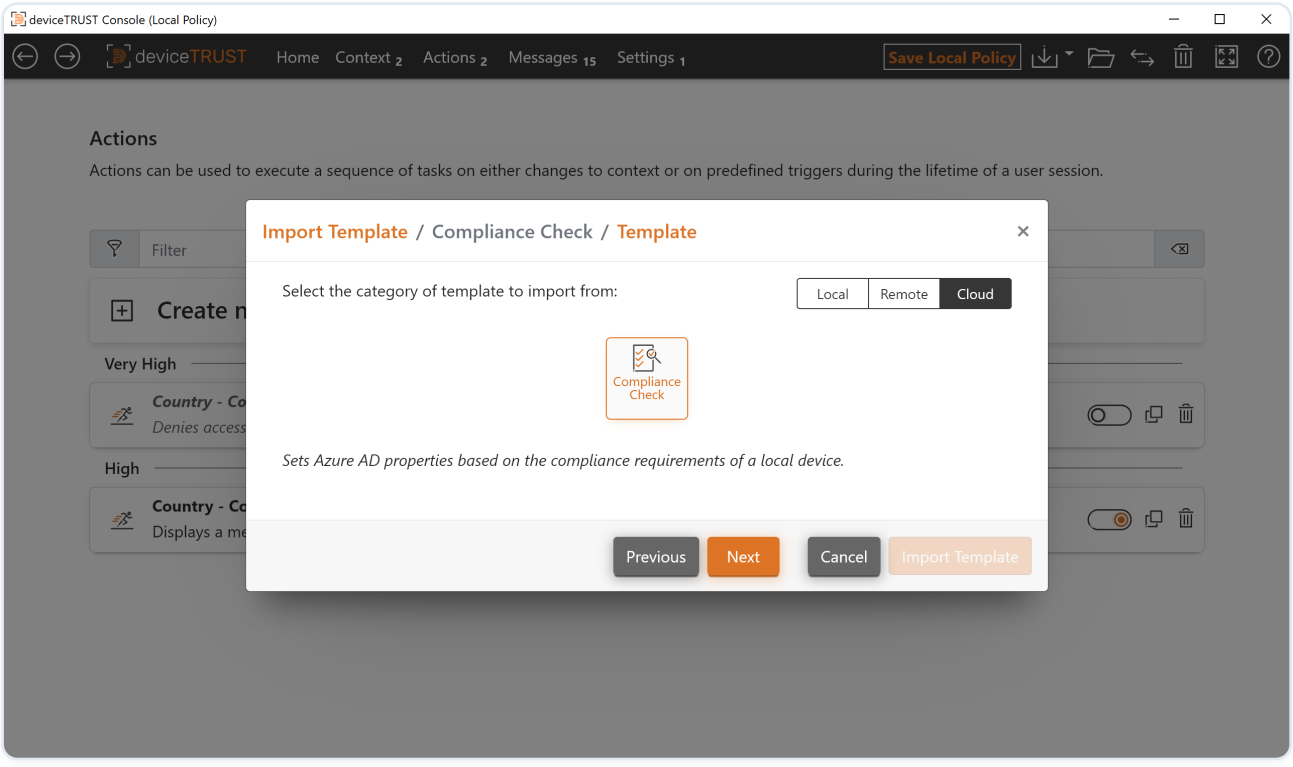
- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.
- Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Compliance Check

Sets Microsoft Entra ID properties based on the compliance requirements of a local device.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Operating System Update State Template

This template creates a configuration that checks if the operating system of the local device has not performed a recent update search or has outstanding critical updates. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If the operating system of the local device has not performed a recent update search or has outstanding critical updates, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on the operating system update state of the local device.
- Sets an Extension Attribute in Microsoft Entra ID based on the operating system update state of the local device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts

© 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Update	Defines if a recent update search has been performed and that all updates have been installed on the local 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 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
Operating System Update - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on the operating system update state of the local device.	Deactivated	None
Operating System Update - Conditional Access -	Sets an Extension Attribute in Microsoft Entra ID based on	Deactivated	You may want to update the following context condition

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - Extension Attribute	the operating system update state of the local device.		with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Remote Controlled Template

This template creates a configuration that checks if the local device is remote controlled. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If the remote device is remote controlled, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on if the local device is remote controlled.
- Sets an Extension Attribute in Microsoft Entra ID based on if the local device is remote controlled.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remote Controlled	Defines if the local device is remote controlled.	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 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
Remote Controlled - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on if the local device is remote controlled.	Deactivated	None
Remote Controlled - Conditional Access -	Sets an Extension Attribute in Microsoft	Deactivated	You may want to update the following

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - Extension Attribute	Entra ID based on if the local device is remote controlled.		context condition with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

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 local device. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If the security state of the local device is unprotected, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on the security state of the local device.
- Sets an Extension Attribute in Microsoft Entra ID based on the security state of the local device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Security State	Defines the security status of the local 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 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
Security State - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on the security state of the local device.	Deactivated	None
Security State - Conditional Access -	Sets an Extension Attribute in Microsoft Entra ID based on	Deactivated	You may want to update the following context condition

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - Extension Attribute	the security state of the local device.		with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Threat Detection Template

This template creates a configuration that checks if a threat is detected or the local device has not been scanned recently. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If a threat is detected or the local device has not been scanned recently, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on if a threat is detected or the local device has not been scanned recently.
- Sets an Extension Attribute in Microsoft Entra ID based on if a threat is detected or the local device has not been scanned recently.

© 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 SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Threat Detection	Defines if the local device has been recently scanned and has no current threats.	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 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
Threat Detection - Conditional Access -	Sets the Compliance State in Microsoft Entra ID based on if	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Enforcement - Compliance State	a threat is detected or the local device has not been scanned recently.		
Threat Detection - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Microsoft Entra ID based on if a threat is detected or the local device has not been scanned recently.	Deactivated	You may want to update the following context condition with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

User Privileges Template

This template creates a configuration that checks the privileges of the user logged into the local device. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

If the privileges of the user logged into the local device are privileged without protection, you can choose between two actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sets the Compliance State in Microsoft Entra ID based on the privileges of the user logged into the local device.
- Sets an Extension Attribute in Microsoft Entra ID based on the privileges of the user logged into the local device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
User Privileges	Defines the privileges of the user logged into the local 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
User Privilege - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on the privileges of the user logged into the local device.	Deactivated	None
User Privilege - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Microsoft Entra ID based on the privileges of the user logged into the local device.	Deactivated	You may want to update the following context condition with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

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 local device is connected to an insecure Wi-Fi network. It can be found in the `COMPLIANCE CHECK` category when filtered for `SAAS` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the local device is connected to an insecure Wi-Fi network, you can choose between two actions:

- Sets the Compliance State in Microsoft Entra ID based on the Wi-Fi Security Mode of the local device.
- Sets an Extension Attribute in Microsoft Entra ID based on the Wi-Fi Security Mode of the local device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your SaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your SaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Contexts
- 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 guide.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the local 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
Wi-Fi Security - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Microsoft Entra ID based on the Wi-Fi Security Mode of the local device.	Deactivated	None
Wi-Fi Security - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Microsoft Entra ID based on the Wi-Fi Security Mode of the local device.	Deactivated	You may want to update the following context condition with data suitable for your environment `Microsoft Entra ID Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable for your organisation.*

NOTE:

- If both actions have been disabled, the contexts will still be created.
- If both actions have been activated, then both the Compliance State and the Extension Attribute will be updated.

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.