deviceTRUST 21.1

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

Contents

Welcome 36

- Quick setup 36
- More information 36

Architecture 37

- TABLE OF CONTENTS 37
- Local Scenario 37
  - deviceTRUST® Agent 37
  - Architecture - Microsoft Windows local devices 37
- Remote Scenario 38
  - deviceTRUST Agent 38
  - deviceTRUST Client Extension 39
  - Architecture - Windows, macOS, Ubuntu, eLux® RP or IGEL OS device 39
- Operating System Compatibility 39
  - Apple iOS and iPadOS 40
  - Apple macOS 40
  - IGEL OS 40
  - Microsoft Windows 41
  - Ubuntu Desktop 42
  - Unicon™ eLux 42
- Platform Compatibility 42
  - Amazon Web Services 42
  - Citrix Systems 43
  - Microsoft 43
  - Parallels 44
  - VMware 44

Getting Started 46

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

Scenario: Remote 46
Scenario: Local 46
Getting Started for Local 46
Step 1: Download the deviceTRUST setup binaries 47
Step 2: Install the deviceTRUST Agent 47
Step 3: Install the deviceTRUST Console 47
Step 4: Enter your deviceTRUST License 48
Step 5: Enable the Unauthorized USB Drive use case 50
Step 6: Test the Unauthorized USB Device use case 53
Next steps 54
Troubleshooting 54
Getting Started for Remote 54
Step 1: Download the deviceTRUST setup binaries 55
Step 2: Install the deviceTRUST Agent 55
Step 3: Install the deviceTRUST Console 55
Step 4: Enter your deviceTRUST License 56
Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device 58
Step 6: Enable the Compliance Check use case 58
Step 7: Check that access is denied when the deviceTRUST Client Extension is not installed 63
Step 8: Test the Compliance Check use case from a Microsoft Windows device 64
Next steps 65
Troubleshooting 66
Download deviceTRUST® Client Extensions 67
Download deviceTRUST 21.1 67
Download previous releases 67
Software components 67
Installation 69
TABLE OF CONTENTS 69

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

Installing the deviceTRUST® Agent 69
Citrix Virtual Channel Security 72
Unattended Installation 72
Installing the deviceTRUST® Console 73
Unattended Installation 75
Installing the deviceTRUST® Client Extension 76
TABLE OF CONTENTS 76
Client Extension installation on Microsoft Windows devices 76
Client Extension Installation Command Line Options 78
Unattended Installation 79
Active Setup Components 79
Client installation on Apple macOS devices 80
Client installation on Ubuntu devices 85
Client installation on IGEL OS devices 88
Enable deviceTRUST for Citrix Independent Computing Architecture (ICA®) 88
Enable deviceTRUST for Microsoft Remote Desktop Protocol (RDP) 89
Client installation on Unicon™ eLux devices 90
Import the deviceTRUST® certificate chain 90
Install the package 90
Deploy the ripe.stat root certificate 92
Templates 94
Local Templates 95
TABLE OF CONTENTS 96
Remote Templates 96
TABLE OF CONTENTS 97
Cloud Templates 98
TABLE OF CONTENTS 98
Reporting 99

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

TABLE OF CONTENTS 99
Splunk Dashboards 99
Step 1: Creating the Splunk Index 100
Step 1.1: Manually creating the Splunk Index 101
Step 1.2: Creating the Splunk Index by installing the app 103
Step 2: Creating the Splunk Data Inputs 103
Step 3: Importing the Splunk app 107
Step 3.1: Downloading the Splunk app 107
Step 3.2: Installing the Splunk app 109
Step 4: Configuring deviceTRUST 112
Step 4.1: The Device-Based Licensing Report 112
Step 4.2: The Status Report 117
ELK Stack Dashboards 121
Step 1: Components 123
Step 1.1: Components - GitHub 123
Step 1.2: Components - Templates 124
Step 2: The Device-Based Licensing Report 125
Step 2.1: Add Index Template to ELK Stack 125
Step 2.2: Import Saved Objects to ELK Stack 130
Step 2.3: Configuring deviceTRUST 132
Step 3: The Status Report 139
Step 3.1: Add Index Template to ELK Stack 139
Step 3.2: Import Saved Objects to ELK Stack 143
Step 3.3: Configuring deviceTRUST 146
Step 3.4: Edit index settings 150
Reference 154
TABLE OF CONTENTS 154
Properties 154

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

Agent Reference 156
TABLE OF CONTENTS 156
Console Reference 156
TABLE OF CONTENTS 156
Troubleshooting 157
Scenario: Remote 157
Scenario: Local 157
Open a support ticket with us 158
Releases 159
TABLE OF CONTENTS 159
TABLE OF CONTENTS 159
Ubuntu Client Extension 21.1.300 159
Support for VMware Horizon View 159
Custom Properties for Linux devices 159
Minor enhancements 160
Bug Fixes 160
Compatibility 160
macOS Client Extension 21.1.300 160
Native support for Apple silicon 160
Bug Fixes 160
Compatibility 160
deviceTRUST 21.1 SP2 (version 21.1.310) 161
User interface refinement 161
New Cloud Templates 162
Other changes 163
Bug fixes in 21.1.300 164
Bug fixes in 21.1.310 164
Minor enhancements to 21.1.310 164

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

Compatibility 164
IGEL Client Extension 21.1.310 165
Custom Properties for IGEL OS devices 165
Native IGEL OS integration 165
Bug fixes 165
Known issues 165
Compatibility 165
index 166
Product Events 174
Application Channel 174
deviceTRUST/Admin Channel 175
deviceTRUST/Usage Channel 207
Actions 208
TABLE OF CONTENTS 208
Audit Event Task 208
Azure AD Task 208
Citrix Policy Task 209
Custom Process Task 210
Deny Access Task 211
FSLogix App Masking Task 212
Task Reference 213
TABLE OF CONTENTS 213
Logon Abort Task 214
Map Drive Task 215
Map Printer Task 216
Microsoft AppLocker Task 217
Popup Message Task 218
Screen Saver Task 220

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

Send Mail Task 220
Shortcut Task 221
Terminate App Task 222
User Session Task 223
Web Request Task 224
Windows Firewall Task 225
Windows Policy Task 226
Windows Registry Task 227
Advanced Settings 228
Auditing Settings 229
Azure AD Settings 230
Custom Properties Settings 230
Local Agent Custom Properties 230
Remote Windows Device Custom Properties 232
Creating Custom Properties 233
File-Based Policy Settings 233
Settings 234
TABLE OF CONTENTS 234
Licensing Settings 235
Mail Server Settings 235
Map Drive Settings 236
Microsoft AppLocker Settings 237
Printer Settings 238
Property Settings 239
Property Filters 240
Property Queries 241
Access Point Queries 243
Certificate Queries 243

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

Display Queries 244
Firewall Queries 244
Logical Disk Queries 245
Mapped Drive Queries 245
Network Queries 246
Printer Queries 246
Security Product Queries 247
Text Constraints 247
Enumeration (Enum) Constraints 248
Number Constraints 248
Date Constraints 249
Boolean Constraints 249
IpAddress Constraints 250
Version Constraints 250
Security Settings 250
System Messages Settings 251
Access Point Properties 252
Browser Properties 259
Cellular Properties 264
Certificate Properties 276
ChromeOS Properties 298
Custom Properties 301
deviceTRUST Properties 303
Display Properties 310
Domain Properties 321
eLux Properties 325
Hardware Properties 336
IGEL Properties 348

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

Input Properties 359
iOS Properties 363
Location Properties 365
Logical Disk Properties 377
macOS Properties 396
macOS Firewall Properties 400
macOS Update Properties 409
Mapped Drive Properties 422
Multihop Properties 429
Name Properties 430
Network Properties 434
OS Properties 460
Password Policy Properties 467
Performance Properties 473
Power Properties 478
Printer Properties 481
Region Properties 496
Remote Control Properties 501
Remoting Client Properties 512
Screen Saver Properties 517
Security Product Properties 522
Session Properties 528
Smartcard Reader Properties 536
User Properties 539
WHOIS Properties 554
Windows Properties 559
Windows Defender Properties 568
Windows Firewall Properties 594

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

Windows Registry Properties 609
Windows Update Properties 613
Country Template 635
Step 1: Prerequisites 635
Step 2: Contexts 635
Step 3: Actions 636
Troubleshooting 638
Compliance Check 638
TABLE OF CONTENTS 639
Operating System Update State Template 639
Step 1: Prerequisites 640
Step 2: Contexts 640
Step 3: Actions 641
Troubleshooting 642
Remote Controlled Template 642
Step 1: Prerequisites 642
Step 2: Contexts 642
Step 3: Actions 643
Troubleshooting 644
Security State Template 644
Step 1: Prerequisites 644
Step 2: Contexts 644
Step 3: Actions 645
Troubleshooting 646
Threat Detection Template 646
Step 1: Prerequisites 647
Step 2: Contexts 647
Step 3: Actions 647

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

Troubleshooting 648
User Privileges Template 649
Step 1: Prerequisites 649
Step 2: Contexts 649
Step 3: Actions 650
Troubleshooting 651
Wi-Fi Security Mode Template 651
Step 1: Prerequisites 652
Step 2: Contexts 652
Step 3: Actions 652
Troubleshooting 653
Access Mode Template 653
Step 1: Prerequisites 654
Step 2: Context 654
Troubleshooting 654
Conditional Application Access Template 654
Step 1: Prerequisites 655
Step 2: Actions 655
Troubleshooting 657
Country Template 657
Step 1: Prerequisites 657
Step 2: Context 657
Troubleshooting 657
Country Provider Template 658
Step 1: Prerequisites 658
Step 2: Context 658
Troubleshooting 658
Device Location IP Address Template 659

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

Step 1: Prerequisites 659
Step 2: Context 659
Troubleshooting 660
Device Location NetBIOS Name Template 660
Step 1: Prerequisites 660
Step 2: Context 660
Troubleshooting 661
Device Location Wi-Fi Access Point Template 661
Step 1: Prerequisites 662
Step 2: Context 662
Troubleshooting 662
Building Blocks Templates 662
TABLE OF CONTENTS 663
Override Template 664
Step 1: Prerequisites 664
Step 2: Context 664
Troubleshooting 665
Policy Mode from AD Group Template 665
Step 1: Prerequisites 665
Step 2: Context 665
Troubleshooting 666
Policy Mode from Date Template 666
Step 1: Prerequisites 666
Step 2: Context 666
Troubleshooting 667
Proximity Template 667
Step 1: Prerequisites 667
Step 2: Context 667

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

Troubleshooting 668
Session Idle Template 668
Step 1: Prerequisites 668
Step 2: Context 668
Troubleshooting 669
Unauthorized USB Device Template 669
Step 1: Prerequisites 670
Step 2: Context 670
Troubleshooting 670
Unauthorized USB Storage Device Template 671
Step 1: Prerequisites 671
Step 2: Context 671
Troubleshooting 672
VPN Connected Template 672
Step 1: Prerequisites 672
Step 2: Context 672
Troubleshooting 673
Wi-Fi Security Mode Template 673
Step 1: Prerequisites 673
Step 2: Context 673
Troubleshooting 674
Working Time Template 674
Step 1: Prerequisites 674
Step 2: Context 674
Troubleshooting 675
Country Template 675
Step 1: Prerequisites 675
Step 2: Contexts 675

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

Step 3: Actions 676
Troubleshooting 679
Compliant Application Access Templates 679
TABLE OF CONTENTS 680
Proximity Template 680
Step 1: Prerequisites 680
Step 2: Contexts 681
Step 3: Actions 681
Troubleshooting 683
Wi-Fi Security Mode Template 683
Step 1: Prerequisites 683
Step 2: Contexts 683
Step 3: Actions 684
Troubleshooting 686
Working Time Template 686
Step 1: Prerequisites 687
Step 2: Contexts 687
Step 3: Actions 687
Troubleshooting 689
Dynamic Policy Templates 690
TABLE OF CONTENTS 690
Session Lock based on Network Type Template 690
Step 1: Prerequisites 691
Step 2: Contexts 691
Step 3: Actions 691
Troubleshooting 692
Session Lock based on VPN Connection Template 692
Step 1: Prerequisites 692

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

Step 2: Contexts 692
Step 3: Actions 693
Troubleshooting 693
Session Lock based on Wi-Fi Security Mode Template 693
Step 1: Prerequisites 693
Step 2: Contexts 694
Step 3: Actions 694
Troubleshooting 694
Conditional Application Access for Country Template 694
Step 1: Prerequisites 695
Step 2: Contexts 695
Step 3: Actions 696
Troubleshooting 698
Conditional Application Access for Proximity Template 699
Step 1: Prerequisites 699
Step 2: Contexts 699
Step 3: Actions 700
Troubleshooting 702
Geolocation Templates 702
TABLE OF CONTENTS 703
Location Aware Printing Templates 703
TABLE OF CONTENTS 704
IP Address Template 704
Step 1: Prerequisites 705
Step 2: Contexts 705
Step 3: Actions 706
Troubleshooting 707
NetBIOS Name Template 707

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

Step 1: Prerequisites 707
Step 2: Contexts 707
Step 3: Actions 708
Troubleshooting 709
Wi-Fi Access Point Template 709
Step 1: Prerequisites 710
Step 2: Contexts 710
Step 3: Actions 711
Troubleshooting 712
Custom Values Template 712
Step 1: Prerequisites 712
Step 2: Contexts 712
Step 3: Actions 713
Troubleshooting 713
Meeting Room Templates 713
TABLE OF CONTENTS 714
IP Address Template 714
Step 1: Prerequisites 715
Step 2: Contexts 715
Step 3: Actions 716
Troubleshooting 716
NetBIOS Name Template 716
Step 1: Prerequisites 717
Step 2: Contexts 717
Step 3: Actions 717
Troubleshooting 718
Time-based Access Template 718
Step 1: Prerequisites 719

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

Step 2: Contexts 719

Step 3: Actions 719

Troubleshooting 722

Time-based Access Templates 722

TABLE OF CONTENTS 723

Unauthorized USB Drives Templates 723

TABLE OF CONTENTS 724

Unauthorized USB Device Template 724

Step 1: Prerequisites 725

Step 2: Contexts 725

Step 3: Actions 726

Troubleshooting 726

Unauthorized USB Storage Device Template 727

Step 1: Prerequisites 727

Step 2: Contexts 727

Step 3: Actions 728

Troubleshooting 729

Access Mode Template 729

Step 1: Prerequisites 730

Step 2: Context 730

Troubleshooting 731

Citrix HDX™ RealTime Media Engine Template 731

Step 1: Prerequisites 732

Step 2: Context 732

Troubleshooting 732

Citrix Workspace™ App Template 732

Step 1: Prerequisites 733

Step 2: Context 733

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

Troubleshooting 733
Computer Certificate Template 733
Step 1: Prerequisites 734
Step 2: Context 734
Troubleshooting 735
Conditional Application Access Template 735
Step 1: Prerequisites 736
Step 2: Actions 736
Troubleshooting 738
Corporate Device Template 738
Step 1: Prerequisites 738
Step 2: Context 738
Troubleshooting 741
Country Template 742
Step 1: Prerequisites 742
Step 2: Context 742
Troubleshooting 742
Country Provider Template 742
Step 1: Prerequisites 743
Step 2: Context 743
Troubleshooting 743
Country Provider with Fallback Template 743
Step 1: Prerequisites 744
Step 2: Context 744
Troubleshooting 744
Country with Fallback Template 744
Step 1: Prerequisites 745
Step 2: Context 745

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

Troubleshooting 745
Device Location IP Address Template 746
Step 1: Prerequisites 746
Step 2: Context 746
Troubleshooting 747
Device Location NetBIOS Name Template 747
Step 1: Prerequisites 747
Step 2: Context 748
Troubleshooting 748
Device Location Wi-Fi Access Point Template 748
Step 1: Prerequisites 749
Step 2: Context 749
Troubleshooting 749
Device Type BYOD Template 750
Step 1: Prerequisites 750
Step 2: Context 750
Troubleshooting 753
Device Type Contractor Template 753
Step 1: Prerequisites 754
Step 2: Context 754
Troubleshooting 757
Device Type Corporate Template 757
Step 1: Prerequisites 757
Step 2: Context 757
Troubleshooting 760
deviceTRUST® Client Extension Availability Template 760
Step 1: Prerequisites 761
Step 2: Context 761

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

Troubleshooting 761
Building Blocks Templates 761
TABLE OF CONTENTS 762
Operating System Template 763
Step 1: Prerequisites 763
Step 2: Context 763
Troubleshooting 764
Operating System Update Template 764
Step 1: Prerequisites 764
Step 2: Context 764
Troubleshooting 765
Override Template 765
Step 1: Prerequisites 765
Step 2: Context 765
Troubleshooting 766
Policy Mode from AD Group Template 766
Step 1: Prerequisites 766
Step 2: Context 766
Troubleshooting 767
Proximity Template 767
Step 1: Prerequisites 767
Step 2: Context 767
Troubleshooting 768
Remote Controlled Template 768
Step 1: Prerequisites 769
Step 2: Context 769
Troubleshooting 769
Security State Template 769

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

Step 1: Prerequisites 770
Step 2: Context 770
Troubleshooting 772
Session Idle Template 772
Step 1: Prerequisites 772
Step 2: Context 772
Troubleshooting 773
Threat Detection Template 773
Step 1: Prerequisites 774
Step 2: Context 774
Troubleshooting 774
Unauthorized USB Device Template 774
Step 1: Prerequisites 775
Step 2: Context 775
Troubleshooting 775
User Privileges Template 776
Step 1: Prerequisites 776
Step 2: Context 776
Troubleshooting 776
Virtualized Template 777
Step 1: Prerequisites 777
Step 2: Context 777
Troubleshooting 777
VPN Connected Template 778
Step 1: Prerequisites 778
Step 2: Context 778
Troubleshooting 778
Wi-Fi Security Mode Template 779

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

Step 1: Prerequisites 779
Step 2: Context 779
Troubleshooting 779
Working Time Template 780
Step 1: Prerequisites 780
Step 2: Context 780
Troubleshooting 781
Conditional Access Template 781
Step 1: Prerequisites 781
Step 2: Contexts 782
Step 3: Actions 787
Troubleshooting 789
Conditional Application Access Template 789
Step 1: Prerequisites 790
Step 2: Contexts 790
Step 3: Actions 796
Troubleshooting 798
BYOD (Bring Your Own Device) Templates 799
TABLE OF CONTENTS 799
Citrix Clients Template 799
Step 1: Prerequisites 800
Step 2: Contexts 800
Step 3: Actions 801
Troubleshooting 802
Compliance Check Template 802
Step 1: Prerequisites 803
Step 2: Contexts 803
Step 3: Actions 806

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

Troubleshooting 808
Computer Certificate Template 808
Step 1: Prerequisites 809
Step 2: Contexts 809
Step 3: Actions 810
Troubleshooting 811
Corporate Device Template 811
Step 1: Prerequisites 811
Step 2: Contexts 811
Step 3: Actions 814
Troubleshooting 815
Country Template 815
Step 1: Prerequisites 816
Step 2: Contexts 816
Step 3: Actions 816
Troubleshooting 818
Country with Fallback Template 818
Step 1: Prerequisites 819
Step 2: Contexts 819
Step 3: Actions 820
Troubleshooting 821
deviceTRUST® Client Extension Availability Template 821
Step 1: Prerequisites 822
Step 2: Contexts 822
Step 3: Actions 823
Troubleshooting 823
Compliance Check 823
Operating System Template 824

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

Step 1: Prerequisites 825
Step 2: Contexts 825
Step 3: Actions 825
Troubleshooting 826
Operating System Update Template 826
Step 1: Prerequisites 827
Step 2: Contexts 827
Step 3: Actions 827
Troubleshooting 828
Remote Controlled Template 828
Step 1: Prerequisites 829
Step 2: Contexts 829
Step 3: Actions 829
Troubleshooting 830
Security State Template 830
Step 1: Prerequisites 830
Step 2: Contexts 831
Step 3: Actions 833
Troubleshooting 833
Threat Detection Template 833
Step 1: Prerequisites 834
Step 2: Contexts 834
Step 3: Actions 835
Troubleshooting 835
User Privileges Template 835
Step 1: Prerequisites 836
Step 2: Contexts 836
Step 3: Actions 836

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

Troubleshooting 837
Virtualized Template 837
Step 1: Prerequisites 838
Step 2: Contexts 838
Step 3: Actions 838
Troubleshooting 839
Wi-Fi Security Mode Template 839
Step 1: Prerequisites 840
Step 2: Contexts 840
Step 3: Actions 840
Troubleshooting 841
Access Mode Template 841
Step 1: Prerequisites 842
Step 2: Contexts 842
Step 3: Actions 843
Troubleshooting 845
Corporate Device Template 845
Step 1: Prerequisites 846
Step 2: Contexts 846
Step 3: Actions 849
Troubleshooting 851
Country Template 851
Step 1: Prerequisites 852
Step 2: Contexts 852
Step 3: Actions 853
Troubleshooting 855
Compliant Application Access Templates 856
Proximity Template 856

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

Step 1: Prerequisites 857
Step 2: Contexts 857
Step 3: Actions 858
Troubleshooting 860
Wi-Fi Security Mode Template 860
Step 1: Prerequisites 860
Step 2: Contexts 860
Step 3: Actions 861
Troubleshooting 863
Working Time Template 863
Step 1: Prerequisites 864
Step 2: Contexts 864
Step 3: Actions 864
Troubleshooting 866
Conditional Access Template 867
Step 1: Prerequisites 867
Step 2: Contexts 867
Step 3: Actions 873
Troubleshooting 875
Compliant Backend Access Templates 875
Citrix Policy Access Mode Template 875
Step 1: Prerequisites 876
Step 2: Contexts 876
Step 3: Actions 876
Troubleshooting 877
Citrix Policy Corporate Device Template 877
Step 1: Prerequisites 878
Step 2: Contexts 878

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

Step 3: Actions 881
Troubleshooting 882
Citrix Policy Wi-Fi Security Mode Template 882
Step 1: Prerequisites 882
Step 2: Contexts 883
Step 3: Actions 883
Troubleshooting 884
Dynamic Policy Templates 884
Secure Screen Saver Template 884
Step 1: Prerequisites 885
Step 2: Contexts 885
Step 3: Actions 885
Troubleshooting 886
Conditional Access Template 886
Step 1: Prerequisites 887
Step 2: Contexts 887
Step 3: Actions 893
Troubleshooting 894
Conditional Application Access Template 895
Step 1: Prerequisites 895
Step 2: Contexts 895
Step 3: Actions 901
Troubleshooting 904
External Partners Templates 904
Conditional Access for Country Template 905
Step 1: Prerequisites 906
Step 2: Contexts 906
Step 3: Actions 906

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

Troubleshooting 908
Conditional Access for Country with Fallback Template 908
Step 1: Prerequisites 909
Step 2: Contexts 909
Step 3: Actions 909
Troubleshooting 911
Conditional Application Access for Country Template 911
Step 1: Prerequisites 912
Step 2: Contexts 912
Step 3: Actions 912
Troubleshooting 915
Conditional Application Access for Proximity Template 915
Step 1: Prerequisites 916
Step 2: Contexts 916
Step 3: Actions 917
Troubleshooting 919
Geolocation Templates 919
Adobe Reader DC Template 920
Step 1: Prerequisites 921
Step 2: Contexts 921
Step 3: Actions 923
Troubleshooting 927
License Compliance Templates 928
Microsoft Office Template 928
Step 1: Prerequisites 929
Step 2: Contexts 929
Step 3: Actions 931
Troubleshooting 936

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

Microsoft Project Template 936
Step 1: Prerequisites 936
Step 2: Contexts 936
Step 3: Actions 939
Troubleshooting 943
Microsoft Visio Template 943
Step 1: Prerequisites 944
Step 2: Contexts 944
Step 3: Actions 947
Troubleshooting 951
Nuance PDF Template 951
Step 1: Prerequisites 952
Step 2: Contexts 952
Step 3: Actions 954
Troubleshooting 958
Location Aware Printing Templates 958
IP Address Template 959
Step 1: Prerequisites 959
Step 2: Contexts 960
Step 3: Actions 960
Troubleshooting 961
NetBIOS Name Template 962
Step 1: Prerequisites 962
Step 2: Contexts 962
Step 3: Actions 963
Troubleshooting 964
Wi-Fi Access Point Template 964
Step 1: Prerequisites 964

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

Step 2: Contexts 965
Step 3: Actions 965
Troubleshooting 966
Custom Values Template 967
Step 1: Prerequisites 967
Step 2: Contexts 967
Step 3: Actions 968
Troubleshooting 968
Meeting Room Templates 968
IP Address Template 969
Step 1: Prerequisites 969
Step 2: Contexts 970
Step 3: Actions 970
Troubleshooting 971
NetBIOS Name Template 971
Step 1: Prerequisites 971
Step 2: Contexts 972
Step 3: Actions 972
Troubleshooting 973
Process Monitoring Templates 973
Microsoft Teams Template 973
Step 1: Prerequisites 974
Step 2: Contexts 974
Step 3: Actions 974
Troubleshooting 976
Access Mode Template 976
Step 1: Prerequisites 976
Step 2: Contexts 976

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

Step 3: Actions 978
Troubleshooting 980
Adobe Acrobat DC Template 980
Step 1: Prerequisites 981
Step 2: Contexts 981
Step 3: Actions 983
Troubleshooting 988
Corporate Device Template 988
Step 1: Prerequisites 988
Step 2: Contexts 988
Step 3: Actions 992
Troubleshooting 994
Country Template 994
Step 1: Prerequisites 994
Step 2: Contexts 994
Step 3: Actions 995
Troubleshooting 998
Silo Optimization Templates 998
Microsoft Office Template 999
Step 1: Prerequisites 999
Step 2: Contexts 999
Step 3: Actions 1002
Troubleshooting 1006
Microsoft Project Template 1006
Step 1: Prerequisites 1007
Step 2: Contexts 1007
Step 3: Actions 1010
Troubleshooting 1014

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

Microsoft Visio Template 1014
Step 1: Prerequisites 1015
Step 2: Contexts 1015
Step 3: Actions 1017
Troubleshooting 1021
Nuance PDF Template 1022
Step 1: Prerequisites 1022
Step 2: Contexts 1022
Step 3: Actions 1025
Troubleshooting 1029
Proximity Template 1029
Step 1: Prerequisites 1030
Step 2: Contexts 1030
Step 3: Actions 1031
Troubleshooting 1033
Wi-Fi Security Mode Template 1033
Step 1: Prerequisites 1033
Step 2: Contexts 1033
Step 3: Actions 1034
Troubleshooting 1036
Working Time Template 1036
Step 1: Prerequisites 1037
Step 2: Contexts 1037
Step 3: Actions 1037
Troubleshooting 1039
Application Log Template 1040
Step 1: Prerequisites 1040
Step 2: Contexts 1040

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

Step 3: Actions 1045
Troubleshooting 1045
ELK Stack Template 1045
Step 1: Prerequisites 1046
Step 2: Contexts 1046
Step 3: Actions 1051
Troubleshooting 1052
Email Template 1052
Step 1: Prerequisites 1052
Step 2: Contexts 1052
Step 3: Actions 1057
Troubleshooting 1057
Graylog Template 1057
Step 1: Prerequisites 1058
Step 2: Contexts 1058
Step 3: Actions 1063
Troubleshooting 1064
Status Report Templates 1064
Log File Template 1064
Step 1: Prerequisites 1065
Step 2: Contexts 1065
Step 3: Actions 1069
Troubleshooting 1070
Splunk Template 1070
Step 1: Prerequisites 1070
Step 2: Contexts 1070
Step 3: Actions 1075
Troubleshooting 1076

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

Conditional Access Template 1076
Step 1: Prerequisites 1077
Step 2: Contexts 1077
Step 3: Actions 1078
Troubleshooting 1078
Conditional Application Access Template 1078
Step 1: Prerequisites 1079
Step 2: Contexts 1079
Step 3: Actions 1080
Troubleshooting 1082
Time-based Access Templates 1082
Unauthorized USB Device Templates 1083
Unauthorized USB Device Template 1083
Step 1: Prerequisites 1084
Step 2: Contexts 1084
Step 3: Actions 1085
Troubleshooting 1086
Unauthorized USB Storage Device Template 1086
Step 1: Prerequisites 1086
Step 2: Contexts 1086
Step 3: Actions 1087
Troubleshooting 1088
Conditional Access Template 1088
Step 1: Prerequisites 1089
Step 2: Contexts 1089
Step 3: Actions 1093
Troubleshooting 1095
Work From Home Templates 1095

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

Welcome

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

Quick setup

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

More information

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

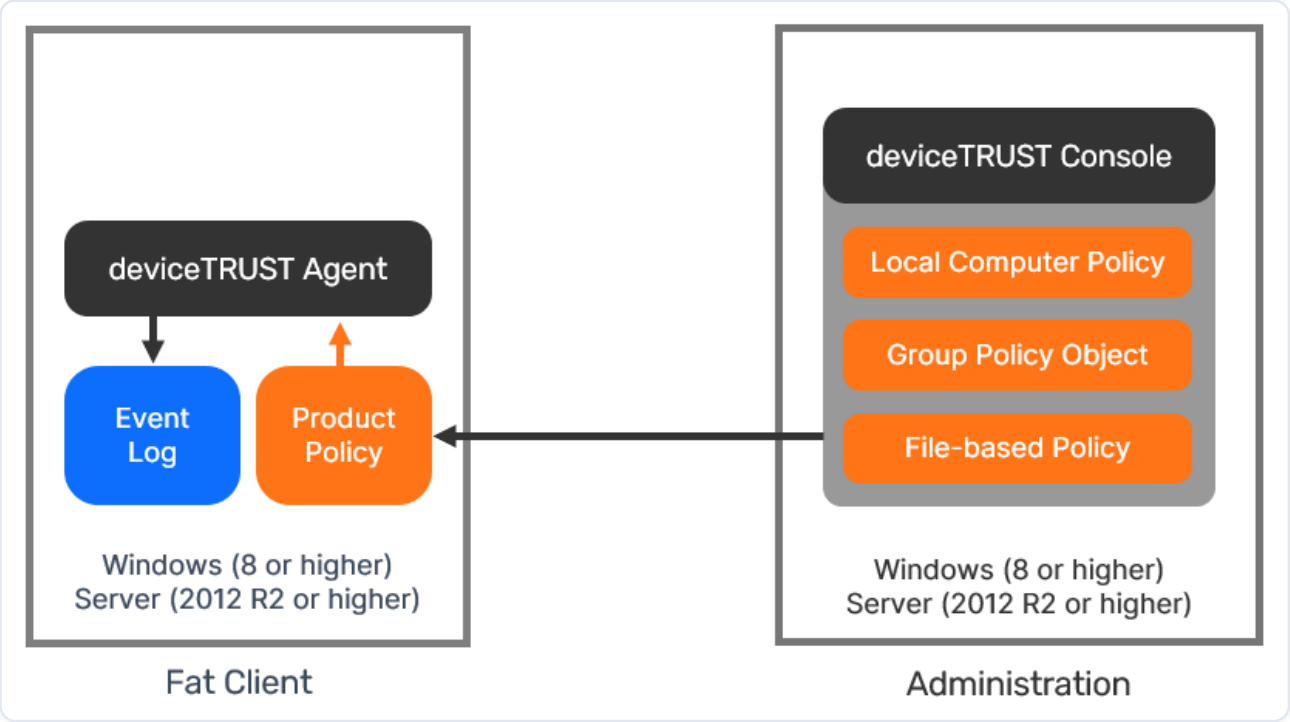
deviceTRUST® Agent

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. The following technologies are supported by deviceTRUST: Amazon WorkSpaces, Citrix Virtual Apps and Desktops™ (CVAD), Microsoft Azure Virtual Desktop (AVD), Microsoft Remote Desktop Session Host (RDSH) or VMware Horizon View.

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

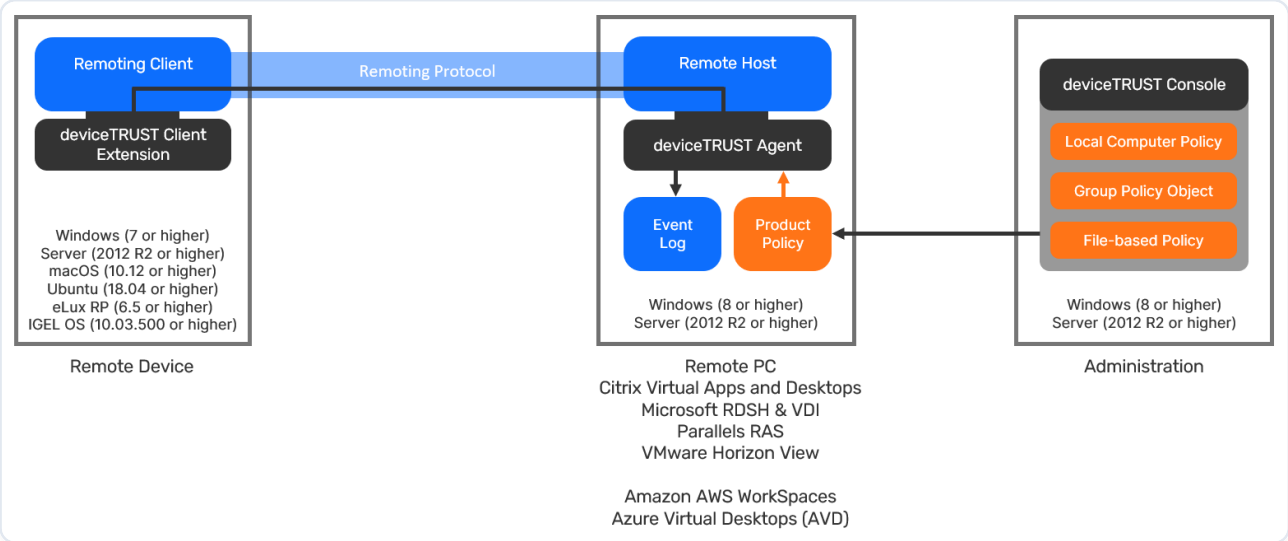
deviceTRUST Client Extension

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

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

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

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



Operating System Compatibility

- Apple iOS and iPadOS
- Apple macOS
- IGEL OS
- Microsoft Windows

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

- Ubuntu Desktop
- Unicon eLux

Apple iOS and iPadOS

Compatible operating systems (deviceTRUST® Client Extension):

- Apple iOS 11.x and later
- Apple iPadOS 11.x and later

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™
- Microsoft Remote Desktop Services
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

Apple macOS

Compatible operating systems (deviceTRUST Client Extension):

- Apple macOS 10.13 and later

Compatible technologies:

- Amazon WorkSpaces (PCoIP)
- Citrix Virtual Apps™ and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services (via FreeRDP 2)
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

IGEL OS

Compatible technologies (deviceTRUST Client Extension):

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

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

NOTE

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

Microsoft Windows

Compatible operating systems (deviceTRUST Agent and Console):

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

Compatible operating systems (deviceTRUST Client Extension):

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

Compatible technologies:

- Amazon WorkSpaces (PCoIP)
- Azure Virtual Desktop
- Azure Active Directory
- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services
- Parallels Remote Application Server
- VMware Horizon View (Blast)

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

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

Ubuntu Desktop

Compatible operating systems (deviceTRUST Client Extension):

- Ubuntu Desktop 18.04 LTS and later

Compatible technologies:

- Amazon WorkSpaces (PCoIP)
- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services (via FreeRDP 2)
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

Unicon™ eLux

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops natively integrated in eLux RP 6.5 and later
- Citrix Cloud natively integrated in eLux RP 6.5 and later
- Microsoft Remote Desktop natively integrated in eLux RP 6.5 and later

Platform Compatibility

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

Amazon Web Services

Compatible technologies:

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

- Amazon WorkSpaces (PCoIP)

Compatible operating systems:

- Apple macOS 10.13 and later
- IGEL OS 11.08.200 or later - 1
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS

NOTE

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

Citrix Systems

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

Compatible operating systems:

- Apple iOS 11.x and later
- Apple iPadOS 11.x and later
- Apple macOS 10.13 and later
- IGEL OS 10.03.500 or later
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS and later
- Unicon eLux RP 6.5 and later

Microsoft

Compatible technologies:

- Microsoft Remote Desktop Services

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

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

Compatible operating systems:

- Apple iOS 11.x and later - 1
- Apple iPadOS 11.x and later - 1
- Apple macOS 10.13 and later (via FreeRDP 2)
- IGEL OS 11.08.200 or later - 3(via RDP Session)
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS and later (via FreeRDP 2)

NOTE

- 1 Compatibility with Azure Virtual Desktop is available on Microsoft Windows and IGEL OS only.
- 2 ompatibility with Azure Active Directory provided by deviceTRUST Agent on Microsoft Windows only.
- 4 Compatibility with previous IGEL OS releases is available by contacting deviceTRUST Support.

Parallels

Compatible technologies:

- Parallels Remote Application Server

Compatible operating systems:

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

VMware

Compatible technologies:

- VMware Horizon View (Blast)

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

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

Compatible operating systems:

- Apple iOS 11.x and later
- Apple iPadOS 11.x and later
- Apple macOS 10.13 and later
- IGEL OS 10.08.230 or later - 1
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 and later
- Ubuntu Desktop 18.04 LTS and later

NOTE

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

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

Getting Started

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

Scenario: Remote

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

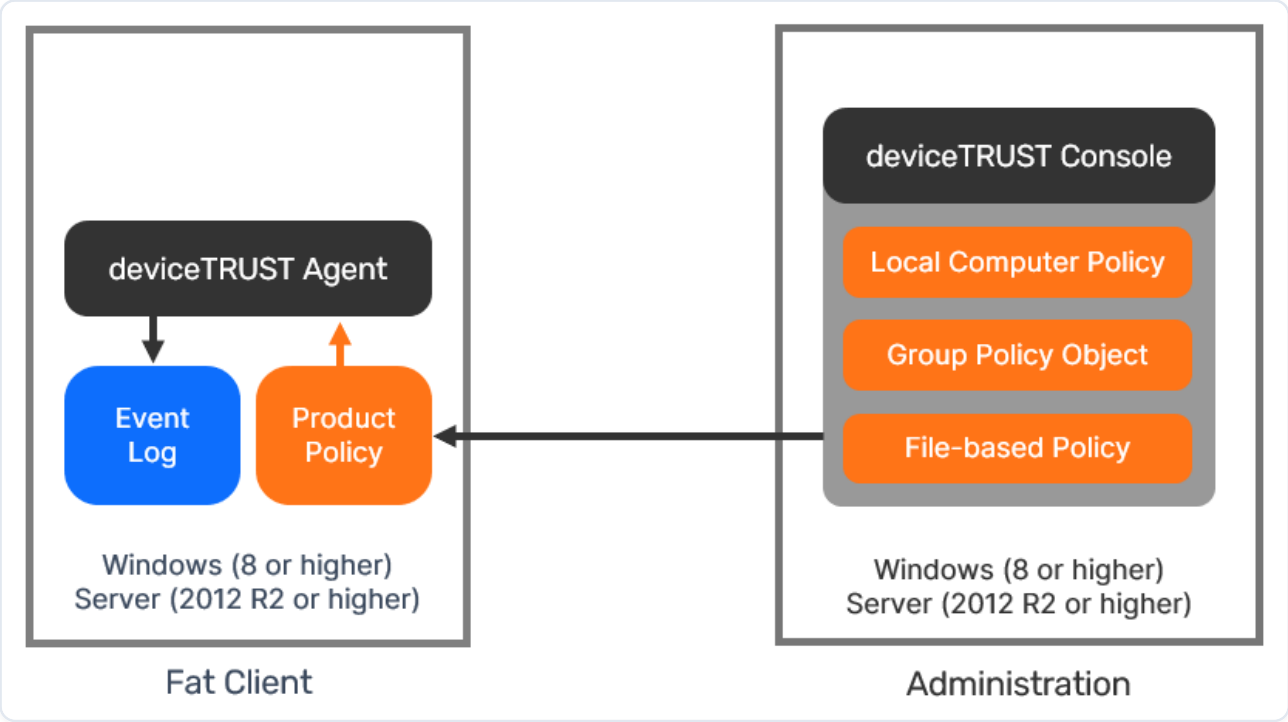
Scenario: Local

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

Getting Started for Local

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

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



We will perform the following steps:

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

Step 1: Download the deviceTRUST setup binaries

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

Step 2: Install the deviceTRUST Agent

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

Step 3: Install the deviceTRUST Console

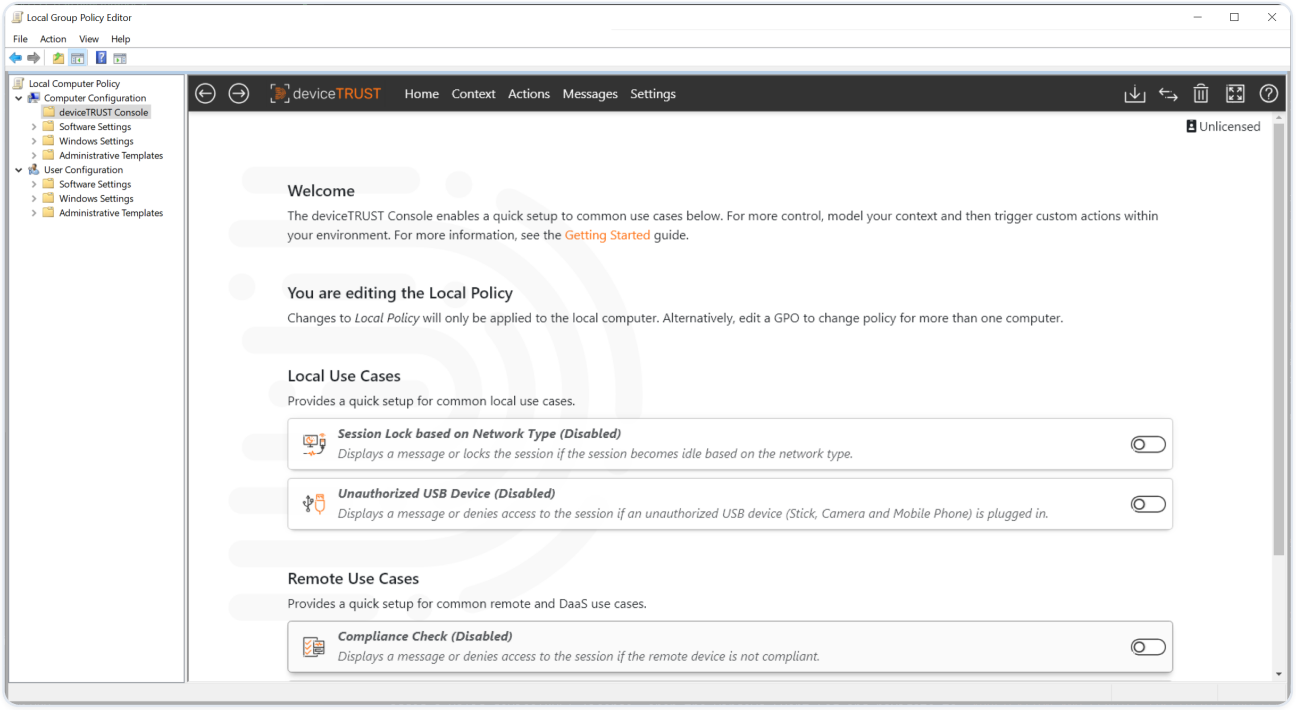
To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the

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

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

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

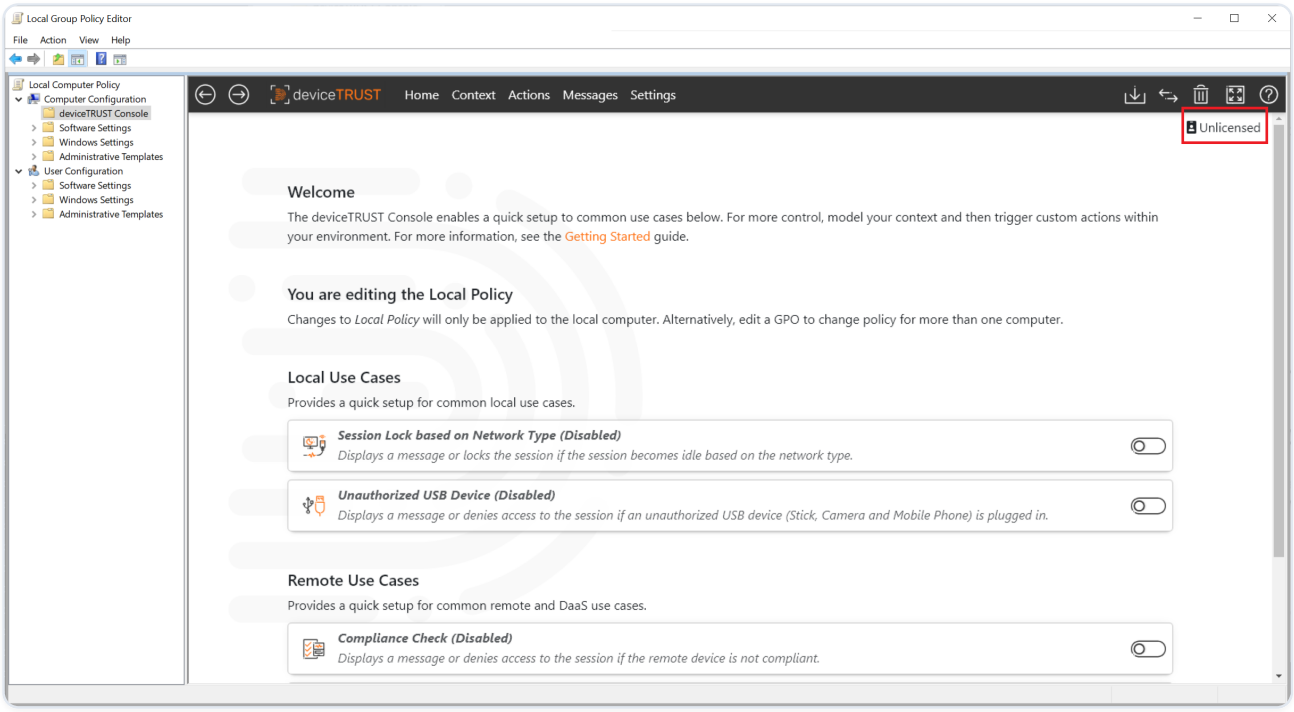
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



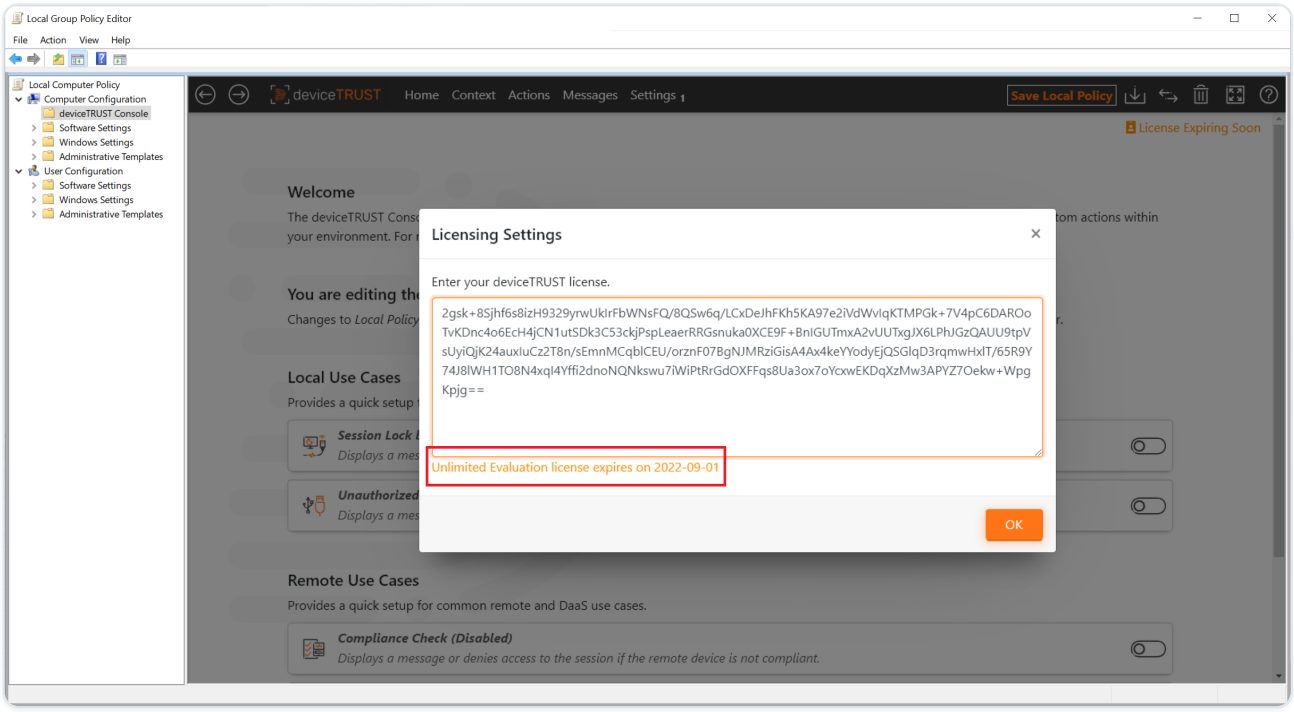
Step 4: Enter your deviceTRUST License

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

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

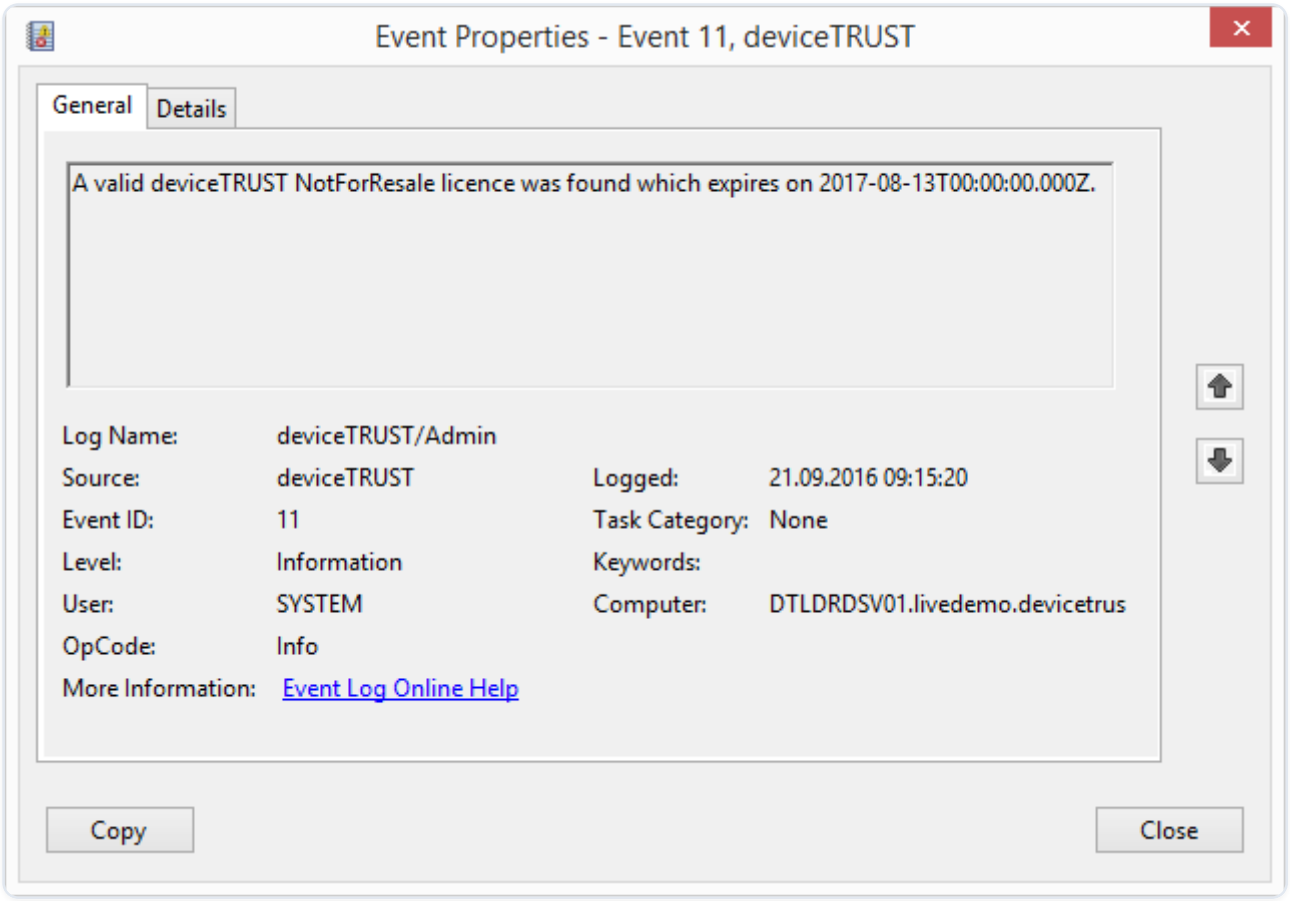


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.



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

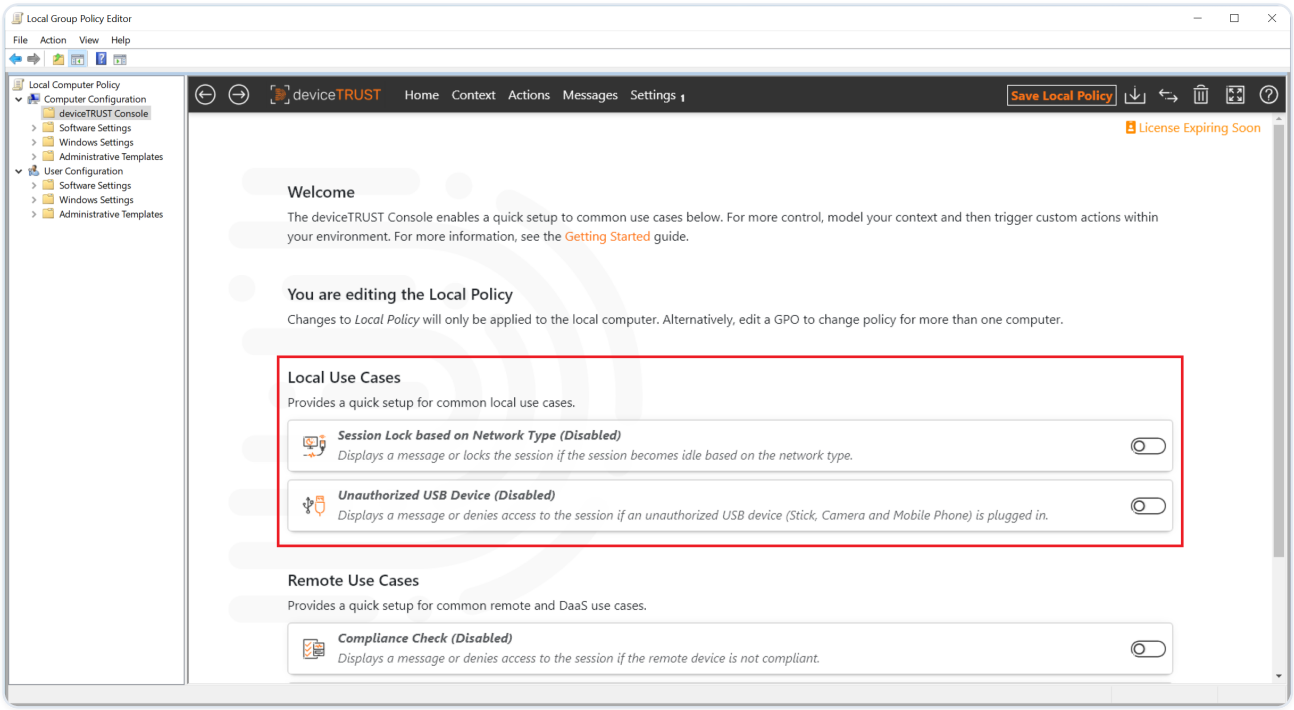
© 1997–2026 Citrix Systems, Inc. All rights reserved.



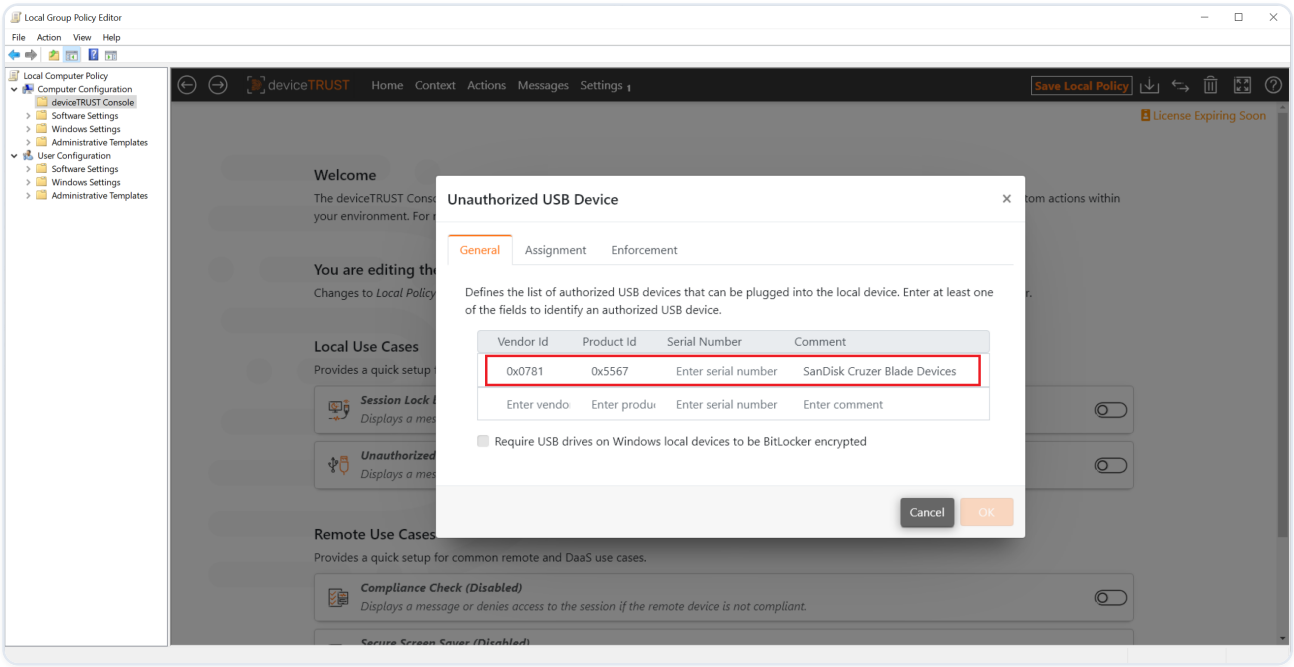
Step 5: Enable the Unauthorized USB Drive use case

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

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

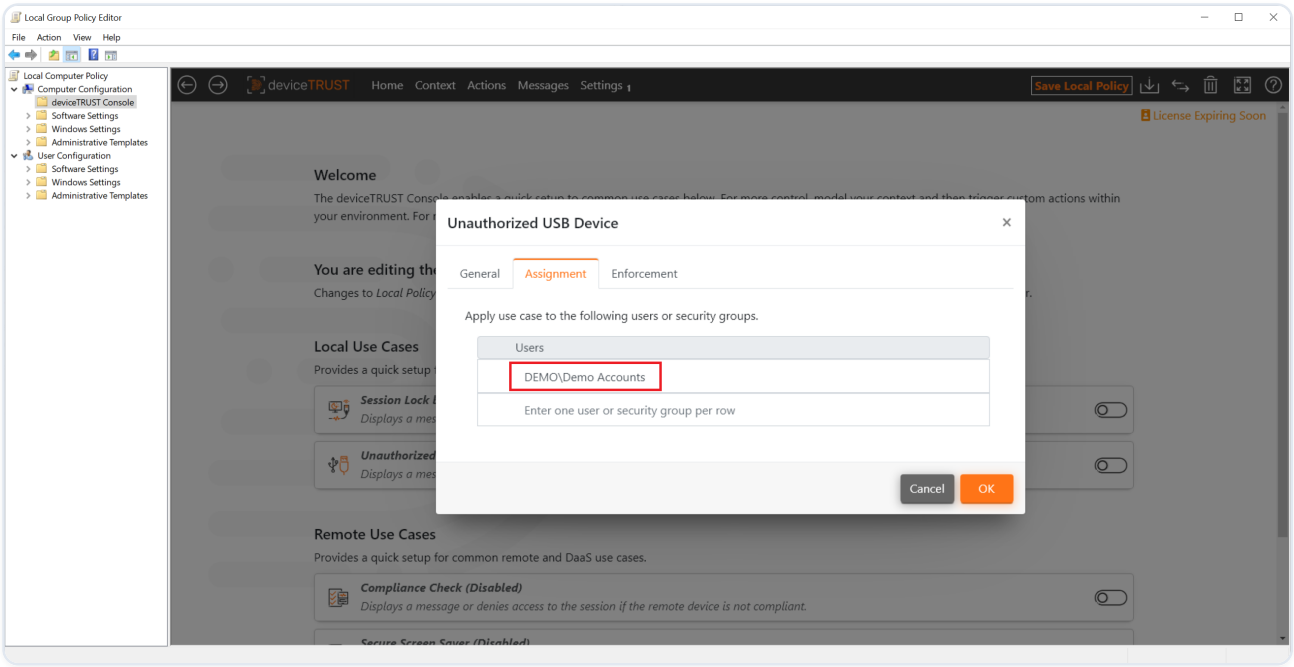


Select the `UNAUTHORIZED USB DEVICE` use case and add authorized USB devices on the `GENERAL` tab into the list of authorized USB devices.

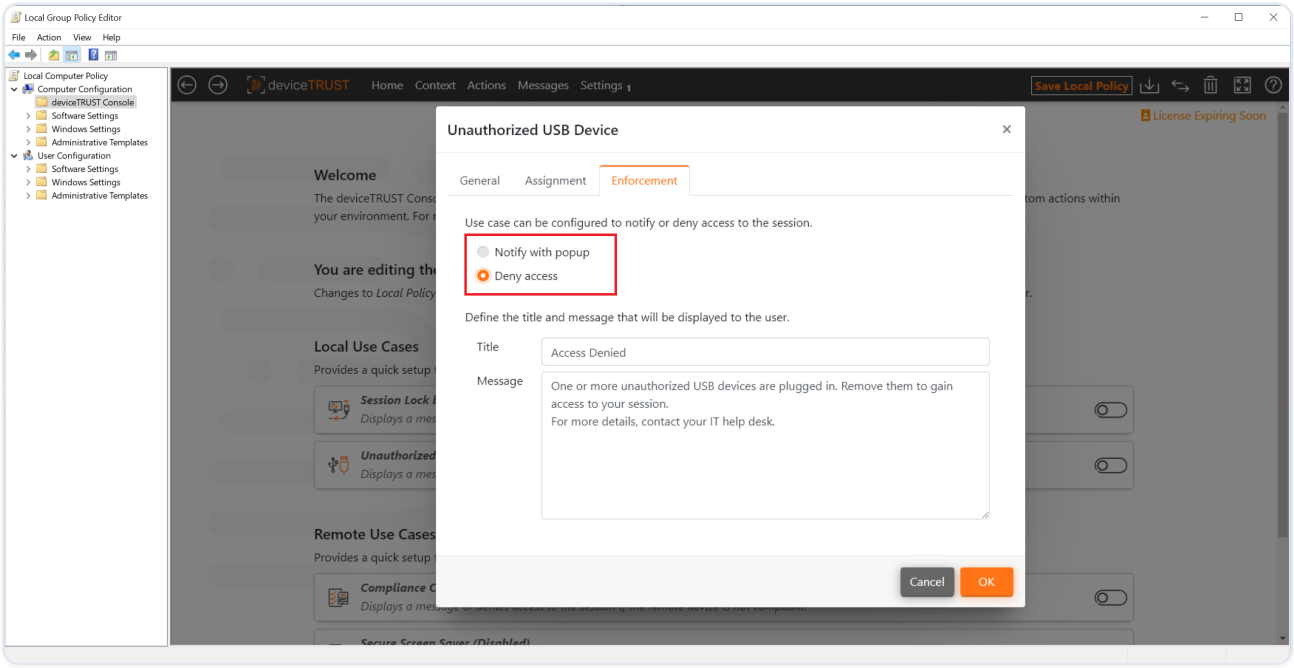


Click on the `ASSIGNMENT` configuration tab and add `USERS` and / or `SECURITY GROUPS` to apply the use case for.

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

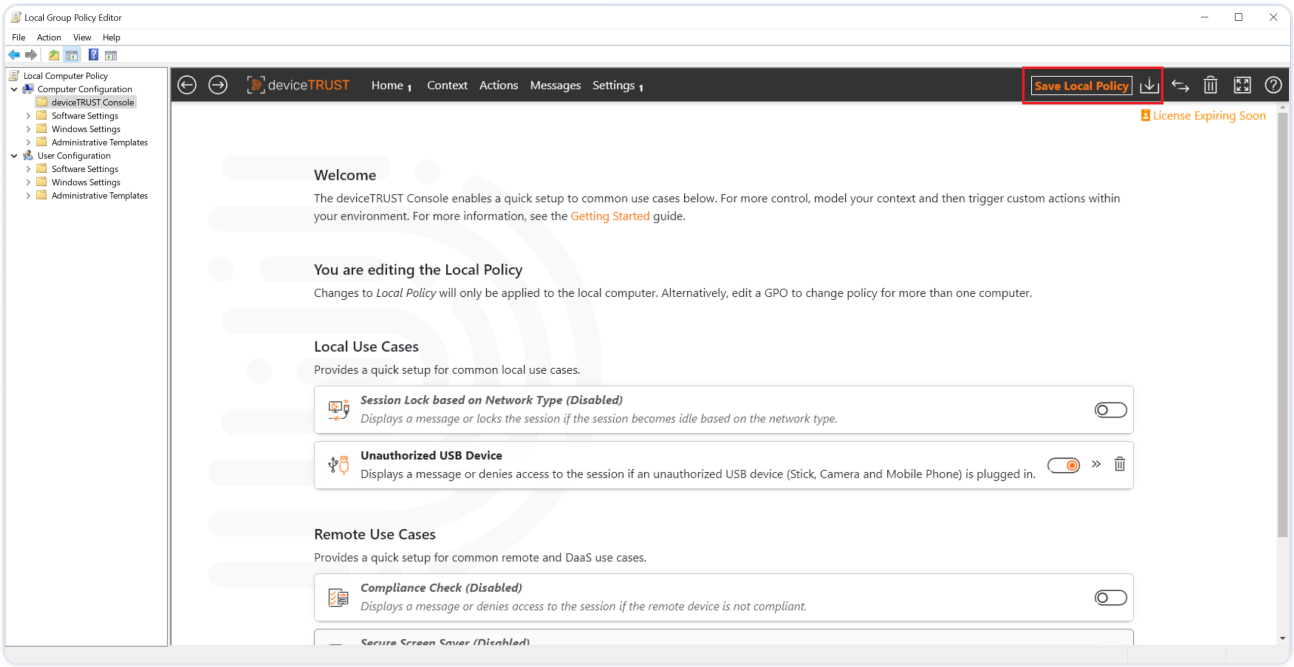


Click on the `ENFORCEMENT` configuration tab and select `DENY ACCESS`.



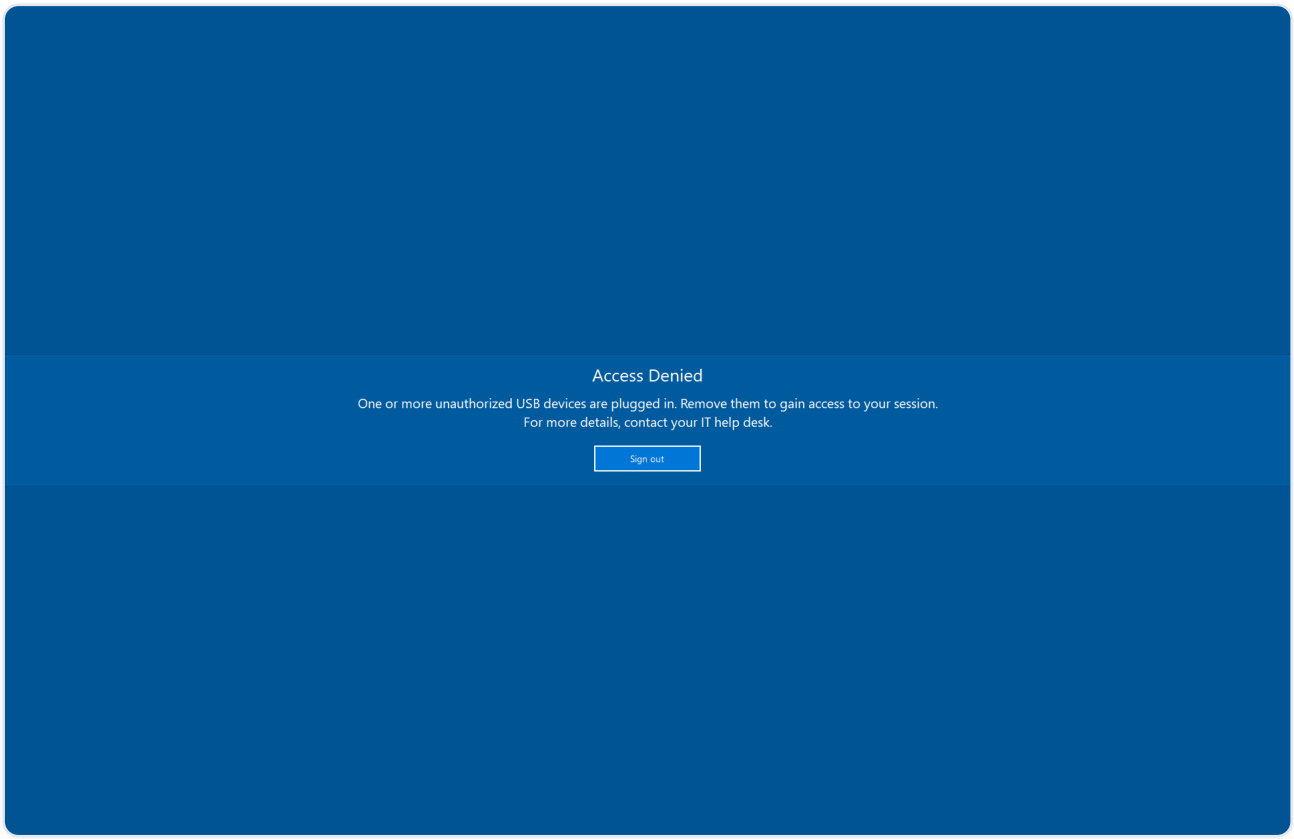
Click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar to save the unauthorized USB device use case to the local computer policy.

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



Step 6: Test the Unauthorized USB Device use case

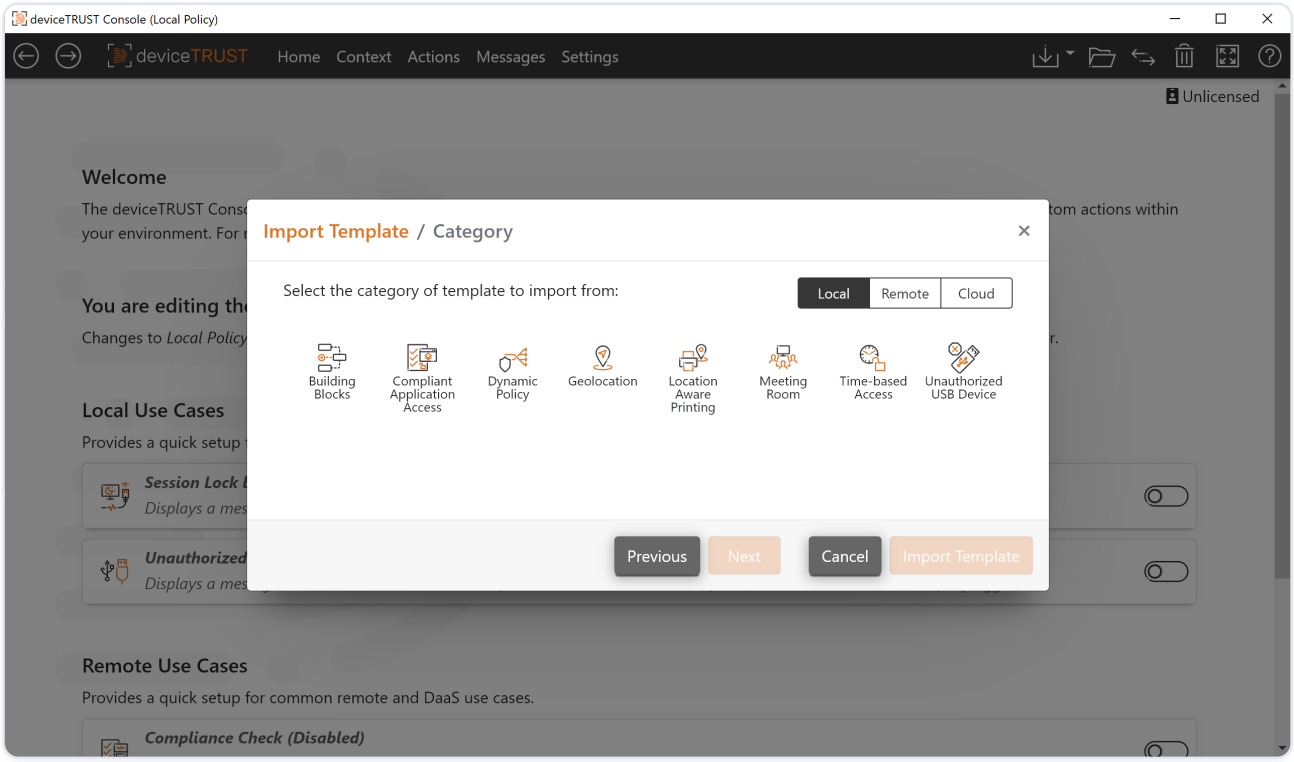
Sign in with a non-administrative user account to the local device and then plug in an authorized USB device at runtime. The authorized USB device is displayed in Windows Explorer and can be used. Now plug in an unauthorized USB device in addition or exclusively to see how deviceTRUST can easily and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



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

Next steps

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



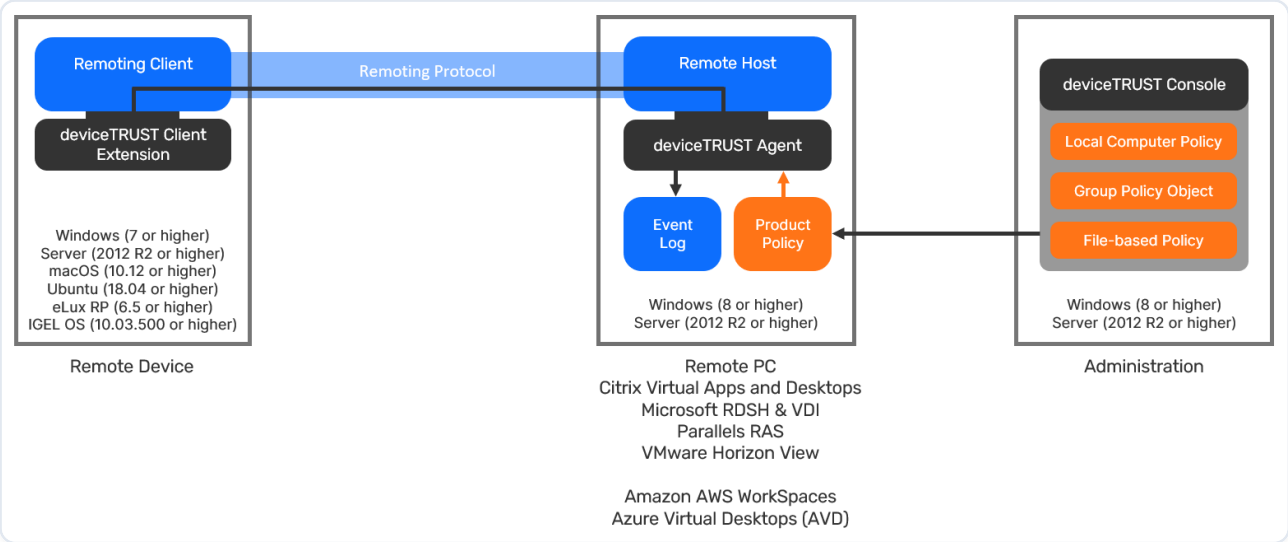
Troubleshooting

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

Getting Started for Remote

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

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



We will perform the following steps:

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

Step 1: Download the deviceTRUST setup binaries

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

Step 2: Install the deviceTRUST Agent

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

Step 3: Install the deviceTRUST Console

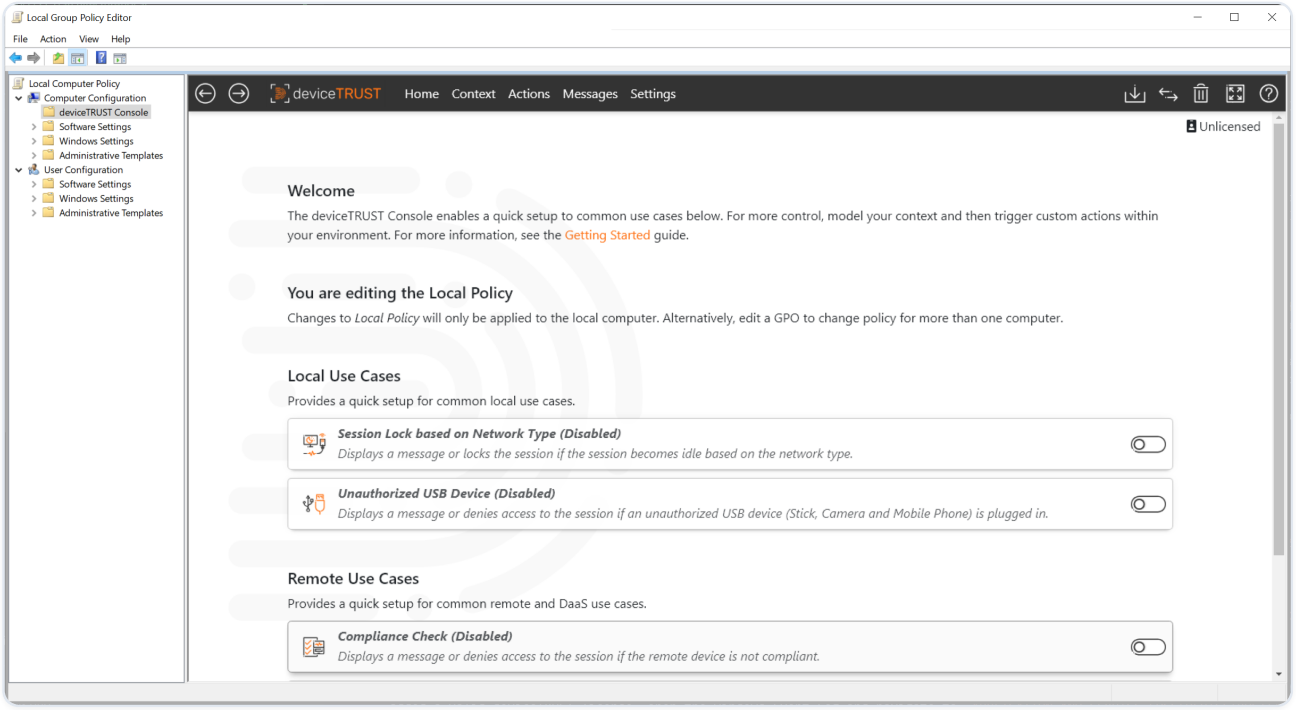
To configure and to apply contextual security policies to the deviceTRUST Agent you need to use the deviceTRUST Console. The deviceTRUST Console supports various ways to provide the

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

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

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

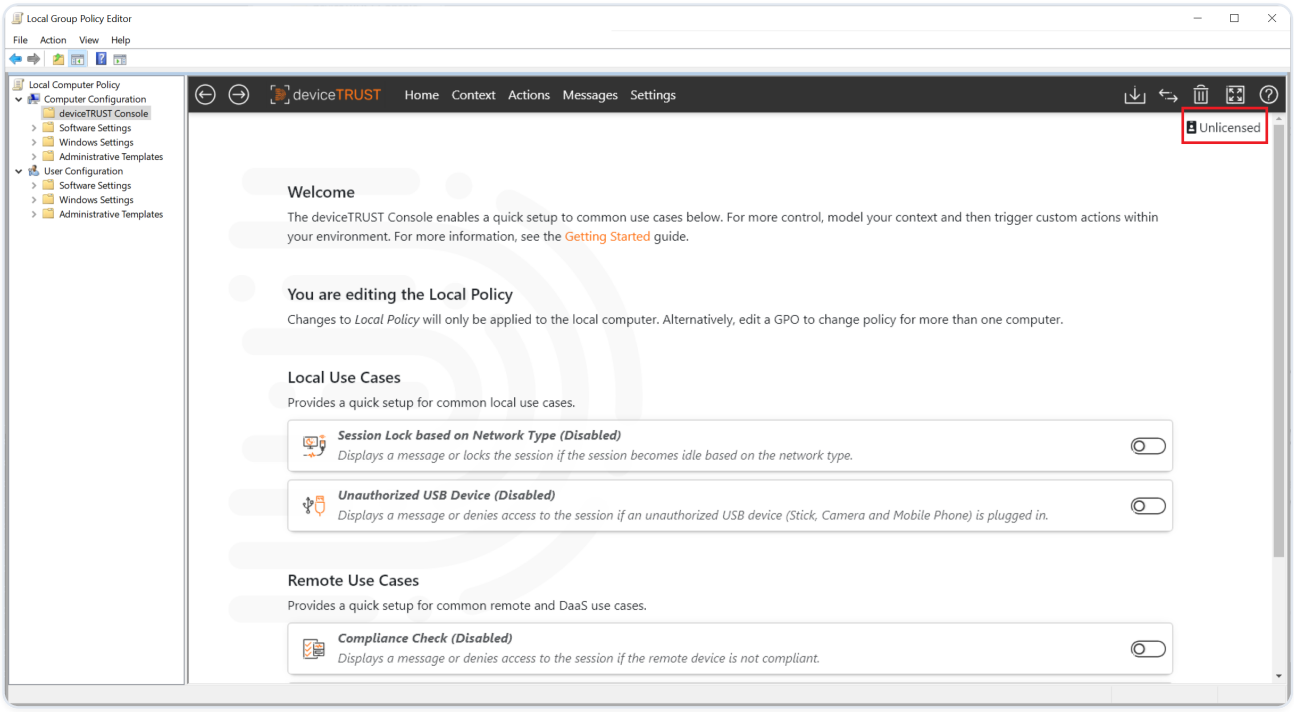
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



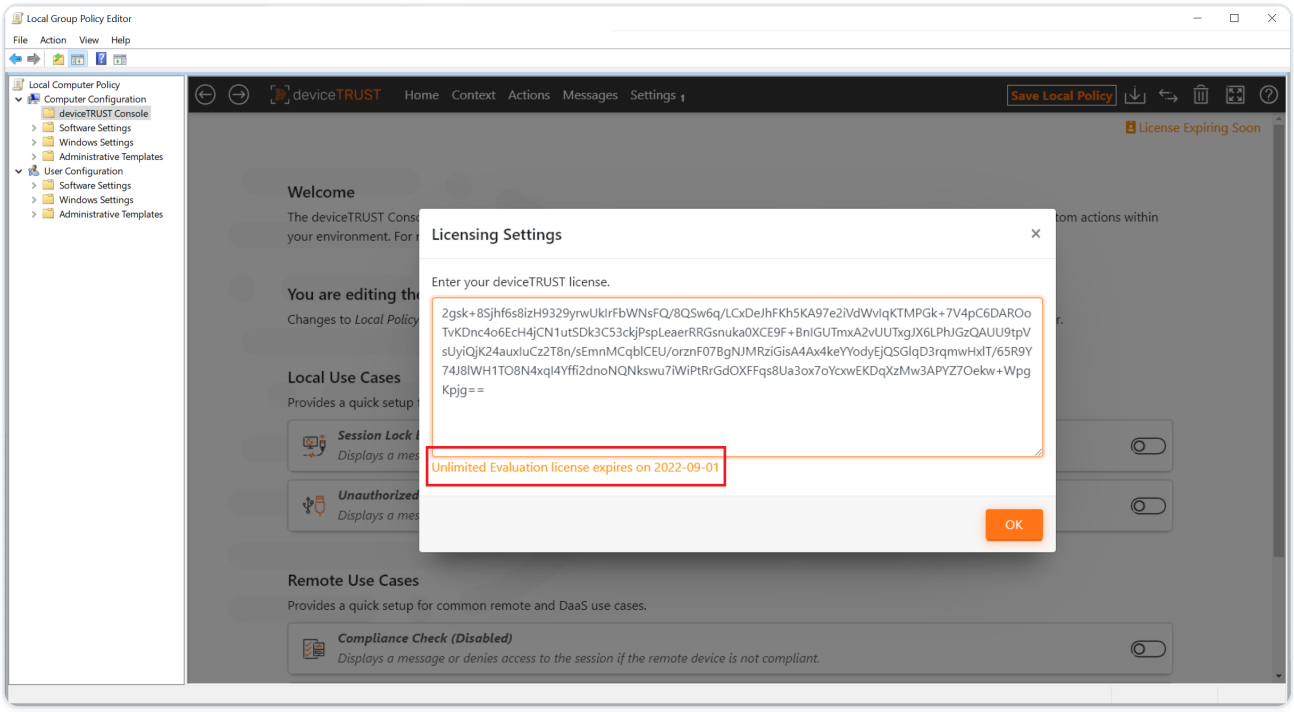
Step 4: Enter your deviceTRUST License

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

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

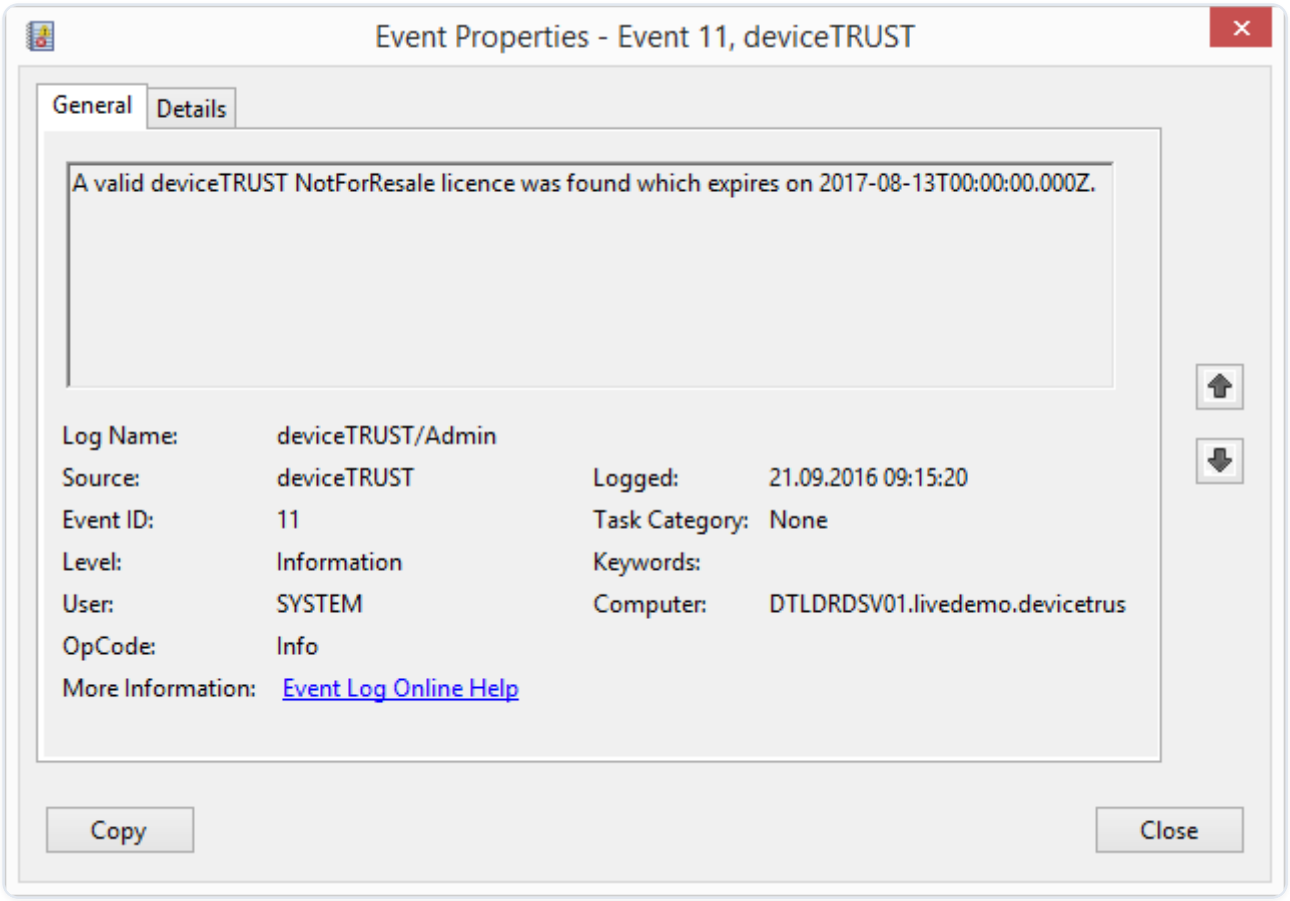


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.



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

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



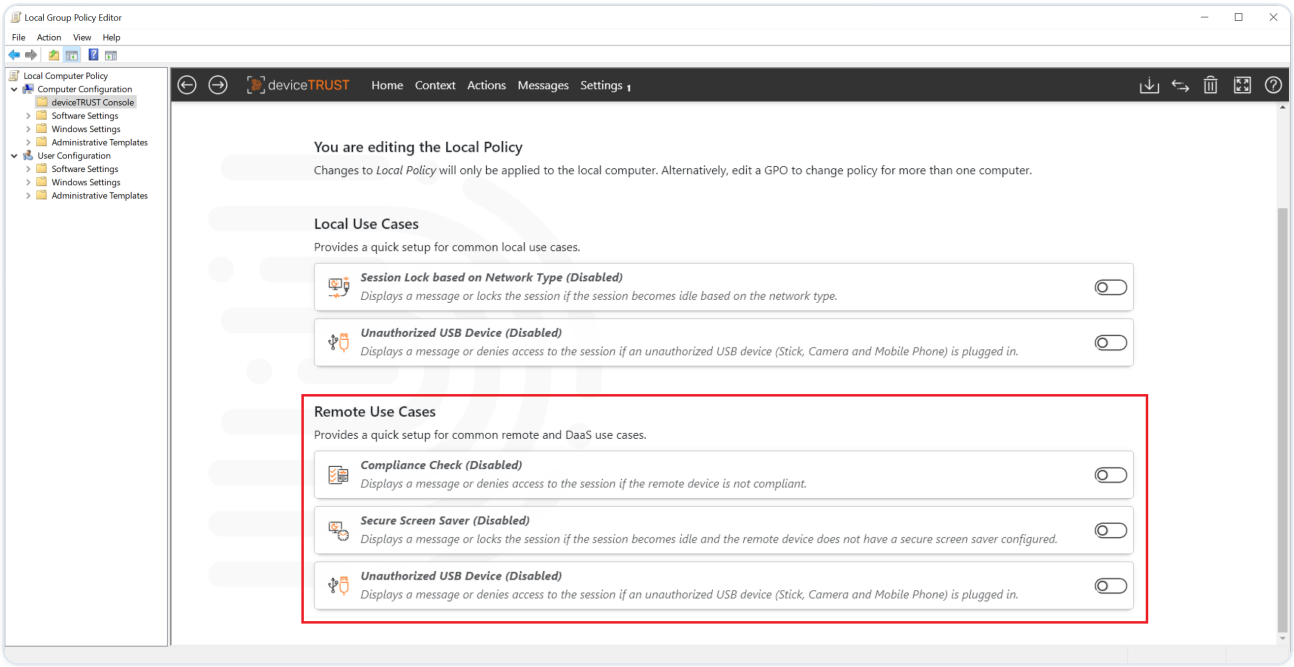
Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device

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

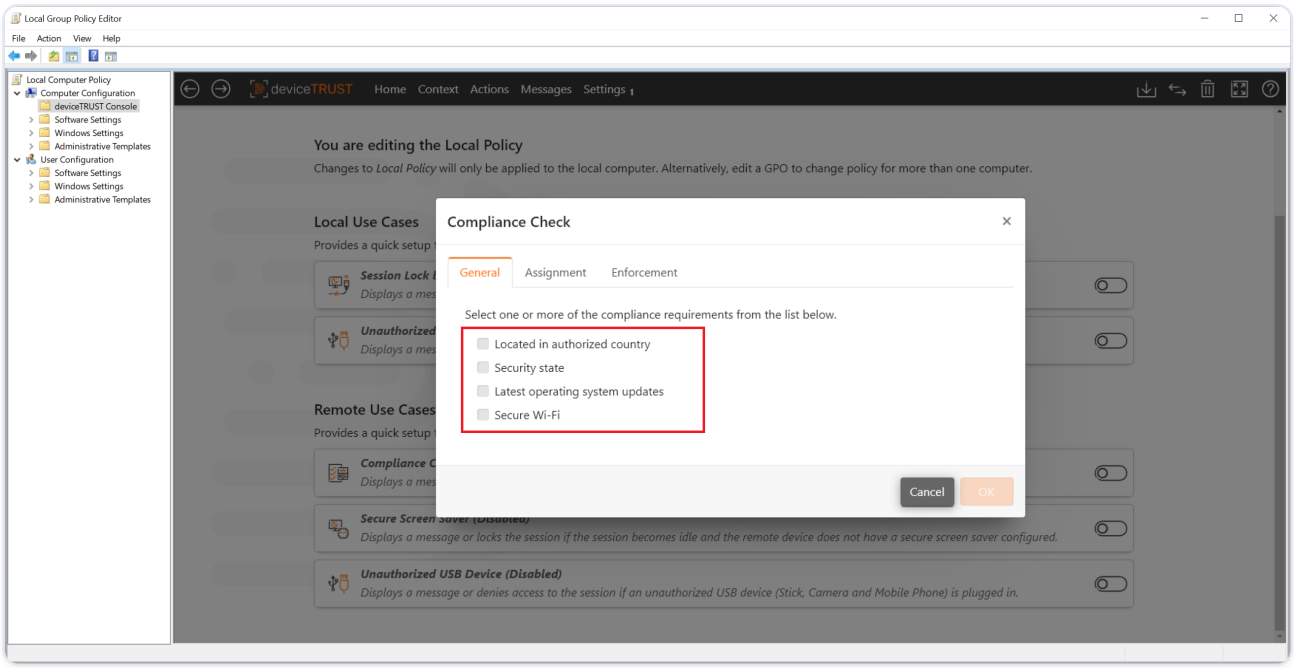
Step 6: Enable the Compliance Check use case

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

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

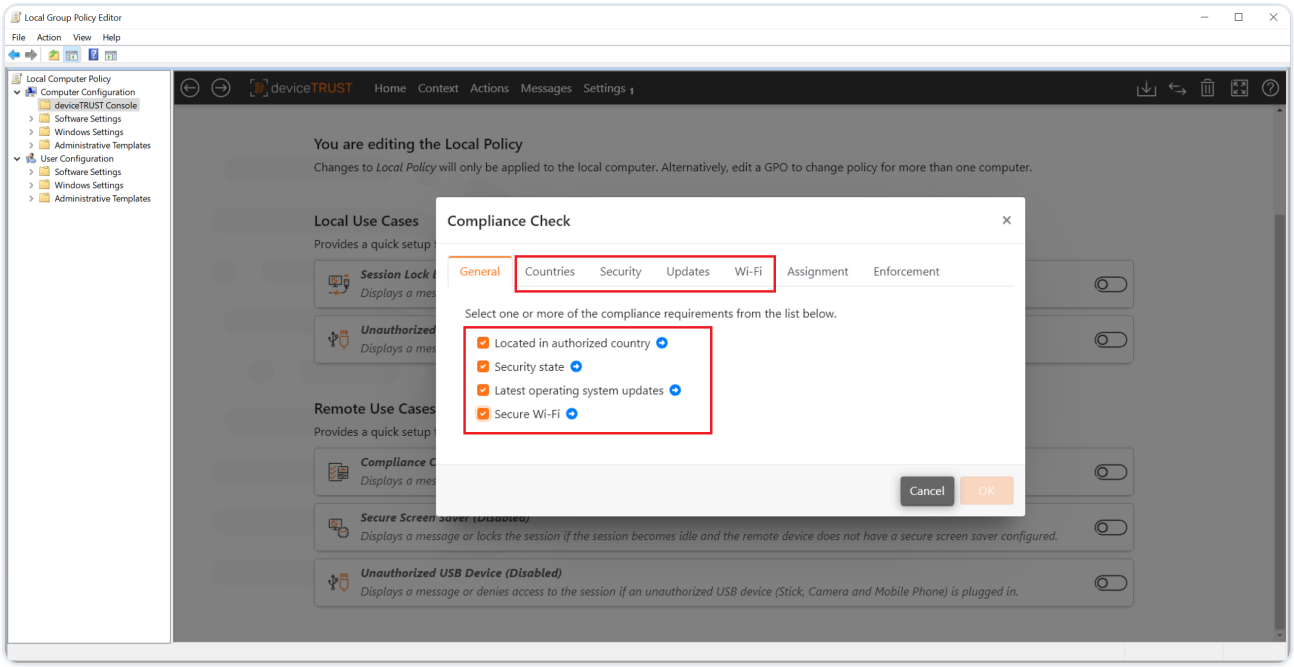


Select the `COMPLIANCE CHECK` use case, select on the `GENERAL` tab all options to be included in the compliance check.

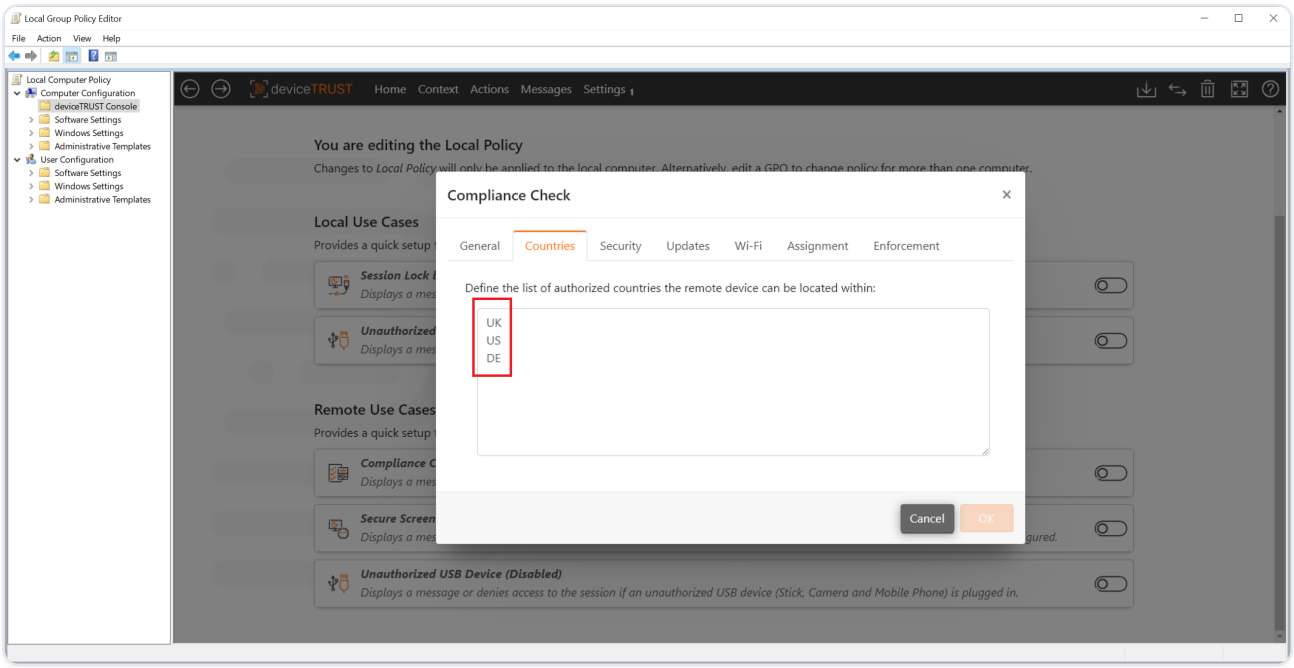


New configuration tabs will become visible.

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

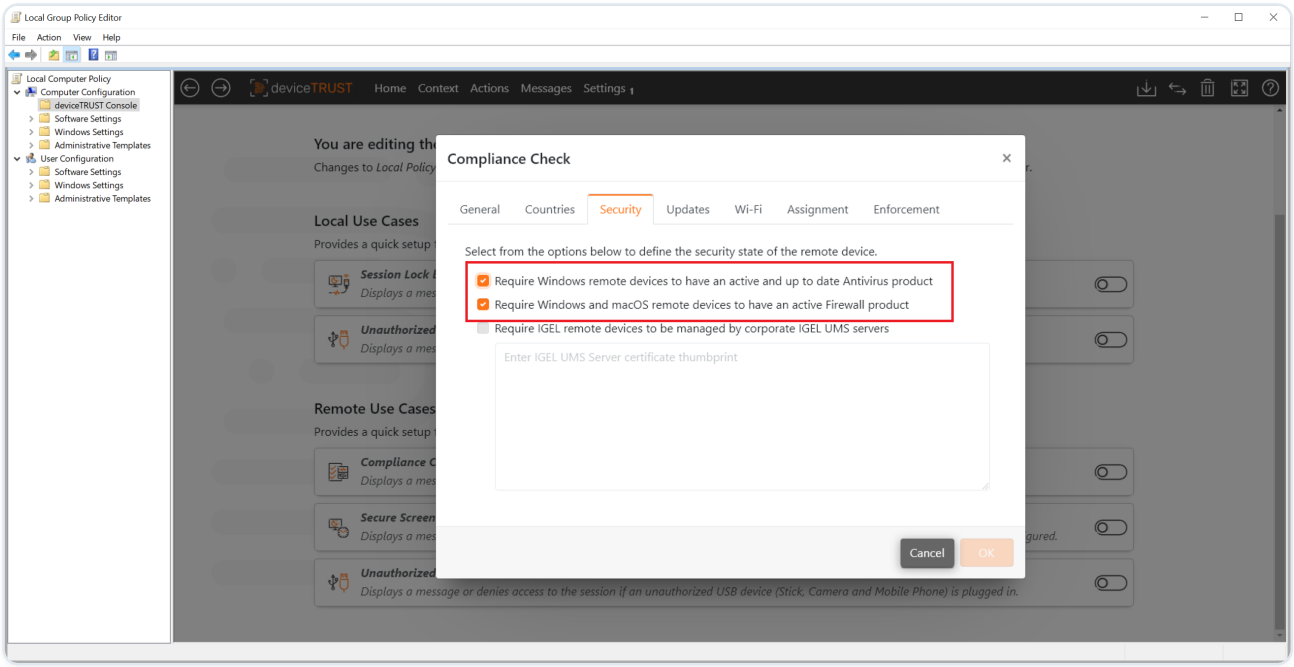


Click on the `COUNTRY` configuration tab and add all authorized countries using ISO 3166-1 Alpha-2 code.

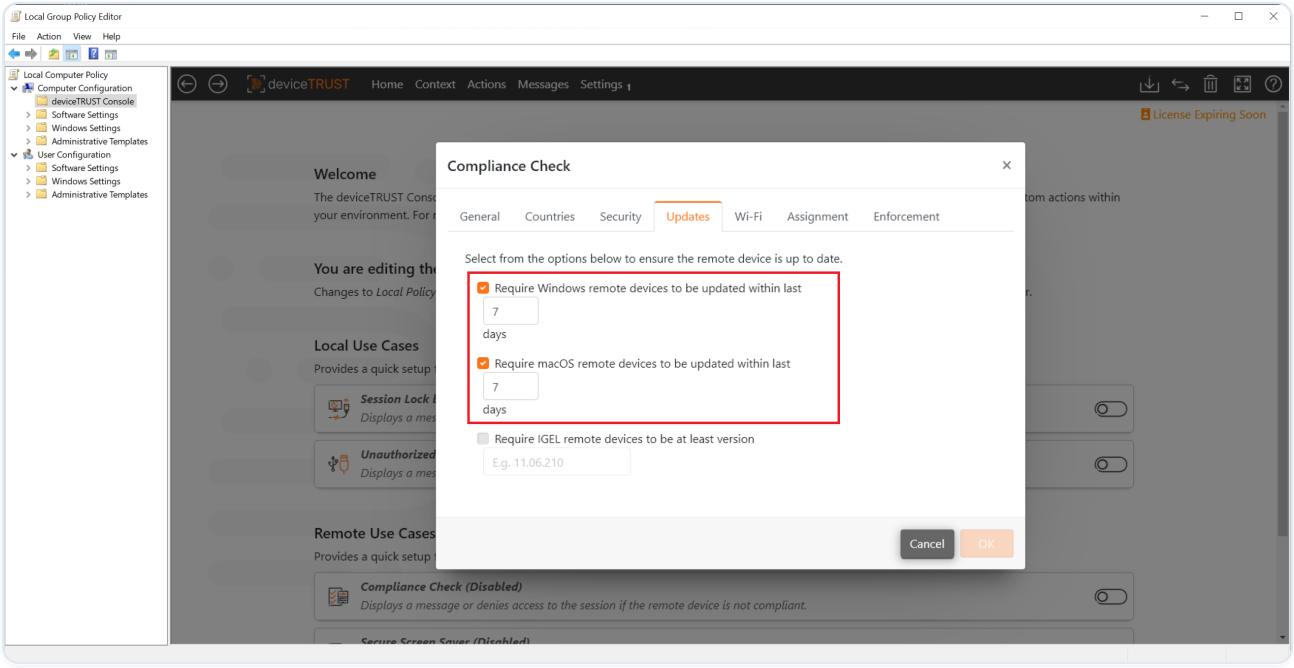


Click on the `SECURITY` configuration tab and enable the `REQUIRE WINDOWS REMOTE DEVICES TO HAVE AN ACTIVE AND UP TO DATE ANTIVIRUS PRODUCT` and `REQUIRE WINDOWS AND MACOS REMOTE DEVICES TO HAVE AN ACTIVE FIREWALL PRODUCT` options.

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

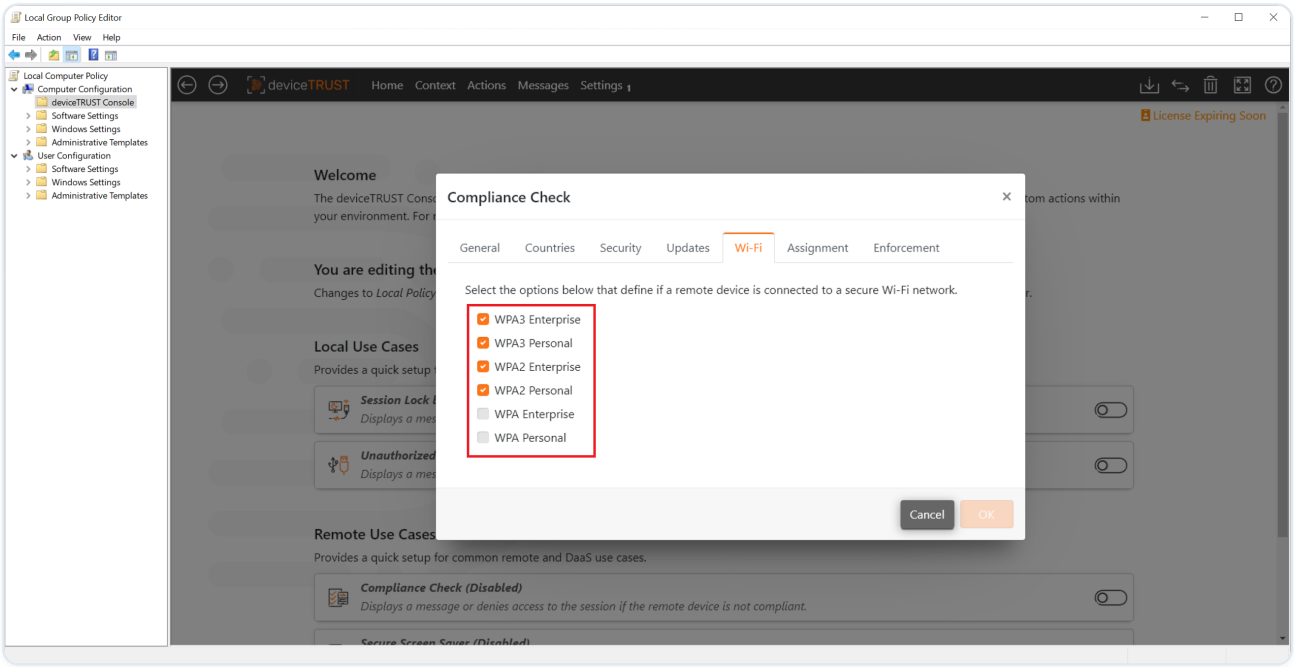


Click on the `UPDATES` configuration tab and enable the `REQUIRE WINDOWS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` and `REQUIRE MACOS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` options.

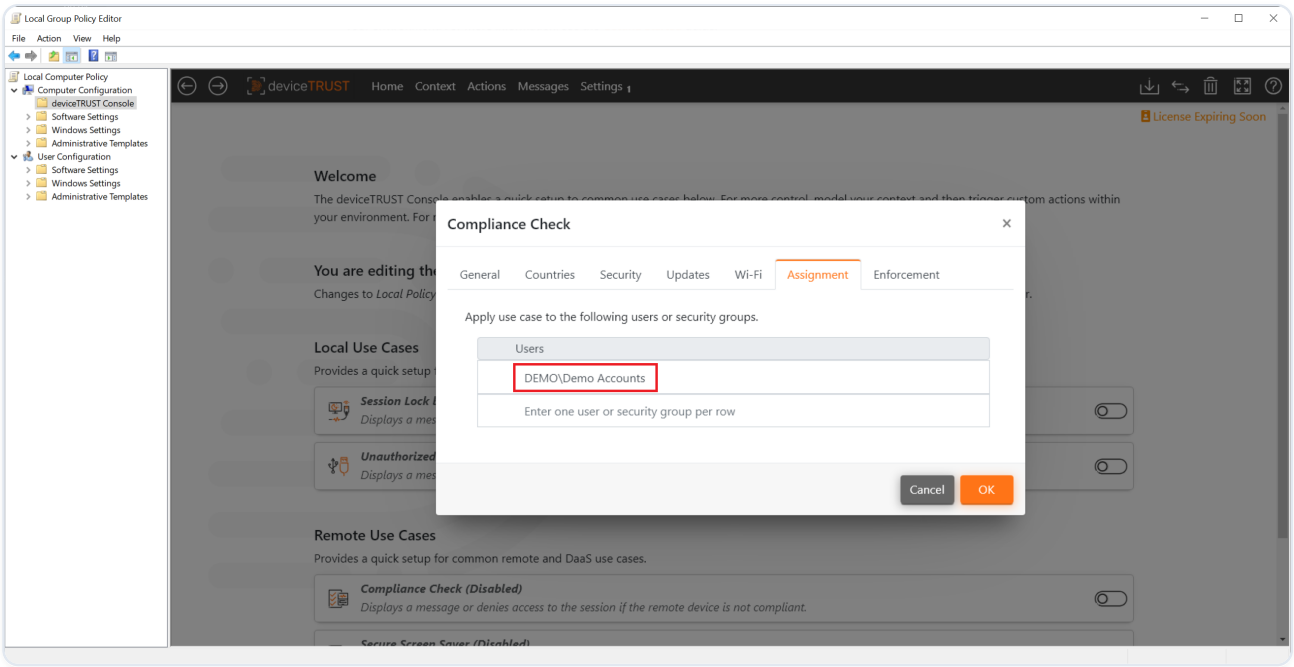


Click on the `WI-FI` configuration tab and enable the `WPA3 ENTERPRISE`, `WPA3 PERSONAL`, `WPA2 ENTERPRISE` and `WPA2 PERSONAL` options.

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

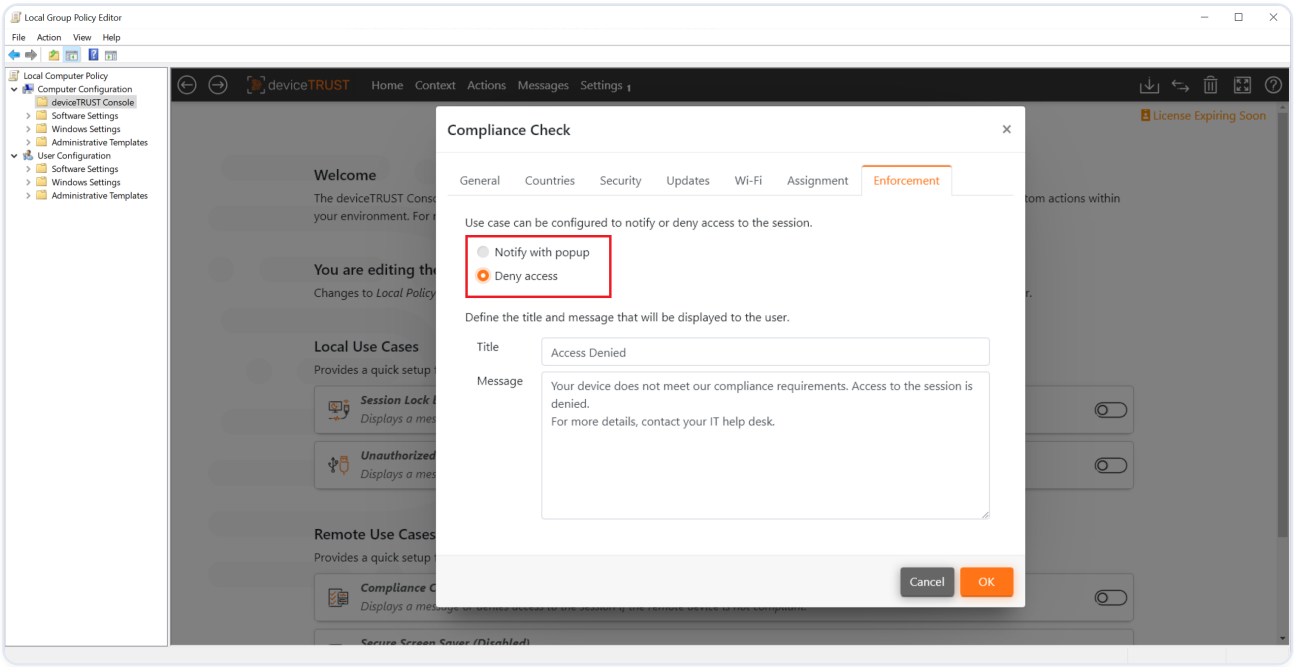


Click on the `ASSIGNMENT` configuration tab and add `USERS` and / or `SECURITY GROUPS` to apply the use case for.

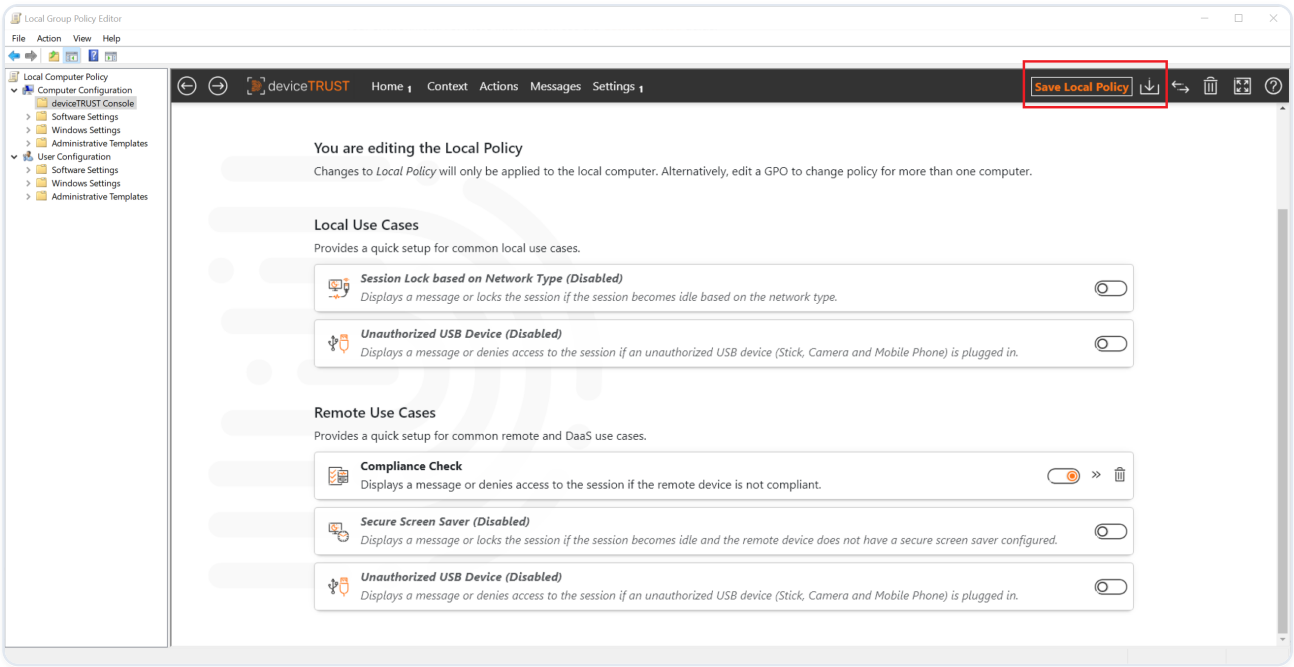


Click on the `ENFORCEMENT` configuration tab and select `DENY ACCESS`.

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



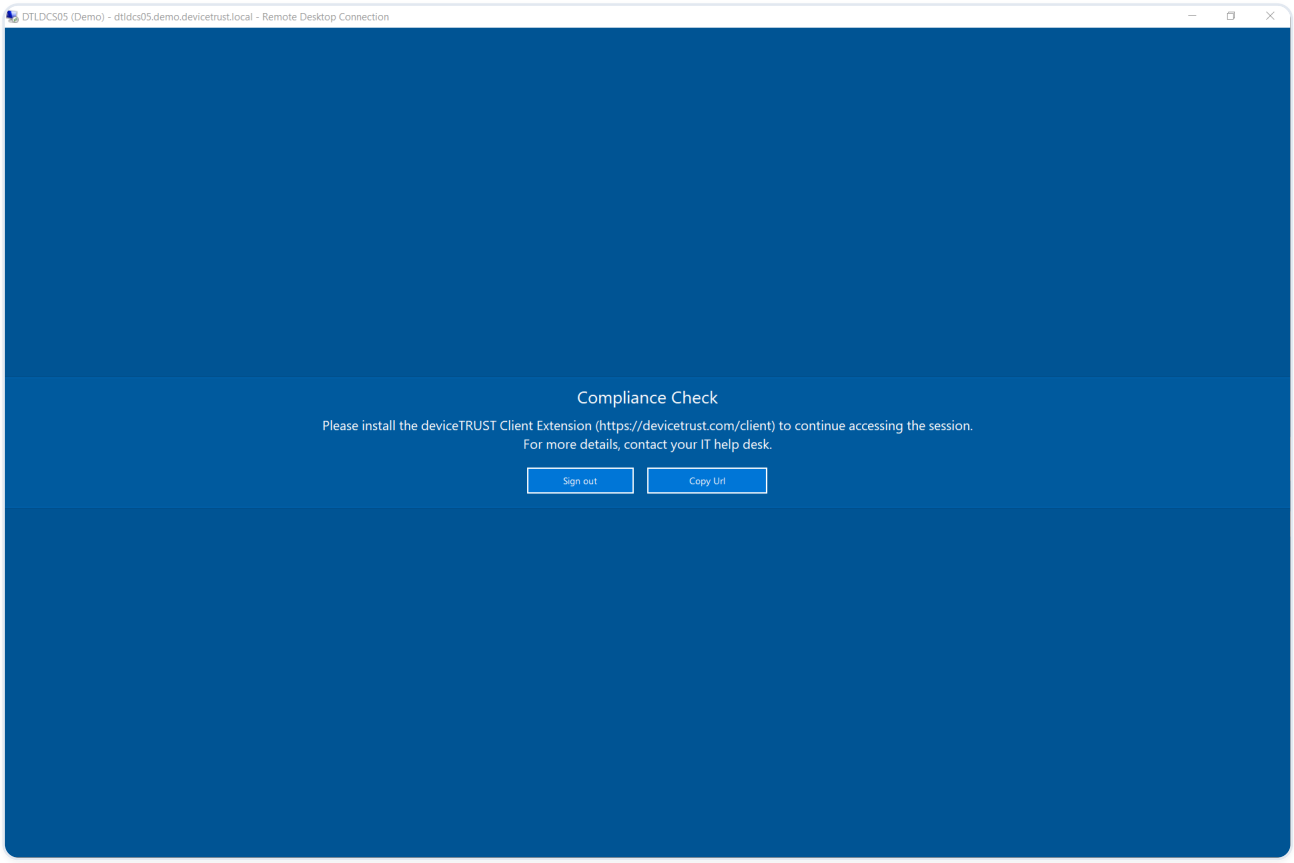
Click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar to save the complianc check use case to the local computer policy.



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

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

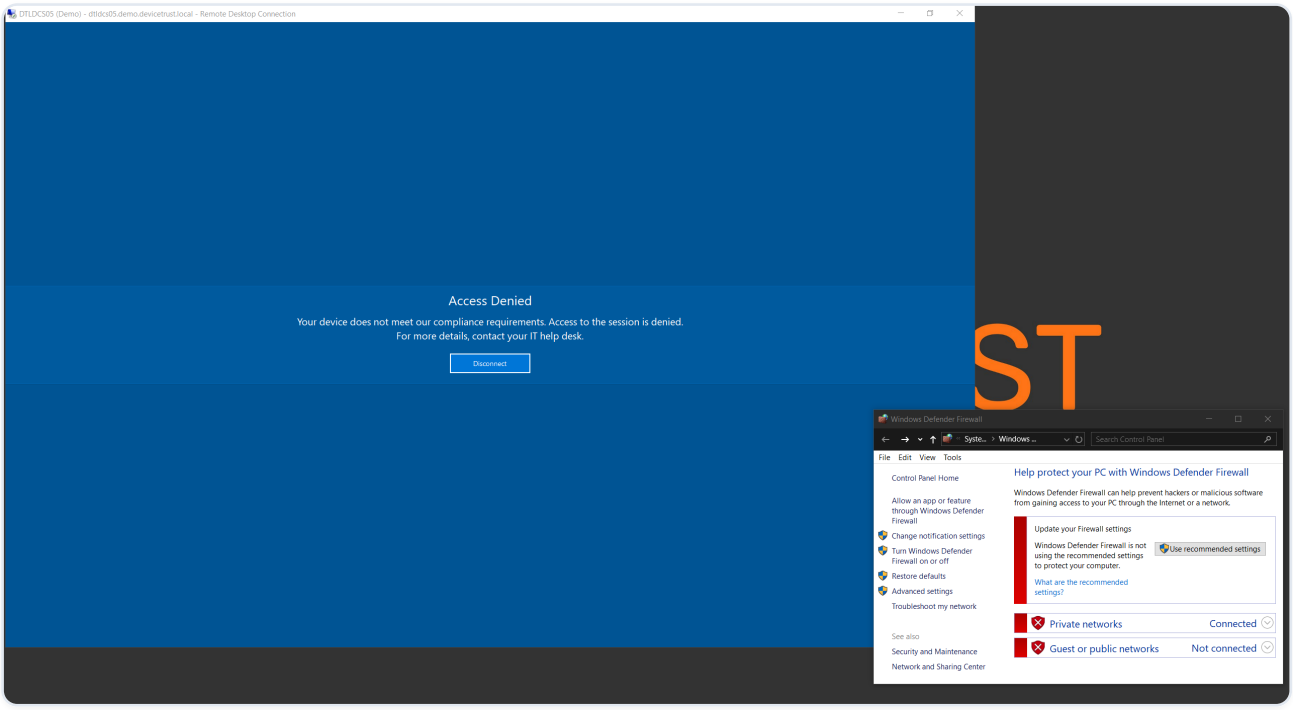
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

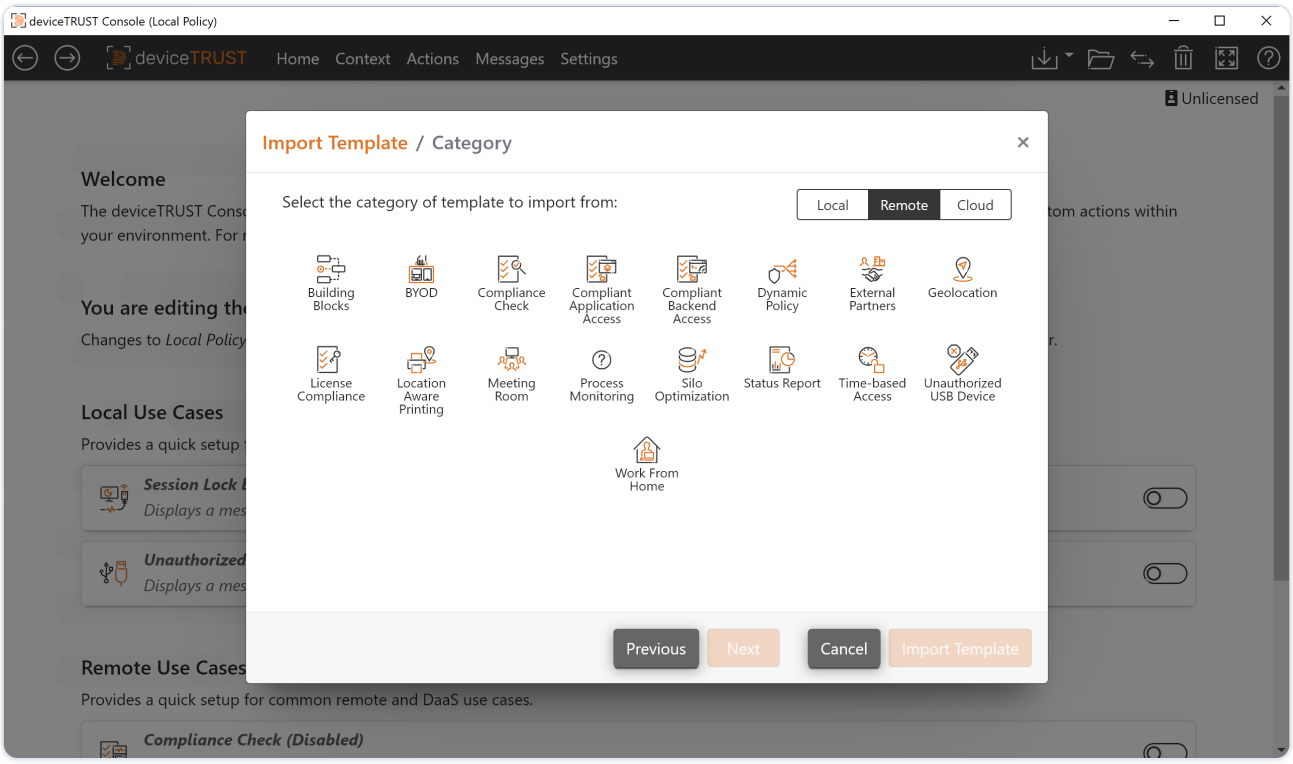
From a Microsoft Windows device with the deviceTRUST Client Extension installed, connect to your remoting or DaaS host system. Toggle the state of the Windows Defender Firewall to see how deviceTRUST can simply and dynamically control access to the session depending on the firewall state of the remote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

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



Next steps

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



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

Troubleshooting

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

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

Download deviceTRUST® Client Extensions

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

Download deviceTRUST 21.1

The latest deviceTRUST 21.1 binaries can be downloaded from the link below:

Version	21.1.310
Release Date	18th October 2022
Link	https://storage.devicetrust.com/download/deviceTRUST-21.1.310.zip
SHA256 Hash	5F7352EE9038C544AC7F5B04000A3DE7569ABB070FAA8F774EF345A04332E4A3

Download previous releases

Previous releases can be downloaded download.

Software components

After downloading the deviceTRUST software, you will find the following components within the compressed ZIP file:

COMPONENT	DESCRIPTION
DTAGENT-X64-RELEASE-x.x.x.x.MSI	The deviceTRUST 64-bit Agent installer.
DTAGENT-X86-RELEASE-x.x.x.x.MSI	The deviceTRUST 32-bit Agent installer.
DTCLIENT-EXTENSION-RELEASE-x.x.x.x.EXE	The deviceTRUST 32-bit and 64-bit Client Extension installer.

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

COMPONENT	DESCRIPTION
DTCONSOLE-X64-RELEASE-x.x.x.x.MSI	The deviceTRUST 64-bit Console installer.
DTCONSOLE-X86-RELEASE-x.x.x.x.MSI	The deviceTRUST 32-bit Console installer.
DTPOLICYDEFINITIONS-x.x.x.x.ZIP	The deviceTRUST ADMX policy definitions for configuring legacy options in the software from Microsoft Active Directory Group Policy (GPO).

NOTE

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

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

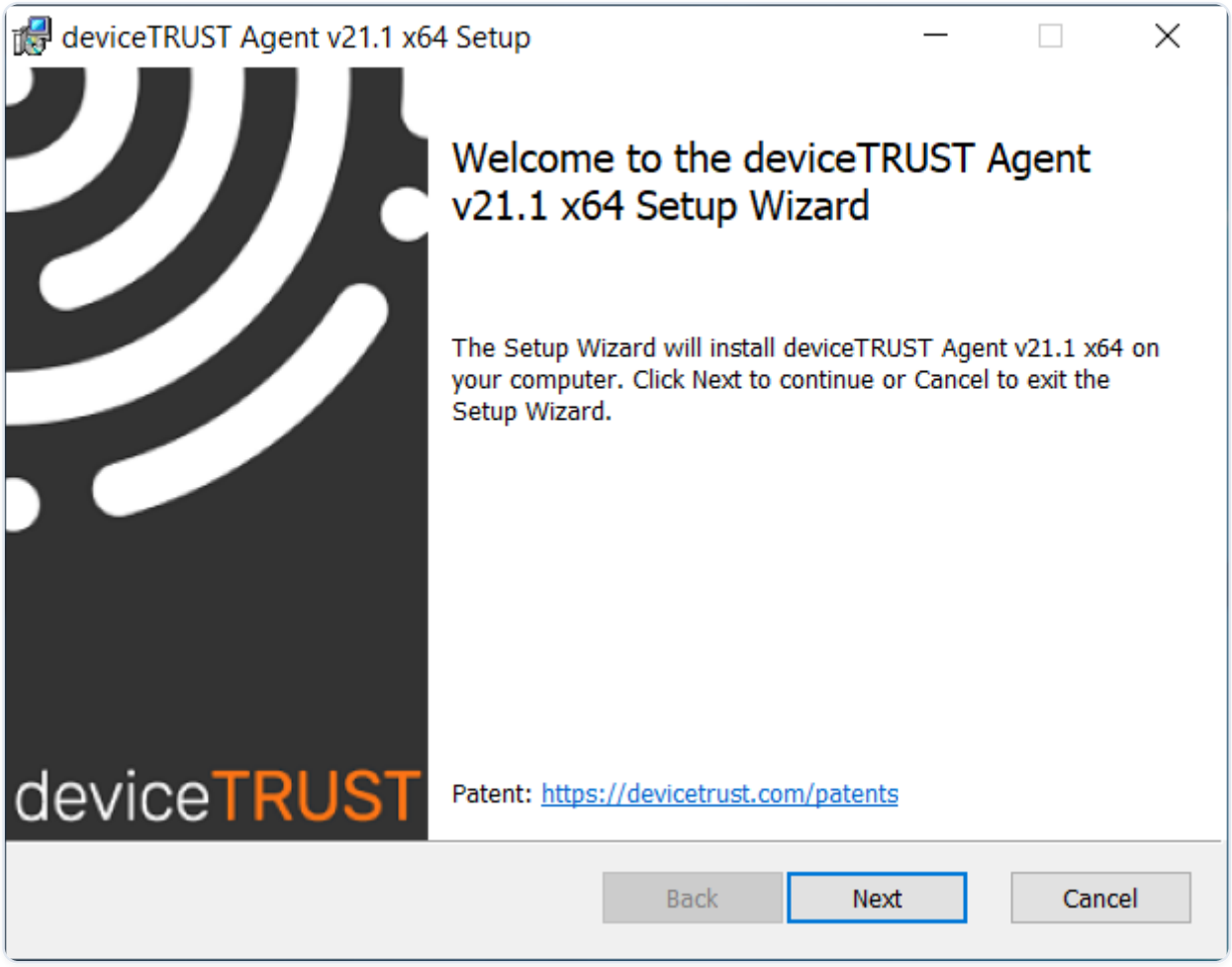
Installation

TABLE OF CONTENTS

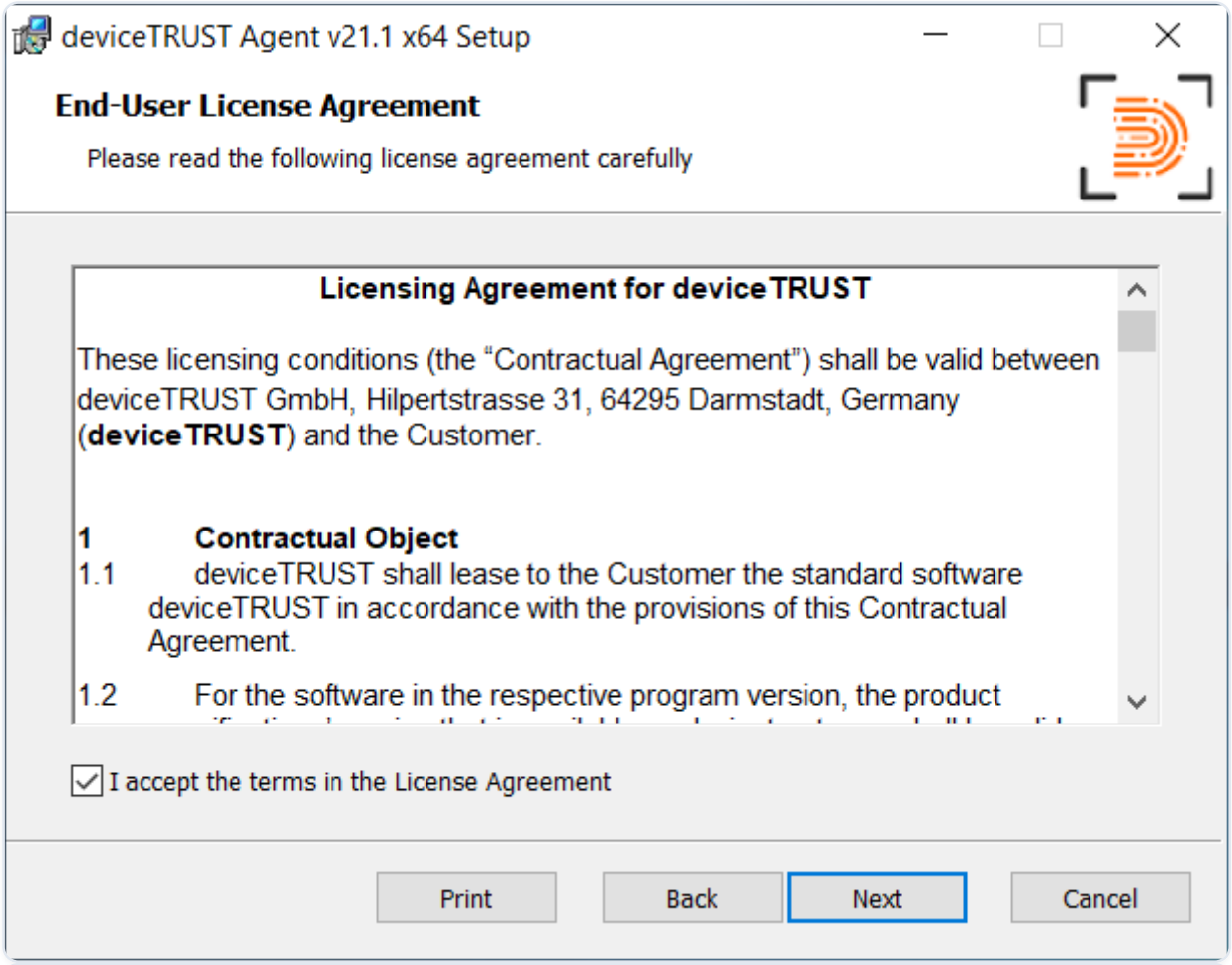
- Agent
- Console
- Client Extension

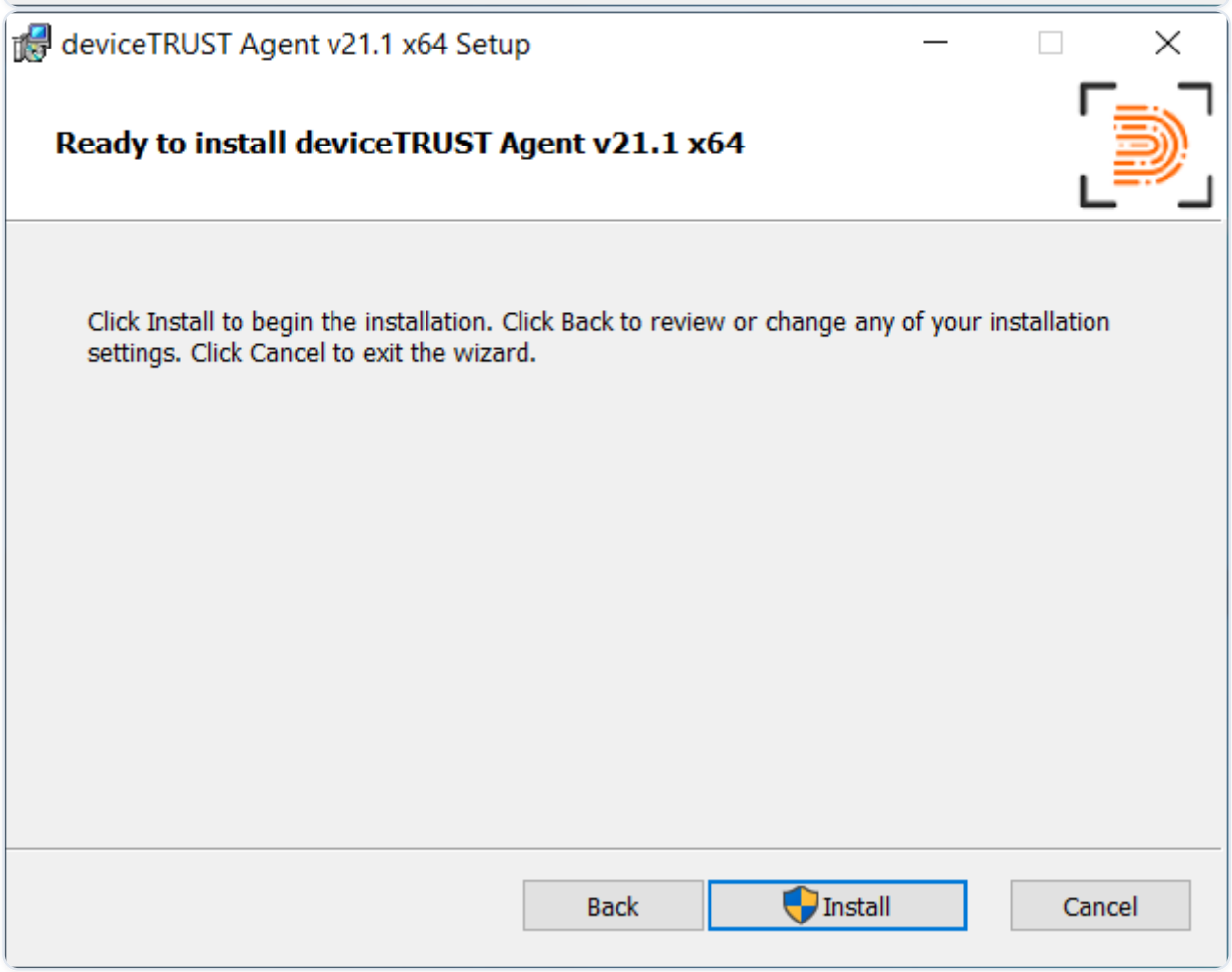
Installing the deviceTRUST® Agent

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

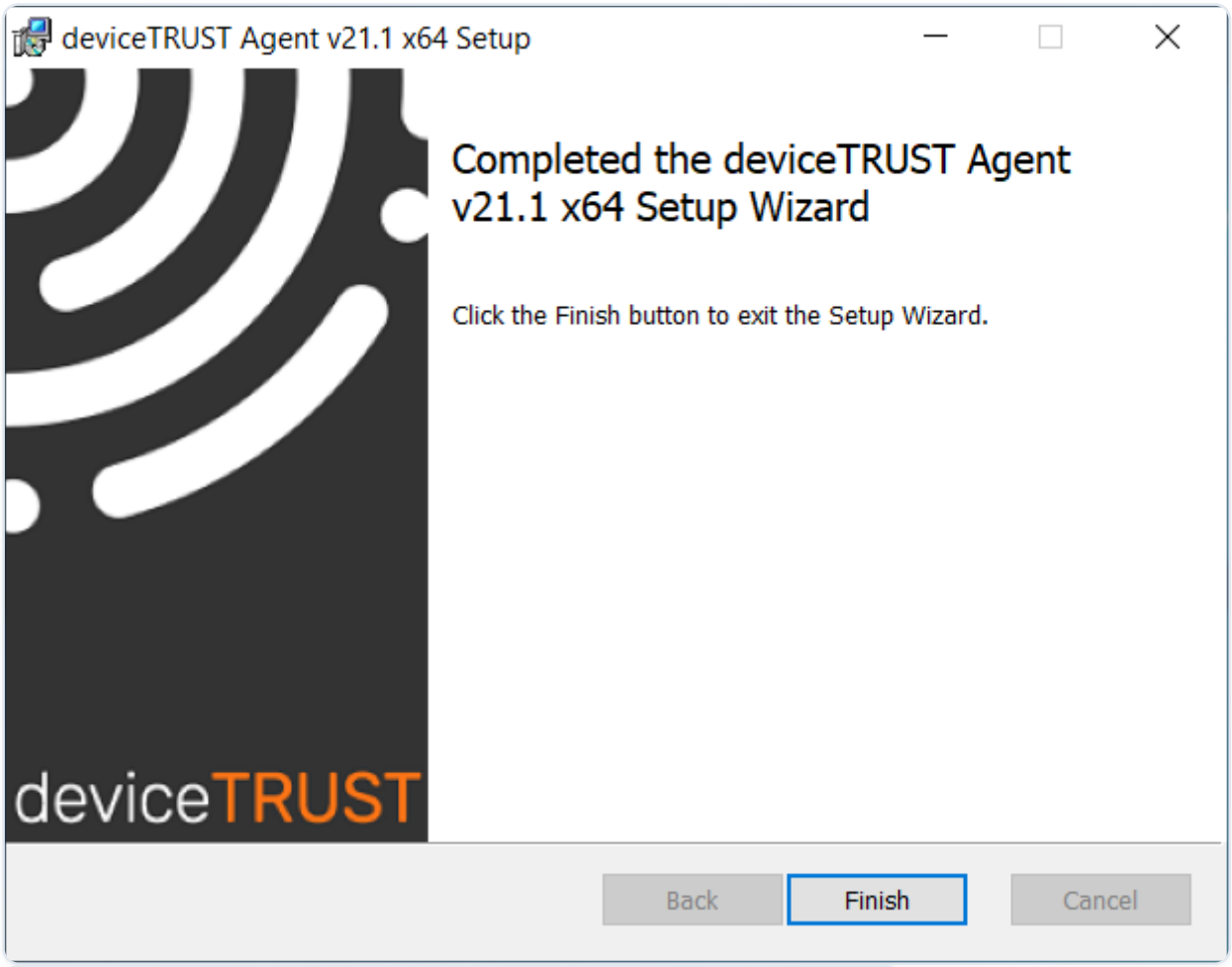


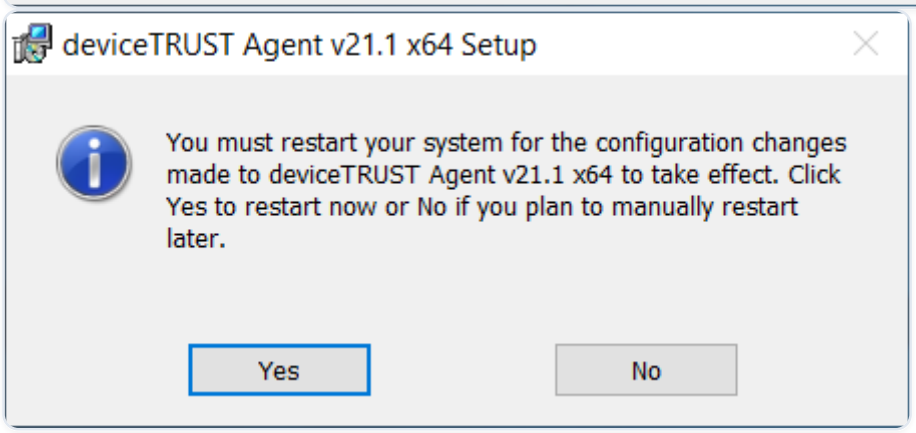
© 1997–2026 Citrix Systems, Inc. All rights reserved.





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





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

NOTE:

- Installation path: `%PROGRAMFILES%\DEVICETRUST\AGENT`
- If the installation of the deviceTRUST Agent has finished successfully, a reboot is required to enable deviceTRUST to get system notifications to act on.
- If the `*Remote Desktop Services*` server role is added after installing the deviceTRUST Agent, the deviceTRUST Agent will need to be reinstalled.
- The deviceTRUST Agent will not function until a valid license is applied.

Citrix Virtual Channel Security

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

Unattended Installation

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

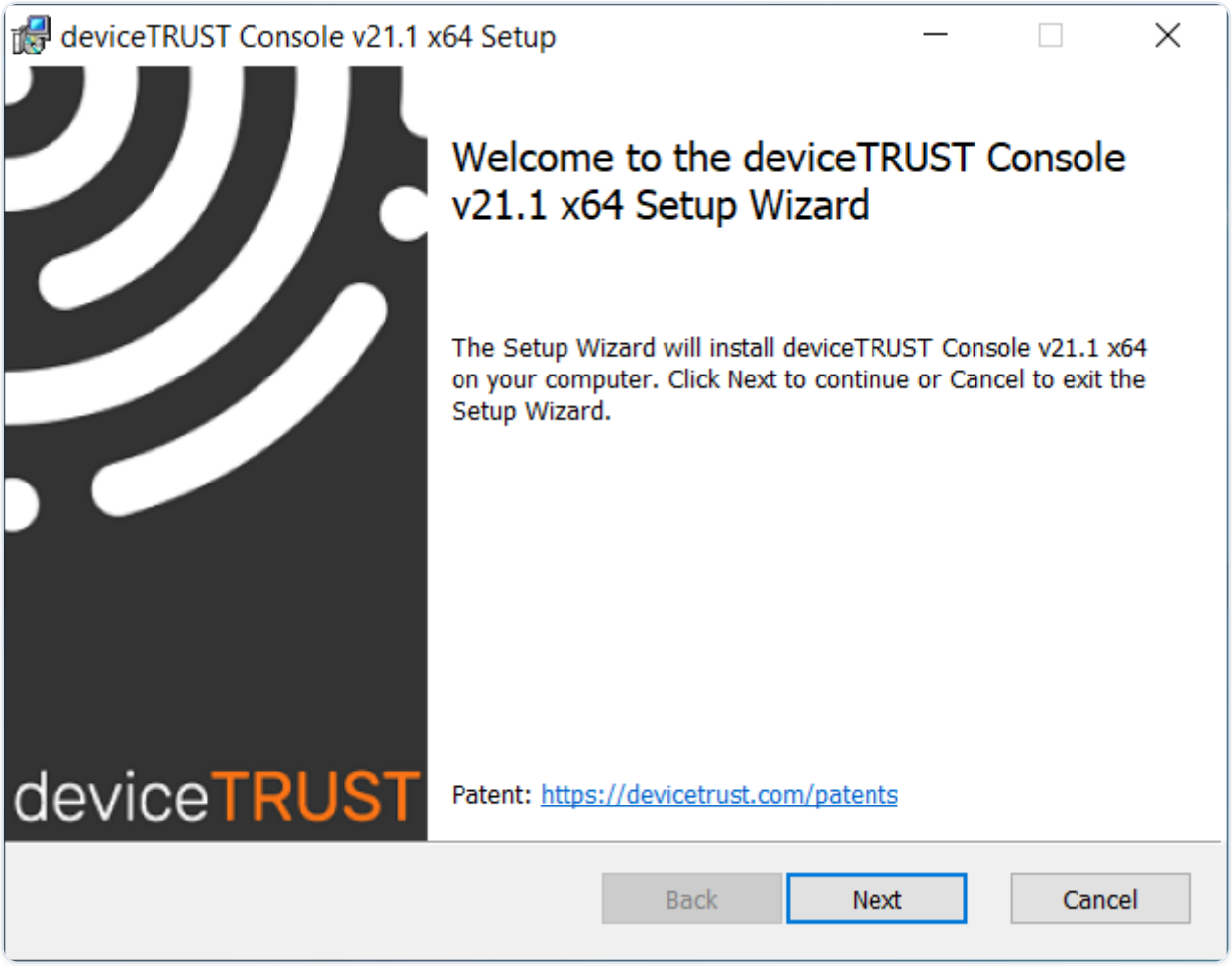
COMPONENT	COMMANDLINE	
dtagent-x64-release-x.x.x.x.msi	The deviceTRUST 64-bit Agent installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters `MSIEXEC.EXE /I DTAGENT-X64-RELEASE-X.X.X.X.MSI /PASSIVE /FORCERESTART`	
dtagent-x86-release-x.x.x.x.msi	The deviceTRUST 32-bit Agent installer file can be customized by common Microsoft Windows Installer parameters. An unattended	

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

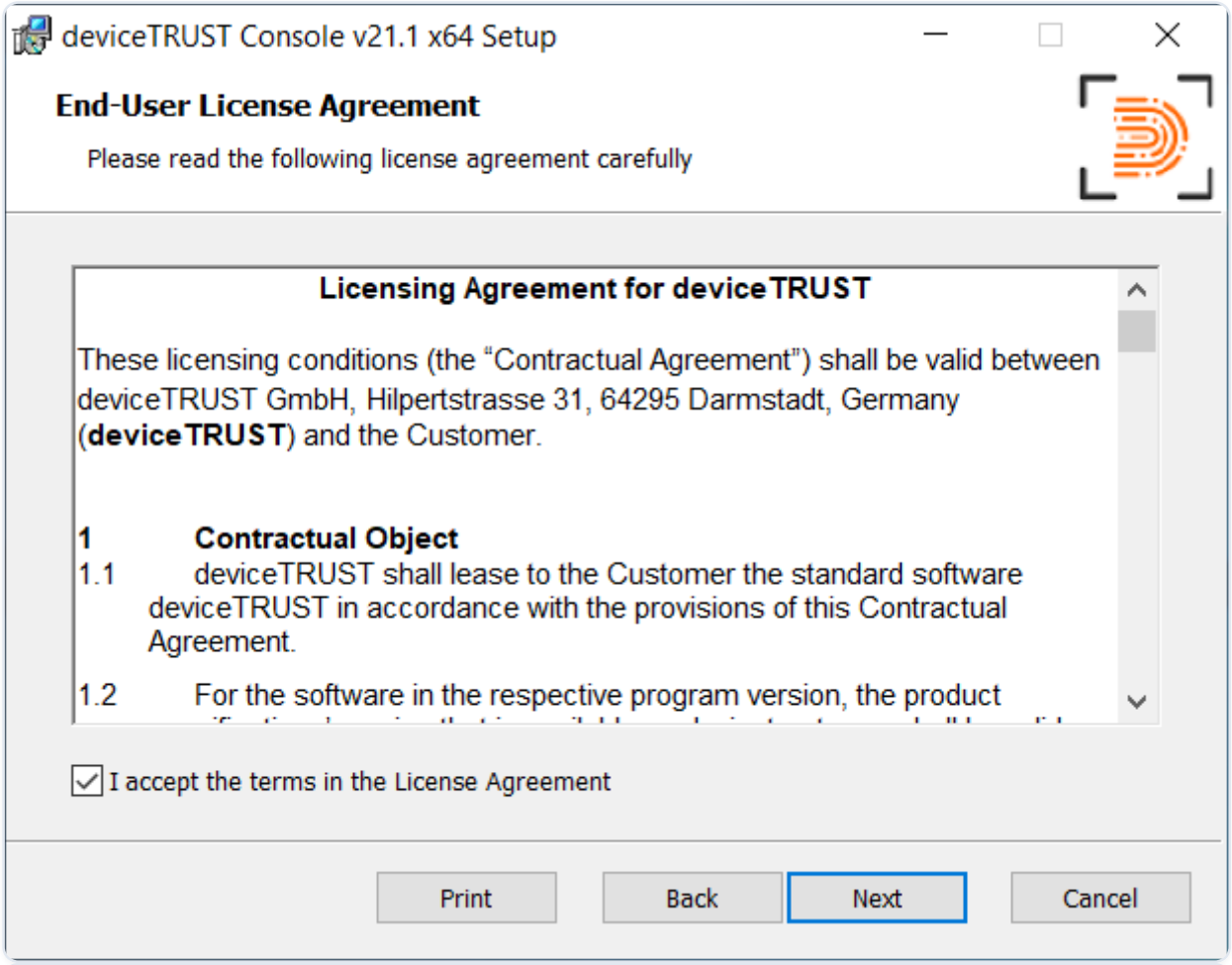
COMPONENT	COMMANDLINE	
	installation can be achieved with the following parameters `MSIEXEC.EXE /I DTAGENT-X86-RELEASE-X.X.X.X.MSI /PASSIVE /FORCERESTART`	

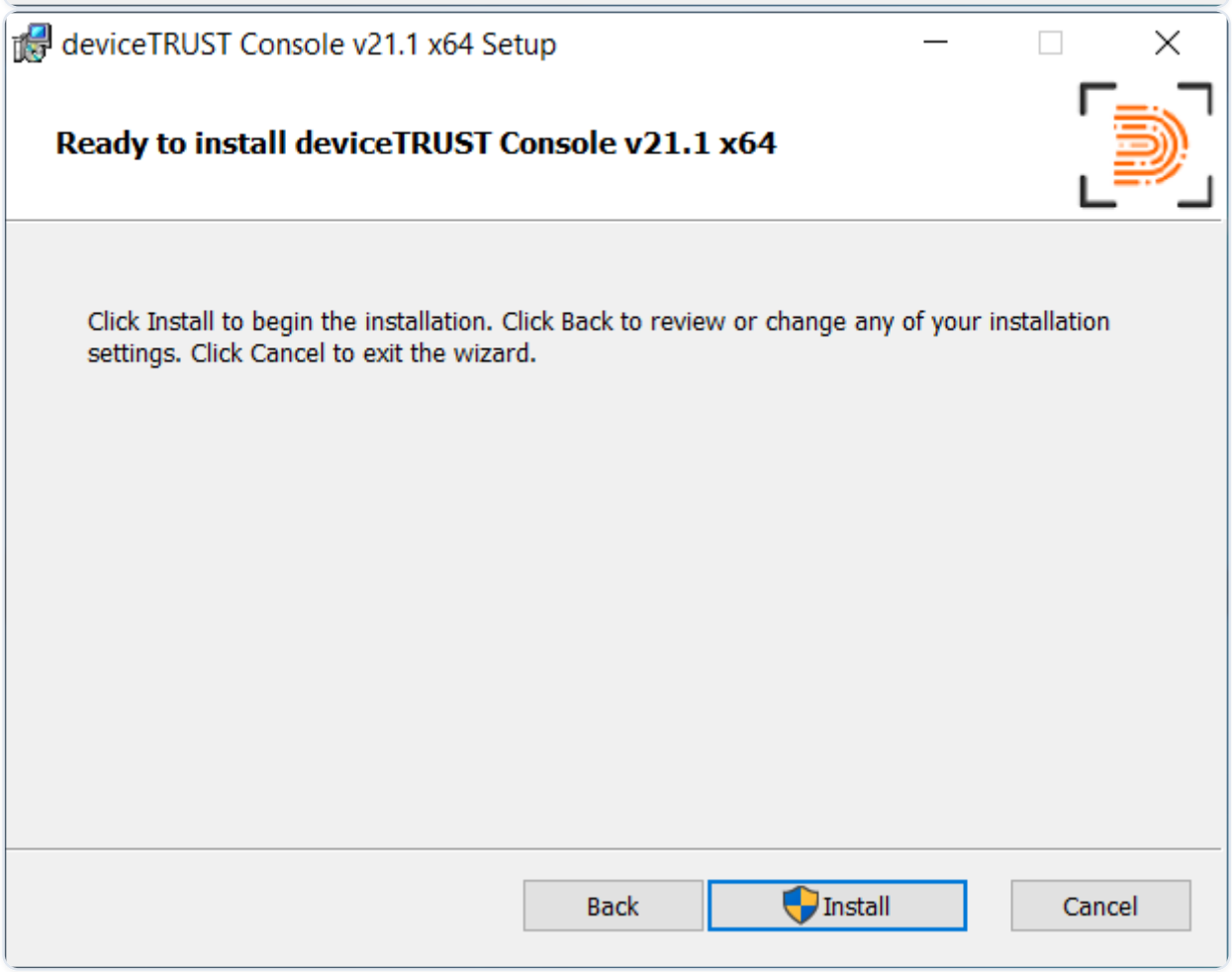
Installing the deviceTRUST® Console

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

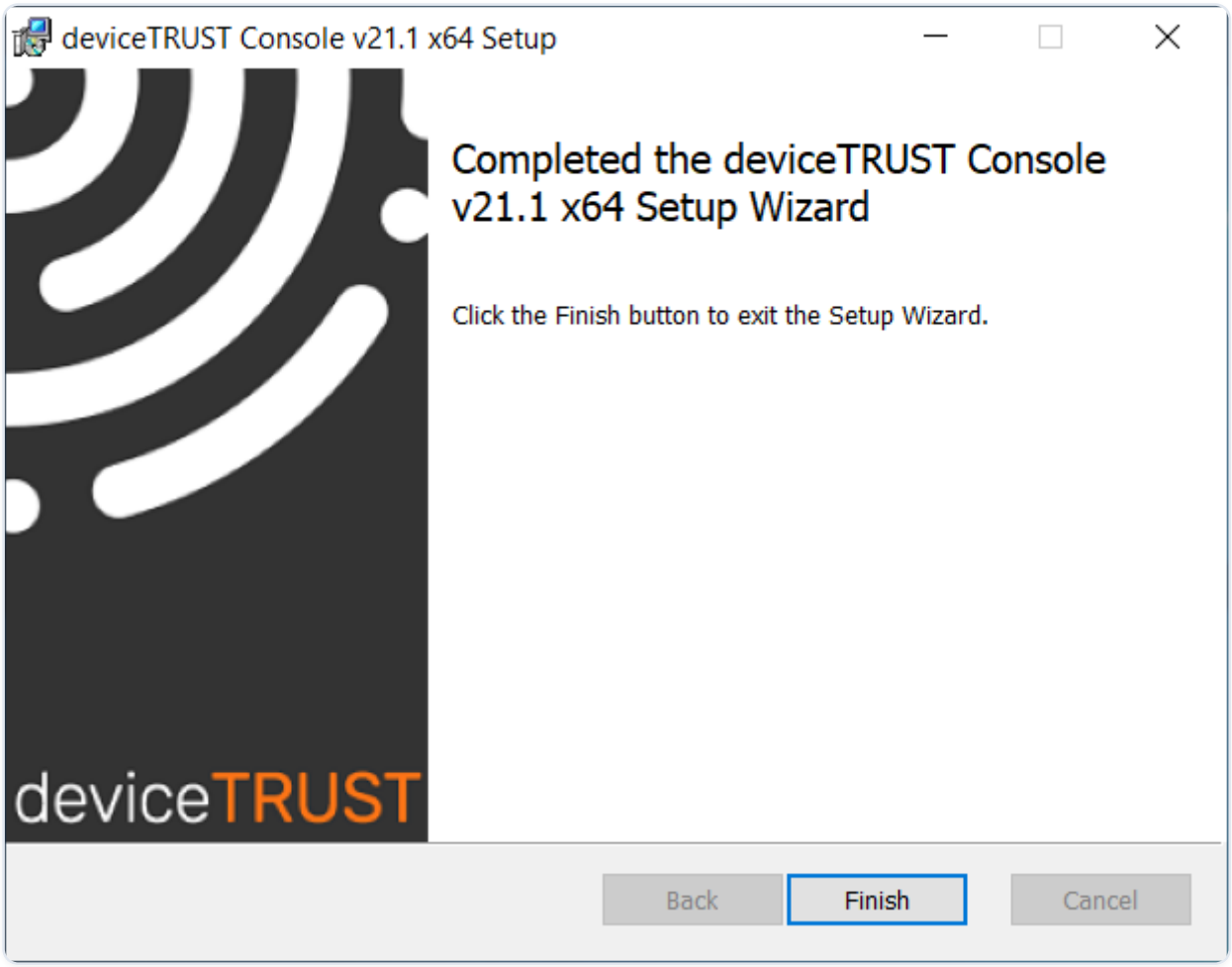


© 1997–2026 Citrix Systems, Inc. All rights reserved.





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



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 64-bit Console installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters

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

COMPONENT	COMMANDLINE	
	`MSIEXEC.EXE /I DTCONSOLE-X64-RELEASE-X.X.X.X.MSI /PASSIVE`	
dtconsole-x86-release-x.x.x.x.msi	The deviceTRUST 32-bit 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-X86-RELEASE-X.X.X.X.MSI /PASSIVE`	

Installing the deviceTRUST® Client Extension

TABLE OF CONTENTS

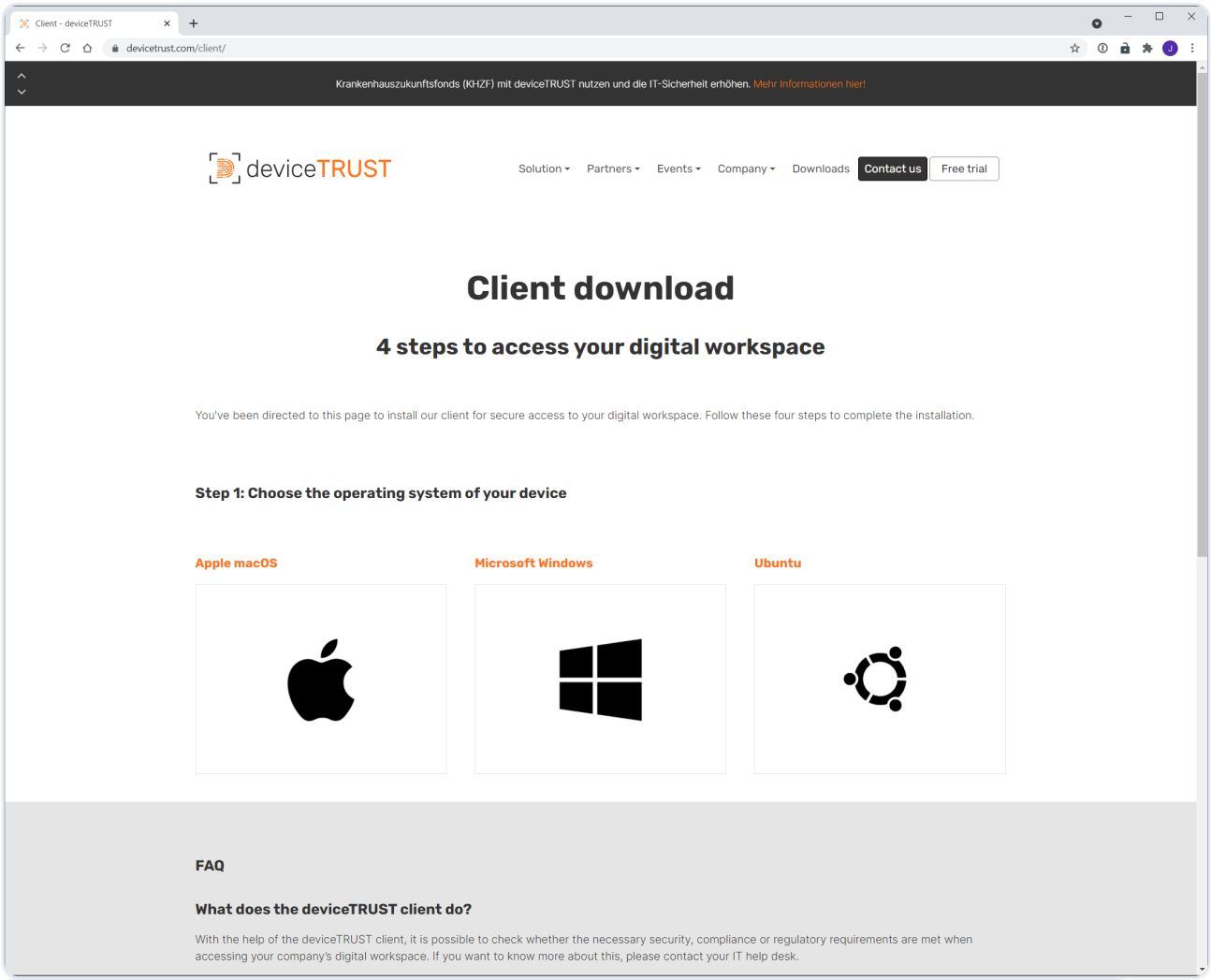
- Microsoft Windows
- Apple macOS
- Ubuntu
- IGEL OS
- Unicon eLux

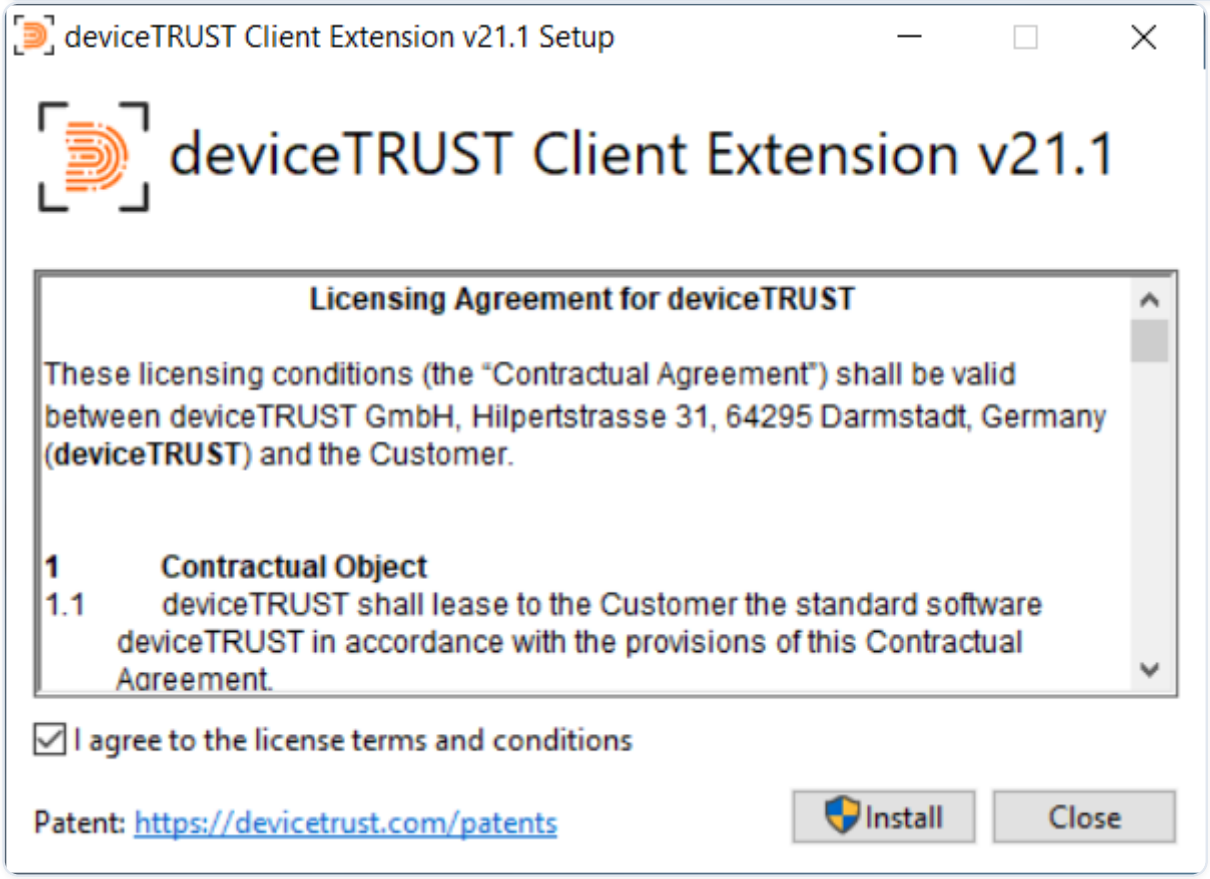
Client Extension installation on Microsoft Windows devices

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

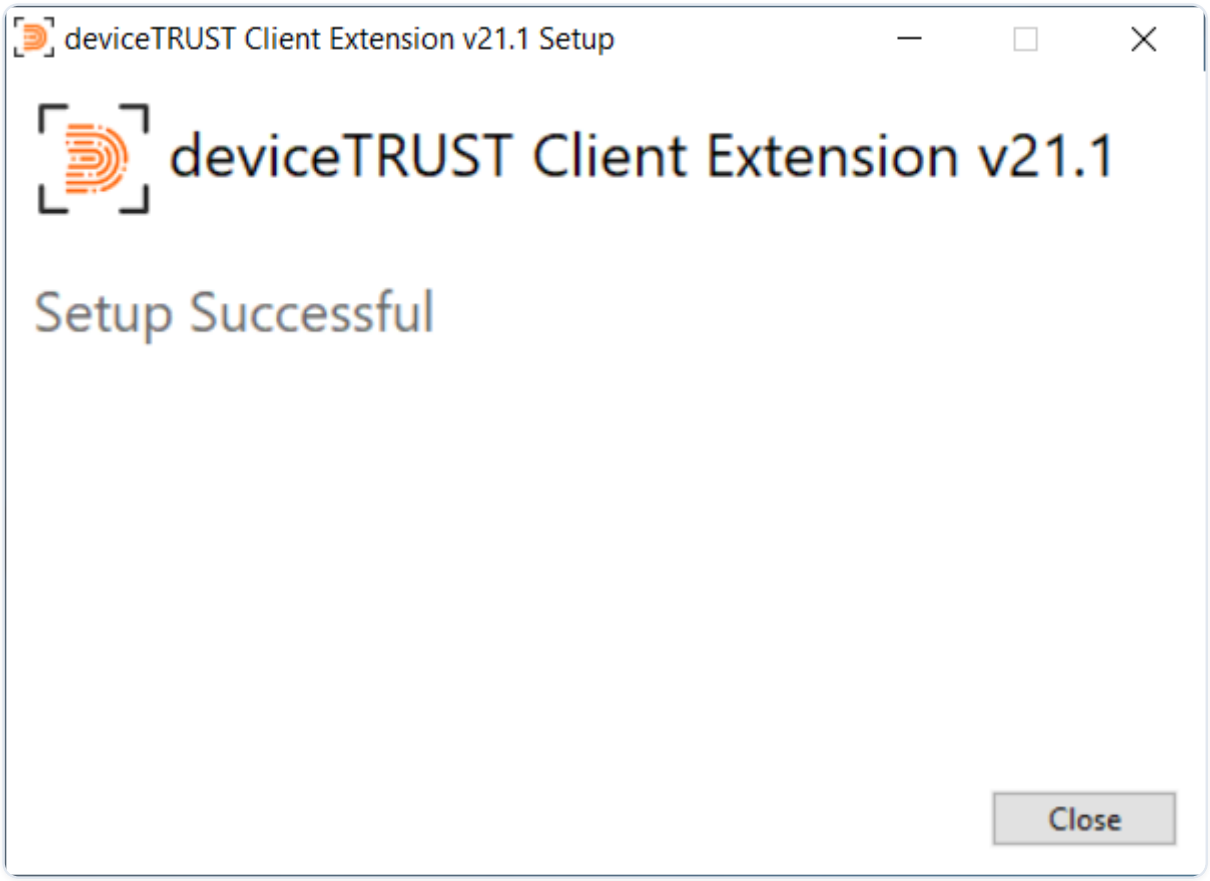
The deviceTRUST® Client Extension for unmanaged Microsoft Windows devices supports an auto-update functionality. If a newer deviceTRUST Client Extension is available, the administrator of the remoting and DaaS environment can enforce a transparent update installation of the local deviceTRUST Client Extension.

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





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



IMPORTANT

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

Client Extension Installation Command Line Options

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

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

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

NOTE:

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

Unattended Installation

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

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

Active Setup Components

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

deviceTRUST Channel Registration 64-bit component

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

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

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

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)

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

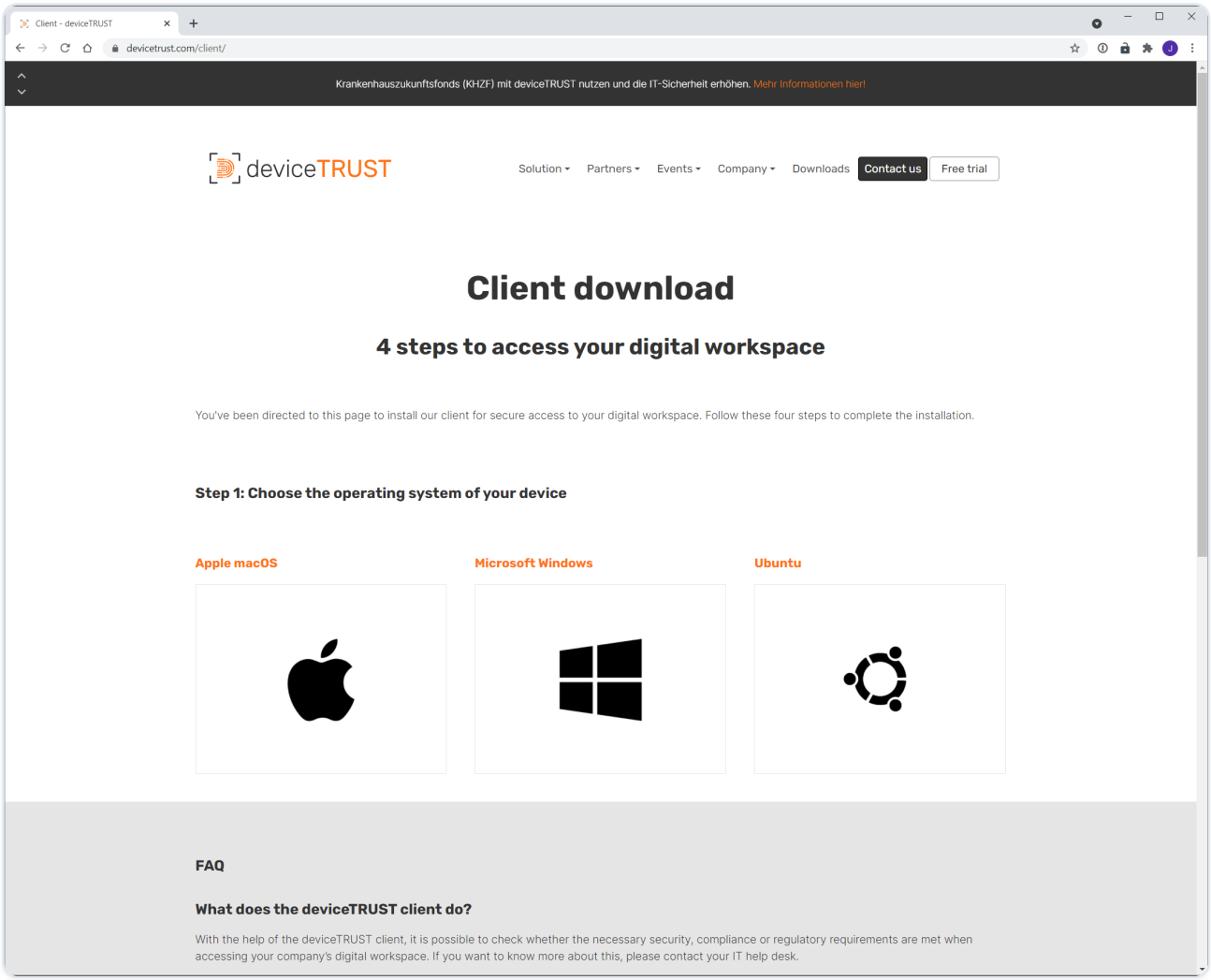
Registry Key: `HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{3d65bd68-a307-4d64-af9c-17bc9c4b36e3}`

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.

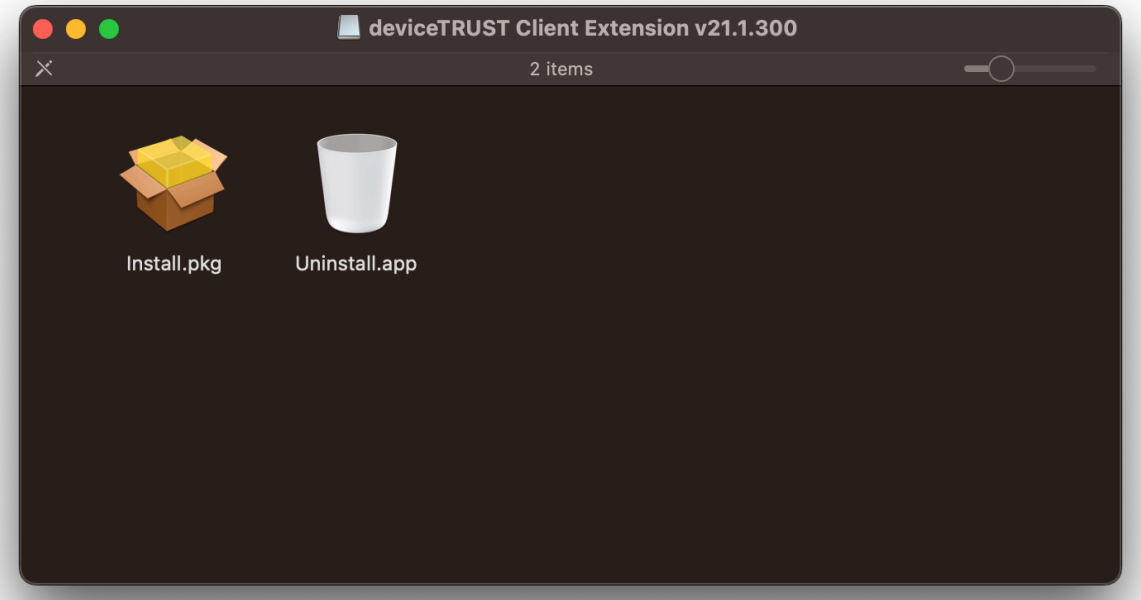
Client installation on Apple macOS devices

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

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

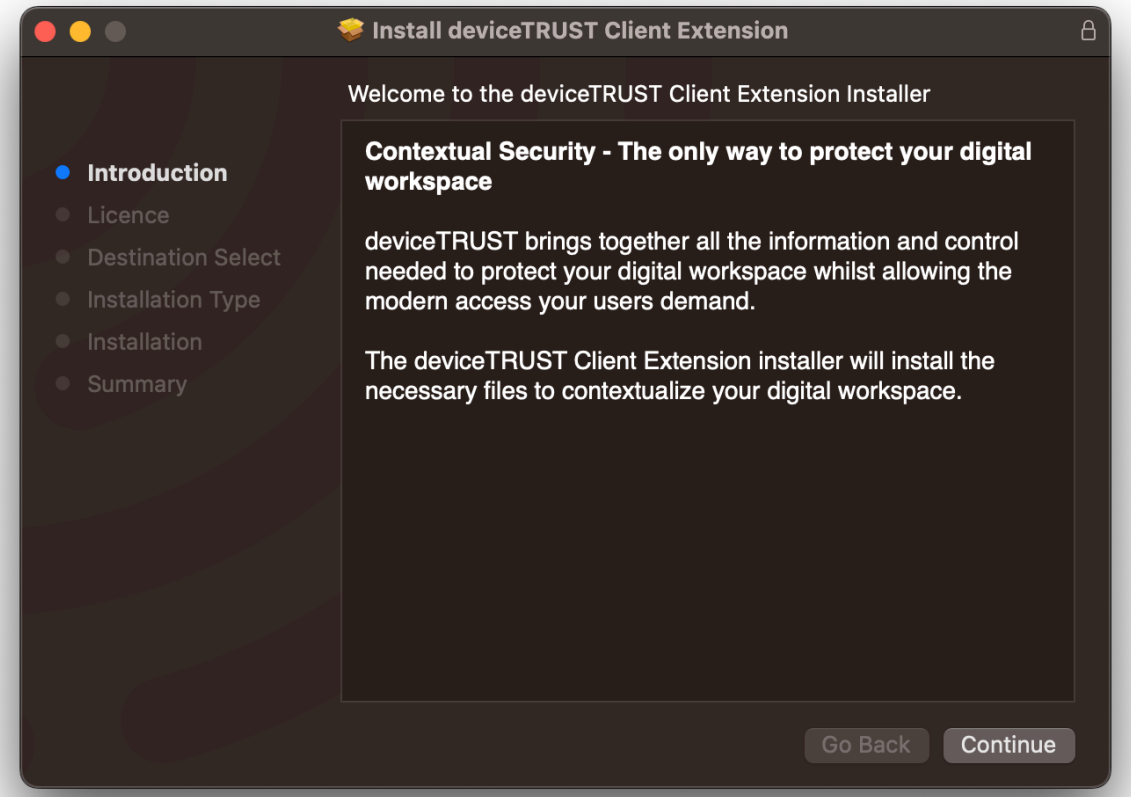


To access the installer, double click on the downloaded 'dtclient-extension-macos-universal-release-W.X.Y.Z.dmg' file.



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

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

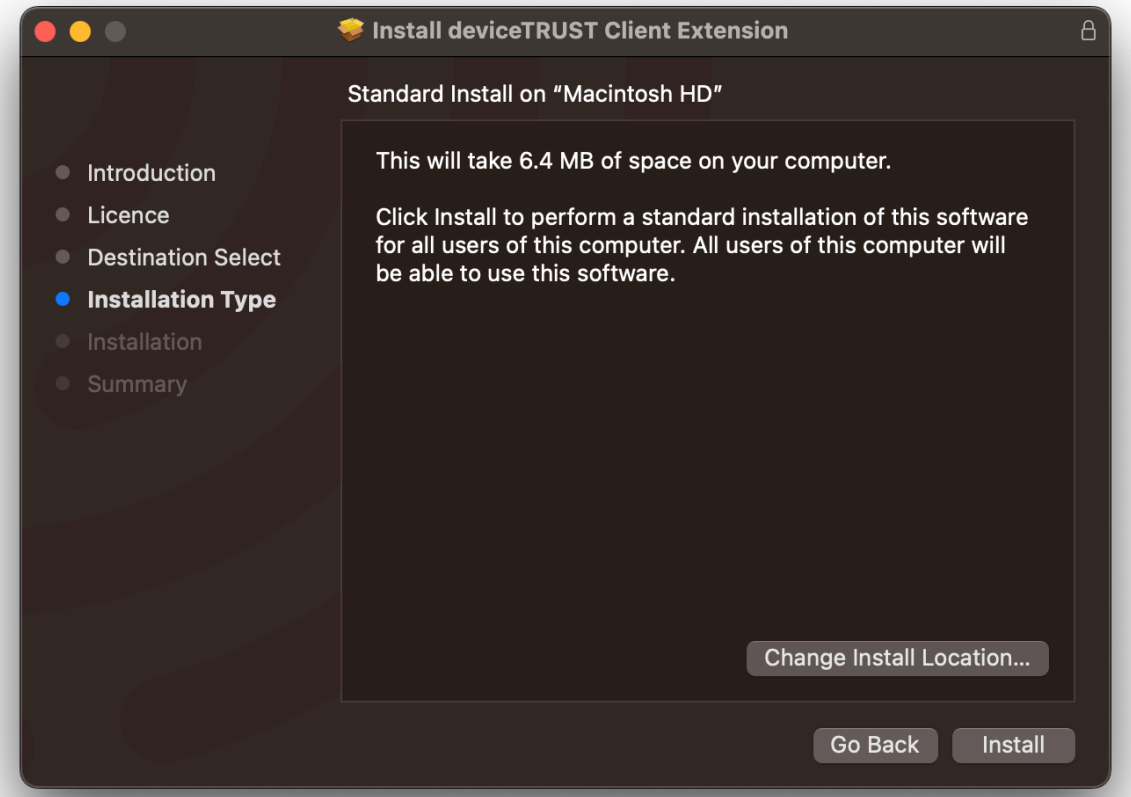


Continue through the installation steps until complete.

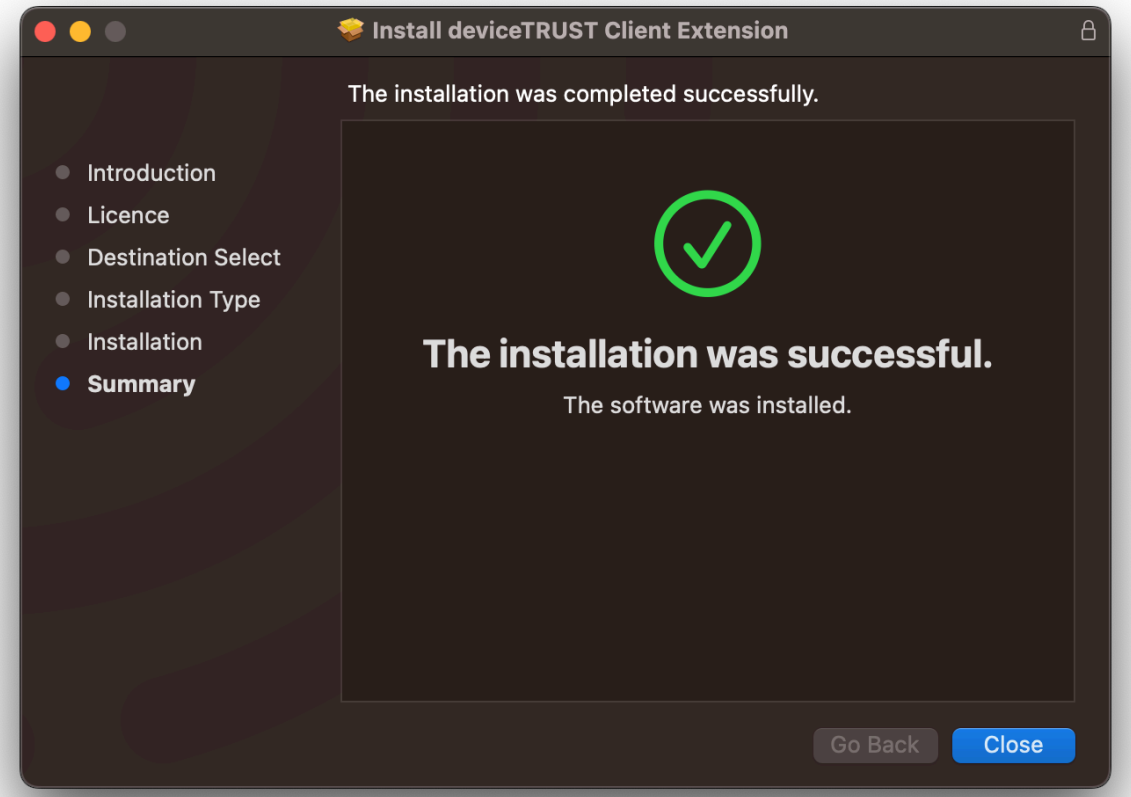
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



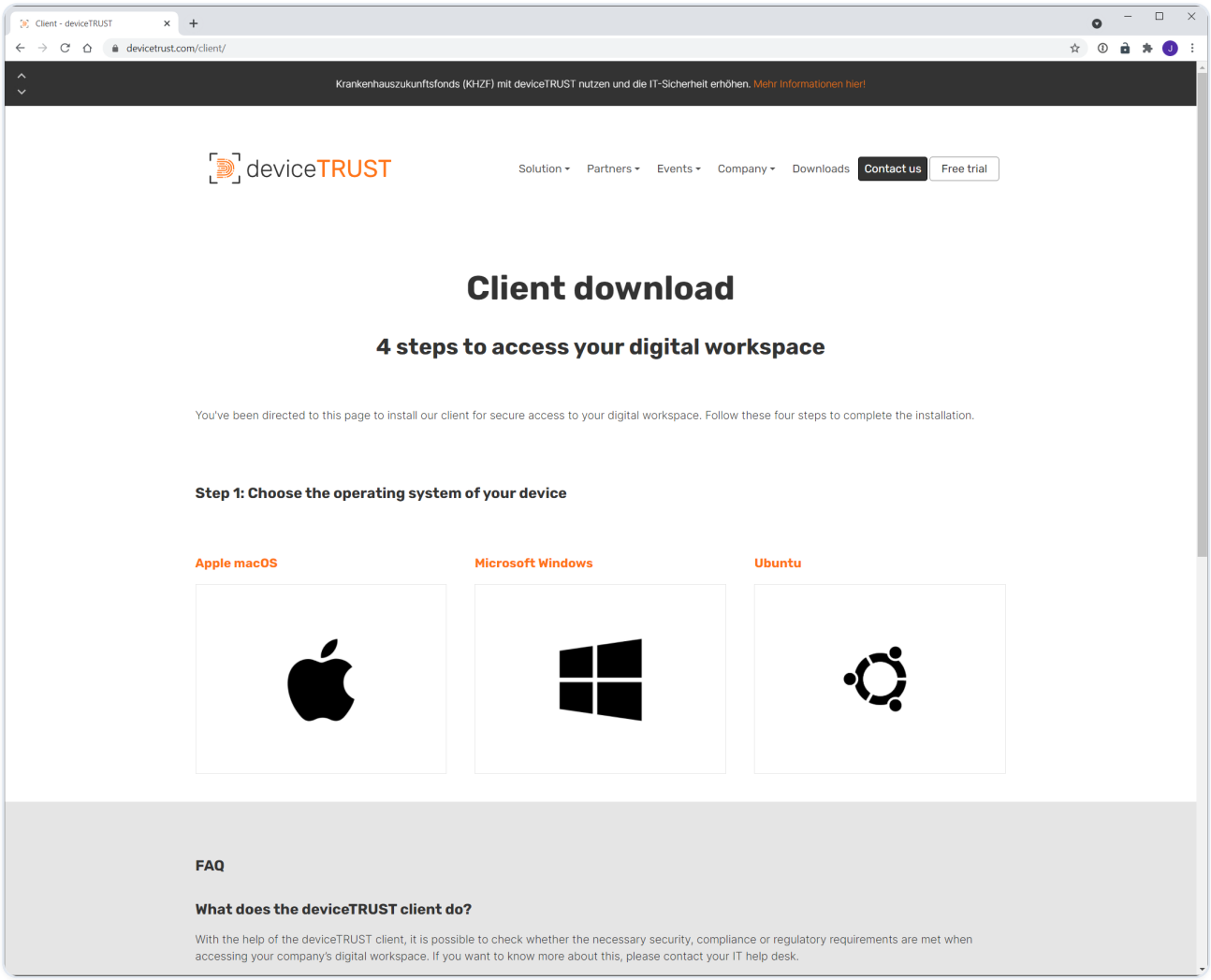
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Client installation on Ubuntu devices

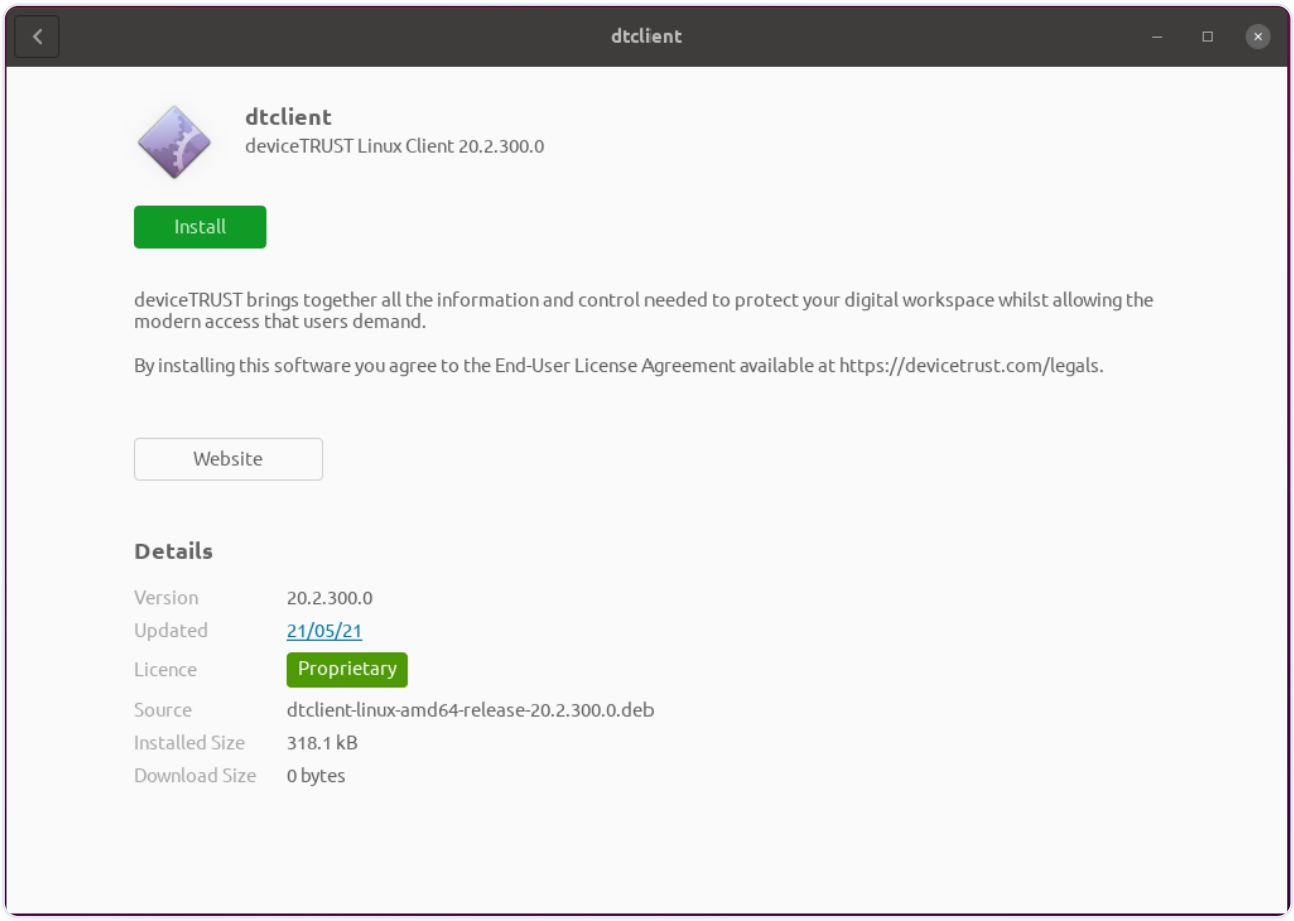
The deviceTRUST Ubuntu Client can be downloaded by following the steps on the deviceTRUST Client Extension Download page.

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



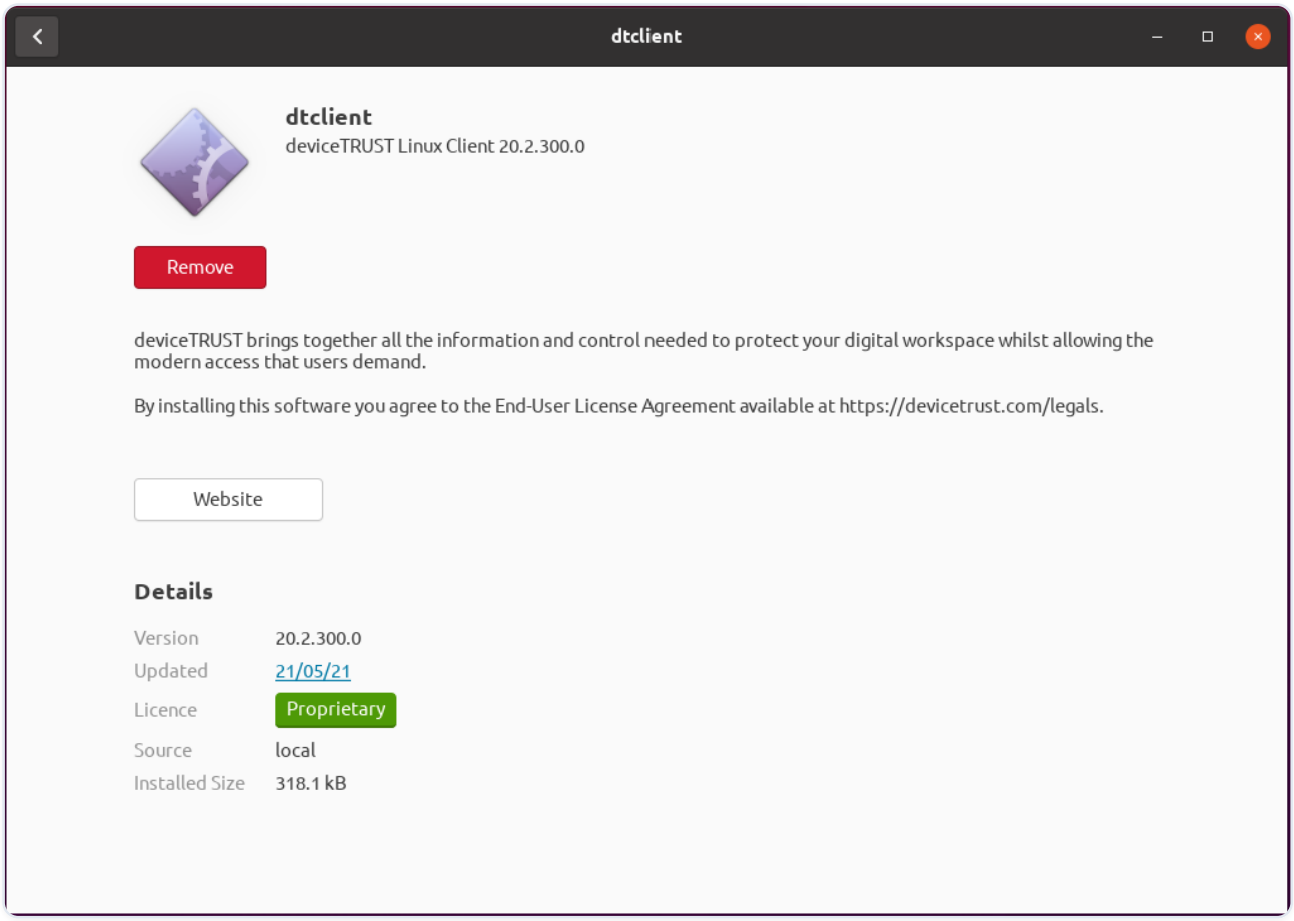
To access the installer, double click on the downloaded 'dtclient-linux-amd64-release-W.X.Y.Z.deb' file.

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



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

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



Client installation on IGEL OS devices

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

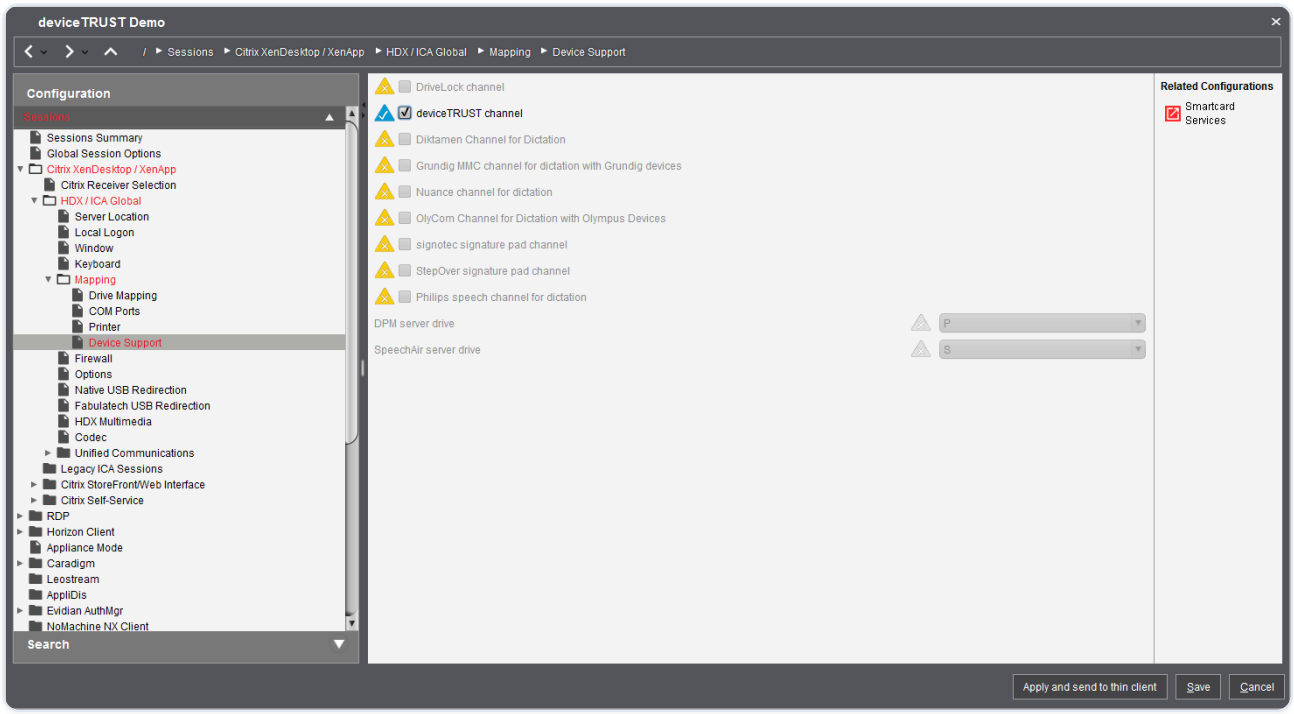
NOTE:

- To enable deviceTRUST® within the IGEL OS you can use the IGEL Universal Management Suite (UMS) or the local administrative interface.
- IGEL devices must be restarted after enabling deviceTRUST.

Enable deviceTRUST for Citrix Independent Computing Architecture (ICA®)

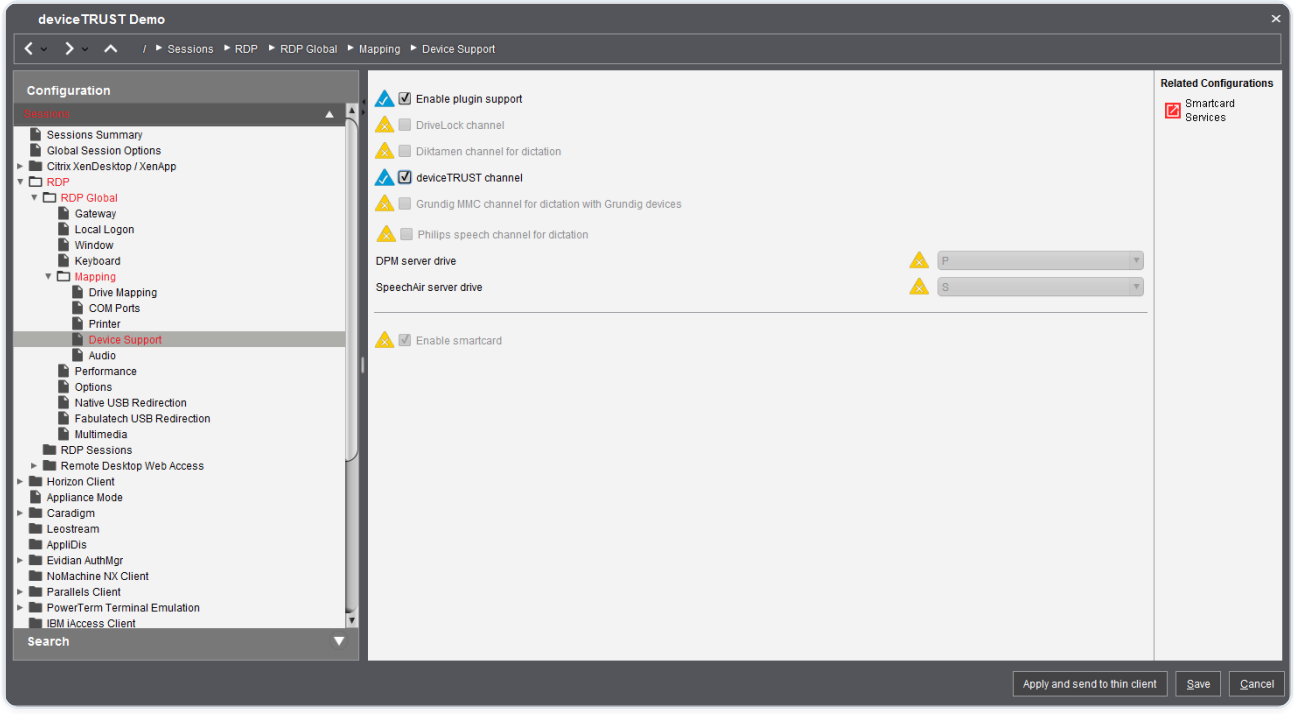
Open the target profile (local or through the UMS) and navigate to SESSIONS\CITRIX XENDESKTOP / XENAPP\HDX / ICA GLOBAL\MAPPING and activate the DEVICETRUST CHANNEL option.

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



Enable deviceTRUST for Microsoft Remote Desktop Protocol (RDP)

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



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

Client installation on Unicon™ eLux devices

Import the deviceTRUST® certificate chain

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

NOTE

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

Within ELIAS:

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

Within the Scout console:

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

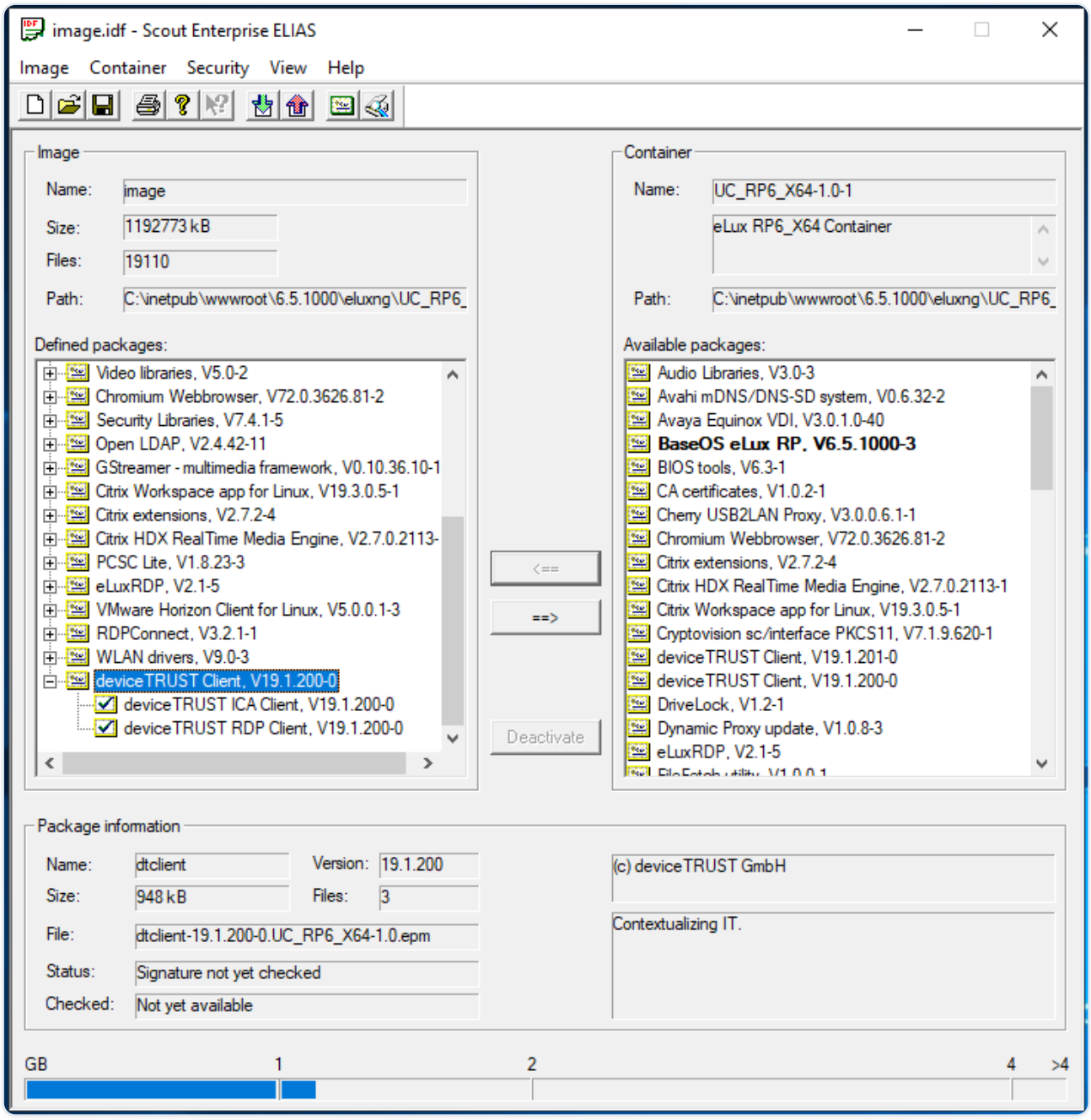
Install the package

Within ELIAS:

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

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

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

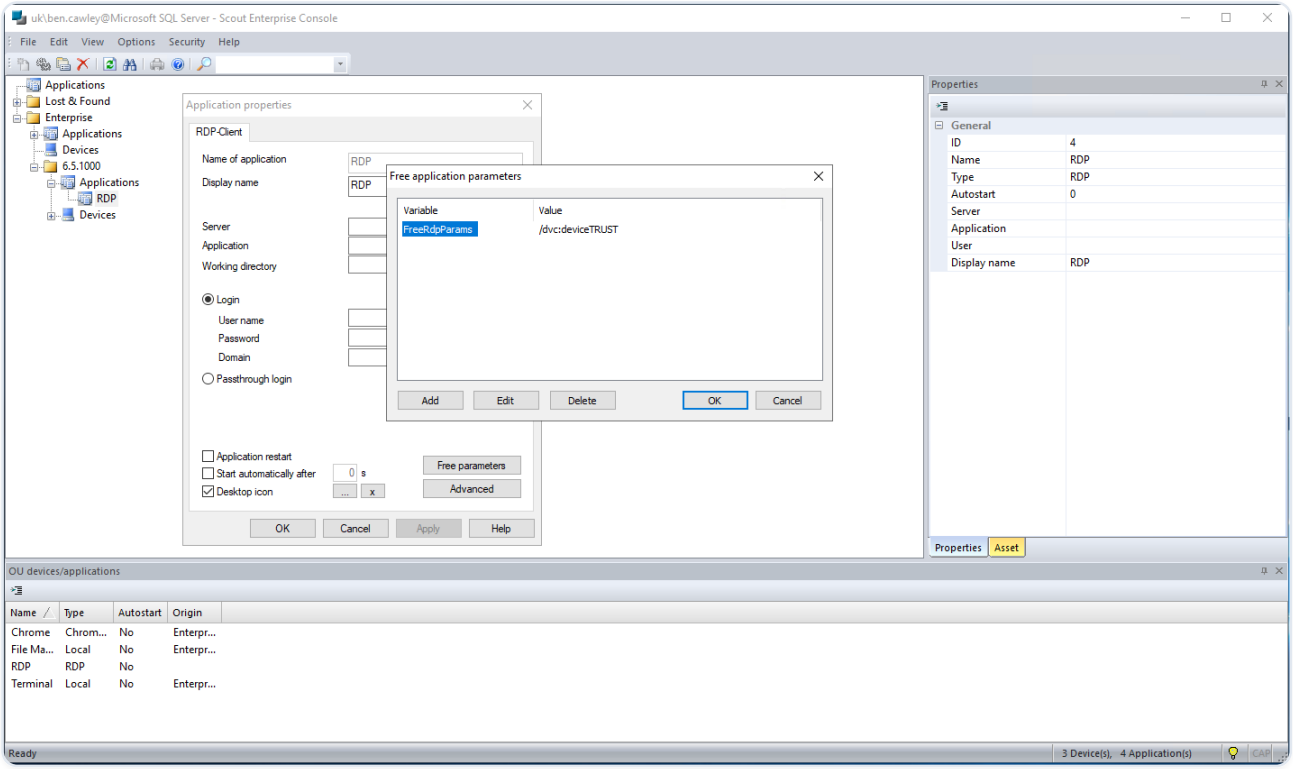


Within the Scout console:

- Update your eLux devices.

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

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



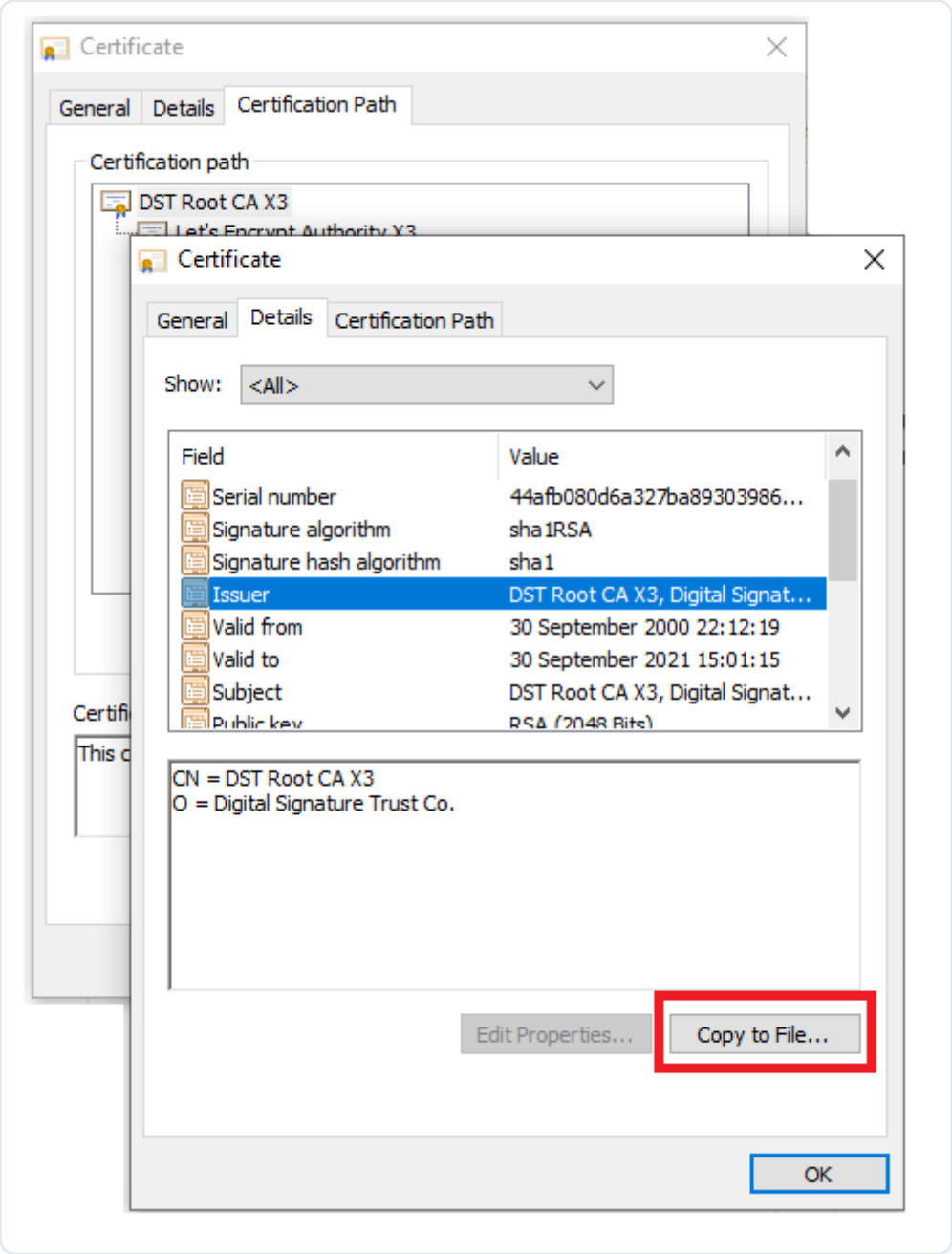
Next time you connect using ICA® or RDP to a server with a licensed deviceTRUST Host, the properties of your eLux device will be available within your virtual session.

Deploy the ripe.stat root certificate

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

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

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

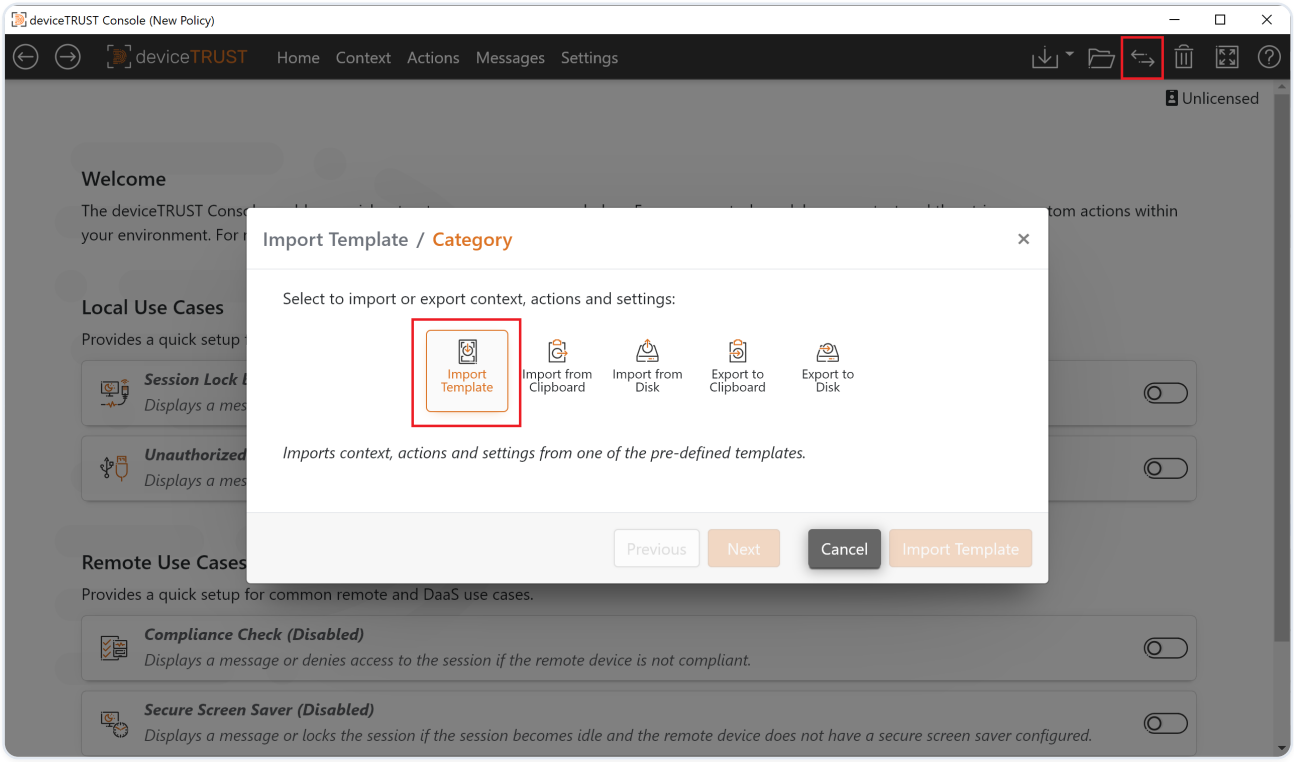


Within the Scout console select 'Advanced device configuration\Files' on the device container, import the certificate and deploy to your device certificate store location.

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

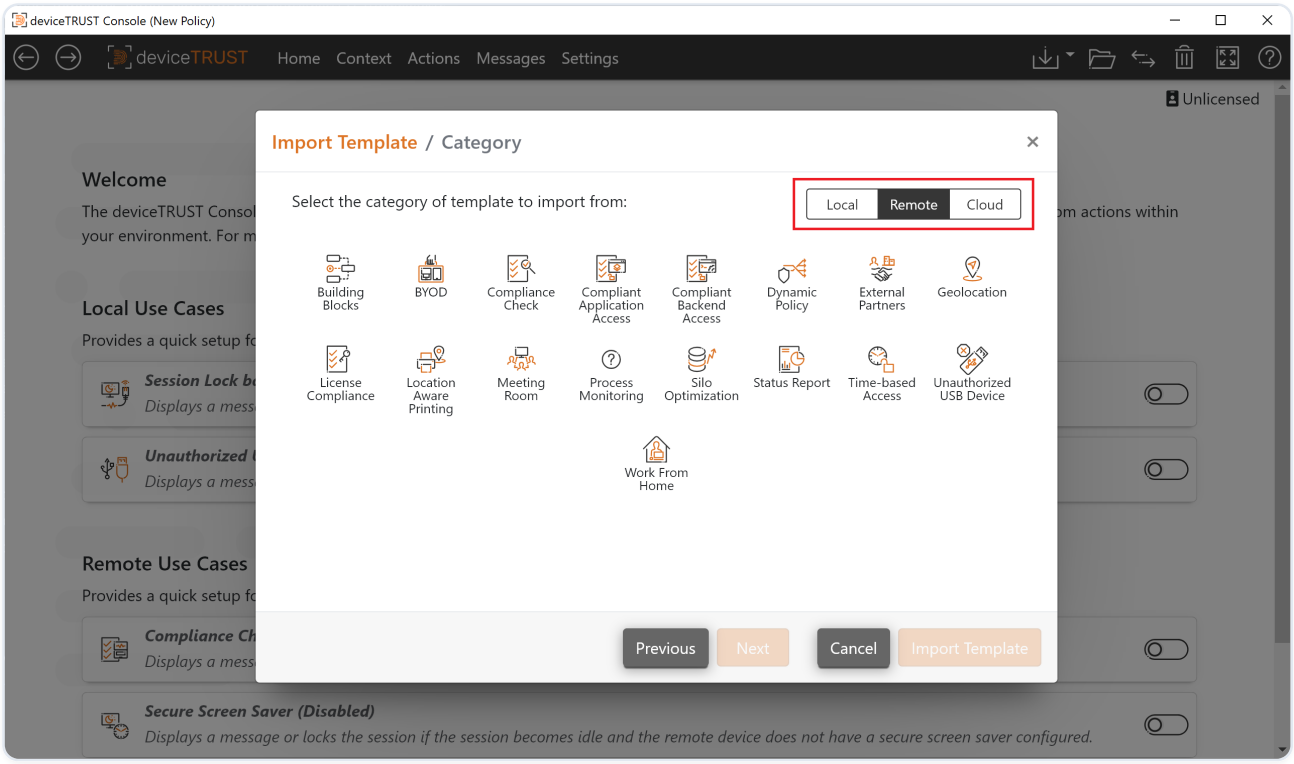
Templates

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`.



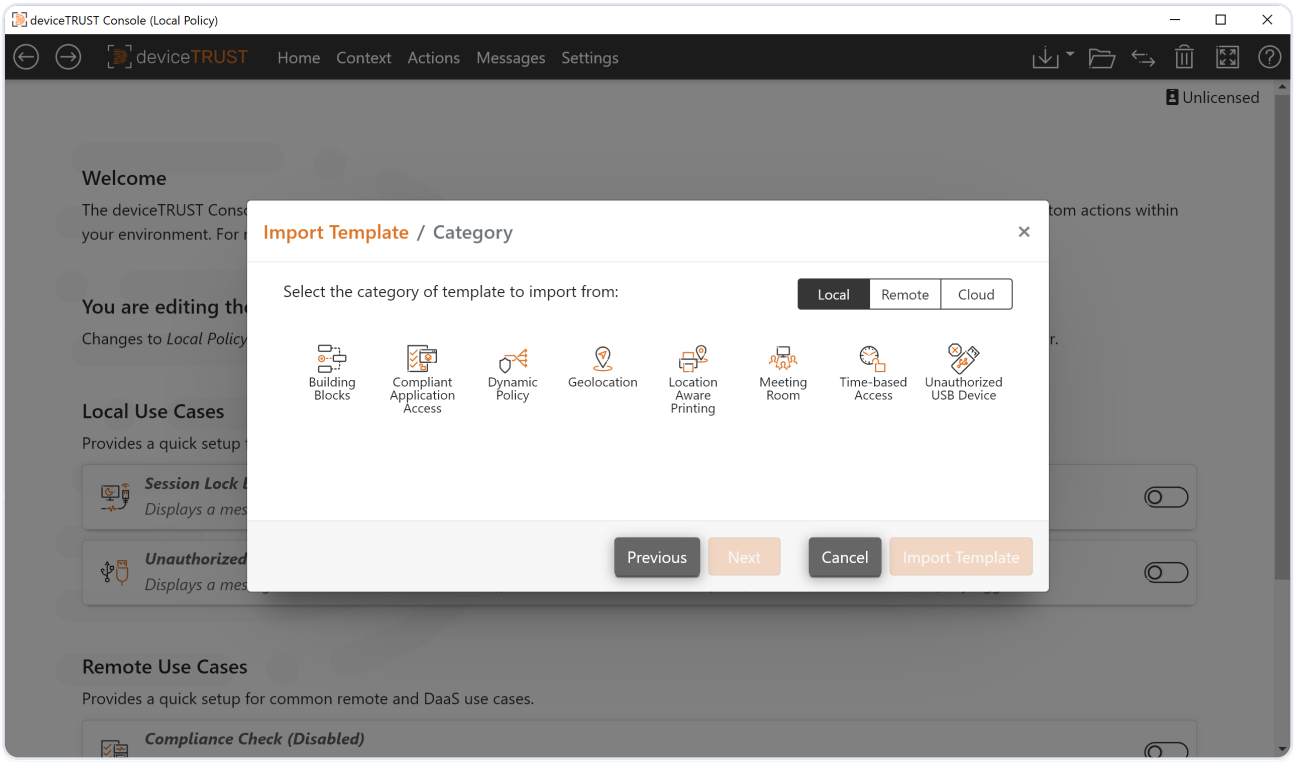
The deviceTRUST use cases are summarized in the following categories for each target platform. Use the filter to select the desired target platform.

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



Local Templates

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



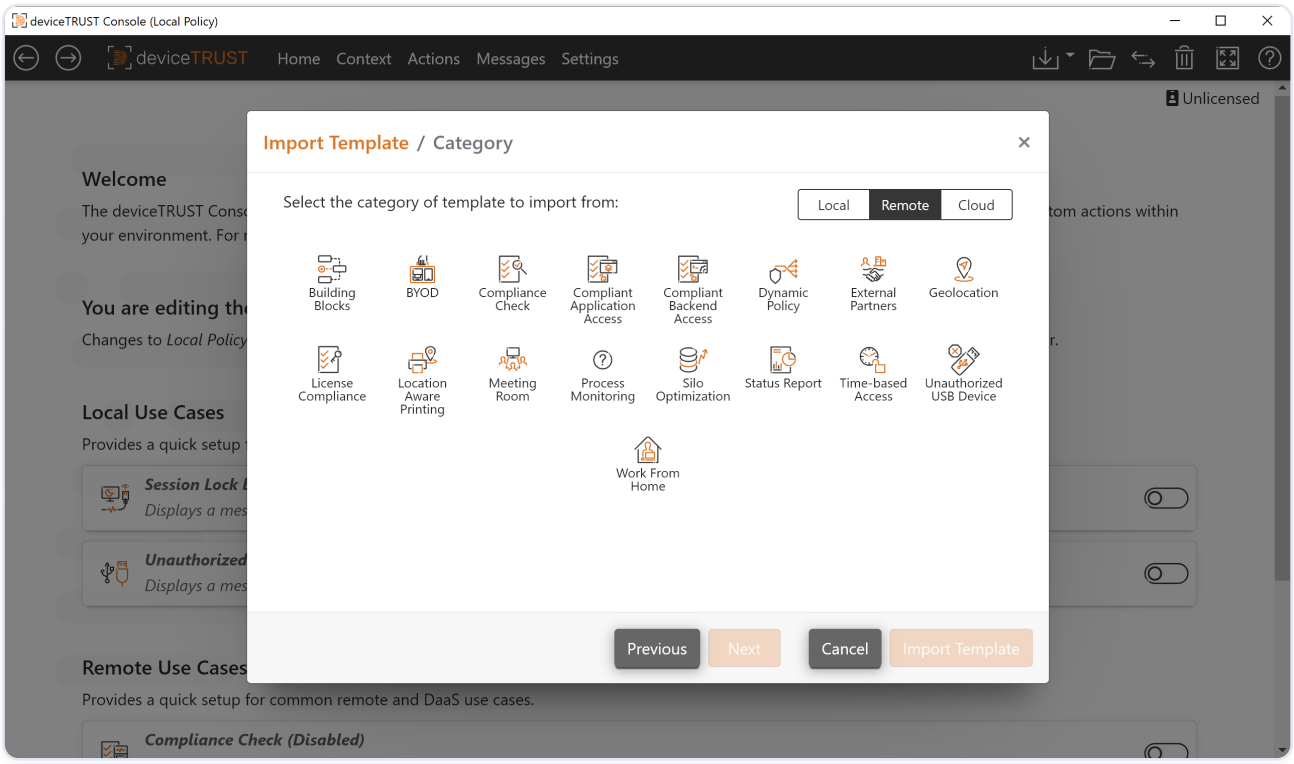
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- Meeting Room - Controls an idle period for devices based upon whether the device is placed within a meeting room.
- 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.
- Meeting Room - Controls an idle period for devices based upon whether the device is placed within a meeting room.
- 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.

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

Cloud Templates

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

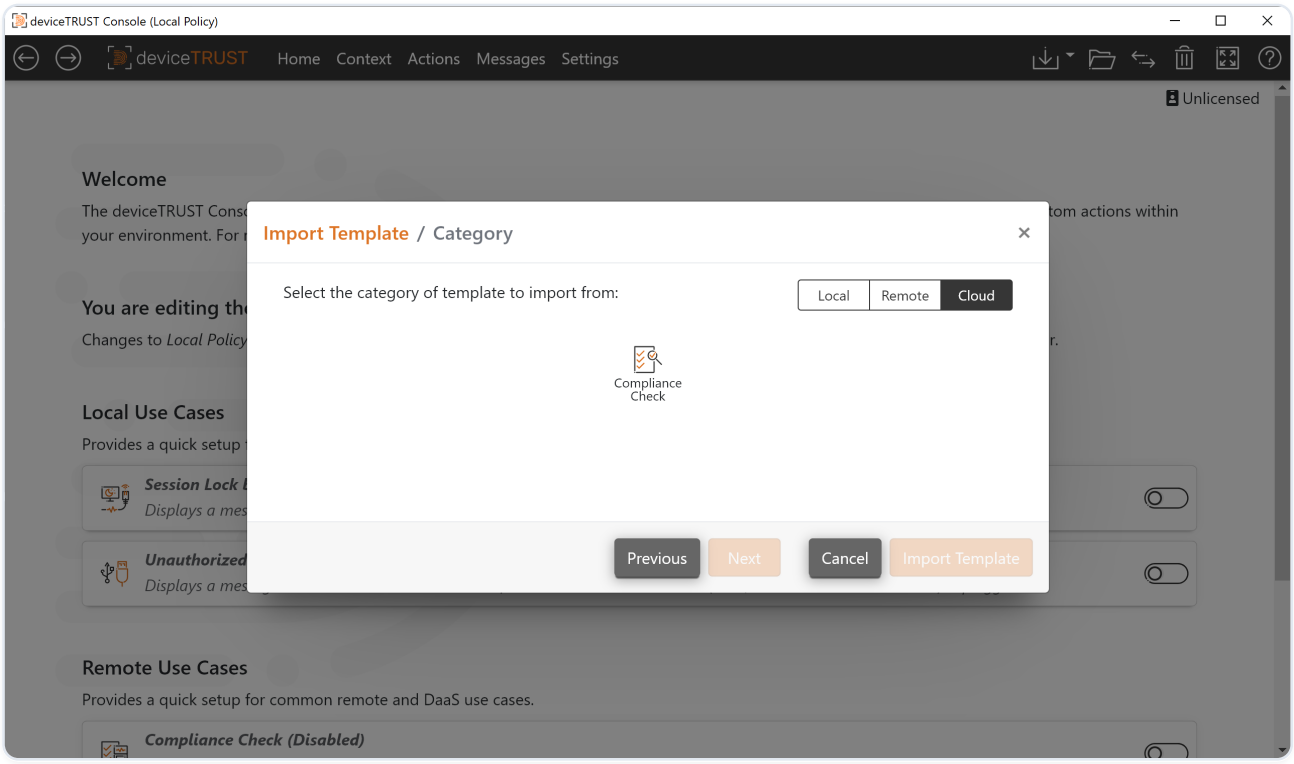


TABLE OF CONTENTS

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.

Reporting

TABLE OF CONTENTS

- Splunk Dashboards
- ELK Stack Dashboards

Splunk Dashboards

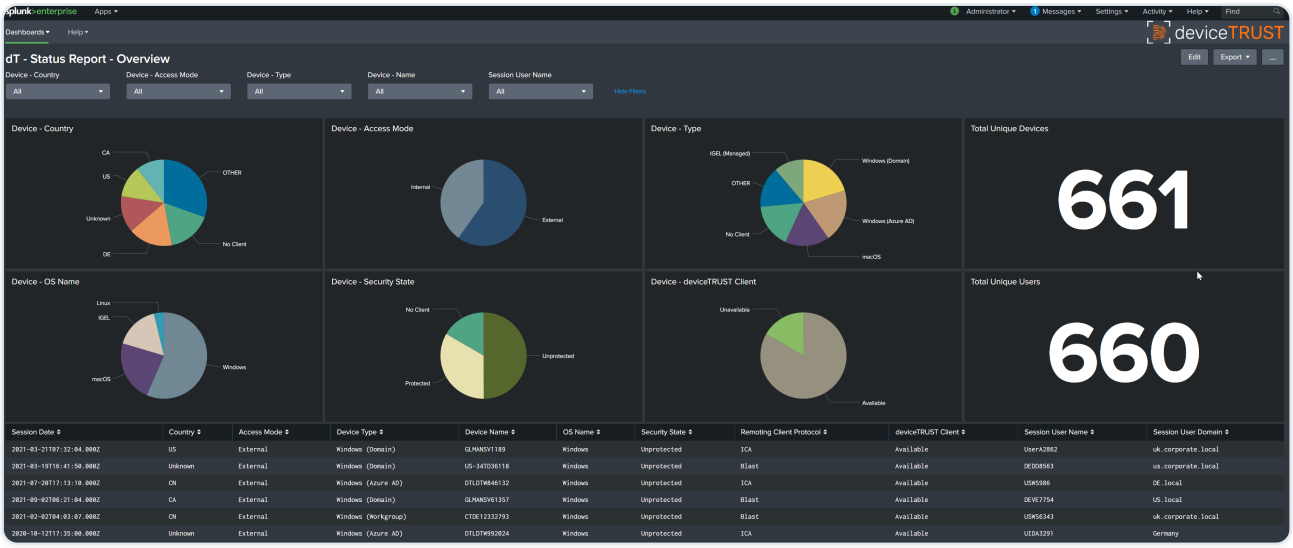
deviceTRUST® includes a Splunk app to easily create a Splunk dashboard to monitor the contextual status of your remoting and DaaS environment.

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



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

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



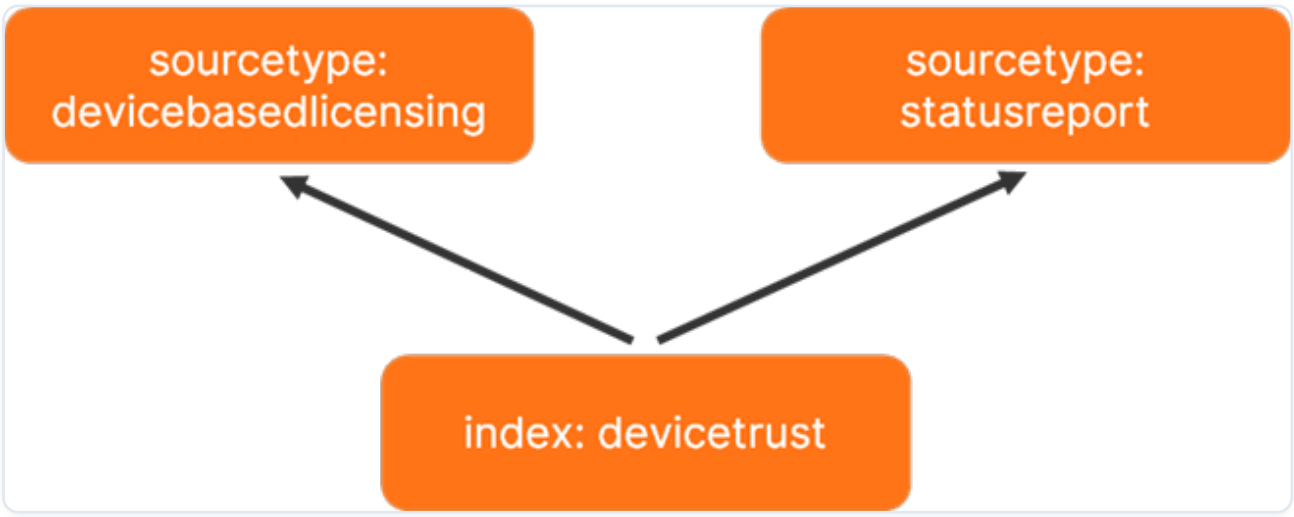
The following steps will be performed:

Step 1: Creating the Splunk Index

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

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

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



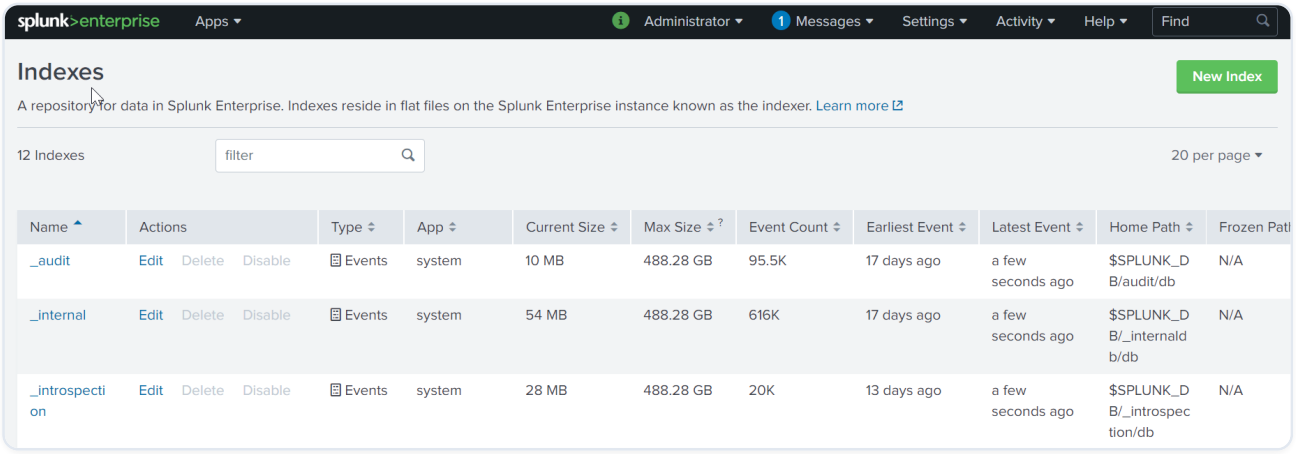
You can either create the index `devicetrust` manually or by importing our prepared app `dt_index`.

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

Step 1.1: Manually creating the Splunk Index

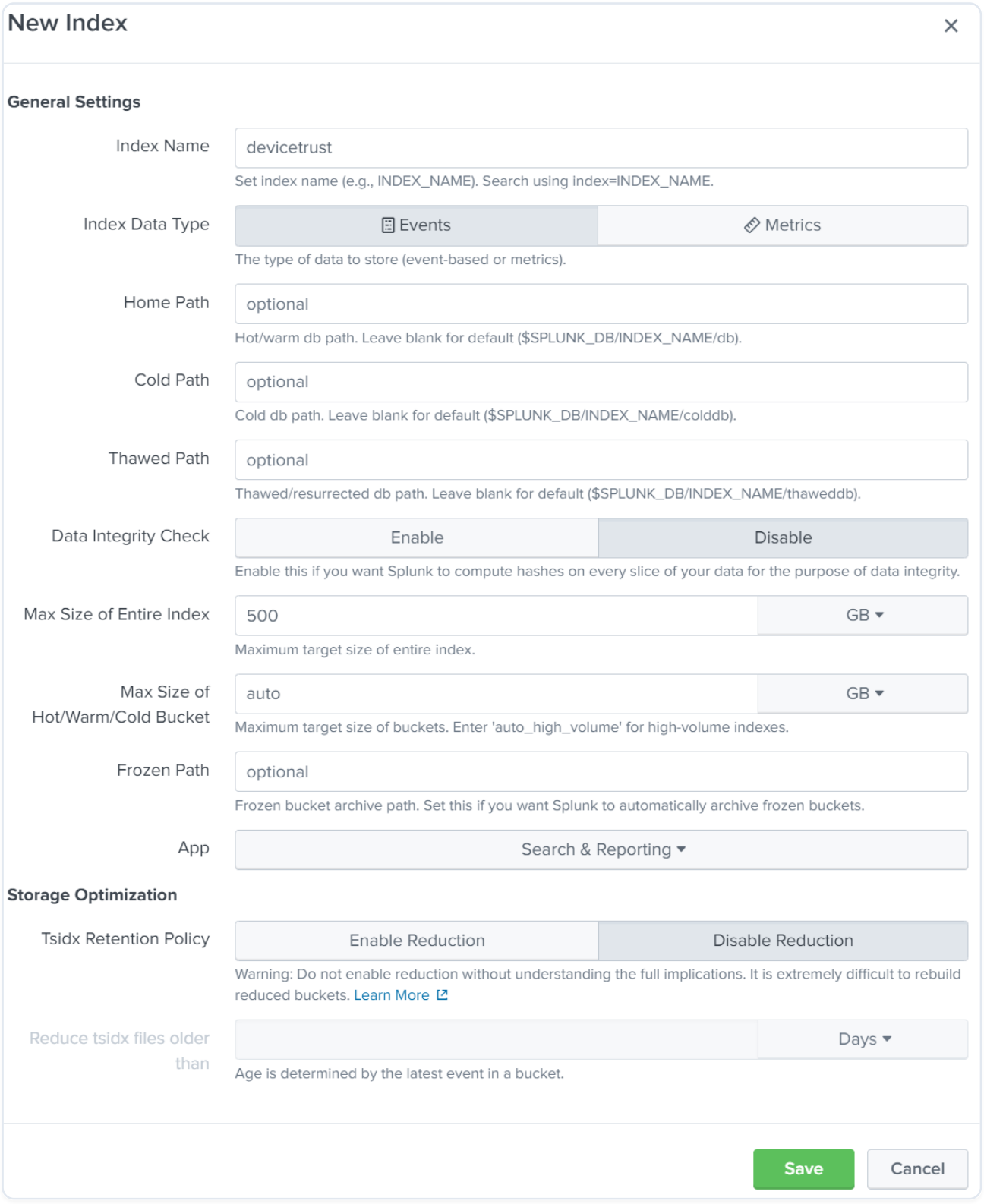
Implementing the index manually does not require any special configuration.

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



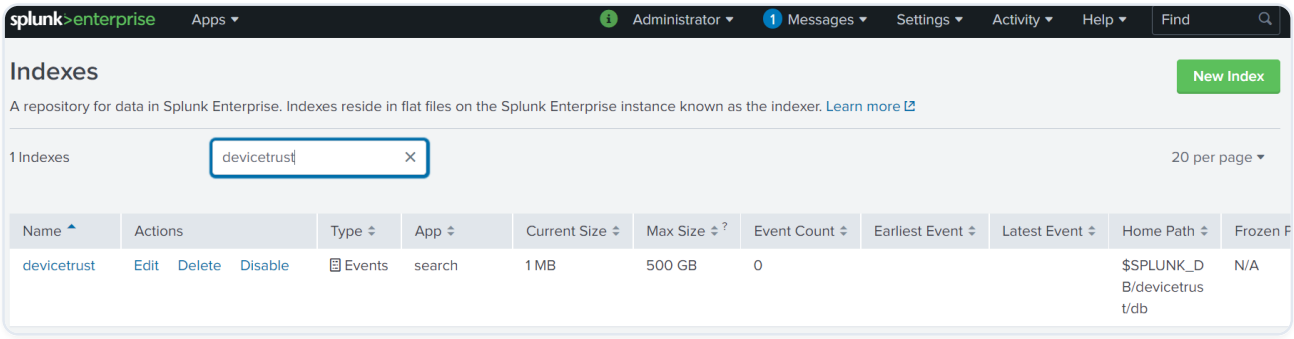
- Set the name to `devicetrust` and all other options are optional.

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



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

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



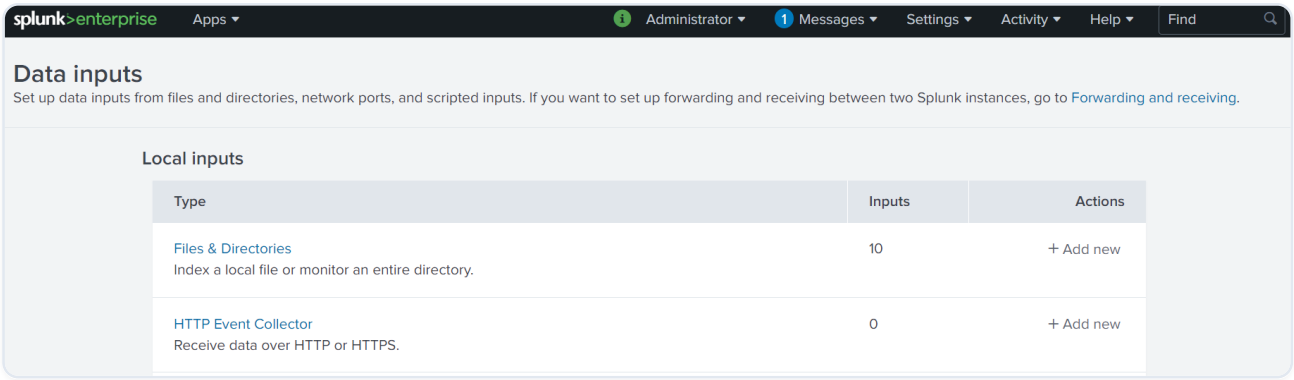
Step 1.2: Creating the Splunk Index by installing the app

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

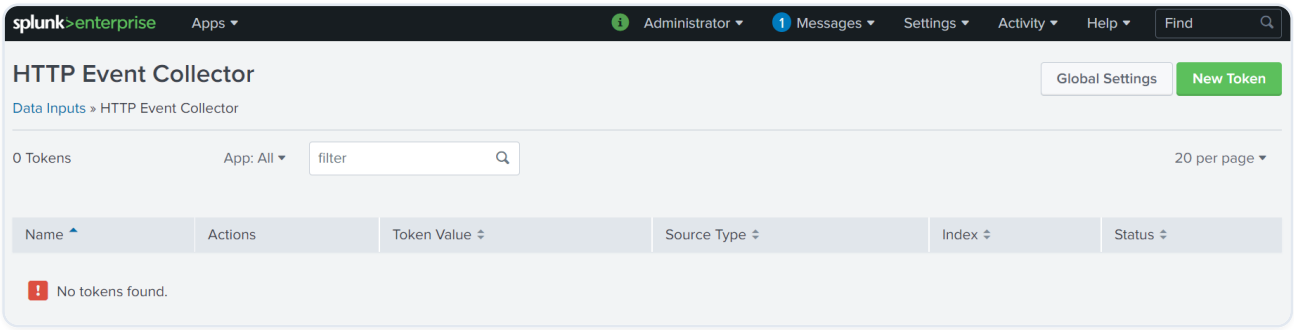
Step 2: Creating the Splunk Data Inputs

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

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



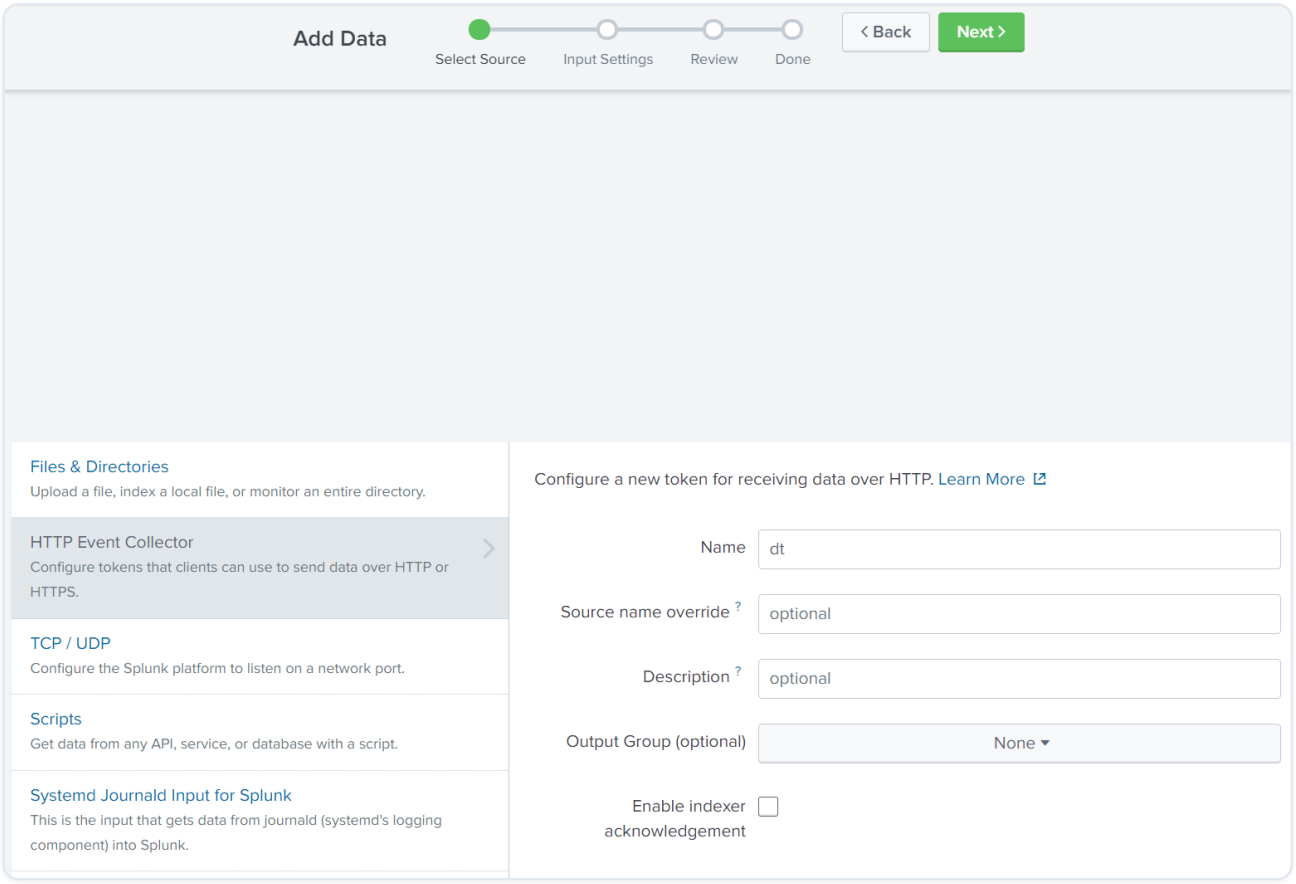
- Select `HTTP Event Collector`
- Click `New Token



- Set a `name` of your choice.

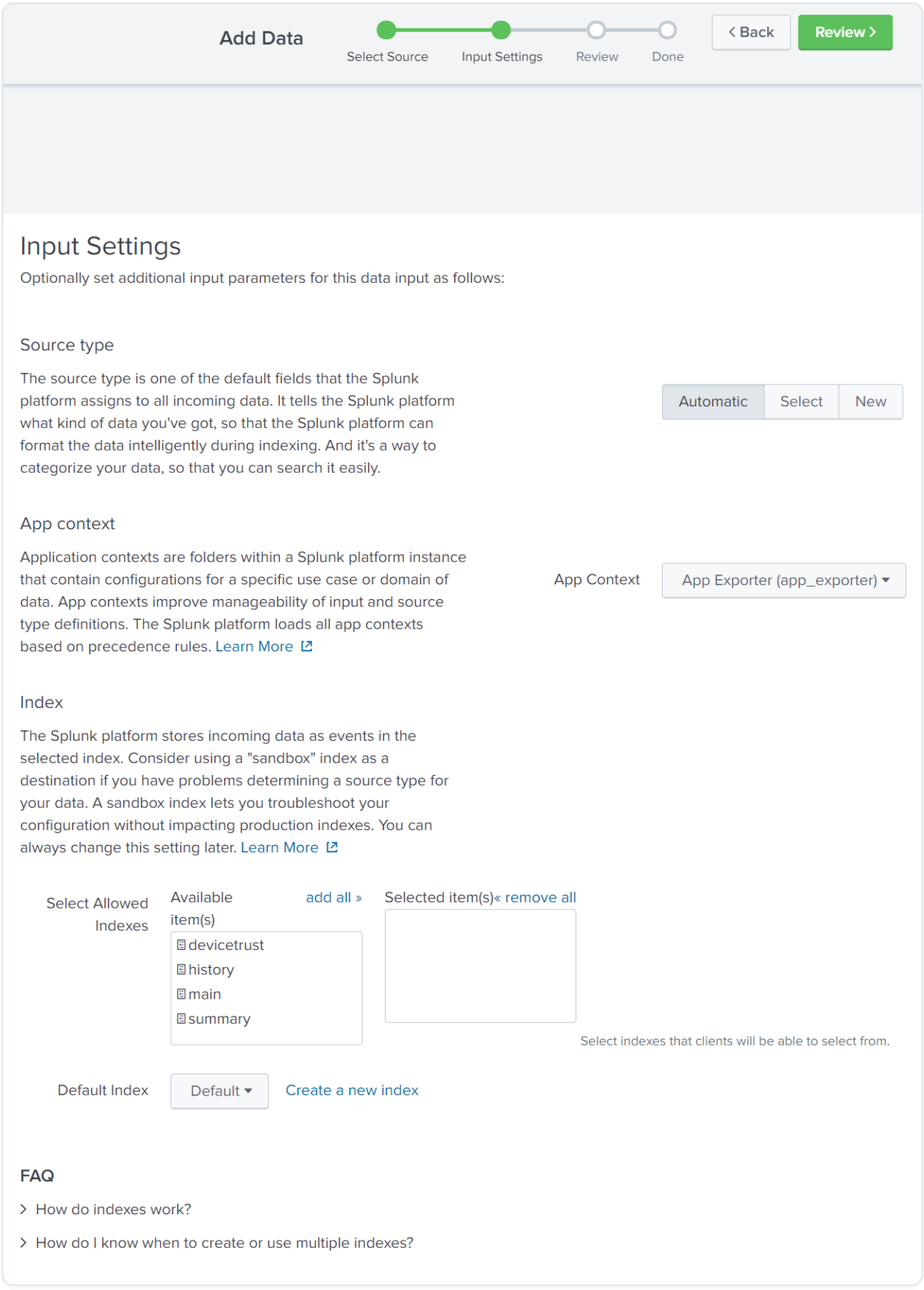
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- All other settings are optional.



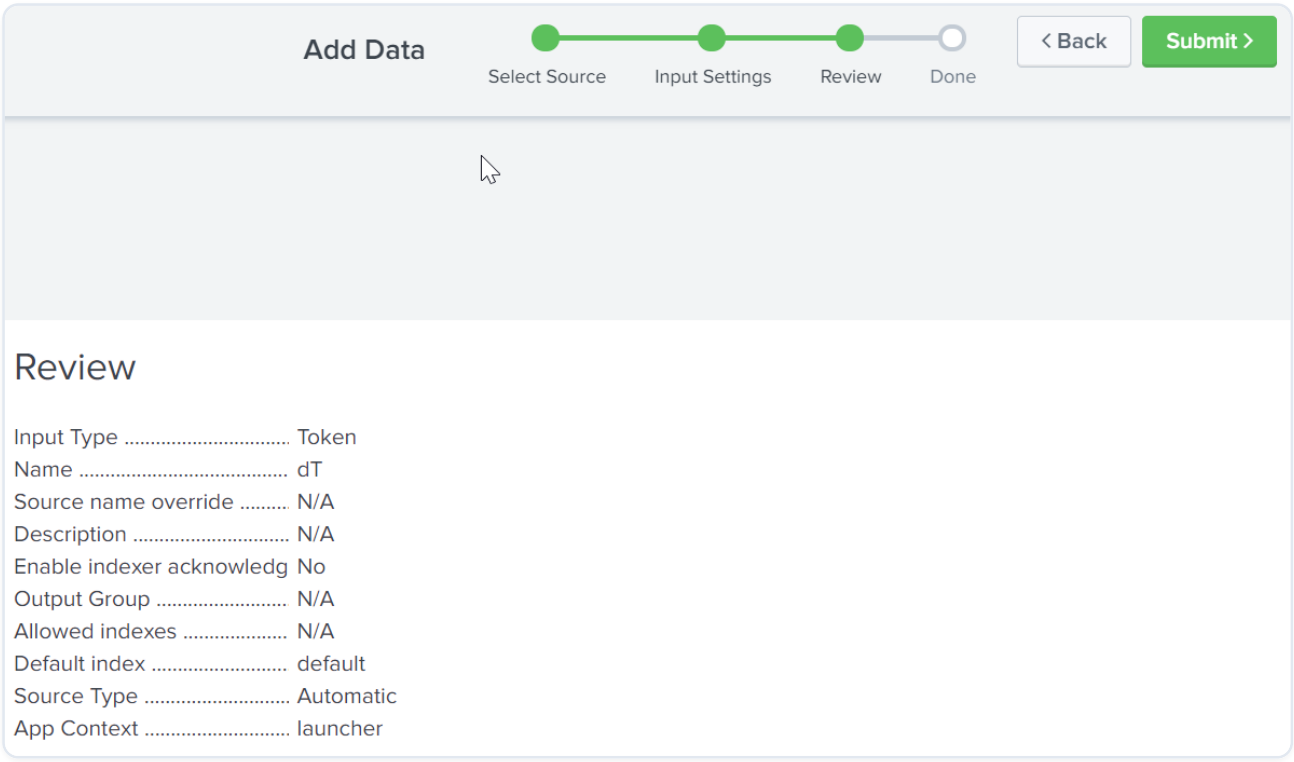
`Input settings` does, for example, allow to restrict access for this data input to certain indexes. Any of these settings may be relevant for your environment. The function of the deviceTRUST reports will not be affected by setting them.

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

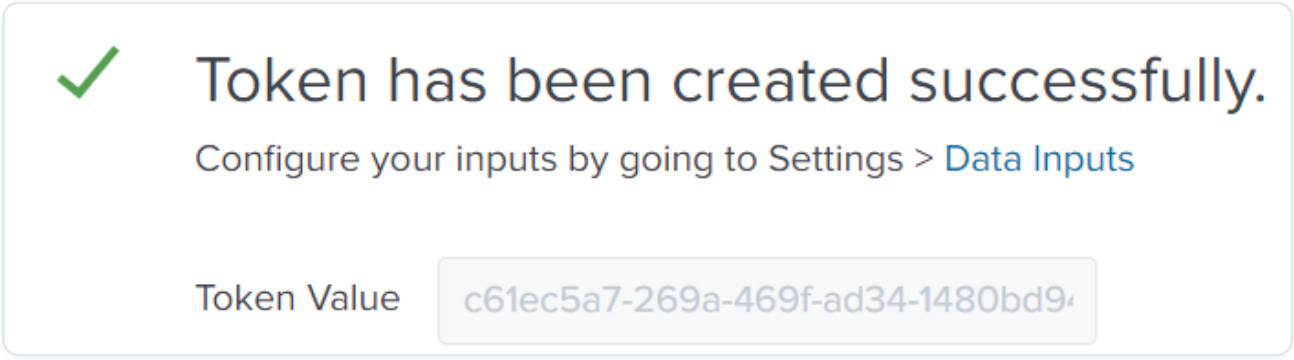


- Review the Settings.
- Click `Submit`.

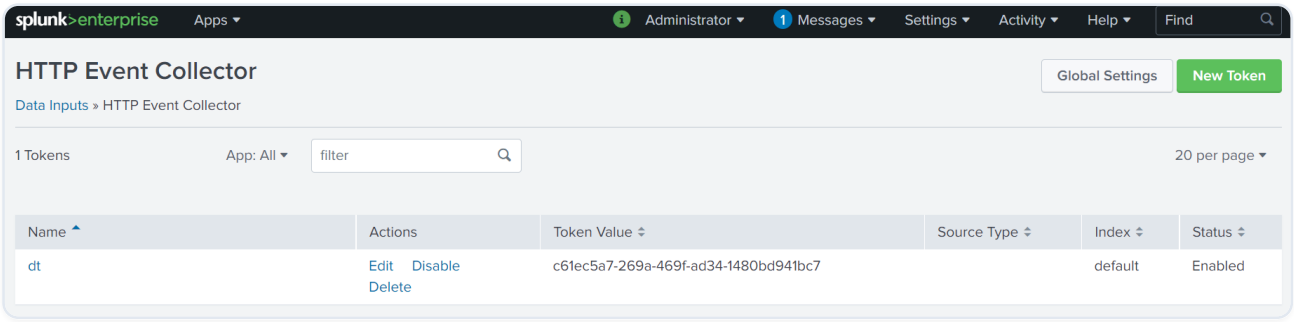
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The created token is shown.



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

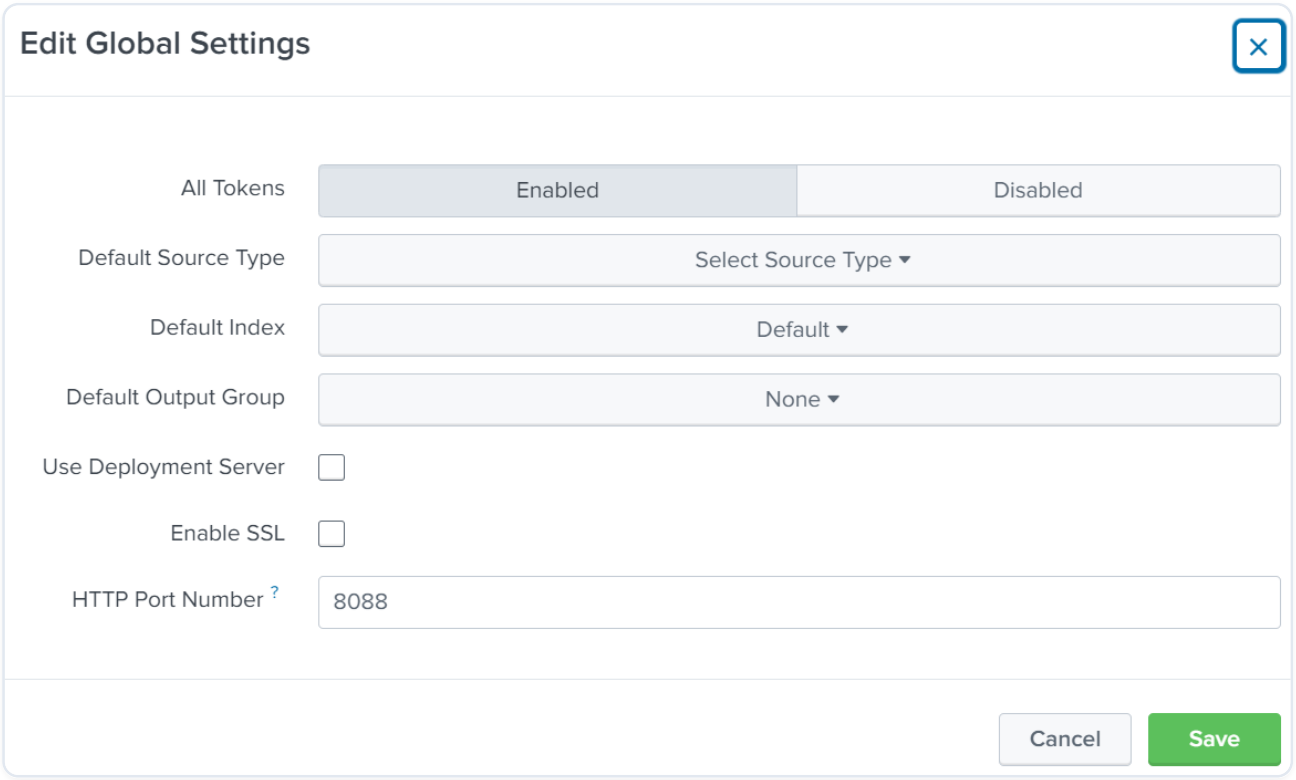


Additionally, the http input method has to be configured. In the most basic configuration, we make sure SSL is not active and all tokens are enabled.

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

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

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



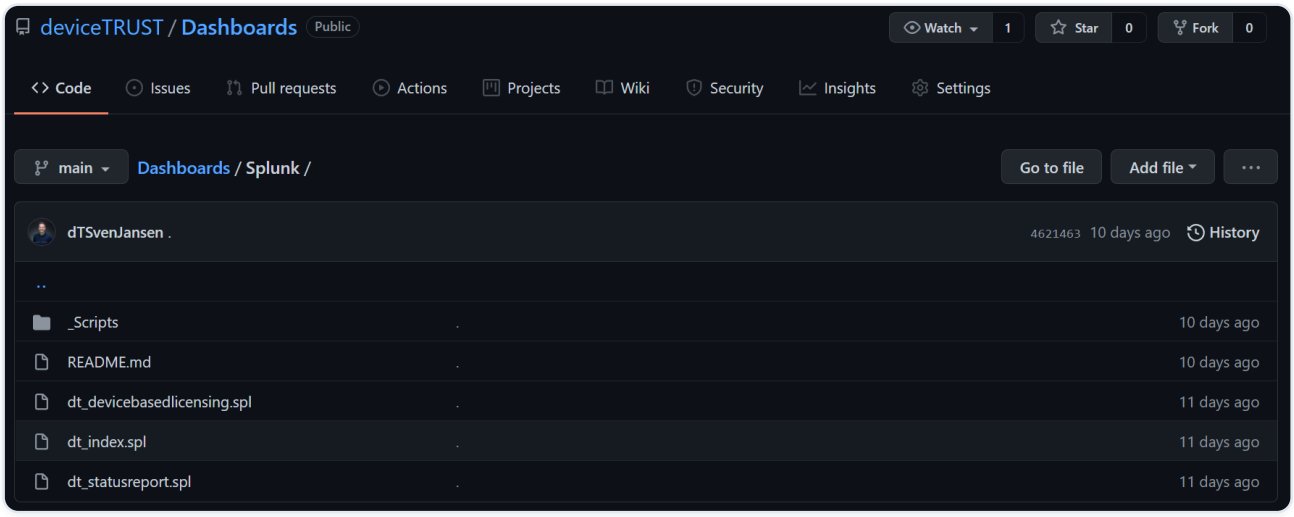
Step 3: Importing the Splunk app

Step 3.1: Downloading the Splunk app

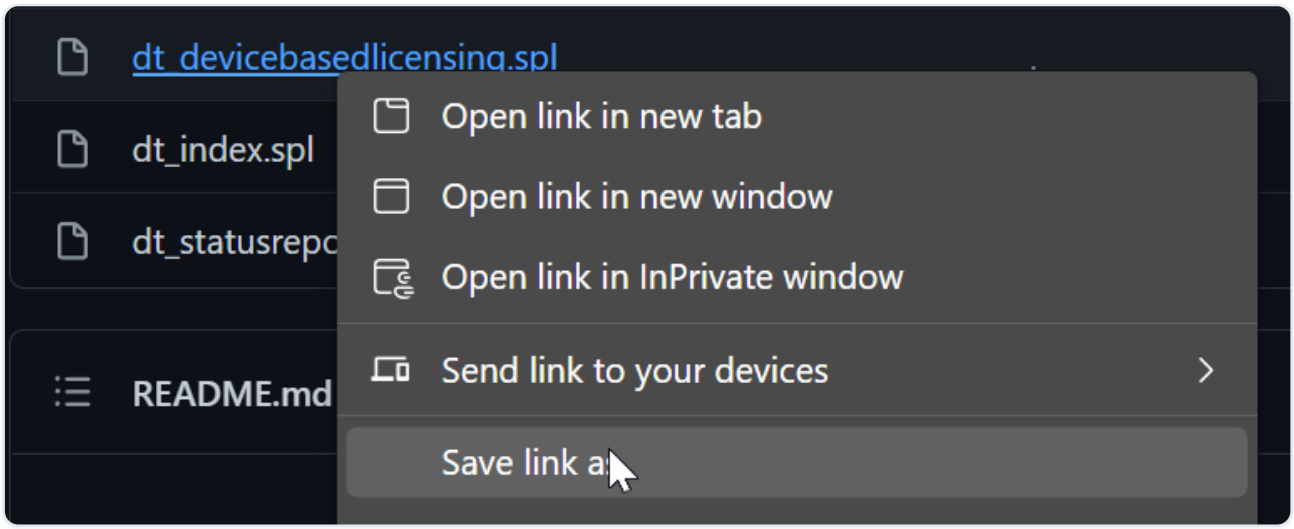
The deviceTRUST reports are delivered as Splunk apps. The apps is available from the deviceTRUST GitHub repository .

- Navigate to the repository and find the Splunk apps.

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



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



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

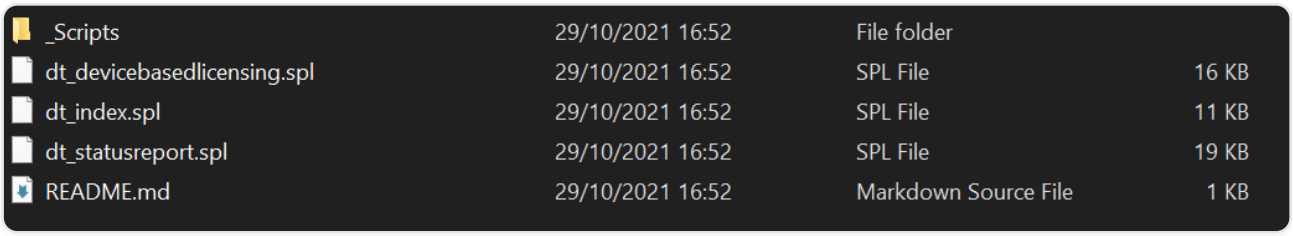
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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


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


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

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

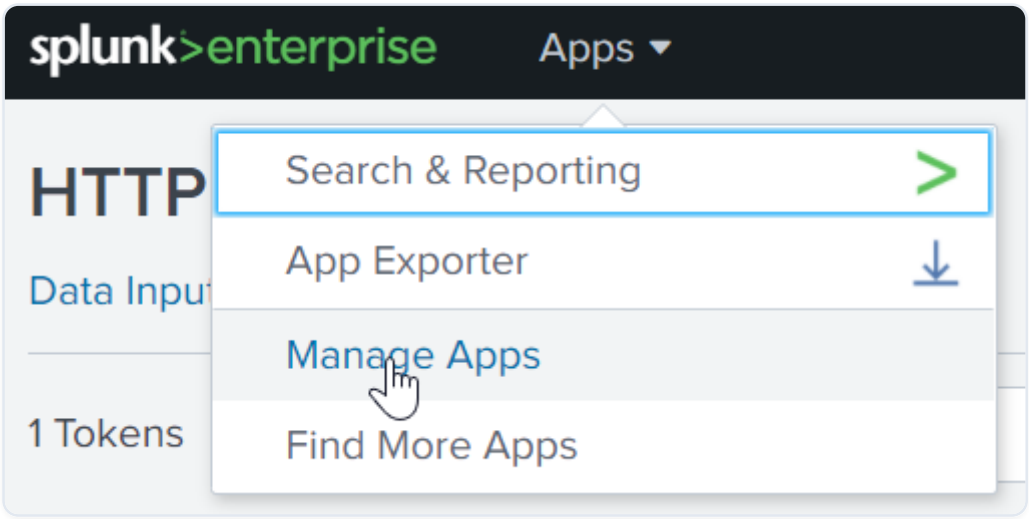


Step 3.2: Installing the Splunk app

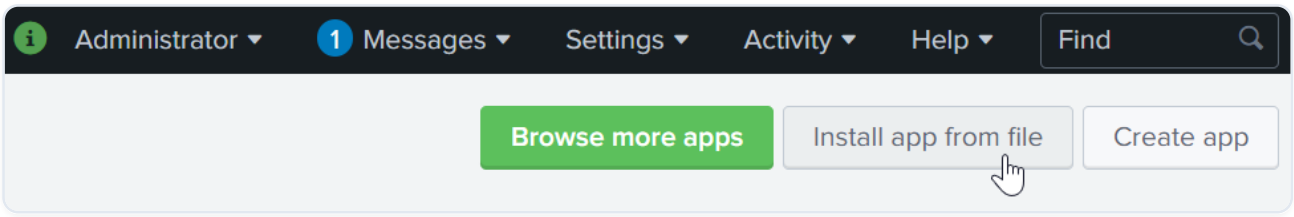
All three deviceTRUST apps are installed the same way. Thus, the app installation is described by using one example.

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

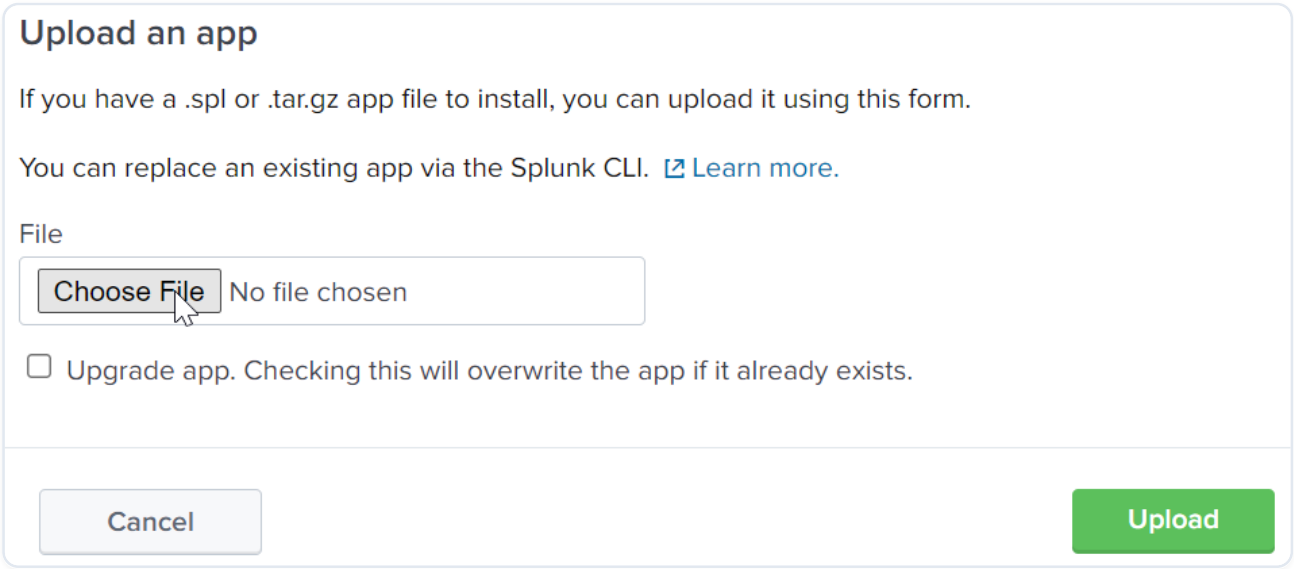
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Click `Install app from file`.

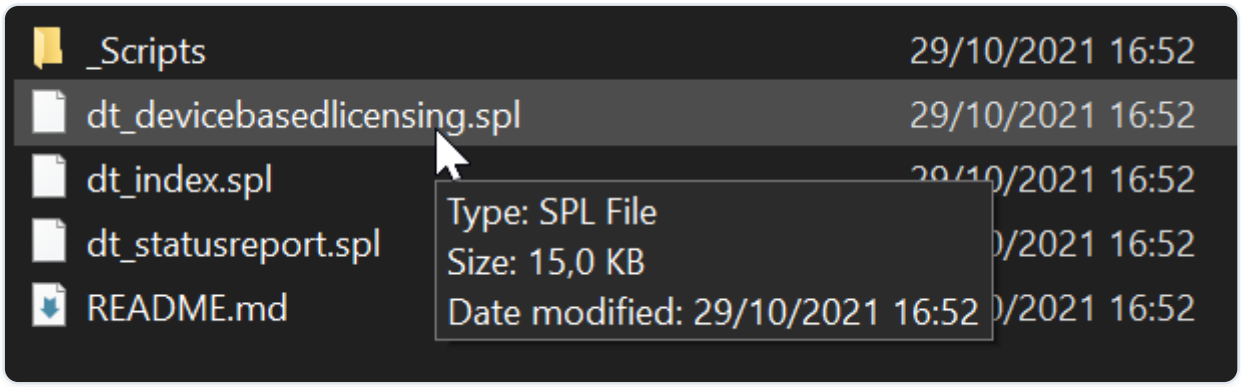


- Click `Choose File`.

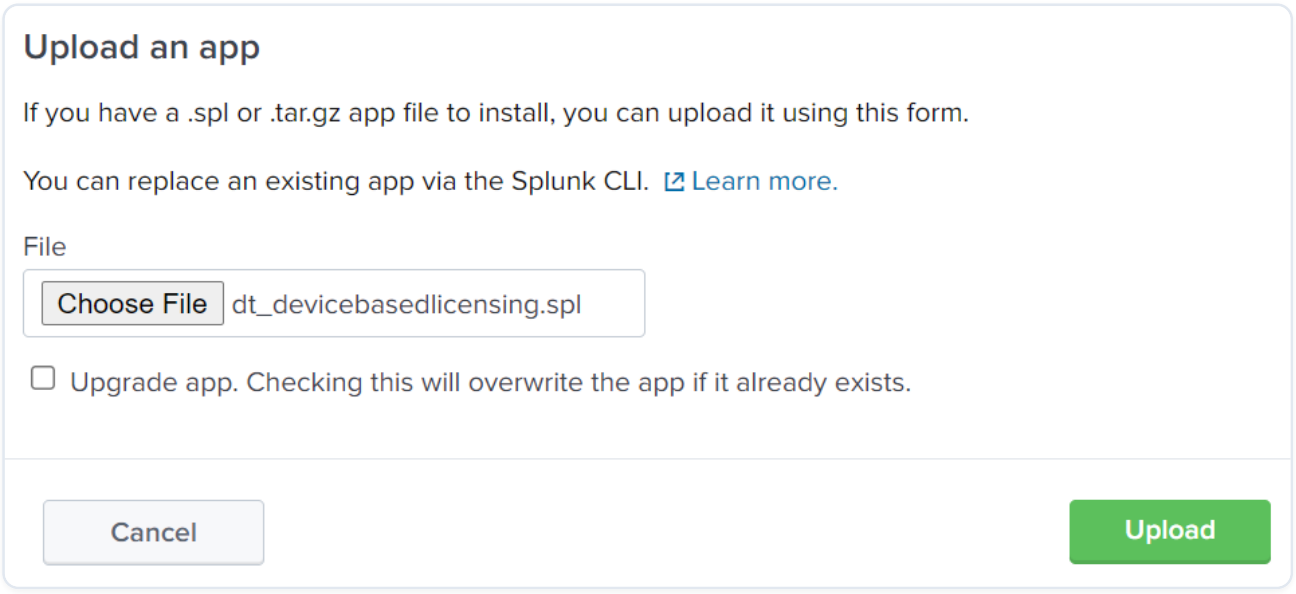


- Select your app file.

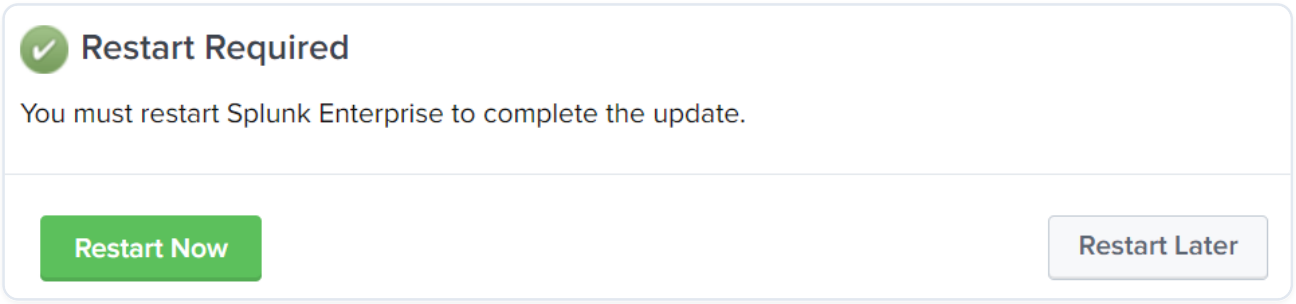
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

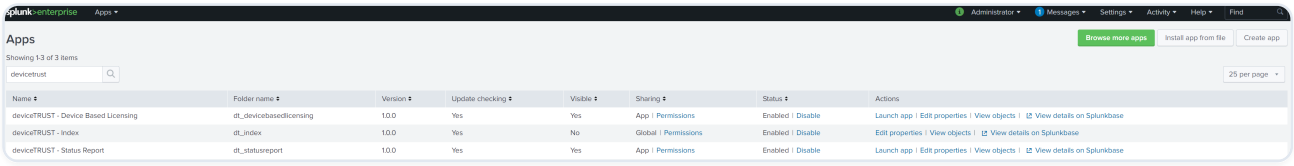


- Splunk will ask to restart the service. This is only required after importing the last app.
- Choose `Restart Now` or `Restart Later` accordingly.



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

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



Step 4: Configuring deviceTRUST

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

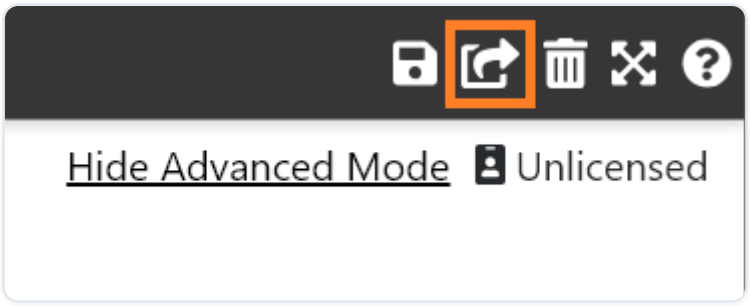
As both reports `Device-Based Licensing` and `Status Report` differ in their details, both are described here separately.

Step 4.1: The Device-Based Licensing Report

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

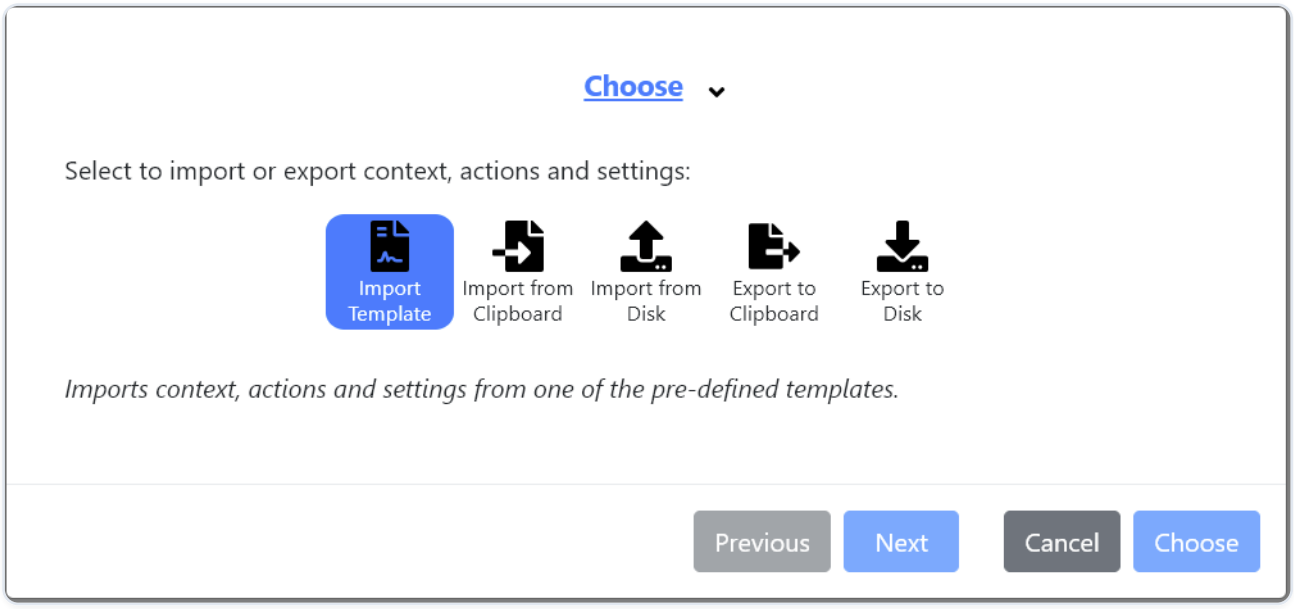
The integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. These five example applications can be easily edited for your own applications, or cloned to represent new applications. The elements are contexts,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

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

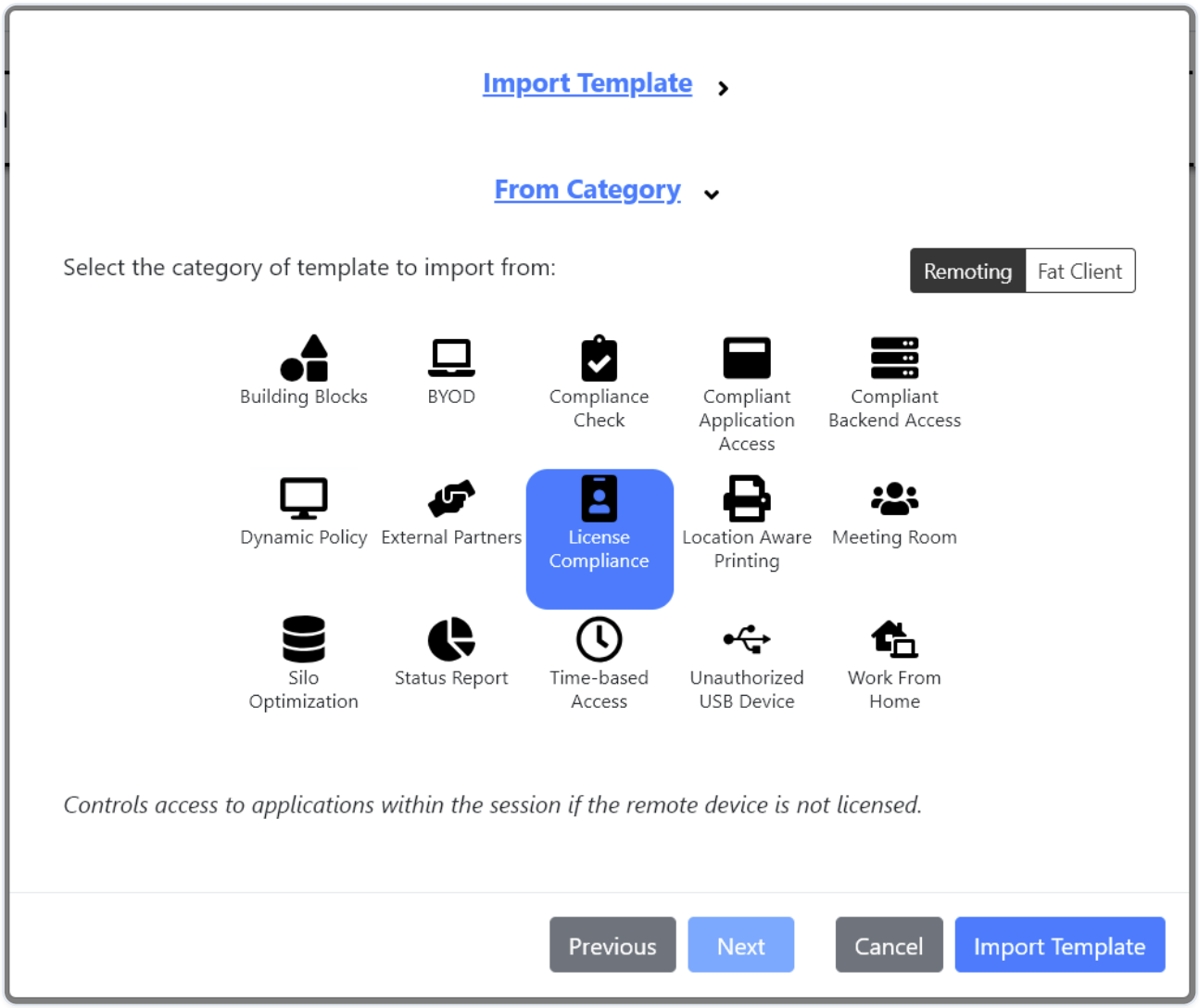


- Select `Import Template`

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

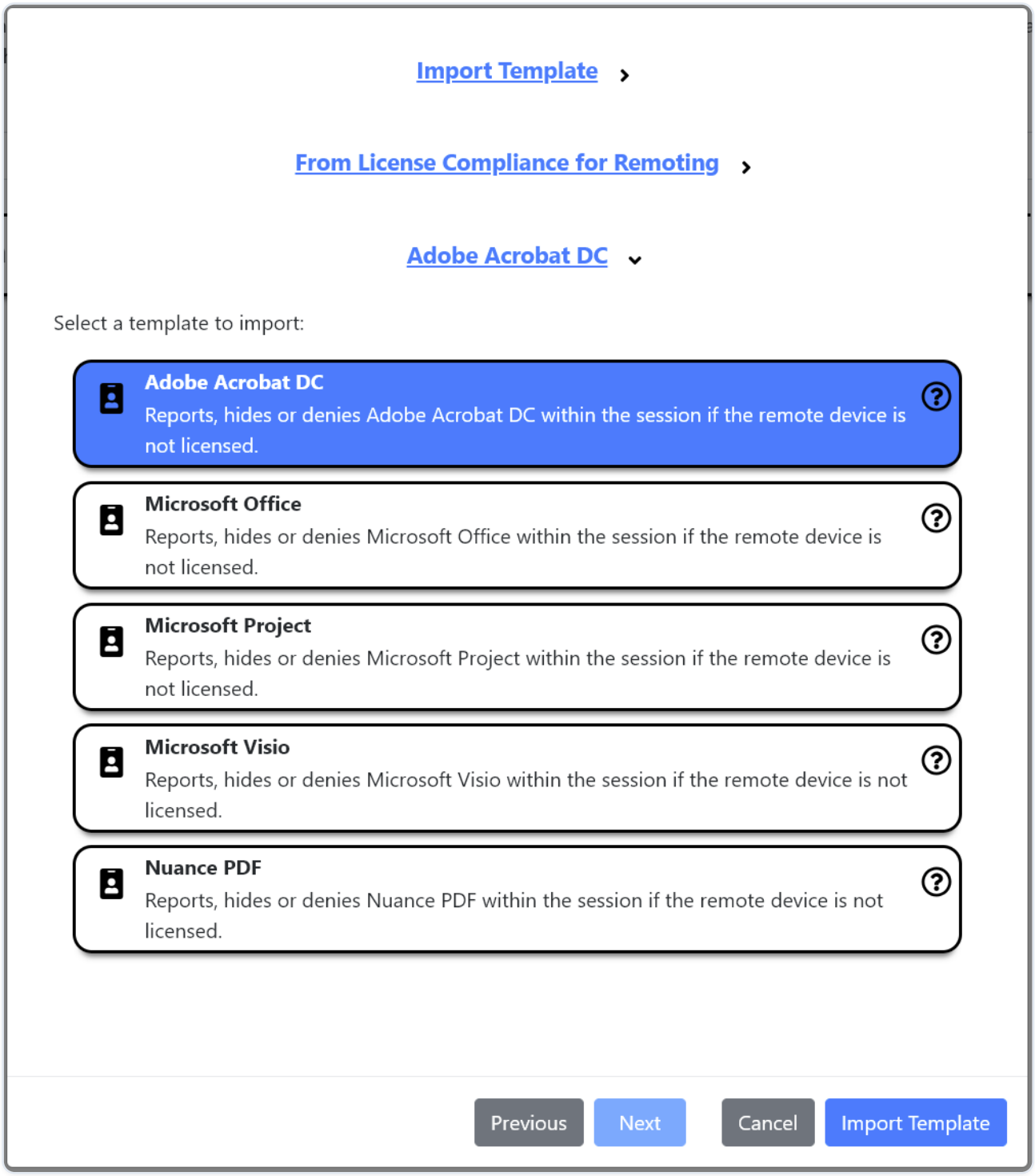


- The report `Device-Based Licensing` can be found within the template category `License Compliance` when `Remoting` is selected.



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

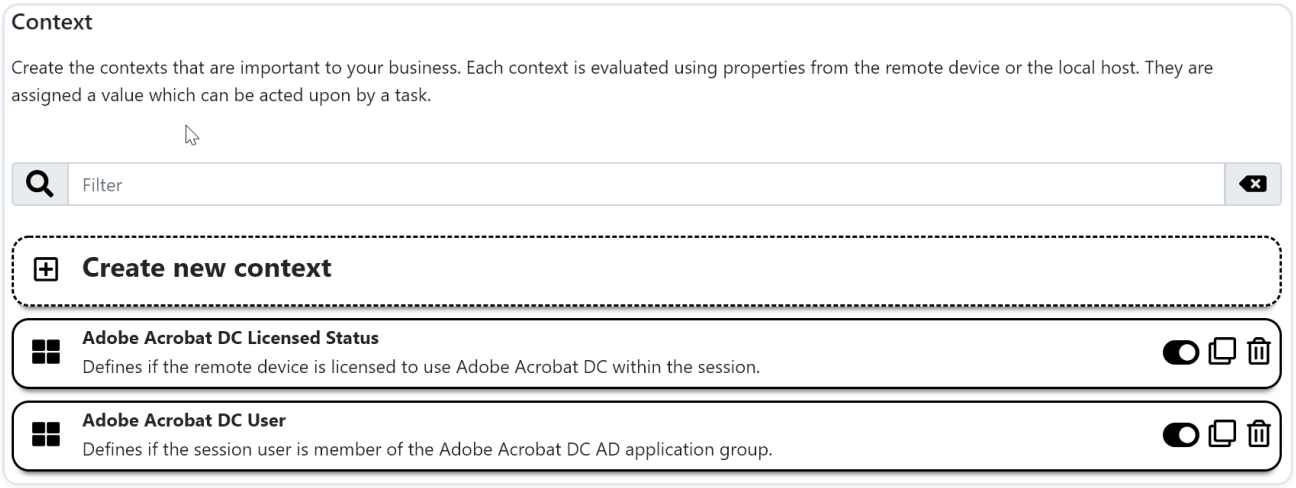
- The category contains templates for different example applications. We use `Adobe Acrobat DC` as an example here.



Two contexts are included within the template:

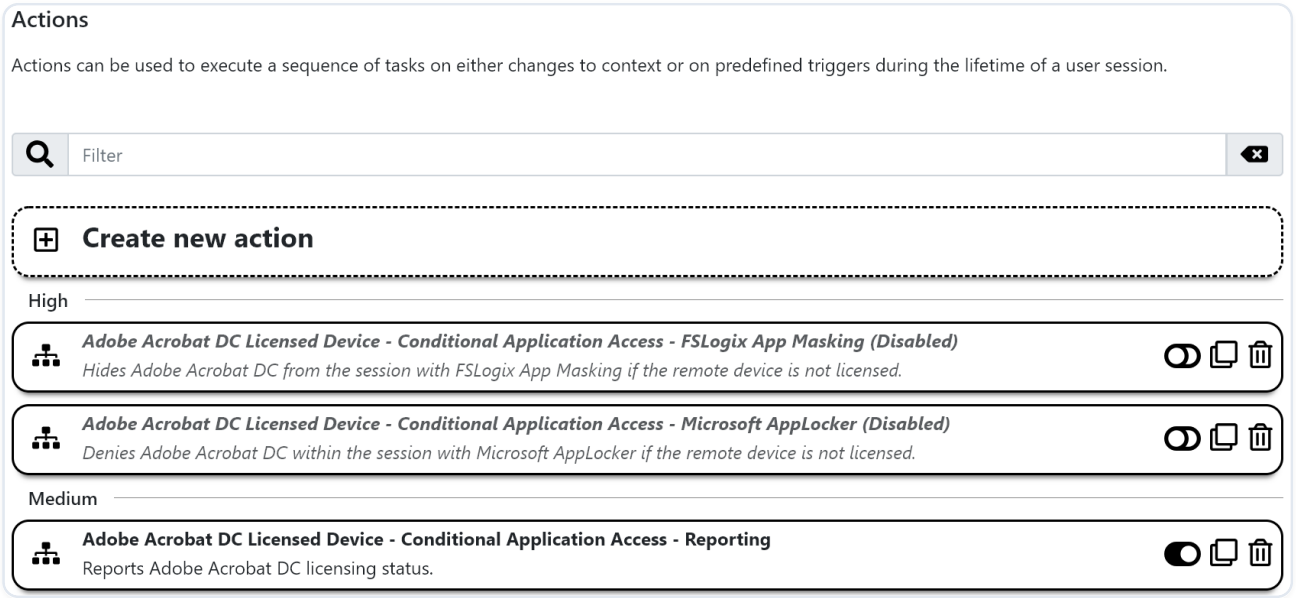
- `Adobe Acrobat DC Licensed Status` to evaluate the device license status.
- `Adobe Acrobat DC User` to define if the accessing user is licensed to use the software.

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



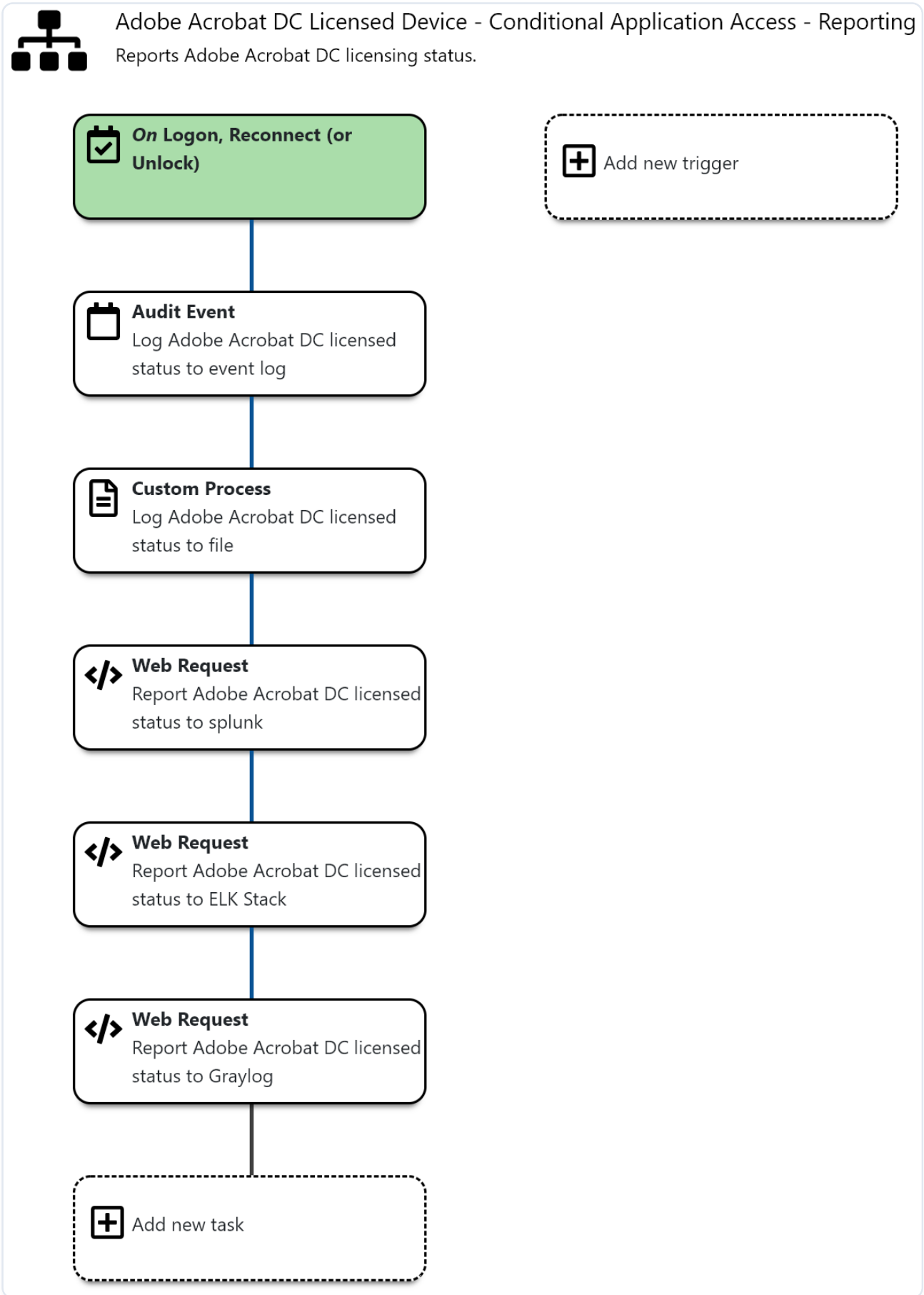
Three actions are included within the template:

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



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

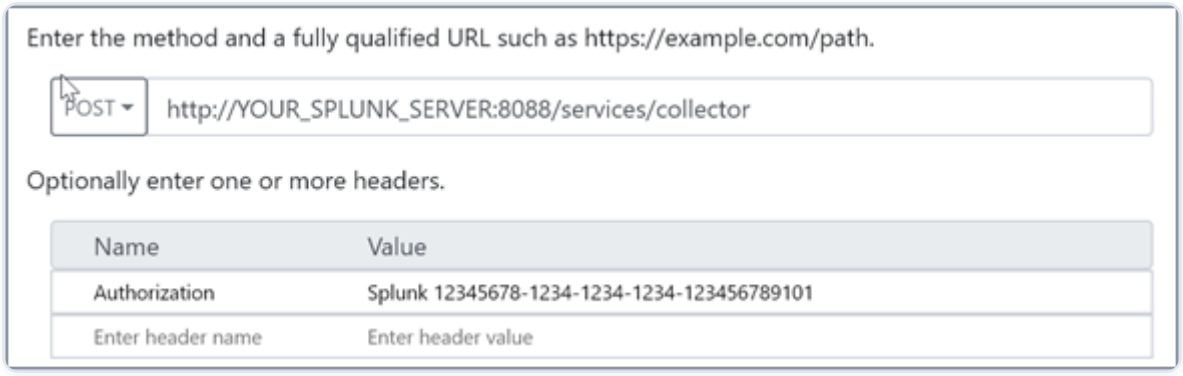
© 1997–2026 Citrix Systems, Inc. All rights reserved.



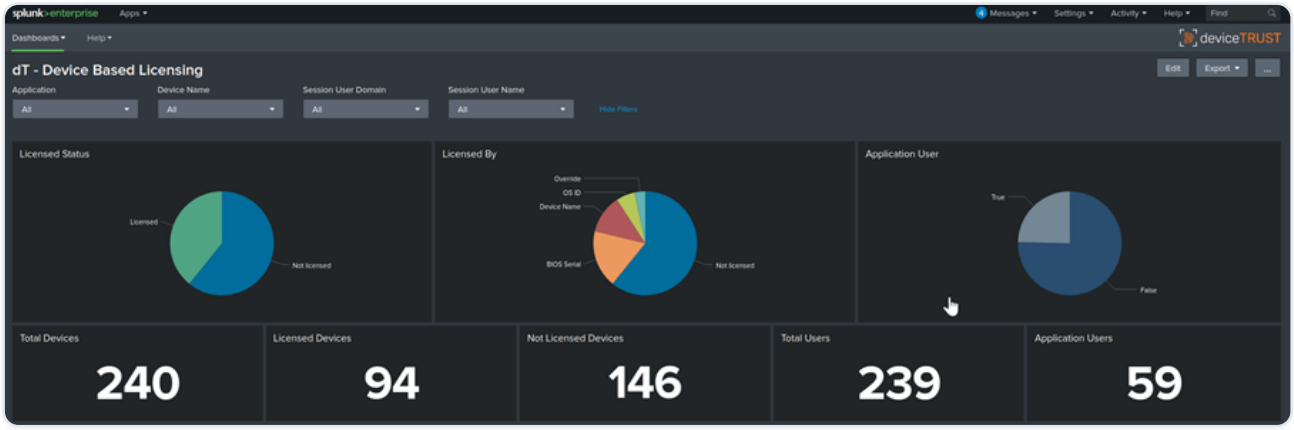
- The Splunk `Web Request` task needs to be edited to suit your environment. If you do not require SSL transport, you'll only have to configure your `server's fqdn` and the

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

`authorization token` (http data input). Make sure to leave the keyword `splunk` and only add/change your authorization token's GUID.



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

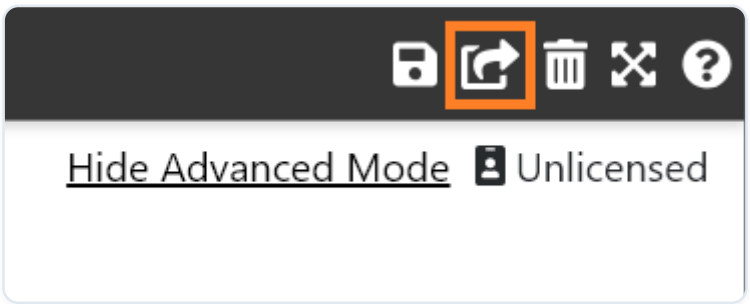


Step 4.2: The Status Report

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

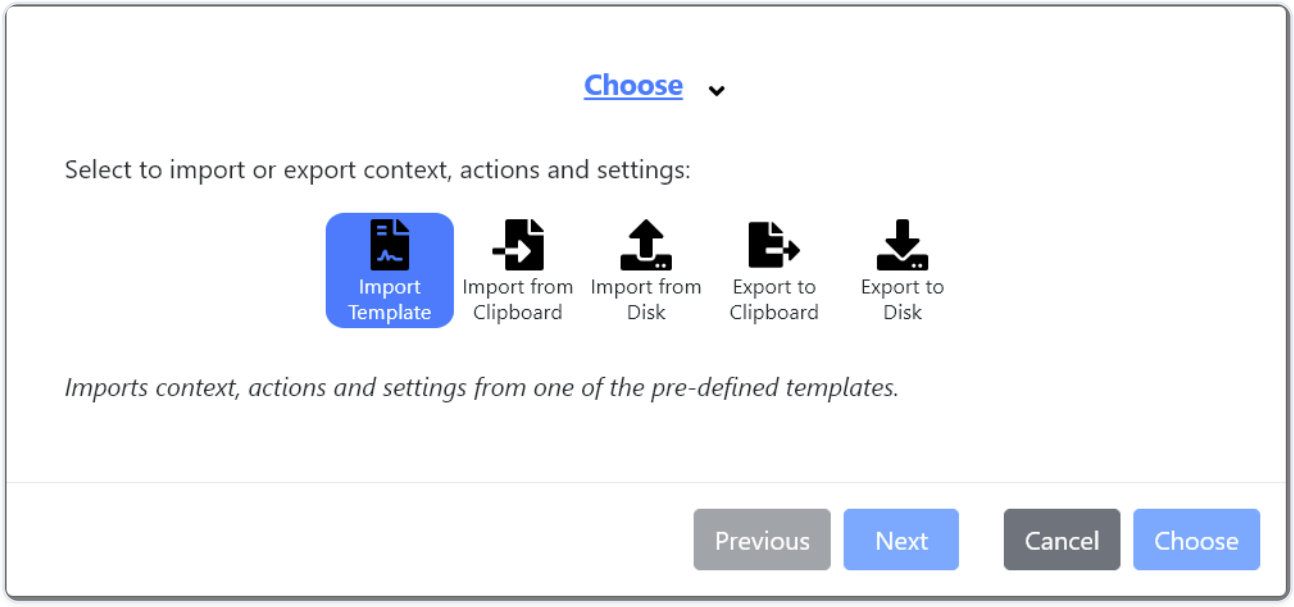
Our integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. The elements are contexts, actions, messages and settings.

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

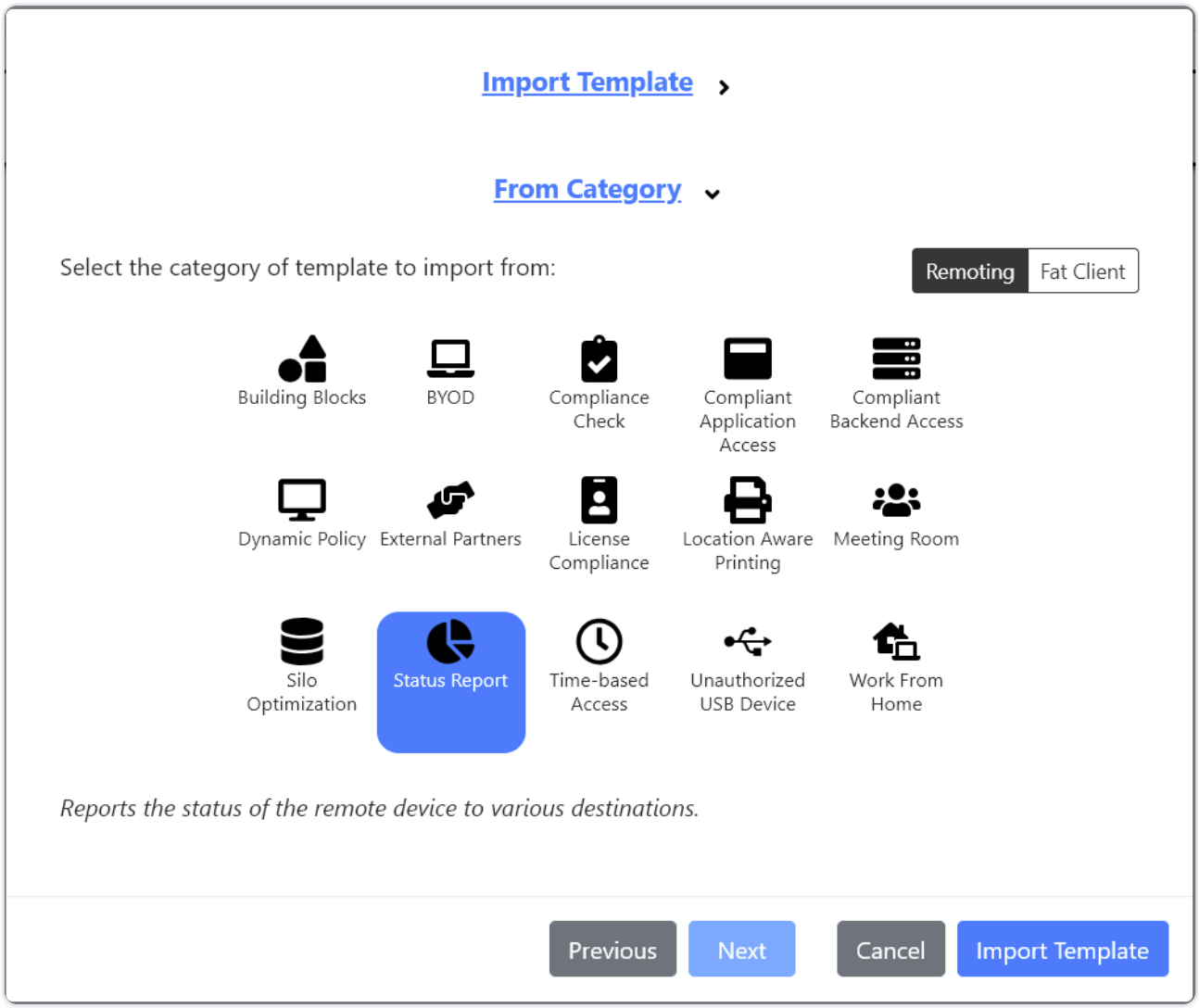


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select `Import Template`

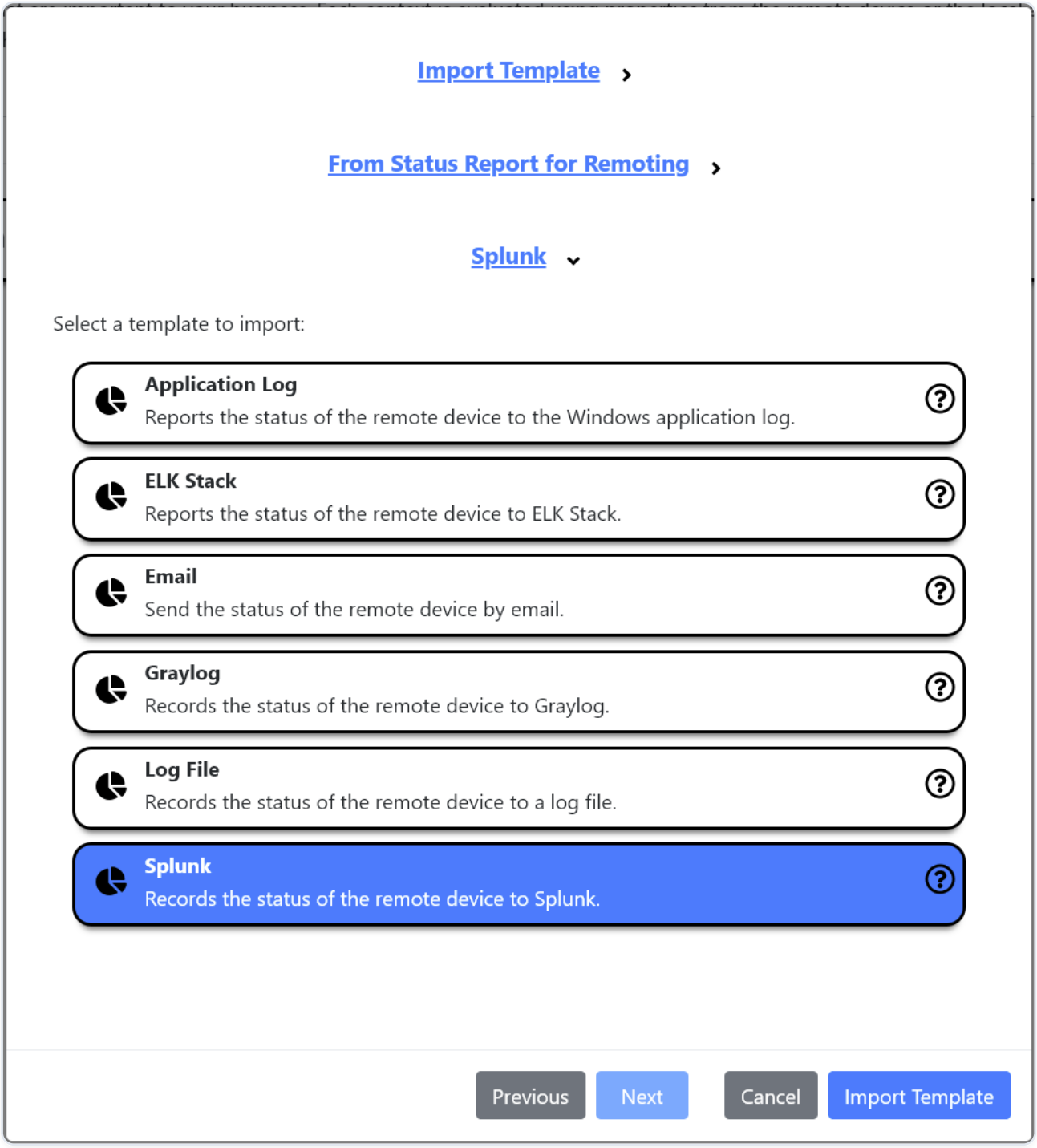


- The `Status Report` template can be found within the template category `Status Report` when `Remoting` is selected.



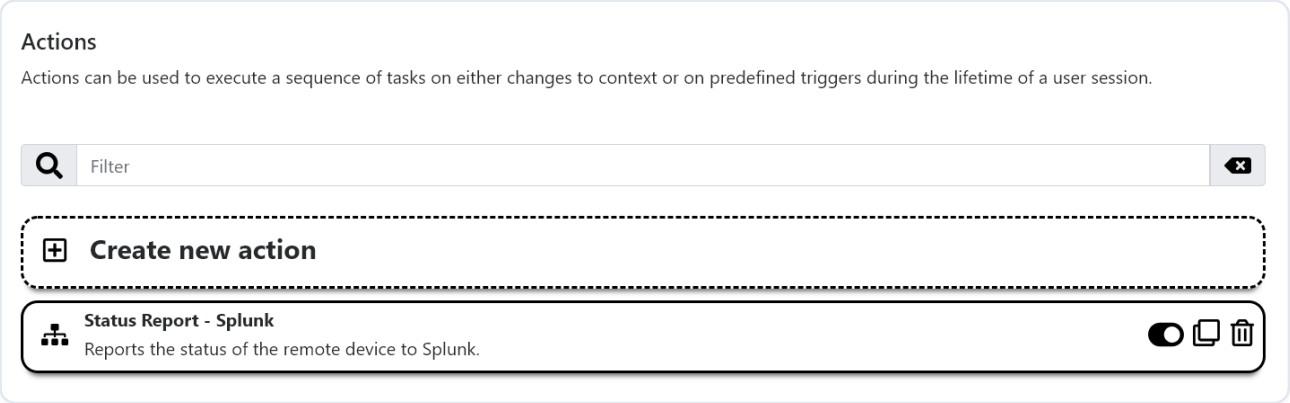
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

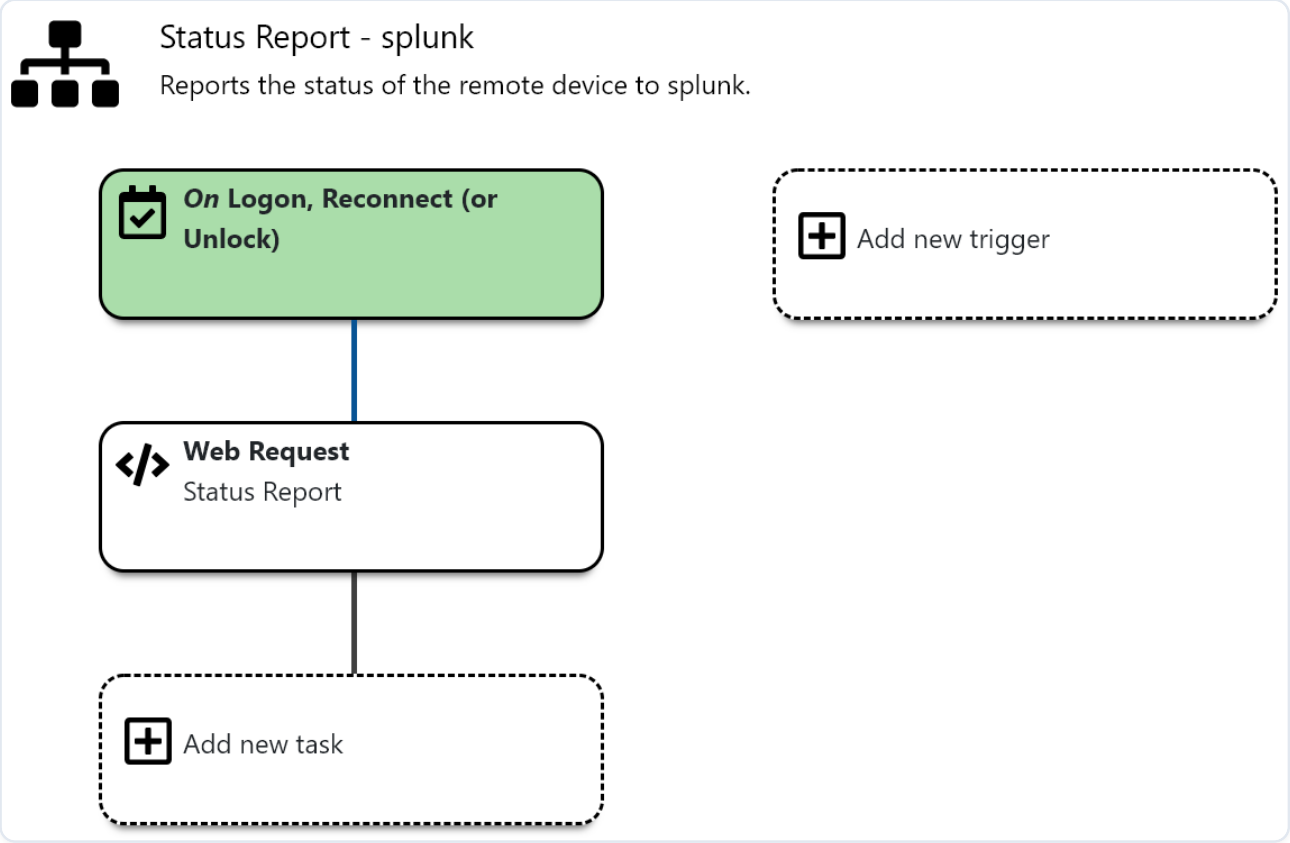


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – Splunk` collects all relevant data and sends them over to Splunk.

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

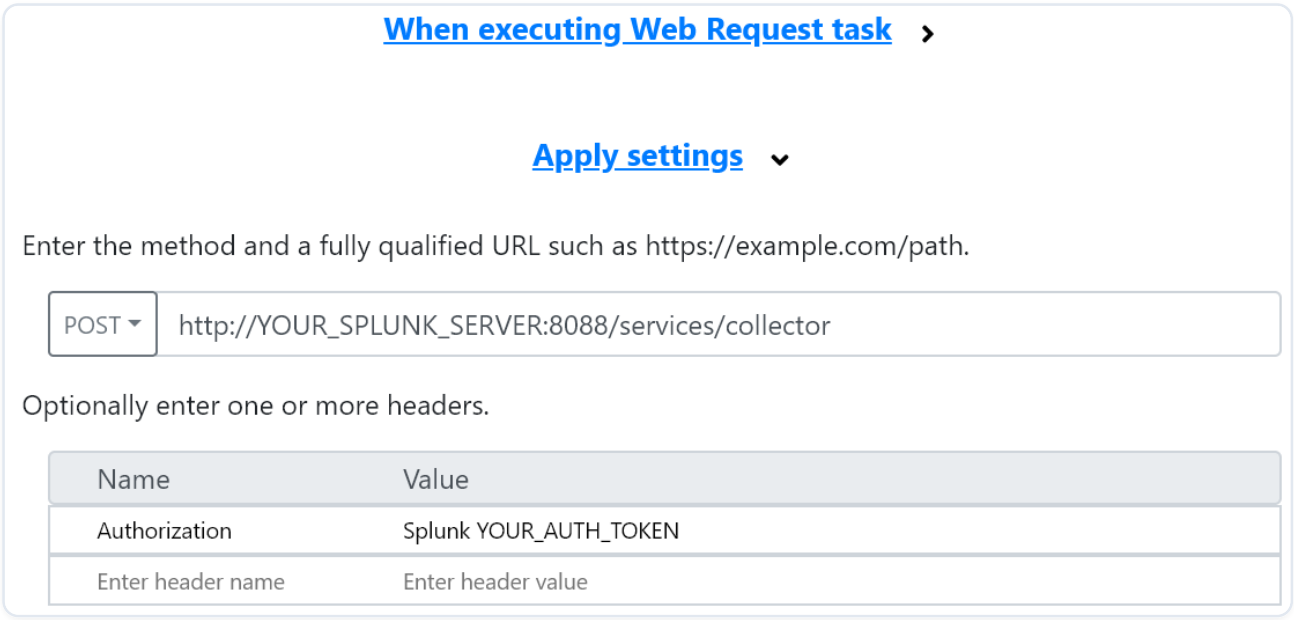


- Sending data to Splunk is configured by using a `Web Request` task.

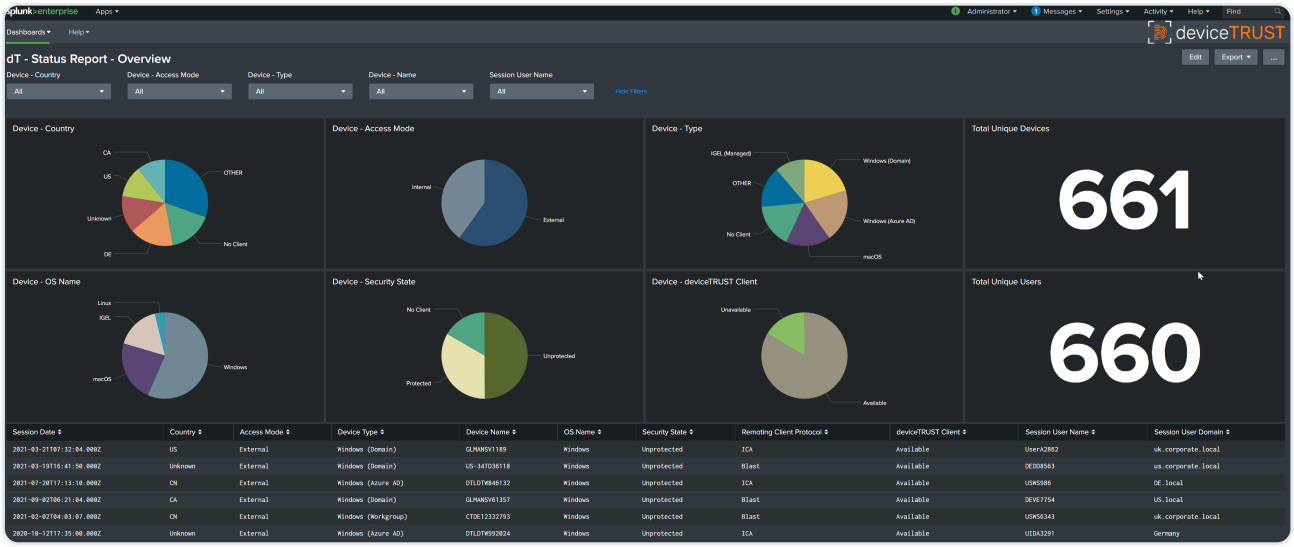


The Web Request task needs to be edited to suit your environment. If you do not require SSL transport, you'll only have to configure your `server's fqdn` and the `authorization token` (http data input). Make sure to leave the keyword `splunk` and only change your authorization token's GUID.

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



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

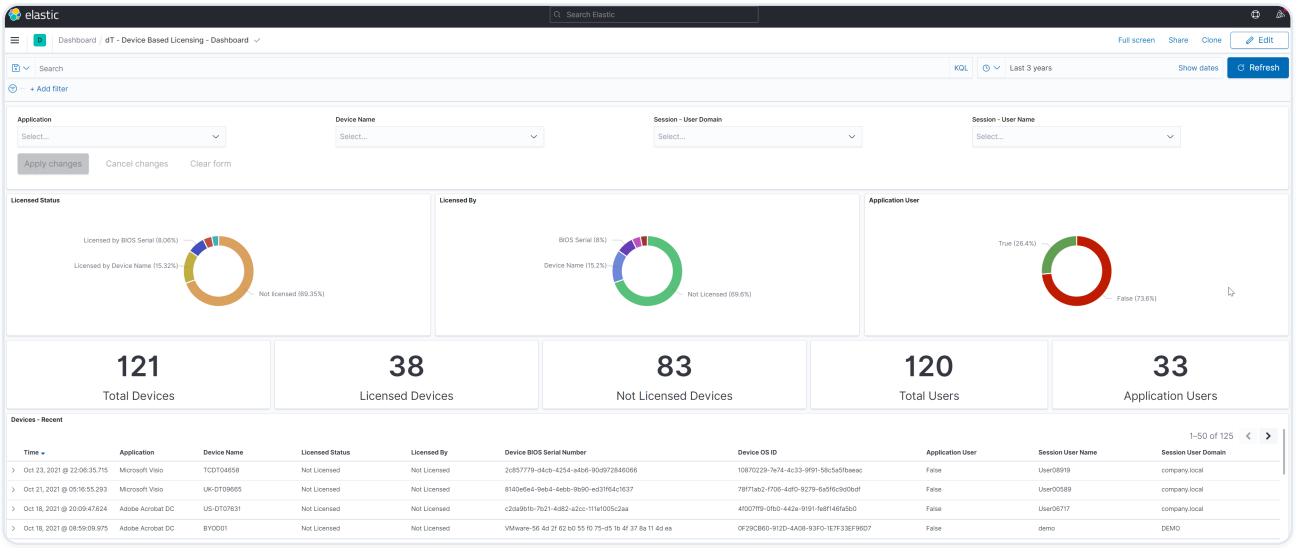


ELK Stack Dashboards

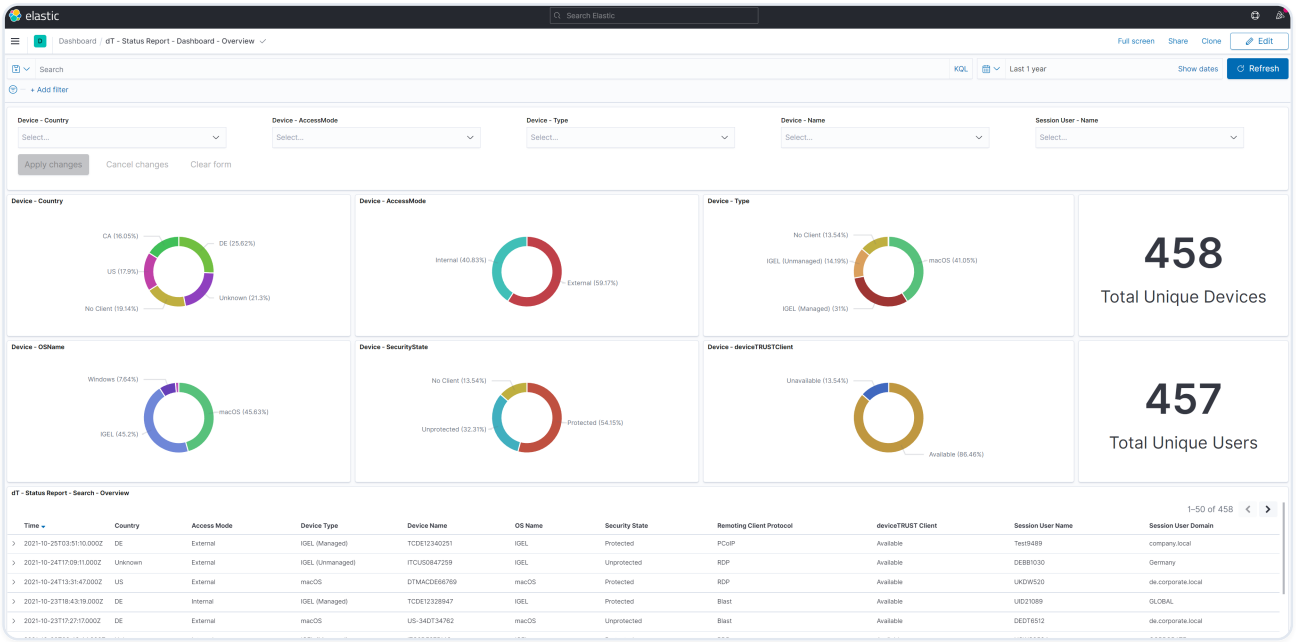
deviceTRUST® includes components for an ELK Stack to easily create a dashboard to monitor the contextual status of your remoting and DaaS environment.

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

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



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



- Step 1: Components
  - Step 1.1: Components - GitHub
  - Step 1.2: Components - Templates
- Step 2: The Device-Based Licensing Report
  - Step 2.1: Add Index Template to ELK Stack
  - Step 2.2: Import Saved Objects to ELK Stack
  - Step 2.3: Configuring deviceTRUST
- Step 3: The Status Report

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

- Step 3.1: Add Index Template to ELK Stack
- Step 3.2: Import Saved Objects to ELK Stack
- Step 3.3: Configuring deviceTRUST
- Step 3.4: Edit index settings

Step 1: Components

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

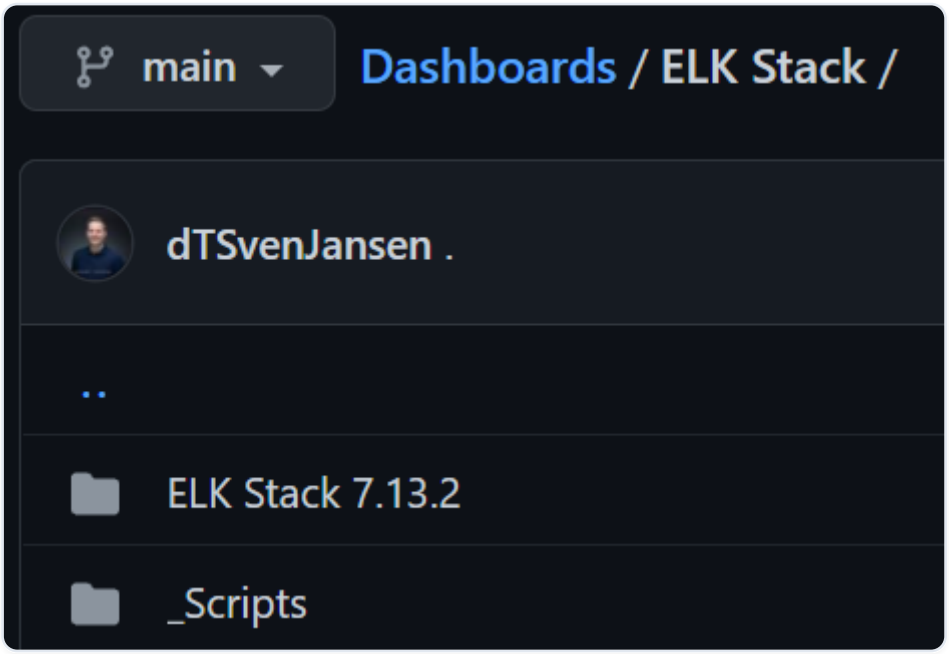
Step 1.1: Components - GitHub

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

NOTE:

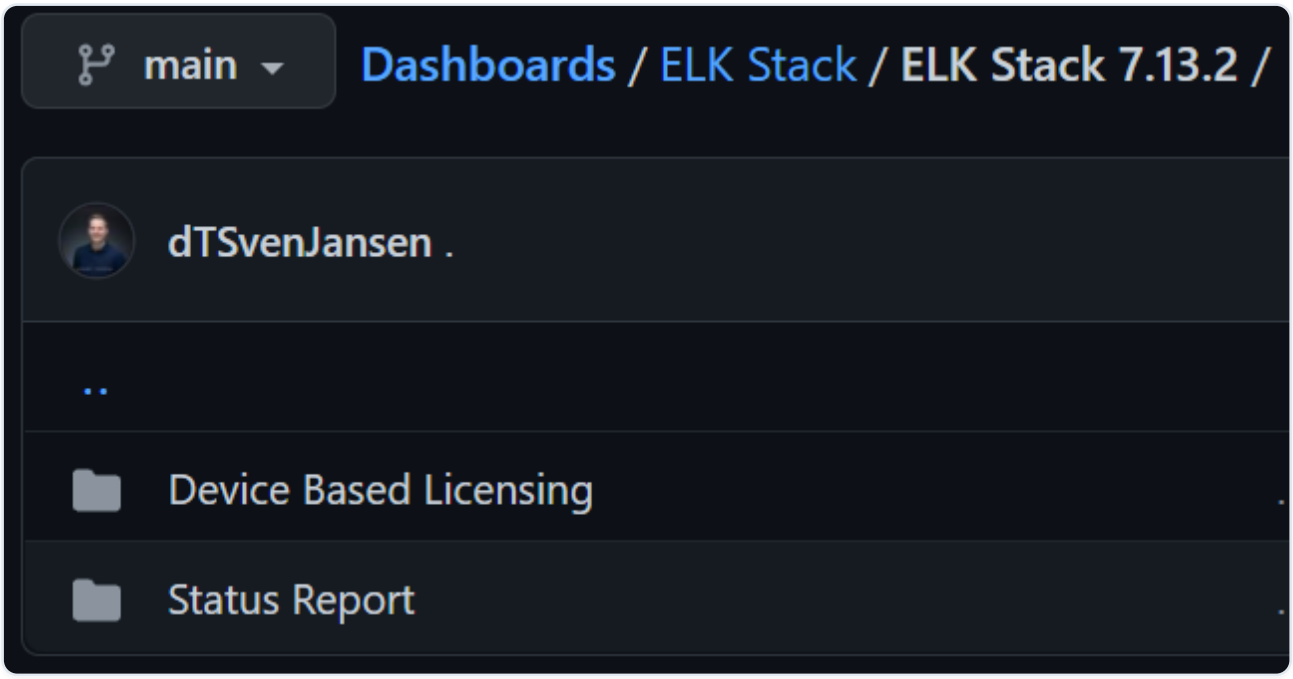
Saved objects for ELK are not backward compatible. Please use only versions matching or older than your system.

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



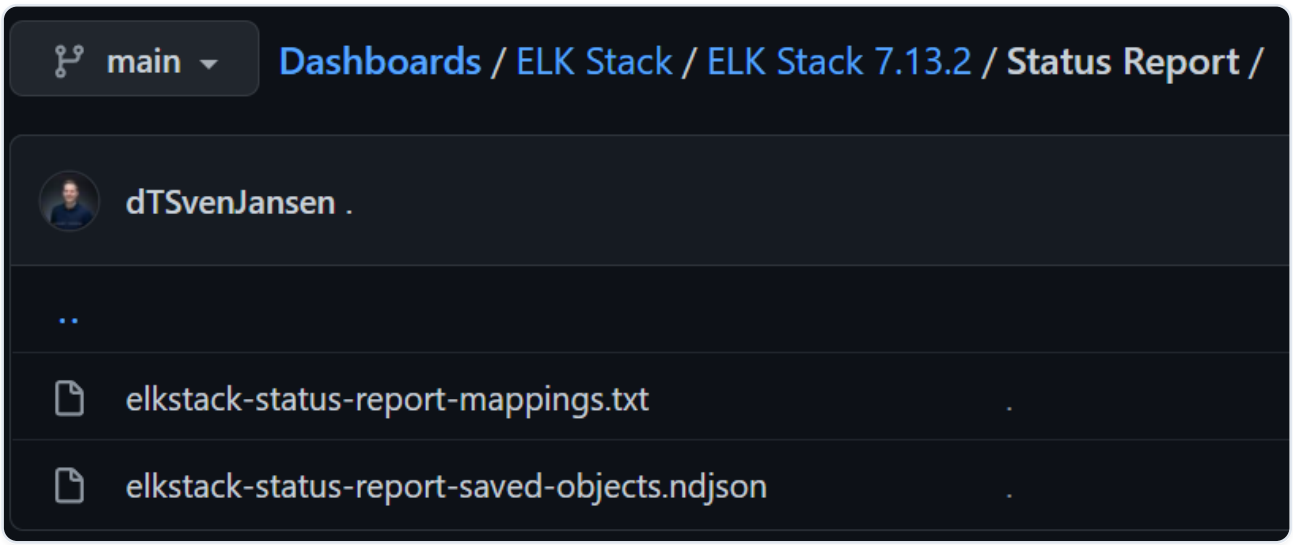
Every version folder contains folders for each use case. Each of these use case folders contains the relevant stored object and mapping files.

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



Each use case folder contains the following files:

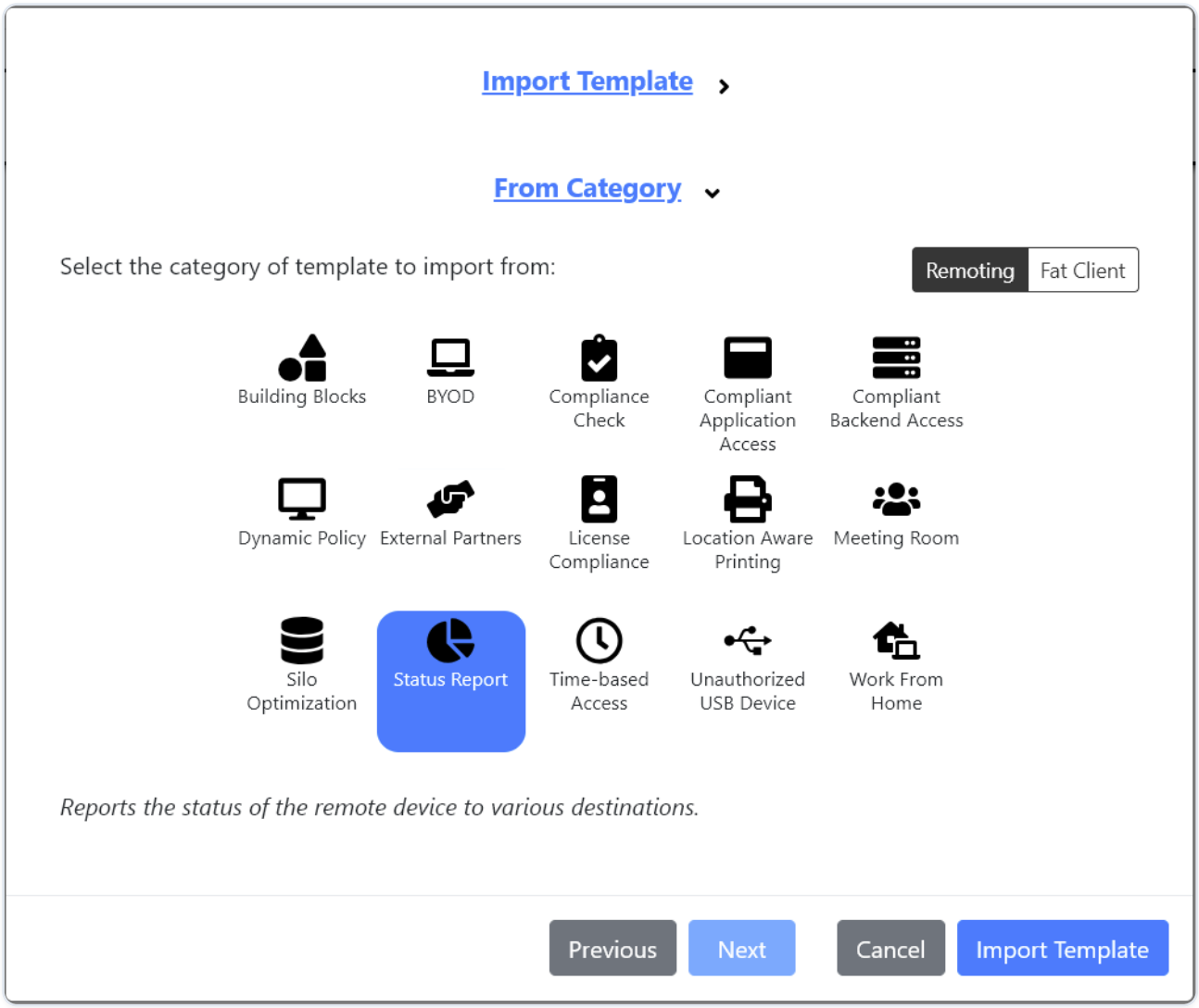
- `elkstack-<use case>-mappings.txt` contains data definitions for the data being sent to ELK Stack index mapping.
- `elkstack-<use case>-saved-objects.ndjson` contains all objects that are required to store, search and visualize data, such as indexes, scripted fields, dashboards and searches.



Step 1.2: Components - Templates

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

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



Step 2: The Device-Based Licensing Report

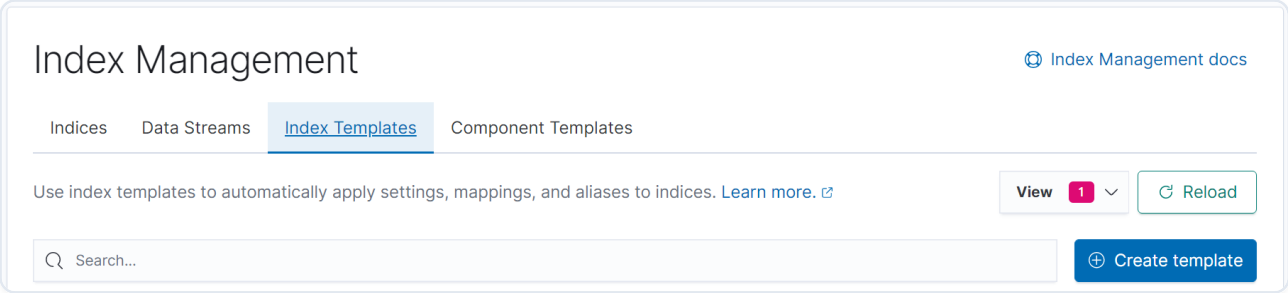
This part of the guide relates to `Device-Based Licensing`. It lists all steps that are required to configure the ELK Stack, and also how to configure the deviceTRUST Agent.

Step 2.1: Add Index Template to ELK Stack

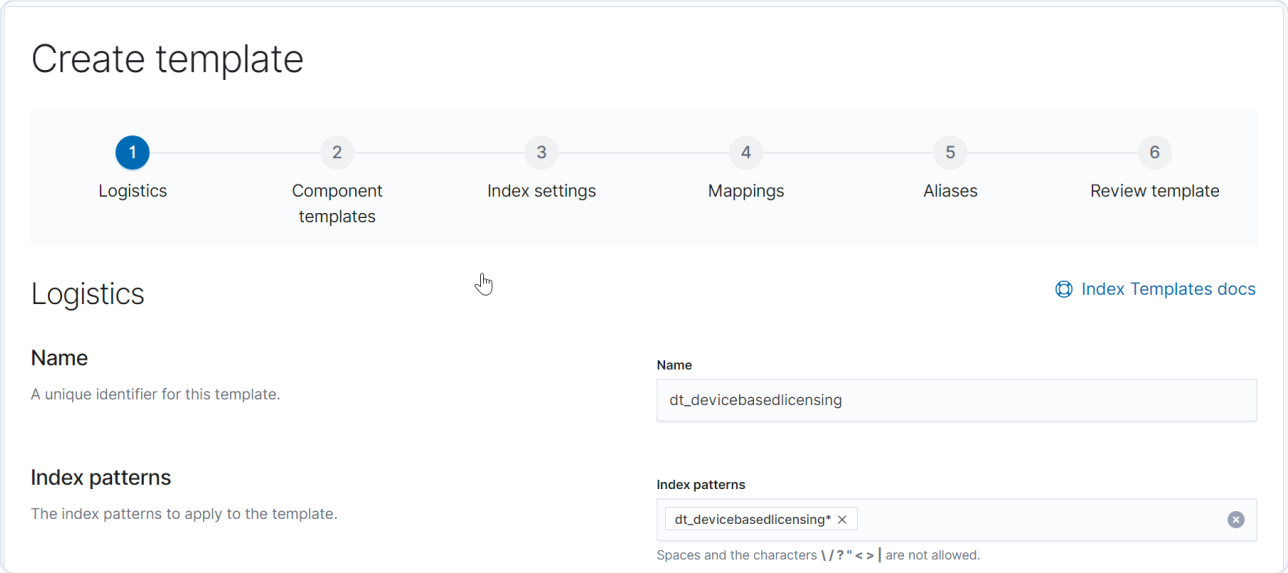
The first step is to create an `Index Template`. Index Templates describe the data that is being sent to an index. They make sure that every date is treated according to its type.

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

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

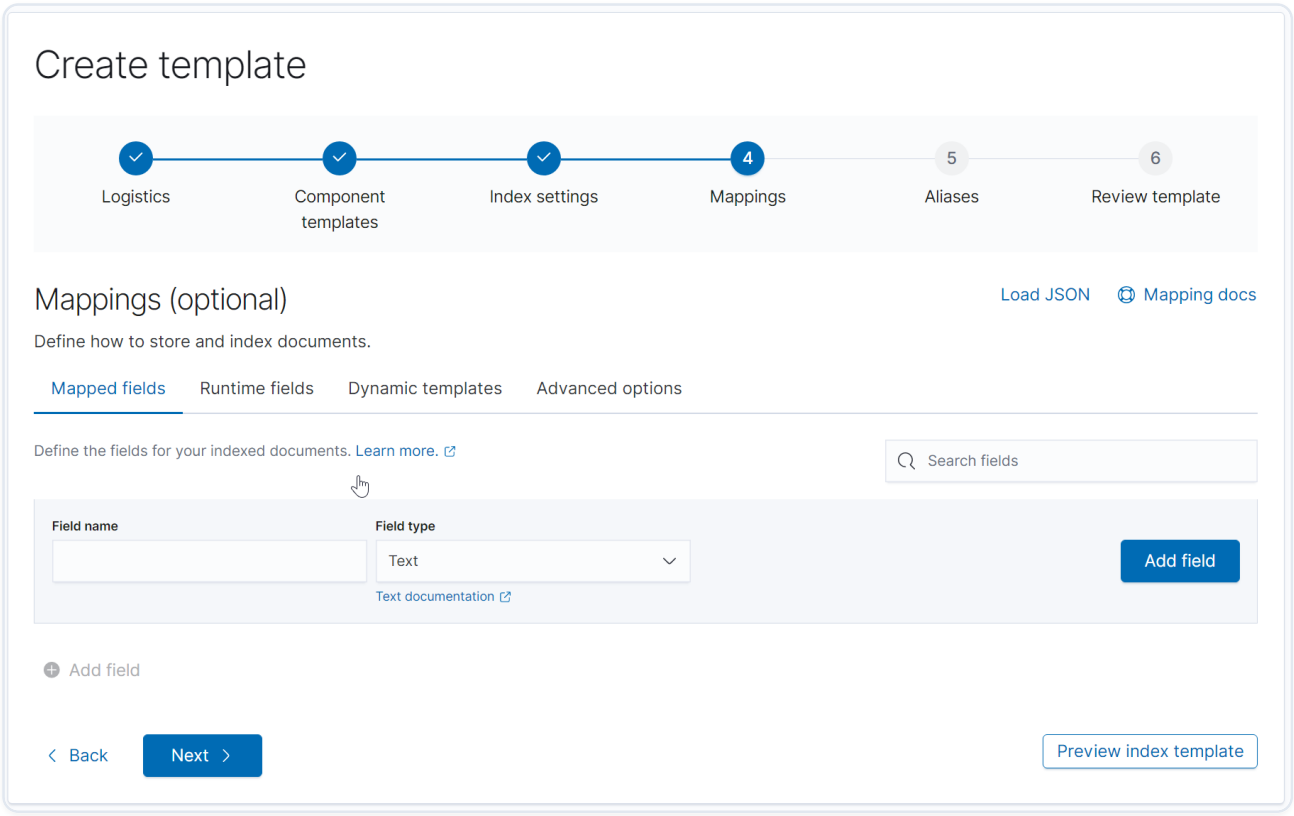


- Set `Name` to `dt_devicebasedlicensing`.
- Set `Index Patterns` to `dt_devicebasedlicensing*`.



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

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



- Proceed with `Load and overwrite`.

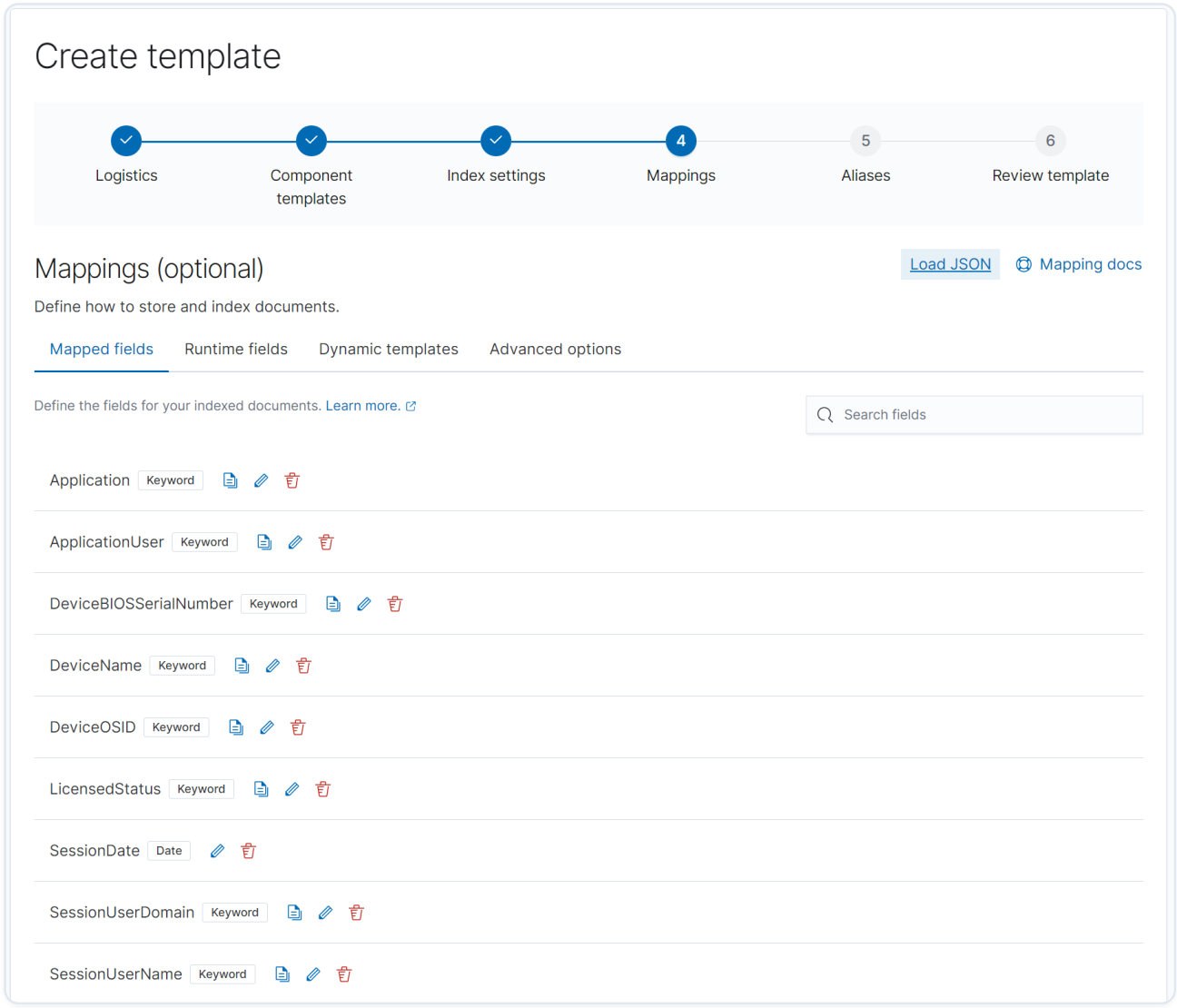
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The imported mappings are displayed. Please review them carefully.

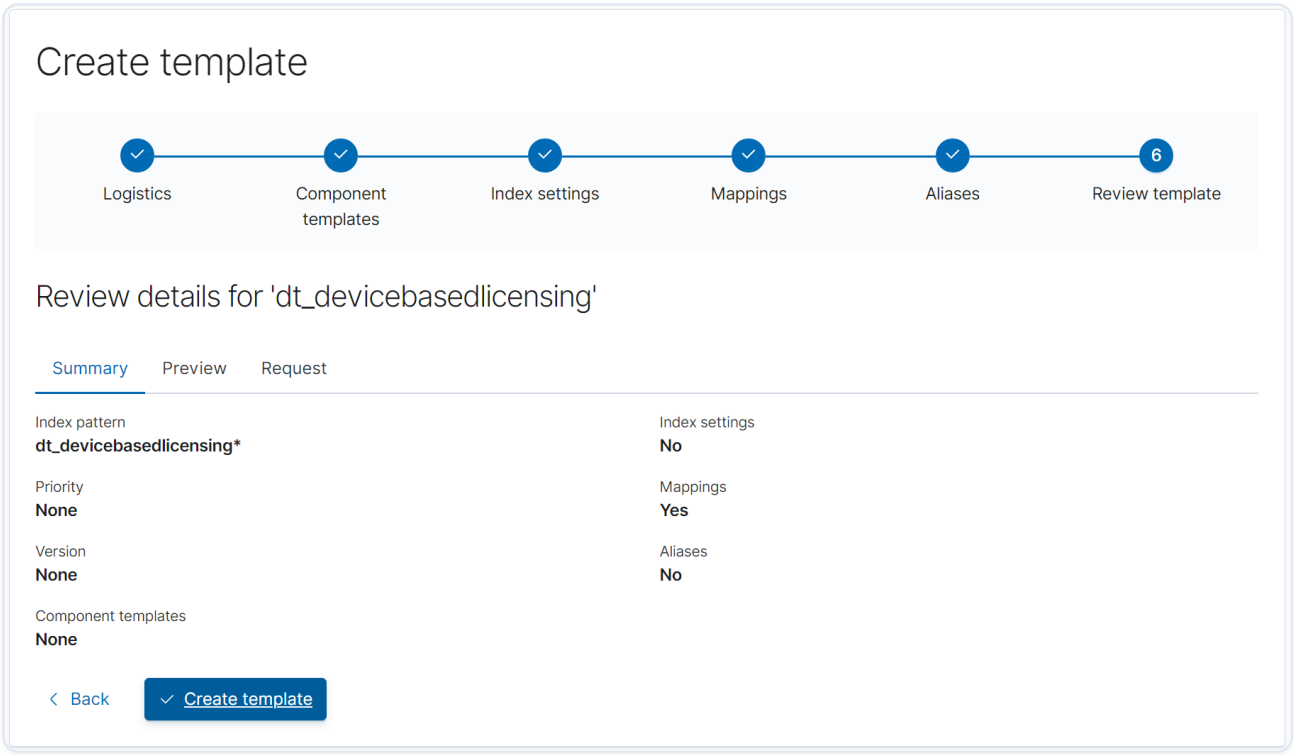
- `SessionDate` needs to be recognized as type `Date` for the report to function properly.

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

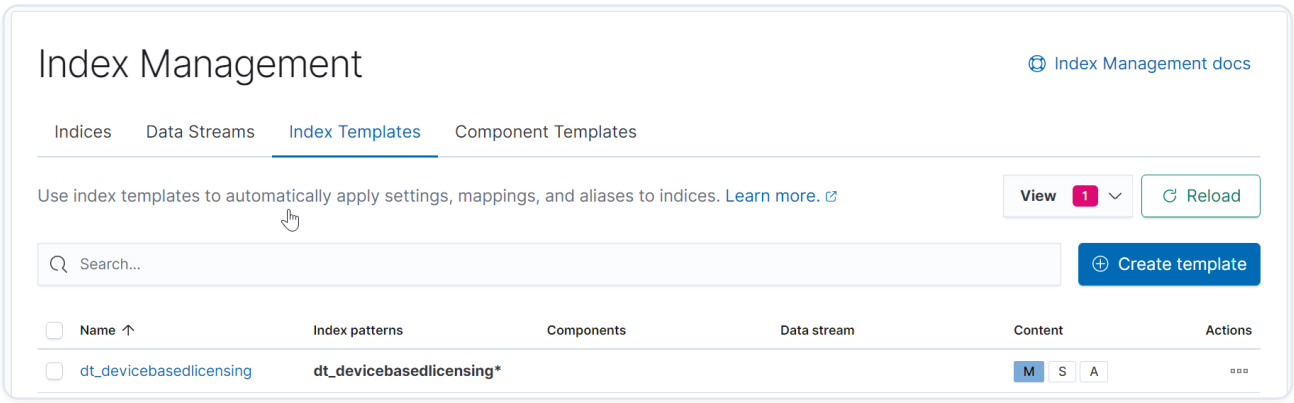


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.

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



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

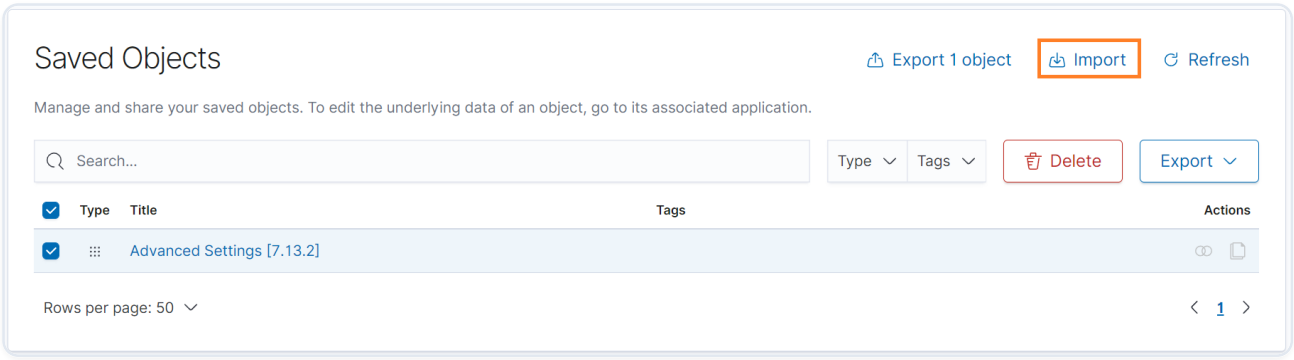


Step 2.2: Import Saved Objects to ELK Stack

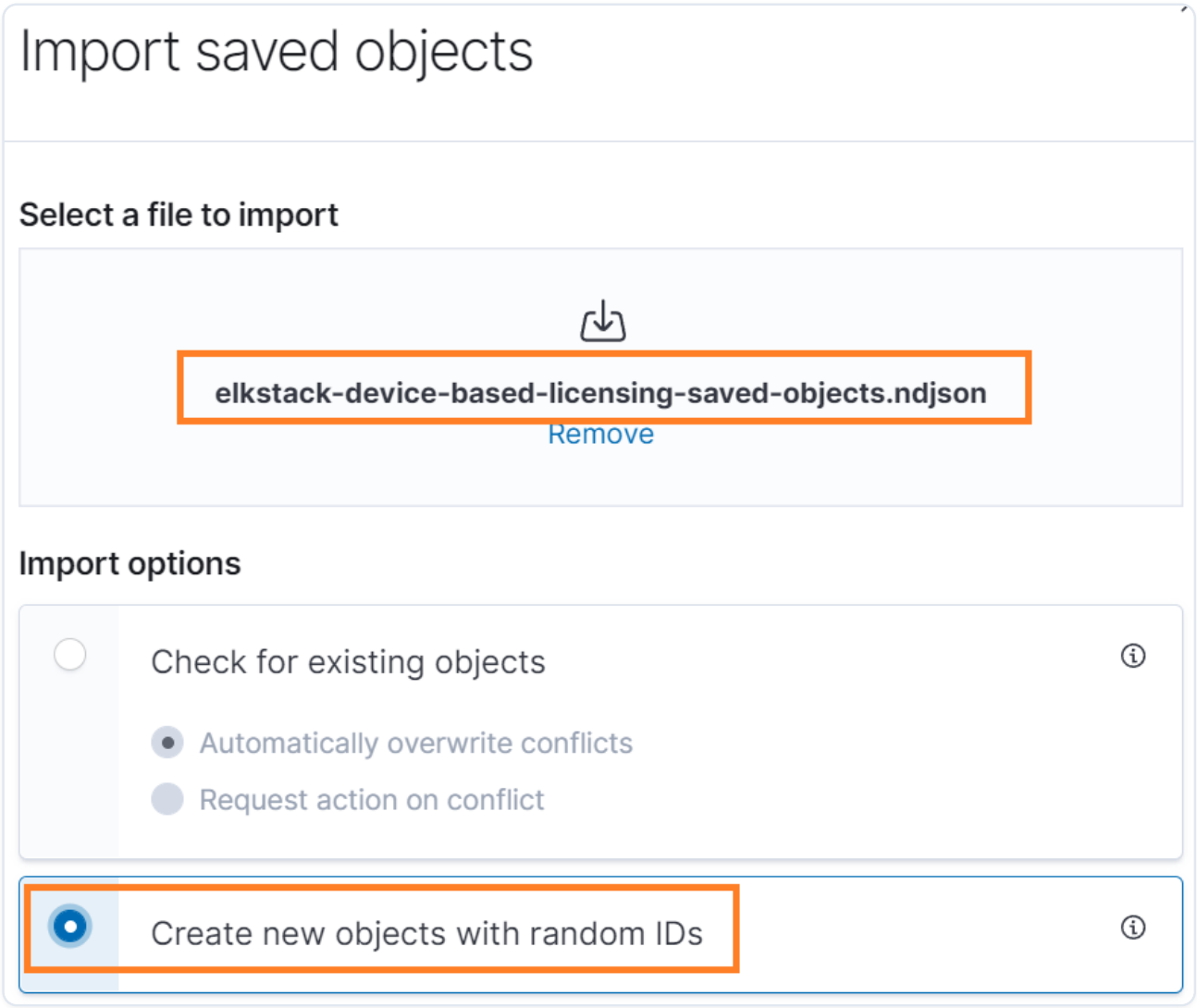
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

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

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

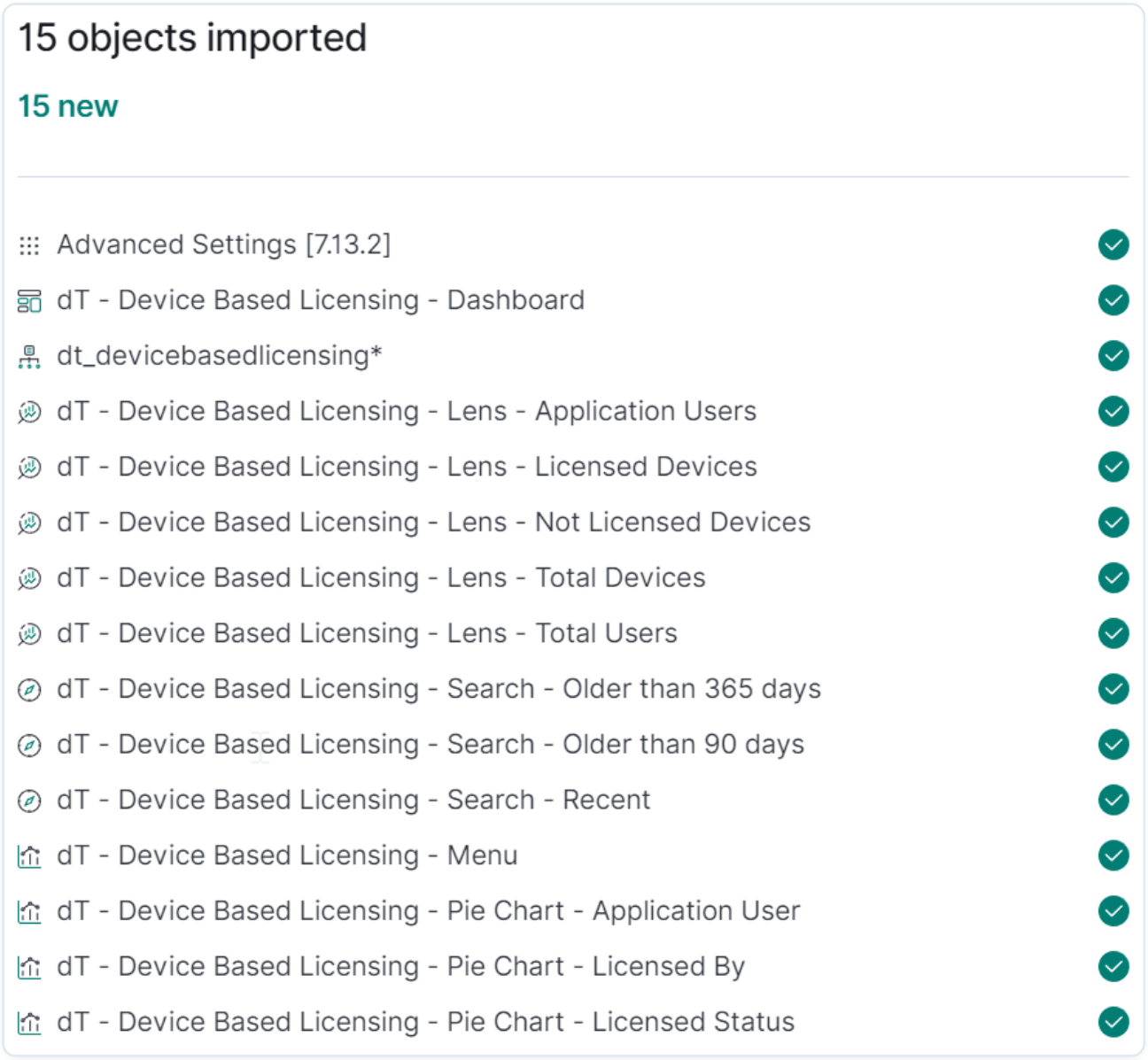


- Select the file `elkstack-device-based-licensing-saved-objects.ndjson`.
- Check `Create new objects with random IDs` to make sure no existing objects are altered.



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

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



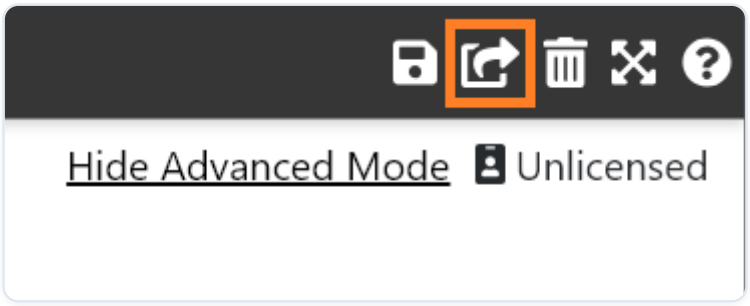
Step 2.3: Configuring deviceTRUST

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

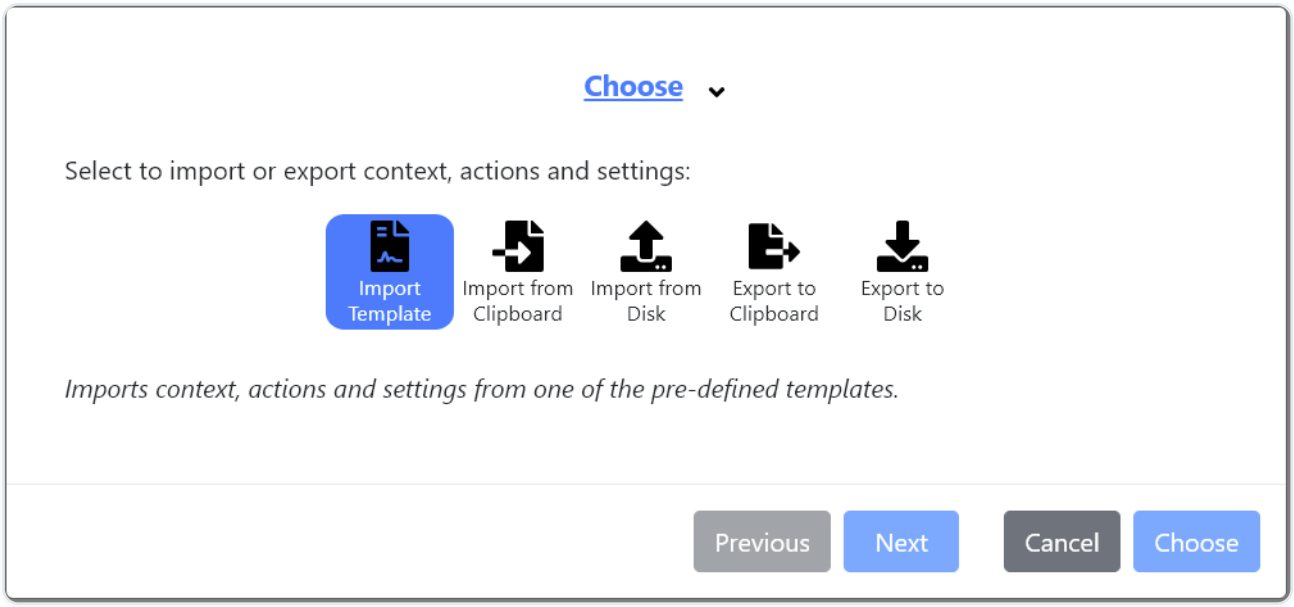
The final step is to create the deviceTRUST configuration that will make sure all the required data is provided.

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

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

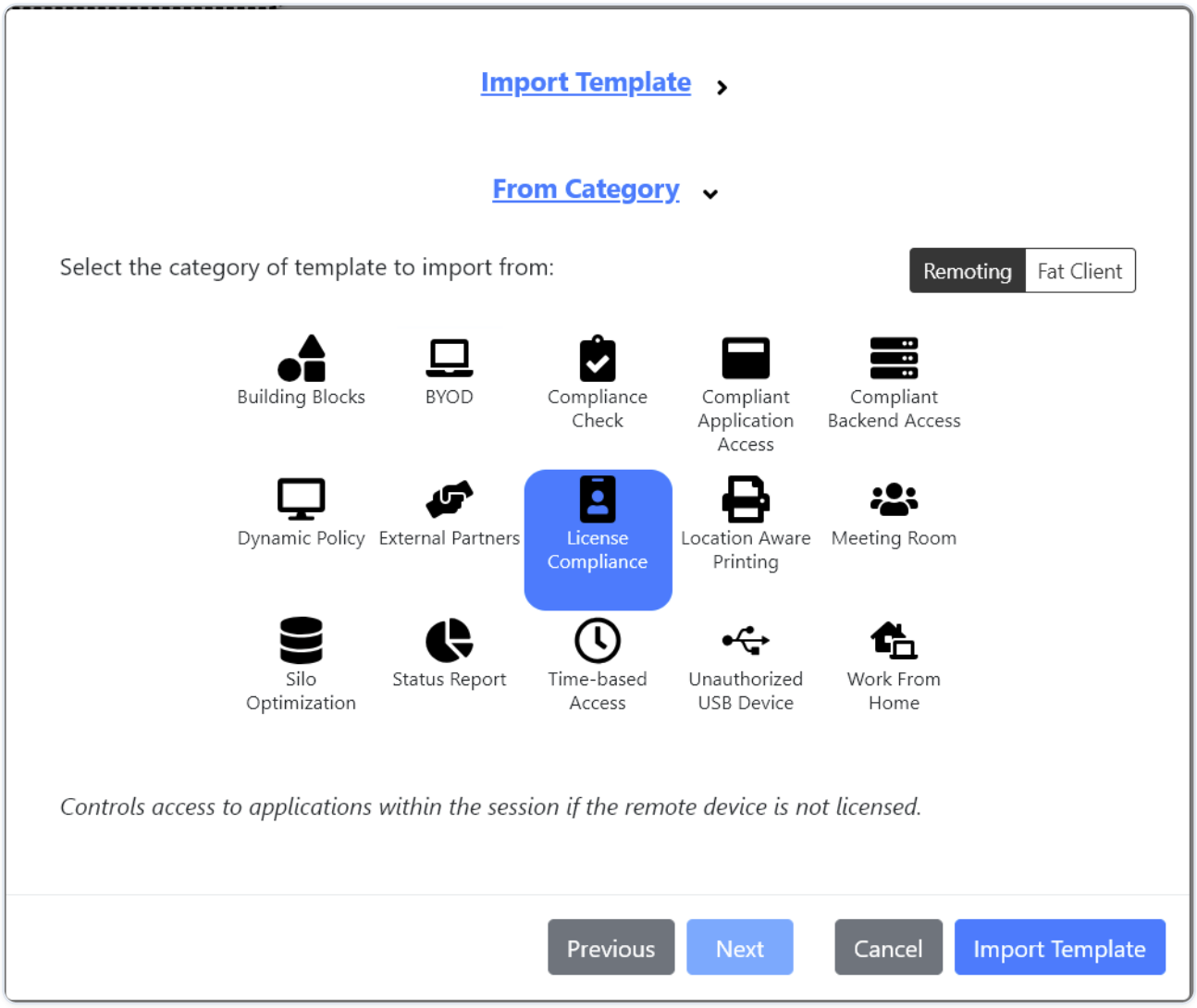


- Select `Import Template`.



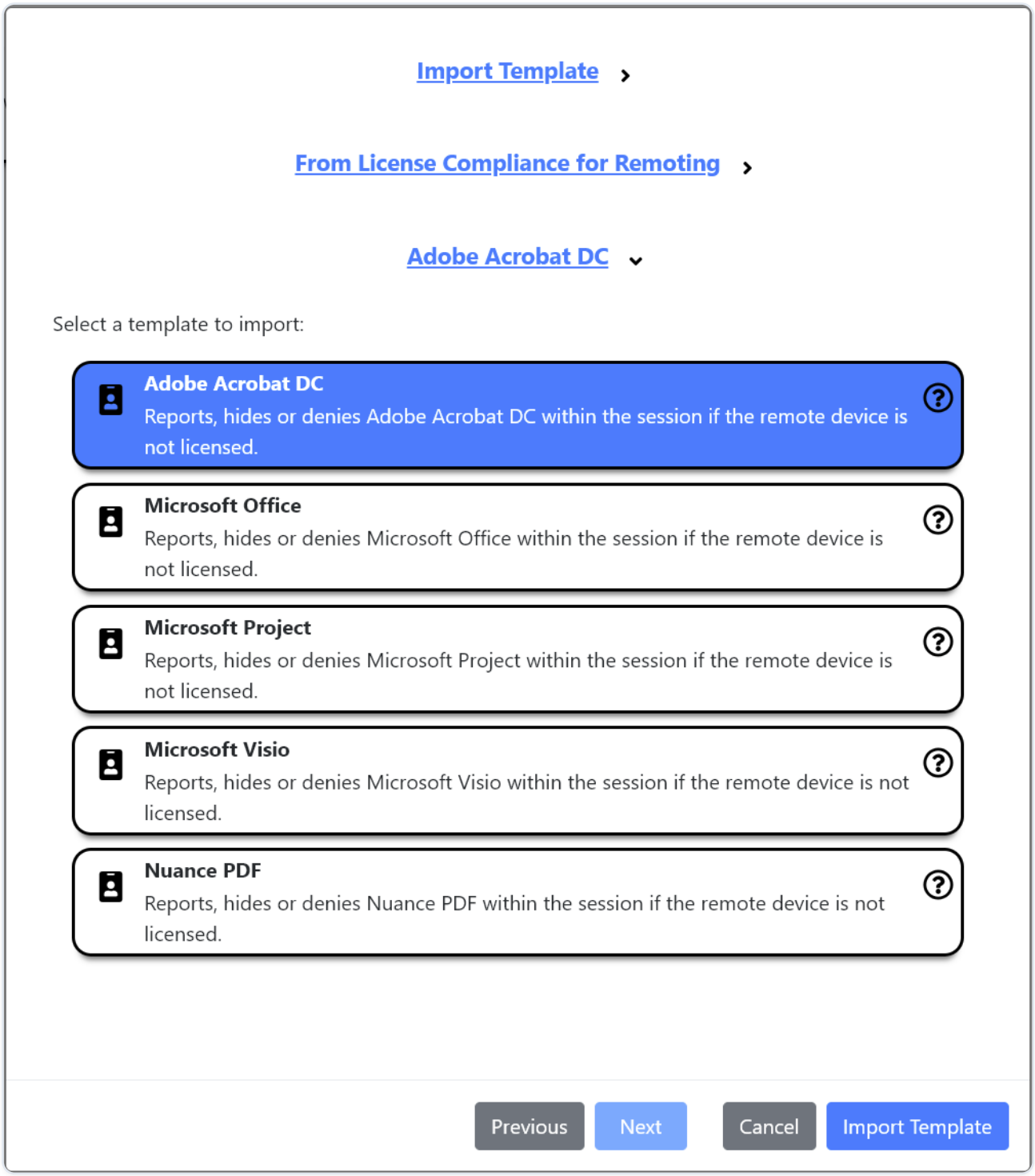
- For `Device-Based Licensing`, the template category `License Compliance` is used.

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



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

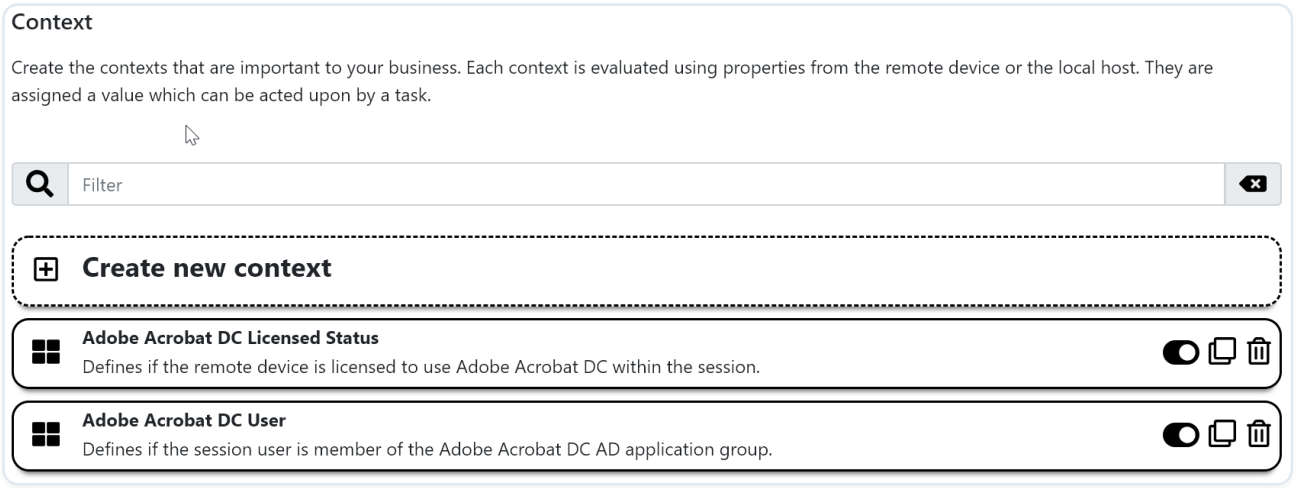
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Two contexts are included:

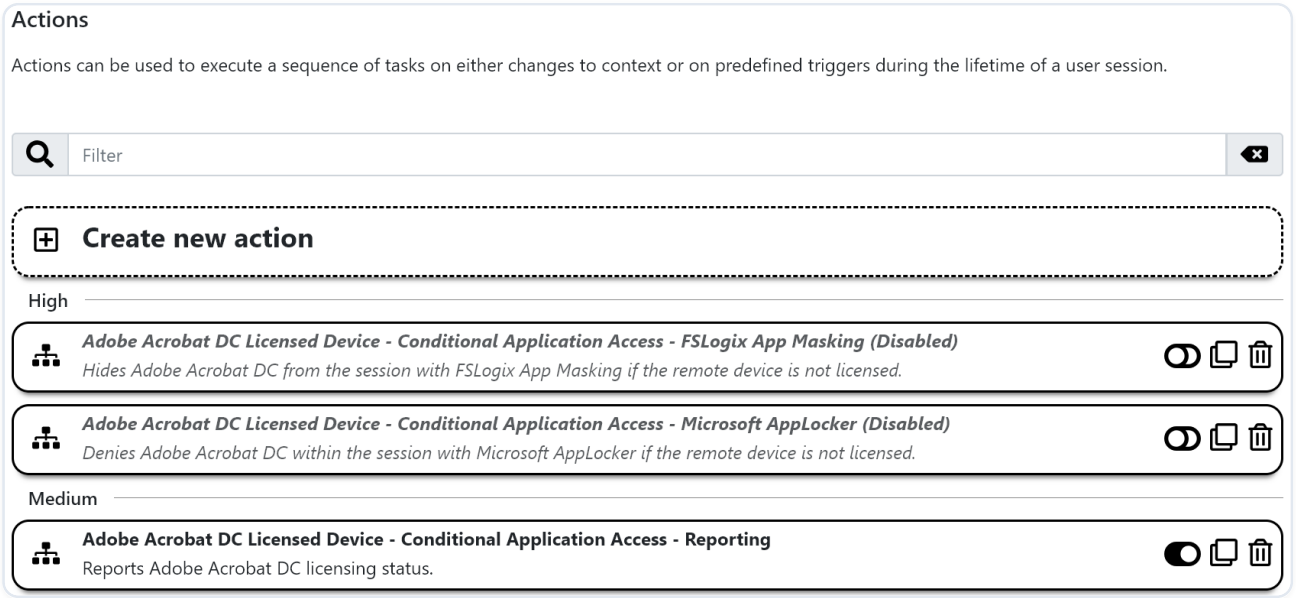
- `Adobe Acrobat DC Licensed Status` to evaluate the device's license status.
- `Adobe Acrobar DC User` to define if the accessing user shall or shall not be using the software.

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



Three actions are included:

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



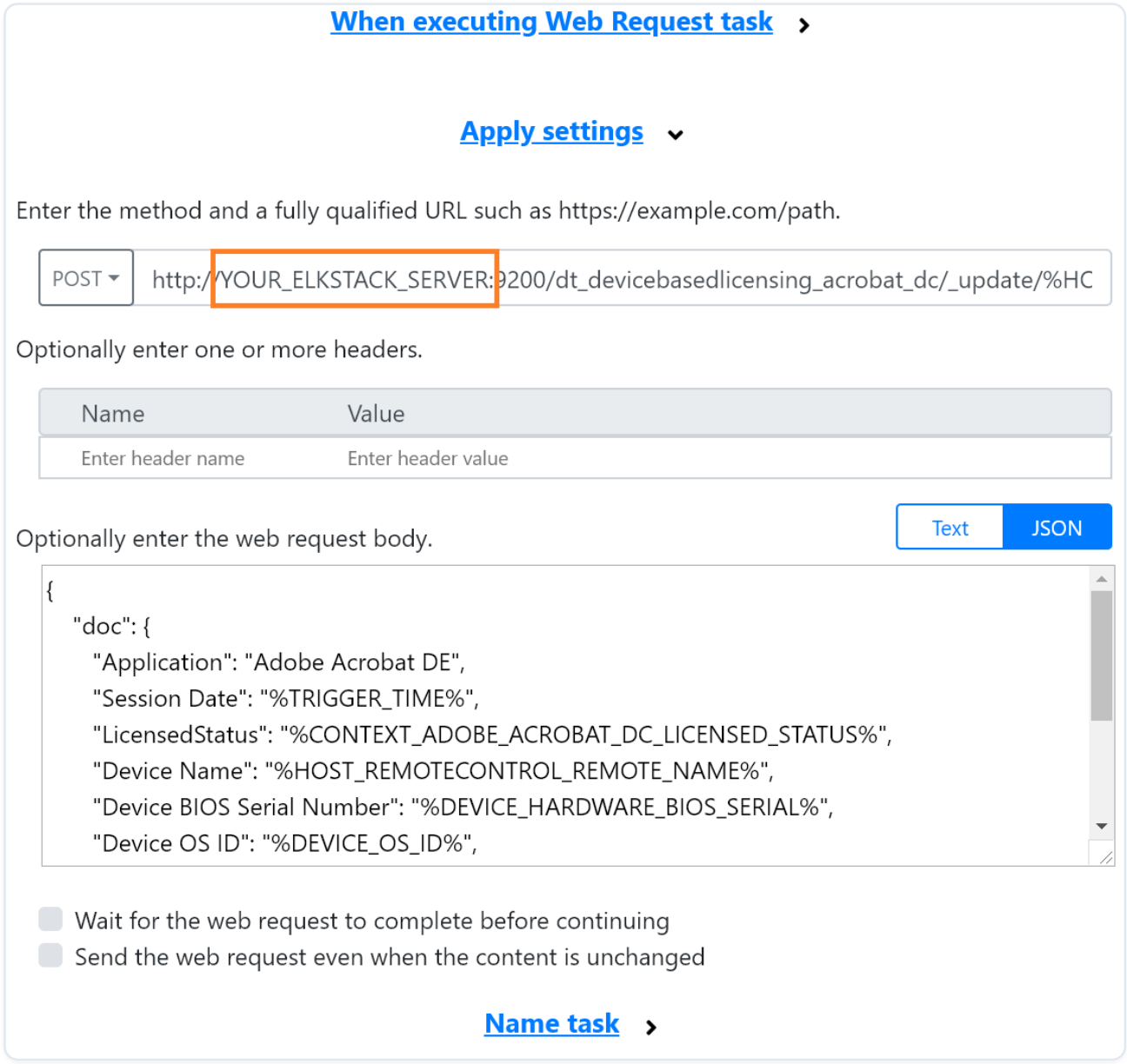
- The action contains multiple ways to store the data. Sending data to ELK Stack is configured by using a `Web Request` task. The `Audit Event`, `Custom Process`, as well as the `Web Request` Tasks for Splunk and Graylog can be deleted, as we are looking at ELK Stack here.

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



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

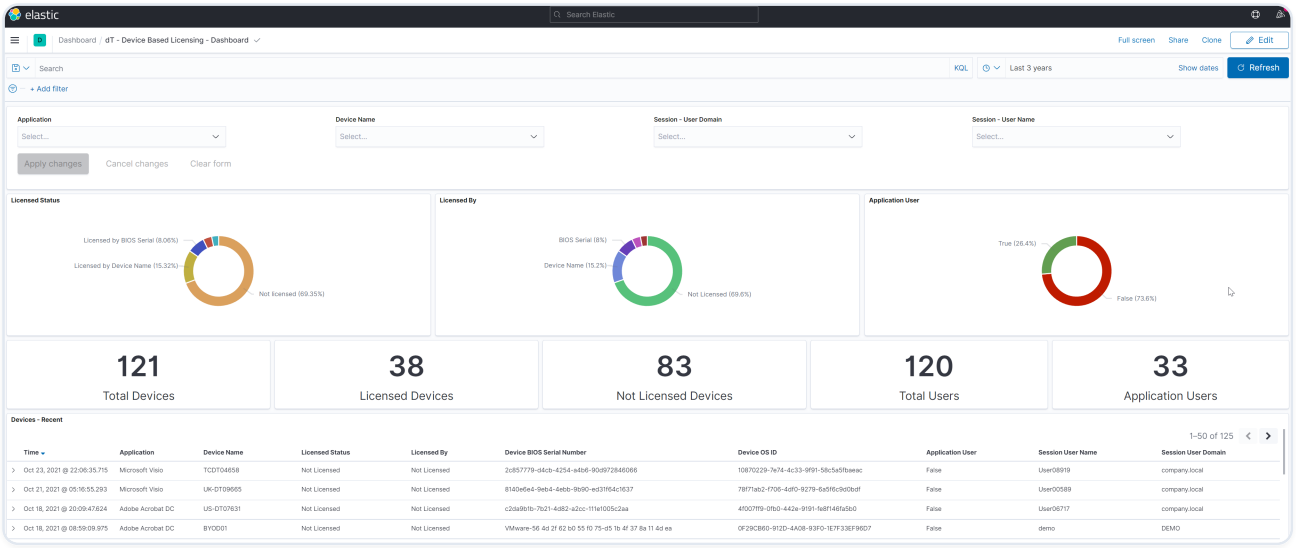
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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



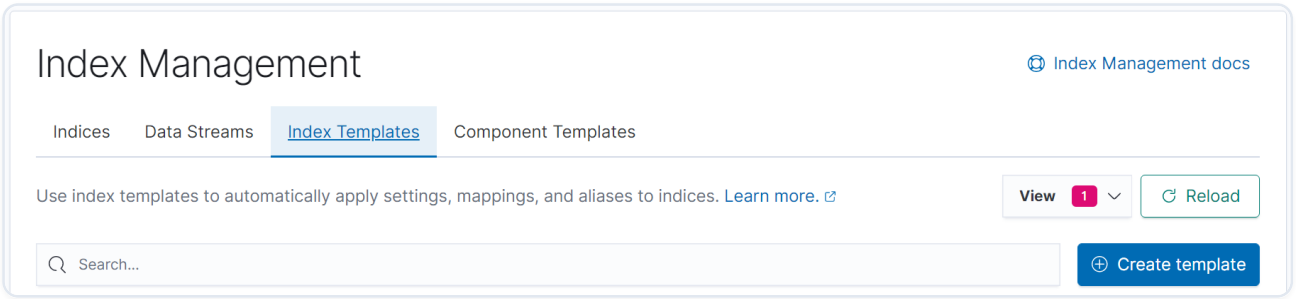
Step 3: The Status Report

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

Step 3.1: Add Index Template to ELK Stack

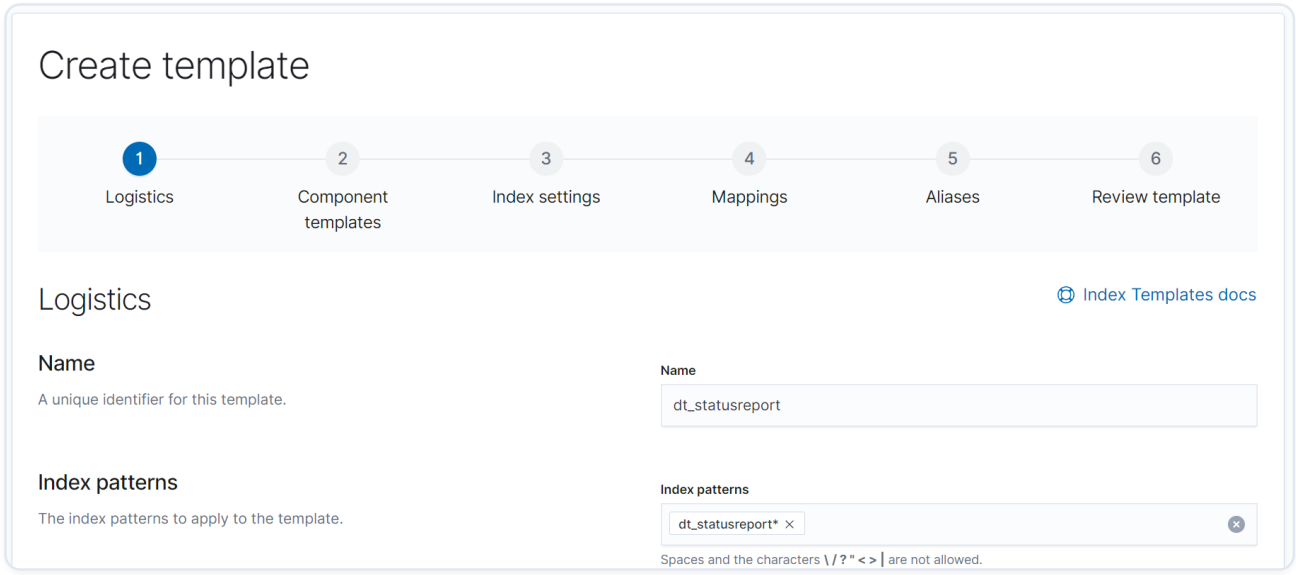
The first step is to create an `Index Template`. Index Templates describe the data that is being sent to an index. They make sure, that every date is treated according to its type.

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

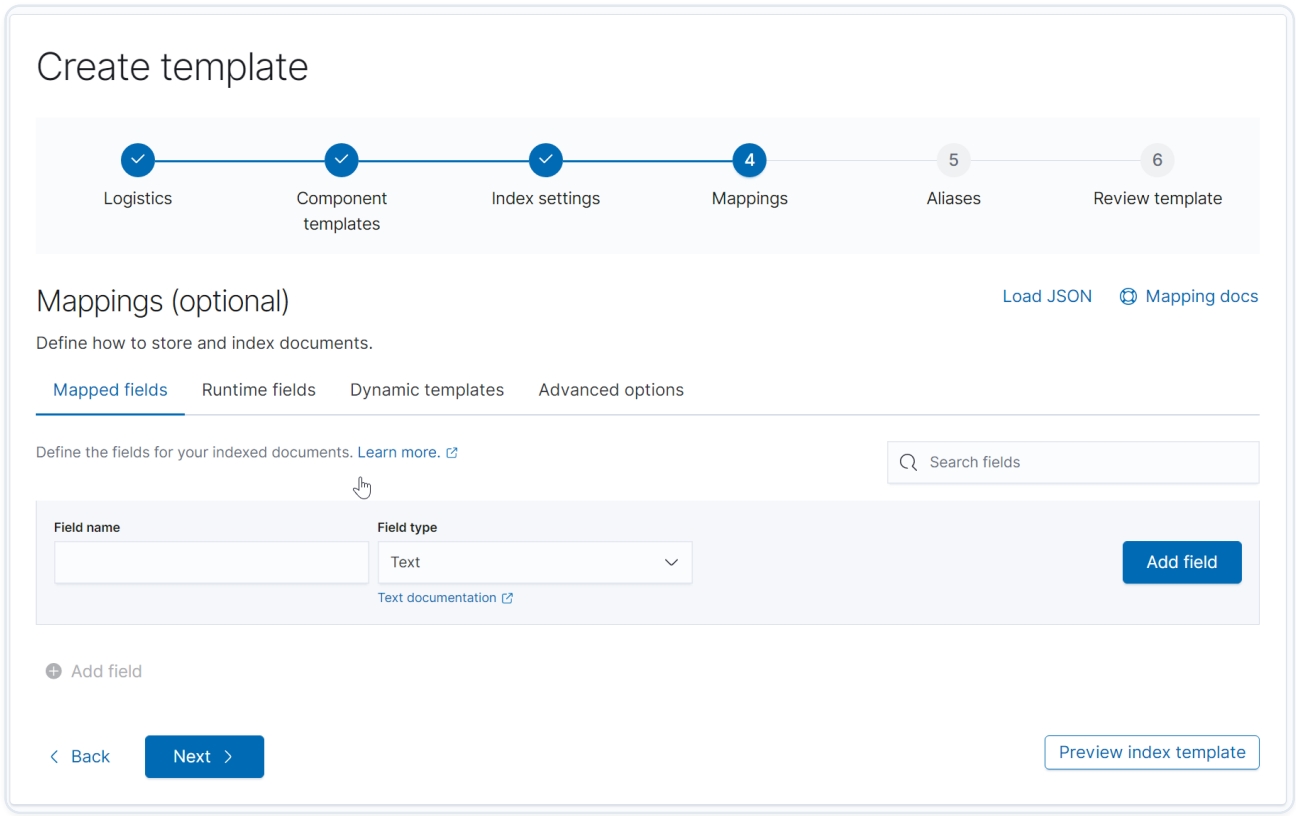


- Set `Name` to `dt_statusreport`.
- Set `Index Patterns` to `dt_statusreport*`.

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



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



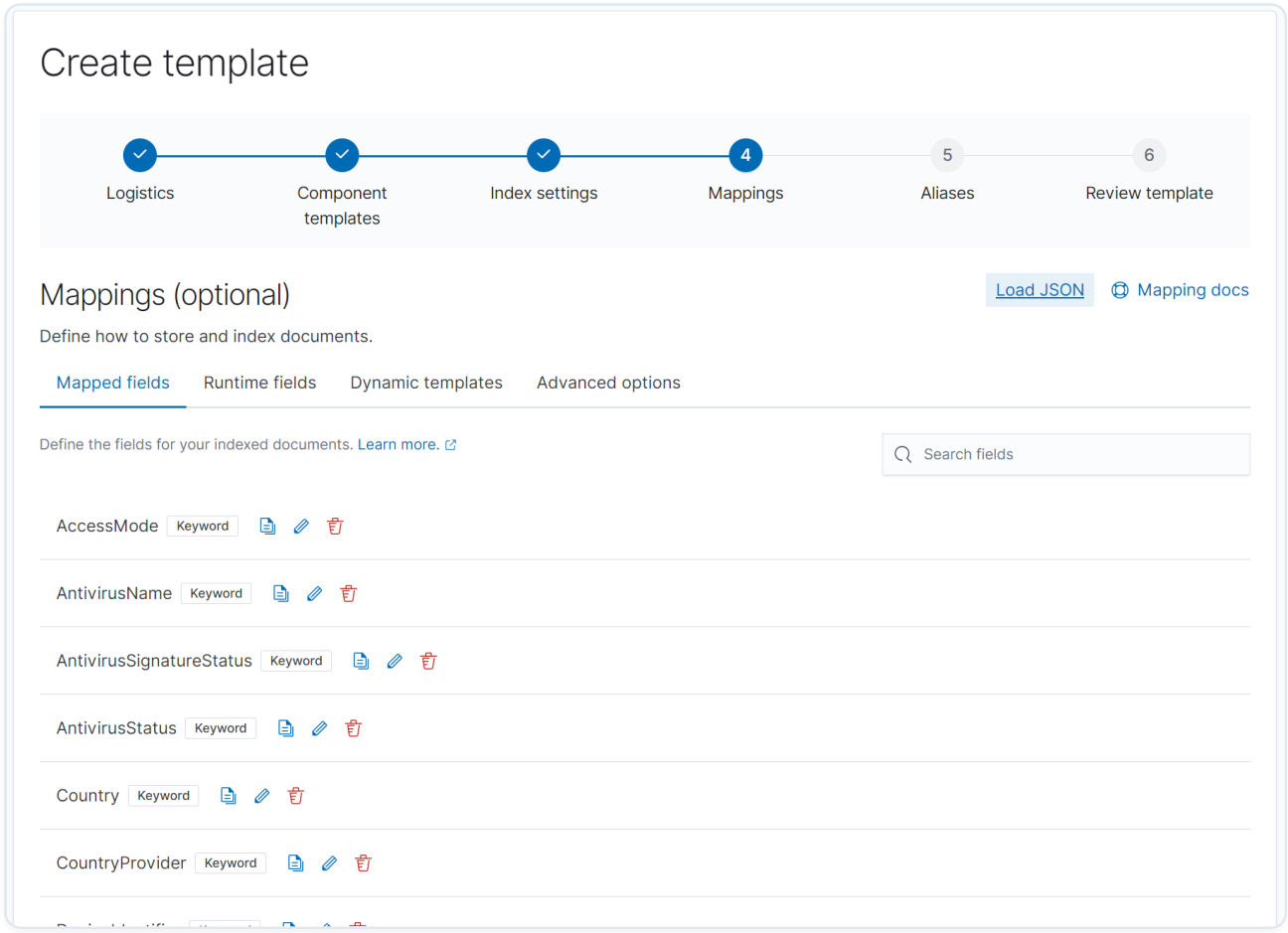
- Proceed with `Load and overwrite`.

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

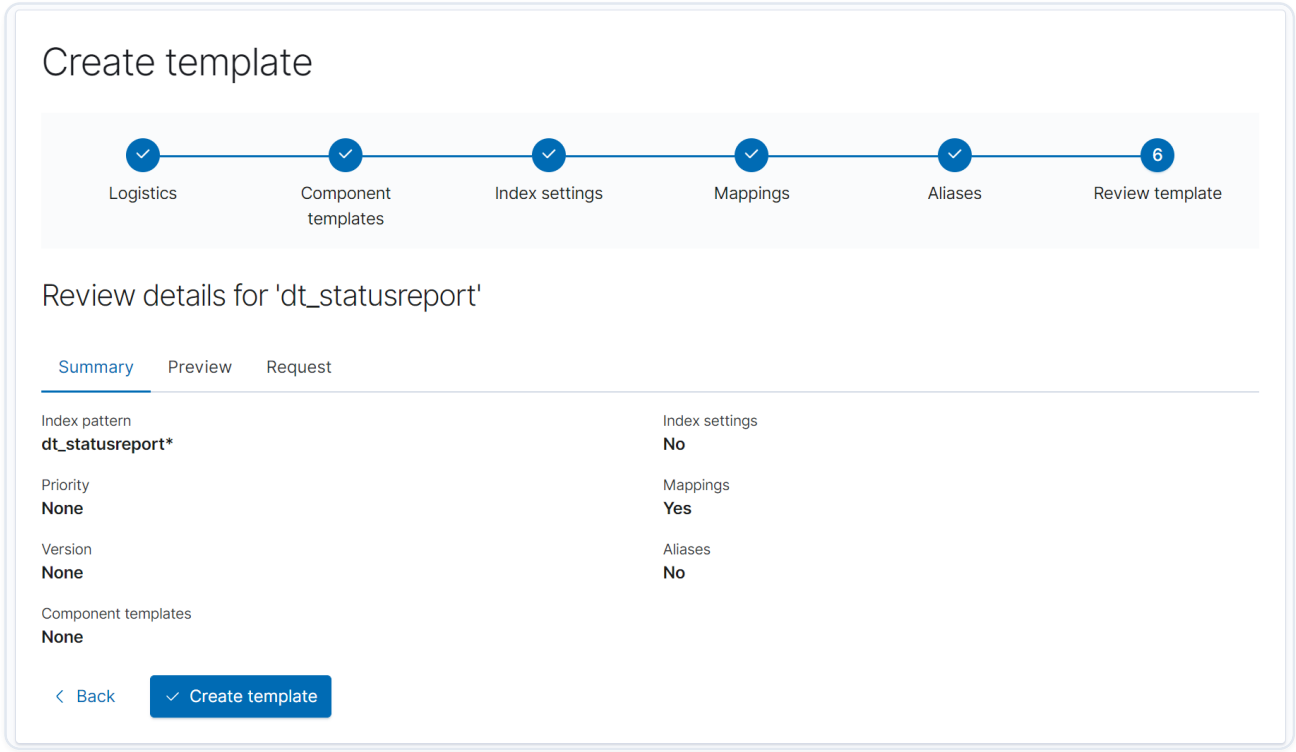


- The imported mappings are displayed. Please review them carefully. `Session Date`, `Anti-Virus Timestamp` and `Hardware BIOS Release Date` need to be recognized as type `Date` for the report to function properly.

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

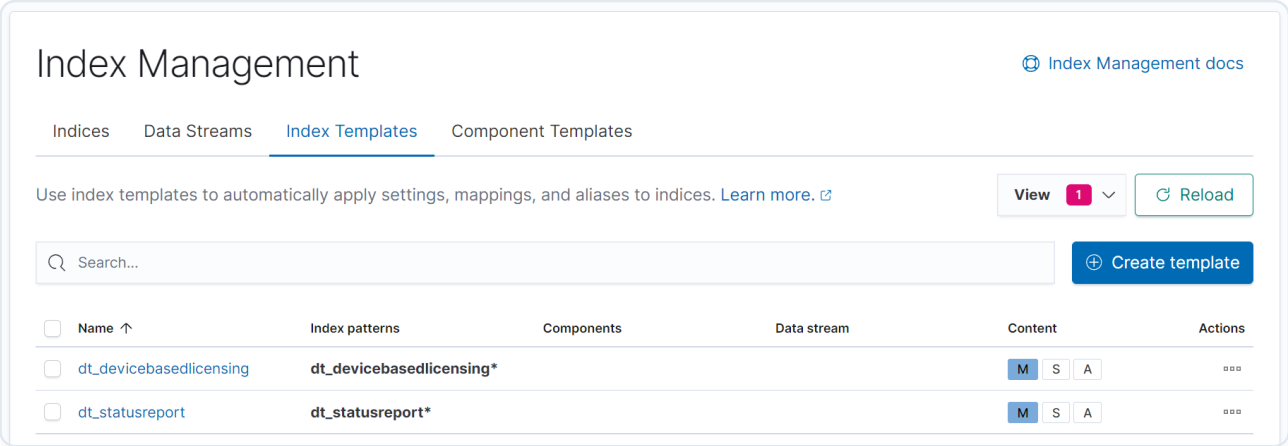


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.



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

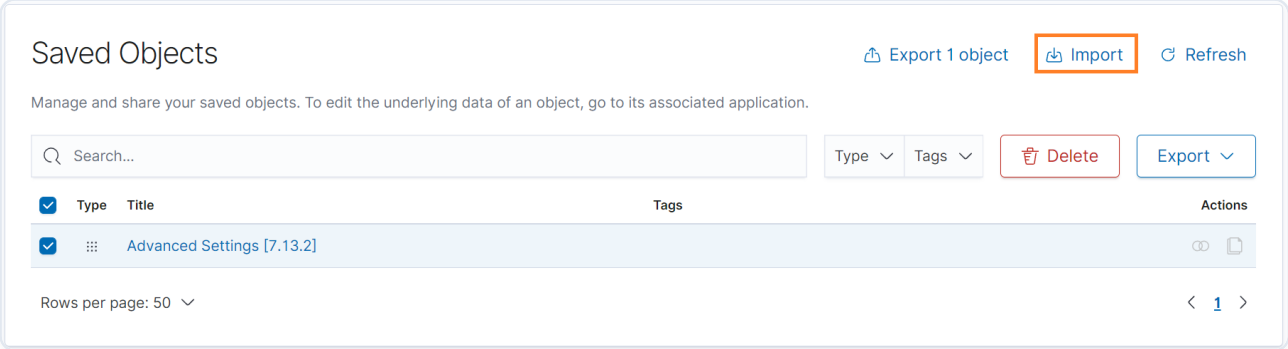
- You'll be given an overview of the created template. A blue marked `M` in the `Content` section indicates, that mappings are available.



Step 3.2: Import Saved Objects to ELK Stack

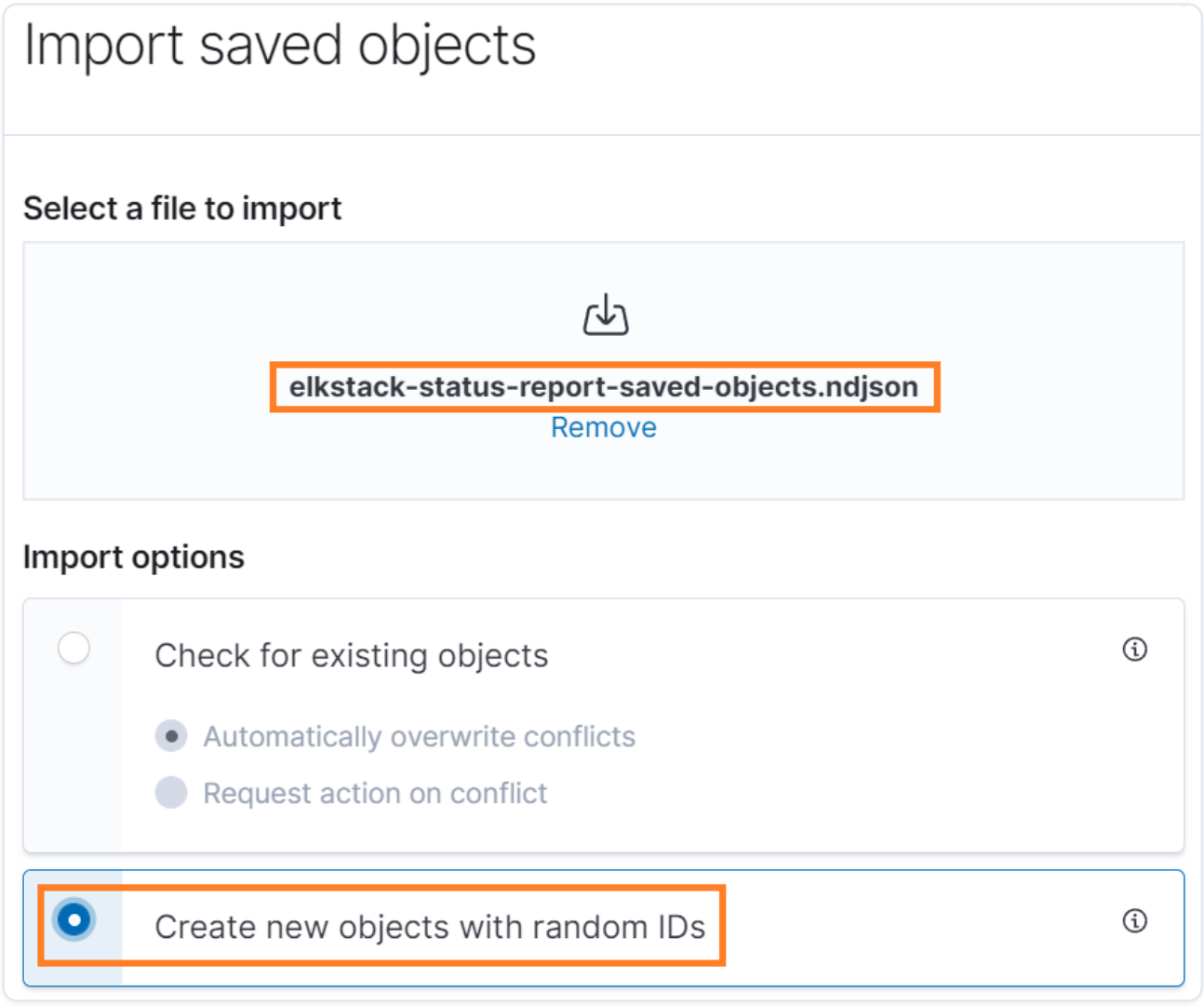
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

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



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

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



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

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

Import saved objects

60 objects imported

60 new

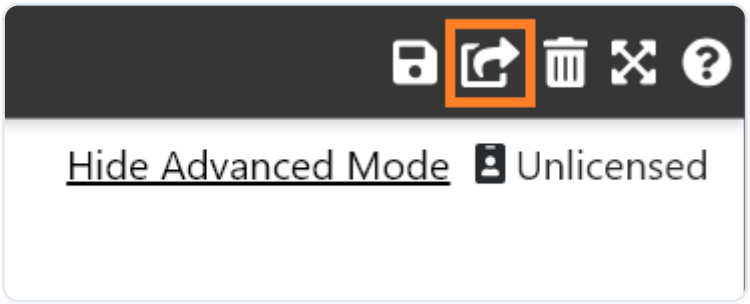
- Advanced Settings [7.13.2]
- dT - Status Report - Dashboard - Hardware
- dT - Status Report - Dashboard - Location
- dT - Status Report - Dashboard - Network
- dT - Status Report - Dashboard - OS
- dT - Status Report - Dashboard - Overview
- dT - Status Report - Dashboard - Remote User
- dT - Status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

Step 3.3: Configuring deviceTRUST

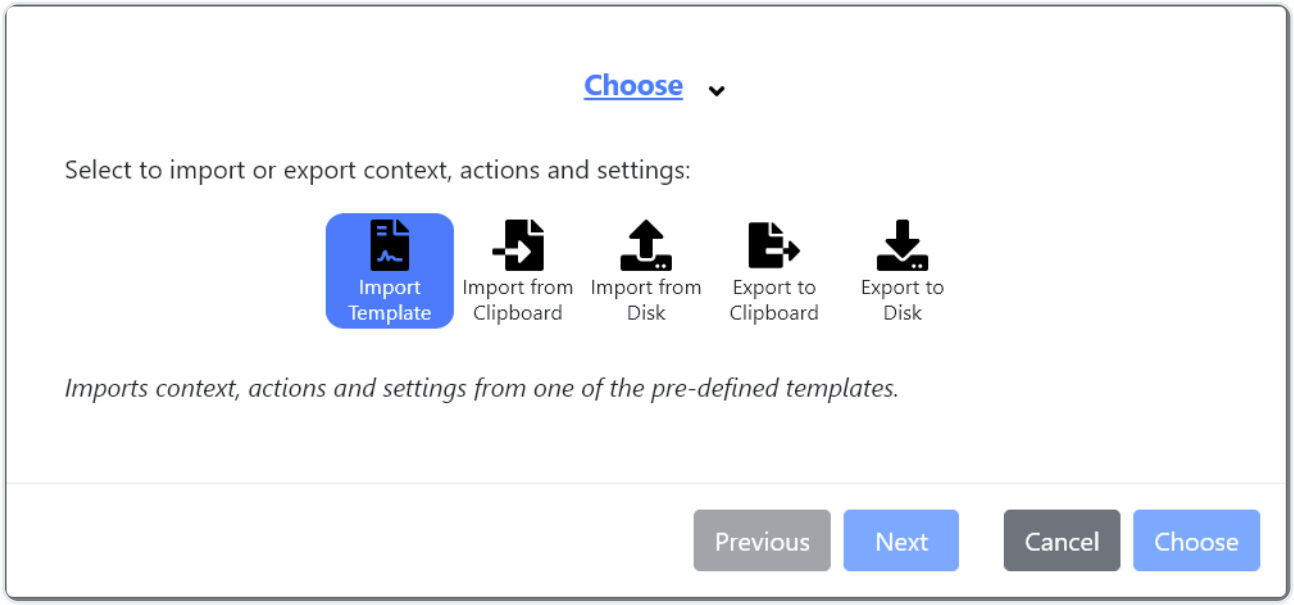
After the Index Mapping has been created, the Saved Objects are included the index has been edited and the agent-side has been configured, the ELK Stack is prepared for storing, sorting, and displaying your data.

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

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

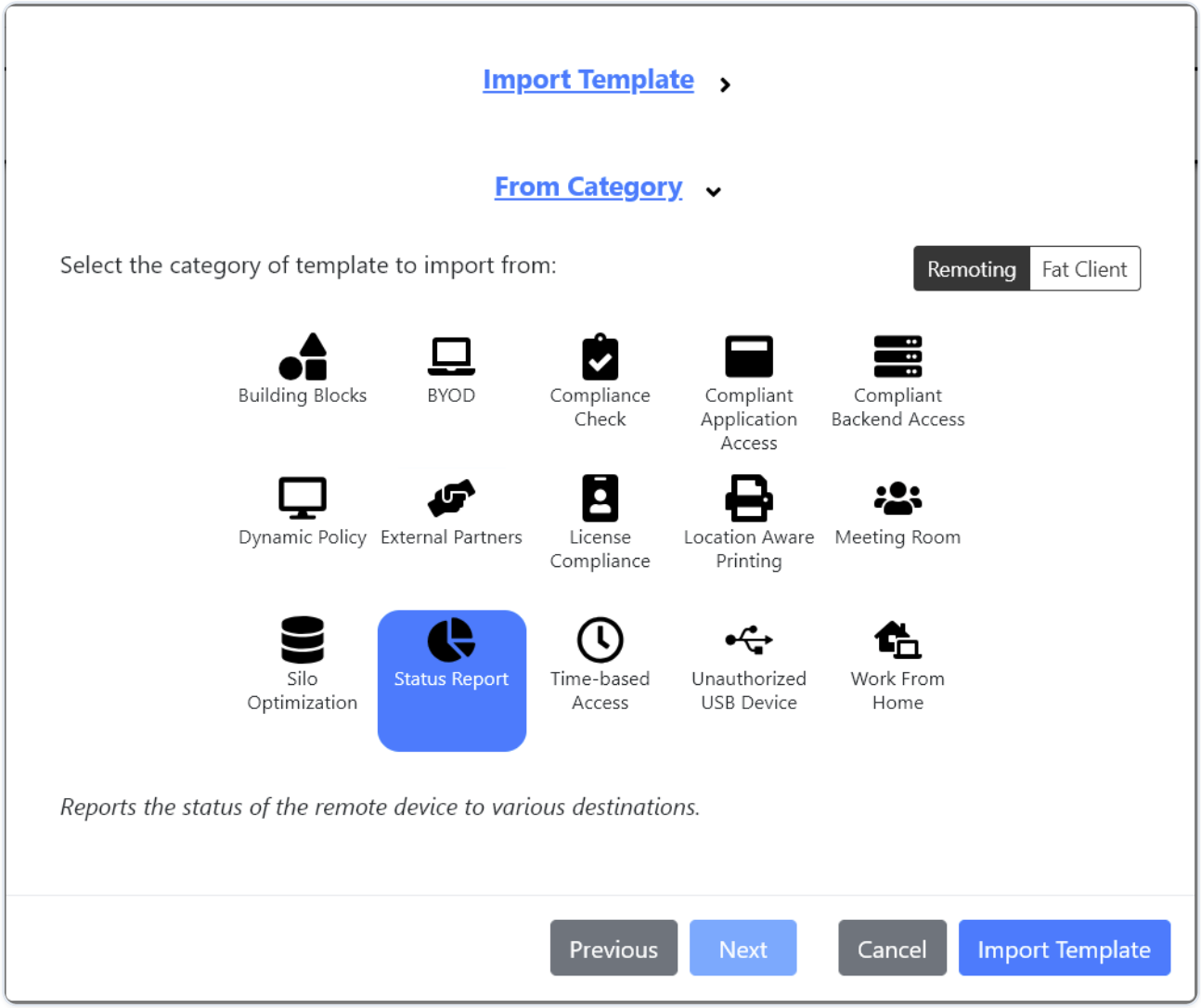


- Select `Import Template`.



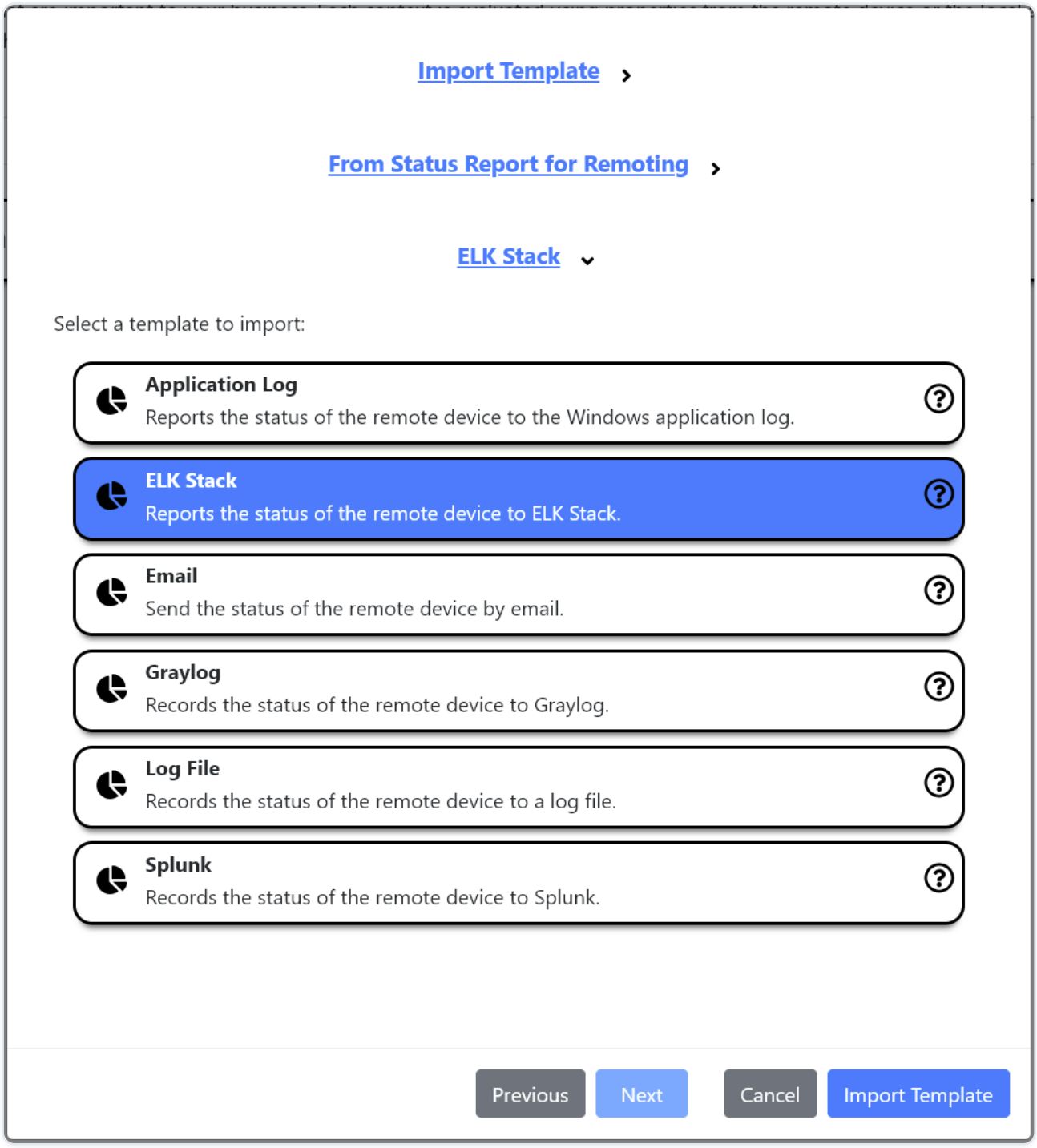
- For `Status Report`, the template category `Status Report` is used.

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



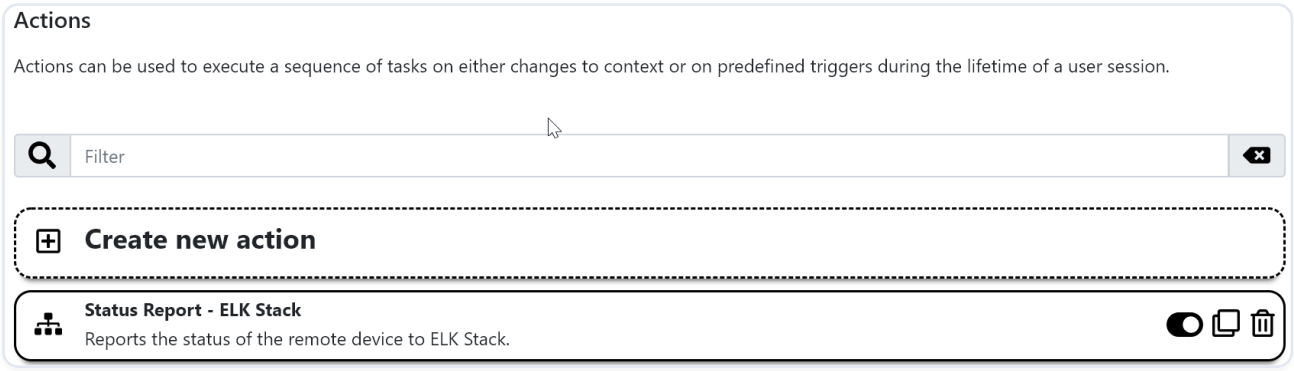
- This category contains templates for several ways of storing data. Choose `ELK Stack`.

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

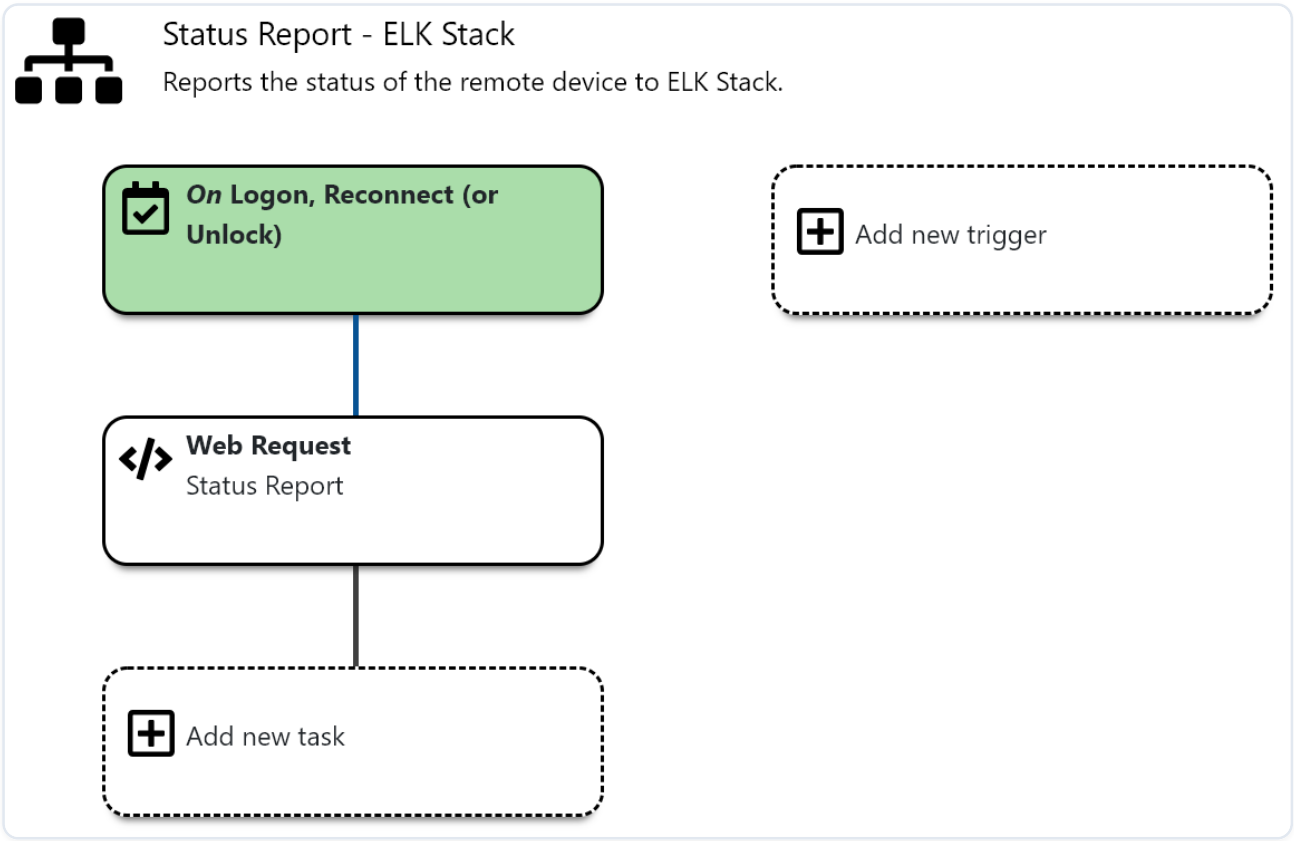


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – ELK Stack` collects all relevant data and sends them over to the ELK Stack.

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

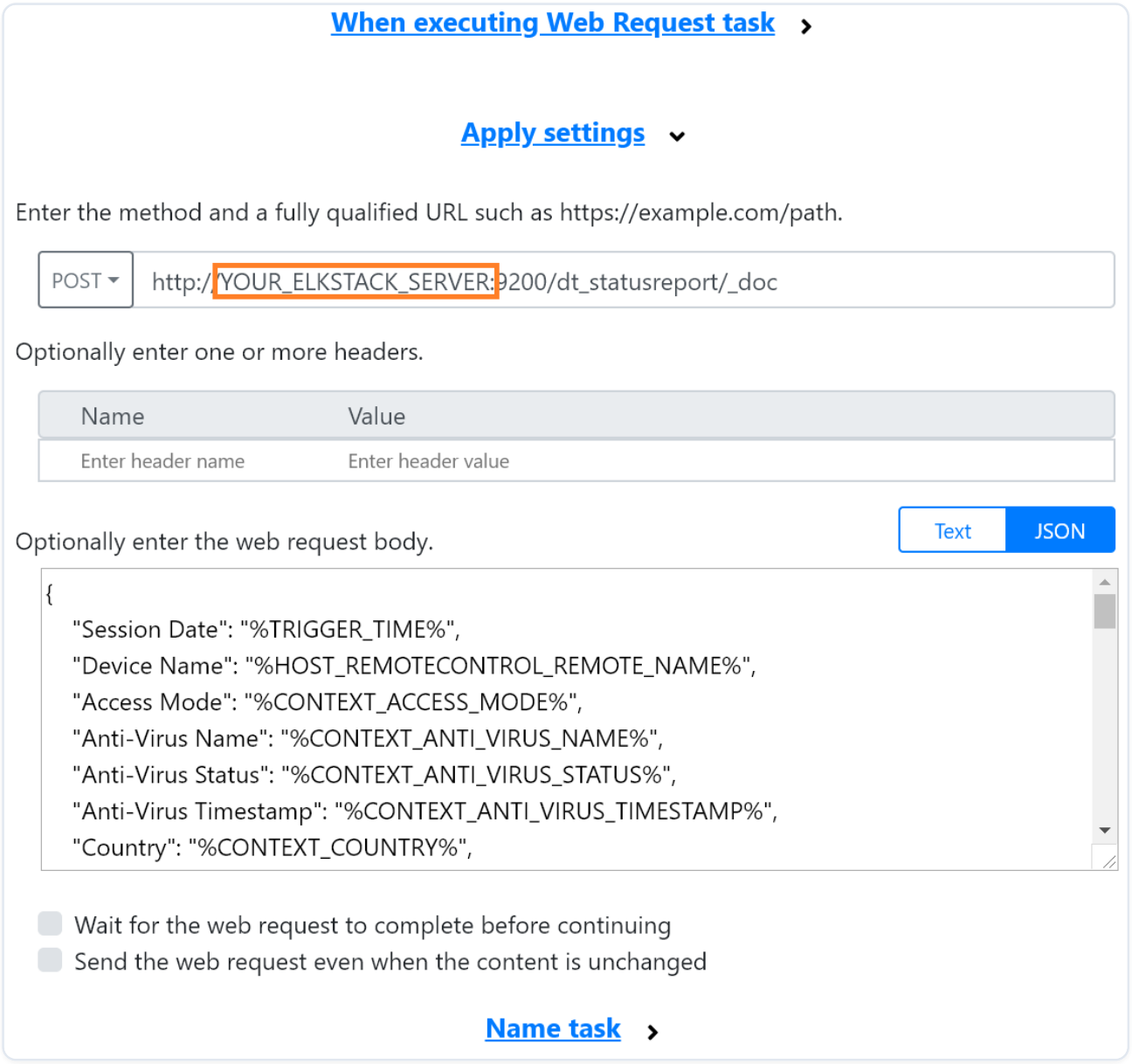


- Sending data to ELK Stack is configured by using a `Web Request` task.



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

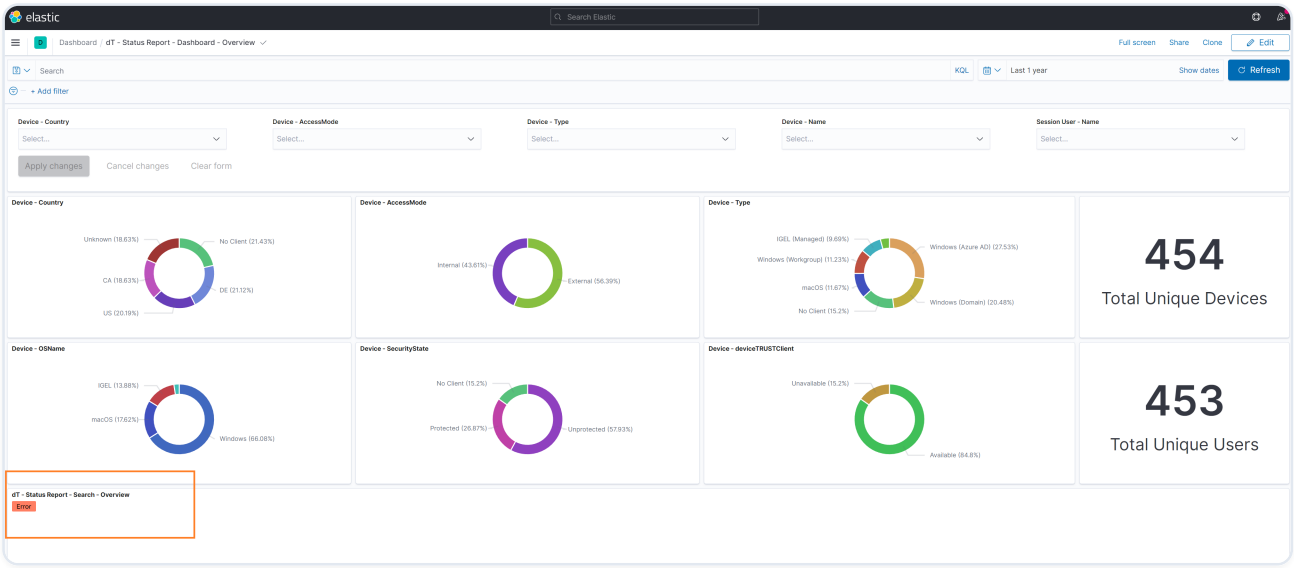
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3.4: Edit index settings

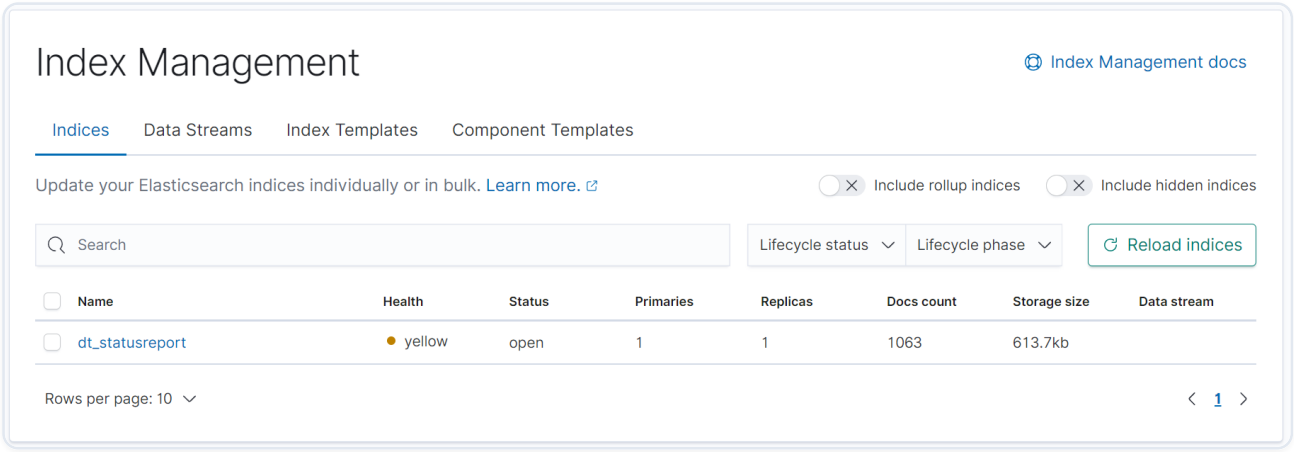
For the Status Report Dashboards to work properly, a configuration needs to be made at the index level: In a basic setting, ELK Stack allows to use 25 "calculated fields" per index. For the Status Report Dashboard, 48 calculated fields are used. Thus, the `allowed number of calculated fields` needs to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

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



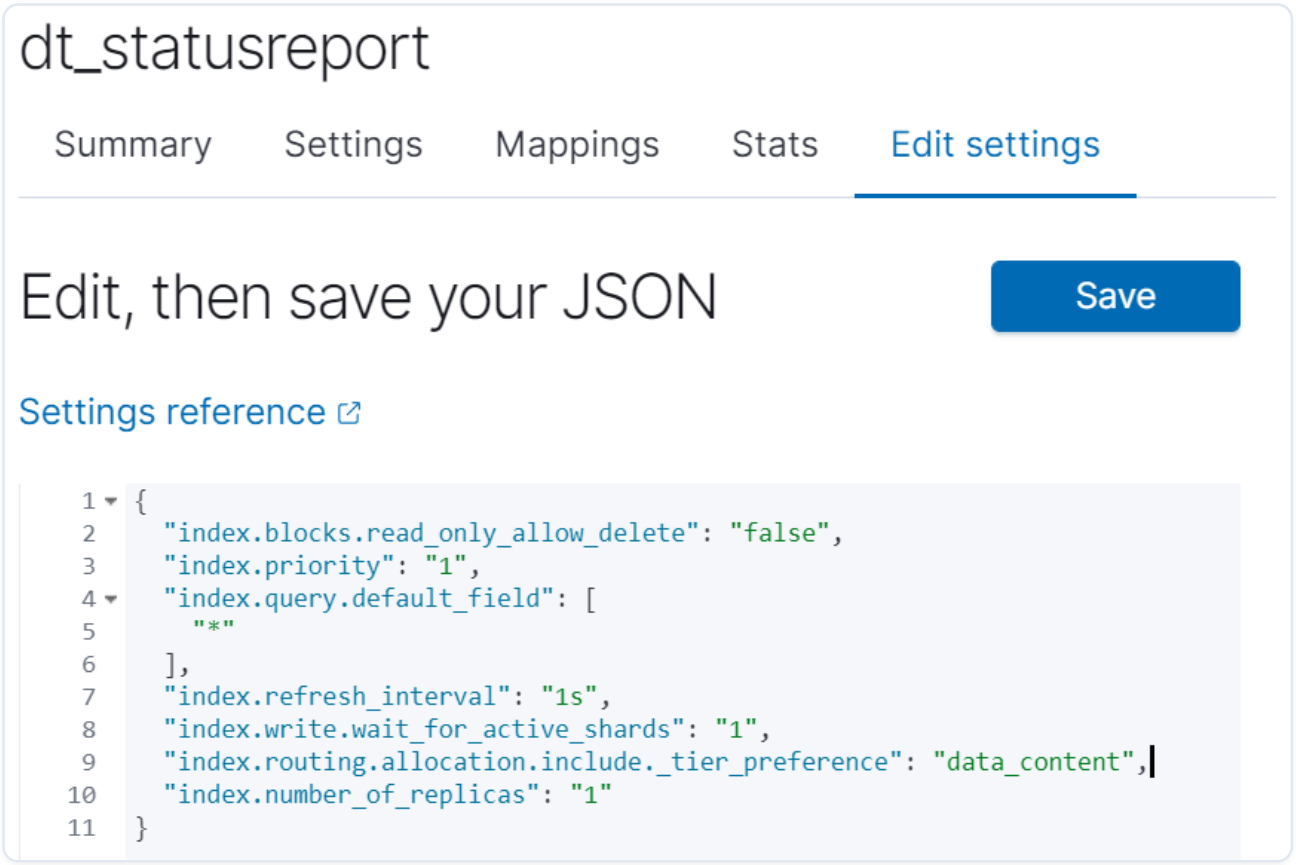
You need to send data to ELK Stack first. Sending data will create the index with basic settings. It can then be edited.

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



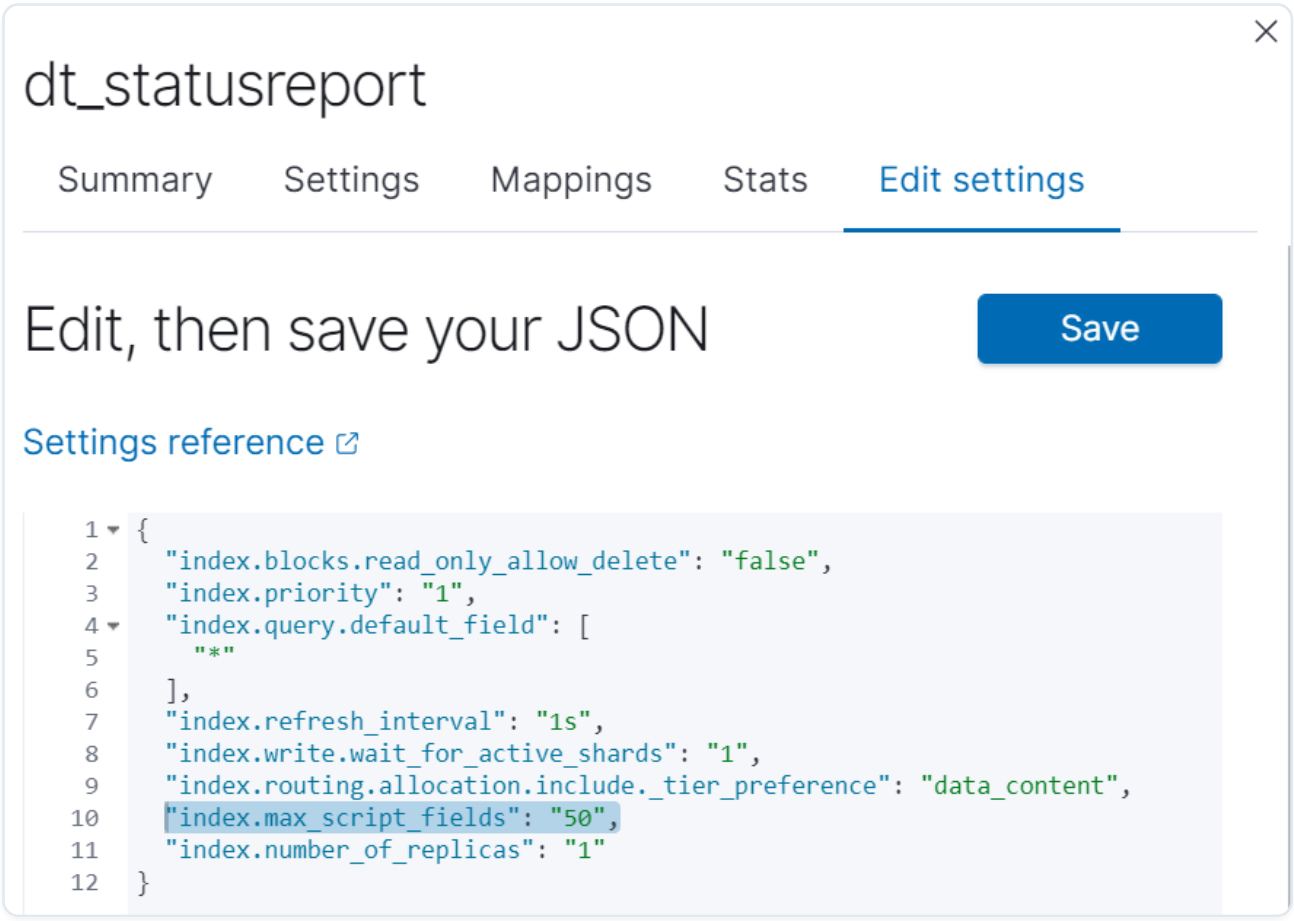
- Select the Index and chose `Edit Settings`. You'll be presented a json configuration view.

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



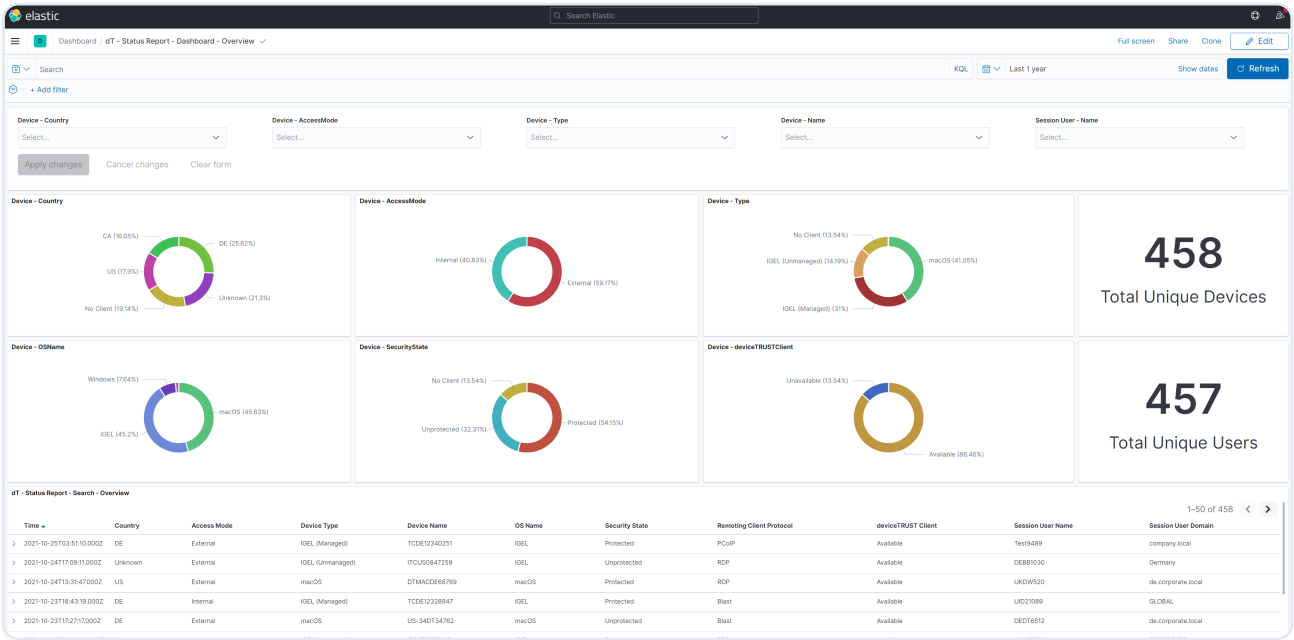
- Add `"index.max_script_fields": "50"` as a new line, making sure to keep the correct json formatting.
- Save your changes.

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



Your Dashboard will now be displayed without errors.

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



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

Reference

TABLE OF CONTENTS

- Properties
- Agent
- Console

Properties

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

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

- 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.
- 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.
- OS Properties - Provides information about the operating system installed on the endpoint.
- Password Policy Properties - Describes the password policy of the logged in user.
- Performance Properties - Describes the performance of the remoting protocol.
- Power Properties - Describes the power profile of the endpoint.
- Printer Properties - Describes the printers available to the user session.
- Region Properties - Describes the regional information of the user session.
- Remote Control Properties - Determines whether the user session is being remote controlled and provides information about the remote controlling endpoint.
- Remoting Client Properties - Provides properties about the remoting client used to remote control the user session.
- Screen Saver Properties - Describes the screen saver applied to the user session.
- Security Product Properties - Provides real-time properties describing the state of the installed Antivirus, Antispyware and Firewall security products.
- Session Properties - Provides information describing the user's logon session.
- Smartcard Reader Properties - Describes the connected smart-card readers available to the user.
- User Properties - Identifies the logged in user.
- 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.

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

- Windows Firewall Properties - Provides real-time properties describing the state of the Microsoft Windows Firewall.
- Windows Registry Properties - Provides access to Windows Registry entries.
- Windows Update Properties - Describes the status of Microsoft

Agent Reference

TABLE OF CONTENTS

- Product Events - Product Events

Console Reference

TABLE OF CONTENTS

- Actions - Actions Reference
- Settings - Settings Reference

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

Troubleshooting

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

Scenario: Remote

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

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

Scenario: Local

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

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

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

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

Open a support ticket with us

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

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

Releases

TABLE OF CONTENTS

- Next Release (23.1)
- Ubuntu Client 21.1.300
- macOS Client 21.1.300
- deviceTRUST 21.1.310
- IGEL Client 21.1.310

TABLE OF CONTENTS

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

Ubuntu Client Extension 21.1.300

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

Support for VMware Horizon View

The deviceTRUST Ubuntu Client now includes support for VMware Horizon View using the Blast, PCoIP or RDP protocols. The full list of supported technologies can be found at Operating System Compatibility

Custom Properties for Linux devices

The Custom Properties Settings now supports remote Linux devices. This allows a custom script to be executed on the remote Linux device to return one or more properties beginning with REMOTE_CUSTOM by writing e.g. `REMOTE_CUSTOM_NAME=VALUE` to the output.

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

Minor enhancements

- Added VPN and Adapter properties to the WHOIS results.

Bug Fixes

- Fixed a potential crash during the logoff or disconnect from a session.

Compatibility

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

macOS Client Extension 21.1.300

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

Native support for Apple silicon

We've integrated native support for Apple silicon processors, such as the Apple M1 and M2, alongside our existing support for Intel processors into a single universal installation package. This removes the previous requirement for Rosetta 2 translations. A remoting client that is also built with native Apple silicon support is required, 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.

Bug Fixes

- Fixed an issue where Location properties were unavailable on macOS Ventura.
- Fixed an issue where Display properties contained unavailable Adapter and Monitor products and vendor properties on Apple silicon processors on macOS Ventura.
- Fixed a potential crash during shutdown of the remoting client.

Compatibility

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

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

deviceTRUST 21.1 SP2 (version 21.1.310)

This service pack release includes minor features and bug fixes to the deviceTRUST Console, Agent and Client Extension for Microsoft Windows. See deviceTRUST 21.1.210 release notes for full details of the changes introduced in 21.1.210. Please refer to Compatibility for changes that may impact users upgrading from previous releases.

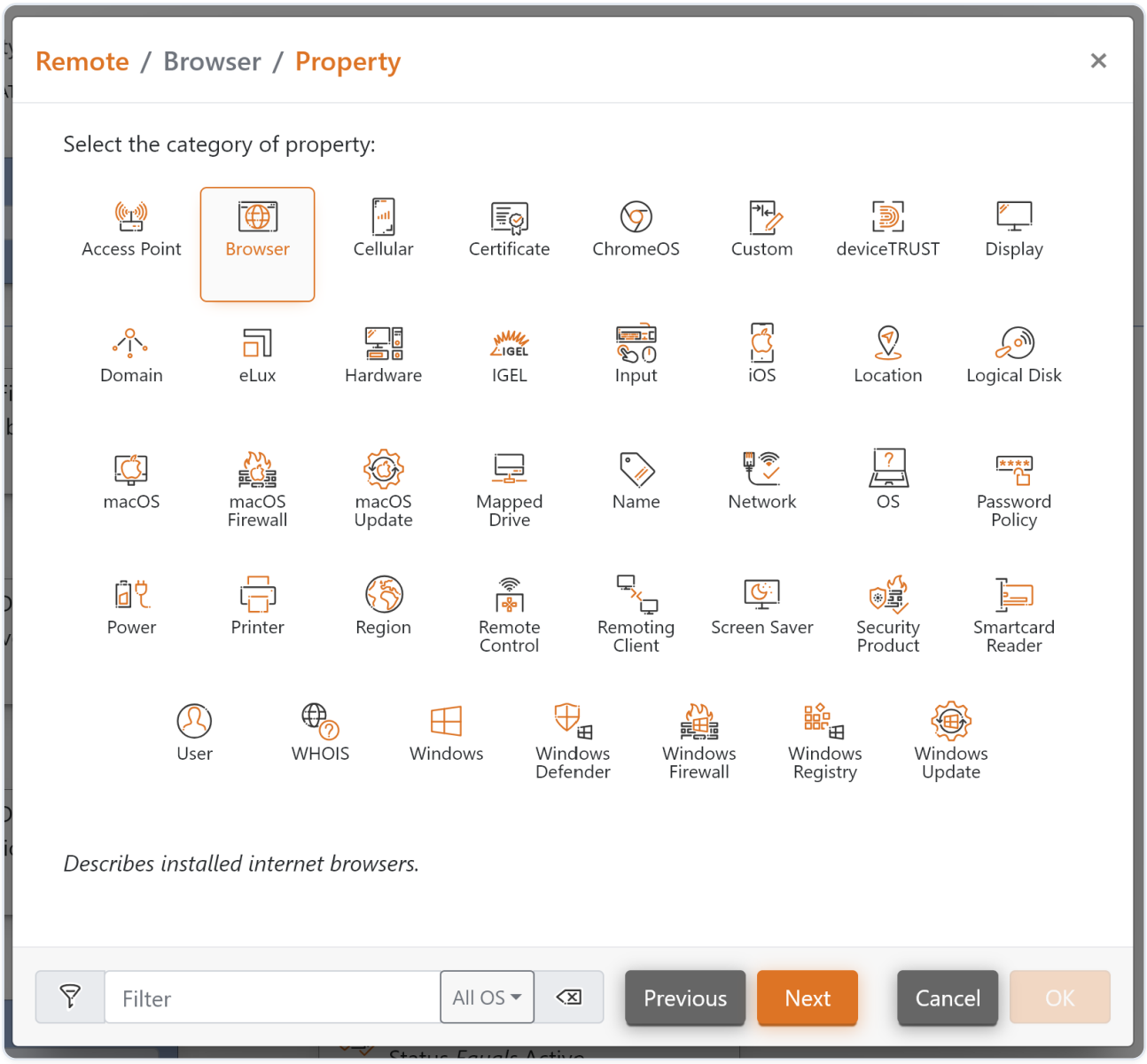
The deviceTRUST 21.1.310 patch includes bugfixes and minor enhancements to the deviceTRUST Console, Agent and Client Extension.

- User interface refinement
- New Cloud Templates
- Other changes
- Bug fixes in 21.1.300
- Bug fixes in 21.1.310
- Minor enhancements to 21.1.310
- Compatibility

User interface refinement

We've refined the branding within the deviceTRUST® Console, and also enhanced the layout of many of our pages. This includes the context condition picker, which now offers a filter allowing faster navigation of properties either by name or by their supported operating system.

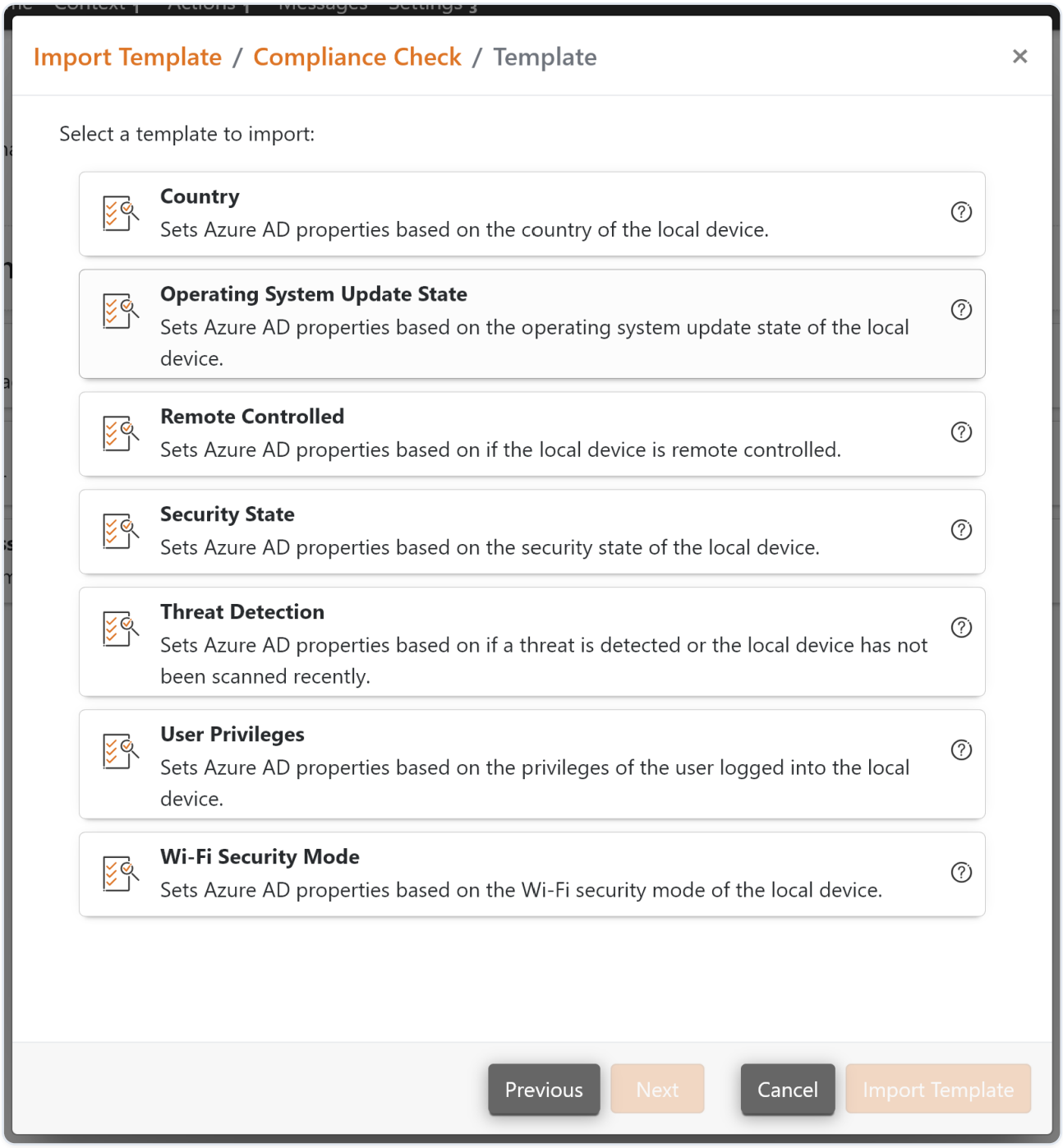
© 1997–2026 Citrix Systems, Inc. All rights reserved.



New Cloud Templates

A new collection of templates targeting the cloud and our Azure AD integration has been added. More information can be found cloud.

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



Other changes

- The Custom Properties Settings now supports remote Linux and IGEL devices. The forthcoming deviceTRUST Client Extension 21.1.300 or later for IGEL and Linux devices is required.
- The Terminate App task now groups together processes with matching names and parent / child relationships.
- When configured with mobile integration, the deviceTRUST Agent no longer calls to the server on Citrix® platforms when Citrix reports that the remote device is Windows, Linux or macOS.

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

Bug fixes in 21.1.300

- Fixed an issue where the Please Wait screen would appear on Local console sessions even when the `Block user session during Logon and Reconnect (or Unlock)` advanced setting was enabled.
- Fixed an issue where multiple resizes of a full screen Citrix session would occur during an Unlock on a Local device running the deviceTRUST Agent.
- Fixed an issue where Remote Custom Properties for Windows would not work when using Local Custom Properties on the same device.
- Fixed an issue where the WHOIS country could be cached even when it was empty.
- Fixed an issue where the deletion of properties would fail when the remote device was running the deviceTRUST Client Extension 20.2 or earlier.
- Fixed an issue where the Terminate App task, when matching processes by process name, could be triggered when the context filter no longer matches.

Bug fixes in 21.1.310

- Fixed a bug where the deviceTRUST Console would very rarely save or export encrypted deviceTRUST Policy files with a truncated random key, preventing the policy from being loaded.
- Fixed issue where Event ID's 201, 202 and 203 from remote custom properties execution would have a 1970 trigger time.

Minor enhancements to 21.1.310

- Added support for session idle time of remote Windows devices.
- Added support for the Popup Task to execute a named trigger when the default OK button is clicked.
- Updated the deviceTRUST Console's supported remote device properties available on Linux, IGEL and iOS platforms.

Compatibility

Please refer to our general approach to compatibility which can be found on the compatibility page.

If upgrading from a version older than deviceTRUST 21.1.210, be sure to refer to the deviceTRUST 21.1.210 Compatibility notes.

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

IGEL Client Extension 21.1.310

This release includes new features and bug fixes, and is natively integrated into IGEL OS 11.08.200 and later.

Custom Properties for IGEL OS devices

The Custom Properties Settings now supports remote IGEL OS devices. This allows a custom script to be executed on the remote IGEL device by writing `REMOTE_CUSTOM_NAME=VALUE` to the output.

Native IGEL OS integration

IGEL OS 11.08.200 now supports native integration of the deviceTRUST Client Extension for Amazon WorkSpaces, Citrix Workspace App, Microsoft Azure Virtual Desktop and Free RDP. Additionally, VMware Horizon View is supported in IGEL OS 11.08.230. For more information, see Supported IGEL Operating Systems for Client Extension.

Bug fixes

- Fixed an issue where the Third Party Geolocation provider could fail to determine a position.

Known issues

- We don't have the necessary permissions to determine the *REMOTE_HARDWARE_BIOS_SERIAL* property on an IGEL device. Until we have a permanent solution, this can be solved by running `dmidecode -s system-serial-number > /wfs/bios_serial_number` within the IGEL configuration at System -> Firmware Customization -> Custom Commands -> Base -> Final initialization command. Please note that the location of this file has changed in this release.

Compatibility

Please see the Known issues for a change to the default location of the `bios_serial_number` file.

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

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

index

- Product Events
- Actions
- Audit Event Task
- Azure AD Task
- Citrix Policy Task
- Custom Process Task
- Deny Access Task
- FSLogix App Masking Task
- Task Reference
- Logon Abort Task
- Map Drive Task
- Map Printer Task
- Microsoft AppLocker Task
- Popup Message Task
- Screen Saver Task
- Send Mail Task
- Shortcut Task
- Terminate App Task
- User Session Task
- Web Request Task
- Windows Firewall Task
- Windows Policy Task
- Windows Registry Task
- Advanced Settings
- Auditing Settings

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

- Azure AD Settings
- Custom Properties Settings
- File-Based Policy Settings
- Settings
- Licensing Settings
- Mail Server Settings
- Map Drive Settings
- Microsoft AppLocker Settings
- Printer Settings
- Property Settings
- Security Settings
- System Messages Settings
- Access Point Properties
- Browser Properties
- Cellular Properties
- Certificate Properties
- ChromeOS Properties
- Custom Properties
- deviceTRUST Properties
- Display Properties
- Domain Properties
- eLux Properties
- Hardware Properties
- IGEL Properties
- Input Properties
- iOS Properties
- Location Properties
- Logical Disk Properties
- macOS Properties
- macOS Firewall Properties

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

- macOS Update Properties
- Mapped Drive Properties
- Multihop Properties
- Name Properties
- Network 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
- WHOIS Properties
- Windows Properties
- Windows Defender Properties
- Windows Firewall Properties
- Windows Registry Properties
- Windows Update Properties
- Country Template
- Compliance Check
- Operating System Update State Template
- Remote Controlled Template
- Security State Template
- Threat Detection Template

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

- User Privileges Template
- Wi-Fi Security Mode Template
- 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
- Override Template
- Policy Mode from AD Group Template
- Policy Mode from Date Template
- Proximity Template
- Session Idle Template
- Unauthorized USB Device Template
- Unauthorized USB Storage Device Template
- VPN Connected Template
- Wi-Fi Security Mode Template
- Working Time Template
- Country Template
- Compliant Application Access Templates
- Proximity Template
- Wi-Fi Security Mode Template
- 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

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

- Conditional Application Access for Proximity Template
- Geolocation Templates
- Location Aware Printing Templates
- IP Address Template
- NetBIOS Name Template
- Wi-Fi Access Point Template
- Custom Values Template
- Meeting Room Templates
- IP Address Template
- NetBIOS Name Template
- Time-based Access Template
- Time-based Access Templates
- Unauthorized USB Drives Templates
- Unauthorized USB Device Template
- Unauthorized USB Storage Device Template
- Access Mode Template
- Citrix HDX™ RealTime Media Engine Template
- Citrix Workspace™ App Template
- Computer Certificate Template
- Conditional Application Access Template
- Corporate Device Template
- Country Template
- Country Provider Template
- Country Provider with Fallback Template
- Country with Fallback Template
- Device Location IP Address Template
- Device Location NetBIOS Name Template
- Device Location Wi-Fi Access Point Template
- Device Type BYOD Template
- Device Type Contractor Template

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

- 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
- 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
- Citrix Clients Template
- Compliance Check Template
- Computer Certificate Template
- Corporate Device Template
- Country Template
- Country with Fallback Template
- deviceTRUST® Client Extension Availability Template
- Compliance Check
- Operating System Template

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

- Operating System Update 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
- Wi-Fi Security Mode Template
- Working Time Template
- Conditional Access Template
- Compliant Backend Access Templates
- 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 Access for Country with Fallback Template
- Conditional Application Access for Country Template
- Conditional Application Access for Proximity Template
- Geolocation Templates
- Adobe Reader DC Template

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

- License Compliance Templates
- Microsoft Office Template
- Microsoft Project Template
- Microsoft Visio Template
- Nuance PDF Template
- Location Aware Printing Templates
- IP Address Template
- NetBIOS Name Template
- Wi-Fi Access Point Template
- Custom Values Template
- Meeting Room Templates
- IP Address Template
- NetBIOS Name Template
- Process Monitoring Templates
- Microsoft Teams Template
- Access Mode Template
- Adobe Acrobat DC Template
- Corporate Device Template
- Country Template
- Silo Optimization Templates
- Microsoft Office Template
- Microsoft Project Template
- Microsoft Visio Template
- Nuance PDF Template
- Proximity Template
- Wi-Fi Security Mode Template
- Working Time Template
- Application Log Template
- ELK Stack Template
- Email Template

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

- Graylog Template
- Status Report Templates
- Log File Template
- Splunk Template
- Conditional Access Template
- Conditional Application Access Template
- Time-based Access Templates
- Unauthorized USB Device Templates
- Unauthorized USB Device Template
- Unauthorized USB Storage Device Template
- Conditional Access Template
- Work From Home Templates

Product Events

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

Application Channel

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

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
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 Agent Service

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				loaded new policies.
4	Policy Load Failed	Error	Policy Load Failed)	The deviceTRUST Agent Service attempted to load new policies but an error occurred.
11	License Validated	Information	License)	The license has been read, is valid, and is not yet expired, or within the expiry threshold (30 days). The license is read on service startup, and any time a new license is deployed by Group Policy.
12	Hard License Expires Soon	Warning	License)	The license is a hard license, is valid, but it expires within the expiry threshold (30 days). Since the license is a hard license, the software will stop functioning once the expiry date is reached.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
13	Soft License Expires Soon	Warning	License)	The license is a soft license, is valid, but it expires within the expiry threshold (30 days). Since the license is a soft license, the software will continue to function after the expiry date is reached.
14	Soft License Expired	Error	License)	The license is a soft license, is valid, but has expired. Since the license is a soft license, the software will continue to function.
15	Hard License Expired	Error	License)	The license is a hard license, is valid, but has expired. Since the license is a hard license, the software will not function.
16	License Invalid	Error	License Invalid)	The license does not exist or contains invalid data.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
17	Unmanaged User Logon	Information	Unmanaged User Logon)	An unmanaged user logged on.
101	Logon	Information	Connection)	A user successfully logged onto a new session.
102	Reconnect	Information	Connection)	A user successfully reconnected to an existing session.
103	Logoff	Information	Session)	A user which previously successfully logged onto a session was logged off.
104	Disconnect	Information	Session)	A user which previously successfully logged onto a session was 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.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
111	Untrusted Device Blocked	Warning	Untrusted Device Blocked)	A user attempted to logon or reconnect to an existing session, but the deviceTRUST Client Extension failed to provide properties of the remote connected device, and the policy determines that this information is required.
112	Trusted Device Blocked	Warning	Trusted Device)	A trusted device, i.e. a device with the deviceTRUST Client Extension installed, was 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.

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

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				to the shell failed.
304	Logon Aborted	Warning	Logon Aborted)	The logon process was aborted.
311	Event Info	Information	Event)	A custom information event was created by the Audit Event task set to Information.
312	Event Warning	Warning	Event)	A custom information event was created by the Audit Event task set to Warning.
313	Event Error	Error	Event)	A custom information event was created by the Audit Event 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

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

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
				discovered by the Terminate App task.
332	Application Shutdown	Information	Application Shutdown)	A user was asked to shutdown an application discovered by the Terminate App task.
341	Popup Shown	Information	Popup Shown)	A popup message was shown to the user.
342	Popup Failed	Error	Popup Failed)	An attempt to display a popup message to the user failed.
351	Registry Updated	Information	Registry Updated)	The registry was updated.
352	Registry Warning	Warning	Registry Warning)	A warning was generated while updating the registry.
353	Registry Failed	Error	Registry Failed)	An attempt to update the registry failed.
361	Printer Mapped	Information	Printer Operation)	Printers were successfully mapped.

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
362	Printer Map Failed	Error	Printer Operation Failed)	An attempt to map printers failed.
363	Printer Unmapped	Information	Printer Operation)	Printers were successfully unmapped.
364	Printer Unmap Failed	Error	Printer Operation Failed)	An attempt to unmap printers failed.
365	Printer Set Default	Information	Printer Operation)	A printer was set as default.
366	Printer Set Default Failed	Error	Printer Operation Failed)	An attempt to set a default printer failed.
367	Printer Map Warning	Warning	Printer Operation Failed)	A warning was generated when attempting to map a printer.
368	Printer Set Default Warning	Warning	Printer Operation Failed)	A warning was generated when attempting to set a default printer.
371	App Masking Update	Information	App Masking Update)	A Microsoft FSLogix App Masking update was successfully applied.

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

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

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

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
413	Drive Map Failed	Error	Drive Operation Failed)	A network drives and any failover drives failed to map.
414	Drive Unmap	Information	Drive Operation)	A network drive was unmapped.
415	Drive Unmap Failed	Error	Drive Operation Failed)	A network drive failed to unmap.
421	Shortcut Creation Succeeded	Information	Shortcut Operation)	A shortcut was successfully created.
422	Shortcut Creation Failed	Error	Shortcut Operation Failed)	A shortcut failed to be created.
423	Shortcut Deletion Succeeded	Information	Shortcut Operation)	A shortcut was successfully deleted.
424	Shortcut Deletion Failed	Error	Shortcut Operation Failed)	A shortcut failed to be deleted.

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.

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

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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	UserName (4)	TEXT	The name of the user logged into the session.
	UserDomain (5)	TEXT	The domain of the user logged into the session.
	UserSID (6)	TEXT	The security identifier of the user logged into the session.
Policy Loaded	Name (1)	TEXT	The name of the service, e.g. deviceTRUST Agent Service.
	Policies (2)	TEXT	A list of the policies that were loaded and the timestamp that 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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	ConnectedId (3)	GUID	Uniquely identifies events from the same connection. Unlike the LogonId, the value of this field changes every time a new connection is established to an existing session.
	ConnectedTime (4)	SYSTEMTIME	The time that the user logged on, or reconnected, to the session.
	SessionId (5)	INT	The session id that the user is connected to.
	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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			field is blank for local console sessions.
	DeviceName (10)	TEXT	The name of the remote connected device. This field is blank for local console sessions.
	DeviceOS (11)	TEXT	The operating system of the remote connected device. This field is blank for local console sessions, and if the deviceTRUST Client Extension did not provide details of the operating system.
	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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Contexts (13)	TEXT	A textual representation of all contexts. The contexts are formatted with the name and value separated by an equals symbol (=), and multiple contexts separated by a newline (\n) character. E.g. CONTEXT1=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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. PROPERTY1=VALUE1\nPROPERTY2=VALUE2\n
	RemovedProperties (10)	TEXT	A textual representation of all properties that were removed. The properties are formatted with the name of each property, with multiple properties separated by a newline (\n) character. E.g. PROPERTY1 \nPROPERTY2 \n

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

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

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			formatted with the name and value separated by an equals symbol (=), and multiple contexts separated by a newline (\n) character. E.g. CONTEXT_ONE=VALUE1\nCONTEXT_TWO=VALUE2\n
	PreviousContexts (10)	TEXT	A textual representation of the previous value of all contexts that were changed or removed. The contexts are formatted with the name and value separated by an equals symbol (=), and multiple properties separated by a newline (\n) character. E.g. CONTEXT_ONE=PREVIOUSVALUE1\nCONTEXT_TWO=PREVIOUSVALUE2\n
	TriggeredBy (11)	TEXT	The name of the property that changed that ultimately caused the context to change.
	Trigger (12)	TEXT	The name of the trigger that generated the

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			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 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	ErrorMessage (14)	TEXT	An error message reported by the upgrade of the

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
(extends Trusted Device Auto Update)			deviceTRUST Client Extension.
Custom Process (extends Session)	TriggerName (9)	TEXT	The name of the trigger that launched the custom process, e.g. Logon or Reconnect.
	TriggerTime (10)	TIME	The time that the custom process was executed.
	TriggeredBy (11)	TEXT	The properties that resulted in the execution of the custom process.
	ActionName (12)	TEXT	The name of the action where the Custom Process task is located.
	SequenceIndex (13)	TEXT	The zero based index of the sequence within the action where the Custom Process task is located.
	TaskName (14)	TEXT	The name of the Custom Process task.
	CommandLine (15)	TEXT	The command line that was executed.
	RunAs (16)	TEXT	Either ‘USER’ or ‘SYSTEM’, depending upon the configuration of the

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
			trigger that was executed.
	Identity (17)	TEXT	The user name of the custom process.
	Pid (18)	INT	The Process ID of the custom process.
	Location (19)	TEXT	Determines whether the custom process was executed locally or remotely.
Custom Process Complete (extends Custom Process)	Duration (20)	INT	The time taken for the custom process to complete, in milliseconds.
	Output (21)	TEXT	The output messages returned by the custom process.
	Error (22)	TEXT	The error messages returned by the custom process.
Custom Process Failed (extends Custom Process)	Duration (20)	INT	The time taken for the custom process to complete, in milliseconds.
	Output (21)	TEXT	The output messages returned 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
User Message (extends Session)	Title (9)	TEXT	A message title displayed to the user.
	Message (10)	TEXT	The message displayed to the user.
	Timeout (11)	INT	The timeout period that the message is displayed to the user.
Access Allowed (extends Session)	Message (9)	TEXT	The message reported by a call to dtcmd.exe ACCESS.
Access Failed (extends Session)	Reason (9)	TEXT	The reason that a call dtcmd.exe ACCESS failed.
	Message (10)	TEXT	The message supplied to a call to dtcmd.exe ACCESS that would have been displayed to the user if the call succeeded.
	Timeout (11)	INT	The timeout period that the user would have had before being disconnected from the session, if the call to dtcmd.exe ACCESS succeeded.
Logon Aborted (extends Session)	Message (9)	TEXT	The message displayed to the user detailing why the logon failed.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Timeout (10)	INT	The timeout period that the user would have had before being logged out from the session.
Event (extends Session)	Message (9)	TEXT	A user supplied message from a call to dtcmd.exe EVENT.
	Report (10)	INT	Set to 1 when the report fields have been populated, or 0 otherwise.
	ReportTrigger (11)	TEXT	The trigger that resulted in the task being executed, such as Logon or ContextChanged.
	ReportAction (12)	TEXT	The name of the action that generated the event.
	ReportDeviceName (13)	TEXT	The name of the remote device that the user was connecting from.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	ReportClientVersion (16)	TEXT	The version of the deviceTRUST Client Extension that was used to establish the remote device information.
	ReportContexts (17)	TEXT	The name and value of all contexts.
	ReportProperties (18)	TEXT	The name and value of all properties.
AppLocker Rule (extends Session)	Name (9)	TEXT	The name of the rule.
	Operation (10)	TEXT	The operation of the AppLocker rule, either Allow, Deny or Delete.
	Target (11)	TEXT	The target of the AppLocker rule, either Executable, Dll, Installer, Script or Package.
	Duration (12)	INT	The time taken for the AppLocker rule to become effective.
	Rule (13)	TEXT	The AppLocker XML fragment that defines the rule.
AppLocker Rule Failed (extends Session)	Name (9)	TEXT	The name of the rule.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Operation (10)	TEXT	The operation of the AppLocker rule, either Allow, Deny or Delete.
	Target (11)	TEXT	The target of the AppLocker rule, either Executable, Dll, Installer, Script or Package.
	Duration (12)	INT	The time taken for the AppLocker rule to become effective.
	Message (13)	TEXT	A message explaining why the rule failed to apply.
AppLocker Policy	Event (1)	TEXT	The event that triggered the regeneration of policy, either 'Policy Change' or 'External Process'.
	Message (2)	TEXT	A description of the changes that were made.
	Duration (3)	INT	The time taken for the AppLocker Policy 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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Pid (10)	INT	The process identifier of the process that attempted to run the script or cmdlet.
	Type (11)	INT	Set to 0 whenever PowerShell was running a cmdlet, or 1 when running a script.
	Script (12)	TEXT	The full path to the script that attempted to execute.
Application Terminated (extends Session)	Title (9)	TEXT	The title displayed to the user following a call to dtcmd.exe APPTERMINATE.
	Message (10)	TEXT	The message displayed to the user following a call to dtcmd.exe APPTERMINATE.
	Applications (11)	TEXT	A comma separated list of all processes and their PID’s that were terminated.
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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
	Message (10)	TEXT	The popup message.
	Timeout (11)	INT	The timeout in seconds to display the popup.
Popup Failed (extends Session)	Reason (9)	TEXT	The reason that the popup failed to shown.
	Title (10)	TEXT	The popup title.
	Message (11)	TEXT	The popup message.
	Timeout (12)	INT	The timeout in seconds to display the popup.
Registry Updated (extends Session)	Values (9)	TEXT	The registry values.
	Persist (10)	TEXT	How to persist the registry values.
	Protect (11)	BOOLEAN	Whether the registry key is protected.
Registry Warning (extends Registry Updated)	Warnings (12)	TEXT	The warning messages generated by the update.
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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Printer Operation Failed (extends Printer Operation)	Reason (10)	TEXT	The reason that the printer operation failed.
App Masking Update (extends Session)	Path (9)	TEXT	The path to the Microsoft FSLogix App Masking Rule Assignment file.
	Operation (10)	TEXT	The type of operation.
	Entry (11)	TEXT	The entry to apply to the file.
App Masking Update Failed (extends App Masking Update)	Error (12)	TEXT	The reason that the Microsoft FSLogix App Masking update failed.
Send Mail (extends Session)	Host Name (9)	TEXT	The host name of the SMTP server.
	Recipients (10)	TEXT	A list of the recipients of the mail message.
	Subject (11)	TEXT	The subject of the mail message.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Send Mail Succeeded (extends Send Mail)	Message Id (14)	TEXT	Uniquely identifies the sent mail message.
Send Mail Failed (extends Send Mail)	Error (14)	TEXT	An error message representing the problem that occurred.
	Response (15)	TEXT	The response from the SMTP server.
Web Request Succeeded (extends Session)	Method (9)	TEXT	The method used in the web request.
	URL (10)	TEXT	The URL that the web request was sent.
	Status Code (11)	INT	The status code reported by the web server.
	Duration (12)	INT	The time in milliseconds taken to perform the web request.
	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.

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

NAME	FIELD NAME (INDEX)	FORMAT	DESCRIPTION
Windows Firewall (extends Session)	Action (9)	TEXT	Whether the firewall rule was an Allow or a Deny.
	RuleName (10)	TEXT	The name of the rule created.
Windows Firewall Failed (extends Windows Firewall)	Error (11)	TEXT	A description of the error that occurred.
Drive Operation (extends Session)	Drive (9)	TEXT	The drive that was mapped or unmapped.
Drive Operation Failed (extends Drive Operation)	Error (10)	TEXT	A description of the error that occurred.
Shortcut Operation (extends Session)	Shortcut Name (9)	TEXT	The name of the shortcut.
	Shortcut Directories (10)	TEXT	A list of directories that the shortcut should be created.
	Target Path (11)	TEXT	The path where the target file exists.
	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.

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

deviceTRUST/Usage Channel

The USAGE channel can be found within the Windows Event Log under APPLICATION AND SERVICE LOGS\DEVICETRUST\USAGE, or queried programmatically using the deviceTRUST/Usage channel. The following event is included.

EVENT ID	NAME	TYPE	DATA FORMAT NAME	DESCRIPTION
21	Usage	Information	Usage)	Raised when a license unit, e.g. a User, logs into the local device for the first time within a 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.

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

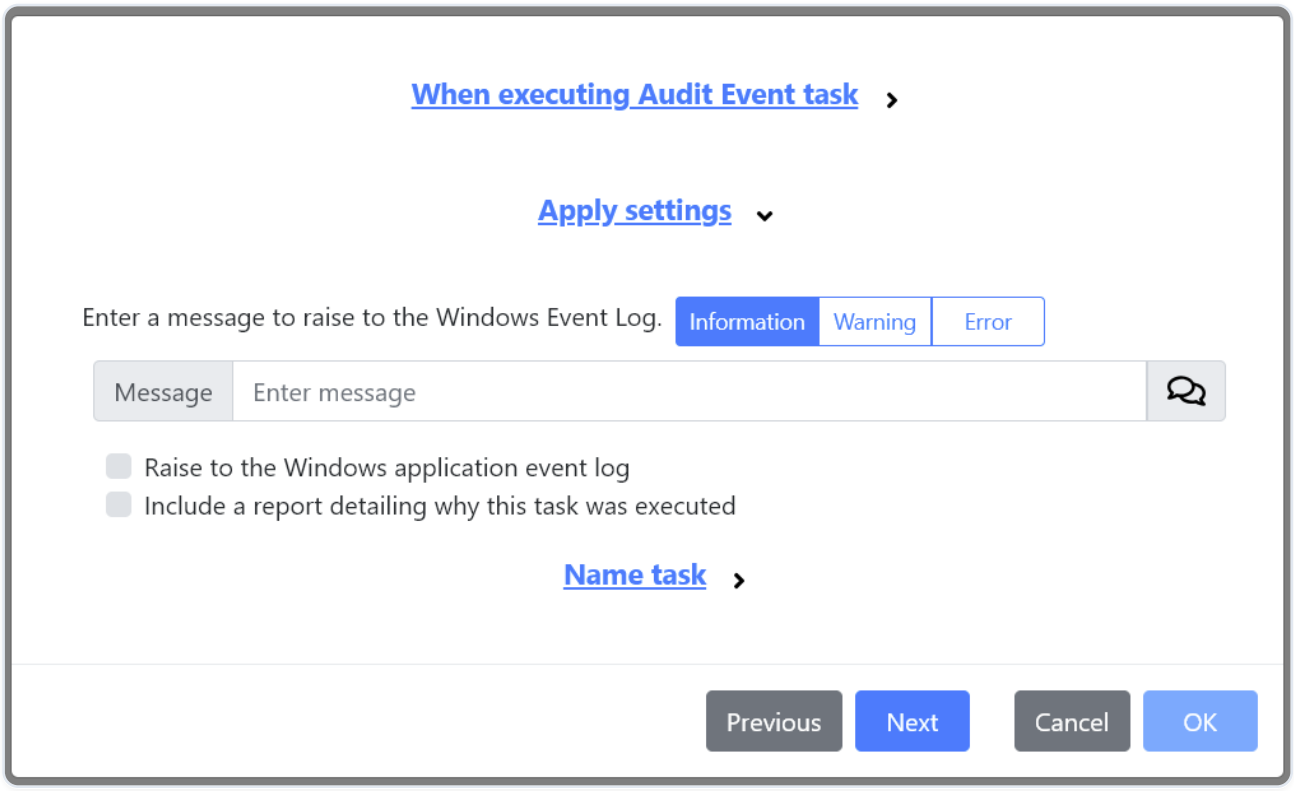
Actions

TABLE OF CONTENTS

- Tasks - Task Reference

Audit Event Task

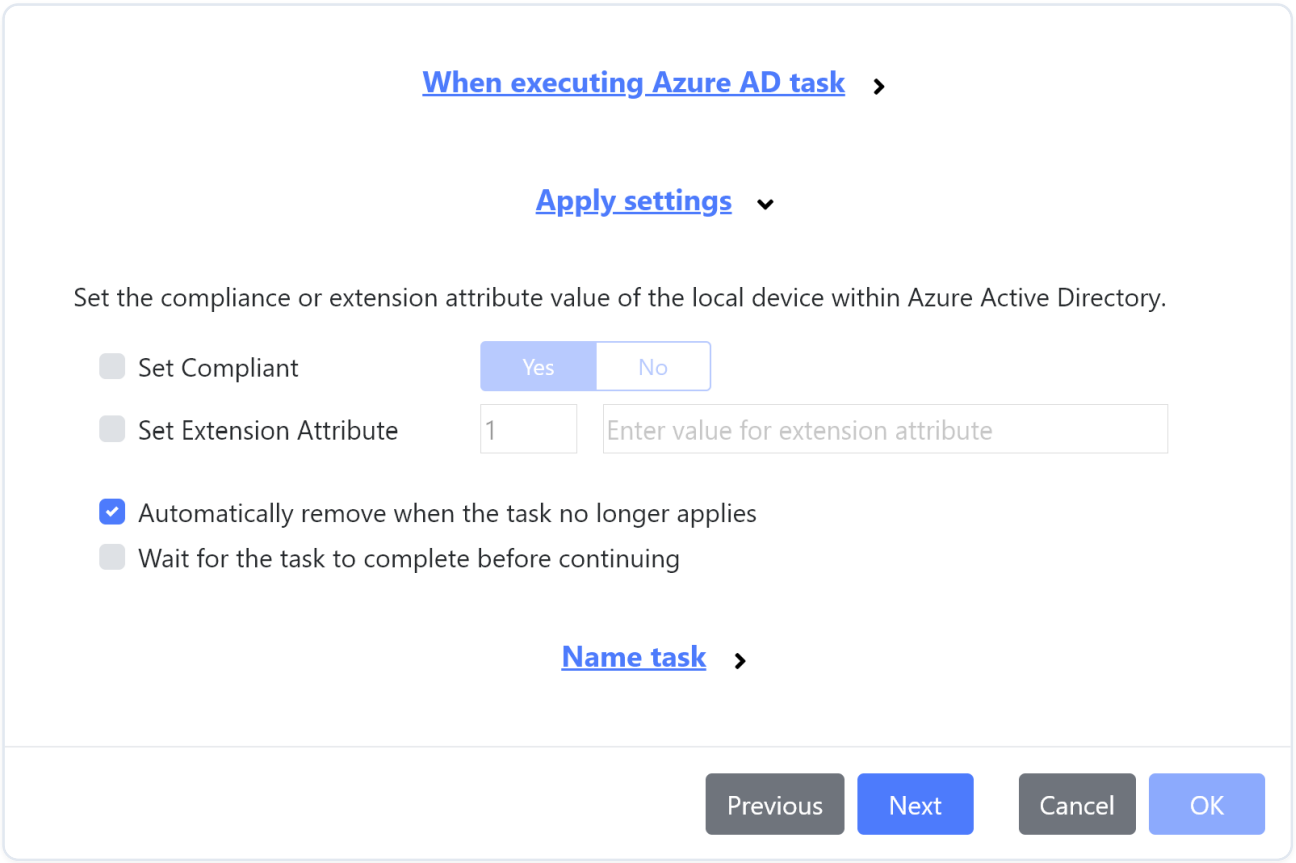
The `Audit Event` task raises an Information, Warning or Error event to the Windows Event Log.



Azure AD Task

The `Azure AD` task updates domain joined device compliance or extension attribute value within Azure Active Directory.

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

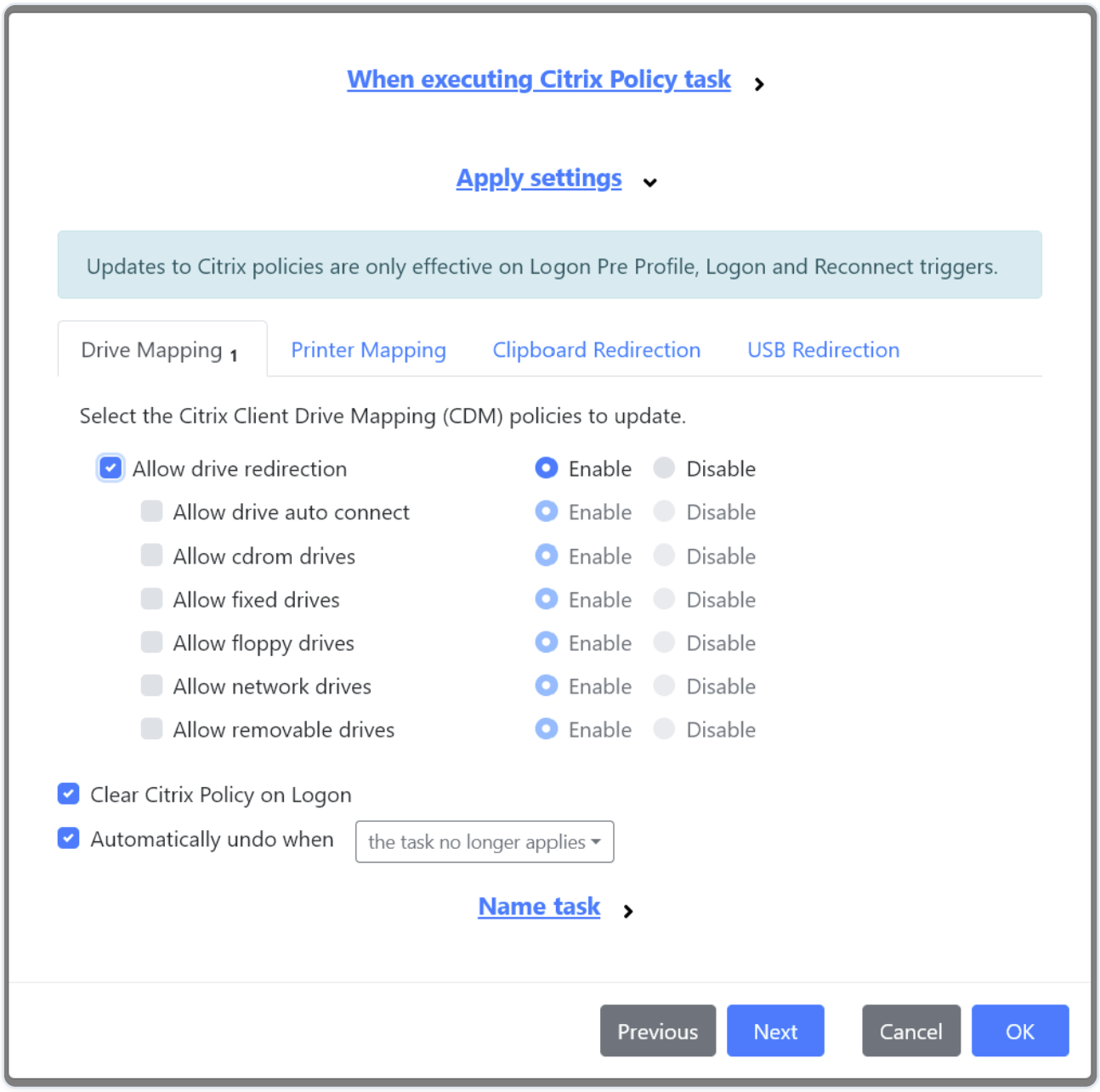


Azure Active Directory Settings must be configured with Device.ReadWrite.All permissions to Microsoft Graph.

Citrix Policy Task

The `Citrix Policy` task updates Citrix policies which control the sharing of data with the remote device.

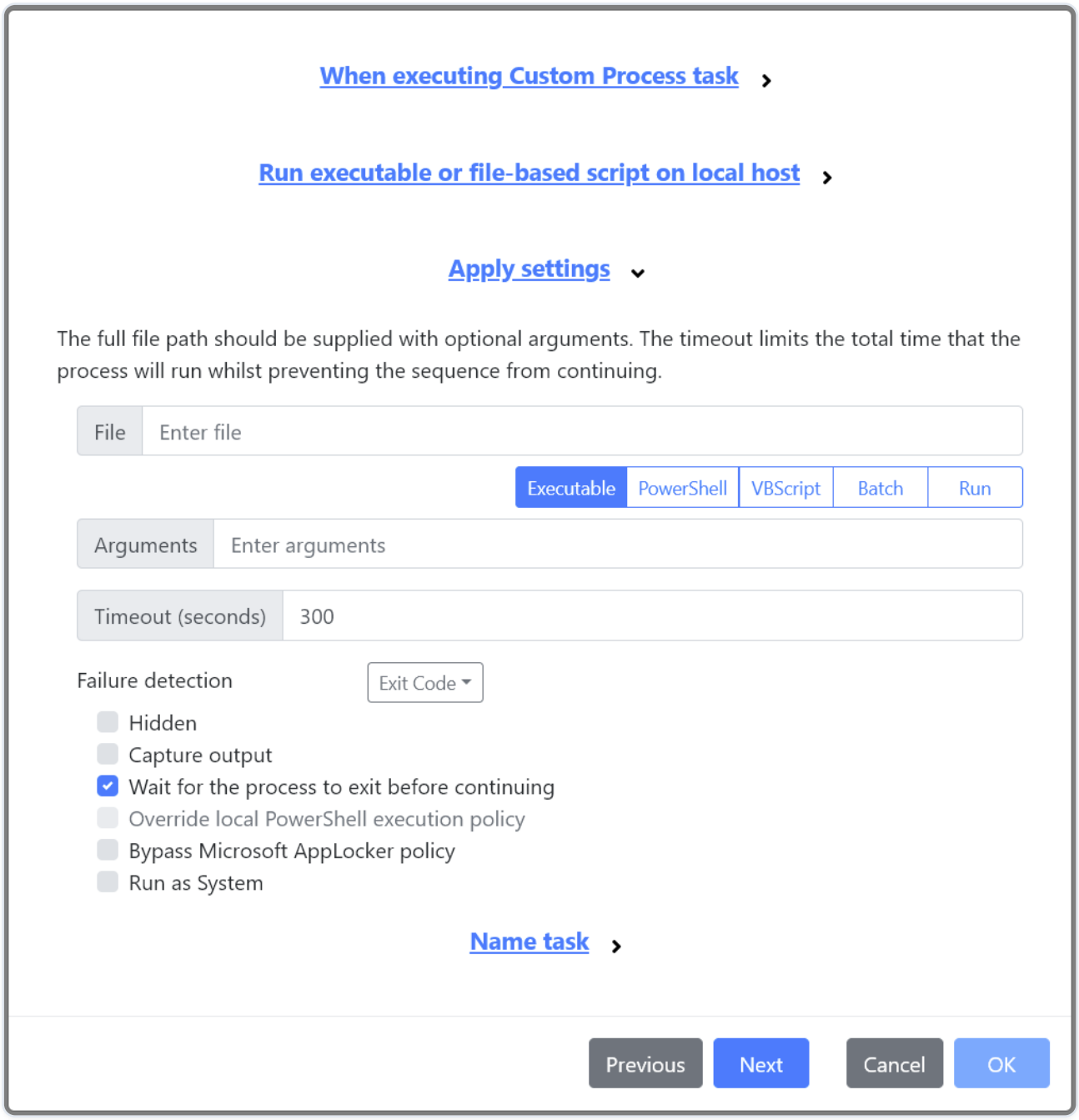
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Custom Process Task

The `Custom Process` task runs an executable or script on the local or remote device.

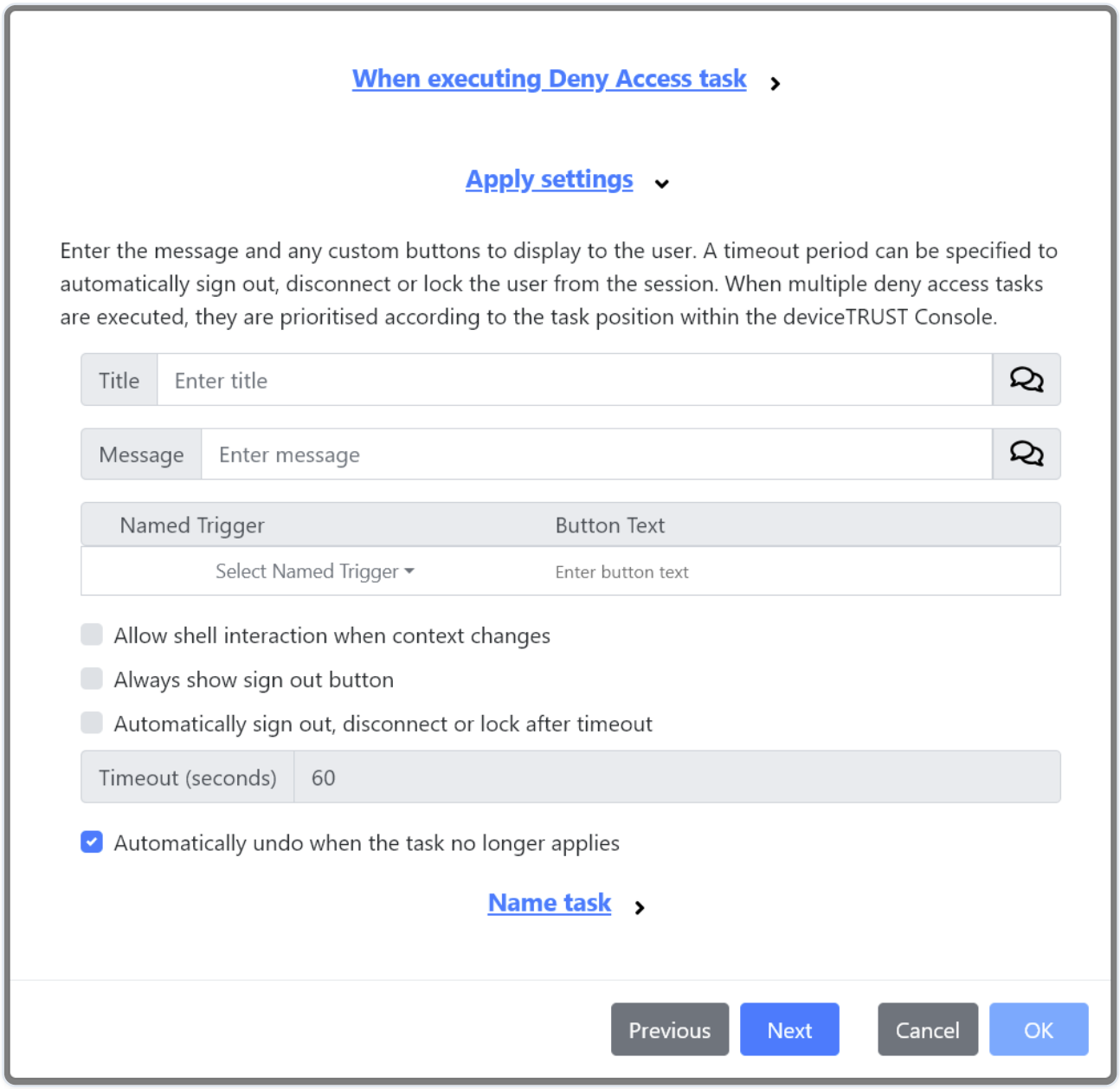
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

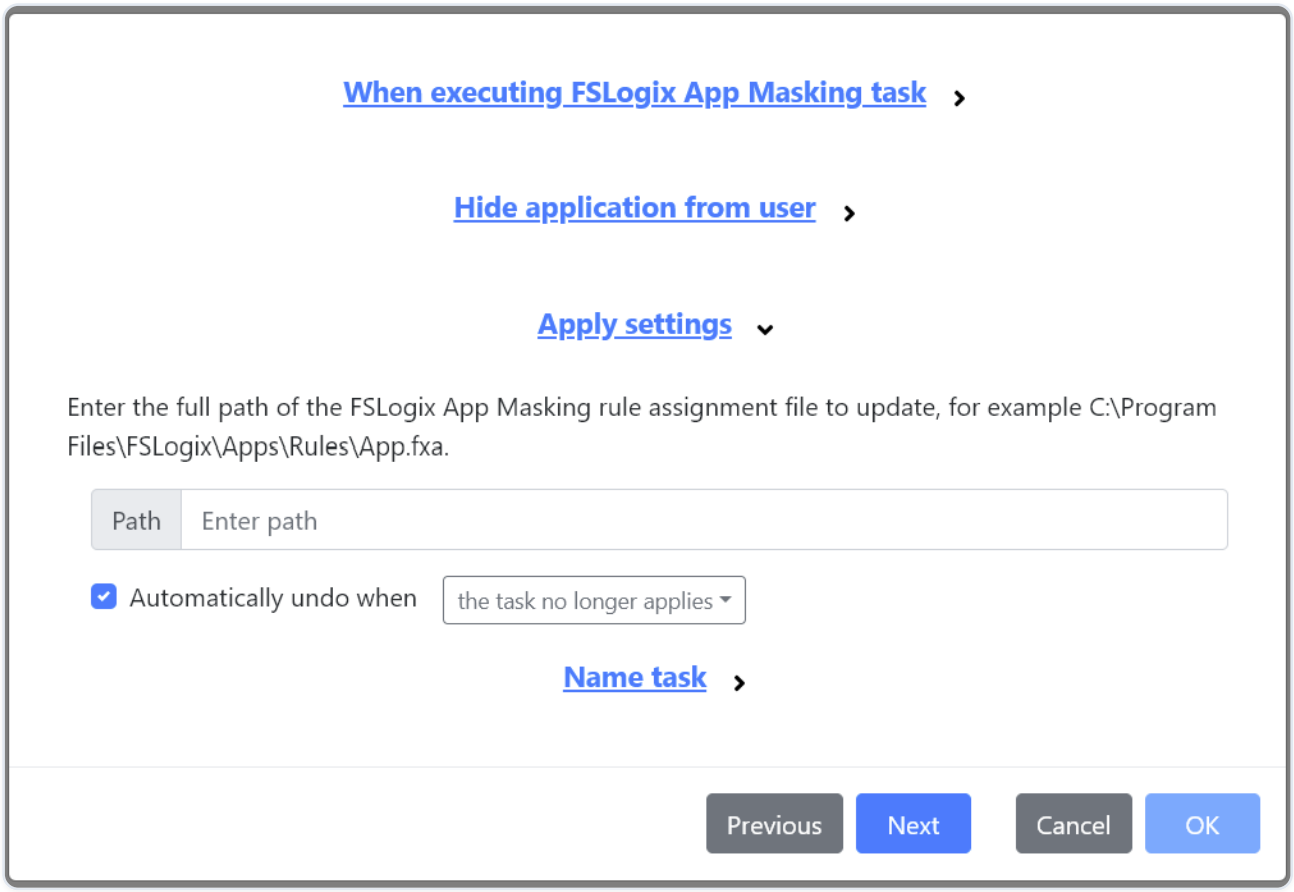
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.
- Azure AD - Updates domain joined device compliance or extension attribute value within Azure Active Directory.
- 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.

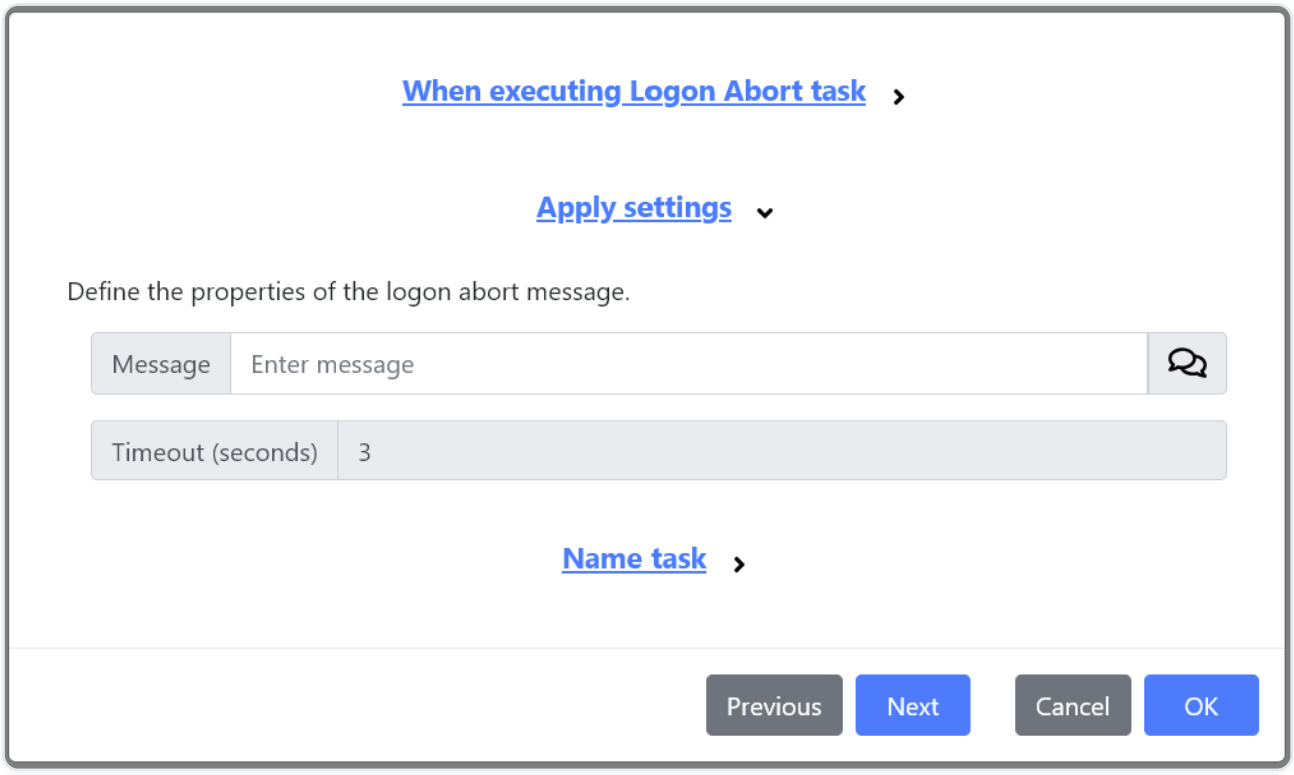
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft AppLocker - Creates, updates and deletes Microsoft AppLocker rules for the logged in user.
- 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.

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.

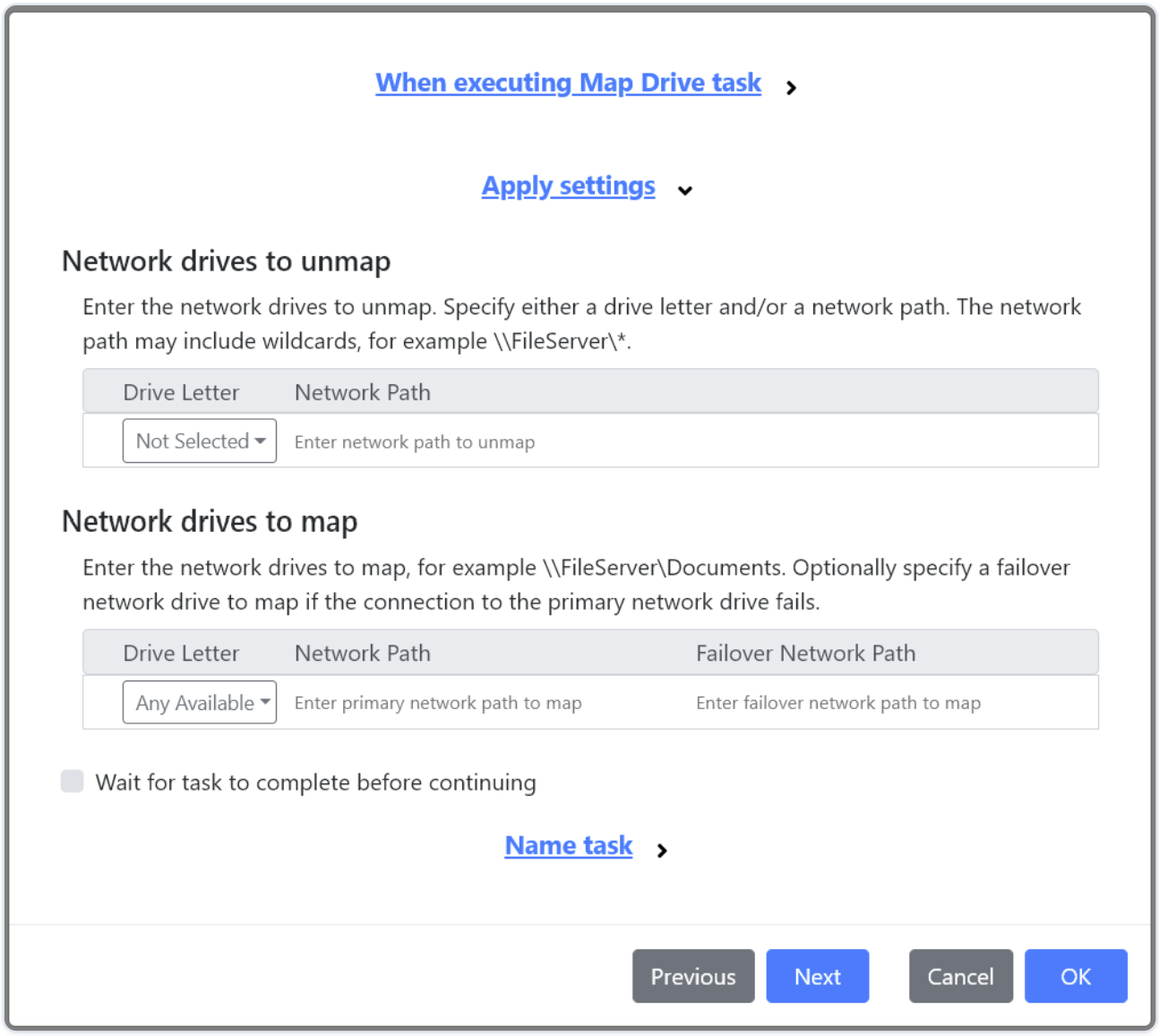
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Drive Task

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

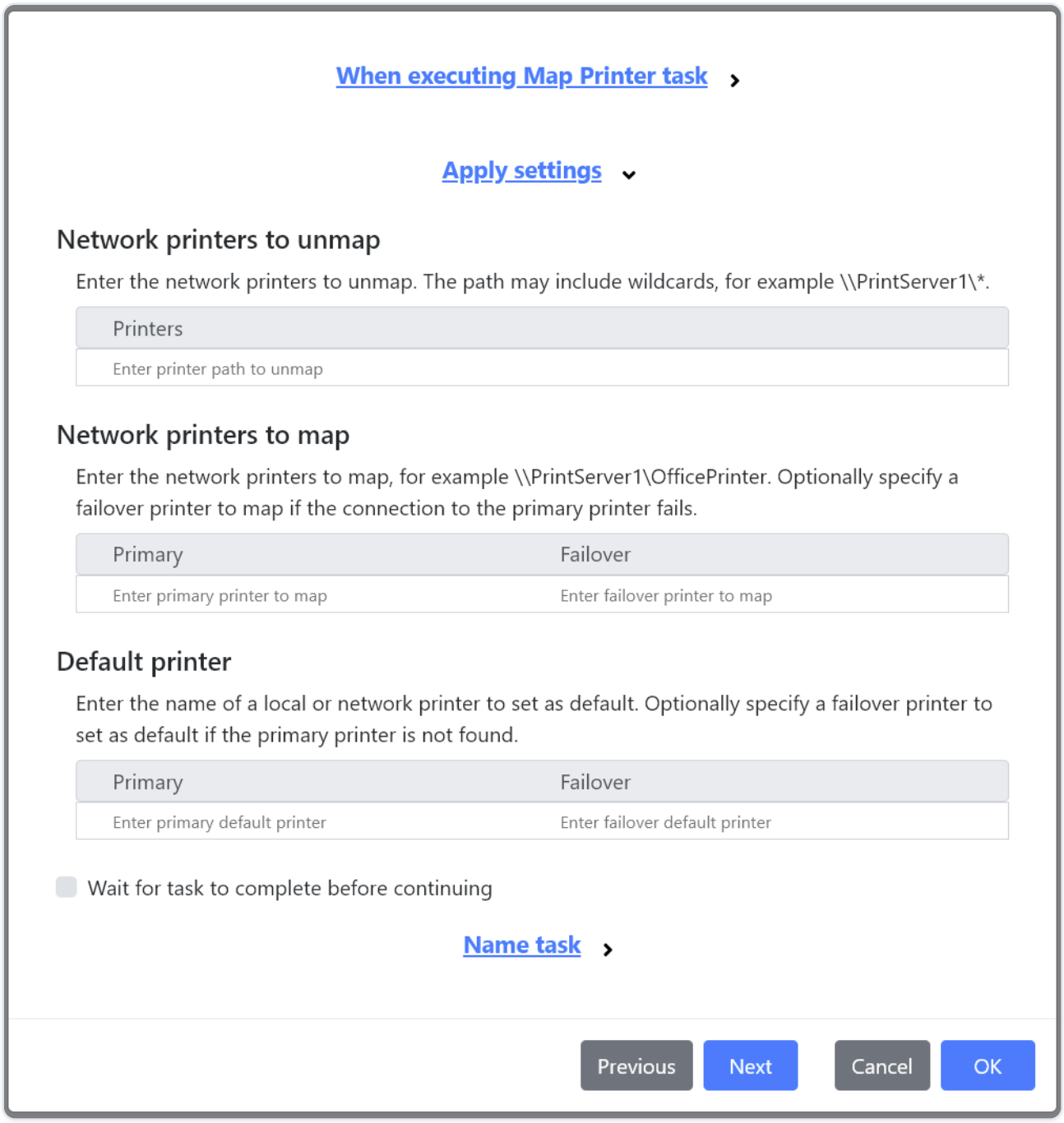
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Printer Task

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

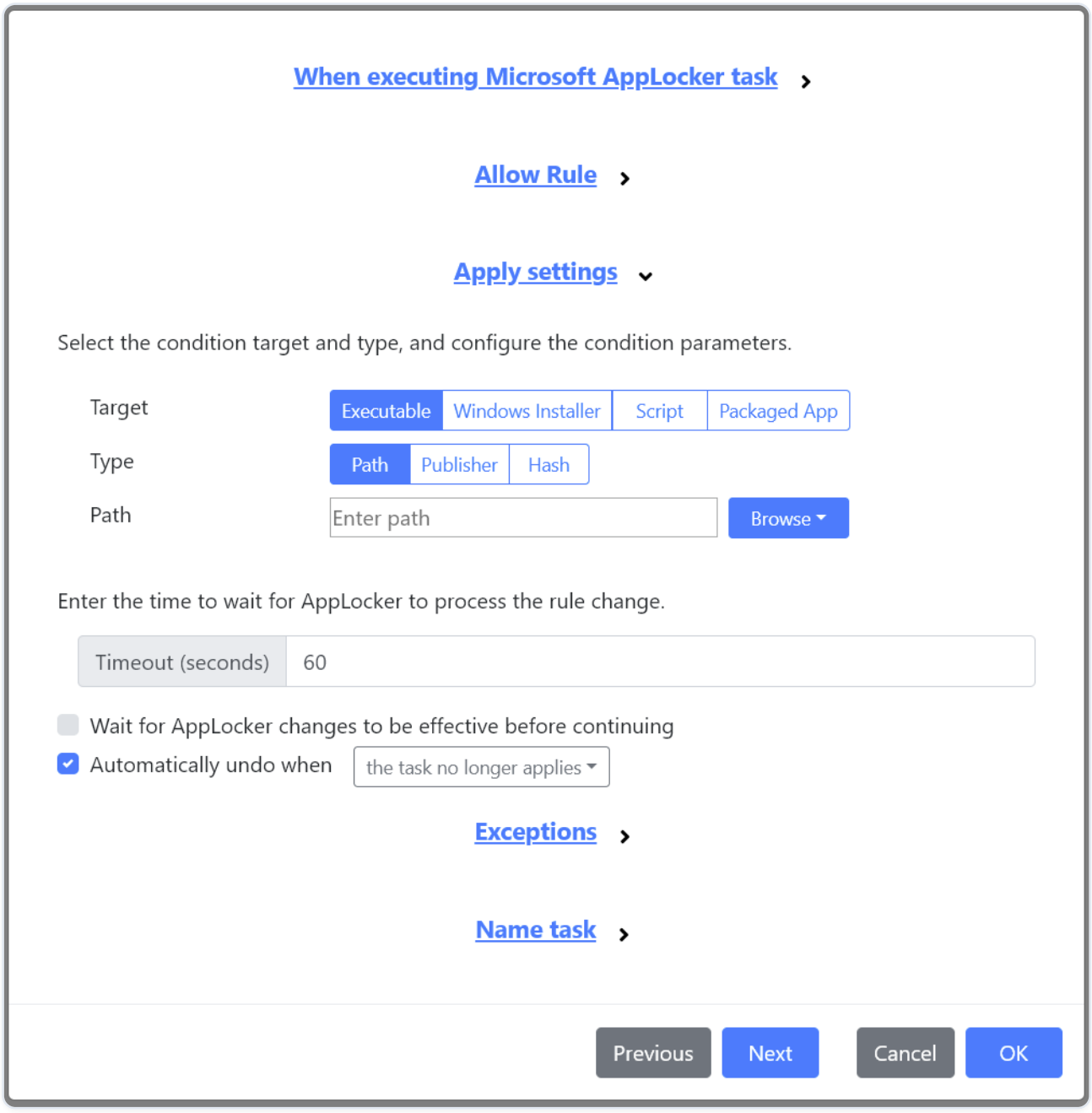
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

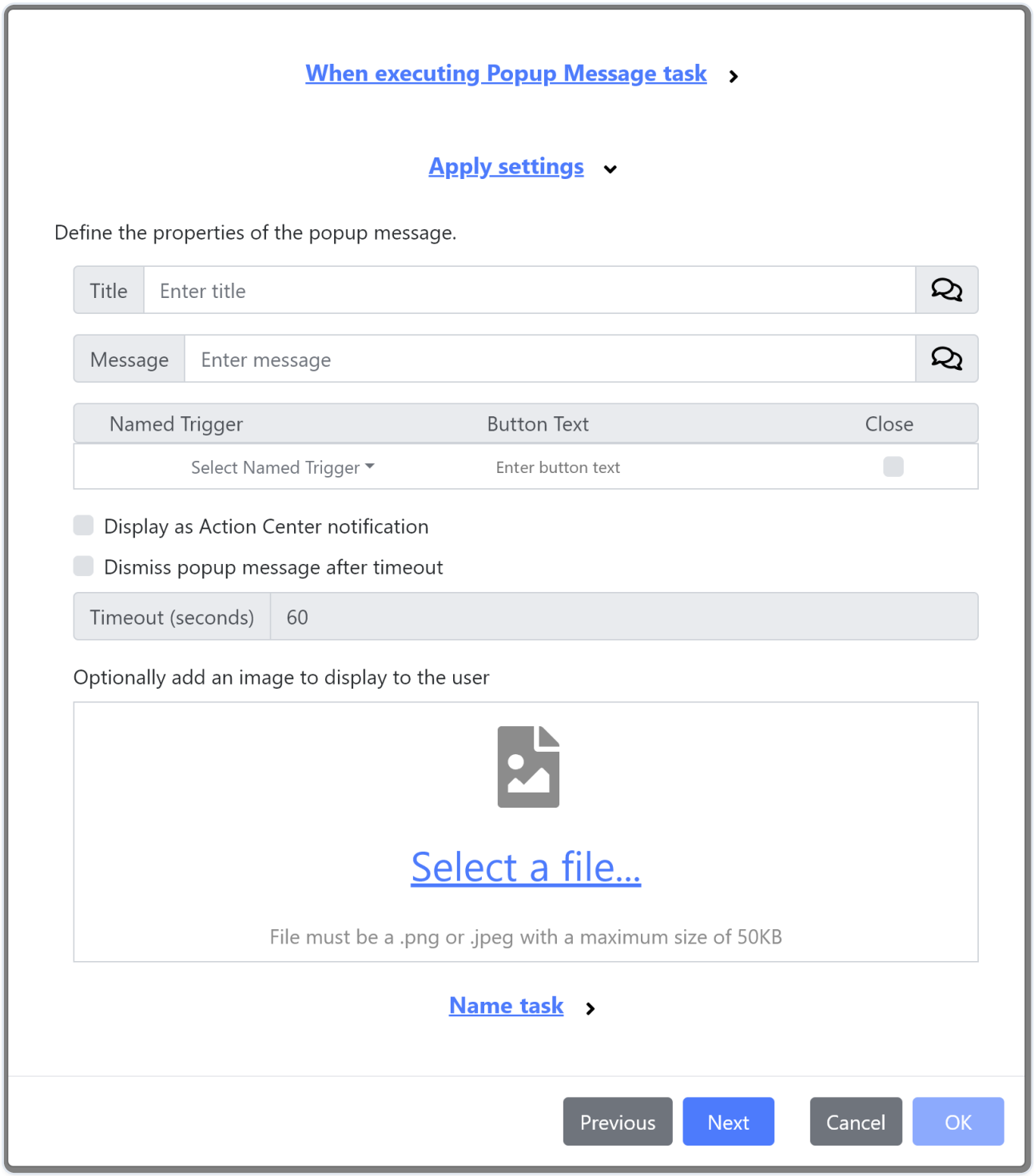
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

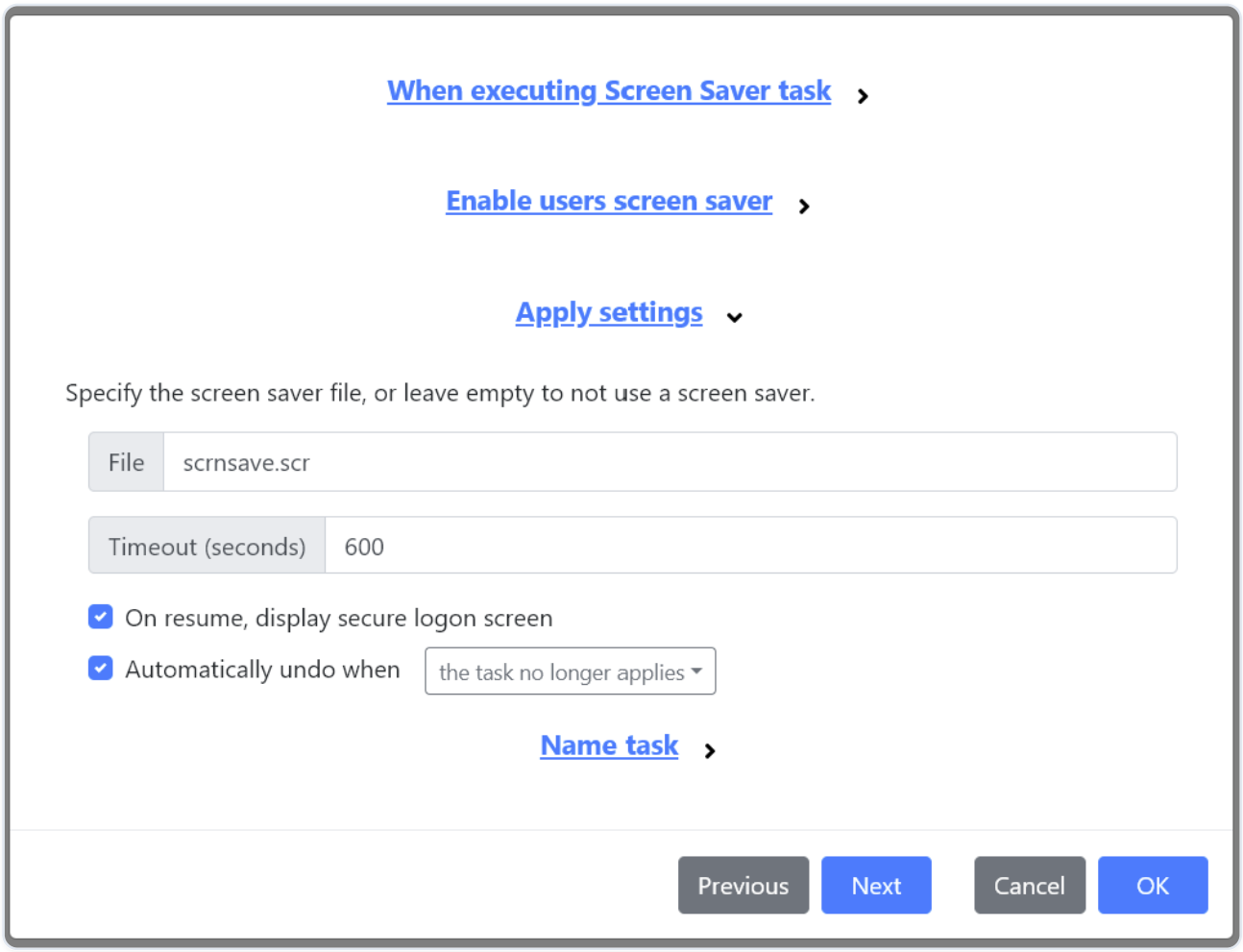
- *Title* - The title of the message displayed to the user.
- *Message* - The message displayed to the user.
- *Buttons* - Optionally, one or more additional buttons to add to the popup:
  - *Named Trigger* - The name of a named trigger to execute when the user clicks the button.
  - *Button Text* -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

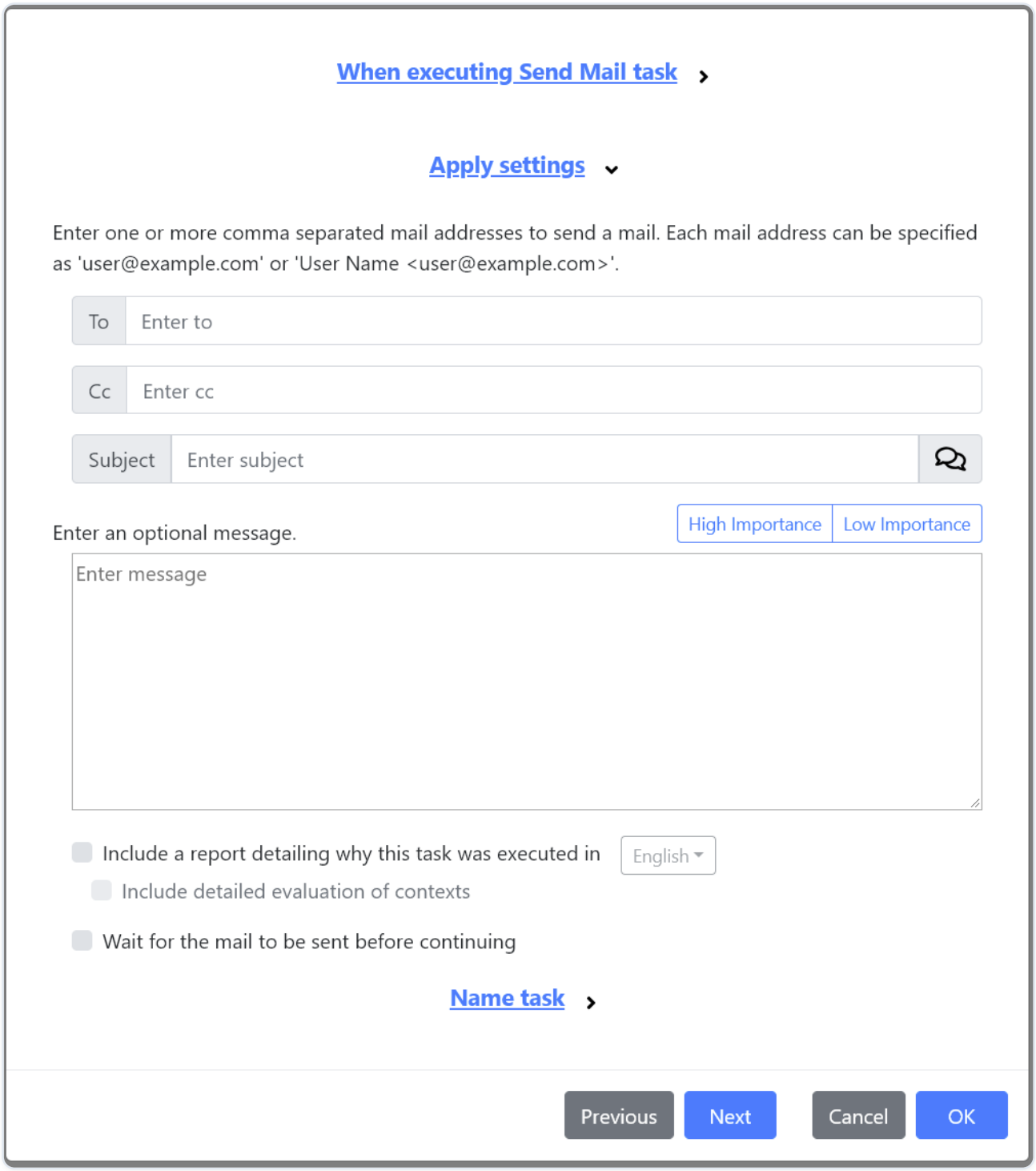
The `Screen Saver` task updates the screen saver settings within the session.



Send Mail Task

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

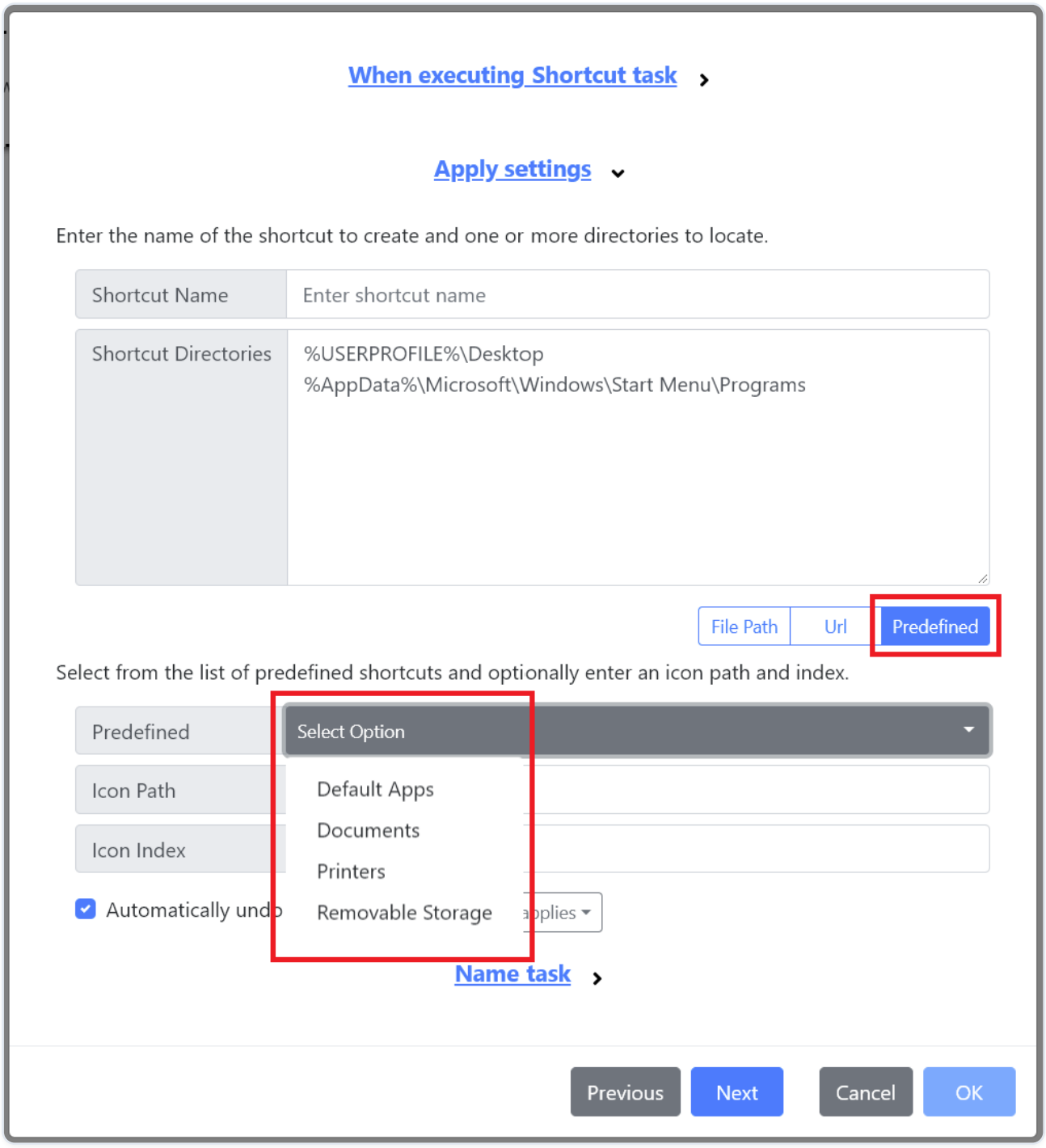
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Shortcut Task

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

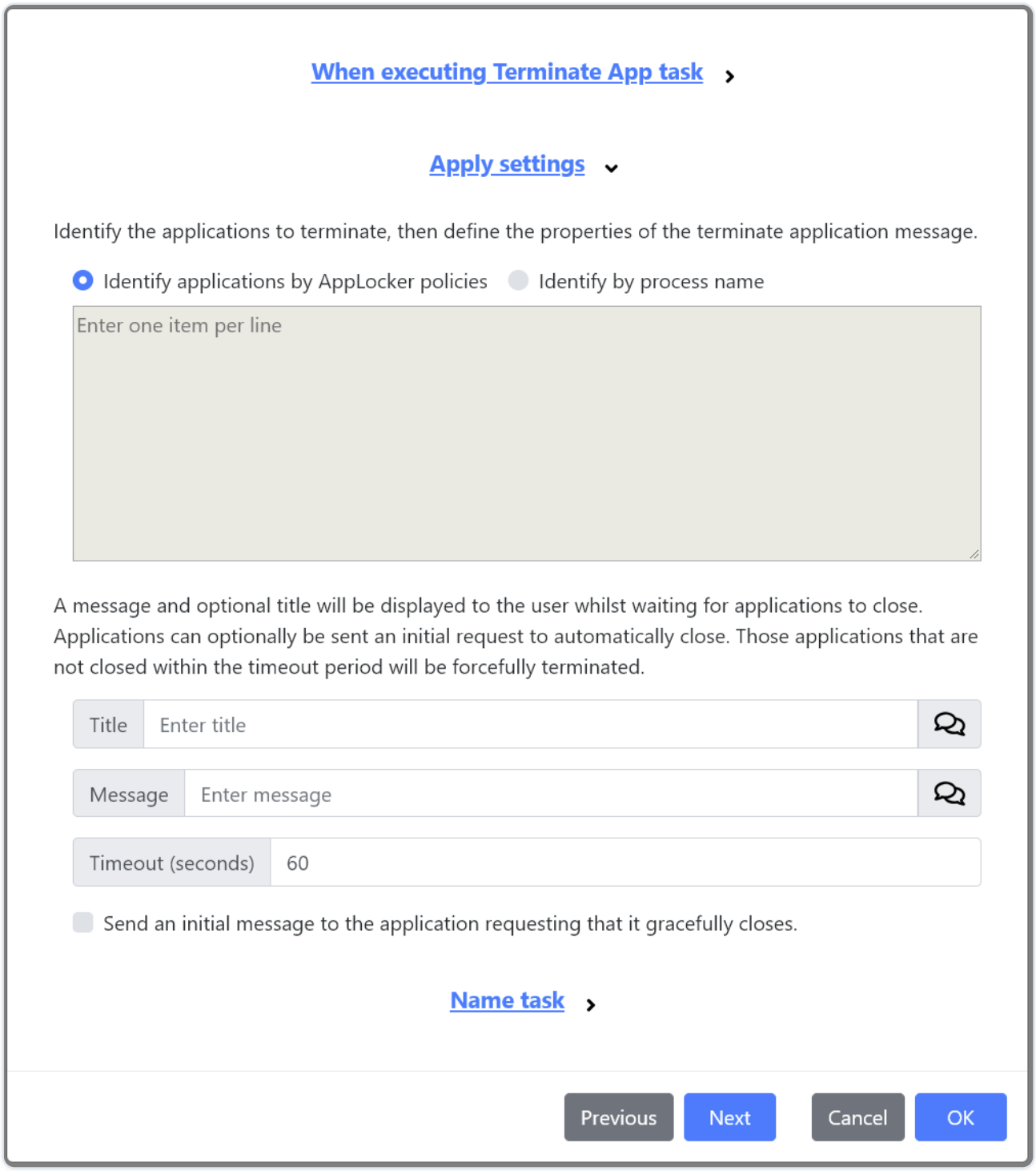
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

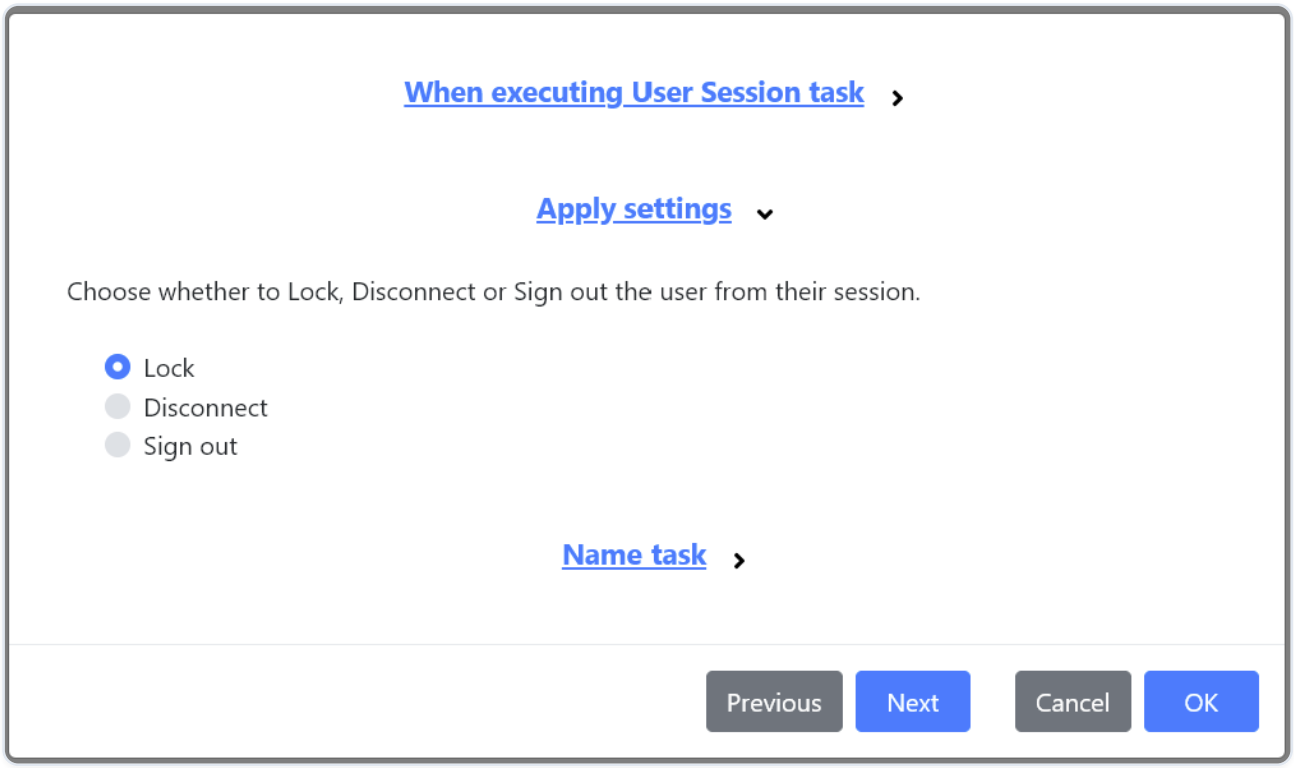
© 1997–2026 Citrix Systems, Inc. All rights reserved.



User Session Task

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

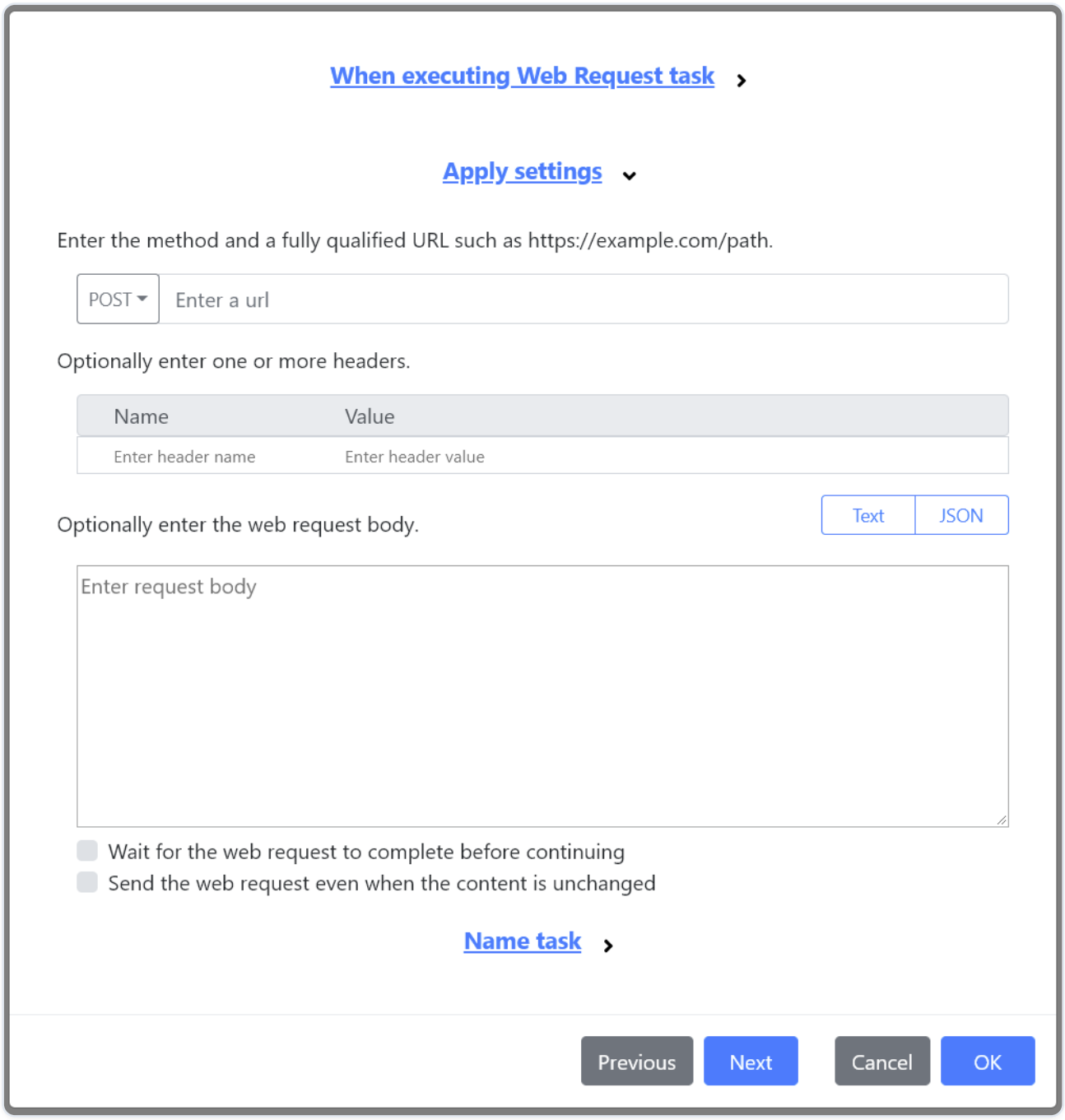
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

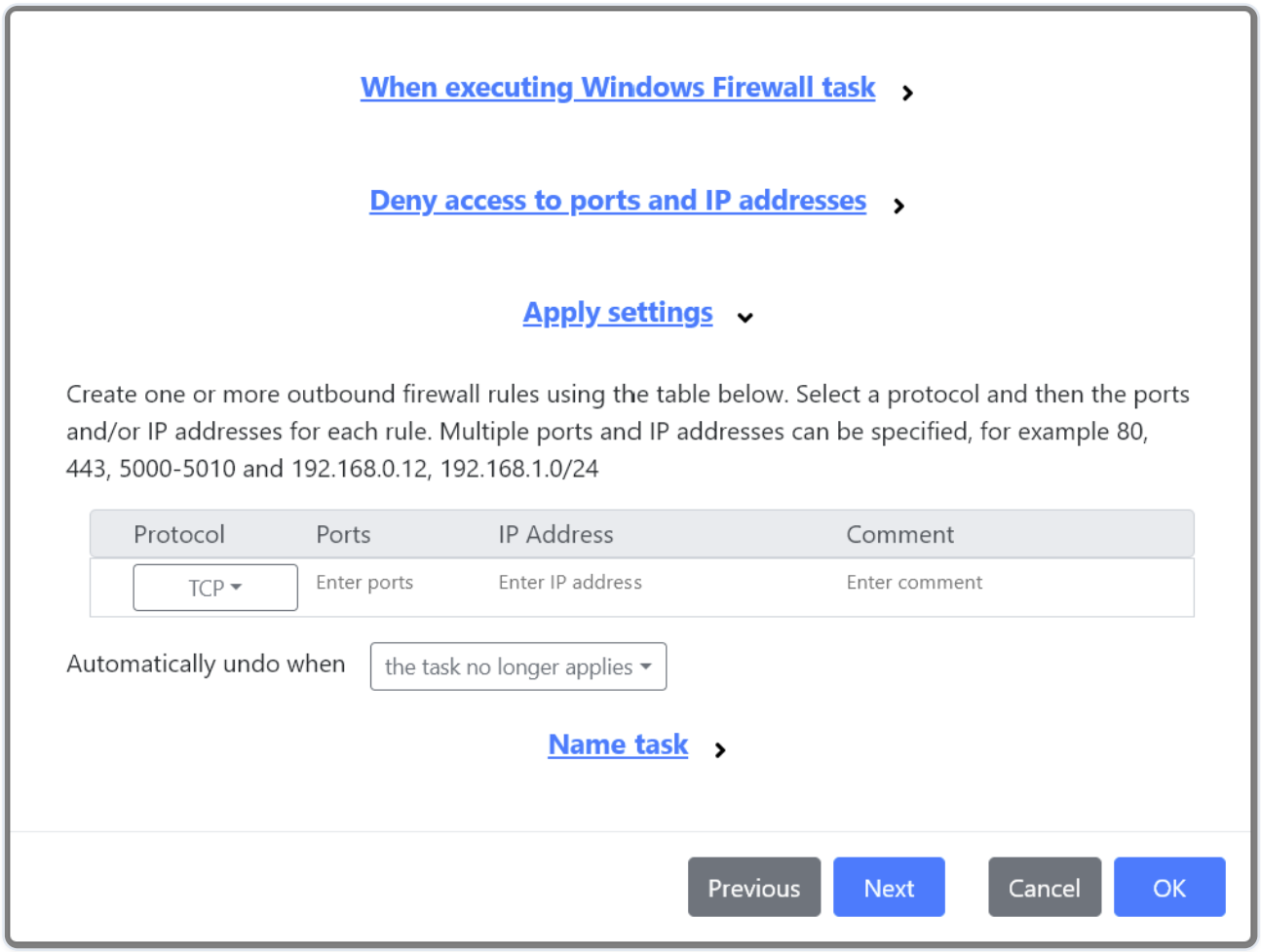
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

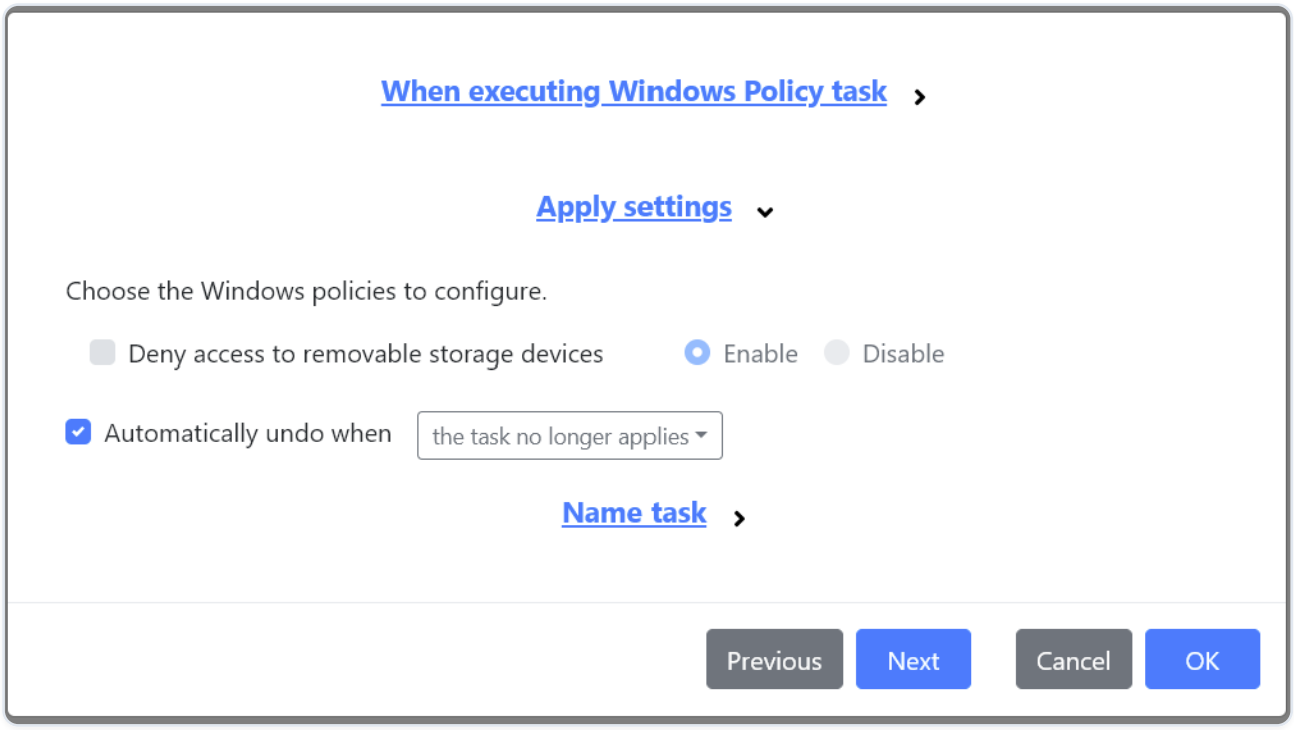
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Policy Task

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

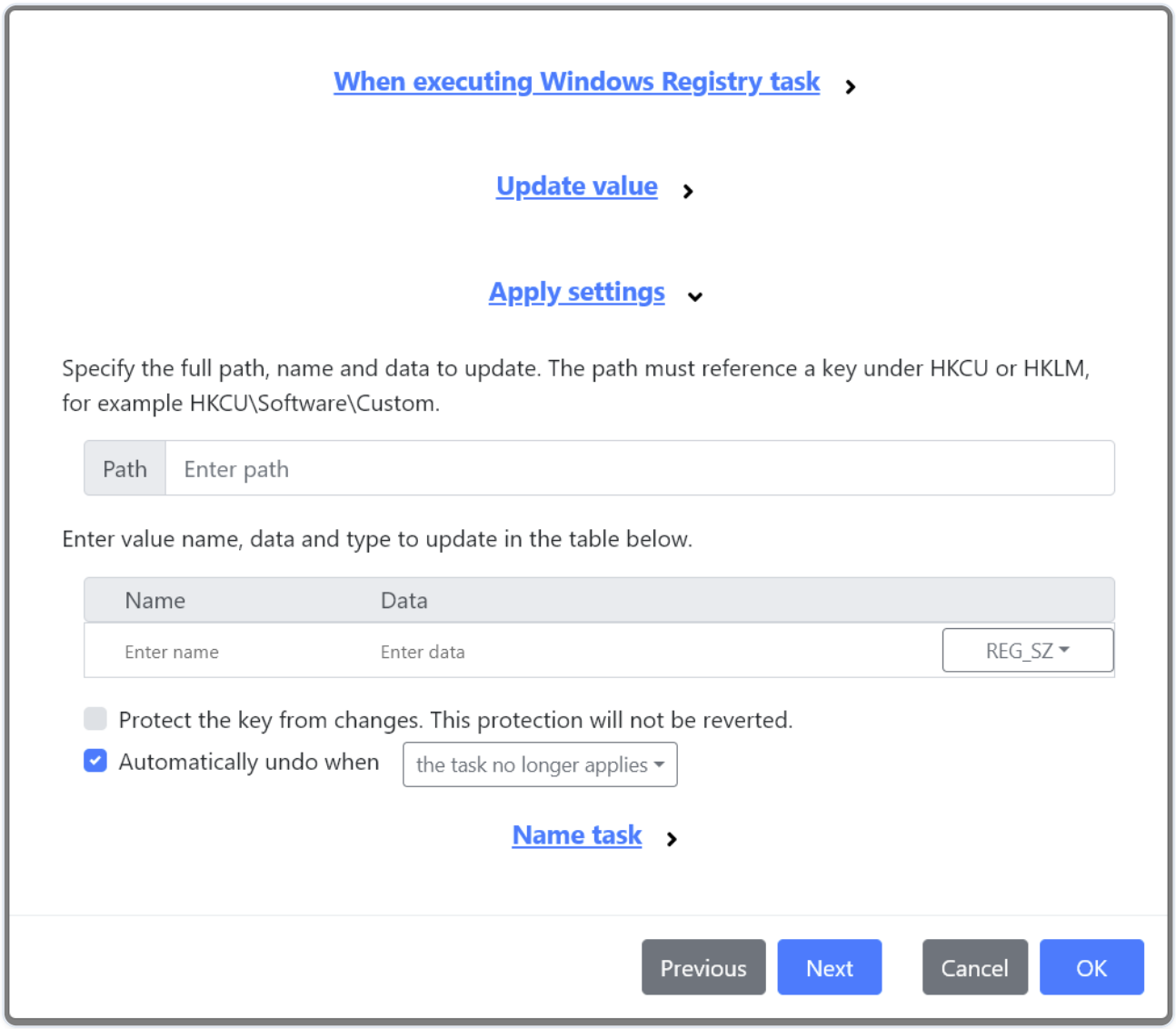
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Registry Task

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

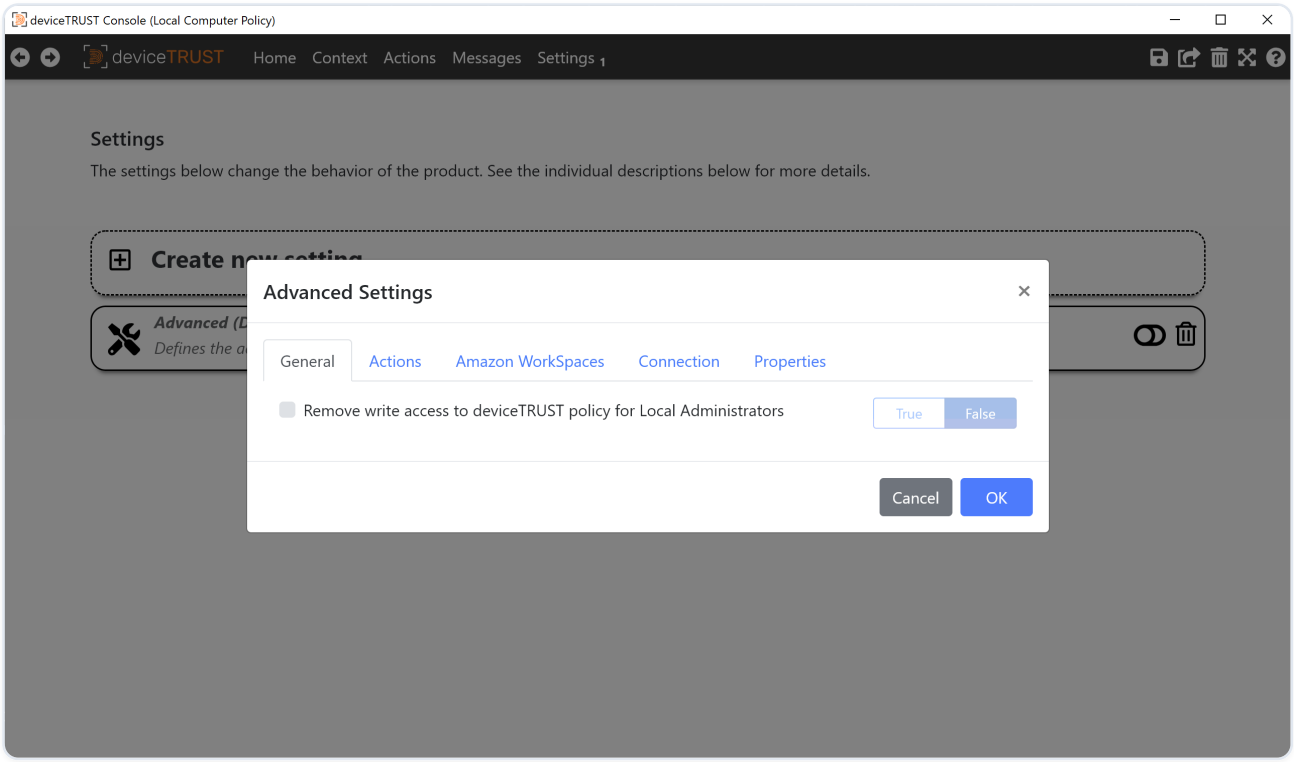
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Advanced Settings

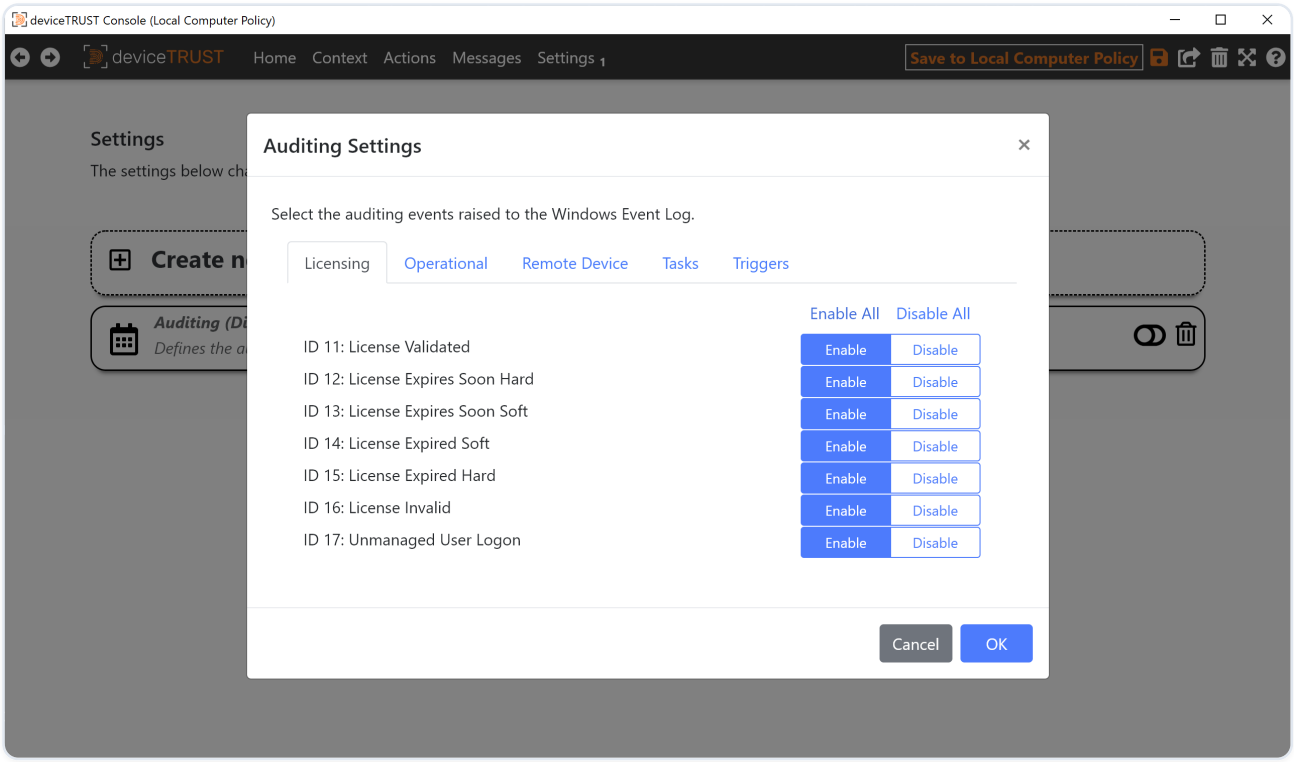
The `Advanced Settings` defines the advanced settings for configuring deviceTRUST® behavior.

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



Auditing Settings

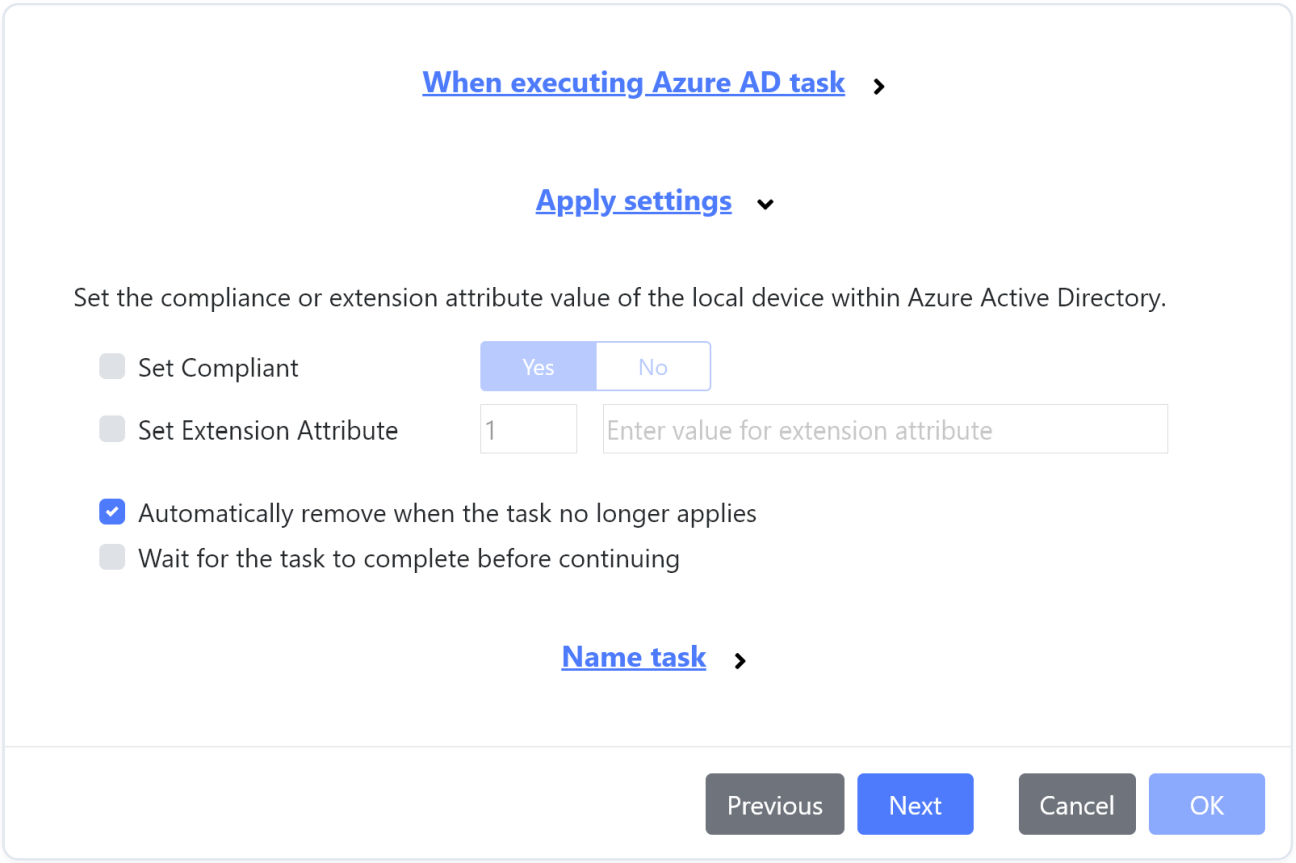
The `Auditing Settings` defines the audit events that are raised to the Windows Event Log.



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

Azure AD Settings

The `Azure AD Settings` defines the Tenant ID, Application (Client) ID and Secret required to manage Azure AD.



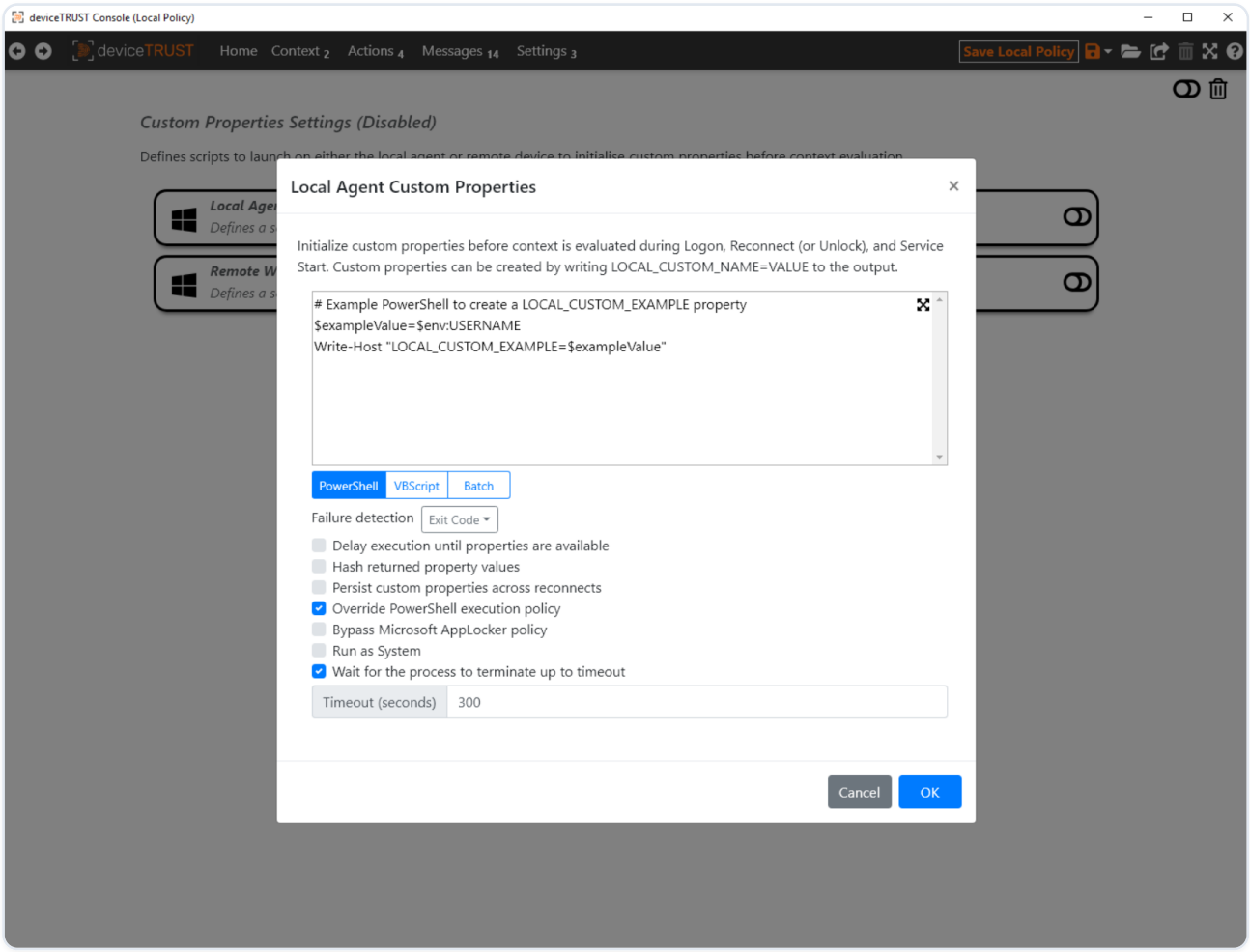
Custom Properties Settings

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

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:

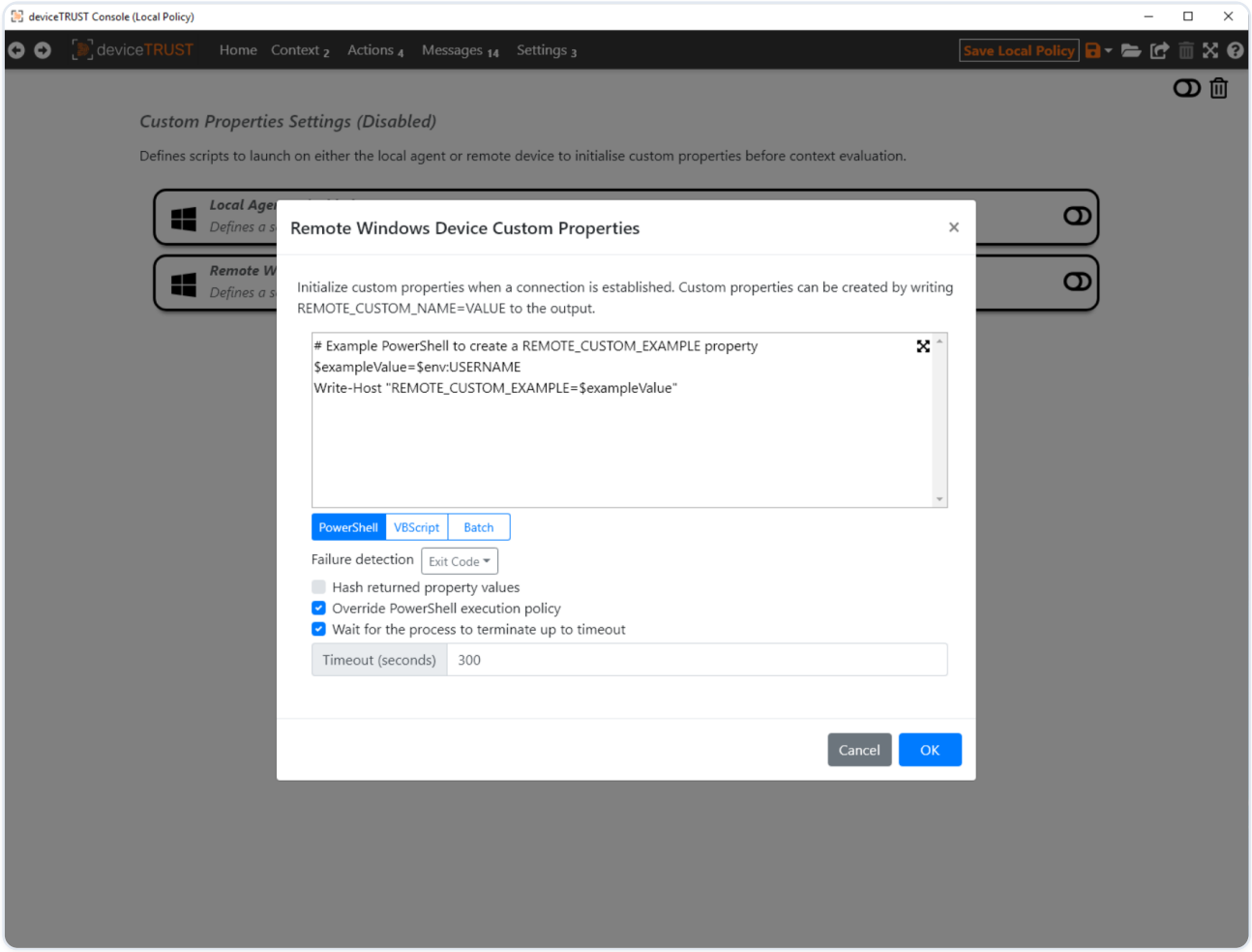
- *Embedded Script* - Defines the script that will be evaluated on the local agent.
- *Embedded Script Language* - Set to either PowerShell, VBScript or Batch, and defines the scripting language used by the embedded script.
- *Delay execution until properties are available* - When checked, will execute 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 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`.

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

- *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 at the start of the virtual session.



The following controls are available for the Remote Windows Device:

- *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.

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

- *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 Logon or Reconnect 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 by calling `Write-Host` in PowerShell, `WScript.Echo` in VBScript or `echo` within a Batch script.

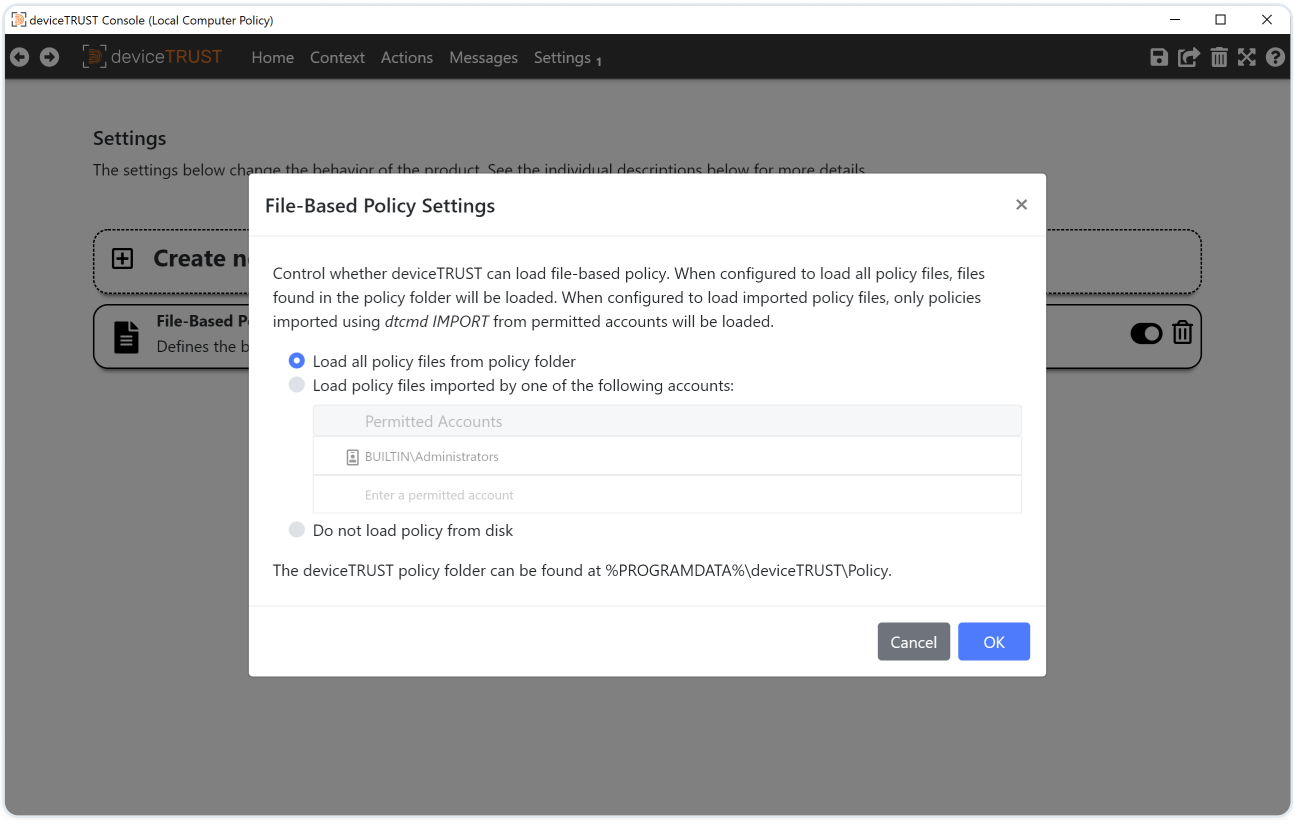
Custom Properties scripts can stay resident in memory for the lifetime of the session, perhaps by entering a loop or by registering for events. Custom properties can be created in the usual way, or deleted by outputing `DELETE LOCAL_CUSTOM_<NAME>` or `DELETE REMOTE_CUSTOM_<NAME>`. After all properties 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.

File-Based Policy Settings

The `File-Based Policy Settings` defines the behavior of file-based policy.

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



Settings

TABLE OF CONTENTS

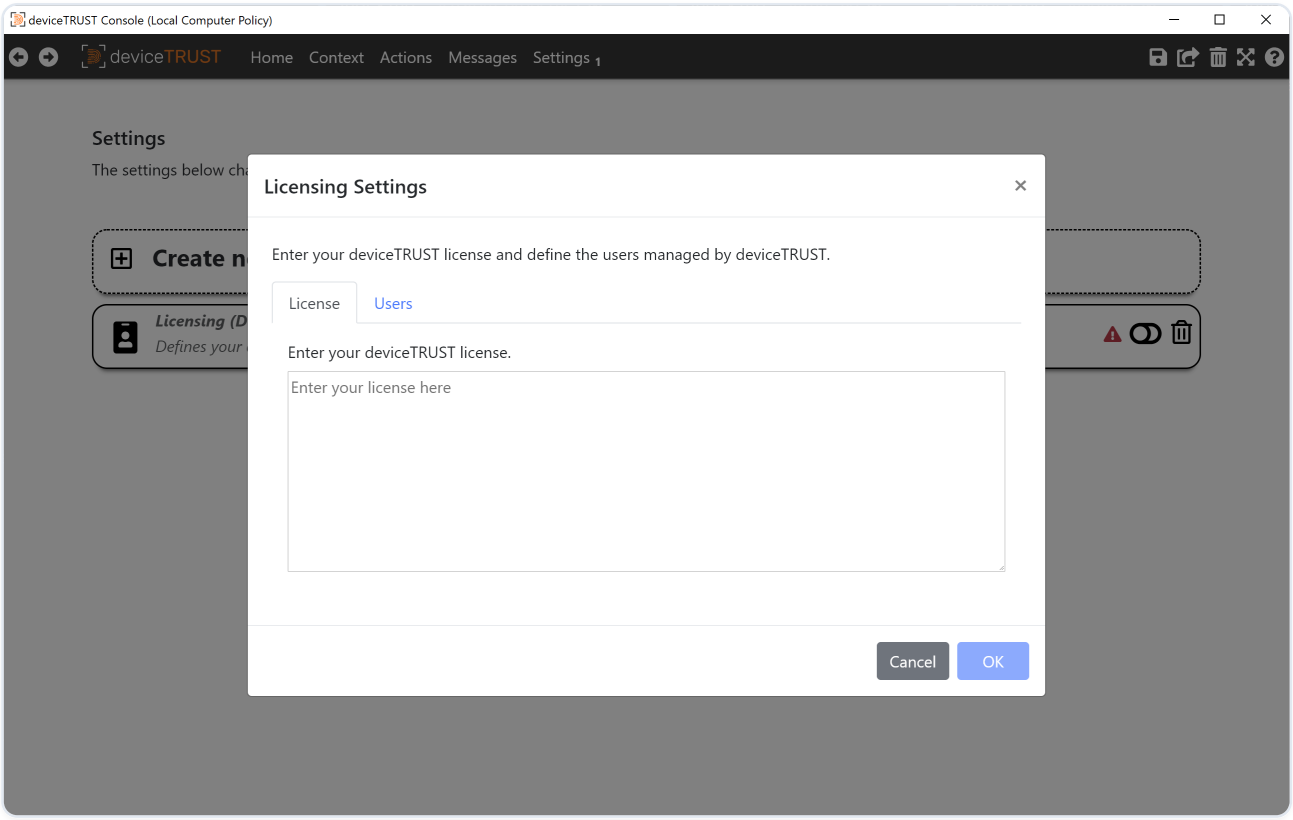
- Advanced - Defines the advanced settings for configuring deviceTRUST behavior.
- Auditing - Defines the audit events that are raised to the Windows Event Log.
- Azure AD - Defines the Tenant ID, Application (Client) ID and Secret required to manage Azure AD.
- Custom Properties - Defines a script launched 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.
- Printer - Defines the printer management options and the retry and timeout settings for the Map Printer task.

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

- 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.

Licensing Settings

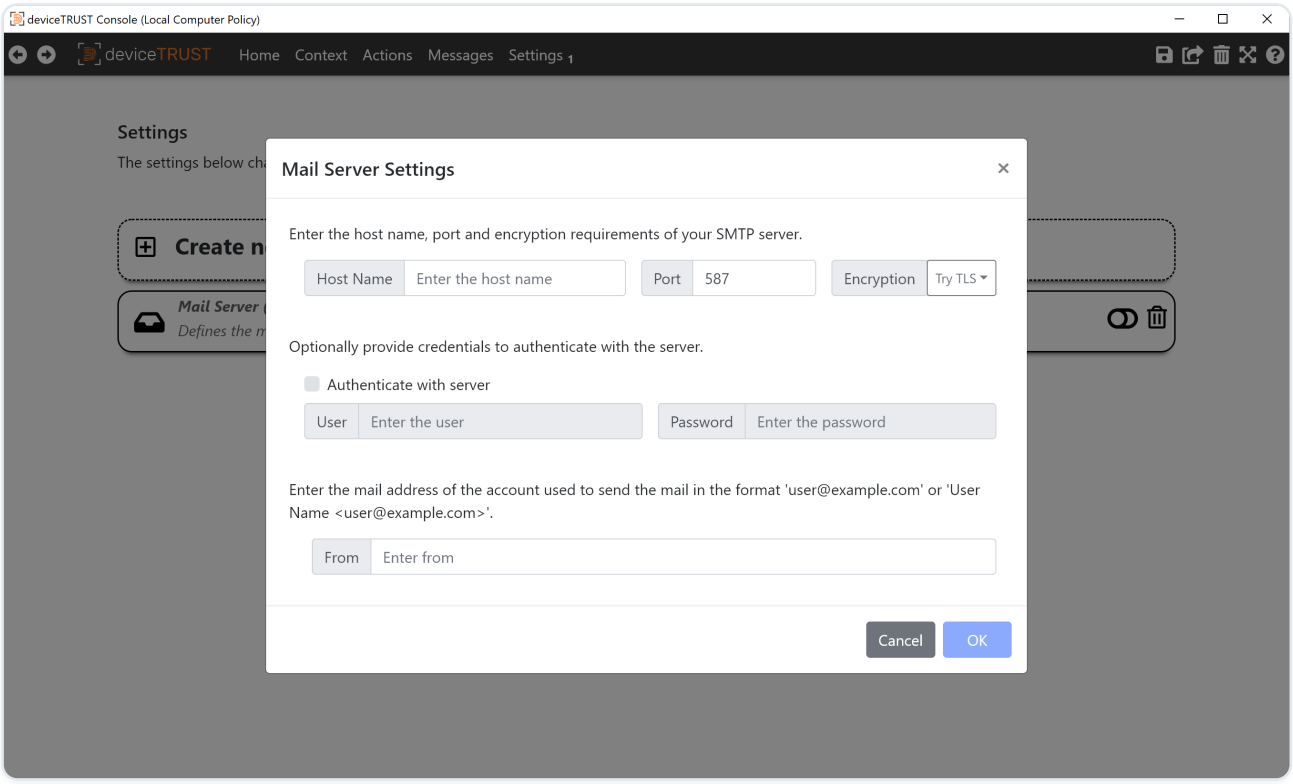
The `Licensing Settings` defines your deviceTRUST® license and the users managed by deviceTRUST.



Mail Server Settings

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

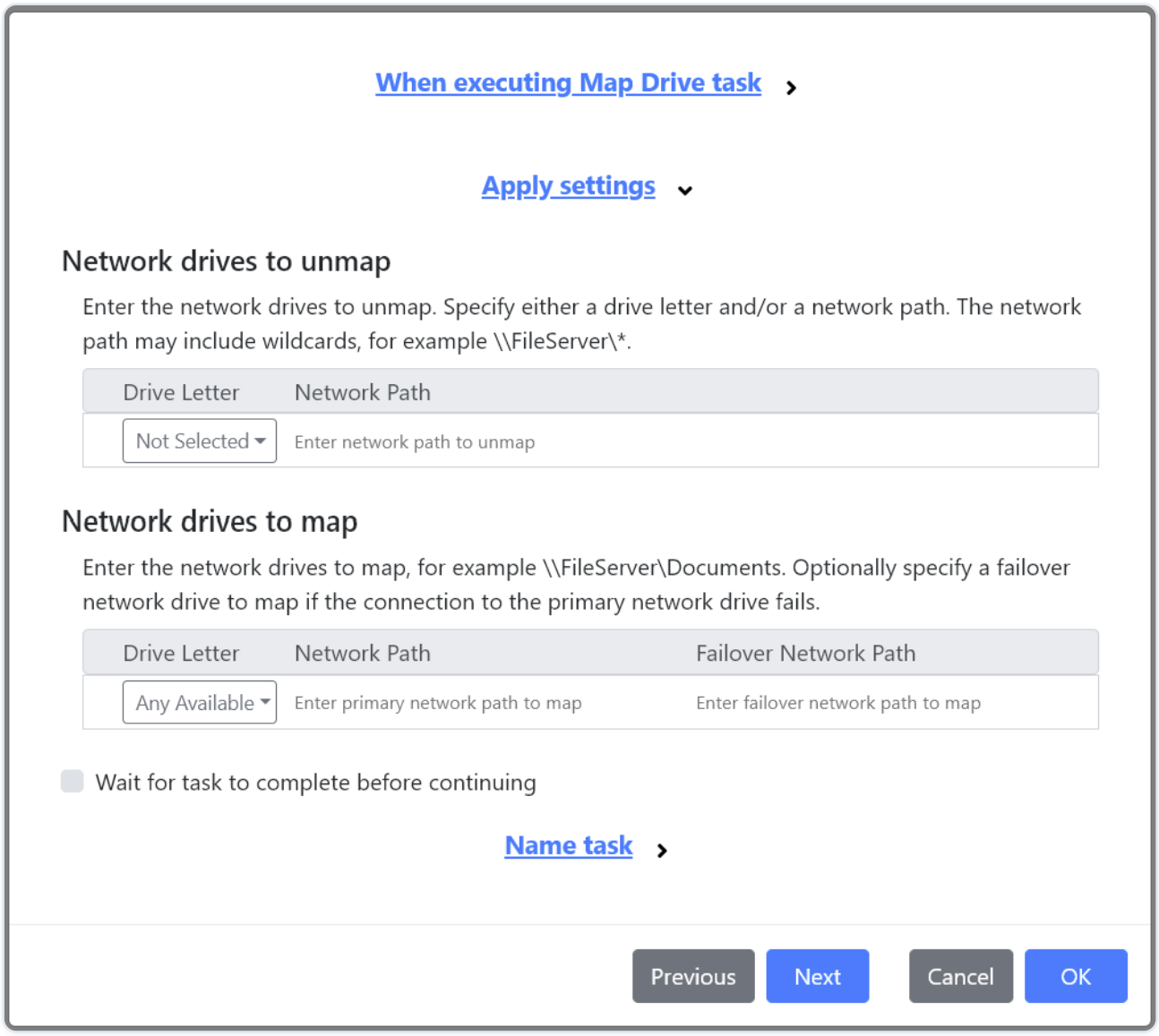
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Map Drive Settings

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

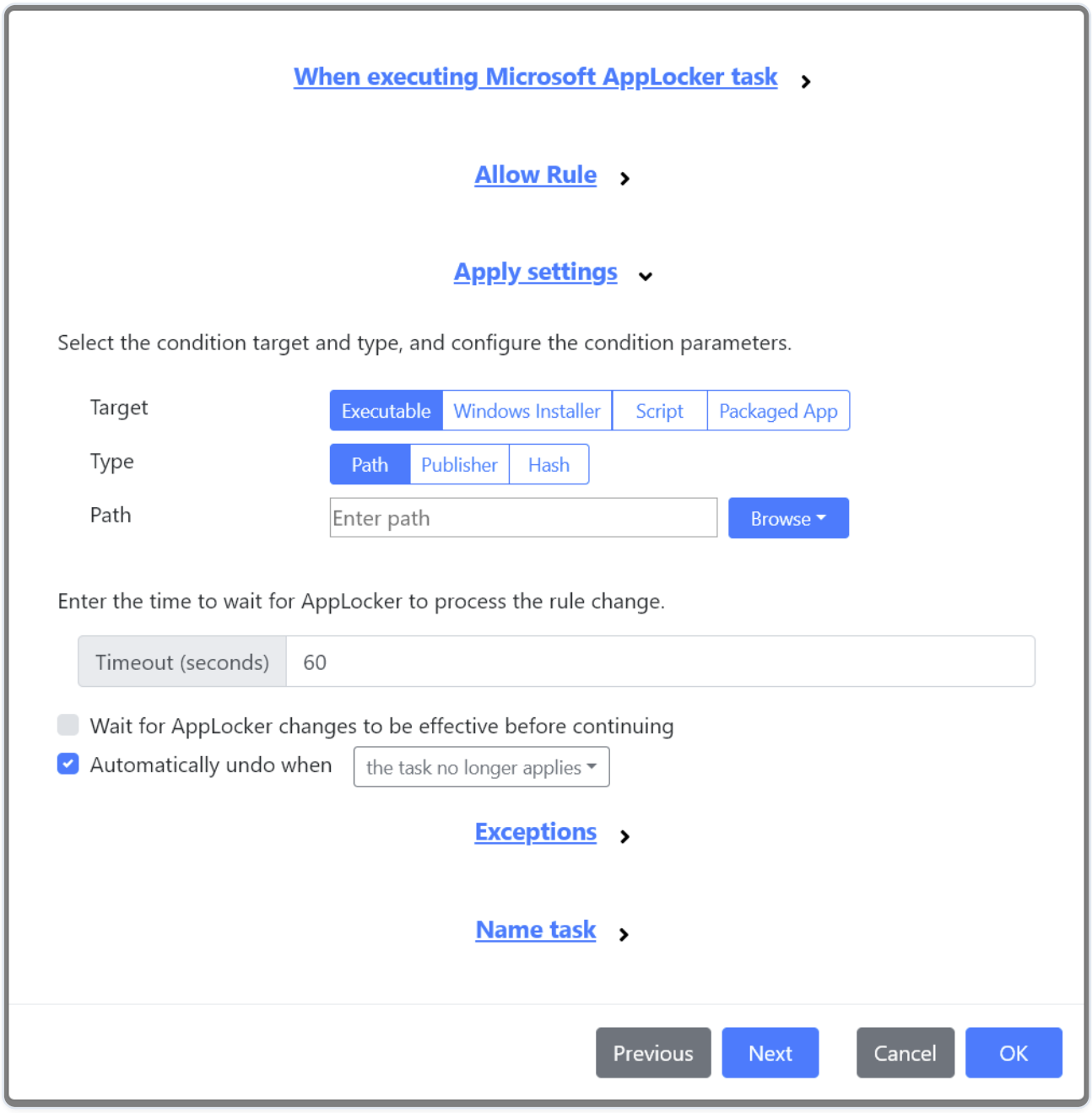
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft AppLocker Settings

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

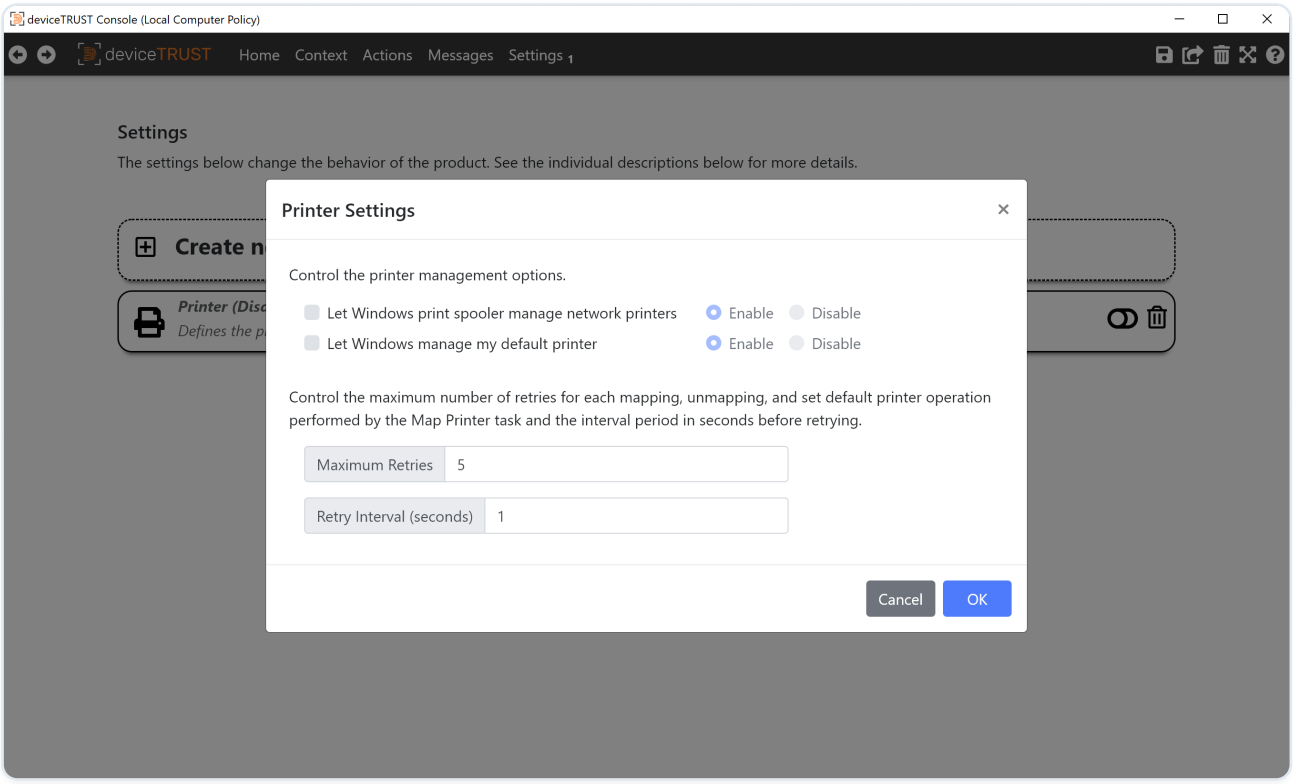
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Printer Settings

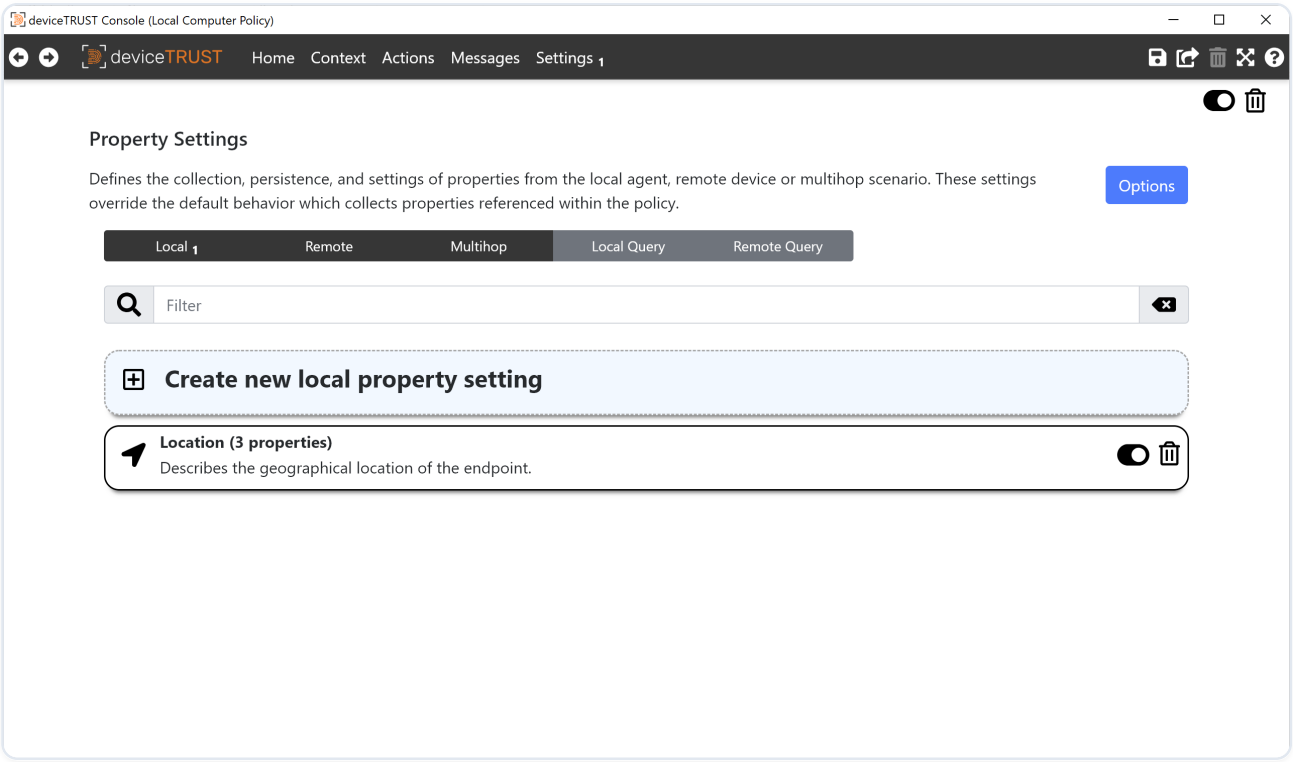
The `Printer Settings` define the printer management options and the retry and timeout settings for the Map Printer task.

© 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.

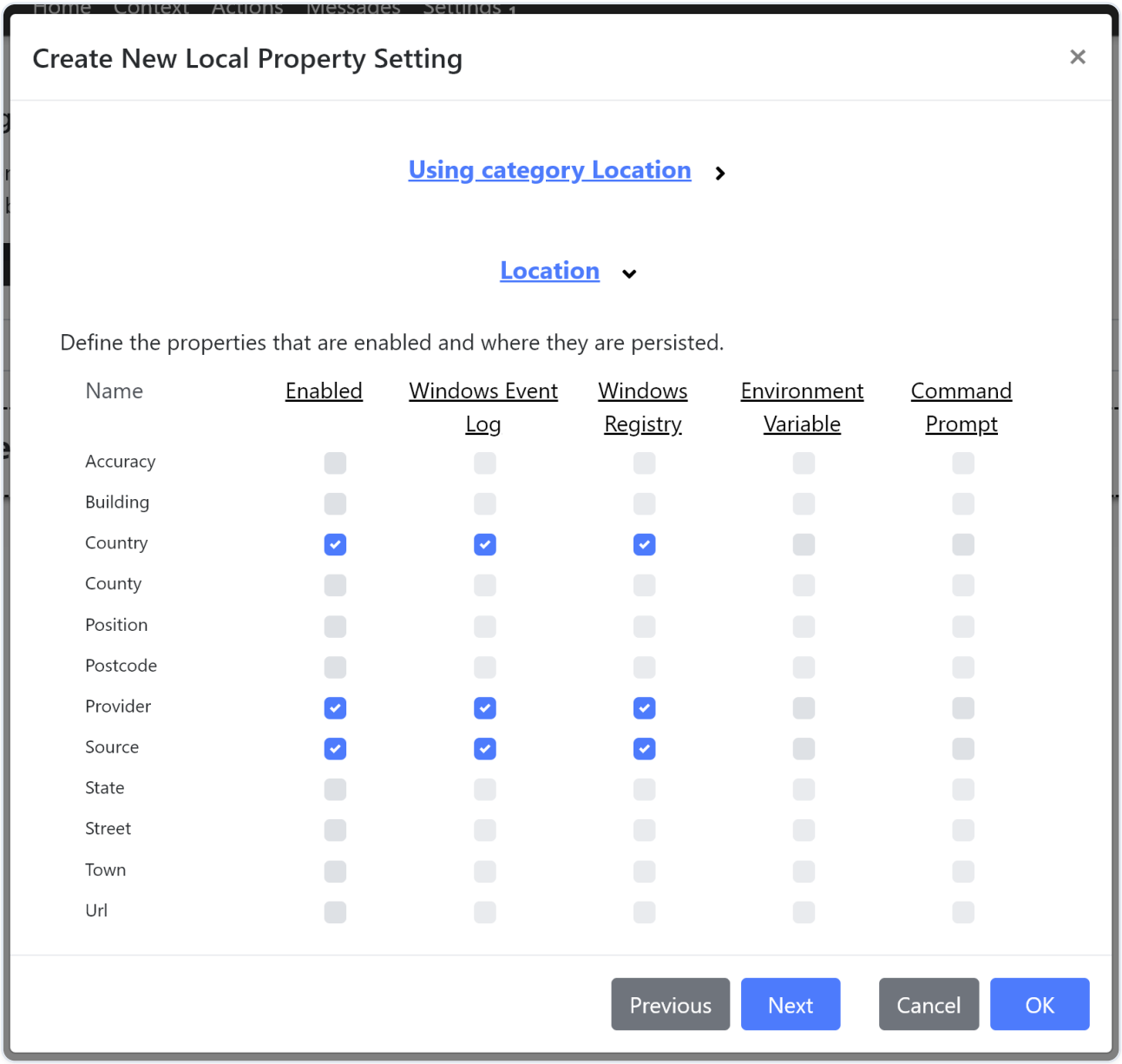


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

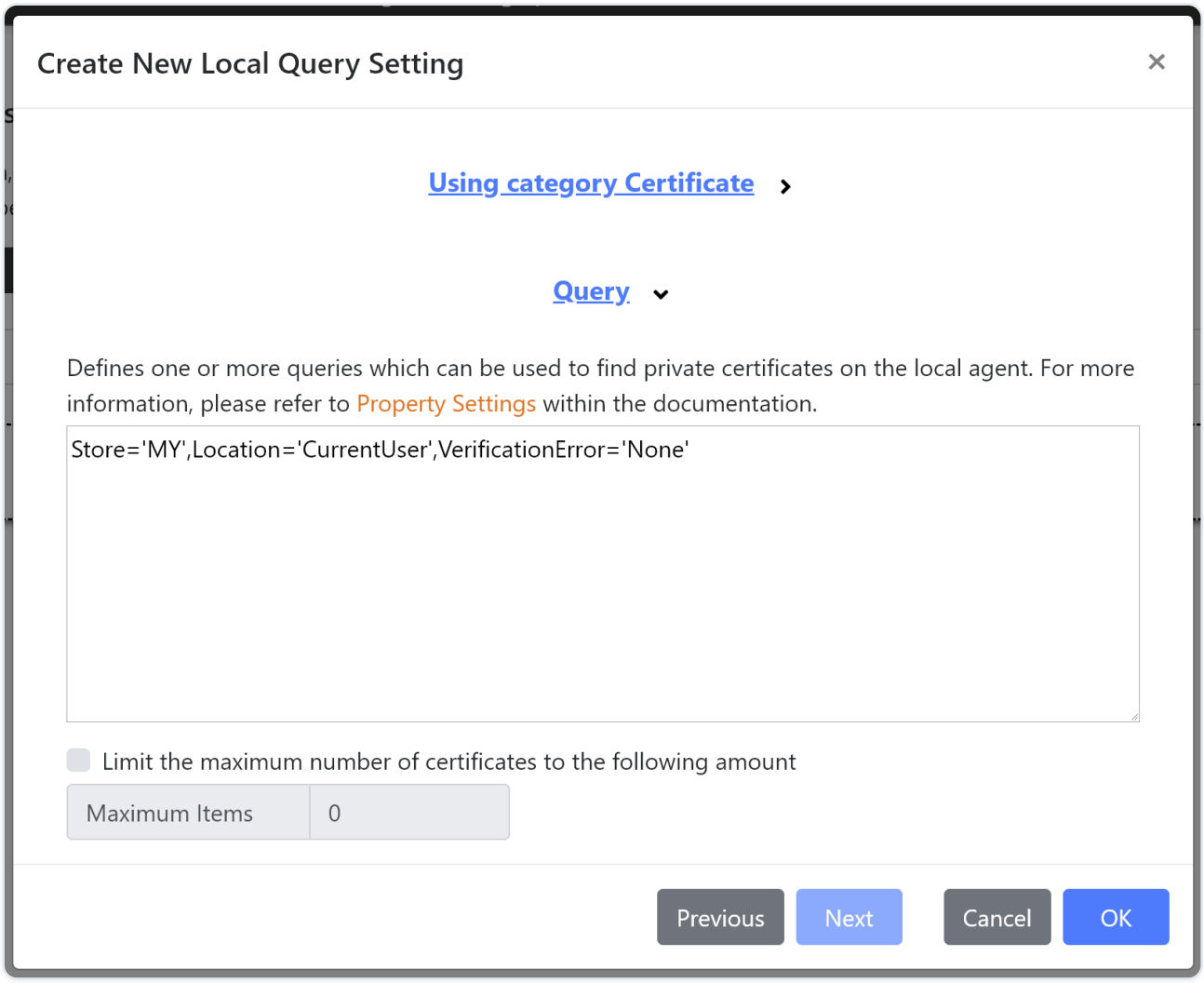
- `Enabled` - determines whether the property is collected from the device.
- `Windows Event Log` - determines whether the property is written to the Windows Event Log.
- `Windows Registry` - determines whether the property is written to the Windows Registry at `HKCU/Software/deviceTRUST/Properties`.
- `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.

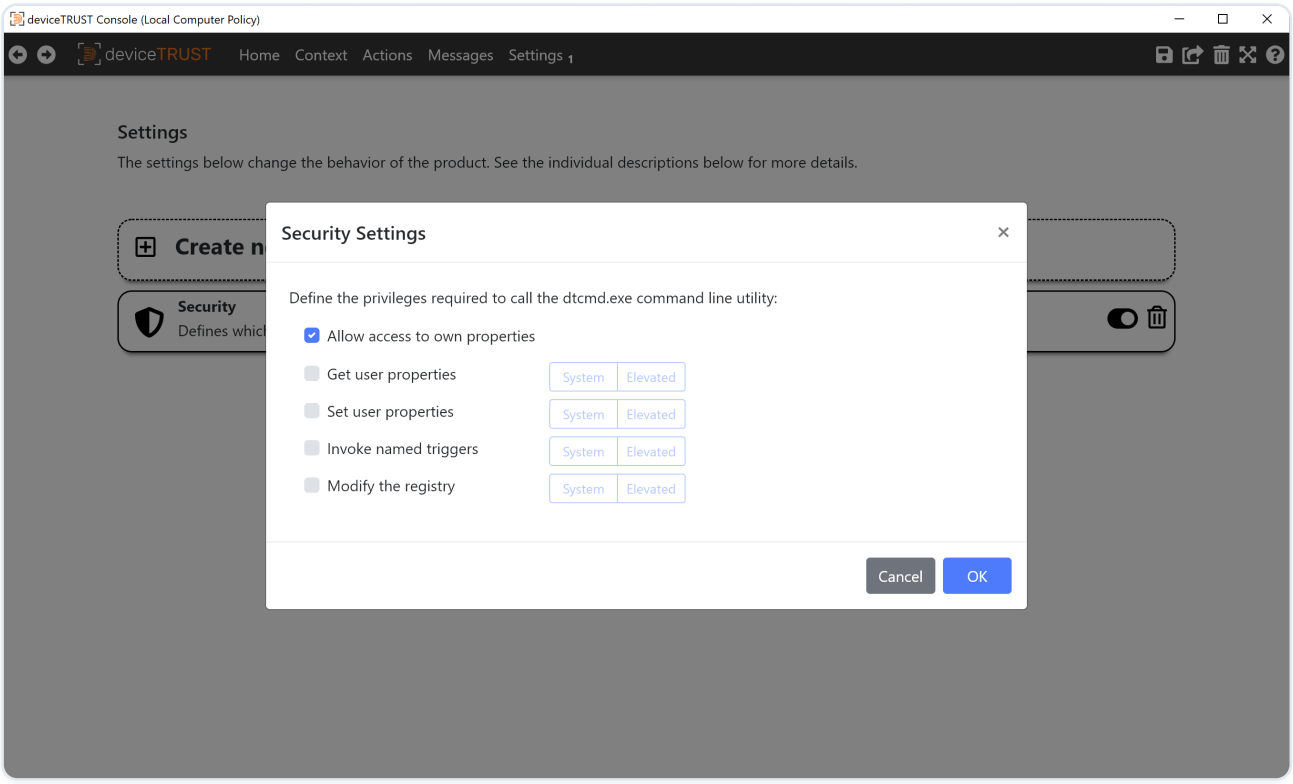
For example:

- 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

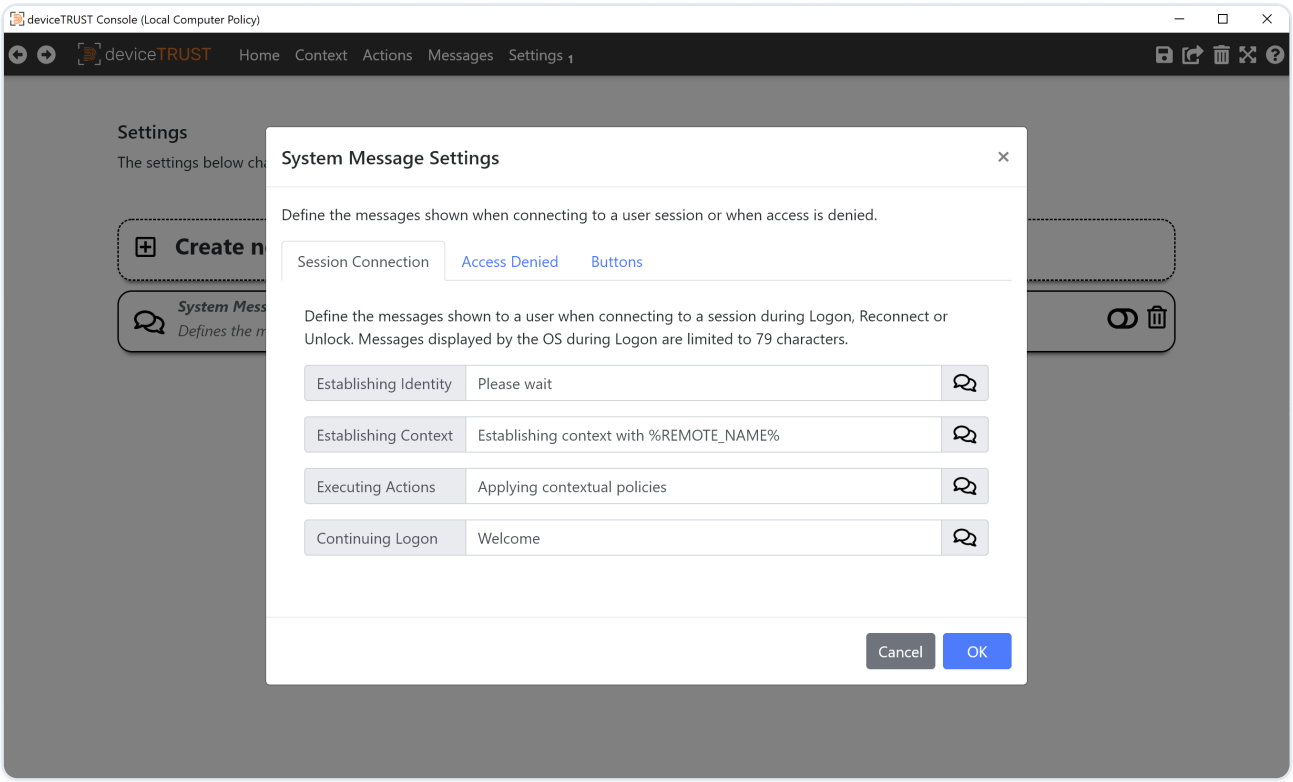
The `Security Settings` defines which external processes have permission to get or set properties, modify the registry, and invoke triggers.

© 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	IGEL OS	Unicon ™ eLux
BSSID							
The Basic Service Set Identifier (BSSID) of the access point. Dynamic property with text data type. Persists as LOCAL_ACCESSPOINT_X_BSSID for the local	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
agent and REMOTE_ACCESSPOINT_X_BSSID for the remote device.							
Count							
The number of available access points. Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_COUNT for the local agent and REMOT	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
E_ACCESSPOINT_COUNT for the remote device.							
Frequency							
The frequency of the response received from the access point, measured in kilohertz (kHz). Dynamic property with number data type. Persists as LOCAL_ACCESSPOI	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
NT_X_FREQUENCY for the local agent and REMOTE_ACCESSPOINT_X_FREQUENCY for the remote device.							
Quality							
The link quality measured as a percentage, with 100 being the highest link quality. Dynamic property with number data type. Persists	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
as LOCAL_ACCESSPOINT_X_QUALITY for the local agent and REMOTE_ACCESSPOINT_X_QUALITY for the remote device.							
Secure							
Set to true if the access point is secured. Dynamic property with boolean data type. Persists as	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
LOCAL_ACCESSPOINT_X_SECURE for the local agent and REMOTE_ACCESSPOINT_X_SECURE for the remote device.							
SSID							
The Service Set Identifier (SSID) of the access point. Dynamic property with text data type. Persists as LOCAL	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
_ACCESSPOINT_X_SSID for the local agent and REMOTE_ACCESSPOINT_X_SSID for the remote device.							
Strength							
The Received Signal Strength Indicator (RSSI) value measured in units of decibels referenced to 1.0 milliwatts (dBm).	✓	✓					

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

ACCESS POINT PROPERTY	AGENT	CLIENT EXTENSION					
Dynamic property with number data type. Persists as LOCAL_ACCESSPOINT_X_STRENGTH for the local agent and REMOTE_ACCESSPOINT_X_STRENGTH for the remote device.							

Browser Properties

BROWSER	AGENT	CLIENT EXTENSION					
Describes installed	Microsoft	Microsoft	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

BROWSER	AGENT	CLIENT EXTENSION					
internet browsers.	Windows	Windows					
Count							
The number of internet browsers. Realtime property with number data type. Persists as `LOCAL_BROWSER_COUNT` for the local agent and `REMOTE_BROWSER_COUNT` for the remote device.	✓	✓					
Default							

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

BROWSER	AGENT	CLIENT EXTENSION					
Determines whether the browser is the default. Realtime property with boolean data type. Persists as `LOCAL_BROWSER_X_DEFAULT` for the local agent and `REMOTE_BROWSER_X_DEFAULT` for the remote device.	✓	✓					
File Path							
The file path of the internet	✓	✓					

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

BROWSER	AGENT	CLIENT EXTENSION					
browser 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 device.							
Name							
The name of the internet browser. Realtime property	✓	✓					

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

BROWSER	AGENT	CLIENT EXTENSION					
with text data type. Persists as `LOCAL_BROWSER_X_NAME` for the local agent and `REMOTE_BROWSER_X_NAME` for the remote device.							
Version							
The version of the internet browser executable. Realtime property with text data type. Persists as `LOCAL_BROWSE`	✓	✓					

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

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

Cellular Properties

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
Describes the active cellular capabilities of an endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Class							
The cellular data class of the active	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
connection to the network provider. Realtime property with enum, text data types with options GPRS, EDGE, UTMS, HSDPA, HSUPA, HSPA, HSPA+, LTE, WCDMA, 1xRTT, 1xEVDO, 1xEVDV, 3xRTT, UMB, HRPD, NRNSA, NRSA. Persists as							

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_CELLULAR_CLASS` for the local agent and `REMOTE_CELLULAR_CLASS` for the remote device.							
Country							
The ISO-3166 country name of the country where the connected network provider resides. This value is only available for GSM devices.	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
Realtime property with text data type. Persists as `LOCAL_CELLULAR_COUNTRY` for the local agent and `REMOTE_CELLULAR_COUNTRY` for the remote device.							
Country Code							
The mobile country code (MCC) of the connected network provider. This	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
value is only available for GSM devices. Realtime property with number data type. Persists as `LOCAL_CELLULAR_COUNTRY_CODE` for the local agent and `REMOTE_CELLULAR_COUNTRY_CODE` for the remote device.							
ID							
For GSM devices, this is	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
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 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 as `LOCAL_CELLULAR_NETWORK_CODE` for the local agent and `REMOTE_CELLULAR_NETWORK_`	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
`CODE` for the remote device.							
Network Name							
The name of the connected network provider. Realtime property with text data type. Persists as `LOCAL_CELLULAR_NETWORK` for the local agent and `REMOTE_CELLULAR_NETWORK` for the	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Product							
The product name of the device providing the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLULAR_PRODUCT` for the local agent and `REMOTE_CELLULAR_PRODUCT` for the remote device.	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
Roaming							
Determines whether the connected network provider is different to the home provider defined by the SIM. Realtime property with boolean data type. Persists as `LOCAL_CELLULAR_ROAMING` for the local agent and `REMOTE_CELLU`	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
`LAR_ROAMING` for the remote device.							
Type							
The cellular communication type supported by the device. Realtime property with enum data type with options GSM, CDMA. Persists as `LOCAL_CELLULAR_TYPE` for the local agent and `REMOTE`	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
`_CELLULAR_TYPE` for the remote device.							
Vendor							
The vendor name of the device providing the cellular service. Realtime property with text data type. Persists as `LOCAL_CELLULAR_VENDOR` for the local agent and `REMOTE_CELLULAR_VENDOR` for the	✓	✓					

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

CELLULAR PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							

Certificate Properties

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
Describes the private certificates availabl e within the users certificat e store.	Microso ft Window s	Microso ft Window s	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Count							
The number of installed certificat es. Dynami c property with number data type. Persists	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_CERTIFICATE_COUNT` for the local agent and `REMOTE_CERTIFICATE_COUNT` for the remote device.							
Extended Usage							
The valid extended usages of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIF`	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`ICATE_X_EXTENDEDUSAGE` for the local agent and `REMOTE_CERTIFICATE_X_EXTENDEDUSAGE` for the remote device.							
Issuer							
The name of the certificate authority that issued the certificate. Dynamic property with text data type. Persists as	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_CERTIFICATE_X_ISSUER` for the local agent and `REMOTE_CERTIFICATE_X_ISSUER` for the remote device.							
Location							
The location of the certificate, such as 'Current User'. Dynamic property with enum data type with options Current	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
User, Local Machine. Persists as `LOCAL_CERTIFICATE_X_LOCATION` for the local agent and `REMOTE_CERTIFICATE_X_LOCATION` for the remote device.							
Name							
The name of the certificate. Dynamic property with text data type. Persists	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_CERTIFICATE_X_NAME` for the local agent and `REMOTE_CERTIFICATE_X_NAME` for the remote device.							
Not After							
The date after which the certificate expires. Dynamic property with datetime data type. Persists as	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_CERTIFICATE_X_NOTAFTER` for the local agent and `REMOTE_CERTIFICATE_X_NOTAFTER` for the remote device.							
Not Before							
The date after which the certificate becomes valid. Dynamic property with datetime data type. Persists	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_CERTIFICATE_X_NOTBEFORE` for the local agent and `REMOTE_CERTIFICATE_X_NOTBEFORE` for the remote device.							
Policies							
The certificate policies identifying the intended purpose of the certificate. Dynamic property with text data	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_CERTIFICATE_X_POLICIES` for the local agent and `REMOTE_CERTIFICATE_X_POLICIES` for the remote device.							
Root Name							
The root name of the certificate. Dynamic property with text data type. Persists as `LOCAL_`	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`CERTIFICATE_X_ROOT_NAME` for the local agent and `REMOTE_CERTIFICATE_X_ROOT_NAME` for the remote device.							
Root Thumbprint SHA256							
The SHA256 Thumbprint of the root certificate. Dynamic property with text data type. Persists as `LOCAL_`	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`CERTIFICATE_X_ROOT_THUMBPRINT_SHA256` for the local agent and `REMOTE_CERTIFICATE_X_ROOT_THUMBPRINT_SHA256` for the remote device.							
Serial Number							
The serial number of the certificate. Dynamic property with text data type. Persists	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_CERTIFICATE_X_SERIALNUMBER` for the local agent and `REMOTE_CERTIFICATE_X_SERIALNUMBER` for the remote device.							
Signature Algorithm							
The algorithm used to create the certificate. Dynamic property with text data	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_CERTIFICATE_X_SIGNATUREALGORITHM` for the local agent and `REMOTE_CERTIFICATE_X_SIGNATUREALGORITHM` for the remote device.							
Store							
The name of the store which contains the certificate, such as 'My'. Dynamic	✓	✓	✓				

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

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

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
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 template which was used to generate the certificate. Dynamic property with text	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `LOCAL_CERTIFICATE_X_TEMPLATE` for the local agent and `REMOTE_CERTIFICATE_X_TEMPLATE` for the remote device.							
Thumbprint SHA256							
The SHA256 Thumbprint of the certificate. Dynamic property with text data	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_CERTIFICATE_X_THUMBPRINT_SHA256` for the local agent and `REMOTE_CERTIFICATE_X_THUMBPRINT_SHA256` for the remote device.							
TPM Key Attestation							
Detects the key attestation issuance policies which prove to	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
a CA that the certificate is protected by a trusted TPM. Dynamic property with enum data type with options None, User Credentials, Hardware Certificate, Hardware Key. Persists as `LOCAL_CERTIFICATE_X_TPM_KEY_ATTESTATION` for the local agent							

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_CERTIFICATE_X_TPM_KEY_ATTESTATION` for the remote device.							
Usage							
The valid usages of the certificate. Dynamic property with text data type. Persists as `LOCAL_CERTIFICATE_X_USAGE` for the local agent and `REMOTE_CERTI`	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`FICATE_X_USAGE` for the remote device.							
Verification Error							
Describes why the certificate failed verification. Dynamic property with enum data type with options None, Cannot Be Verified, Revoked, Untrusted Root, Untrusted Test	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
Root, Chaining, Wrong Usage, Expired, Invalid Name, Invalid Policy, Basic Constraints, Critical, Validity Period Nesting, No Revocation Check, Revocation Offline. Persists as `LOCAL_CERTIFICATE_X_VERIFICATIONERROR` for the local agent and `REMOTE_CERTI`							

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`FICATE_X_VERIFICATIONERROR` for the remote device.							
Version							
The x509 format version of the certificate. Dynamic property with enum data type with options Version 1, Version 2, Version 3. Persists as `LOCAL_CERTIFICATE_`	✓	✓	✓				

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

CERTIFICATE PROPERTY	AGENT	CLIENT EXTENSION					
`X_VERSION` for the local agent and `REMOTE_CERTIFICATE_X_VERSION` for the remote device.							

ChromeOS Properties

CHROMEOS PROPERTY	AGENT	CLIENT EXTENSION					
Provides properties unique to a Chrome OS device.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Asset ID							
The administrator-annotat					✓		

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

CHROMEOS PROPERTY	AGENT	CLIENT EXTENSION					
ed Asset ID. Static property with text data type. Persists as `REMOTE_CHROMEOS_ASSETID` for the remote device.							
Directory Device ID							
The directory device ID. Static property with text data type. Persists as `REMOTE_CHROMEOS_DIRECTOR`					✓		

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

CHROMEOS PROPERTY	AGENT	CLIENT EXTENSION					
`YDEVICEID` for the remote device.							
Location							
The administrator-annotated Location. Static property with text data type. Persists as `REMOTE_CHROMEOS_LOCATION` for the remote device.					✓		

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

Custom Properties

CUSTOM PROPERTY	AGENT	CLIENT EXTENSION					
Provides a condition that can operate on any property, including custom properties created using 'dtcmd.exe'.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	UniconeLux
Condition							
This is a placeholder custom property to allow the creation of a custom condition. This text does	✓	✓		✓		✓	

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

CUSTOM PROPERTY	AGENT	CLIENT EXTENSION					
not appear within the console. Realtime property with text, number, boolean, datetime, ip, position data types. Persists as `LOCAL_CUSTOM_CONDITION` for the local agent and `REMOTE_CUSTOM_CONDITION` for the remote device.							

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

deviceTRUST Properties

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
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.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Connected							
Determines whether	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
the deviceTRUST Agent has established a connection with the deviceTRUST Client Extension. Static property with boolean data type. Persists as `LOCAL_DEVICETRUST_CONNECTED` for the local agent.							
License Count							
Determines the number of	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
deviceTRUST licensed units. Static property with number data type. Persists as `LOCAL_DEVICE TRUST_ LICENS E_COUN T` for the local agent.							
License Expiry Date							
Determines the date that the deviceTRUST license expires. Static property with datetime data	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_DEVICETRUST_LICENSE_EXPIRYDATE` for the local agent.							
License Issue Date							
Determines the date that the deviceTRUST license was issued. Static property with datetime data type. Persists as `LOCAL_DEVICETRUST_LICENS`	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
`E_ISSUEDATE` for the local agent.							
License Type							
Determines the deviceTRUST license type. Static property with text data type. Persists as `LOCAL_DEVICE TRUST_LICENSE_TYPE` for the local agent.	✓	✓					
License Unit							
Determines the deviceTRUST licensab	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
le unit, e.g., a User or Device. Static property with enum data type with options User, Device, Unlimited. Persists as `LOCAL_DEVICE TRUST_ LICENS E_UNIT` for the local agent.							
License Valid							
Determines whether the deviceTRUST license is valid.	✓	✓					

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
Static property with boolean data type. Persists as `LOCAL_DEVICE TRUST_ LICENS E_VALI D` for the local agent.							
Version							
The version of the deviceT RUST softwar e. Static property with version data type. Persists as `LOCAL_ DEVICE TRUST_ VERSIO N` for	✓	✓	✓	✓		✓	✓

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

DEVICE TRUST PROPERTY	AGENT	CLIENT EXTENSION					
the local agent and `REMOTE_DEVICETRUST_VERSION` for the remote device.							

Display Properties

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
Describes the displays available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Adapter Product							
The product name of the display adapter. Realtime	✓	✓	✓				

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
property with text data type. Persists as `LOCAL_DISPLAY_X_ADAPTER_PRODUCT` for the local agent and `REMOTE_DISPLAY_X_ADAPTER_PRODUCT` for the remote device.							
Adapter Vendor							
The vendor of the display adapter. Realtime property with text data	✓	✓	✓				

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_DISPLAY_X_ADAPTER_VENDOR` for the local agent and `REMOTE_DISPLAY_X_ADAPTER_VENDOR` for the remote device.							
BPP							
The number of bits per pixel. Realtime property with number data type. Persists as	✓	✓	✓	✓		✓	✓

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

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

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_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 the local agent and `REMOTE_DISPLAY_X_DPI` for the remote device.	✓	✓	✓	✓		✓	✓

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
Height							
The height of the screen in pixels. Realtime property with number data type. Persists as `LOCAL_DISPLAY_X_HEIGHT` for the local agent and `REMOTE_DISPLAY_X_HEIGHT` for the remote device.	✓	✓	✓	✓		✓	✓
Monitor External							
Set to true	✓	✓	✓				

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
when the monitor 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_MONITOR_EXTERNAL` for the remote device.							
Monitor Product							

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
The monitor's product name. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_PRODUCT` for the local agent and `REMOTE_DISPLAY_X_MONITOR_PRODUCT` for the remote device.	✓	✓	✓				
Monitor Serial Number							

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
The serial number of the monitor. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_SERIAL NUMBER` for the local agent and `REMOTE_DISPLAY_X_MONITOR_SERIALNUMBER` for the remote device.	✓	✓	✓				
Monitor Vendor							

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
The vendor of the monitor. Realtime property with text data type. Persists as `LOCAL_DISPLAY_X_MONITOR_VENDOR` for the local agent and `REMOTE_DISPLAY_X_MONITOR_VENDOR` for the remote device.	✓	✓	✓				
Name							
The name of the display adapter.	✓			✓		✓	✓

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
Realtime property with text data type. Persists 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 property with number data type.	✓	✓	✓	✓		✓	✓

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

DISPLAY PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_DISPLAY_X_WIDTH` for the local agent and `REMOTE_DISPLAY_X_WIDTH` for the remote device.							

Domain Properties

DOMAIN PROPERTY	AGENT	CLIENT EXTENSION					
Describes the domain membership of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
DNS							
The Domain Name	✓	✓	✓				

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

DOMAIN PROPERTY	AGENT	CLIENT EXTENSION					
System (DNS) name of the domain. Static property with text data type. Persists 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 Active Director	✓	✓					

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

DOMAIN PROPERTY	AGENT	CLIENT EXTENSION					
y this is the domain SID. When joined to Azure Active Directory this is the tenant ID. Static property with text data type. Persists as `LOCAL_DOMAIN_ID` for the local agent and `REMOTE_DOMAIN_ID` for the remote device.							
Join							
Determines the type of	✓	✓	✓				

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

DOMAIN PROPERTY	AGENT	CLIENT EXTENSION					
domain that is joined. Static property with enum data type with options None, Workgroup, Domain, Azure AD. Persists as `LOCAL_DOMAIN_JOIN` for the local agent and `REMOTE_DOMAIN_JOIN` for the remote device.							
Name							
The name of the	✓	✓	✓				

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

DOMAIN PROPERTY	AGENT	CLIENT EXTENSION					
domain. Static property with text data type. Persists as `LOCAL_DOMAIN_NAME` for the local agent and `REMOTE_DOMAIN_NAME` for the remote device.							

eLux Properties

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
Provides properties unique to an eLux device.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
Environment Variable Count							
The number of ELUX environment variables. Static property with number data type. Persists as `REMOTE_ELUX_ENVIRONMENT_COUNT` for the remote device.							✓
Environment Variable Name							
The name of the ELUX environment							✓

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
variable. Static property with text data type. Persists as `REMOTE_ELUX_ENVIRONMENT_X_NAME` for the remote device.							
Environment Variable Value							
The value of the ELUX environment variable. Static property with text, number, boolean, datetime, ip data							✓

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

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

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
property of 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 property with text data type. Persists as `REMOTE_ELUX_INFO2` for the remote device.							✓

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
Info3							
The Info3 property of the eLux device. Static property with text data type. Persists as `REMOTE_ELUX_INFO3` for the remote device.							✓
Organization Unit ID							
The ID property of the Organization Unit containing the eLux device. Static property with							✓

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
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 server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIF`							✓

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
`ICATE_SERIAL NUMBER` for the remote device.							
Scout Cert Subject							
The subject of the certificate used to connect to the eLux Scout server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_SUBJECT` for the remote device.							✓

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
Scout Cert Thumbprint SHA256							
The SHA256 thumbprint of the certificate used to connect to the eLux Scout server. Static property with text data type. Persists as `REMOTE_ELUX_SCOUT_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.							✓

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

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

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

ELUX PROPERTY	AGENT	CLIENT EXTENSION					
as `REMOTE_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 `REMOTE_ELUX_SCOUT_VERSION` for the remote device.							✓

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

Hardware Properties

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
Describes the hardware and its capabilities.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
BIOS Release 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_HARDW`	✓	✓		✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
`ARE_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 as `LOCAL_HARDWARE_BIOS_SERIAL` for the local agent and `REMOTE_HARDWARE_BIOS_SER`	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
`IAL` for the remote device.							
BIOS Version							
The version number of the BIOS. Static property with version data type. Persists as `LOCAL_HARDWARE_BIOS_VERSION` for the local agent and `REMOTE_HARDWARE_BIOS_VERSION` for the remote device.	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
CPU							
The CPU availabl e on the device. Static property with text data type. Persists as `LOCAL_HARDWARE_CPU` for the local agent and `REMOTE_HARDWARE_CPU` for the remote device.	✓	✓	✓	✓	✓	✓	✓
CPU Count							
The number of CPUs. Static property	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
with number data type. Persists as `LOCAL_HARDWARE_CPU_COUNT` for the local agent and `REMOTE_HARDWARE_CPU_COUNT` for the remote device.							
CPU Speed							
The speed of the CPU in MHz. Static property with number data type. Persists	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_HARDWARE_CPU_SPEED` for the local agent and `REMOTE_HARDWARE_CPU_SPEED` for the remote device.							
Lid							
Determines if the lid of the device is open or closed. Realtime property with enum data type with options Open,	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
Closed. Persists as `LOCAL_HARDWARE_LID` for the local agent and `REMOTE_HARDWARE_LID` for the remote device.							
Model							
The model of the device. Static property with text data type. Persists as `LOCAL_HARDWARE_MODEL` for the local agent and	✓	✓	✓	✓	✓	✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_HARDWARE_MODEL` for the remote device.							
Role							
The role of the device, such as Laptop, Tablet, or Desktop. Static property with enum data type with options Server, Desktop, Laptop, Tablet, Virtual. Persists as `LOCAL_HARDWARE_ROLE` for	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
the local agent and `REMOTE_HARDWARE_ROLE` for the remote device.							
Secure Boot							
Determines if the device was booted using secure boot. Static property with boolean data type. Persists as `LOCAL_HARDWARE_SECUREBOOT` for the local agent	✓	✓		✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_HARDWARE_SECUREBOOT` for the remote device.							
System Memory							
The amount of physical memory in MB. Static property with number data type. Persists as `LOCAL_HARDWARE_SYSTEMMEMORY` for the local agent and `REMOTE_HARDWARE_SY`	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
`STEMMEMORY` for the remote device.							
Vendor							
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 device.	✓	✓	✓	✓	✓	✓	✓
Virtualization							

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
The type of virtualization used to host the device. Static property with enum data type with options None, VMware, Xen®, VirtualPC, Parallels, VirtualBox, Hyper-V. Persists as `LOCAL_HARDWARE_VIRTUALIZATION` for the local agent and `REMOTE`	✓	✓	✓	✓		✓	✓

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

HARDWARE PROPERTY	AGENT	CLIENT EXTENSION					
`_HARDWARE_VIRTUALIZATION` for the remote device.							

IGEL Properties

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
Provides properties unique to an IGEL device.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Environment Variable Count							
The number of IGEL environment variables. Static property with number						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `REMOTE_IGEL_ENVIRONMENT_COUNT` for the remote device.							
Environment Variable Name							
The name of the IGEL environment variable. Static property with text data type. Persists as `REMOTE_IGEL_ENVIRONMENT_X_NAME` for the						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Environment Variable Type							
Determines whether IGEL environment 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 device.						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
Environment Variable Value							
The value of the IGEL environment variable. Static property with text, number, boolean, datetime, ip data types. Persists as `REMOTE_IGEL_ENVIRONMENT_X_VALUE` for the remote device.						✓	
ICG Cert Serial							

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
The serial number of the certificate used to connect to the ICG server. Static property with text data type. Persists as `REMOTE_IGEL_ICG_CERTIFICATE_SERIALNUMBER` for the remote device.						✓	
ICG Cert Subject							
The subject of the certificate used to						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
connect to the ICG server. Static property with text data type. Persists as `REMOTE_IGEL_ICG_CERTIFICATE_SUBJECT` for the remote device.							
ICG Cert Thumbprint SHA256							
The SHA256 thumbprint of the certificate used to connect to the ICG server.						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
Static property with text data type. Persists as `REMOTE_IGEL_ICG_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.							
ICG Server							
The name of the ICG server. Static property with text data type. Persists as `REMOTE_IGEL_ICG_SERVER` for the						✓	

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

IGEL PROPERTY	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 device.						✓	
UMS Cert Serial							
The serial number of the certificate used to connect to the						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
UMS server. Static property with text data type. 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 server. Static property with text data type.						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `REMOTE_IGEL_UMS_CERTIFICATE_SUBJECT` for the remote device.							
UMS Cert Thumbprint SHA256							
The SHA256 thumbprint of the certificate used to connect to the UMS server. Static property with text data type. Persists as `REMOTE_IGEL_`						✓	

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

IGEL PROPERTY	AGENT	CLIENT EXTENSION					
`UMS_CERTIFICATE_THUMBPRINT_SHA256` for the remote device.							
UMS Server							
The name and port of the UMS server. 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 PROPERTY	AGENT	CLIENT EXTENSION					
Describes the input devices available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Keyboard							
Set to true when the remote device has a keyboard available. Dynamic property with boolean data type. Persists as `LOCAL_INPUT_KEYBOARD` for the local	✓	✓	✓	✓		✓	✓

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

INPUT PROPERTY	AGENT	CLIENT EXTENSION					
agent and `REMOTE_INPUT_KEYBOARD` for the remote device.							
Mouse							
Set to true when 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`	✓	✓	✓	✓		✓	✓

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

INPUT PROPERTY	AGENT	CLIENT EXTENSION					
for the 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 and `REMOTE_INPUT_PEN` for the remote device.	✓	✓	✓	✓		✓	✓
Touch							

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

INPUT PROPERTY	AGENT	CLIENT EXTENSION					
Set to true when the remote device has a touchscreen. Dynamic property with boolean data type. Persists as `LOCAL_INPUT_TOUCH` for the local agent and `REMOTE_INPUT_TOUCH` for the remote device.	✓	✓	✓	✓		✓	✓

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

iOS Properties

IOS PROPERTY	AGENT	CLIENT EXTENSION					
Provides properties unique to an iOS endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Biometrics							
Determines the biometrics configured to authenticate the user. Static property with enum data type with options None, TouchID, FaceID. Persists as `REMOTE`							

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

IOS PROPERTY	AGENT	CLIENT EXTENSION					
`_IOS_BIOMETRICS` for the remote device.							
Jailbroken							
Determines whether the device has been jailbroken. Static property with boolean data type. Persists as `REMOTE_IOS_JAILBROKEN` for the remote device.							
Passcode							
Determines							

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

IOS PROPERTY	AGENT	CLIENT EXTENSION					
whether a passcode is required to unlock the iOS device. Static property with boolean data type. Persists as `REMOTE_IOS_PASSCODE` for the remote device.							

Location Properties

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
Describes the geographical location of the	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
endpoint.							
Accuracy							
The accuracy of the latitude and longitude values. Static property with number data type. Persists as `LOCAL_LOCATION_ACCURACY` for the local agent and `REMOTE_LOCATION_ACCURACY` for the remote device.	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
Building							
The building where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_BUILDING` for the local agent and `REMOTE_LOCATION_BUILDING` for the remote device.	✓	✓	✓	✓		✓	✓
Country							
The country code where	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_COUNTRY` for the local agent and `REMOTE_LOCATION_COUNTRY` for the remote device.							
County							
The county where the device is located. Static property	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
with text data type. Persists as `LOCAL_LOCATION_COUNTY` for the local agent and `REMOTE_LOCATION_COUNTY` for the remote device.							
Position							
The geographical position as determined by the latitude and longitude of the device. Static property with	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
position data type. Persists as `LOCAL_LOCATION_POSITION` for the local agent and `REMOTE_LOCATION_POSITION` for the remote device.							
Postcode							
The postcode where the device is located. Static property with text data type. Persists as	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_LOCATION_POSTCODE` for the local agent and `REMOTE_LOCATION_POSTCODE` for the remote device.							
Provider							
The provider that was used to determine the position. Static property with enum data type with options Third Party, Operating System.	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_LOCATION_PROVIDER` 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 with enum data type with options Cellular,	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
Satellite, Wi-Fi, IP Address. Persists as `LOCAL_LOCATION_SOURCE` for the local agent and `REMOTE_LOCATION_SOURCE` for the remote device.							
State							
The state where the device is located. Static property with text data type. Persists as	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_LOCATION_STATE` for the local agent and `REMOTE_LOCATION_STATE` for the remote device.							
Street							
The street where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_STREET` for the local agent and	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_LOCATION_STREET` for the remote device.							
Town							
The town where the device is located. Static property with text data type. Persists as `LOCAL_LOCATION_TOWN` for the local agent and `REMOTE_LOCATION_TOWN` for the remote device.	✓	✓	✓	✓		✓	✓

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

LOCATION PROPERTY	AGENT	CLIENT EXTENSION					
URL							
A URL displaying the location of the device. Static 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 PROPERTY	AGENT	CLIENT EXTENSION					
Describes the logical disks available to the user.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Bus Type							
Set to the name of the bus that the device is connected, e.g., SATA, SCSI, USB, NVMe, etc. Realtime property with enum data type. Persists as `LOCAL_`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`LOGICALDISK_X_BUSTYPE` for the local agent and `REMOTE_LOGICALDISK_X_BUSTYPE` for the remote device.							
Count							
The number of logical disks. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_COUNT` for the	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
local agent and `REMOTE_LOGICALDISK_COUNT` for the remote device.							
Drive							
The drive where the logical disk is mounted. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_DRIVE` for the local agent and	✓	✓					

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_LOGICALDISK_X_DRIVE` for the remote device.							
Encrypted							
Determines whether the disk is encrypted with Microsoft BitLocker Drive Encryption. Realtime property with boolean data type. Persists as `LOCAL_LOGICALDISK_`	✓	✓					

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`X_ENCRYPTED` for the local agent and `REMOTE_LOGICALDISK_X_ENCRYPTED` for the remote device.							
Filesystem							
The underlying filesystem. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_FILESYSTEM` for the	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
local agent and `REMOTE_LOGICALDISK_X_FILESYSTEM` for the remote device.							
Flags							
Flags associated with the logical disk. Realtime property with flags data type. Persists as `LOCAL_LOGICALDISK_X_FLAGS` for the local agent	✓	✓					

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_LOGICALDISK_X_FLAGS` for the remote device.							
Free							
The free space as a percentage of the total space. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_X_FREE` for the local agent and `REMOTE`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`_LOGICALDISK_X_FREE` for the remote device.							
Free MB							
The free/available size in MB. Realtime property with number data type. Persists as `LOCAL_LOGICALDISK_X_FREEMB` for the local agent and `REMOTE_LOGICALDISK_X_FRE`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`EMB` for the remote device.							
Hidden							
Set to true if the logical disk is hidden. Realtime property with boolean data type. Persists as `LOCAL_LOGICALDISK_X_HIDDEN` for the local agent and `REMOTE_LOGICALDISK_X_HIDDEN` for the	✓	✓					

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Identity							
Enter one 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 `REMOTE_LOGIC`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`ALDISK_X_IDENTITY` for the remote device.							
Label							
The volume label associated with the logical disk. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_LABEL` for the local agent and `REMOTE_LOGICALDISK_X_LAB`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`EL` for the remote device.							
Name							
The name of the logical 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_NAM`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`E` 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 agent and `REMOTE_LOGICALDISK_X_PATH` for the	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Product Id							
For USB connected disks, this is the USB product id. For PCI connected disks, this is the device id. Realtime property with text data type. Persists as `LOCAL_LOGICALDISK_X_PRODUCT_ID` for the local	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
agent and `REMOTE_LOGICALDISK_X_PRODUCT_ID` for the remote 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 agent	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_LOGICALDISK_X_SERIALNUMBER` for the remote device.							
System							
Determines whether the disk is the system drive, i.e., if it contains the Operating System installation. Realtime property with boolean data type. Persists as	✓	✓	✓				

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_LOGICALDISK_X_SYSTEM` for the local agent and `REMOTE_LOGICALDISK_X_SYSTEM` for the remote device.							
Total MB							
The total size in MB of the logical disk. Realtime property with number data type. Persists as `LOCAL_`	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
`LOGICALDISK_X_TOTALMB` for the local agent and `REMOTE_LOGICALDISK_X_TOTALMB` for the remote device.							
Type							
The type of the logical disk, such as Fixed, Removable, or Portable Device. Realtime property with enum data type. Persists	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_LOGICALDISK_X_TYPE` for the local agent and `REMOTE_LOGICALDISK_X_TYPE` for the remote device.							
Vendor Id							
The vendor id of the logical disk for USB or PCI connected disks. Realtime property with text data type.	✓	✓	✓	✓		✓	✓

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

LOGICAL DISK PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_LOGICALDISK_X_VENDOR_ID` for the local agent and `REMOTE_LOGICALDISK_X_VENDOR_ID` for the remote device.							

macOS Properties

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Describes properties unique to a macOS endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Gatekeeper							
Determines the Gatekeeper setting which defines the trust level of software that can run on the Mac. Static property with enum data type with options Anywhere, App Store and Identified Developers, App Store. Persists as `REMOTE_MACOS_GATEK`			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
`EEPER` for the remote device.							
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 remote device.			✓				
Secure Virtual Memory							
Determines whether			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
the swap file is encrypted. Static property with boolean data type. Persists as `REMOTE_MACOS_SECUREVIRTUALMEMORY` for the remote device.							
System Integrity Protection							
Determines whether System Integrity Protection is enabled, which helps protect			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Mac users from malicious software. Static property with boolean data type. Persists as `REMOTE_MACOS_SYSTEMINTEGRITYPROTECTION` for the remote device.							

macOS Firewall Properties

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Provides real-time properties describi	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
ng the state of the macOS Firewall.							
Allow Signed Downloaded Inbound							
Determines whether the firewall is configured to allow signed downloaded software to receive inbound connections. Realtime property with boolean data type. Persists			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
as `REMOTE_MACOS_FIREWALL_ALLOWSIGNEDDOWNLOADINBOUND` for the remote device.							
Allow Signed Inbound							
Determines whether the firewall is configured to allow built-in software to receive inbound connections. Realtime property with			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
boolean data type. Persists as `REMOTE_MACOSFIREWALL_ALLOWSIGNEDINBOUND` for the remote device.							
Block All Inbound							
Determines whether the firewall is configured to block all inbound connections. Realtime property with boolean			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `REMOTE_MACOS FIREWALL_BLOCKALLINBOUND` for the remote device.							
Enabled							
Determines whether the firewall is enabled. Realtime property with boolean data type. Persists as `REMOTE_MACOS FIREWALL_ENA`			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
`BLED` for the remote device.							
Inbound Exception Rules							
The exceptions to the firewall rules. Realtime property with text data type. Persists as `REMOTE_MACOSFIREWALL_INBOUNDRULES_EXCEPTIONS` for the remote device.			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Inbound Program Rules							
The firewall rules configured to allow programs to receive inbound connections. Realtime property with text data type. Persists as `REMOTE_MACOSFIREWALL_INBOUNDRULES_PROGRAMS` for the remote device.			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Inbound Service Rules							
The firewall rules configured to allow services to receive inbound connections. Realtime property with text data type. Persists as `REMOTE_MACOS FIREWALL_INBOUNDRULES_SERVICES` for the remote device.			✓				
Stealth Mode							

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Determines whether the firewall is configured to ignore ICMP packets. Realtime property with boolean data type. Persists as `REMOTE_MACOS_FIREWALL_STEALTHMODE` for the remote device.			✓				
Version							
The version number of the firewall.			✓				

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

MACOS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Realtime property with version data type. Persists as `REMOTE_MACOS FIREWALL_VERSION` for the remote device.							

macOS Update Properties

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Describes the status of macOS Software Update settings and updates.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Auto Check For Updates							
Set to true when macOS is configured to automatically check for updates. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_CHECK` for the remote device.			✓				
Auto Downlo							

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
ad Updates							
Set to true when macOS is configured to automatically download updates. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_DOWNLOAD` for the remote device.			✓				
Auto Install App							

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Store Updates							
Set to true when macOS is configured to automatically install App Store updates. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_INSTALL_APPSTORE` for the remote device.			✓				
Auto Install							

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Data Updates							
Set to true when macOS is configured to automatically install system data files. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_INSTALL_DATA` for the remote device.			✓				
Auto Install macOS Updates							

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Set to true when macOS is configured to automatically install macOS updates. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_INSTALL_MACOS` for the remote device.			✓				
Auto Install Security Updates							

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Set to true when macOS is configured to automatically install security updates. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_AUTO_INSTALL_SECURITY` for the remote device.			✓				
Enabled							
Determines whether the			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Software Update service is running and the last attempt to update was successful. Realtime property with boolean data type. Persists as `REMOTE_MACOS_UPDATE_ENABLED` for the remote device.							
Ignore Update							
The name of any updates			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
that are not to be installed. Realtime property with text data type. Persists as `REMOTE_MACOS_UPDATE_IGNOREUPDATE` for the remote device.							
Last Search							
The time that the Software Update service last checked for updates. Realtim			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
e property with datetime data type. Persists as `REMOTE_MACOS_UPDATE_LASTSEARCH` for the remote device.							
Update Count							
The number of updates that are waiting to be installed. Realtime property with number data type. Persists as `REMOTE`			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
`_MACOS_UPDATE_UPDATE_COUNT` for the remote device.							
Update Name							
The name of the update that is waiting to be installed. Realtime property with text data type. Persists as `REMOTE_MACOS_UPDATE_UPDATE_X_NAME` for the remote device.			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
Update Product Key							
The product key of the update that is waiting to be installed. Realtime property with text data type. Persists as `REMOTE_MACOS_UPDATE_UPDATE_X_PRODUCTKEY` for the remote device.			✓				
Update Version							
The version of the			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
update that is waiting to be installed. Realtime property with version data type. Persists as `REMOTE_MACOS_UPDATE_UPDATE_X_VERSION` for the remote device.							
Version							
The version number of the Software Update service that last checked for updates			✓				

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

MACOS PROPERTY	AGENT	CLIENT EXTENSION					
. Realtime property with version data type. Persists as `REMOTE_MACOS_UPDATE_VERSION` for the remote device.							

Mapped Drive Properties

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
Describes the mapped drives available within a user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Count							

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
The number of mapped drives available. Dynamic property with number data type. Persists as `LOCAL_MAPPED DRIVE_COUNT` for the local agent and `REMOTE_MAPPEDDRIVE_COUNT` for the remote device.	✓	✓					
Drive							
The drive where	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
the mapped drive is mounted. Dynamic property with text data type. Persists as `LOCAL_MAPPED DRIVE_X_DRIVE` for the local agent and `REMOTE_MAPPEDDRIVE_X_DRIVE` for the remote device.							
Hidden							
Set to true if the mapped drive is	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
hidden. Dynamic property with boolean data type. Persists as `LOCAL_MAPPED DRIVE_X_HIDDEN` for the local agent and `REMOTE_MAPPEDDRIVE_X_HIDDEN` for the remote device.							
Provider							
The provider of the mapped drive. Dynamic property	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
with text data type. Persists as `LOCAL_MAPPED DRIVE_X_PROVIDER` for the local agent and `REMOTE_MAPPEDDRIVE_X_PROVIDER` for the remote device.							
Server							
The name of the remote server. Dynamic property with text data type. Persists	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_MAPPED DRIVE_X_SERVER` for the local agent and `REMOTE_MAPPEDDRIVE_X_SERVER` for the remote device.							
Share							
The name of the share on the remote server. Dynamic property with text data type. Persists as `LOCAL_MAPPED`	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
`DRIVE_X_SHARE` for the local agent and `REMOTE_MAPPEDDRIVE_X_SHARE` for the remote device.							
User							
The name of the user authenticating the connection to the remote server. Dynamic property with text data type. Persists as `LOCAL_`	✓	✓					

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

MAPPED DRIVE PROPERTY	AGENT	CLIENT EXTENSION					
`MAPPED DRIVE_ X_USER` for the local agent and `REMOTE _MAPPE DDRIVE _X_USE R` for the remote device.							

Multihop Properties

MULTIHOP PROPERTY	AGENT	CLIENT EXTENSION					
Describes the number of hops taken by the user over deviceTRUST connected	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

MULTIHOP PROPERTY	AGENT	CLIENT EXTENSION					
sessions.							
Count							
The number of multihop properties. Static property with number data type. Persists as undefined.		✓					

Name Properties

NAME PROPERTY	AGENT	CLIENT EXTENSION					
Identifies the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
DN							
The Distingu	✓	✓	✓				

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

NAME PROPERTY	AGENT	CLIENT EXTENSION					
ished Name of the device within Active Directory. Static property with text data type. Persists as `LOCAL_NAME_DN` for the local agent and `REMOTE_NAME_DN` for the remote device.							
DNS							
The DNS name of the device. Static property with text data type.	✓	✓	✓	✓		✓	✓

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

NAME PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_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 with text data type. Persists as `LOCAL_ID` for the local agent and `REMOTE_ID` for	✓	✓	✓	✓		✓	✓

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

NAME PROPERTY	AGENT	CLIENT EXTENSION					
the remote device.							
Name							
The name of the device. Static property with text data type. Persists as `LOCAL_NAME` for the local agent and `REMOTE_NAME` for the remote device.	✓	✓	✓	✓	✓	✓	✓
SID							
The SID of the device within Active Directory. Static property with text	✓	✓	✓				

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

NAME PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `LOCAL_NAME_SID` for the local agent and `REMOTE_NAME_SID` for the remote device.							

Network Properties

NETWORK PROPERTY	AGENT	CLIENT EXTENSION					
Describes the network adapters and their bound network addresses.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

CATEGORY							
Set to Public, Private, or Domain depending upon the OS categorization of 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_NETWORK_X_CATEGOR`	✓	✓				✓	✓

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

CATEGORY							
`Y` for the remote device.							

COUNT							
The number of network adapters. Dynamic property with number data type. Persists as `LOCAL_NETWORK_COUNT` for the local agent and `REMOTE_NETWORK_COUNT` for the remote device.	✓	✓	✓	✓		✓	✓

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

DESCRIPTION							
The description of the network adapter. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_DESCRIPTION` for the local agent and `REMOTE_NETWORK_X_DESCRIPTION` for the remote device.	✓	✓	✓	✓		✓	✓

DHCP ENABLED							
Set to true when the	✓	✓	✓	✓		✓	✓

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

DHCP ENABLED							
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 `REMOTE_NETWORK_X_DHCP_ENABLED` for the remote device.							

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

DHCP EXPIRES							
The time that the IP address expires. Dynamic property with datetime data type. Persists as `LOCAL_NETWORK_X_DHCP_EXPIRES` for the local agent and `REMOTE_NETWORK_X_DHCP_EXPIRES` for the remote device.	✓	✓		✓		✓	✓

DHCP LEASE							
The lease	✓	✓		✓		✓	✓

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

DHCP 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_LEASE` for the remote device.							

DHCP SERVER							
The IP address of the DHCP server.	✓	✓	✓	✓		✓	✓

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

DHCP SERVER							
Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_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 with ip, text	✓	✓	✓	✓		✓	✓

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

DNS							
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 suffixes. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_DNS_SUFFIX` for the local agent	✓	✓	✓	✓		✓	✓

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

DNS SUFFIX							
and `REMOTE_NETWORK_X_DNS_SUFFIX` for the remote device.							

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_NETWORK_X_GATEWAY`	✓	✓	✓	✓		✓	✓

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

GATEWAY							
for the remote device.							

GATEWAY MAC							
The MAC address of the gateway. Dynamic property with text data type. Persists as `LOCAL_NETWORK_X_GATEWAY_MAC` for the local agent and `REMOTE_NETWORK_X_GATEWAY_MAC` for the remote device.	✓	✓	✓	✓		✓	✓

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

IPV4 ADDRESS							
The IPv4 address of the network adapter. Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_X_IPV4` for the local agent and `REMOTE_NETWORK_X_IPV4` for the remote device.	✓	✓	✓	✓		✓	✓

IPV4 SUBNET							
The IPv4 subnet of the	✓	✓	✓	✓		✓	✓

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

IPV4 SUBNET							
network adapter. Dynamic property with ip, text data types. Persists as `LOCAL_NETWORK_X_IPV4_SUBNET` for the local agent and `REMOTE_NETWORK_X_IPV4_SUBNET` for the remote device.							

IPV6 ADDRESS							
The IPv6 address of the network adapter. Dynami	✓	✓	✓	✓		✓	✓

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

IPV6 ADDRESS							
c property with ip, text data types. Persists as `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. Dynamic property with ip, text data	✓	✓	✓	✓		✓	✓

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

IPV6 SUBNET							
types. Persists as `LOCAL_NETWORK_X_IPV6_SUBNET` for the local agent and `REMOTE_NETWORK_X_IPV6_SUBNET` for the remote device.							

MAC ADDRESS							
The physical MAC address of the network adapter. Dynamic property with text data type. Persists as	✓	✓	✓	✓		✓	✓

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

MAC ADDRESS							
`LOCAL_NETWORK_X_MAC` for the local agent and `REMOTE_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_NAME` for the local agent and `REMOTE`	✓	✓	✓	✓		✓	✓

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

NAME							
`_NETWORK_X_NAME` for the remote device.							

SPEED							
The speed of the network adapter. Dynamic property with number data type. Persists as `LOCAL_NETWORK_X_SPEED` for the local agent and `REMOTE_NETWORK_X_SPEED` for the remote device.	✓	✓		✓		✓	✓

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

STATUS							
The status of the 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_NETWORK_X_STATUS` for the remote device.	✓	✓	✓	✓		✓	✓

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

TYPE							
The type of network adapter, such as Ethernet or Wi-Fi. Dynamic property with enum data type with options Other, 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	✓	✓	✓	✓		✓	✓

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

TYPE							
remote device.							

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_VIRTUAL` for the local agent and `REMOTE_NETWORK_X_VIRTUAL` for the	✓	✓	✓	✓		✓	

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

VIRTUAL							
remote device.							

WI-FI BSSID							
For Wi-Fi network adapters, the BSSID of the connected access 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	✓	✓	✓	✓		✓	✓

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

WI-FI BSSID							
remote device.							

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, Enhanced Open, WEP, WPA Personal, WPA Enterprise, WPA2	✓	✓	✓	✓		✓	✓

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

WI-FI SECURITY							
Personal, WPA2 Enterprise, WPA3 Personal, WPA3 Enterprise. Persists as `LOCAL_NETWORK_X_WIFI_SECURITY` for the local agent and `REMOTE_NETWORK_X_WIFI_SECURITY` for the remote device.							

WI-FI SSID								
For Wi-Fi network adapters,	✓	✓	✓	✓		✓	✓	

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

WI-FI SSID									
the SSID of any connected networks. 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									

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

WI-FI SSID									
remote device.									

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 local agent and `REMOTE_NETWORK_X_WIFI_STRENGTH`	✓	✓	✓	✓		✓	✓

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

WI-FI STRENGTH							
for the remote device.							

WINS							
The IP address of the WINS server. Dynamic property with ip, text 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.

OS Properties

OS PROPERTY	AGENT	CLIENT EXTENSION					
Provides information about the operating system installed on the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Description							
A textual description of the OS. Static property with text data type. Persists as `LOCAL_OS_DESCRIPTION` for the local agent and `REMOTE`	✓	✓		✓		✓	✓

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
`_OS_DESCRIPTION` for the remote device.							
Id							
An arbitrary identifier that uniquely identifies the installation of the OS. Static property with text data type. Persists as `LOCAL_OS_ID` for the local agent and `REMOTE_OS_ID` for the remote device.	✓	✓	✓	✓		✓	✓
Name							

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
The name of the OS. Static property with enum data type with options Windows, macOS, iOS, IGEL, eLux®, Rangee, Linux, Chrome OS. Persists as `LOCAL_OS_NAME` for the local agent and `REMOTE_OS_NAME` for the remote device.	✓	✓	✓	✓	✓	✓	✓
Platform							

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
The platform of the OS, such as x64. Static property with enum data type with options x86, x64, ARM, ARM64, MIPS, MIPS64. Persists as `LOCAL_OS_PLATFORM` for the local agent and `REMOTE_OS_PLATFORM` for the remote device.	✓	✓	✓	✓	✓	✓	✓
Release							

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
The release version of the OS. Static property with text, number data types. Persists as `LOCAL_OS_RELEASE` for the local agent and `REMOTE_OS_RELEASE` for the remote device.	✓	✓		✓		✓	✓
Startup Time							
The time that the OS started. Static property with	✓	✓		✓		✓	✓

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
datetime data type. Persists as `LOCAL_OS_STARTUPTIME` for the local agent and `REMOTE_OS_STARTUPTIME` for the remote device.							
Type							
The type of the OS, such as Client or Server. Static property with enum data type with options Client, Server. Persists	✓	✓		✓	✓	✓	✓

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_OS_TYPE` for the local agent and `REMOTE_OS_TYPE` for the remote device.							
Version							
The version number of the OS. Static property with version data type. Persists as `LOCAL_OS_VERSION` for the local agent and `REMOTE_OS_VERSION`	✓	✓	✓	✓	✓	✓	✓

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

OS PROPERTY	AGENT	CLIENT EXTENSION					
for the remote device.							

Password Policy Properties

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
Describes the password policy of the logged in user.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Force Logoff							
The amount of time in days between the end of the valid logon time and the time when the user is forced	✓	✓					

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
to log off the network. Dynamic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_FORCELOGOFF` for the local agent and `REMOTE_POLICY_PASSWORD_FORCELOGOFF` for the remote device.							
Maximum Password Age							

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
The maximum period of time in days before the system requires the user to change it. Dynamic property with text data type. Persists as `LOCAL_POLICY_PASSWORD_MAXAGE` for the local agent and `REMOTE_POLICY_PASSWORD_MAXAGE` for the	✓	✓					

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Minimum Password Age							
The minimum period of time in days before the system can require the user to change it. Dynamic property with number data type. Persists as `LOCAL_POLICY_PASSWORD_MINAGE` for the	✓	✓					

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
local agent and `REMOTE_POLICY_PASSWORD_MINAGE` for the remote device.							
Minimum Password Length							
The minimum number of characters required. Dynamic property with text data type. Persists as `LOCAL_POLICY`	✓	✓					

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
`_PASSWORD_MINLENGTH` for the local agent and `REMOTE_POLICY_PASSWORD_MINLENGTH` for the remote device.							
Password History							
The number of unique passwords associated with the user before an old password can be reused. Dynami	✓	✓					

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

PASSWORD POLICY PROPERTY	AGENT	CLIENT EXTENSION					
c property with text data type. Persists as `LOCAL_POLICY_PASSWORD_HISTORY` for the local agent and `REMOTE_POLICY_PASSWORD_HISTORY` for the remote device.							

Performance Properties

PERFORMANCE PROPERTY	AGENT	CLIENT EXTENSION					
Describes the performance of	Microsoft	Microsoft	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

PERFORMANCE PROPERTY	AGENT	CLIENT EXTENSION					
the remoting protocol.	Windows	Windows					
Bandwidth							
The bandwidth status of the remoting protocol. Dynamic property with enum data type with options Unavailable, Loading, Excellent, Good, Moderate, Poor. Persists as	✓	✓					

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

PERFORMANCE PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_PERFORMANCE_BANDWIDTH` for the local agent.							
Bandwidth Speed							
The bandwidth of the remoting protocol in kBps. Dynamic property with number data type. Persists as `LOCAL_PERFORMANCE_BANDWIDTH_SPEED` for the local agent.	✓	✓					

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

PERFORMANCE PROPERTY	AGENT	CLIENT EXTENSION					
Latency							
The latency status of the remoting protocol. Dynamic property with enum data type with options Unavailable, Loading, Excellent, Good, Moderate, Poor. Persists as `LOCAL_PERFORMANCE_LATENCY` for the local agent.	✓	✓					

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

PERFORMANCE PROPERTY	AGENT	CLIENT EXTENSION					
Latency Speed							
The latency of the remoting protocol in milliseconds. Dynamic property with number data type. Persists as `LOCAL_PERFORMANCE_LATENCY_SPEED` for the local agent.	✓	✓					

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

Power Properties

POWER PROPERTY	AGENT	CLIENT EXTENSION					
Describes the power profile of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
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 `LOCAL_POWER_`	✓	✓	✓	✓		✓	✓

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

POWER PROPERTY	AGENT	CLIENT EXTENSION					
`AC` for the local agent and `REMOTE_POWER_AC` for the remote device.							
Battery							
Set to High, Medium, Low or Critical depending upon the available battery. Dynamic property with enum data type with options High, Low, Critical, None, Medium.	✓	✓	✓	✓		✓	✓

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

POWER PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_POWER_BATTERY` for the local agent and `REMOTE_POWER_BATTERY` for the remote device.							
Scheme							
The current power scheme. Dynamic property with text data type. Persists as `LOCAL_POWER_SCHEME` for the local agent and	✓	✓					

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

POWER PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_POWER_SCHEME` for the remote device.							

Printer Properties

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
Describes the printers available to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Count							
The number of printers available. Realtime property with number data type. Persists	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_PRINTER_COUNT` for the local agent and `REMOTE_PRINTER_COUNT` 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_DEFAULT`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
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 Directory. Realtime property with boolean data type. Persists as `LOCAL_`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`PRINTER_X_DIRECTORY_PUBLISHED` for the local agent and `REMOTE_PRINTER_X_DIRECTORY_PUBLISHED` for the remote device.							
Driver							
The name of the printer driver. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_DRIVER`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
for the 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 as `LOCAL_PRINTER_X_DRIVER_FILE` for the local agent and `REMOTE_PRINT`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`ER_X_DRIVER_FILE` for the remote device.							
Driver Manufacturer							
The manufacturer of the printer driver. Realtime property with text data type. Persists as `LOCAL_PRINTER_X_DRIVER_MANUFACTURER` for the local agent and `REMOTE_PRINTER_X_D`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`RIVER_MANUFACTURER` for the remote device.							
Driver Version							
The version of the printer driver. Realtime property with version data type. Persists as `LOCAL_PRINTER_X_DRIVER_VERSION` for the local agent and `REMOTE_PRINTER_X_DRIVER_VERSIO`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`N` for the remote device.							
Errors							
Lists any errors currently reported 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 Availabl	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
e, Toner Low, No Toner, Cannot Print Page, User Intervention, Out Of Memory, Door Open, Server Unknown, Server Offline, Driver Update Needed. Persists as `LOCAL_PRINTER_X_ERRORS` for the local agent and `REMOTE_PRINTER_X_ERRORS` for the							

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Keep Print Jobs							
Set to true when print jobs 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_PRINT_JO`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`BS` 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_LOCAL` for the local agent and `REMOTE_PRINTER_X_LOCAL` for the remote device.	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
Location							
The location of the printer. Realtime property with text data type. 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.	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
Realtime 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 used by the printer. Realtime property with text data type. Persists as `LOCAL_`	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
`PRINTER_X_PORT` for the local agent and `REMOTE_PRINTER_X_PORT` for the remote 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 PROPERTY	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 `LOCAL_PRINTER_X_SHARE` for the local agent and `REMOTE_PRINTER_X_SHARE` for the	✓	✓					

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

PRINTER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							

Region Properties

REGION PROPERTY	AGENT	CLIENT EXTENSION					
Describes the regional information of the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Keyboard Language							
The language configured by the keyboard. Dynamic property with text data type. Persists	✓	✓	✓	✓		✓	✓

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

REGION PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_REGION_KEYBOARD_LANGUAGE` for the local agent and `REMOTE_REGION_KEYBOARD_LANGUAGE` for the remote device.							
Keyboard Locale							
The locale configured by the keyboard. Dynamic property with text data type. Persists	✓	✓	✓	✓		✓	✓

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

REGION PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_REGION_KEYBOARD_LOCALE` for the local agent and `REMOTE_REGION_KEYBOARD_LOCALE` for the remote device.							
Language							
The language configured by the OS. Dynamic property with text data type. Persists as `LOCAL_REGION`	✓	✓	✓	✓		✓	✓

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

REGION PROPERTY	AGENT	CLIENT EXTENSION					
`_LANGUAGE` for the local agent and `REMOTE_REGION_LANGUAGE` for the remote device.							
Locale							
The locale configured by the OS. Dynamic property with text data type. Persists as `LOCAL_REGION_LOCALE` for the local agent and `REMOTE_REGION_LOCA`	✓	✓	✓	✓		✓	✓

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

REGION PROPERTY	AGENT	CLIENT EXTENSION					
`LE` for the remote device.							
Timezone Offset							
The offset in minutes relative to UTC. Dynamic property with number data type. Persists as `LOCAL_REGION_TIMEZONE_OFFSET` for the local agent and `REMOTE_REGION_TIMEZONE_OFFSET` for the	✓	✓	✓	✓		✓	✓

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

REGION PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							

Remote Control Properties

REMOTE CONTROL PROPERTY	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	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Active							
Set to true when	✓	✓				✓	

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
the session is remote controlled. Dynamic property with boolean data type. Persists as `LOCAL_REMOTECONTROL_ACTIVE` for the local agent and `REMOTE_REMOTECONTROL_ACTIVE` for the remote device.							
Gateway							

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
Set to true whenever a gateway was used to access the virtual session. Supported on Citrix® and VMware only. Dynamic property with boolean data type. Persists as `LOCAL_REMOTE CONTROL_GATEWAY` for the local agent.	✓	✓					
Gateway IP							

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
Set to the IP address of the gateway used to access the virtual session. Supported on Citrix and VMware only. Dynamic property with ip, text data types. Persists as `LOCAL_REMOTE CONTROL_GATEWAY_IP` for the local agent.	✓	✓					
Protocol							

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION				
Determines the protocol used to remote control the device. Currently supports Console, RDP, ICA®, PCoIP, Blast, and VNC for IGEL clients. Dynamic property with enum data type with options Unknown, RDP, ICA, PCoIP, Blast, VNC.	✓	✓				✓	

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_REMOTECONTROL_PROTOCOL` for the local agent and `REMOTE_REMOTECONTROL_PROTOCOL` for the remote device.							
Remote Install Path							
The installation path of the remote client. Supported on Citrix only. Dynamic	✓	✓					

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_INSTALLPATH` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_INSTALLPATH` for the remote device.							
Remote IP							
The IP address of the remote user. Dynami	✓	✓					

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
c property with ip, text data types. Persists as `LOCAL_REMOTECONTROL_REMOTE_IP` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_IP` for the remote device.							
Remote Name							
The NetBIOS name of the remote device. Dynami	✓	✓					

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
c property with text data type. Persists as `LOCAL_REMOTECONTROL_REMOTE_NAME` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_NAME` for the remote device.							
Remote Platform							
The platform of the remote client. Dynamic	✓	✓					

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
property with text data type. Persists as `LOCAL_REMOTE CONTROL_REMOTE_PLATFORM` for the local agent and `REMOTE_REMOTECONTROL_REMOTE_PLATFORM` for the remote device.							
Remote Version							
The version number of the remote client. Support	✓	✓					

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

REMOTE CONTROL PROPERTY	AGENT	CLIENT EXTENSION					
ed on Citrix and VMware only. Dynamic property with version data type. Persists as `LOCAL_REMOTE CONTROL_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 PROPERTY	AGENT	CLIENT EXTENSION					
Provides properties about the remoting client used to remote control the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Outbound Address							
The IP address of the outbound connection established by the remoting client. Dynamic property with ip, text		✓					

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

REMOTING CLIENT PROPERTY	AGENT	CLIENT EXTENSION					
data types. Persists as `REMOTE_REMOTINGCLIENT_OUTBOUND_ADDRESS` for the remote device.							
Outbound DNS							
The DNS name established from a reverse DNS lookup, of the outbound connection of the remoting client. Dynamic		✓					

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

REMOTING CLIENT PROPERTY	AGENT	CLIENT EXTENSION					
property with text data type. Persists as `REMOTE_REMOTINGCLIENT_OUTBOUND_DNS` for the remote device.							
Runtime							
The runtime of the remoting client. Static property with text data type. Persists as `REMOTE_REMOTINGCLIENT_RUNTIME` for the		✓					

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

REMOTING CLIENT PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Skype Plugin							
Set to true whenever the Skype plugin is detected. Dynamic property with boolean data type. Persists as `REMOTE_REMOTINGCLIENT_PLUGINS_SKYPE` for the remote device.		✓					
Skype Plugin Version							

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

REMOTING CLIENT PROPERTY	AGENT	CLIENT EXTENSION					
Set to the version number of the Skype plugin. Dynamic property with version data type. Persists as `REMOTE_REMOTINGCLIENT_PLUGINS_SKYPE_VERSION` for the remote device.		✓					
Version							
The version of the remoting client. Static property		✓					

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

REMOTING CLIENT PROPERTY	AGENT	CLIENT EXTENSION					
with version data type. Persists as `REMOTE_REMOTINGCLIENT_VERSION` for the remote device.							

Screen Saver Properties

SCREEN SAVER PROPERTY	AGENT	CLIENT EXTENSION					
Describes the screen saver applied to the user session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Enabled							
Determines if the	✓	✓	✓			✓	✓

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

SCREEN SAVER PROPERTY	AGENT	CLIENT EXTENSION					
screensaver is enabled. Realtime property with boolean data type. Persists as `LOCAL_SCREENSAVER_ENABLED` for the local agent and `REMOTE_SCREENSAVER_ENABLED` for the remote device.							
Filename							
The filename of the screens	✓	✓	✓			✓	✓

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

SCREEN SAVER PROPERTY	AGENT	CLIENT EXTENSION					
aver 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` for the remote device.							
Secure							
Determines if a password is required	✓	✓				✓	✓

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

SCREEN SAVER PROPERTY	AGENT	CLIENT EXTENSION					
when the screensaver is deactivated. Realtime property with boolean data type. Persists as `LOCAL_SCREEN SAVER_SECURE` for the local agent and `REMOTE_SCREENSAVER_SECURE` for the remote device.							
Timeout							
Determines the amount	✓	✓	✓			✓	✓

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

SCREEN SAVER PROPERTY	AGENT	CLIENT EXTENSION					
of user idle time in seconds before the screensaver is displayed. Realtime property with number data type. Persists as `LOCAL_SCREENSAVER_TIMEOUT` for the local agent and `REMOTE_SCREENSAVER_TIMEOUT` for the remote device.							

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

Security Product Properties

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
Provides real-time properties describing the state of the installed Antivirus, Antispyware and Firewall security products.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Category							
The category of security product, such as Firewall or Antivirus. Realtim	✓	✓	✓				

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
e property with enum data type with options Firewall, Antivirus, Antispyware. Persists as `LOCAL_SECURITYPRODUCT_X_CATEGORY` for the local agent and `REMOTE_SECURITYPRODUCT_X_CATEGORY` for the remote device.							
Count							

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
The number of security products. Realtime property with number data type. Persists as `LOCAL_SECURITYPRODUCT_COUNT` for the local agent and `REMOTE_SECURITYPRODUCT_COUNT` for the remote device.	✓	✓	✓				
Name							
The name of	✓	✓	✓				

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
the security product. Realtime property with text data type. Persists as `LOCAL_SECURITYPRODUCT_X_NAME` for the local agent and `REMOTE_SECURITYPRODUCT_X_NAME` for the remote device.							
Signature Status							
Set to Up-To-Date or Out-Of-	✓	✓	✓				

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
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 `LOCAL_SECURITYPRODUCT_X_SIGNATURESTATUS` for the local agent and `REMOTE`							

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
`_SECURITYPRODUCT_X_SIGNATURESTATUS` for the remote device.							
Status							
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_`	✓	✓	✓				

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

SECURITY PRODUCT PROPERTY	AGENT	CLIENT EXTENSION					
`SECURITYPRODUCT_X_STATUS` for the local agent and `REMOTE_SECURITYPRODUCT_X_STATUS` for the remote device.							

Session Properties

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
Provides information describing the user's logon session.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
Connect Id							
Uniquely identifies 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							
The time the session connected. Static property with	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
datetime data type. Persists as `LOCAL_SESSION_CONNECT_TIME` for the local agent.							
Delivery Name							
Set to a semi-colon separated list of published applications when the delivery type is Application, or the name of the published desktop when	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
delivery type is Desktop. Static property with text data type. Persists as `LOCAL_SESSION_DELIVERY_NAME` for the local agent.							
Delivery Type							
Set to Application when the session contains one or more published applications, or Desktop when the session	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
is a published desktop. Static property with enum data type with options Unknown, Desktop, Application. Persists as `LOCAL_SESSION_DELIVERY_TYPE` for the local agent.							
Id							
The session id of the user as assigned by the operating	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
system. Static property with number data 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 number data type. Persists	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_SESSION_IDLE PERIOD` for the local agent and `REMOTE_SESSION_IDLEPERIOD` for the remote device.							
Logon Id							
Uniquely identifies the logon session of the user. Static property with text data type. Persists as `LOCAL_SESSIO`	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
`N_LOGON_ID` for the local agent.							
Logon Time							
The time of the session logon. Static property with datetime data type. Persists as `LOCAL_SESSION_LOGON_TIME` for the local agent.	✓	✓					
Time							
The current session time. Static property with	✓	✓					

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

SESSION PROPERTY	AGENT	CLIENT EXTENSION					
datetime data type. Persists as `LOCAL_SESSION_TIME` for the local agent.							

Smartcard Reader Properties

SMART CARD READER PROPERTY	AGENT	CLIENT EXTENSION					
Describes the connected smart-card readers available to the user.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Count							
The number of smartca	✓	✓		✓		✓	✓

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

SMART CARD READER PROPERTY	AGENT	CLIENT EXTENSION					
rd readers connected. Dynamic property with number data type. Persists as `LOCAL_SMARTCARDREADER_COUNT` for the local agent and `REMOTE_SMARTCARDREADER_COUNT` for the remote device.							
Name							
The name of the smartca	✓	✓		✓		✓	✓

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

SMART CARD READER PROPERTY	AGENT	CLIENT EXTENSION					
rd reader. Dynamic property with text data type. Persists 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 PROPERTY	AGENT	CLIENT EXTENSION					
Identifies the logged in user.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Attribute Count		Client Extension					
The number of user attributes read from Active Directory. Static property with number data type. Persists as `LOCAL_USER_ATTRIBUTE_COUNT` for the local agent and `REMOTE_USER_ATTRIBUTE_CO`	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
`UNT` for the remote device.							
Attribute Name							
The name of a user attribute 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 remote device.	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
Attribute Value							
The value of a user attribute read from Active Directory. Static property with text, number, boolean, datetime data types. Persists as `LOCAL_USER_ATTRIBUTE_X_VALUE` for the local agent and `REMOTE_USER_ATTRIBUTE_X_VALUE` for the	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Auth							
The authentication used to authenticate 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							
The internet provider	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
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_AUTH_PRINCIPAL` for the remote device.							
Auth Provider							
The internet provider. Static property with text	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `LOCAL_USER_AUTH_PROVIDER` for the local agent and `REMOTE_USER_AUTH_PROVIDER` for the remote device.							
Cached Credentials							
Set to true whenever the user has cached credentials. Static property with boolean data	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_USER_CACHEDCREDENTIALS` for the local agent and `REMOTE_USER_CACHEDCREDENTIALS` for the remote device.							
DN							
The distinguished name of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DN`	✓	✓	✓				

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
for the local agent and `REMOTE_USER_NAME_DN` for the remote 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_NAME_DOMAIN_DNS` for	✓	✓	✓	✓		✓	✓

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
the remote device.							
Domain							
The domain of the user. Static property with text data type. Persists as `LOCAL_USER_NAME_DOMAIN` for the local agent and `REMOTE_USER_NAME_DOMAIN` for the remote device.	✓	✓	✓	✓		✓	✓
Domain Logon							
Set to true whenev	✓	✓	✓	✓		✓	✓

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
er the user belongs to a domain. Static property with boolean data type. Persists as `LOCAL_USER_DOMAINLOGON` for the local agent and `REMOTE_USER_DOMAIN LOGON` for the remote device.							
Groups							
The security groups that the user is a member of. Only	✓	✓					

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
security groups referenced below will be evaluated. Static property with text data type. Persists as `LOCAL_USER_GROUPS` for the local agent and `REMOTE_USER_GROUPS` for the remote device.							
Local Admin							
Set to true whenever the user has admin	✓	✓	✓	✓	✓	✓	✓

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
rights. Static property with boolean 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 property with text data type. Persists as `LOCAL_USER_N`	✓	✓	✓	✓	✓	✓	✓

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
`AME` for the local agent and `REMOTE_USER_NAME` for the remote device.							
Password Age							
The age of the user password in days. Available only for Active Directory and workgroup accounts. Static property with number data type. Persists as `LOCAL_`	✓	✓	✓				

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
`USER_PASSWORD_AGE` for the local 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 boolean data type. Persists as `LOCAL_USER_PASSWORD_AUTO`	✓	✓	✓				

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
`LOGON` for the local agent and `REMOTE_USER_PASSWORD_AUTOLOGON` for the remote device.							
SID							
The Security Identifier (SID) of the user. Static property with text data type. Persists as `LOCAL_USER_SID` for the local agent and `REMOTE_USER_SID` for the	✓	✓	✓		✓		

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

USER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							

WHOIS Properties

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
Provides the results of a WHOIS lookup of the endpoint.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Adapter							
The name of the network adapter used to query the whois data. Dynamic property with text data type. Persists as	✓	✓	✓	✓		✓	✓

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

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
`LOCAL_WHOIS_ADAPTER` for the local agent and `REMOTE_WHOIS_ADAPTER` for the remote device.							
Country							
The country where the remote device is located. Dynamic property with text data type. Persists as `LOCAL_WHOIS_COUNTRY` for the local agent	✓	✓	✓	✓		✓	✓

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

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_WHOIS_COUNTRY` for the remote device.							
DNS							
The DNS address of the remote device. Dynamic property with text data type. Persists as `LOCAL_WHOIS_DNS` for the local agent and `REMOTE_WHOIS_DNS` for the remote device.	✓	✓	✓	✓		✓	✓
IP							

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

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
The IP address of the remote device. Dynamic property with ip, text data types. Persists as `LOCAL_WHOIS_IP` for the local agent and `REMOTE_WHOIS_IP` for the remote device.	✓	✓	✓	✓		✓	✓
ISP							
The ISP of the remote device. Dynamic property with text data type.	✓	✓	✓	✓		✓	✓

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

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_WHOIS_ISP` for the local agent and `REMOTE_WHOIS_ISP` for the remote device.							
VPN							
Determines whether the whois data was queried using a VPN connection. Dynamic property with boolean data type. Persists as `LOCAL_`	✓	✓	✓	✓		✓	✓

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

WHOIS PROPERTY	AGENT	CLIENT EXTENSION					
`WHOIS_VPN` for the local agent and `REMOTE_WHOIS_VPN` for the remote device.							

Windows Properties

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
Provides real-time properties unique to Microsoft Windows.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
SmartScreen for Microsoft Edge							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
The state of SmartScreen for Microsoft Edge. Requires at 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 the local agent and	✓	✓					

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_WINDOWS_SMARTSCREEN_EDGE` for the remote device.							
SmartScreen for Microsoft Store							
The state of SmartScreen for Microsoft Store apps. Requires at least Windows 10 or Windows Server 2016. Realtime property with enum data	✓	✓					

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
type with options Off, Warn. Persists as `LOCAL_WINDOWS_SMARTSCREEN_STORE` for the local agent and `REMOTE_WINDOWS_SMARTSCREEN_STORE` for the remote device.							
SmartScreen for Windows Explorer							
The state of SmartScreen for	✓	✓					

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
Windows Explorer. Requires at least Windows 10 or Windows Server 2016. Realtime property with enum data type with options Off, Warn, Block. Persists as `LOCAL_WINDOWS_SMARTSCREEN_EXPLORER` for the local agent and `REMOTE_WINDO`							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
`WS_SMARTSCREEN_EXPLORER` for the remote device.							
UAC Enabled							
Set to true if the User Access Control (UAC) consent prompt is enabled. Realtime property with boolean data type. Persists as `LOCAL_WINDOWS_UAC_ENABLED` for the local	✓	✓					

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
agent and `REMOTE_WINDOWS_UAC_ENABLED` for the remote device.							
UAC Policy							
The User Access Control (UAC) consent prompt policy applied to administrators. Realtime property with enum data type with options Elevate without prompti	✓	✓					

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
ng, Prompt for credentials on secure desktop, Prompt for consent on secure desktop, Prompt for credentials on users desktop, Prompt for consent on users desktop, Prompt for consent for non-Windows binaries on secure							

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

WINDOWS PROPERTY	AGENT	CLIENT EXTENSION					
desktop, Prompt for consent for non-Windows binaries on users desktop. Persists as `LOCAL_WINDOWS_UAC_POLICY` for the local agent and `REMOTE_WINDOWS_UAC_POLICY` for the remote device.							

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

Windows Defender Properties

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
Provides real-time properties describing the state of Microsoft Windows Defender Antivirus.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Antimalware Version							
The version of the anti-malware component. Realtime property with version	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTIMALWARE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTIMALWARE` for the remote device.							
Antispyware Version							
The version of the anti-spyware compon	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
ent. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTISPYWARE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTISPYWARE` for the remote device.							
Antivirus Version							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
The version of the anti-virus component. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ANTIVIRUS` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ANTIVIRUS` for the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Behavior Threats							
Determines the number of threats identified by behavioral analysis. Realtime property with number data type. Persists as `LOCAL_WINDOWSDEFENDER_BEHAVIORTHREATS` for the local agent and	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_WINDOWSDEFENDER_BEHAVIORTHREATS` for the remote device.							
Cloud Protection							
Defines the status of Cloud Delivered Protection, which enables Windows Defender to receive the latest protection from the cloud. Realtim	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
e property with enum data type with options Disabled, Basic, Advanced. Persists as `LOCAL_WINDOWSDEFENDER_CLOUDPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_CLOUDPROTECTION` for the remote device.							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
Controlled Folder Access							
Defines the status of Windows Defender Exploit Guard's controlled folder access, which protects files, folders, and memory from unauthorized changes by unfriendly applications. Realtime	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
property with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_CONTROLLEDFOLDERACCESS` for the local agent and `REMOTE_WINDOWSDEFENDER_CONTROLLEDFOLDERACCESS` for the remote device.							
Engine Version							
The version of the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
engine. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_ENGINE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_ENGINE` for the remote device.							
Excluded Extensions							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
Defines the file extensions excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_EXTENSIONS` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_EXTENSIO`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`NS` for the remote device.							
Excluded Paths							
Defines the files or folders excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOWSDEFENDER_EXCLUSIONS_PATHS` for the local agent and	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_WINDOWSDEFENDER_EXCLUSIONS_PATHS` for the remote device.							
Excluded Processes							
Defines the process names excluded from Windows Defender. Realtime property with text data type. Persists as `LOCAL_WINDOW`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`SDEFENDER_EXCLUSIONS_PROCESSES` for the local agent and `REMOTE_WINDOWSDEFENDER_EXCLUSIONS_PROCESSES` for the remote device.							
Last Full Scan							
The time of the last full scan. Realtime property with datetime data	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
type. Persists as `LOCAL_WINDOWSDEFENDER_LASTFULLSCAN` for the local agent and `REMOTE_WINDOWSDEFENDER_LASTFULLSCAN` for the remote device.							
Last Quick Scan							
The time of the last quick scan. Realtime property with	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
datetime data type. Persists as `LOCAL_WINDOWSDEFENDER_LASTQUICKSCAN` for the local agent and `REMOTE_WINDOWSDEFENDER_LASTQUICKSCAN` for the remote device.							
Network Definition Version							
The version of the network definitions.	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION` for the remote device.							
Network Engine Version							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
The version of the network engine. Realtime property with version data type. Persists as `LOCAL_WINDOWSDEFENDER_VERSION_NETWORKENGINE` for the local agent and `REMOTE_WINDOWSDEFENDER_VERSION_NETWORKENGINE` for the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Real-Time Protection							
Set to true when Windows Defender's real-time protection is enabled, including behavior monitoring, downloaded files and attachment scanning, monitoring of file and	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
program activity, raw volume write notifications, and process scanning. Realtime property with boolean data type. Persists as `LOCAL_WINDOWSDEFENDER_REALTIMEPROTECTION` for the local agent and `REMOTE_WINDOWSDEFENDER_REALTIM`							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`EPROTECTION` for the remote device.							
Sample Submission							
Defines the status of Windows Defender sample submission, which sends sample files to Microsoft when further analysis is required. Realtime property with enum	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
data type with options Prompt, Send Safe Samples Automatically, Never Send Samples, Send All Samples Automatically. Persists as `LOCAL_WINDOWSDEFENDER_SAMPLESUBMISSION` for the local agent and `REMOTE_WINDOWSDEFENDER_S`							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`AMPLESUBMISSION` for the remote device.							
Signature Threats							
Determines the number of threats identified by their signature. Realtime property with number data type. Persists as `LOCAL_WINDOWSDEFENDER_SIGNATURETHREA`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`TS` for the local agent and `REMOTE_WINDOWSDEFENDER_SIGNATURETHREATS` for the remote device.							
Status							
The status of Windows Defender. Realtime property with enum data type with options Active, Pending Full Scan,	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
Pending Reboot, Pending Manual Steps, Pending Offline Scan, Due Full 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 PROPERTY	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 type. Persists as `LOCAL_WINDOWSDEFENDER_TAMPERPROTECTI`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS DEFENDER PROPERTY	AGENT	CLIENT EXTENSION					
`ON` for the local agent and `REMOTE_WINDOWSDEFENDER_TAMPERPROTECTION` for the remote device.							

Windows Firewall Properties

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Provides real-time properties describing the state of the Microsoft Window	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
s Firewall.							
Active Profile Block All Inbound							
Determines the active profiles which are configured to block all inbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREW`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
`ALL_ACTIVEPROFILES_BLOCKALLINBOUND` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_BLOCKALLINBOUND` for the remote device.							
Active Profile Disabled							
Determines the active profiles where the firewall is	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
disabled. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED` for the							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Active Profile Inbound Allowed							
Determines the active profiles which are configured to allow inbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_AC`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
`TIVEPROFILES_INBOUNDALLOWED` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_INBOUNDALLOWED` for the remote device.							
Active Profile Name							
Determines the names of the active profiles. Realtime property with enum	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_NAME` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_NAME` for the remote device.							
Active Profile Notifications							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Disabled							
Determines the active profiles which do not display a notification to the user when a program is blocked from receiving inbound connections. Realtime property with enum data type with options Domain, Private, Public. Persists	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFICATIONS` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFICATIONS` for the remote device.							
Active Profile Outbound Allowed							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
Determines the active profiles which are configured to allow outbound traffic. Realtime property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED` for the local	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED` for the remote device.							
Active Profile Respond to Multicast							
Determines the active profiles which respond to multicast or broadcast network traffic. Realtim	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
e property with enum data type with options Domain, Private, Public. Persists as `LOCAL_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for the local agent and `REMOTE_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST` for							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
the remote device.							
Any Inbound Rules							
Determines the port numbers which are allowed to receive an incoming connection from any process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_IN`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
`BOUNDRULES_ANY` for the local agent and `REMOTE_WINDOWSFIREWALL_INBOUNDRULES_ANY` for the remote device.							
Any Outbound Rules							
Determines the port numbers which are allowed to make an outgoing connection from any	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS FIREWALL PROPERTY	AGENT	CLIENT EXTENSION					
process. Realtime property with text data type. Persists as `LOCAL_WINDOWSFIREWALL_OUTBOUNDRULES_ANY` for the local agent and `REMOTE_WINDOWSFIREWALL_OUTBOUNDRULES_ANY` for the remote device.							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Registry Properties

WINDOWS REGISTRY PROPERTY	AGENT	CLIENT EXTENSION					
Provides access to Windows Registry entries.	Microsoft Windows	Microsoft Windows	Apple macOS	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Count							
The number of Windows Registry entries. Static property with number data type. Persists as `LOCAL_WINDOWSREGISTRY_COUNT` for the local agent and	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY PROPERTY	AGENT	CLIENT EXTENSION					
`REMOTE_WINDOWSREGISTRY_COUNT` for the remote device.							
Data							
The Windows Registry data. Static property with text, number, boolean, datetime, ip, position data types. Persists as `LOCAL_WINDOWSREGISTRY_X_DATA` for the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY PROPERTY	AGENT	CLIENT EXTENSION					
local agent and `REMOTE_WINDOWSREGISTRY_X_DATA` for the remote device.							
Path							
The Windows Registry path. Static property with text data type. Persists as `LOCAL_WINDOWSREGISTRY_X_PATH` for the local agent and `REMOTE`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY PROPERTY	AGENT	CLIENT EXTENSION					
`_WINDOWSREGISTRY_X_PATH` for the remote device.							
Value							
The Windows Registry value. Static property with text data type. Persists as `LOCAL_WINDOWSREGISTRY_X_VALUE` for the local agent and `REMOTE_WINDOWSREGISTRY_X_VALUE`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS REGISTRY PROPERTY	AGENT	CLIENT EXTENSION					
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	Ubuntu	Chrome OS	IGEL OS	Unicon ™ eLux
Critical KB							
The knowledge base article IDs of any pending critical updates.	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICAL` for the local agent and `REMOTE_WINDOWSUPDATE_CRITICAL` for the remote device.							
Critical Release Date							
The deployment date of the oldest	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
pending critical update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_CRITICAL_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_CRITICAL_RELEASEDATE` for the remote device.							
Definition KB							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
The knowledge base article IDs of any pending definition updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_DEFINITION` for the local agent and `REMOTE_WINDOWSUPDATE_DEFINITION` for the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Definition Release Date							
The deployment date of the oldest pending definition update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_DEFINITION_RELEASEDATE` for the local agent	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
and `REMOTE_WINDOWSUPDATE_DEFINITION_RELEASEDATE` for the remote device.							
Enabled							
Set to true whenever the Windows Update service is enabled. Realtime property with boolean data type. Persists as `LOCAL_`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
`WINDOWSUPDATE_ENABLED` for the local agent and `REMOTE_WINDOWSUPDATE_ENABLED` for the remote device.							
Last Install							
Set to the time that Windows Update last installed updates. Realtime property with datetime data type.	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
Persists as `LOCAL_WINDOWSUPDATE_LASTINSTALL` for the local agent and `REMOTE_WINDOWSUPDATE_LASTINSTALL` for the remote device.							
Last Search							
Set to the time that Windows Update last checked for updates. Realtim	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
e property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_LASTSEARCH` for the local agent and `REMOTE_WINDOWSUPDATE_LASTSEARCH` for the remote device.							
Notification Level							
Represents how Windows	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
Update is configured to notify the user. Realtime property with enum data type with options Not Configured, Disabled, Notify Before Download, Notify Before Install, Scheduled Install. Persists as `LOCAL_WINDOWSUPDATE_NOTI`							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
`FICATIONLEVEL` for the local agent and `REMOTE_WINDOWSUPDATE_NOTIFICATIONLEVEL` for the remote device.							
Reboot Required							
Set to true whenever Windows Update is awaiting a reboot to finish updating. Realtime	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
property with boolean data type. Persists as `LOCAL_WINDOWSUPDATE_REBOOTREQUIRED` for the local agent and `REMOTE_WINDOWSUPDATE_REBOOTREQUIRED` for the remote device.							
Rollup KB							
The knowledge base article IDs of any	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
pending rollup updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_ROLLUP` for the local agent and `REMOTE_WINDOWSUPDATE_ROLLUP` for the remote device.							
Rollup Release Date							
The deployment	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
date of the oldest pending rollup update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_ROLLUP_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_ROLLUP_RELEASEDATE` for the remote device.							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
Security KB							
The knowledge base article IDs of any pending security updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_SECURITY` for the local agent and `REMOTE_WINDOWSUPDATE_SECURITY` for the	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
remote device.							
Security Release Date							
The deployment date of the oldest pending security update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_SECURITY_RELEASEDATE` for the local agent and `REMOTE`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
`_WINDOWSUPDATE_SECURITY_RELEASEDATE` for the remote device.							
Service Pack KB							
The knowledge base article IDs of any pending service pack updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDAT`	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
`E_SERVICEPACK` for the local agent and `REMOTE_WINDOWSUPDATE_SERVICEPACK` for the remote device.							
Service Pack Release Date							
The deployment date of the oldest pending service pack update. Realtime property with datetim	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
e data type. Persists as `LOCAL_WINDOWSUPDATE_SERVICEPACK_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_SERVICEPACK_RELEASEDATE` for the remote device.							
Update KB							
The knowledge base article IDs of any	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
pending updates. Realtime property with text data type. Persists as `LOCAL_WINDOWSUPDATE_UPDATE` for the local agent and `REMOTE_WINDOWSUPDATE_UPDATE` for the remote device.							
Update Release Date							
The deployment date of	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
the oldest pending update. Realtime property with datetime data type. Persists as `LOCAL_WINDOWSUPDATE_UPDATE_RELEASEDATE` for the local agent and `REMOTE_WINDOWSUPDATE_UPDATE_RELEASEDATE` for the remote device.							
Version							

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WINDOWS UPDATE PROPERTY	AGENT	CLIENT EXTENSION					
Set to the version number of Windows Update. Realtime property with version data type. Persists as `LOCAL_WINDOWSUPDATE_VERSION` for the local agent and `REMOTE_WINDOWSUPDATE_VERSION` for the remote device.	✓	✓					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 `CLOUD` platform.

If the local device is not located within an authorized country, you can choose between two actions:

- Sets the Compliance State in Azure AD based on the country of the local device.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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
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.

© 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
Country - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Azure AD 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 Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X with the same

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			list of authorized countries as above.
Country - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Azure AD 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 Of AUTHORIZED_COUNTRY_1
			Replace AUTHORIZED_COUNTRY_X with the same list of authorized

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			countries as above.
			`Azure AD 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.
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 Azure AD properties based on the compliance requirements of a local device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

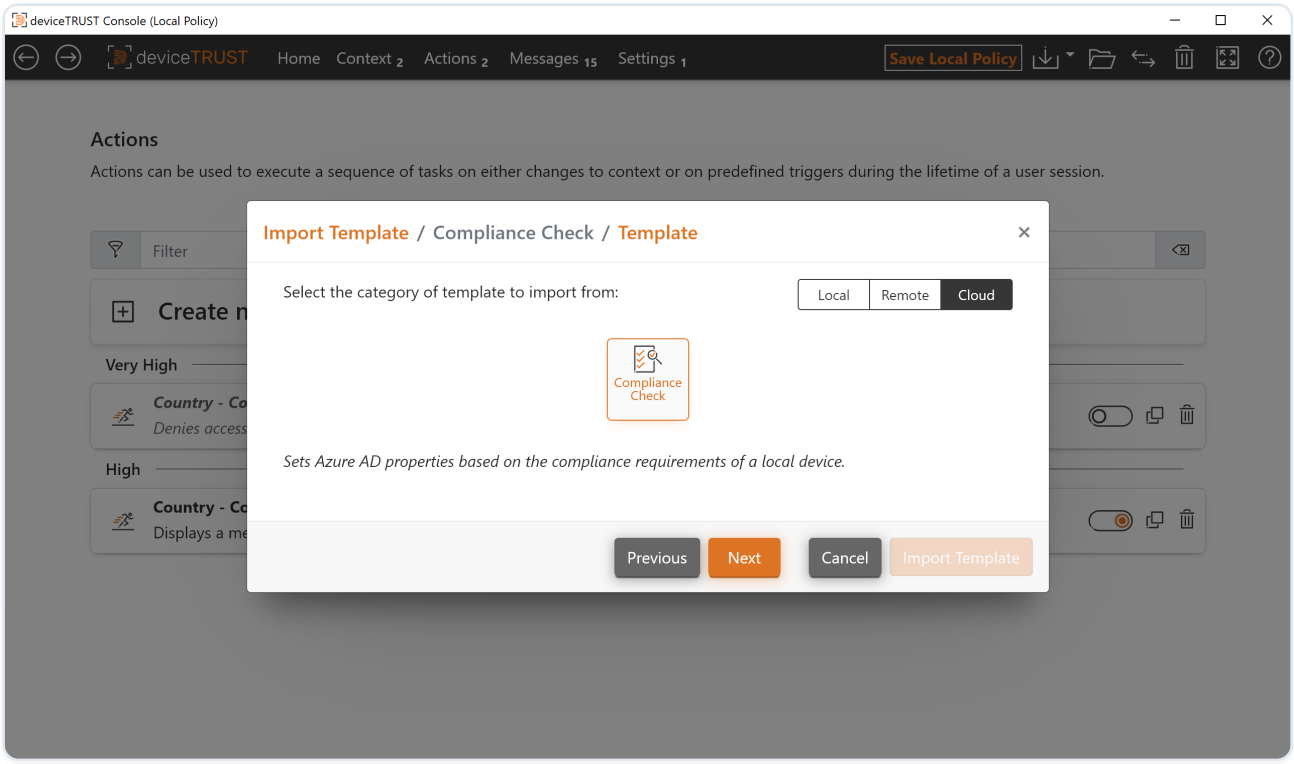


TABLE OF CONTENTS

- Country - Sets Azure AD properties based on the country of the local device.
- Operating System Update State - Sets Azure AD properties based on the operating system update state of the local device.
- Remote Controlled) - Sets Azure AD properties based on if the local device is remote controlled.
- Security State - Sets Azure AD properties based on the security state of the local device.
- Threat Detection - Sets Azure AD properties based on if a threat is detected or the local device has not been scanned recently.
- User Privileges - Sets Azure AD properties based on the privileges of the user logged into the local device.
- Wi-Fi Security Mode - Sets Azure AD 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 `CLOUD` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Azure AD based on the operating system update state of the local device.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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
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.

© 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 Update - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Azure AD based on the operating system update state of the local device.	Deactivated	None
Operating System Update - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Azure AD based on the operating system update state of the local device.	Deactivated	You may want to update the following context condition with data suitable for your environment `Azure AD 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 `CLOUD` platform.

If the remote device is remote controlled, you can choose between two actions:

- Sets the Compliance State in Azure AD based on if the local device is remote controlled.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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
Remote Controlled	Defines if the local device is remote controlled.	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
Remote Controlled - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Azure AD based on if the local device is remote controlled.	Deactivated	None
Remote Controlled - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Azure AD based on if the local device is remote controlled.	Deactivated	You may want to update the following context condition with data suitable for your environment
			`Azure AD Set Extension Attribute [1]`
			Set Extension Attribute may be changed to a value suitable for your organisation.

© 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, 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 `CLOUD` platform.

If the security state of the local device is unprotected, you can choose between two actions:

- Sets the Compliance State in Azure AD based on the security state of the local device.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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 context:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Azure AD based on the security state of the local device.	Deactivated	None
Security State - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Azure AD based on the security state of the local device.	Deactivated	You may want to update the following context condition with data suitable for your environment
			`Azure AD Set Extension Attribute [1]`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 `CLOUD` 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 Azure AD based on if a threat is detected or the local device has not been scanned recently.
- Sets an Extension Attribute in Azure AD based on if a threat is detected or the local device has not been scanned recently.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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
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 - Enforcement -	Sets the Compliance State in Azure AD based on if a threat is detected or the	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Compliance State	local device has not been scanned recently.		
Threat Detection - Conditional Access - Enforcement - Extension Attribute	Sets an Extension Attribute in Azure AD 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 `Azure AD 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.

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 `CLOUD` platform.

If the privileges of the user logged into the local device are privileged without protection, you can choose between two actions:

- Sets the Compliance State in Azure AD based on the privileges of the user logged into the local device.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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

© 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
User Privilege - Conditional Access - Enforcement - Compliance State	Sets the Compliance State in Azure AD 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 Azure AD 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 `Azure AD Set Extension Attribute [1]` *Set Extension Attribute may be changed to a value suitable*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 `CLOUD` platform.

If the local device is connected to an insecure Wi-Fi network, you can choose between two actions:

- Sets the Compliance State in Azure AD based on the Wi-Fi Security Mode of the local device.
- Sets an Extension Attribute in Azure AD 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 cloud environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your cloud 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
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.

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 Azure AD based on the Wi-Fi Security Mode of the local device.	Deactivated	None
Wi-Fi Security - Conditional Access - Enforcement -	Sets an Extension Attribute in Azure AD	Deactivated	You may want to update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Extension Attribute	based on the Wi-Fi Security Mode of the local device.		condition with data suitable for your environment
			`Azure AD 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
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: 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: 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

© 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
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

© 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 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:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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.

© 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 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:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

Step 2: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a local device	You must update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
	based on its NetBIOS name.	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

© 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
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.

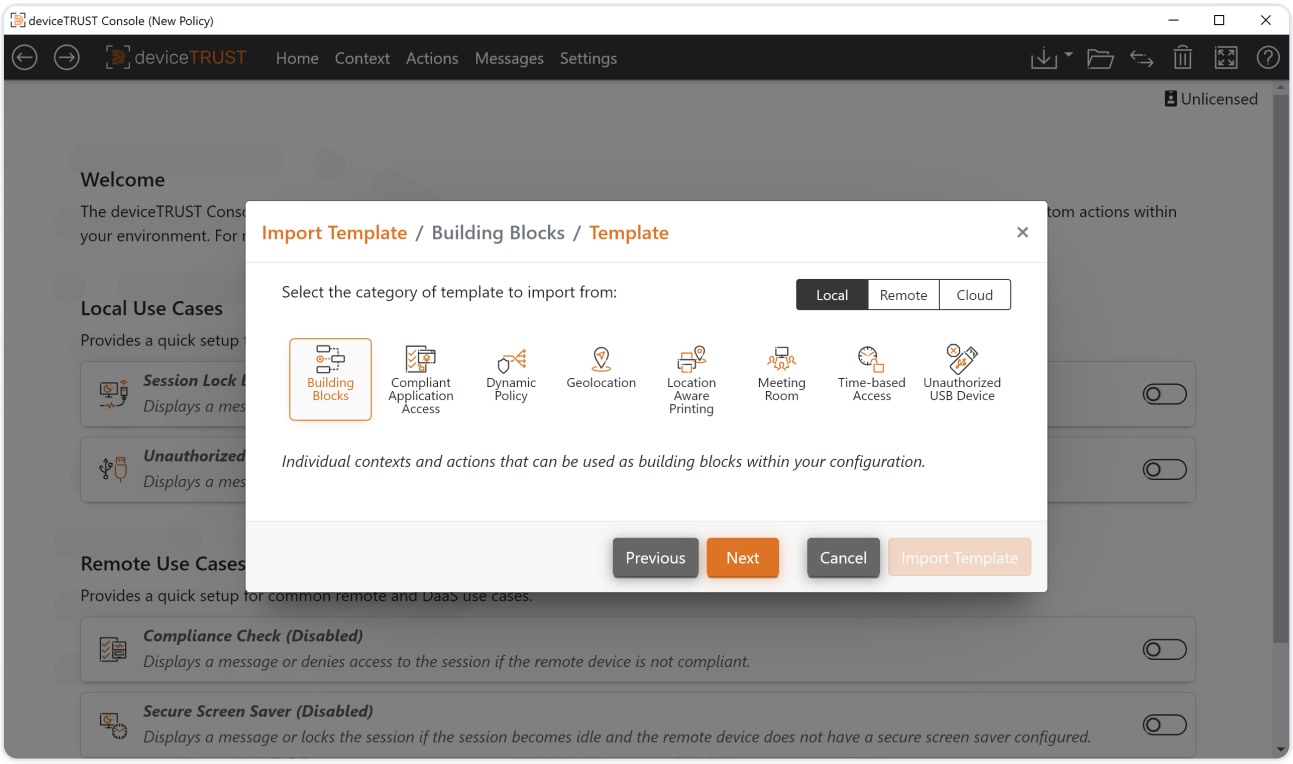


TABLE OF CONTENTS

- 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.
- 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.
- Proximity - Defines the proximity of the local device to a given position.
- Session Idle - Defines if the session is idle.

© 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 local device.
- Unauthorized USB Storage Device - Defines if an unauthorized USB storage device 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.

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:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		(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:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Policy Mode	Defines if the deviceTRUST policy runs in active or passive mode based upon	You can add one or more user groups from your Microsoft Active Directory (AD) to activate the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	the membership of an AD group.	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:

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.

© 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.

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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Replace 0,0 with your target position and define the range to the given position on all conditions.
		Example: 49.8971,8.9258

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

© 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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unauthorized USB Storage Device Template

This template imports a predefined context that defines whether an unauthorized USB storage device 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:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Unauthorized USB Storage Device	Defines if an unauthorized USB storage device is 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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

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
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.

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

© 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.

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:

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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: Context
- 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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%

© 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.

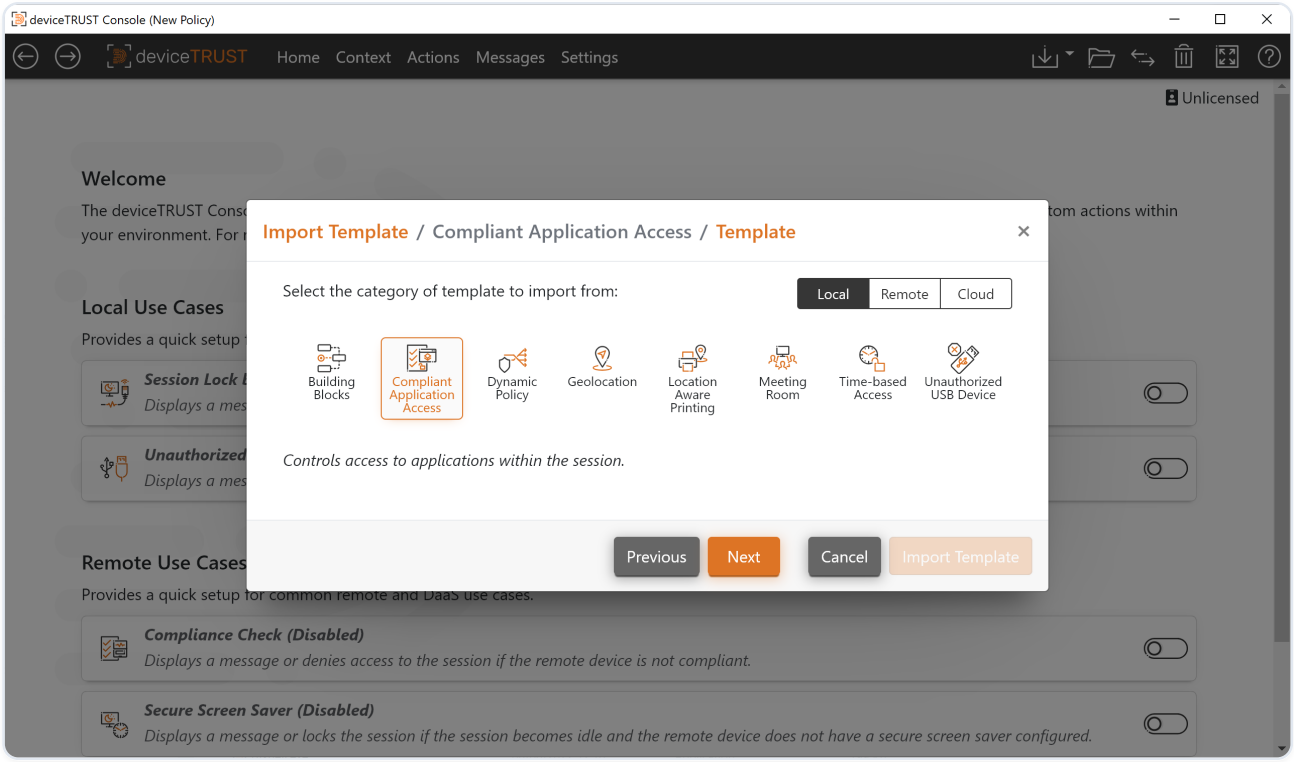
Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

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.
- 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.
- 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: Context
- 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
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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`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
			`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: Context
- 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 tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles% \FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Wi-Fi Security Mode - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker for insecure Wi-Fi networks.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Working Time Template

This template creates a configuration that 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- 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.*

NOTE:

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: notepad++.exe
Working Time - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE:

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dynamic Policy Templates

Applies a dynamic policy within the session.

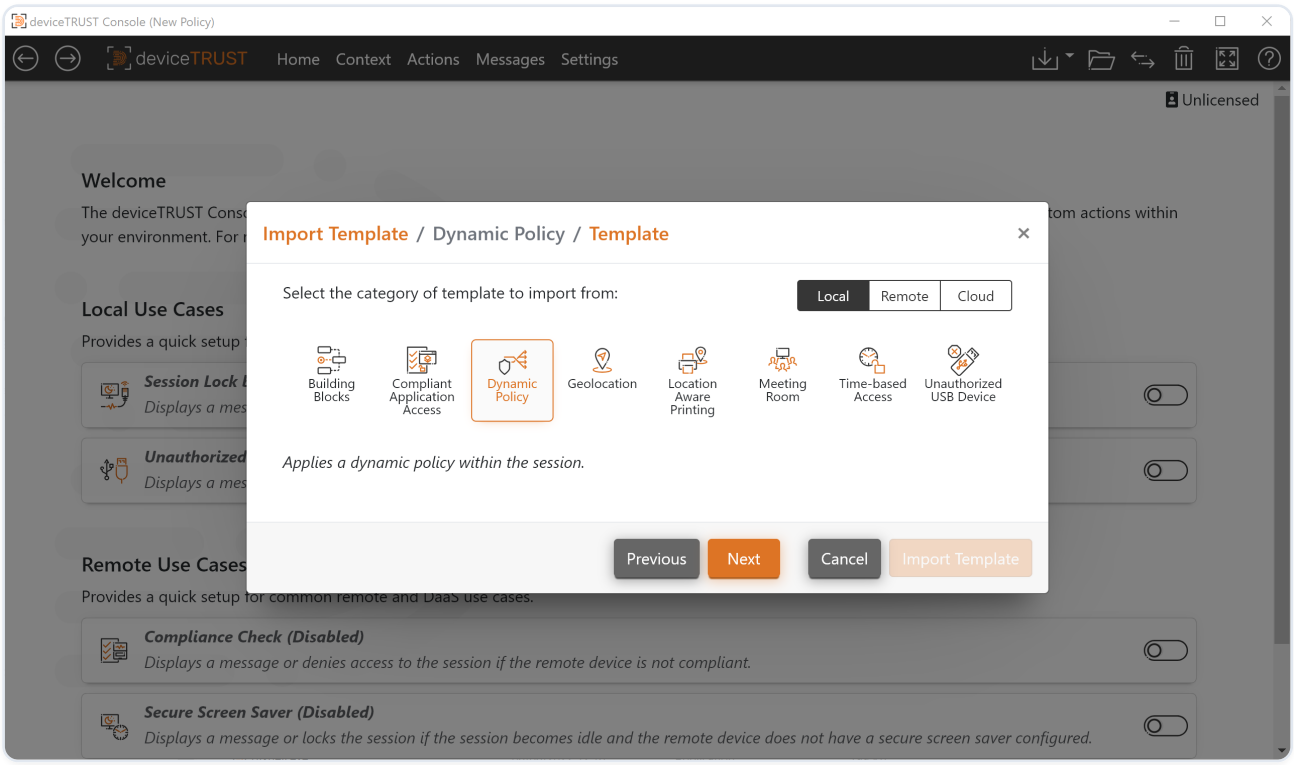


TABLE OF CONTENTS

- 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- 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: Context
- 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: Context
- 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: Context
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Country - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			with your authorized countries using the ISO 3166-1 Alpha-2 code. *Example: US* `MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.* *Example: %PROGRAMFILES%\Notepad++\notepad++.exe*

NOTE

If both actions have been disabled, the contexts will still be created.

Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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: Context
- 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
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.

Geolocation Templates

Validates and controls access based on geolocation information of the local device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

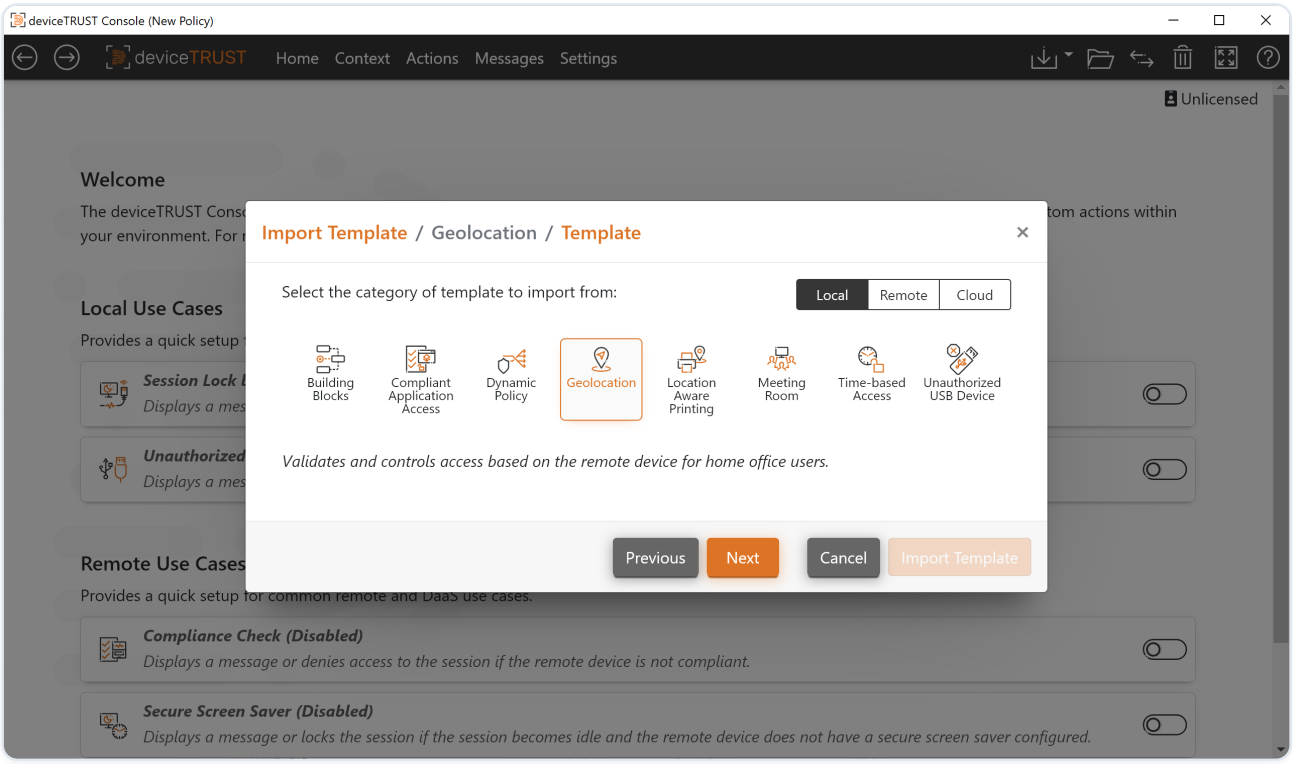


TABLE OF CONTENTS

- 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.

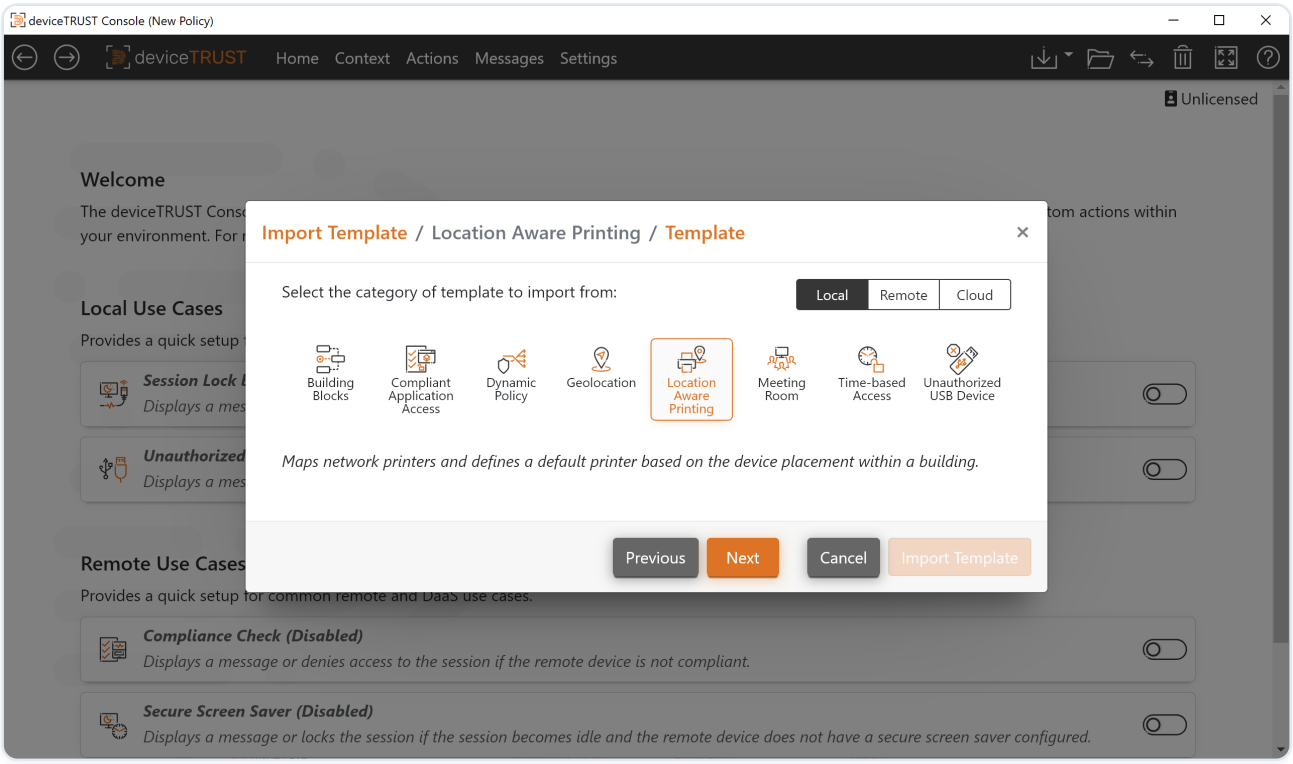


TABLE OF CONTENTS

- 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: Context

© 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.

© 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 - IP Address	Maps network printers and defines a default printer based on the location of the 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.

© 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.

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: Context
- 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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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 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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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: Context
- 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.

© 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 - Wi-Fi access point	Maps network printers and defines a default printer based on the location of the 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.

© 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.

Custom Values Template

This template creates a configuration that locks the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on custom values on the local device. It can be found in the `MEETING ROOM` 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: 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 if the session is idle. Differs between meeting rooms and other locations based on custom values.	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 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.

Meeting Room Templates

Controls an idle period for devices based upon whether the device is placed within a meeting room.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

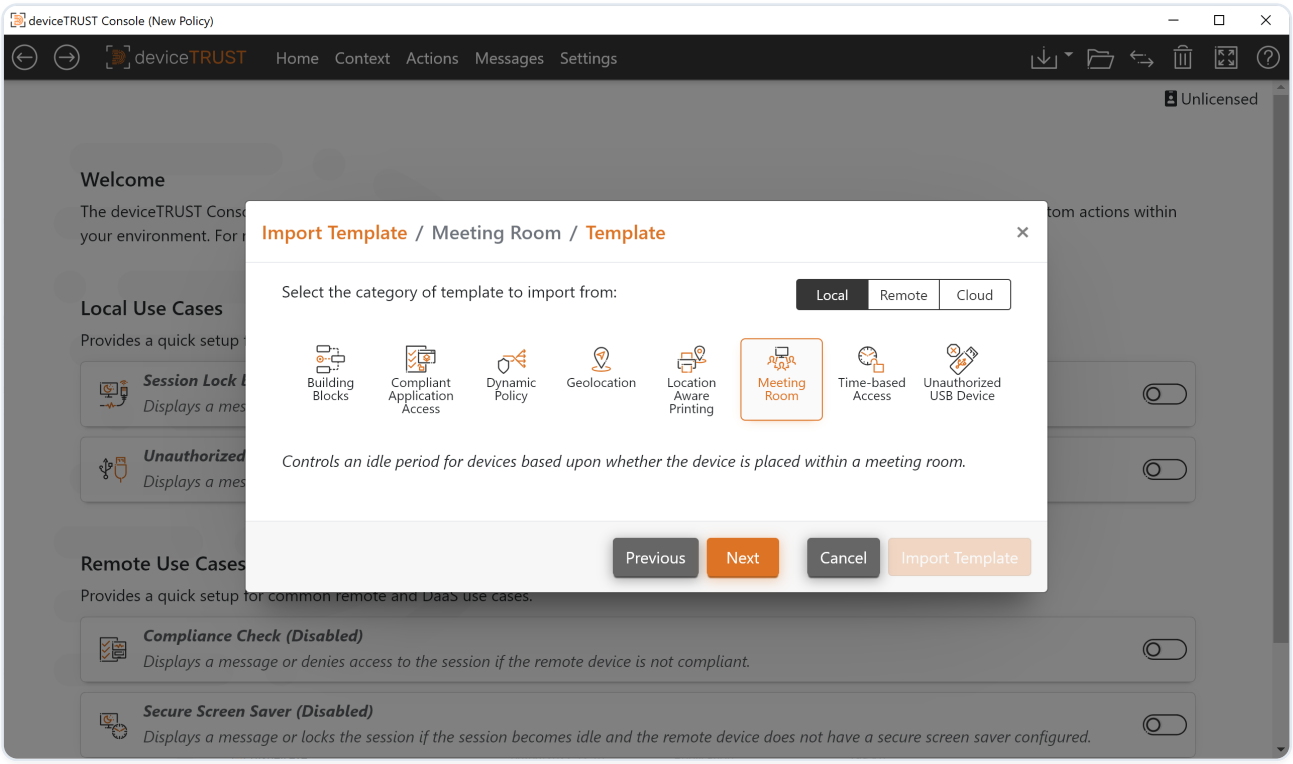


TABLE OF CONTENTS

- Custom Values - Locks the session after an idle period which differs between meeting rooms and other locations based on custom values on the local device.
- IP Address - Locks the session after an idle period which differs between meeting rooms and other locations based on the IP address of the local device.
- NetBIOS Name - Locks the session after an idle period which differs between meeting rooms and other locations based on the NetBIOS name of the local device.

IP Address Template

This template creates a configuration that locks the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on the IP address of the local device. It can be found in the `MEETING ROOM` 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- 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 if the session is idle. Differs between meeting rooms and other locations based on the 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 with your meeting room device IPv4 range.* *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.

© 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.

NetBIOS Name Template

This template creates a configuration that locks the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on the NetBIOS name of the local device. It can be found in the `MEETING ROOM` 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: 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
Session Idle	Defines if the session is idle. Differs between meeting rooms and other locations based on the NetBIOS name.	You must update the following context condition with data suitable for your environment `LOCAL - NAME NAME Any Of 3 ITEMS` *Replace MEETING_ROOM_DEVICE_NAME_X with your meeting room device name.* *Example: MEETING-ROOM-1*

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.

Time-based 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: Context
- 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
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00`
		Adjust your work hours to fit your requirements.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`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%

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			\FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
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.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

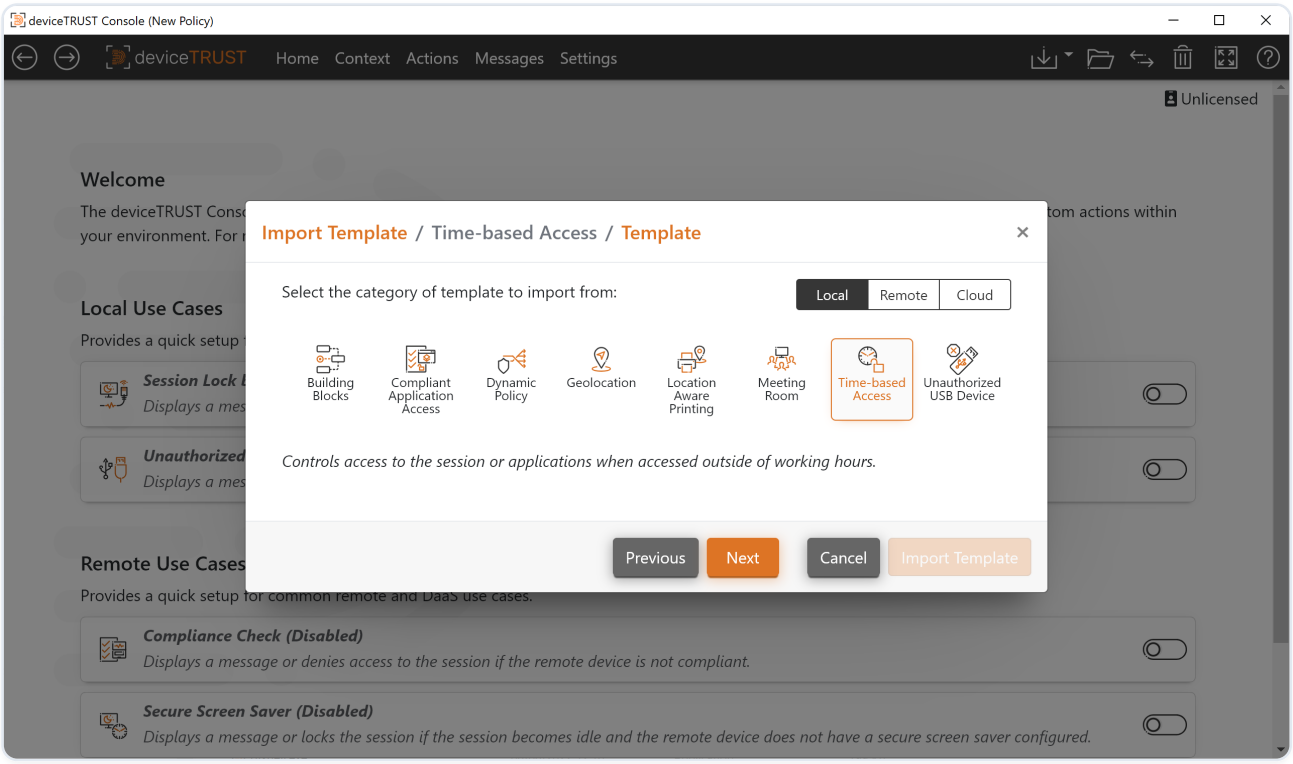


TABLE OF CONTENTS

- Conditional Application Access - Hides or denies access to applications in the session outside of working hours.

Unauthorized USB Drives Templates

Denies access to the session when an unauthorized USB device is plugged in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

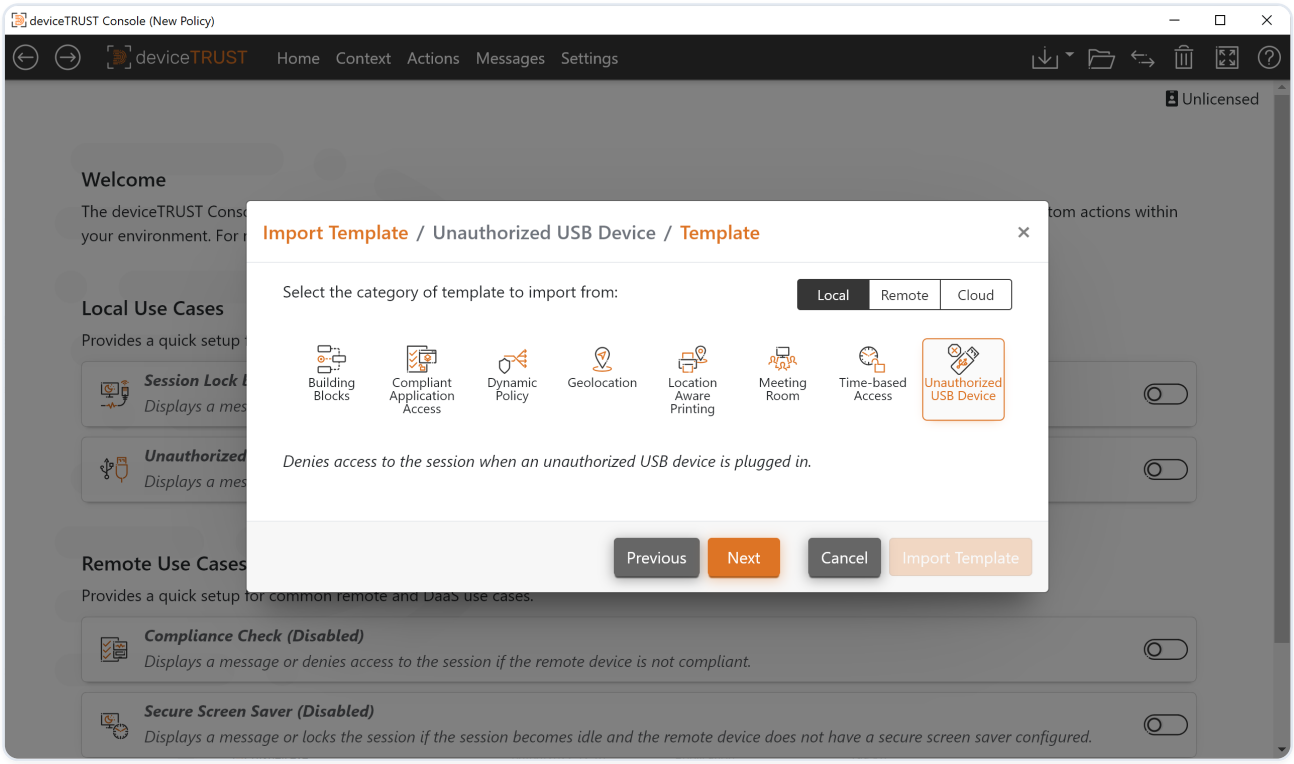


TABLE OF CONTENTS

- Unauthorized USB Device
- Unauthorized USB Storage 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 local device. It can be found in the `UNAUTHORIZED USB DEVICE` category when filtered for `LOCAL` platform.

If an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the local device, you can choose between two actions:

- Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.
- Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- 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
Unauthorized USB Device	Defines if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.	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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes a notifying action that displays a message to the user about a context status and an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Unauthorized USB Device Enforcement	Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.	Deactivated	None
Unauthorized USB Device Notification	Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.	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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unauthorized USB Storage Device Template

This template creates a configuration that checks if an unauthorized USB storage device is plugged into the local device. It can be found in the `UNAUTHORIZED USB DEVICE` category when filtered for `LOCAL` platform.

If an unauthorized USB storage device is plugged into the local device, you can choose between two actions:

- Denies access to the session if an unauthorized USB storage device is plugged in.
- Displays a message in the session if an unauthorized USB storage device is plugged in.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

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.

Step 2: Contexts

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Unauthorized USB Device	Defines if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged in.	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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.

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 Storage Device Enforcement	Denies access to the session if an unauthorized USB storage device is plugged in.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Unauthorized USB Storage Device Notification	Displays a message in the session if an unauthorized USB storage device is plugged in.	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.

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
- 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: 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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`*.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*

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Citrix HDX™ RealTime Media Engine Template

This template imports a predefined context that defines whether a supported version of the Citrix HDX RealTime media engine 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 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: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Citrix HDX RealTime Media Engine Version	Defines if a supported version of the Citrix HDX RealTime media engine is 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.

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 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: 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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
		`REMOTE - CERTIFICATE ROOT NAME Equals ADD_ROOT_NAME`
		Replace ADD_ROOT_NAME with your root certification authority (CA) name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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%

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			\FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
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.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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
- 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: Context

The template has imported the following context:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Azure AD 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	

© 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

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 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: 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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: 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: 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.

Country Provider with Fallback Template

This template imports a predefined context that defines the country provider that reports the country in which the remote device is located, including a fallback to the previous known country

© 1997–2026 Citrix Systems, Inc. All rights reserved.

within a timeout period, 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: 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: 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.

Country with Fallback Template

This template imports a predefined context that defines the country in which the remote device is located, including a fallback to the previous known country within a timeout period, and can be

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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: 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: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located. Includes a fallback to the previous known country within a timeout period.	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 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: 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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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 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 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: 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 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 remote 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 `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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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

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 Type BYOD Template

This template imports a predefined context that defines the device type of the remote device as BYOD 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 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: 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
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Azure AD domain joined devices, replace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`_THUMBPRINT_SHA256`
		When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.
		Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56

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 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: 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
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Azure AD 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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: 0d57fdd21474ef7806818a661a5f1d1cb33

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		61a8bb4ccd660dae6 930a6a135a56	
		`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_SHA25 6`	
		When using eLux devices, replace SCOUT_CERTIFICA TE_THUMBPRINT_ SHA256 with your eLux Scout Server certificate thumprint.	
		Example: 0d57fdd21474ef7806 818a661a5f1d1cb33 61a8bb4ccd660dae6 930a6a135a56	

© 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 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 simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		When using AD or Azure AD 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Context

The template has imported the following context:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

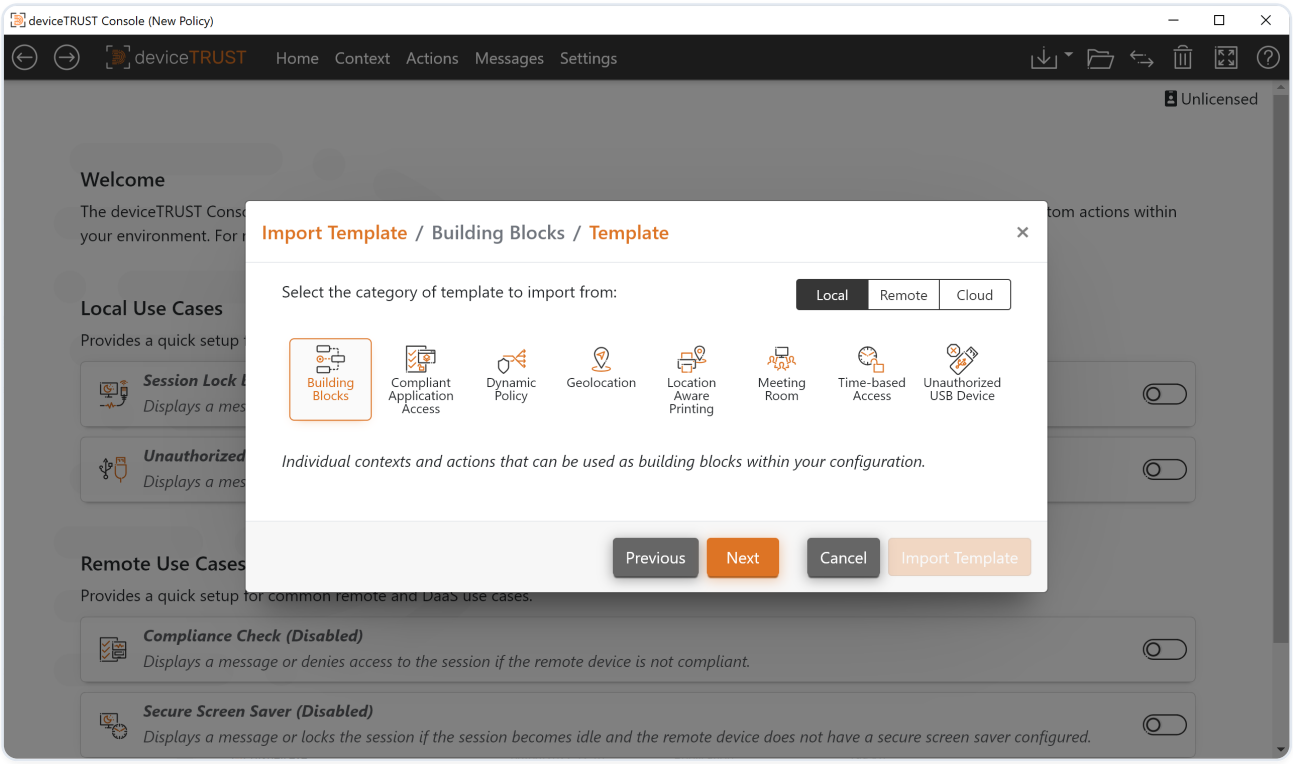


TABLE OF CONTENTS

- 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.

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 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: 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 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: 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 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: 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 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: 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.

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 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: Context

The template has imported the following context:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Proximity	Defines the proximity of the remote device to a given position.	You must update the following context condition with data suitable for your environment
		`REMOTE - LOCATION POSITION In Range 500 METERS FROM 0,0,...`
		Replace 0,0 with your target position and define the range to the given position on all conditions. Example: 49.8971,8.9258

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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.

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 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: 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
		`REMOTE - IGEL UMS CERT THUMPRINT SHA256 Equals UMS_CERTIFICATE_THUMBPRINT_SHA256`
		When using IGEL OS devices, replace UMS_CERTIFICATE_THUMBPRINT_SH

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		A256 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: 0d57fdd21474ef7806818a661a5f1d1cb33

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		61a8bb4ccd660dae6930a6a135a56

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 `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		suitable for your environment	
		`LOCAL - SESSION IDLE PERIODE Greater Than 10`	
		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.

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 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: 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.

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 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: 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 / 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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: Context

The template has imported the following context:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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: Context

The template has imported the following context:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Virtualized	Defines if the remote device is virtualized.	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.

VPN Connected Template

This template imports a predefined context that defines whether a network adapter of the remote device is connected to a VPN networ, 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: 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: 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 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: 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 Azure AD 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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	Denies access to the session if the remote	Deactivated	You must update the following

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Access - Enforcement	BYOD is not compliant.		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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
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 Azure AD domain joined devices, replace DOMAIN_SID and AZURE_TENANT_ID with your corporate values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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_CERTIFICA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		TE_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.
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

© 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
Compliance Check - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within 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 AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code.
			Example: US
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
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
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			with your authorized countries using the ISO 3166-1 Alpha-2 code.
			Example: US
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES%\Notepad++\notepad++.exe

NOTE

If both actions have been disabled, the contexts will still be created.

Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

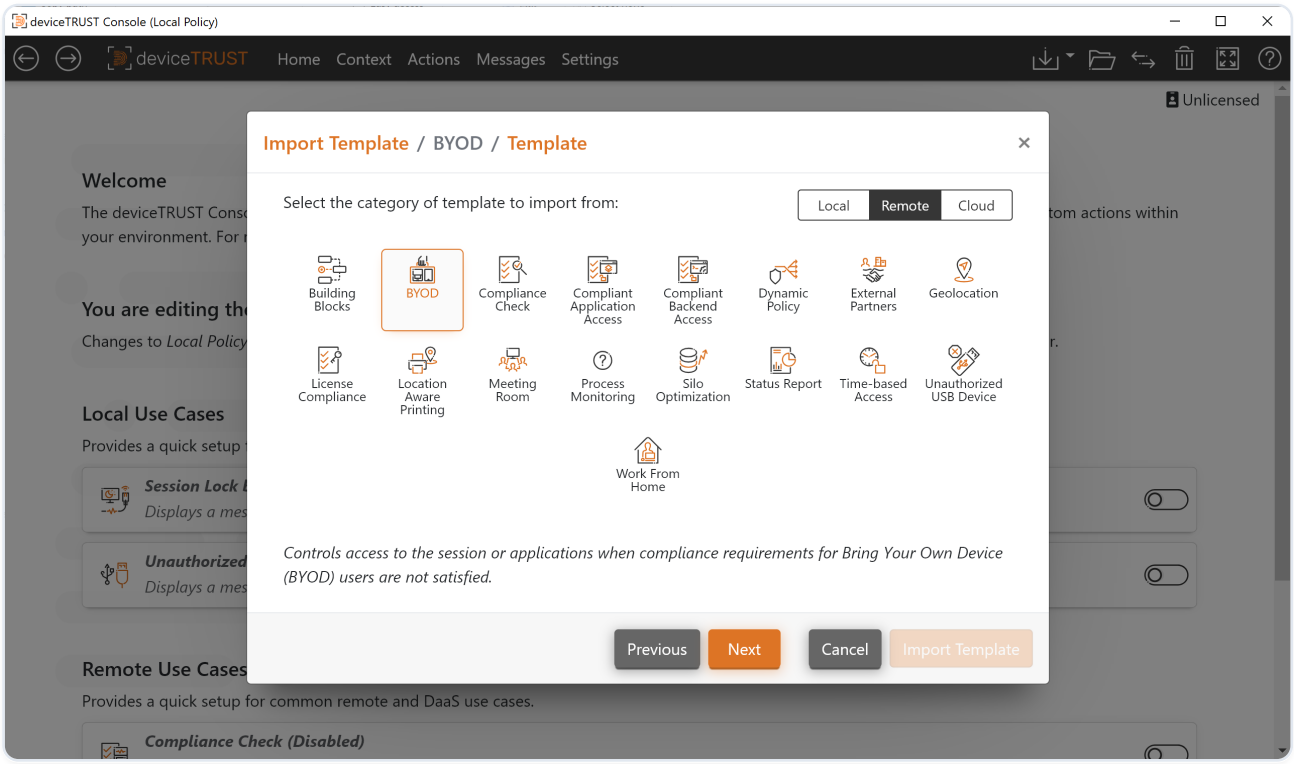


TABLE OF CONTENTS

- 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.

Citrix Clients Template

This template creates a configuration that checks if the version of Citrix Workspace™ app or Citrix HDX™ RealTime media engine on the remote device is supported. It can be found in the `COMPLIANCE CHECK` category when filtered for `REMOTE` platform.

If the version of Citrix Workspace app or Citrix HDX RealTime media engine on the remote device is not supported, you can choose between the following actions:

- Denies access to the session if the Citrix HDX RealTime media engine version of the remote device is not supported or missing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Denies access to the session if the Citrix Workspace App version of the remote device is not supported.
- Displays a message in the session if the Citrix HDX RealTime media engine version of the remote device is not supported or missing.
- Displays a message in the session if the Citrix Workspace App version 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Citrix HDX RealTime Media Engine Version	Defines if a supported version of the Citrix HDX RealTime media engine is installed on the remote device.	None
Citrix Workspace App Version	Defines if a supported version of the Citrix Workspace	You must update the following context condition with data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
	App is installed on the remote device.	suitable for your environment	
		`LOCAL - REMOTE CONTROL REMOTE VERSION Greater Than Or Equals 20.1`	
		Configure the minimal Citrix Workspace App version for your environment.	
		Example: 20.1	

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 notifying actions that displays a message to the user about a context status and enforcement actions that actively controls access to the session. By default, only the notifying actions are enabled and the enforcement actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Citrix HDX RealTime Media Engine Version - Conditional Access - Enforcement	Denies access to the session if the Citrix HDX RealTime media engine version of the remote device is not supported or missing.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Citrix Workspace App Version - Conditional Access - Enforcement	Denies access to the session if the Citrix Workspace App version of the remote device is not supported.	Deactivated	None
Citrix HDX RealTime Media Engine Version - Conditional Access - Notification	Displays a message in the session if the Citrix HDX RealTime media engine version of the remote device is not supported or missing.	Activated	None
Citrix Workspace App Version - Conditional Access - Notification	Displays a message in the session if the Citrix Workspace App version of the remote device is not supported.	Activated	None

NOTE

If all actions have been disabled, the contexts will still be created.

If all 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
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	

© 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
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

© 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.

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:

- 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: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
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	
		`REMOTE - CERTIFICATE ROOT THUMPRINT SHA256 Equals ADD_ROOT_THUMPRINT`	
		Replace ADD_ROOT_THUMPRINT with your root certification authority	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		(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

NOTE

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Corporate Device	Defines if the remote device is a corporate managed device.	You must update the following context condition with data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		suitable for your environment	
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`	
		When using AD or Azure AD 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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

Country with Fallback Template

This template creates a configuration that checks the country of the remote device including a fallback to the previous known country within a timeout period. 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.
- Displays a message in the session based on the country of the remote device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located. Includes a fallback to the previous known country within a timeout period.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes 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

© 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*

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 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
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 installed on 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.

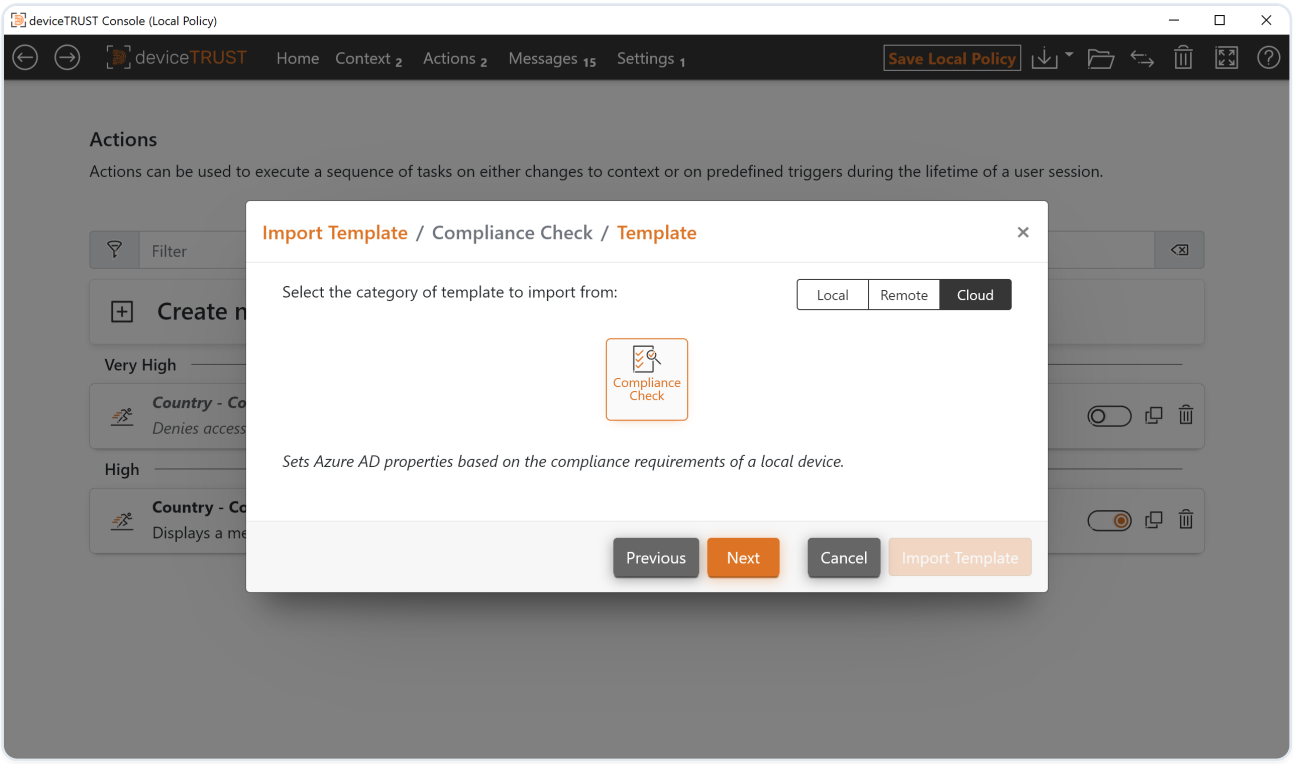
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

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.



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.

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: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System	Defines if the operating system of the remote device is supported.	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 - 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

© 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.

Operating System Update Template

This template creates a configuration that checks if the operating system of the remote 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 `REMOTE` platform.

If the operating system of the remote device has not performed a recent update search or has outstanding critical updates, you can choose between two actions:

- Denies access to the session if the operating system of the remote device has not performed a recent update search or has outstanding updates.
- Displays a message in the session if the operating system of the remote device has not performed a recent update search or has outstanding updates.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Update	Defines if a recent update search has been performed and that all updates have been installed 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
Operating System Update - Conditional Access - Enforcement	Denies access to the session if the operating system of the remote device has not performed a recent update search or has outstanding updates.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Operating System Update - Conditional Access - Notification	Displays a message in the session if the operating system of the remote device has not performed a recent update search or has outstanding updates.	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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

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

© 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.

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
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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.

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 security state of the remote device.	Deactivated	None
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 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
Threat Detection - Conditional Access - Enforcement	Denies access if a threat is detected or the device has not been scanned recently.	Deactivated	None
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Virtualized - Conditional Access - Notification	Displays a message in the session if the remote device is virtualized.	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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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	Activated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	connected to an insecure Wi-Fi network.		

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: Context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	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`

© 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*

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	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
	is connected externally.		
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Access Mode - Conditional Application Access - Enforcement -	Denies access to applications with Microsoft AppLocker within the session if the	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft AppLocker	remote device is connected externally.		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:

© 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Corporate Device	Defines if the remote device is a corporate managed device.	You must update the following context condition with data suitable for your environment
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Azure AD domain joined devices, replace DOMAIN_SID and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`_THUMBPRINT_SHA256` *When using eLux devices, replace SCOUT_CERTIFICATE_THUMBPRINT_SHA256 with your eLux Scout Server certificate thumprint.* *Example: 0d57fdd21474ef7806818a661a5f1d1cb3361a8bb4ccd660dae6930a6a135a56*

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Corporate Device - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is not a corporate	Deactivated	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	managed device.		
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Corporate Device - Conditional Application Access - Enforcement -	Denies access to applications with Microsoft AppLocker within the session if the	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft AppLocker	remote device is not a corporate managed device.		your environment `MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.* *Example: %PROGRAMFILES% \Notepad++ \notepad++.exe*

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Country Template

This template creates a configuration that checks the country of the remote device. It can be found in the `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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hides applications with FSLogix App Masking within the session based on the country of the remote device.
- Denies access to applications with Microsoft AppLocker within the session based on the country of the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Country - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session based on the country of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code.
			Example: US
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Country - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session based on the country of the remote device.	Deactivated	You must update the following context condition with data suitable for your environment
			`COUNTRY None Of AUTHORIZED_COUNTRY_1,...`
			Replace AUTHORIZED_COUNTRY_X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			with your authorized countries using the ISO 3166-1 Alpha-2 code. *Example: US* `MICROSOFT APPLOCKER` *Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.* *Example: %PROGRAMFILES%\Notepad++\notepad++.exe*

NOTE

If both actions have been disabled, the contexts will still be created.

Country codes are based on ISO 3166-1 Alpha-2 code.

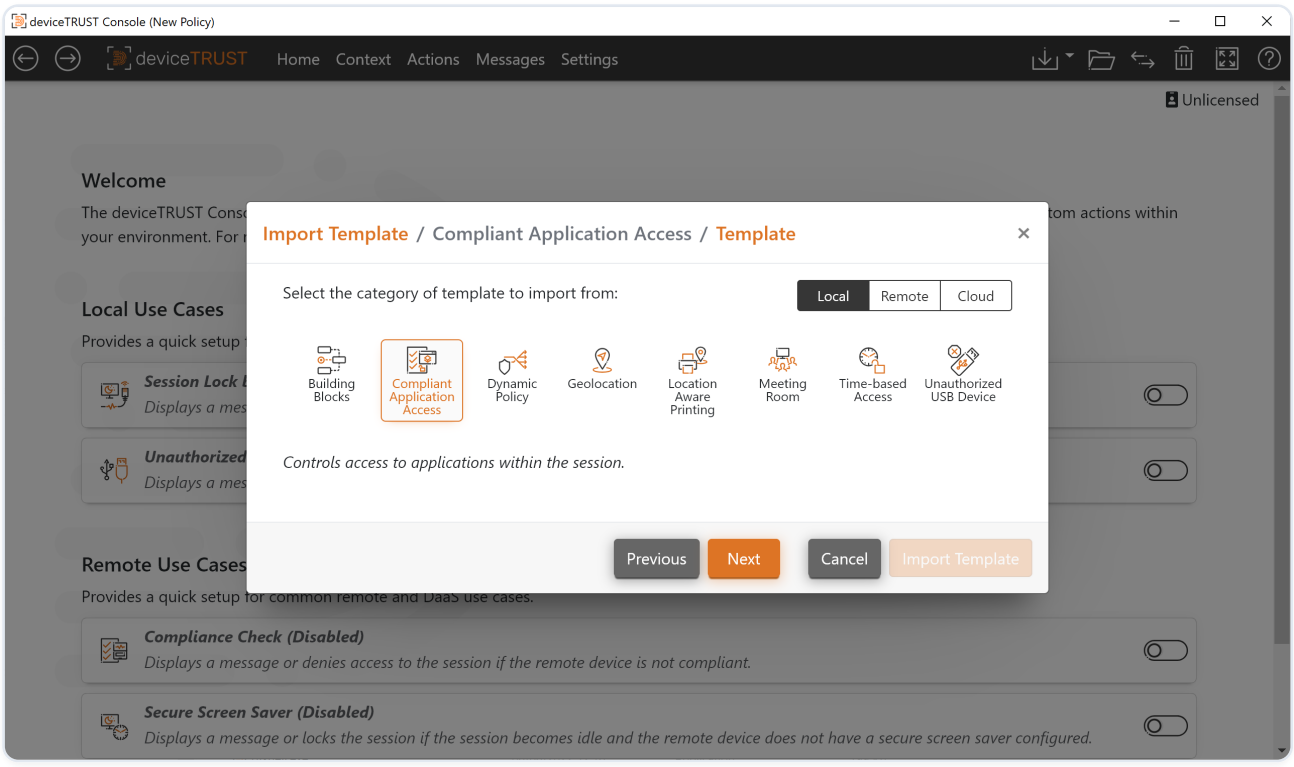
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compliant Application Access Templates

Controls access to applications within the session.



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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Wi-Fi Security Mode - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles%\FSLogix\Apps\Rules\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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks. *Example: %PROGRAMFILES% \Notepad++ \notepad++.exe*

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Working Time Template

This template creates a configuration that checks if the session is accessed outside of working hours. It can be found in the `COMPLIANT APPLICATION 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00`
		Adjust your work hours to fit your requirements.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: notepad++.exe
Working Time - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Corporate Device	Defines if the remote device is a corporate managed device.	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Azure AD 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

© 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*
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

© 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*
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	

© 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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If both actions have been disabled, the contexts will still be created.

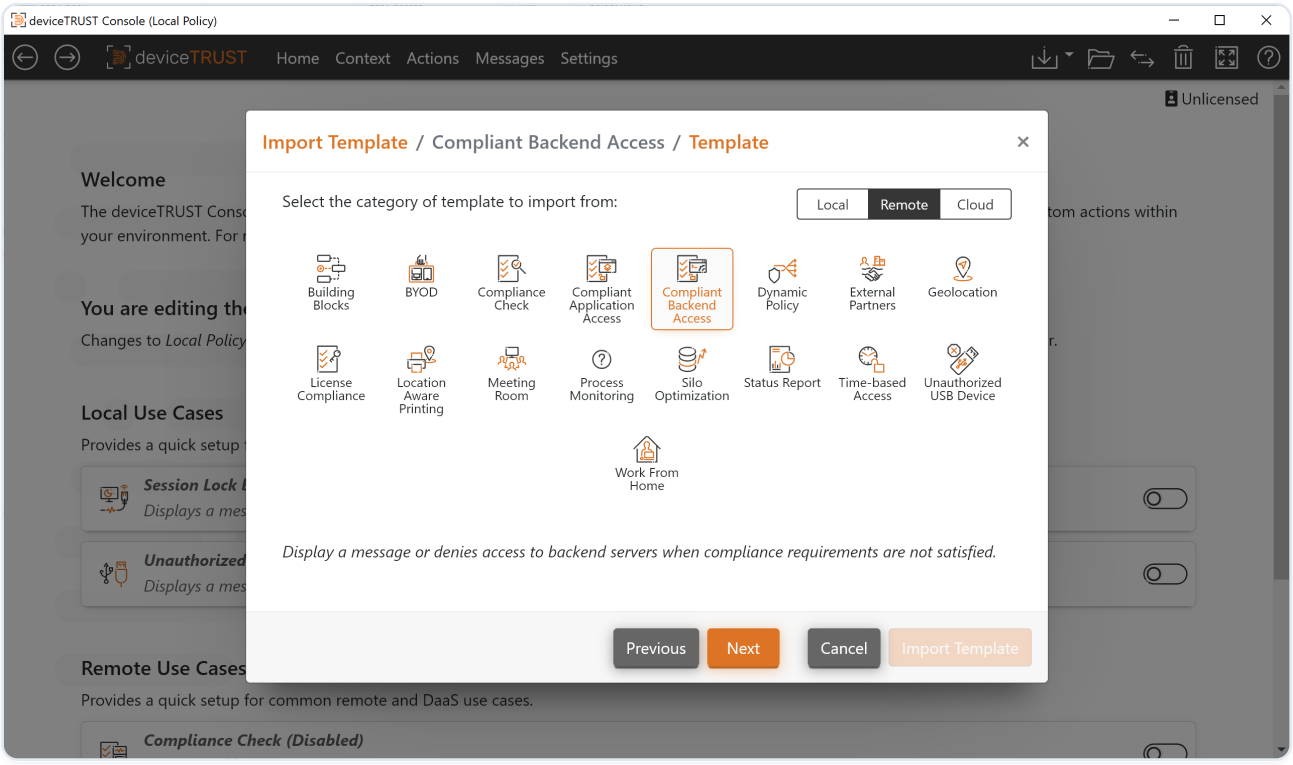
If both actions have been activated, the deny access task will take priority over the displaying of the notification message.
Country codes are based on ISO 3166-1 Alpha-2 code.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Compliant Backend Access Templates

Display a message or denies access to backend servers when compliance requirements are not satisfied.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None

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 - 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Corporate Device	Defines if the remote device is a corporate managed device.	You must update the following context condition with data suitable for your environment
		`REMOTE - DOMAIN ID Any Of 2 ITEMS`
		When using AD or Azure AD domain joined devices, replace DOMAIN_SID and AZURE_TENANT_ID with your corporate values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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_CERTIFICA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		TE_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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
		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 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
		enabled within the task.	

NOTE

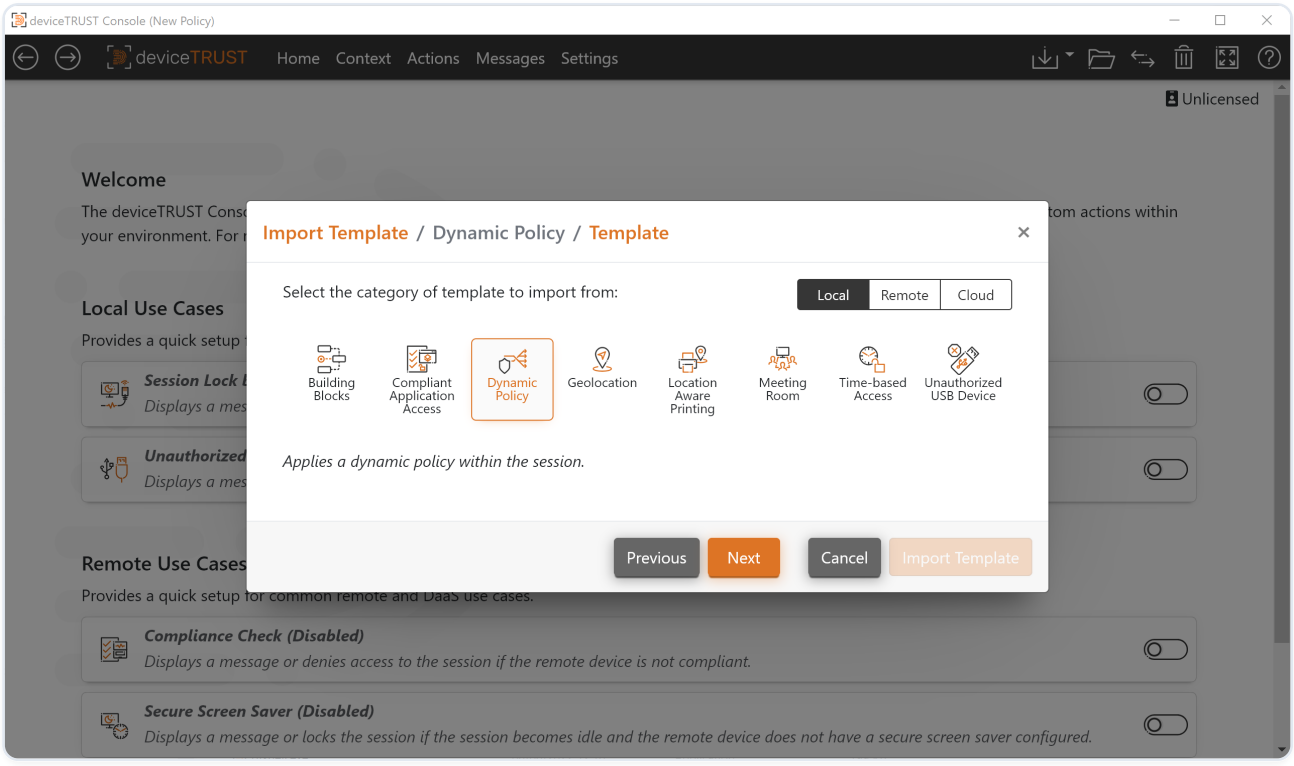
If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Dynamic Policy Templates

Applies a dynamic policy within the session.



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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 Azure AD domain joined devices, replace DOMAIN_SID and AZURE_TENANT_ID with your corporate values.
		Example: S-1-5-21-1397108472-4176295369-1616

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		608269 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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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
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	Displays a message in the session if the	Activated	You must update the following

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
Access - Notification	contractor's device is not compliant.		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 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	the country of the remote device.	
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 Azure AD 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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: 0d57fdd21474ef7806818a661a5f1d1cb33

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		61a8bb4ccd660dae6930a6a135a56
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 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	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
	device is not compliant.		
			`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

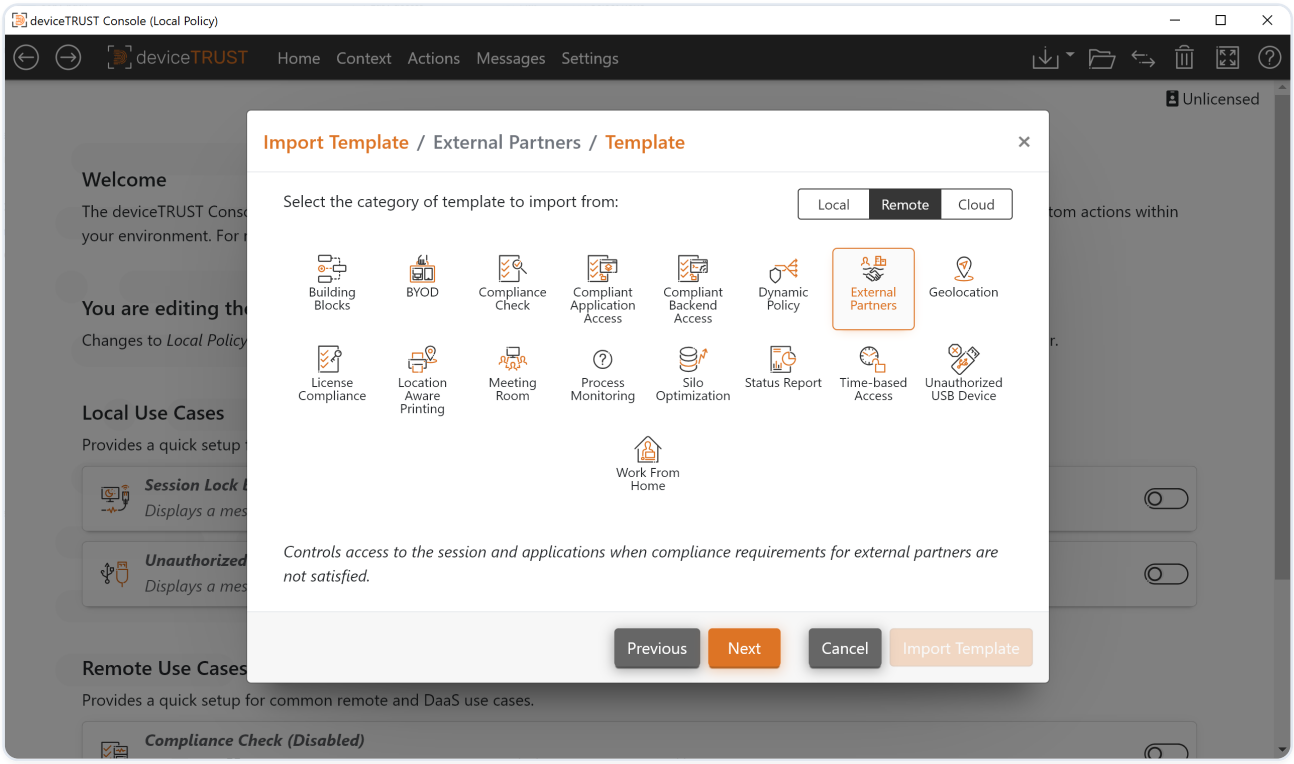
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

External Partners Templates

The external partners templates controls access to the session and applications when compliance requirements for external partners are not satisfied.

© 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: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 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	

© 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	
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.

Conditional Access for Country with Fallback Template

This template creates a configuration that checks the country of the remote device including a fallback to the previous known country within a timeout period. 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: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located. Includes a fallback to the previous known country within a timeout period.	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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

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 -	Hides applications with FSLogix App Masking	Deactivated	You must update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
Enforcement - FSLogix App Masking	within the session based on the country of the remote device.		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\Notepad PlusPlus.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
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

© 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.

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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_PATH_HERE with your target .fxa file path on all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			all Microsoft AppLocker tasks. *Example: %PROGRAMFILES% \Notepad++ \notepad++.exe*

NOTE

If both actions have been disabled, the contexts will still be created.

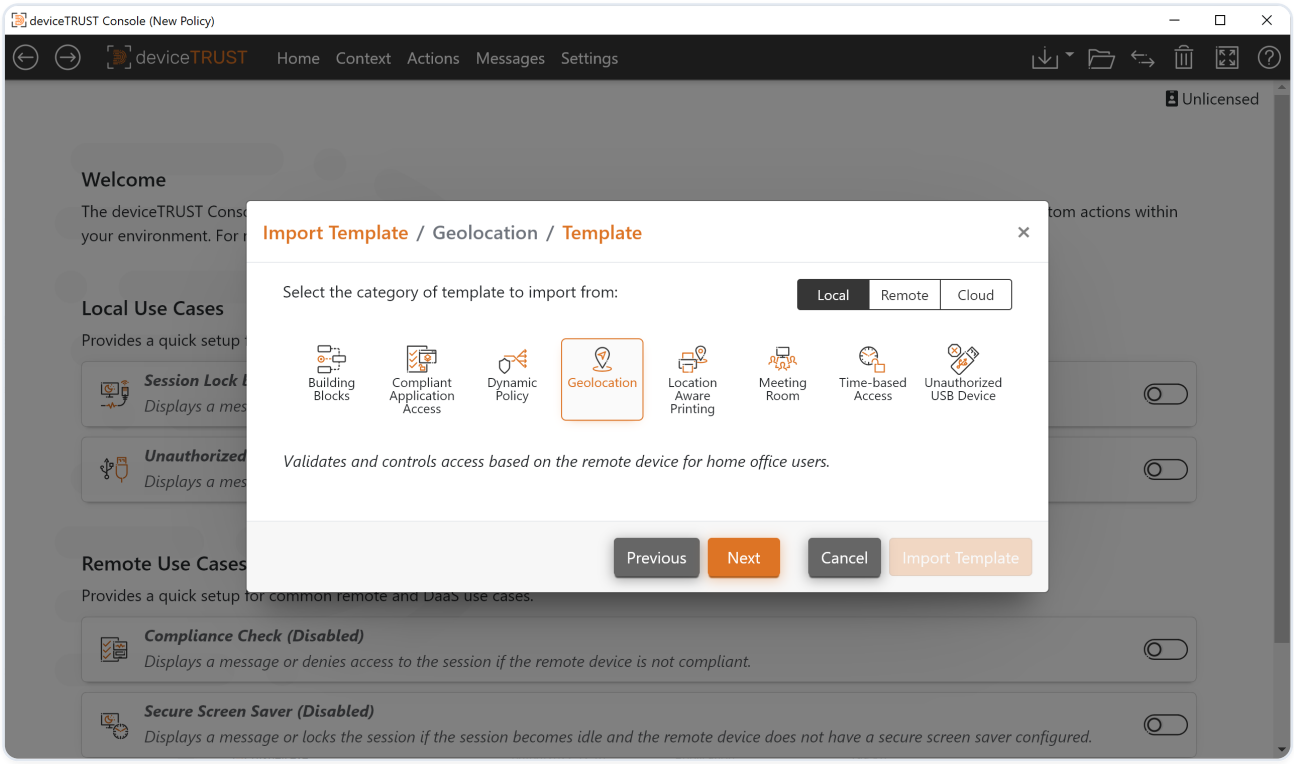
Troubleshooting

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.



Adobe Reader DC Template

This template creates a configuration that checks if the remote device is licensed for Adobe Reader DC. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Adobe Reader DC, you can choose between two actions:

- Hides Adobe Reader DC from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Adobe Reader DC within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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\Adobe Reader DC License Override
Adobe Reader DC User	Defines if the session user is member of the Adobe Reader DC	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	AD application group.	
		`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.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Adobe Reader DC Licensed Device - Conditional Application Access -	Hides Adobe Reader DC from the session with FSLogix App Masking if the	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
FSLogix App Masking	remote device is not licensed.		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\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Adobe Reader DC Licensed Device - Conditional Application	Denies Adobe Reader DC within the session with Microsoft	Deactivated	You must update the following context condition with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Access - Microsoft AppLocker	AppLocker if the remote device is not licensed.		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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 configuration.
			Example: dtldss02.demo.devicetrust.local:9200

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`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.

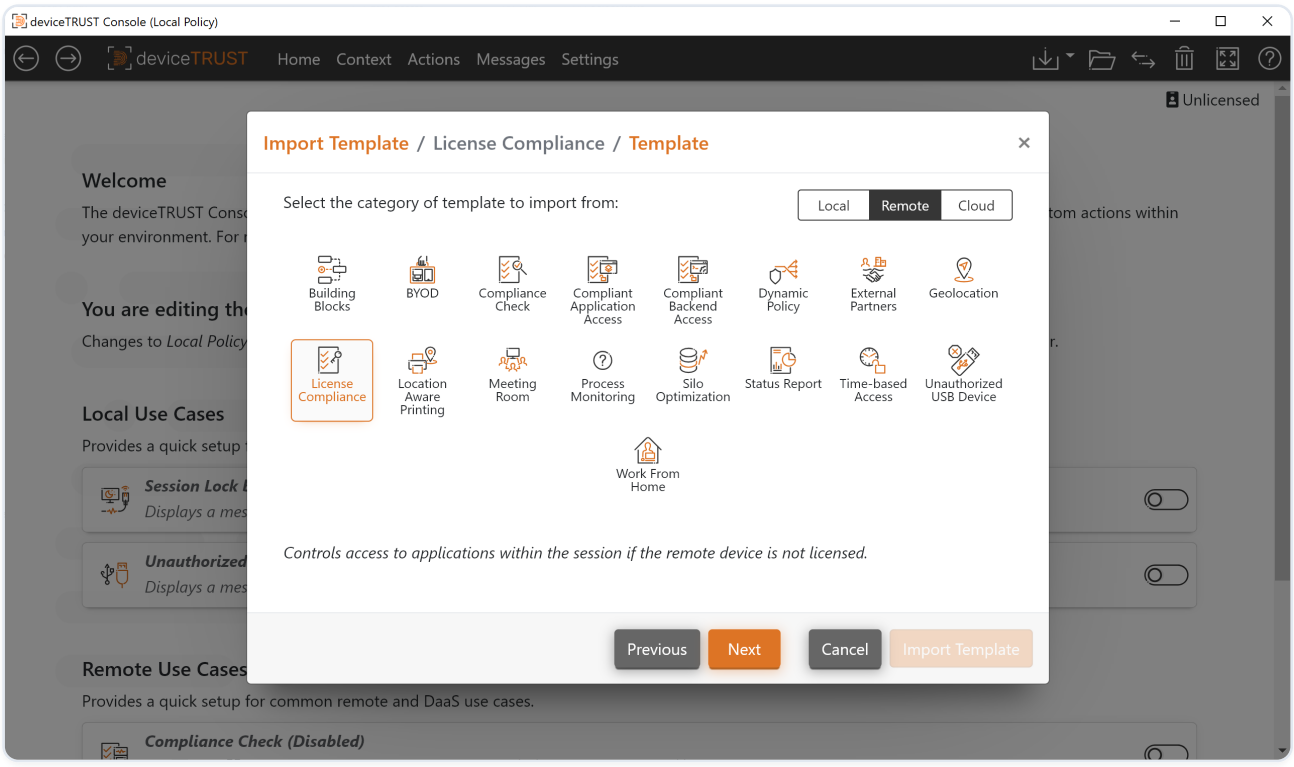
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

License Compliance Templates

Controls access to applications within the session if the remote device is not licensed.



Microsoft Office Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Office. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Office, you can choose between two actions:

- Hides Microsoft Office from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Office 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Office Licensed Status	Defines if the remote device is licensed to use Microsoft Office 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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\Microsoft Office License Override
Microsoft Office User	Defines if the session user is member of the	You must update the following context condition with data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
	Microsoft Office AD application group.	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 Office Licensed Users

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft Office Licensed Device - Conditional Application	Hides Microsoft Office from the session with FSLogix App Masking if the	Deactivated	You must update the following context condition with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Access - FSLogix App Masking	remote device is not licensed.		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\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Microsoft Office Licensed Device - Conditional	Denies Microsoft Office within the session with	Deactivated	You must update the following context

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Application Access - Microsoft AppLocker	Microsoft AppLocker if the remote device is not licensed.		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
Microsoft Office Licensed Device - Conditional Application Access - Reporting	Reports Microsoft Office licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT MICROSOFT OFFICE LICENSED STATUS TO SPLUNK`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 OFFICE LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT MICROSOFT OFFICE 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 Office Licensed Device - Conditional Application Access - Reporting` action can be deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Project Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Project. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Project, you can choose between two actions:

- Hides Microsoft Project from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Project within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Microsoft Project Licensed Status	Defines if the remote device is licensed to use Microsoft Project within the session.	You must update the following context condition with data suitable for your environment	
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`	
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.	
		Example: PF1J8T36	
		`REMOTE - OS ID Any Of 3 ITEMS`	
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.	
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73	
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.	
		Example: DE-SG01	
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`	
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.	
		Example: DEMO\Microsoft Project License Override	
Microsoft Project User	Defines if the session user is member of the Microsoft Project AD application group.	You must update the following context condition with data suitable for your environment	
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`	
		To identify users which are allowed to use the licensed application, replace	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		DOMAIN\GROUP with a security group. *Example: DEMO\Microsoft Project Licensed Users*

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft Project Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Microsoft Project from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			path on all FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Microsoft Project Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Project within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe
Microsoft Project Licensed Device - Conditional Application Access - Reporting	Reports Microsoft Project licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT MICROSOFT PROJECT LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT MICROSOFT PROJECT LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT MICROSOFT PROJECT LICENSED STATUS TO GRAYLOG`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Project Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Visio Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Visio. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Visio Licensed Status	Defines if the remote device is licensed to use Microsoft Visio within the session.	You must update the following context condition with data suitable for your environment
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.	
		Example: DEMO\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_PROCES

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			S_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Microsoft Visio Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe
Microsoft Visio Licensed Device - Conditional Application	Reports Microsoft Visio licensing status.	Activated	You must update the following context condition with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
Access - Reporting			data suitable for your environment	
			`WEB REQUEST REPORT 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`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT MICROSOFT VISIO LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Visio Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Nuance PDF Template

This template creates a configuration that checks if the remote device is licensed for Nuance PDF. It can be found in the `LICENSE COMPLIANCE` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Nuance PDF, you can choose between two actions:

- Hides Nuance PDF from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Nuance PDF within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Nuance PDF Licensed Status	Defines if the remote device is licensed to use Nuance PDF within the session.	You must update the following context condition with data suitable for your environment	
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`	
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.	
		Example: PF1J8T36	
		`REMOTE - OS ID Any Of 3 ITEMS`	
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF Licensed Users

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Nuance PDF Licensed Device - Conditional Application Access -	Denies Nuance PDF within the session with Microsoft AppLocker if the remote	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft AppLocker	device is not licensed.		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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT NUANCE PDF LICENSED STATUS TO ELK STACK`
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT NUANCE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`PDF LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Nuance PDF Licensed Device - Conditional Application Access - Reporting` action can be deleted.

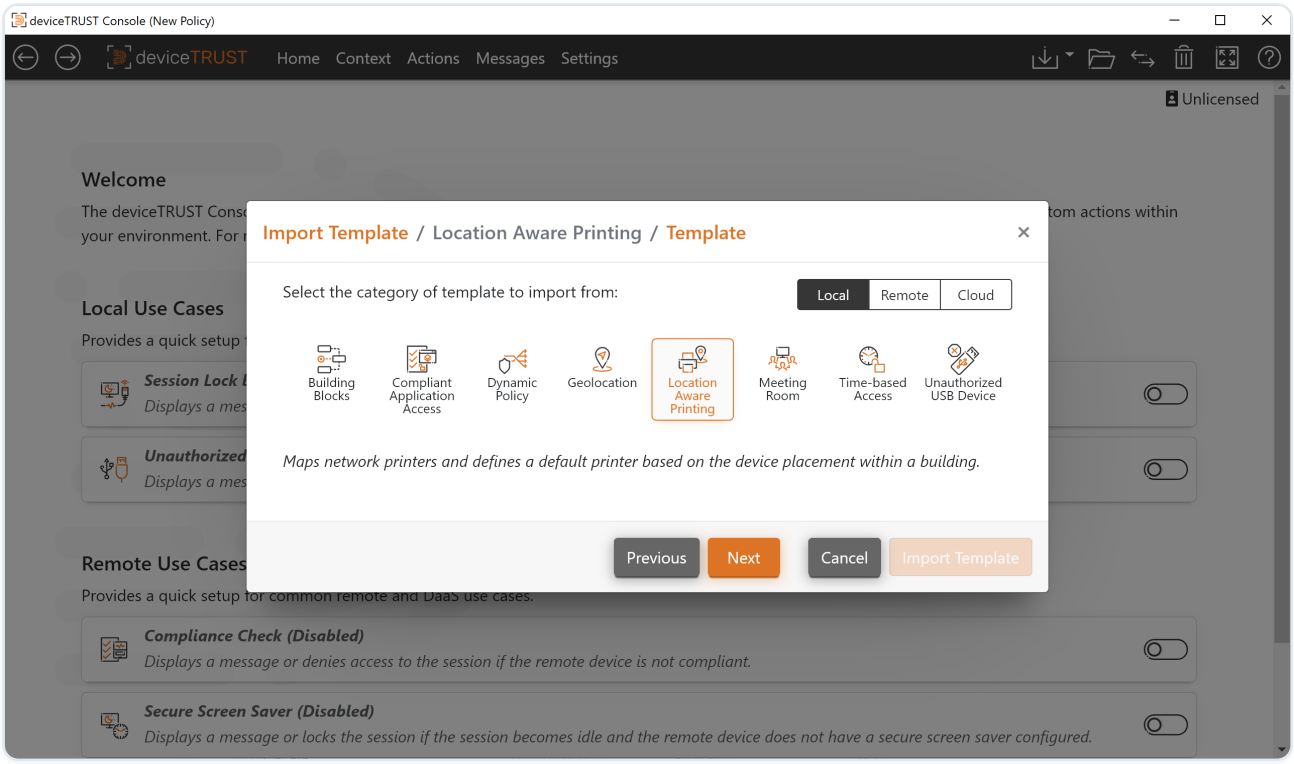
Troubleshooting

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



IP Address Template

This template creates a configuration that maps network printers and defines a default printer based on the location of the remote device using its IP address. It can be found in the `LOCATION AWARE PRINTING` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 - 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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Location	Defines the location of a remote device based on its 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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Custom Values Template

This template creates a configuration that disconnects the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on custom values on the remote device. It can be found in the `MEETING ROOM` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines if the session is idle for remote devices. Differs between meeting rooms and other locations based on custom values.	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	Disconnects the session for remote devices if the session becomes idle.	Activated	None

NOTE

If the action has been disabled, the context will still be created.

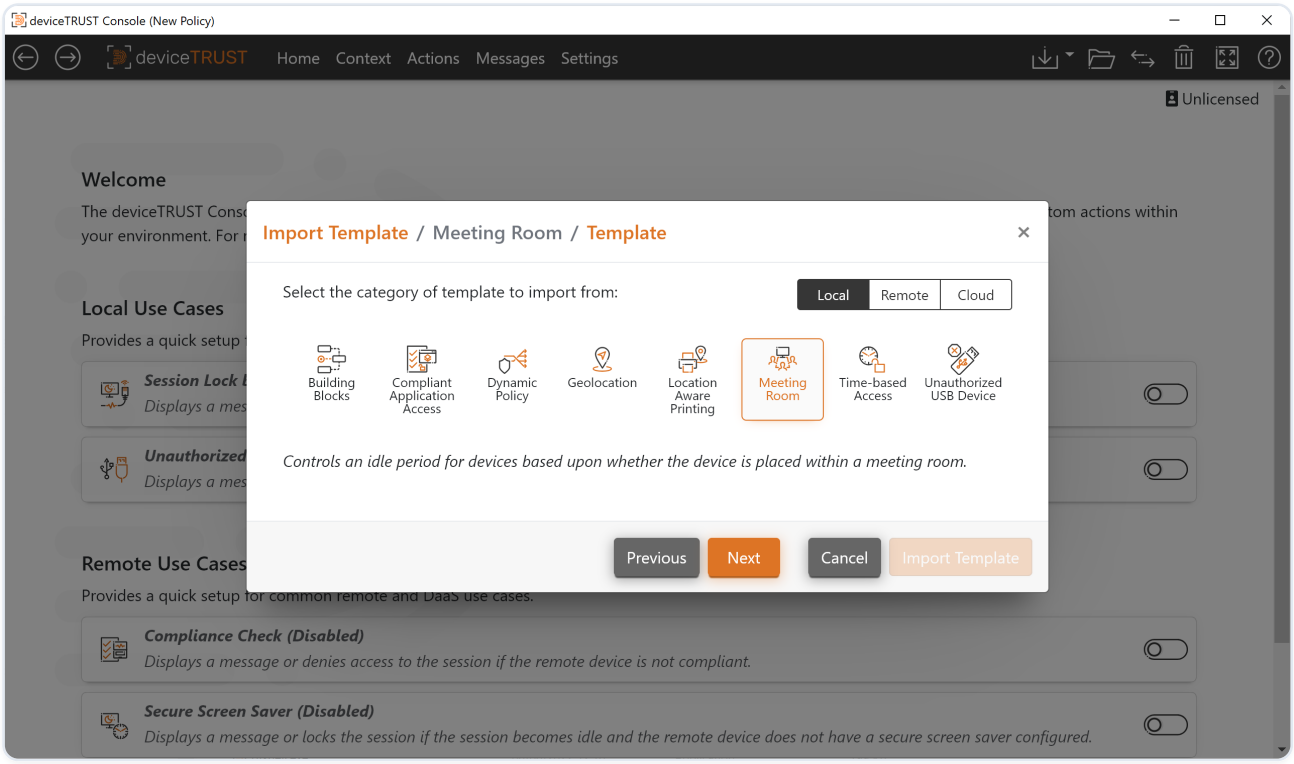
Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Meeting Room Templates

Controls an idle period for devices based upon whether the device is placed within a meeting room.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



IP Address Template

This template creates a configuration that disconnects the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on the IP address of the remote device. It can be found in the `MEETING ROOM` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines if the session is idle for remote devices. Differs between meeting rooms and other locations based on the device's 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 with your meeting room IPv4 range.* *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 controls access to the session. By default, the enforcement action is enabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Session Idle - Conditional Access - Enforcement	Disconnects the session for remote devices if the	Activated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
	session becomes idle.		

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 disconnects the session after an idle period which differs between meeting rooms (30 minutes idle time) and other locations (10 minutes idle time) based on the NetBIOS name of the remote device. It can be found in the `MEETING ROOM` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Session Idle	Defines if the session is idle for remote devices. Differs between meeting rooms and other locations based on the device's NetBIOS name.	You must update the following context condition with data suitable for your environment `REMOTE - NAME NAME Any Of 3 ITEMS` *Replace MEETING_ROOM_DEVICE_NAME_X with your meeting room device name.* *Example: MEETING-ROOM-1*

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	Disconnects the session for remote devices if the session becomes idle.	Activated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

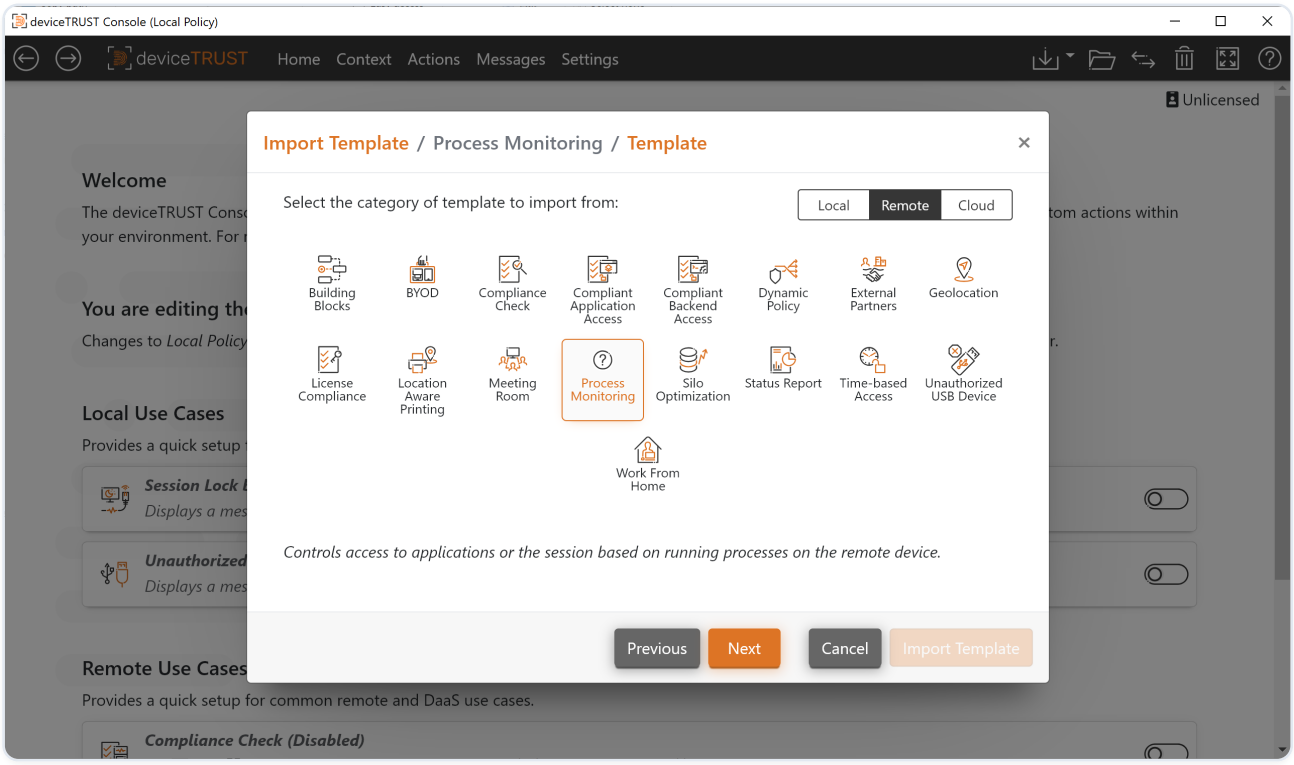
If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Process Monitoring Templates

Controls access to applications or the session based on running processes 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.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Process Monitoring - Microsoft Teams	Defines if Microsoft Teams is running on the remote device. Uses a custom property for evaluation.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Process Monitoring - Microsoft Teams - Conditional Application Access - Enforcement - FSLogix App Masking	Hides Microsoft Teams with FSLogix App Masking within the session if Microsoft Teams is running on the remote device.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.* *Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa*
Process Monitoring - Microsoft Teams - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to Microsoft Teams with Microsoft AppLocker within the session if Microsoft Teams is running on the remote device.	Deactivated	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If the action has been disabled, the context will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
Access Mode	Defines if the remote device is internal or external to the corporate network.	You must update the following context condition with data suitable for your environment	
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Equals *.REMOTING_HOST_DNS_HERE\:3389`	
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389 with your remoting hosts dns suffix.*	
		*Example: *.demo.devicetrust.local:3389*	
		`REMOTE - REMOTING CLIENT OUTBOUND DNS Not Equals *.REMOTING_HOST_DNS_HERE\:3389`	
		*When using Microsoft RDP remoting protocol, replace *.REMOTING_HOST_DNS_HERE:3389*	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		with your remoting hosts dns suffix. *Example: *.demo.devicetrust.local:3389*

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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			FSLogix App Masking tasks.
			Example: %ProgramFiles% \FSLogix\Apps\ Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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\Adobe Reader DC License Override

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			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.	
			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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT ADOBE READER DC LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unnecessary reporting options within the `Adobe Reader DC Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Corporate Device Template

This template creates a configuration that checks if the remote device is a corporate managed device. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not a corporate managed device, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the remote device is not a corporate managed device.
- Denies access to applications with Microsoft AppLocker within the session if the remote device is not a corporate managed device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Azure AD 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	

© 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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 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 App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			process name on all Terminate App tasks. *Example: notepad++.exe*
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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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.

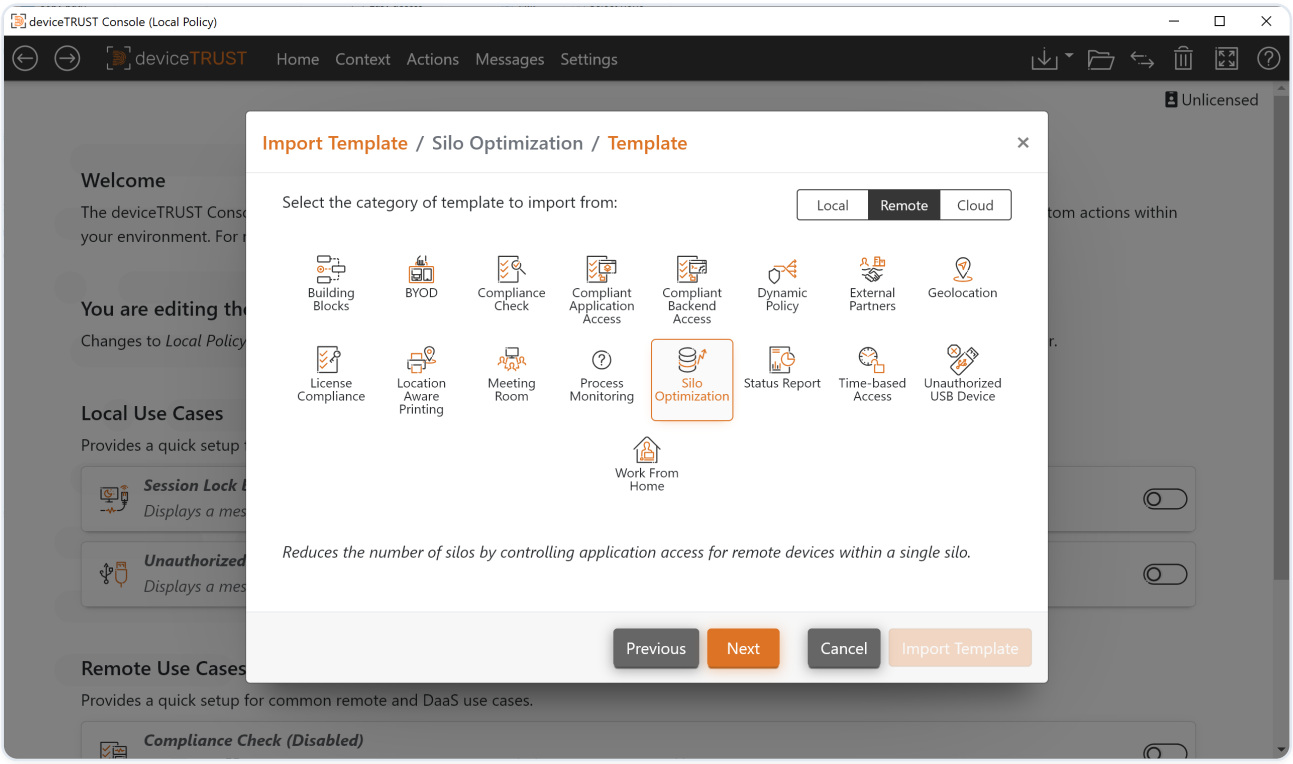
Country codes are based on ISO 3166-1 Alpha-2 code.

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.

Microsoft Office Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Office. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Office, you can choose between two actions:

- Hides Microsoft Office from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Office within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Office Licensed Status	Defines if the remote device is licensed to use Microsoft Office within the session.	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		of your licensed devices.	
		Example: DE-SG01	
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`	
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.	
		Example: DEMO\Microsoft Office License Override	
Microsoft Office User	Defines if the session user is member of the Microsoft Office 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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Office Licensed Users

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft Office Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Microsoft Office from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles% \FSLogix\Apps\Rules\NotepadPlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Microsoft Office Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Office within the session with Microsoft AppLocker if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe
Microsoft Office Licensed Device - Conditional Application Access - Reporting	Reports Microsoft Office licensing status.	Activated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST REPORT MICROSOFT OFFICE LICENSED STATUS TO SPLUNK`
			When using Splunk for license compliance reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: dtldss02.demo.devicetrust.local:8088	
			`WEB REQUEST REPORT MICROSOFT OFFICE LICENSED STATUS TO ELK STACK`	
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.	
			Example: dtldss02.demo.devicetrust.local:9200	
			`WEB REQUEST REPORT MICROSOFT OFFICE LICENSED STATUS TO GRAYLOG`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Office Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Project Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Project. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Project, you can choose between two actions:

- Hides Microsoft Project from the session with FSLogix App Masking if the remote device is not licensed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Denies Microsoft Project within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Microsoft Project Licensed Status	Defines if the remote device is licensed to use Microsoft Project within the session.	You must update the following context condition with data suitable for your environment
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Microsoft Project License Override
Microsoft Project User	Defines if the session user is member of the Microsoft Project 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 Project 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 Project Licensed Device - Conditional Application Access - FSLogix App Masking	Hides Microsoft Project from the session with FSLogix App Masking if the remote device is not licensed.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCES

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			S_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe
Microsoft Project Licensed Device - Conditional Application Access - Microsoft AppLocker	Denies Microsoft Project 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
Microsoft Project Licensed Device - Conditional	Reports Microsoft Project licensing status.	Activated	You must update the following context condition with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
Application Access - Reporting			data suitable for your environment	
			`WEB REQUEST REPORT MICROSOFT PROJECT 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 PROJECT LICENSED STATUS TO ELK STACK`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using ELK Stack for license compliance reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200
			`WEB REQUEST REPORT MICROSOFT PROJECT LICENSED STATUS TO GRAYLOG`
			When using Graylog for license compliance reporting, replace YOUR_GRAYLOG_SERVER:12201 with your Graylog configuration.
			Example: dtldss02.demo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Microsoft Project Licensed Device - Conditional Application Access - Reporting` action can be deleted.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Microsoft Visio Template

This template creates a configuration that checks if the remote device is licensed for Microsoft Visio. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is not licensed for Microsoft Visio, you can choose between two actions:

- Hides Microsoft Visio from the session with FSLogix App Masking if the remote device is not licensed.
- Denies Microsoft Visio within the session with Microsoft AppLocker if the remote device is not licensed.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

© 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	
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.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS	
		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\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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS

			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.
			Example: notepad++.exe

Microsoft Visio Licensed Device - Conditional Application Access -	Denies Microsoft Visio within the session with Microsoft AppLocker if the remote	Deactivated	You must update the following context condition with data suitable for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Microsoft AppLocker	device is not licensed.		your environment
			`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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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 YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Nuance PDF Licensed Status	Defines if the remote device is licensed to use Nuance PDF within the session.	You must update the following context condition with data suitable for your environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`REMOTE - HARDWARE BIOS SERIAL NUMBER Any Of 3 ITEMS`
		When identifying physical devices, replace BIOS_SERIAL_NUMBER_X with BIOS serial numbers of your licensed devices.
		Example: PF1J8T36
		`REMOTE - OS ID Any Of 3 ITEMS`
		When identifying physical devices, replace OS_ID_X with OS ID of your licensed devices.
		Example: 31f75261-7066-485b-9a95-de9b2c7d4b73
		`LOCAL - REMOTE CONTROL REMOTE NAME Any Of 3 ITEMS`
		When identifying physical devices, replace REMOTE_DEVICE_NAME_X with Name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		of your licensed devices.
		Example: DE-SG01
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users who can use any physical device, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF License Override
Nuance PDF User	Defines if the session user is member of the Nuance PDF AD application group.	You must update the following context condition with data suitable for your environment
		`LOCAL - USER GROUPS Is Member Of Any DOMAIN\GROUP`
		To identify users which are allowed to use the licensed application, replace DOMAIN\GROUP with a security group.
		Example: DEMO\Nuance PDF Licensed Users

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled. In addition, an active report action with various report options has been added too.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
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%	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			\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 your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088
			`WEB REQUEST REPORT NUANCE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: dtldss02.demo.devicetrust.local:12201

NOTE

If all actions have been disabled, the contexts will still be created.

Unnecessary reporting options within the `Nuance PDF Licensed Device - Conditional Application Access - Reporting` action can be deleted.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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.

© 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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			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.

Wi-Fi Security Mode Template

This template creates a configuration that checks if the remote device is connected to an insecure Wi-Fi network. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the remote device is connected to an insecure Wi-Fi network, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session if the remote device is connected to an insecure Wi-Fi network.
- Denies access to applications with Microsoft AppLocker within the session if the remote device is connected to an insecure Wi-Fi network.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Wi-Fi Security Mode - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	You must update the following context condition with data suitable for your environment `FSLOGIX APP MASKING` *Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles%\FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
Wi-Fi Security Mode - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session if the remote device is connected to an insecure Wi-Fi network.	Deactivated	You must update the following context condition with data suitable for your environment	
			`MICROSOFT APPLOCKER`	
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Working Time Template

This template creates a configuration that checks if the session is accessed outside of working hours. It can be found in the `SILO OPTIMIZATION` category when filtered for `REMOTE` platform.

If the session is accessed outside of working hours, you can choose between two actions:

- Hides applications with FSLogix App Masking within the session when accessed outside of working time.
- Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00`
		Adjust your work hours to fit your requirements.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.
			Example: %ProgramFiles%\FSLogix\Apps\Rules\NotepadPlusPlus.fxa
			`TERMINATE APP`
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Example: notepad++.exe
Working Time - Conditional Application Access - Enforcement - Microsoft AppLocker	Denies access to applications with Microsoft AppLocker within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`MICROSOFT APPLOCKER`
			Replace ENTER_YOUR_PATH_HERE with your target configuration on all Microsoft AppLocker tasks.
			Example: %PROGRAMFILES% \Notepad++ \notepad++.exe

NOTE

If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application Log Template

This template creates a configuration that reports the status of the remote device to the Windows application log. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Application Log	Reports the status of the remote device to the Windows application log.	Deactivated	None

NOTE

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

ELK Stack Template

This template creates a configuration that reports the status of the remote device to ELK Stack. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - ELK Stack	Reports the status of the remote device to ELK Stack.	Deactivated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST STATUS REPORT`
			When using ELK Stack for status reporting, replace YOUR_ELKSTACK_SERVER:9200 with your ELK Stack configuration.
			Example: dtldss02.demo.devicetrust.local:9200

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Email Template

This template creates a configuration that reports the status of the remote device by email. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Email	Send the status of the remote device by email.	Deactivated	None

NOTE

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Graylog Template

This template creates a configuration that reports the status of the remote device to Graylog. It can be found in the `STATUS REPORT` category when filtered for `REMOTE` platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Country Provider	Defines the country provider that reports the country of the remote device.	None
Device Identifier	Defines the device identifier of the remote device.	None
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Name	Defines the operating system name of the remote device.	None
Operating System Platform	Defines the operating system platform of the remote device.	None
Operating System Release	Defines the operating system release of the remote device.	None
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Remoting Client Version	Defines the version of the remoting client installed on the remote device.	None
Secure Screen Saver	Defines whether the remote device is using a secure screen saver.	None
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template contains an active reporting action that submits the status of the remote device to the appropriate source.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Status Report - Graylog	Reports the status of the remote device to Graylog.	Deactivated	You must update the following context condition with data suitable for your environment
			`WEB REQUEST STATUS REPORT`
			When using Graylog for status 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

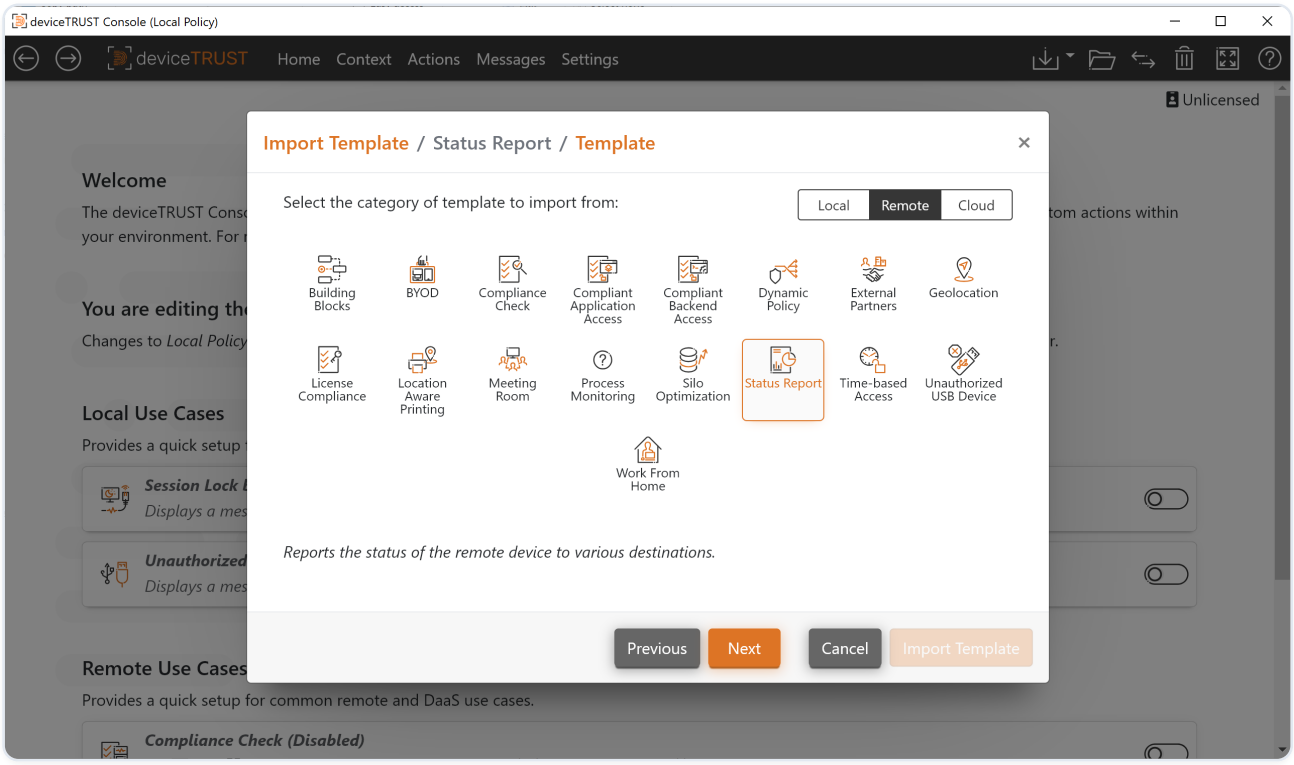
If the action have been disabled, the contexts will still be created.

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.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	None
Antivirus Name	Defines the available antivirus product used on the remote device.	None
Antivirus Signature Status	Defines the signature status of the active antivirus product used on the remote device.	None
Antivirus Status	Defines the status of the active antivirus product used on the remote device.	None
Country	Defines the country in which the remote device is located.	None
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Device Type	Defines the device type of the remote device.	None
deviceTRUST Client	Defines the availability of the deviceTRUST Client Extension on the remote device.	None
Economic Region	Defines the economic region the remote device is located within.	None
Firewall Name	Defines the available firewall product used on the remote device.	None
Firewall Status	Defines the status of the active firewall product used on the remote device.	None
Hardware Bios Release Date	Defines the hardware BIOS release date of the remote device.	None
Hardware Model	Defines the hardware model of the remote device.	None
Hardware Role	Defines the hardware role of the remote device.	None
Hardware Secure Boot	Defines the hardware secure boot of the remote device.	None
Hardware Vendor	Defines the hardware vendor of the remote device.	None
Network Address Assignment	Defines the network address assignment of the remote device.	None

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Network DHCP Server	Defines the network DHCP server of the remote device.	None
Network DNS Server	Defines the network DNS server of the remote device.	None
Network DNS Suffix	Defines the network DNS suffix of the remote device.	None
Network Gateway	Defines the network gateway of the remote device.	None
Network Gateway MAC	Defines the network gateway mac address of the remote device.	None
Network IP Address	Defines the network ip address of the remote device.	None
Network MAC Address	Defines the network MAC address of the remote device.	None
Network Subnet	Defines the network subnet of the remote device.	None
Operating System Description	Defines the operating system description of the remote device.	None
Operating System Disk Encryption	Defines the operating system disk encryption of the remote device.	None
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Operating System Type	Defines the operating system type of the remote device.	None
Operating System Updates	Defines if a recent update search has been performed and that all updates have been installed on the remote device.	None
Operating System Version	Defines the operating system version of the remote device.	None
Override	Defines if the session user is member of the override AD group.	You can add one or more user groups from your Microsoft Active Directory (AD) to exclude group members from actions.
Region Keyboard Locale	Defines the region keyboard locale of the remote device.	None
Region Locale	Defines the region locale of the remote device.	None
Region Timezone Offset	Defines the region timezone offset of the remote device.	None
Remote Controlled	Defines if the remote device is remote controlled.	None
Remoting Client Protocol	Defines the remoting protocol used for the session.	None
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Security State	Defines the security status of the remote device.	None
Session User Domain	Defines the user domain of the user account used within the session.	None
Session User Name	Defines the user name of the user account used within the session.	None
User Authentication	Defines the authentication of the user account used on the remote device.	None
User Privileges	Defines the privileges of the user logged into the remote device.	None
Virtualized	Defines if the remote device is virtualized.	None
VPN Connected	Defines if a network adapter of the remote device is connected to a VPN network.	None
Wi-Fi Security Mode	Defines if the remote device is connected to a secure Wi-Fi network.	None

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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			When using Splunk for status reporting, replace YOUR_SPLUNK_SERVER:8088 and YOUR_SPLUNK_AUTH_TOKEN with your Splunk configuration.
			Example: dtldss02.demo.devicetrust.local:8088

NOTE

If the action have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
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 a notifying action that displays a message to the user about a context status and an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Access - Enforcement	Denies access to the session if the remote BYOD is not compliant.	Deactivated	None
Working Time - Conditional Access - Notification	Displays a message in the session when accessed outside working time.	Activated	None

NOTE

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

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.

© 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: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Working Time	Defines if the current time is within the working time.	You must update the following context condition with data suitable for your environment
		`LOCAL - SESSION TIME Time Of Day EVERYDAY BETWEEN 08:00 AND 18:00`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		Adjust your work hours to fit your requirements.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes an FSLogix App Masking and a Microsoft AppLocker enforcement action that actively controls access to applications, depending on the technology available. By default both actions are disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Working Time - Conditional Application Access - Enforcement - FSLogix App Masking	Hides applications with FSLogix App Masking within the session when accessed outside of working time.	Deactivated	You must update the following context condition with data suitable for your environment
			`FSLOGIX APP MASKING`
			Replace ENTER_YOUR_FXA_PATH_HERE with your target .fxa file path on all FSLogix App Masking tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS	
			Example: %ProgramFiles% \FSLogix\Apps\Rules\Notepad PlusPlus.fxa	
			`TERMINATE APP`	
			Replace ADD_PROCESS_NAME_X with your target process name on all Terminate App tasks.	
			Example: notepad++.exe	
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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			AppLocker tasks. *Example: %PROGRAMFILES% \Notepad++ \notepad++.exe*

NOTE

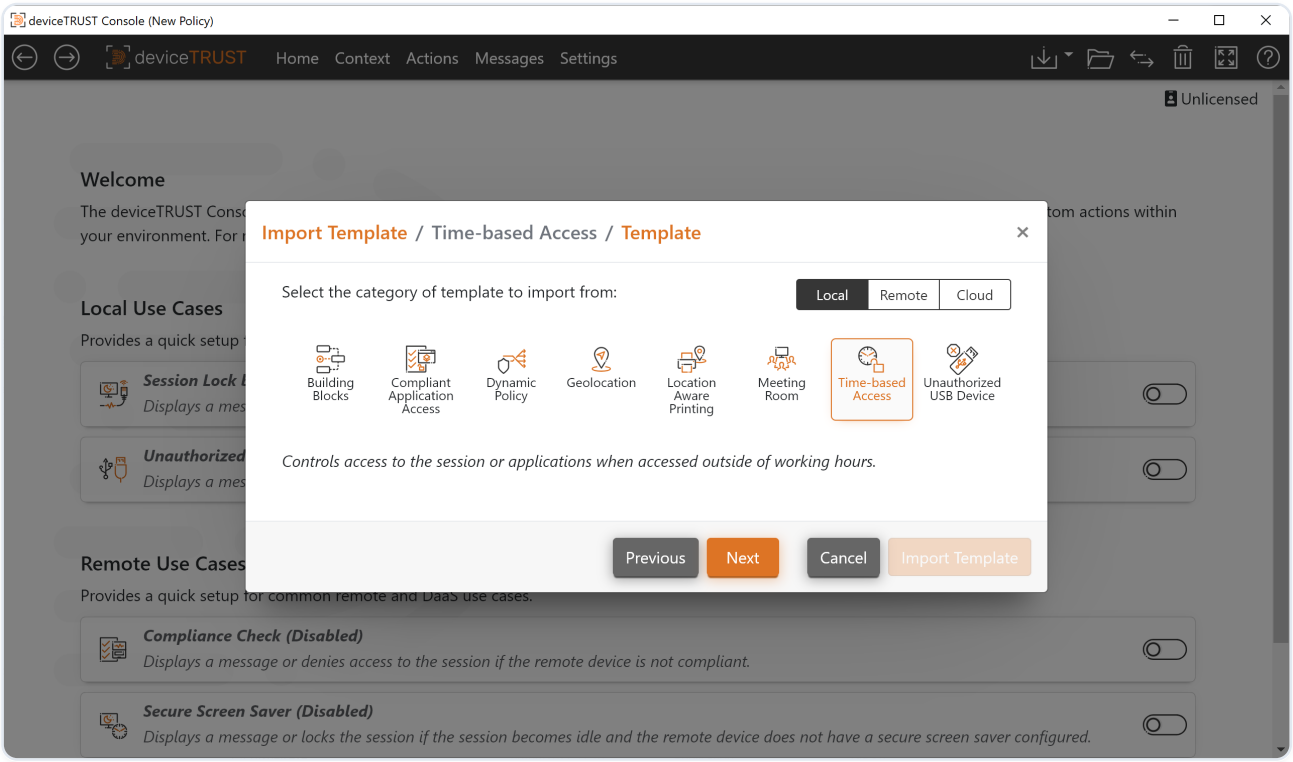
If both actions have been disabled, the contexts will still be created.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Time-based Access Templates

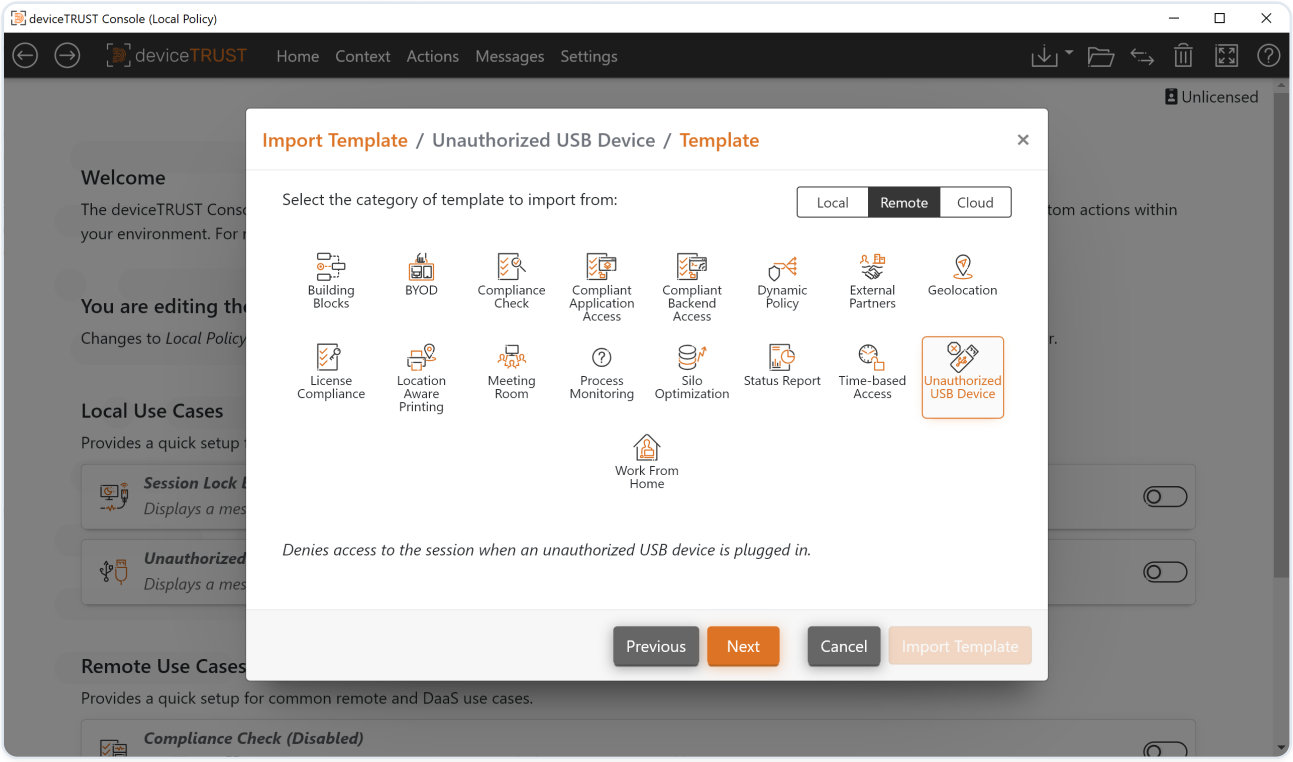
Controls access to the session or applications when accessed outside of working hours.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unauthorized USB Device Templates

Denies access to the session when an unauthorized USB device is plugged in.



Unauthorized USB Device Template

This template creates a configuration that checks if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device. It can be found in the `UNAUTHORIZED USB DEVICE` category when filtered for `REMOTE` platform.

If an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device, you can choose between two actions:

- Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.
- Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Unauthorized USB Device	Defines if an unauthorized USB device, such as a Stick, Camera or Mobile Phone, is plugged into the remote device.	You must update the following context condition with data suitable for your environment
		`REMOTE - LOGICAL DISK IDENTITY Not Equals 0x000,0x000,ABC123456`
		When checking for unauthorized USB devices, add all of your authorized USB devices by Vendor ID (VID), Product ID (PID) and / or Serial Number.
		Example: 0x0781,0x5567,4C530000110526106001 SanDisk Cruzer Blade USB Device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If a context is not needed, it can be deactivated or deleted. In addition, the corresponding task sequence within the relevant action must be deleted too.

Step 3: Actions

The template includes a notifying action that displays a message to the user about a context status and an enforcement action that actively controls access to the session. By default, only the notifying action is enabled and the enforcement action is disabled.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
Unauthorized USB Device Enforcement	Denies access to the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.	Deactivated	None
Unauthorized USB Device Notification	Displays a message in the session if an unauthorized USB device (Stick, Camera and Mobile Phone) is plugged into the remote device.	Activated	None

NOTE

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your deviceTRUST installation or configuration does not work as expected, you can use the Troubleshooting guide to start troubleshooting.

Unauthorized USB Storage Device Template

This template creates a configuration that checks if an an unauthorized USB storage device 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 storage device is plugged into the remote device, you can choose between two actions:

- Denies access to the session if an unauthorized USB storage device is plugged into the remote device.
- Displays a message in the session if an unauthorized USB storage device is plugged into the remote device.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

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
Unauthorized USB Storage Device	Defines if an unauthorized USB storage device is plugged into the remote device.	You must update the following context condition with data suitable for your environment
		`REMOTE - LOGICAL DISK IDENTITY Not Equals 0x000,0x000,ABC123456`
		When checking for unauthorized USB devices, add all of your authorized USB devices by Vendor ID (VID), Product ID (PID) and / or Serial Number.
		Example: 0x0781,0x5567,4C530000110526106001 SanDisk Cruzer Blade USB Device.

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
Unauthorized USB Storage Device Enforcement	Denies access to the session if an unauthorized USB storage device is plugged into the remote device.	Deactivated	None
Unauthorized USB Storage Device Notification	Displays a message in the session if an unauthorized USB storage device is plugged into the remote device.	Activated	None

NOTE

If both actions have been disabled, the contexts will still be created.

If both actions have been activated, the deny access task will take priority over the displaying of the notification message.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deviceTRUST® requires some simple but essential configuration steps to be performed to enable the template for your remoting and DaaS environments. We will guide you step-by-step through simple deviceTRUST configuration steps to enable the template within your remoting or DaaS environment.

We will perform the following steps:

- Step 1: Prerequisites
- Step 2: Context
- Step 3: Actions

Step 1: Prerequisites

If the required deviceTRUST components (Agent, Console, Client Extension and License) are not yet installed, please visit the Getting Started for Remote guide and complete step 1 to 5 and then continue here with step 2 below.

Step 2: Contexts

The template has imported the following contexts:

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
Access Mode	Defines if the remote device is internal or external to the corporate network.	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*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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
Detected Home Office	Defines the detected home office of the users 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
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTEXT	DESCRIPTION	CUSTOMIZATIONS
		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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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,...`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	DEFAULT STATE	CUSTOMIZATIONS
			Replace AUTHORIZED_COUNTRY_X with your authorized countries using the ISO 3166-1 Alpha-2 code. *Example: US*
Home Office Validation - Conditional Access - Enforcement	Validates the home office context and controls session access for external remoting devices.	Deactivated	None

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.

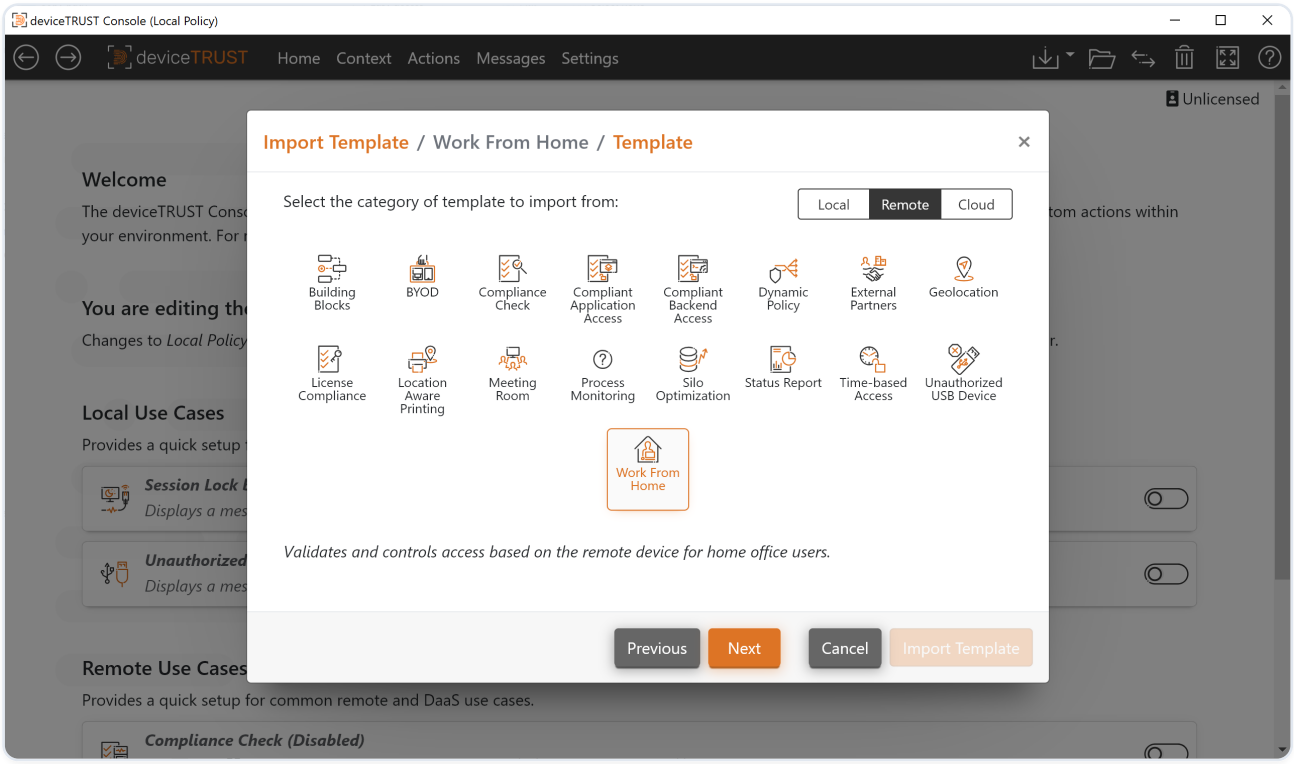
Troubleshooting

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.