deviceTRUST 23.1

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

Contents

Welcome 4

Architecture 4

Local Scenario 5

Remote Scenario 6

Operating System Compatibility 7

Platform Compatibility 11

Getting Started 14

Getting Started for Local 14

Getting Started for Remote 22

Download deviceTRUST 23.1 for Windows 34

Installation 35

Installing the deviceTRUST® Agent 36

Installing the deviceTRUST® Console 39

Installing the deviceTRUST® Client Extension 41

Templates 42

Local Templates 43

Remote Templates 44

SaaS Templates 46

Compliance Check 47

Reporting 48

Splunk Dashboards 48

ELK Stack Dashboards 68

Reference 98

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

Properties 98

Agent Reference 99

Client Extension Reference 100

Console Reference 100

Troubleshooting 100

Knowledge Base 101

General 101

Configuration 102

Connectivity 102

Diagnostics 102

Installation 102

Licensing 103

Support 103

Compatibility 103

Properties 103

Reporting 103

Features 104

Releases 104

TABLE OF CONTENTS 104

IGEL OS 11 Client Extension 23.1.400 104

IGEL OS 12 Client Extension 23.1.400 105

iOS Client Extension 23.1.400 107

macOS Client Extension 23.1.410 109

Stratodesk NoTouch OS Client Extension 23.1.100 111

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

Ubuntu Client Extension 23.1.400 **113**

deviceTRUST 23.1.410 **113**

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

Welcome

September 6, 2025

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

Quick setup

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

More information

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

Architecture

July 23, 2025

- Local Scenario
- Remote Scenario
- OS Compatibility

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

- Platform Compatibility

Local Scenario

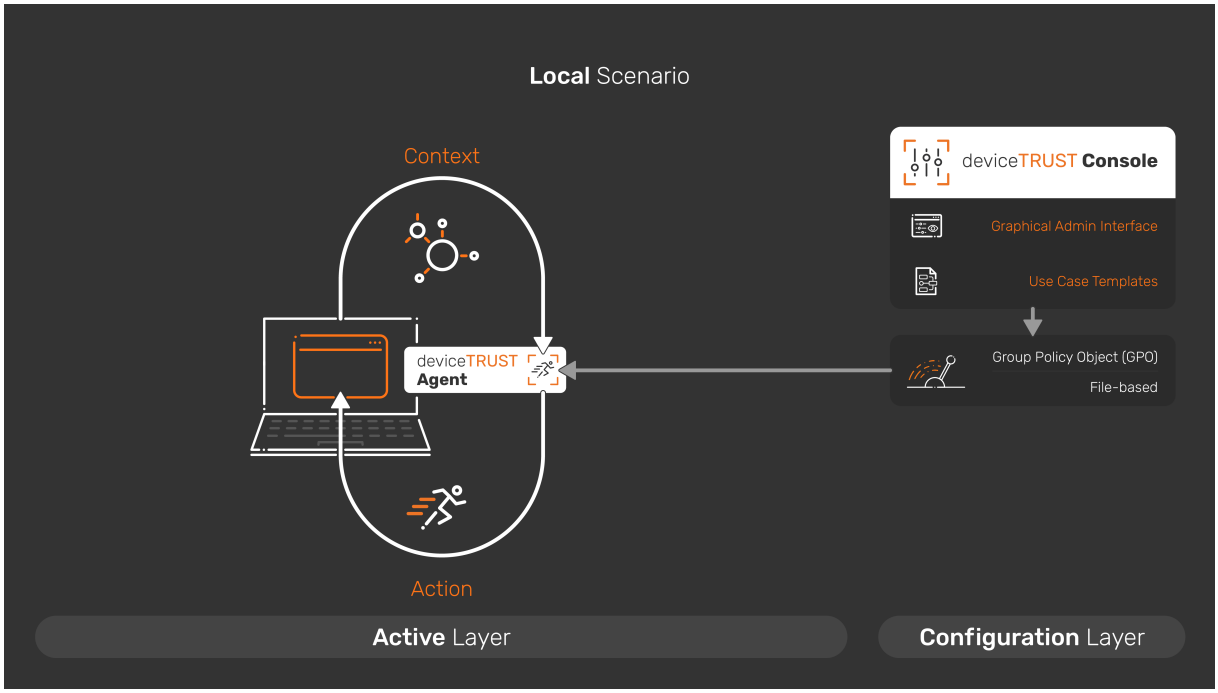
deviceTRUST requires only one main component when installing on local devices, the deviceTRUST Agent. The deviceTRUST component can be installed and configured within minutes and can be fully integrated with existing deployment processes and management tools. No additional infrastructure (e.g. a database 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.

deviceTRUST Client Extension

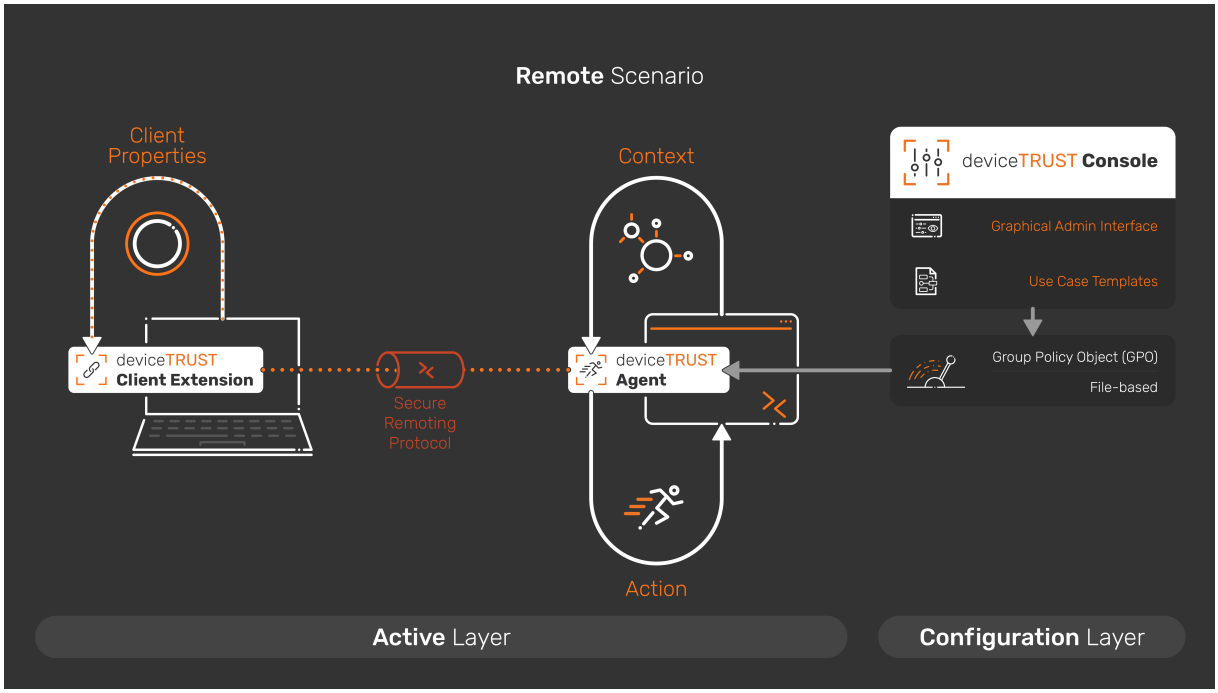
This component needs to be installed on the remote device which will be used to connect to the remote host delivering the published applications and desktops. It is not required to have deviceTRUST Client Extension installed onto all of your remote devices but recommended to get the full range of context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

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



Operating System Compatibility

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

Apple iOS and iPadOS

Compatible operating systems (deviceTRUST® Client Extension):

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

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

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

> **Note:**
>
> iOS 17 support requires deviceTRUST Agent 23.1.200 or later, and deviceTRUST Client Extension for iOS 23.1.200 or later.

Apple macOS

Compatible operating systems (deviceTRUST Client Extension):

- Apple macOS 10.15 and later

Compatible technologies:

- Amazon AppStream
- Amazon WorkSpaces (PCoIP) $_{1}$
- Amazon WorkSpaces (WSP) $_{2}$
- Citrix Virtual Apps™ and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services (via FreeRDP 2)
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

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

IGEL OS 10 and 11

Compatible technologies (deviceTRUST Client Extension):

- Amazon WorkSpaces (PCoIP) natively integrated in IGEL OS 11.08.200 and later {1}
- Citrix Virtual Apps and Desktops natively integrated in IGEL OS 10.03.500 and later
- Citrix Cloud natively integrated in IGEL OS 10.03.500 and later

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

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

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

IGEL OS 12

Compatible technologies (deviceTRUST Client Extension):

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

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

Microsoft Windows

Compatible operating systems (deviceTRUST Agent and Console):

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

Compatible operating systems (deviceTRUST Client Extension):

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

Compatible technologies:

- Amazon AppStream
- Amazon WorkSpaces (PCoIP)
- Amazon WorkSpaces (WSP) {1}
- Azure Virtual Desktop
- Azure Active Directory

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

- Citrix Virtual Apps and Desktops
- Citrix Cloud
- Microsoft Remote Desktop Services
- Nice DCV Standalone
- Parallels Remote Application Server
- VMware Horizon View (Blast)
- VMware Horizon View (PCoIP)
- VMware Horizon View (RDP)

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

Stratodesk NoTouch

Compatible technologies (deviceTRUST Client Extension):

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

Ubuntu Desktop

Compatible operating systems (deviceTRUST Client Extension):

- Ubuntu Desktop 18.04 LTS and later

Compatible technologies:

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

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

Unicon™ eLux

Compatible technologies (deviceTRUST Client Extension):

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

Platform Compatibility

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

Amazon Web Services

Compatible technologies:

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

Compatible operating systems:

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

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

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

> be found in our Enabling DCV extensions on Amazon WorkSpaces WSP

Citrix Systems

Compatible technologies:

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

Compatible operating systems:

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

> **Note:**
>
> {1} Compatibility with HTML5 delivered apps and desktops is not yet available.

Microsoft

Compatible technologies:

- Microsoft Remote Desktop Services
- Azure Virtual Desktop {1}
- Azure Active Directory {2}

Compatible operating systems:

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

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

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

Parallels

Compatible technologies:

- Parallels Remote Application Server

Compatible operating systems:

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

VMware

Compatible technologis:

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

Compatible operating systems:

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

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

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

Getting Started

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

Scenario: Remote

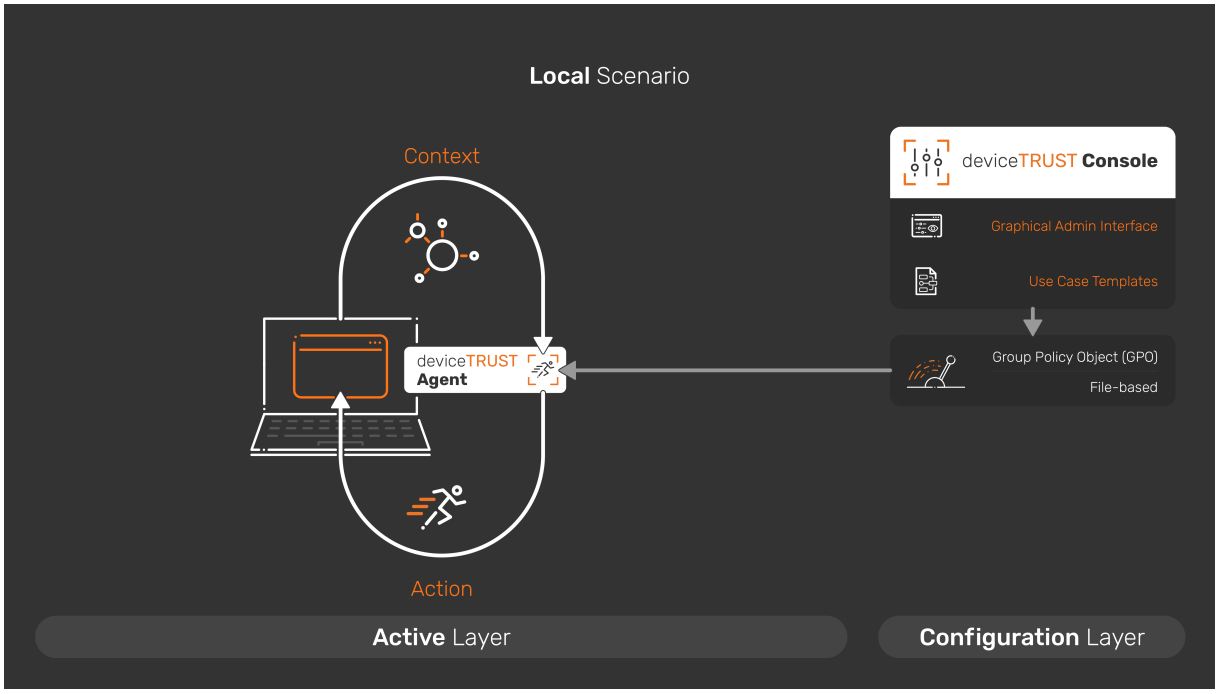
In remote scenarios, deviceTRUST transports the context information from the users remote device into the virtual session where the configuration is enforced. Please visit Getting Started for Remote Devices to begin the guide.

Scenario: Local

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

Getting Started for Local

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



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

We will perform the following steps:

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

Step 1: Download the deviceTRUST setup binaries

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

Step 2: Install the deviceTRUST Agent

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

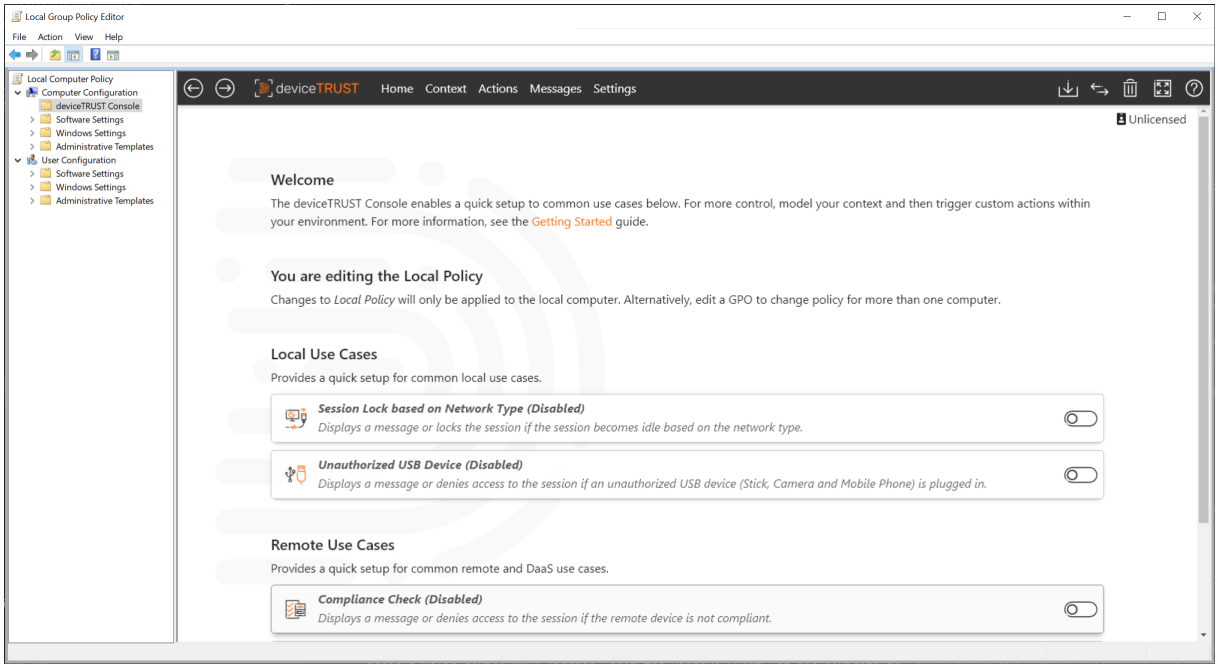
Step 3: Install the deviceTRUST Console

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

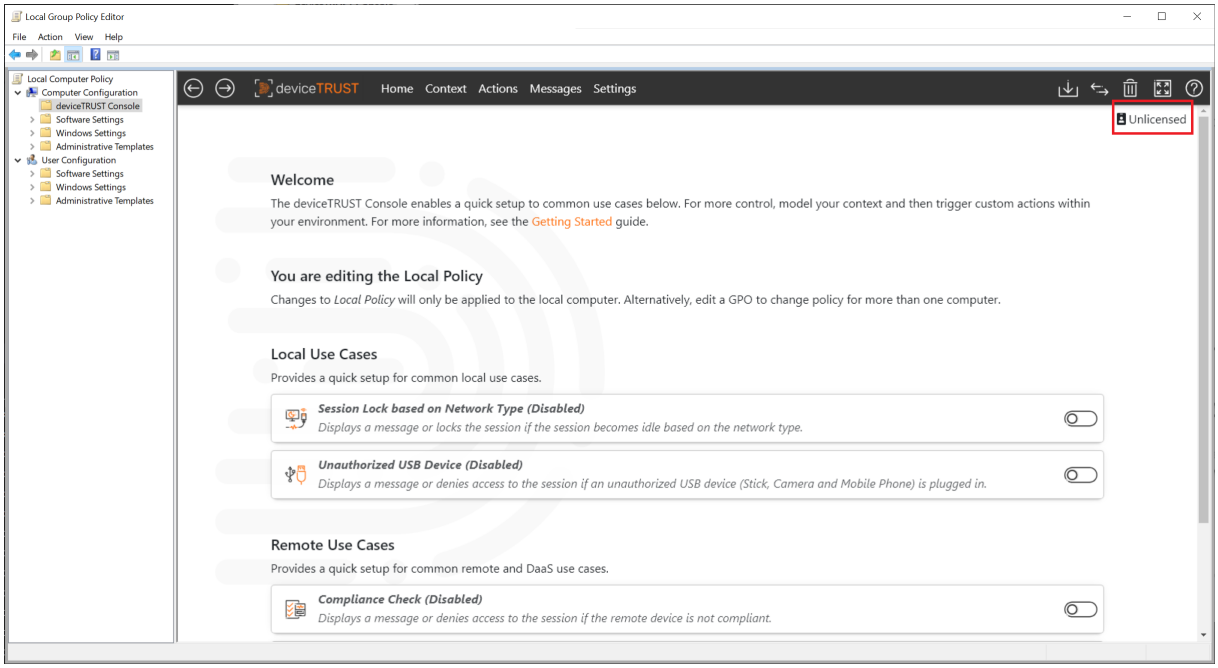
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION \DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.

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



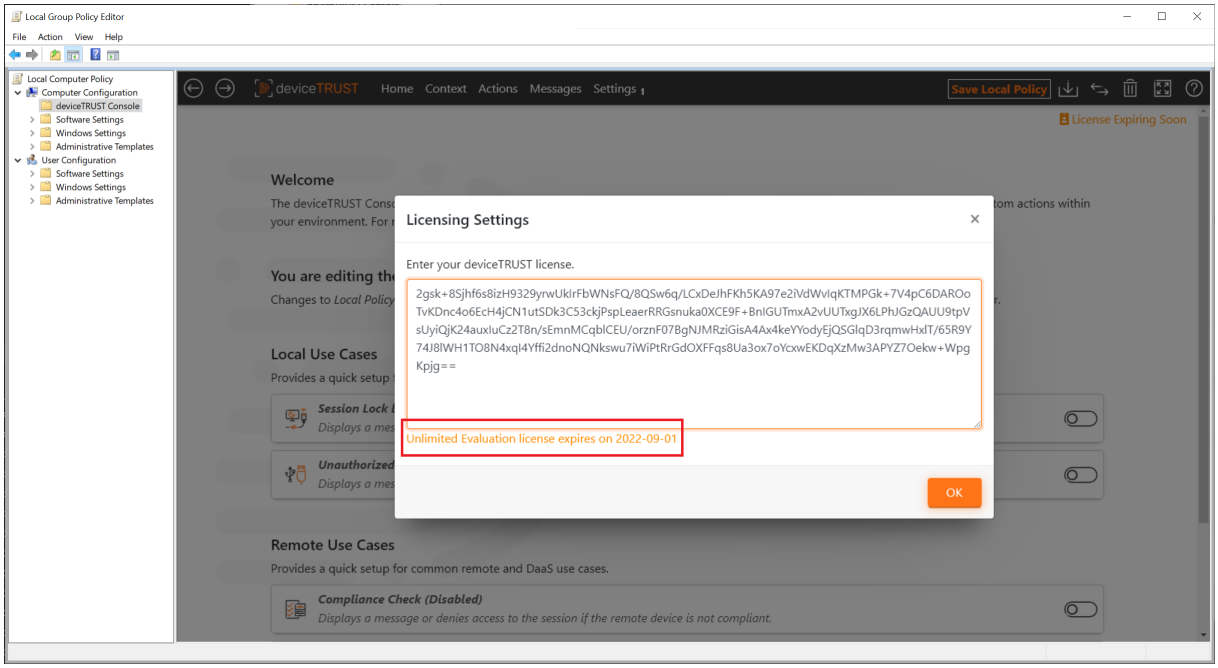
Step 4: Enter your deviceTRUST License

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.

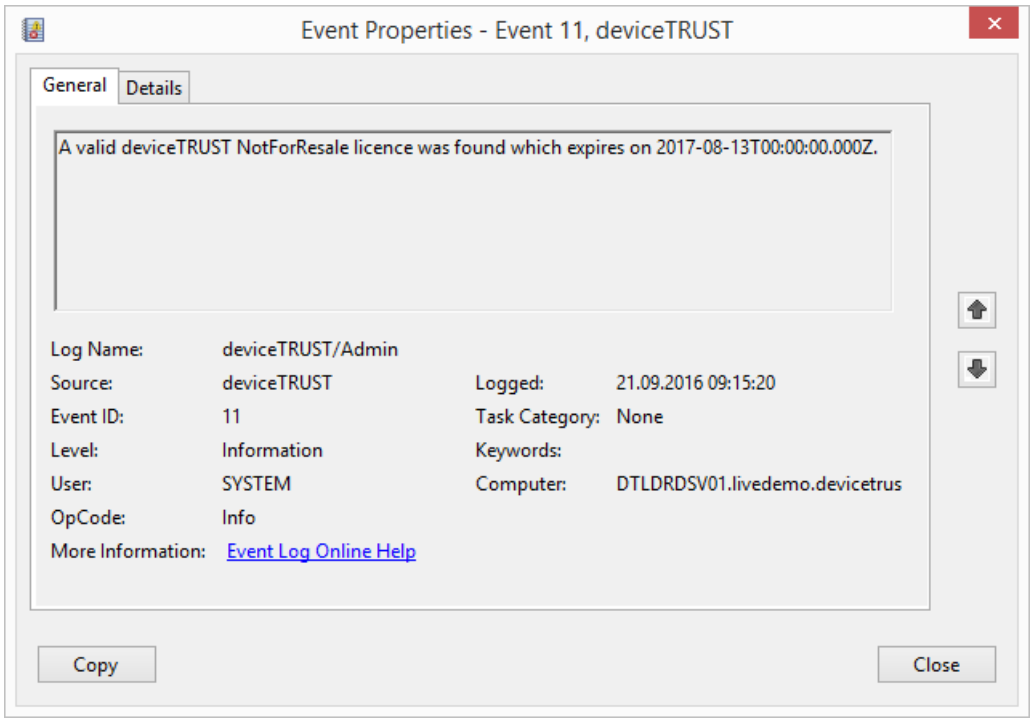


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.

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



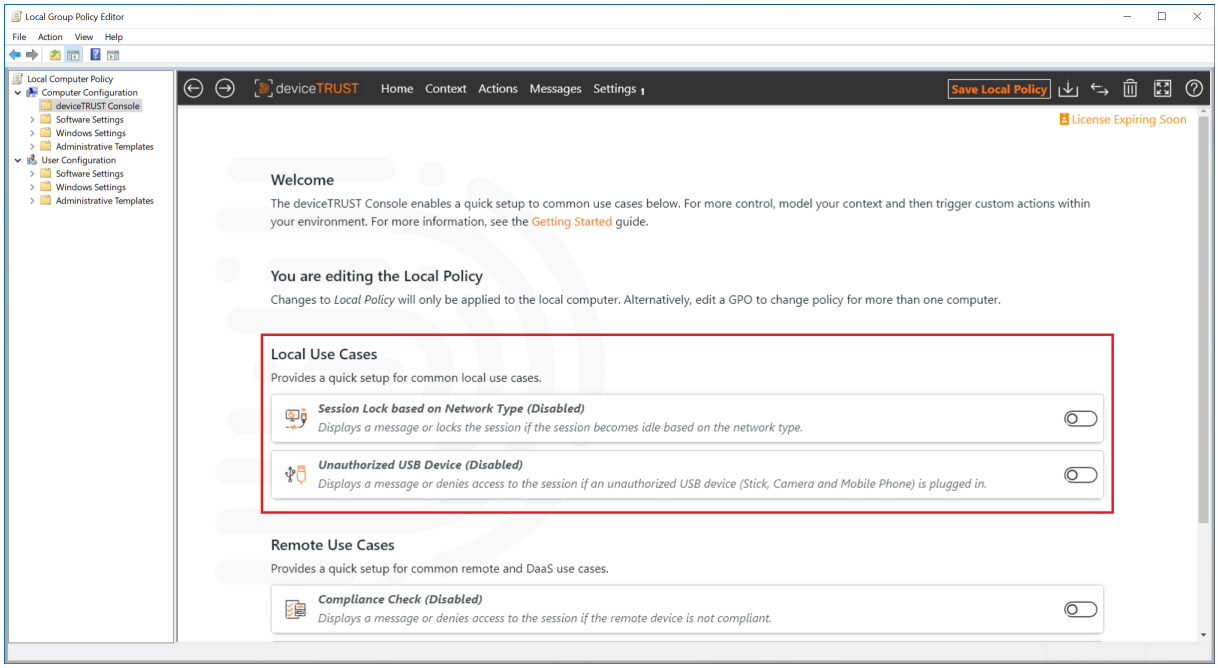
deviceTRUST is now enabled and will work for all users except local administrators connecting to that remoting or DaaS host system with deviceTRUST Agent installed. To check if you have added a valid deviceTRUST license, open the Windows Event Log and navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN`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



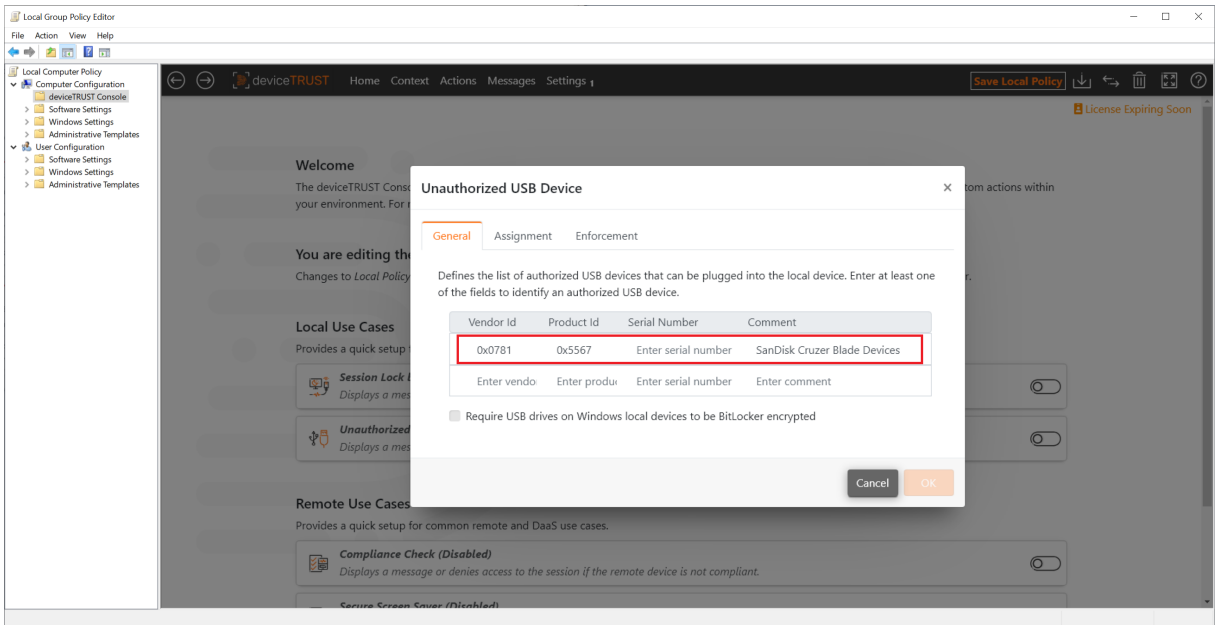
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5: 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.



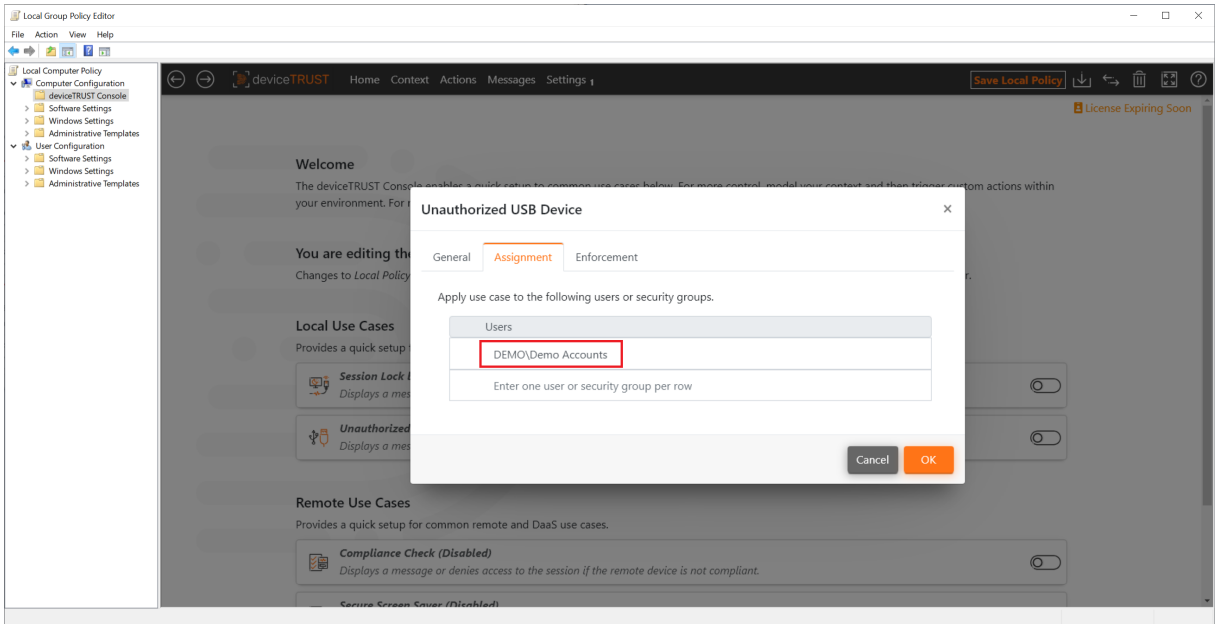
Select the UNAUTHORIZED USB DEVICE use case and add authorized USB devices on the GENERAL tab into the list of authorized USB devices.



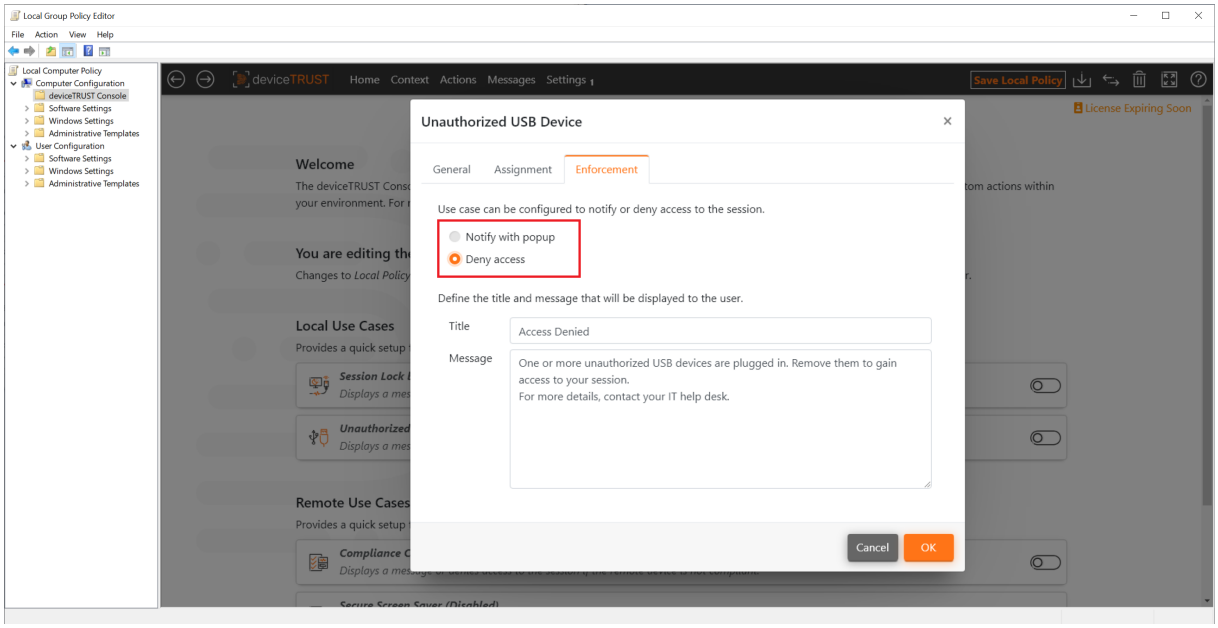
Click on the ASSIGNMENT configuration tab and add USERS and / or SECURITY GROUPS to apply

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

the use case for.

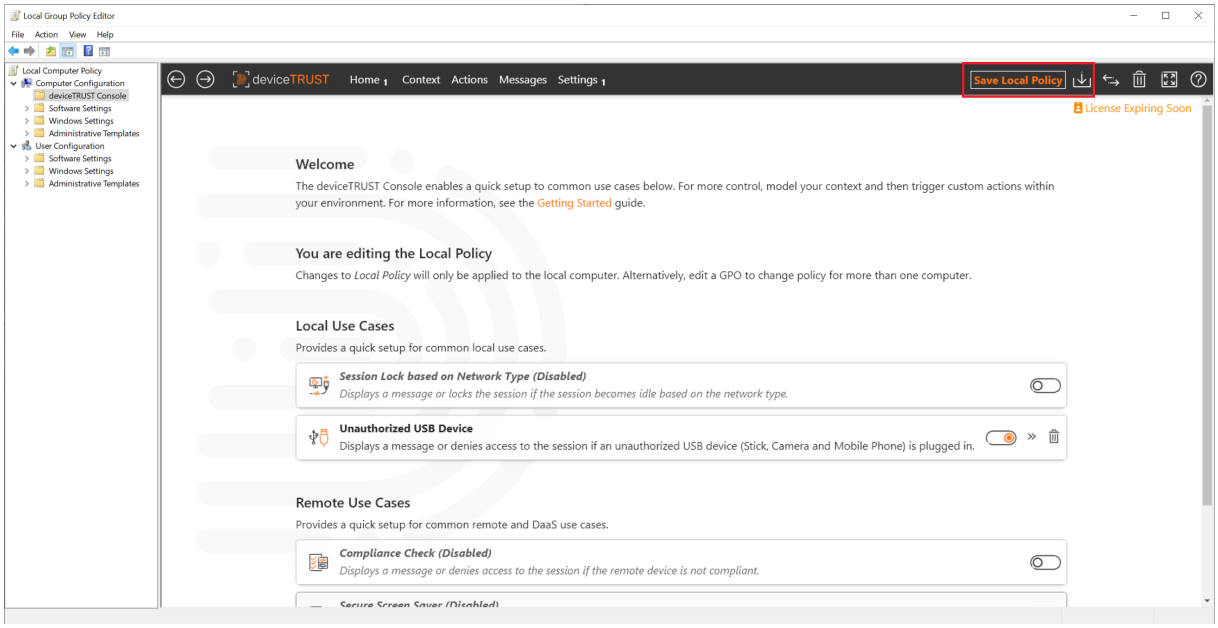


Click on the ENFORCEMENT configuration tab and select DENY ACCESS.



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.

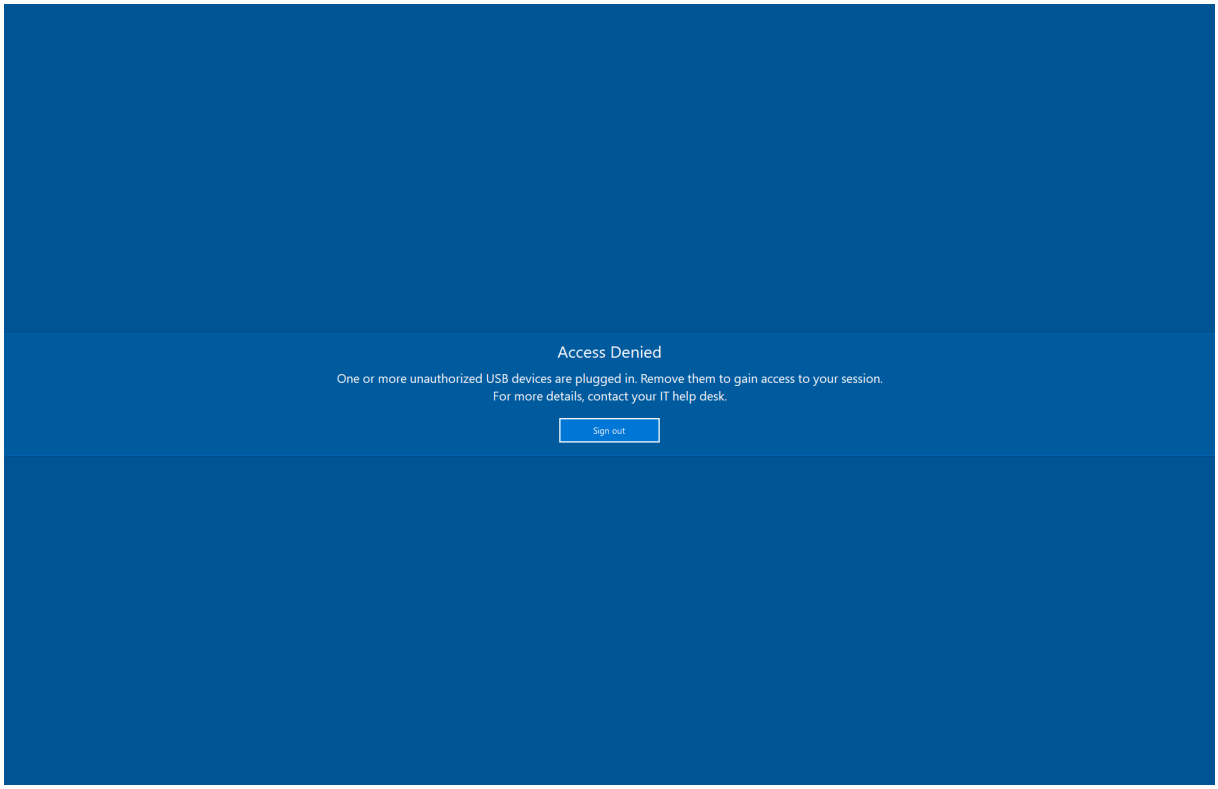
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

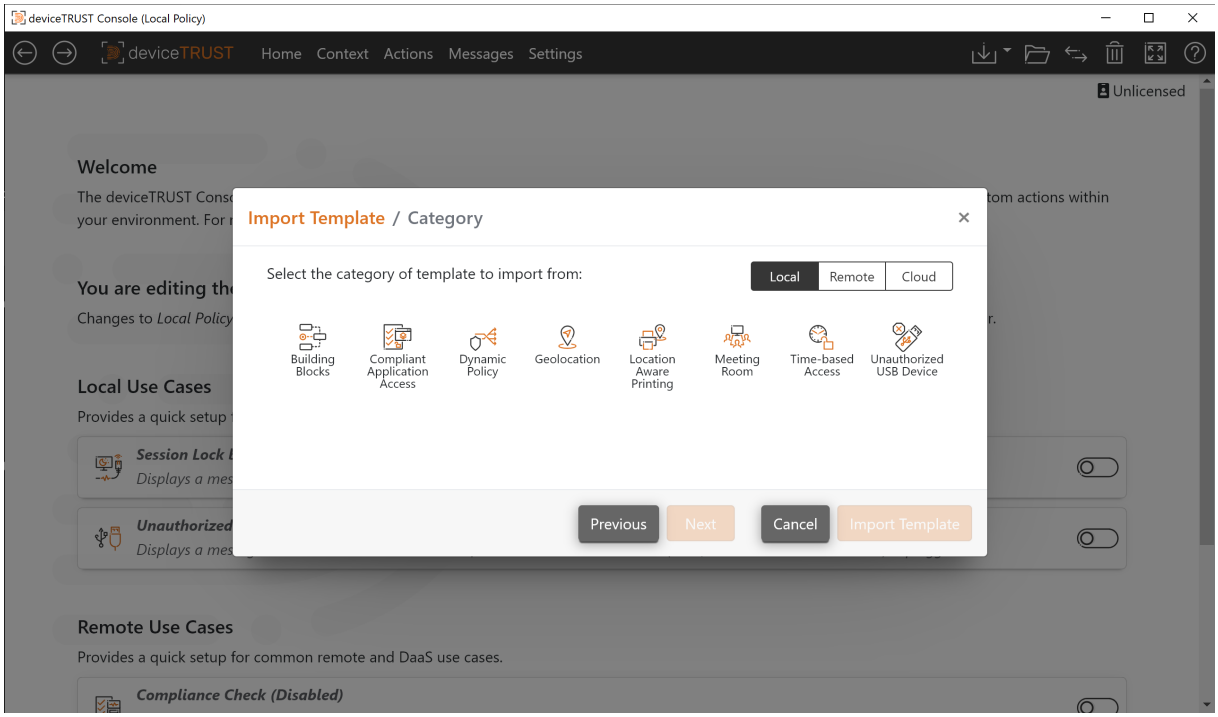
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

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



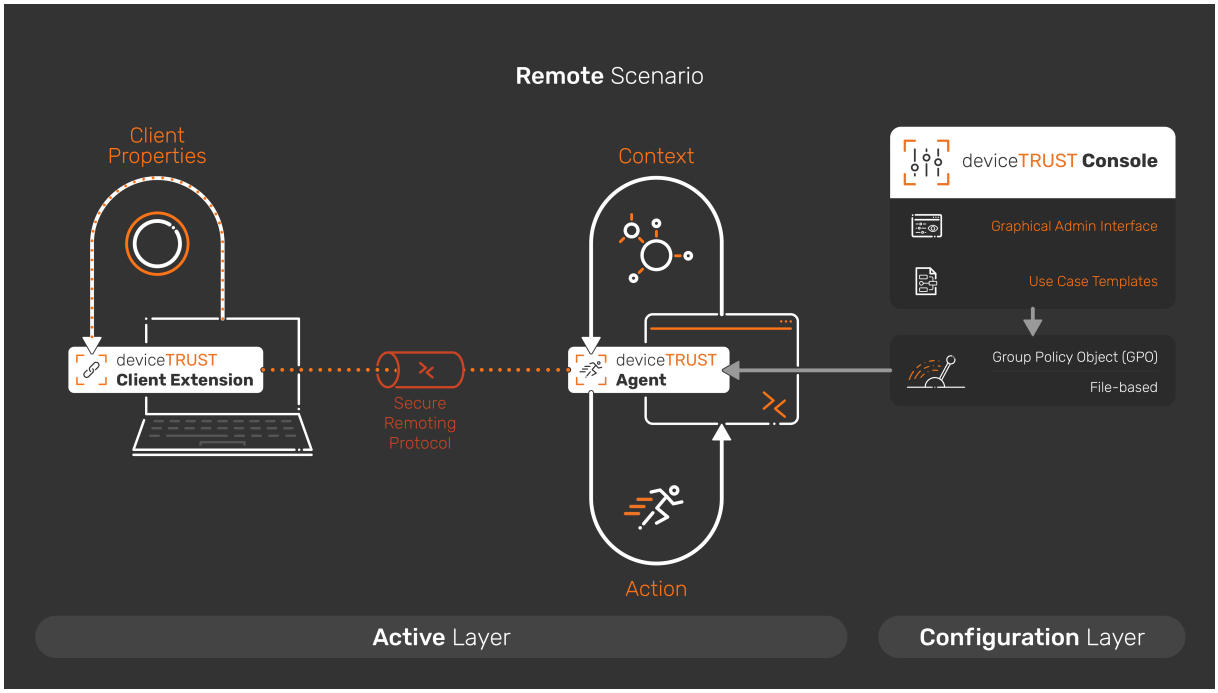
Troubleshooting

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

Getting Started for Remote

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

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



We will perform the following steps:

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

Step 1: Download the deviceTRUST setup binaries

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

Step 2: Install the deviceTRUST Agent

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

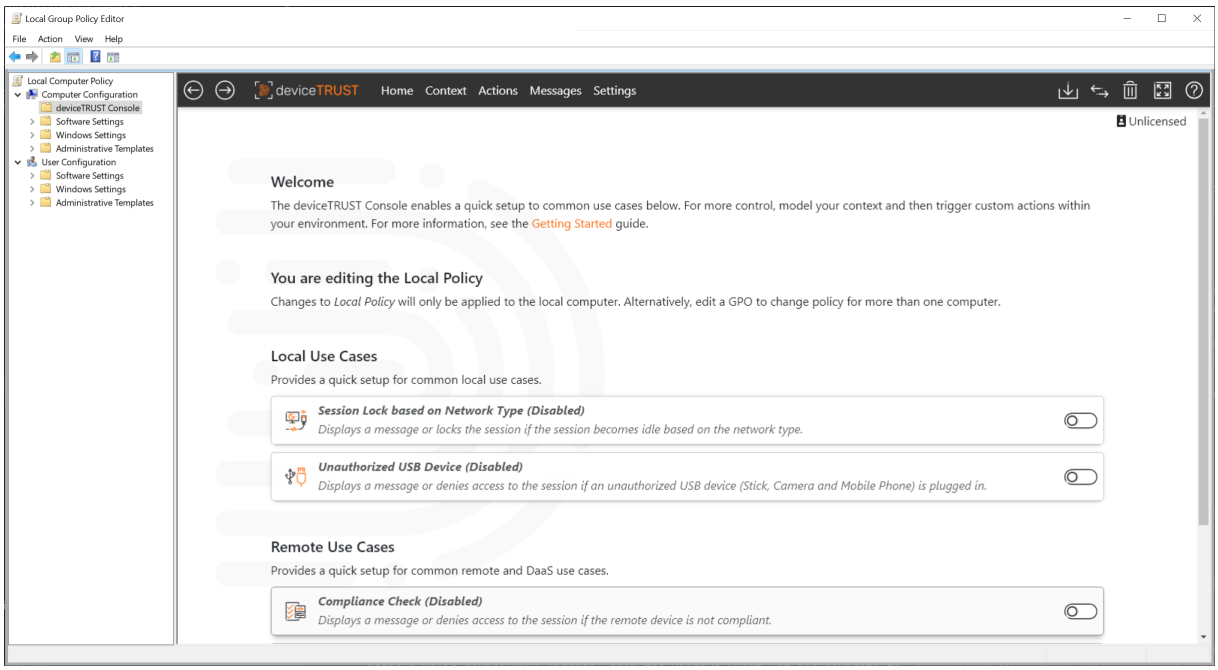
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Install the deviceTRUST Console

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

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

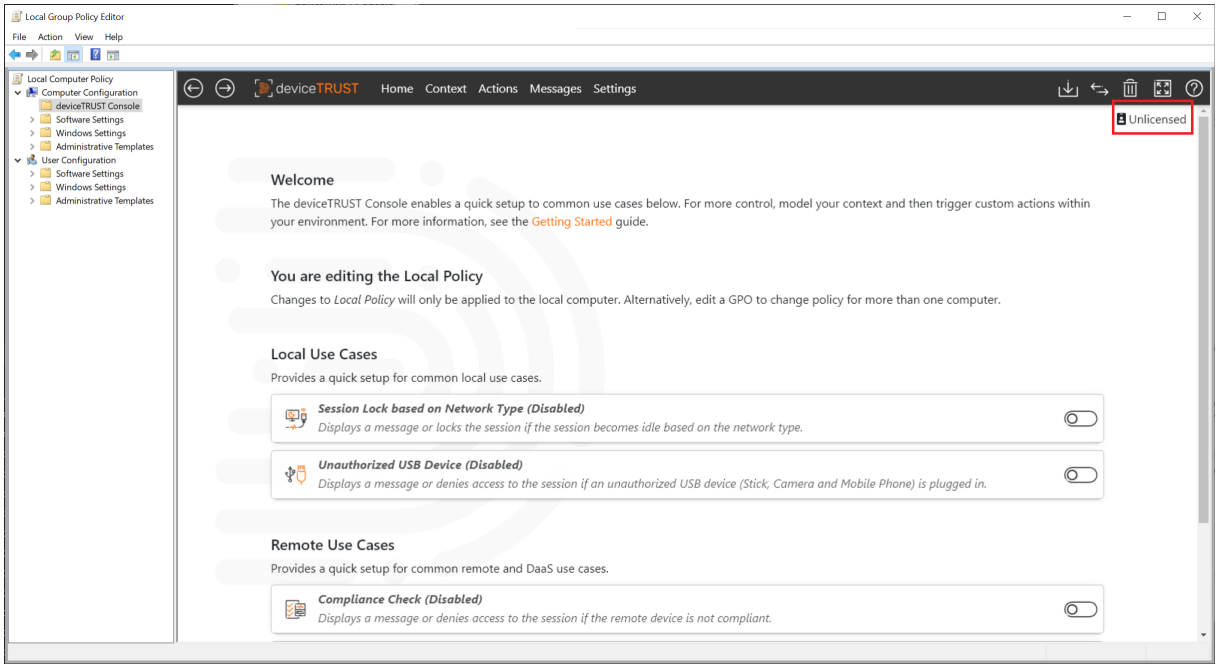
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



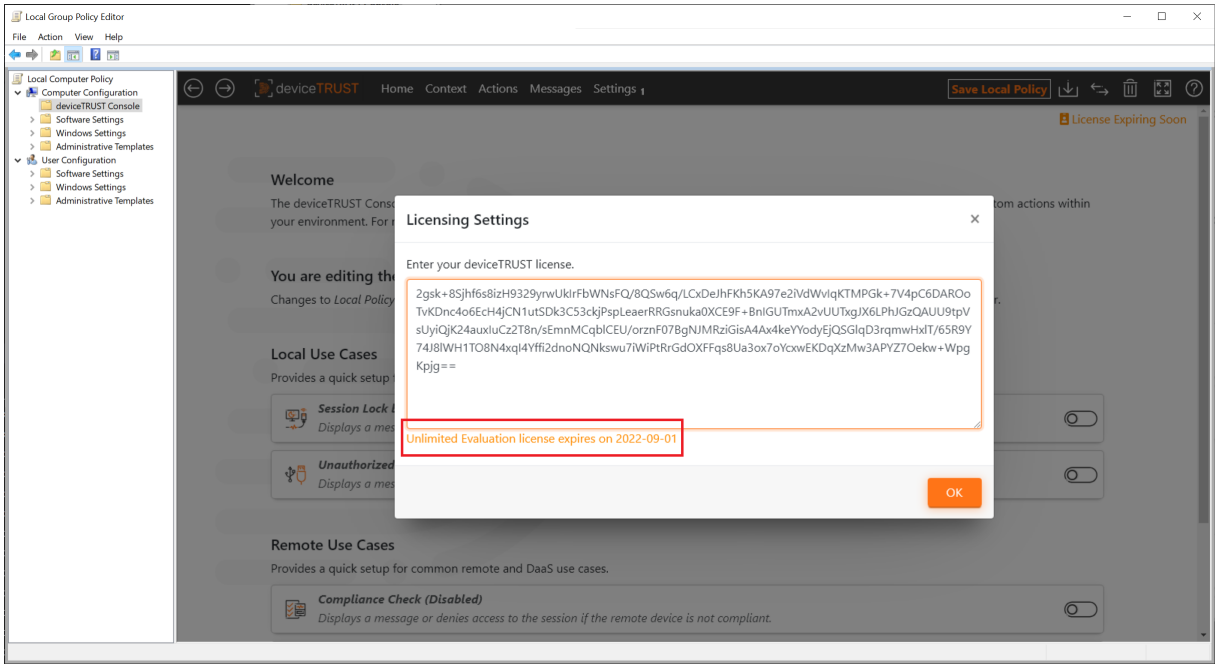
Step 4: Enter your deviceTRUST License

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

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

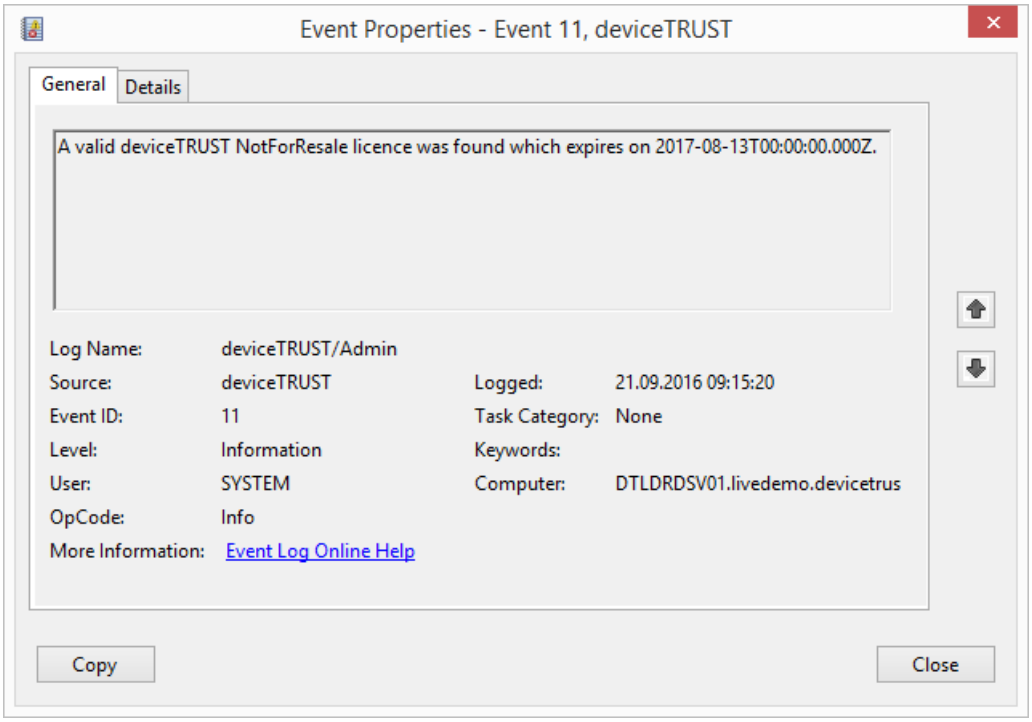


Enter your deviceTRUST license and make sure it is valid. Close the license editor with `OK` and click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar.



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

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



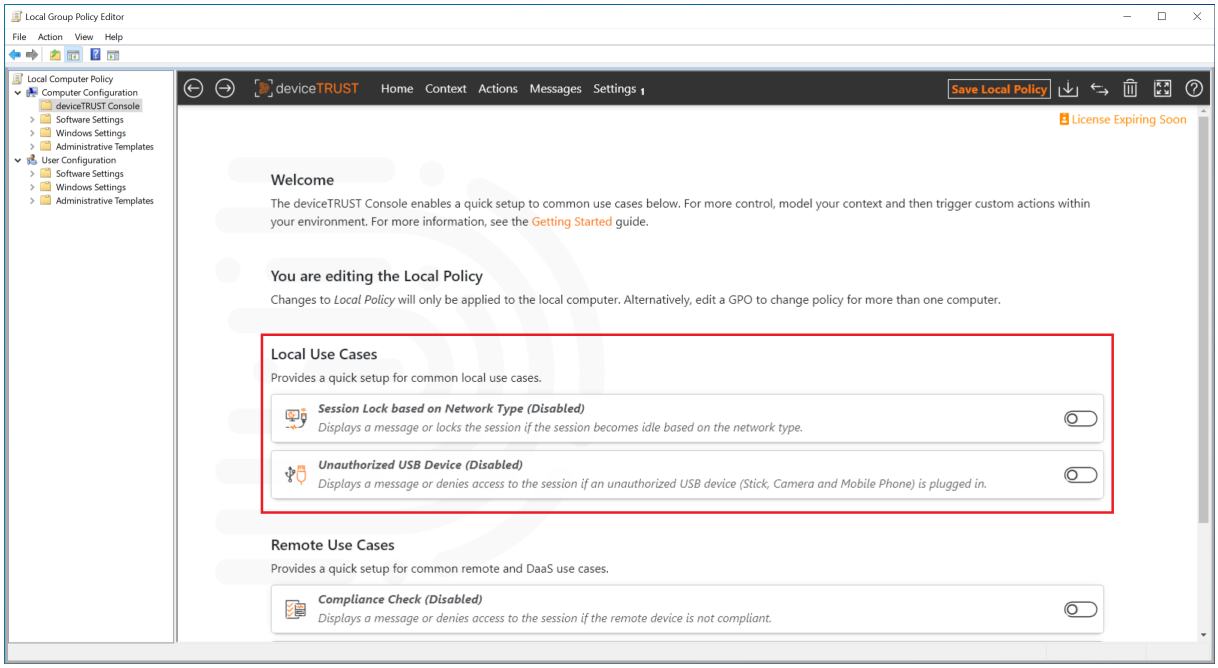
Step 5: Install the deviceTRUST Client Extension on a Microsoft Windows device

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

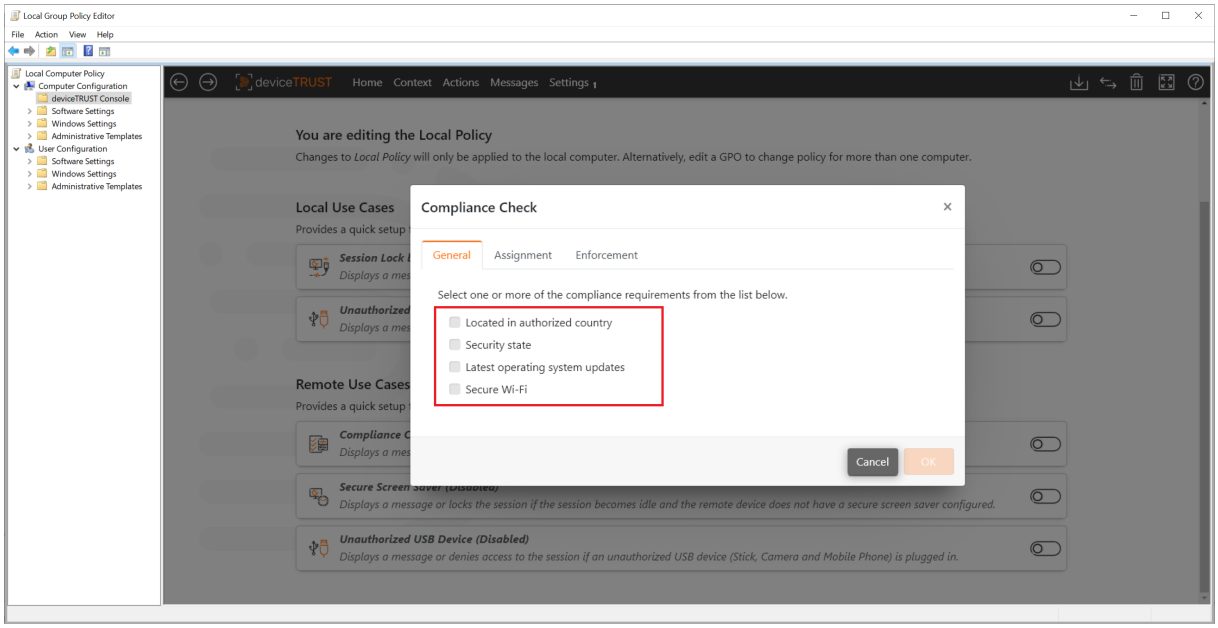
Step 6: Enable the Compliance Check use case

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

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

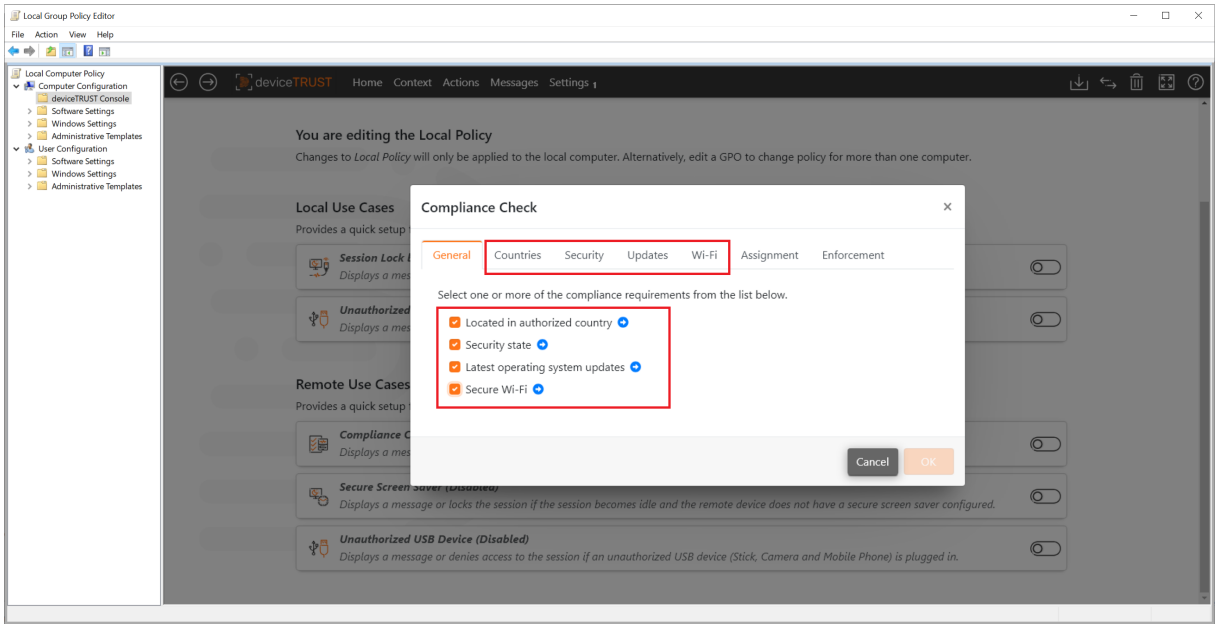


Select the `COMPLIANCE CHECK` use case, select on the `GENERAL` tab all options to be included in the compliance check.

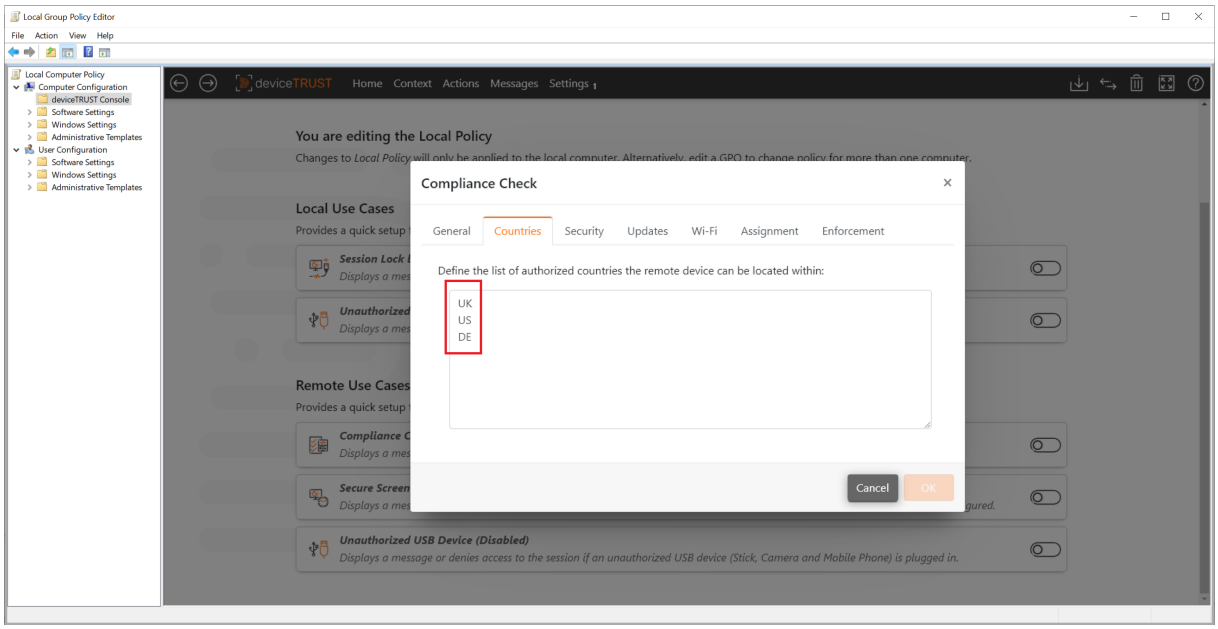


New configuration tabs will become visible.

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

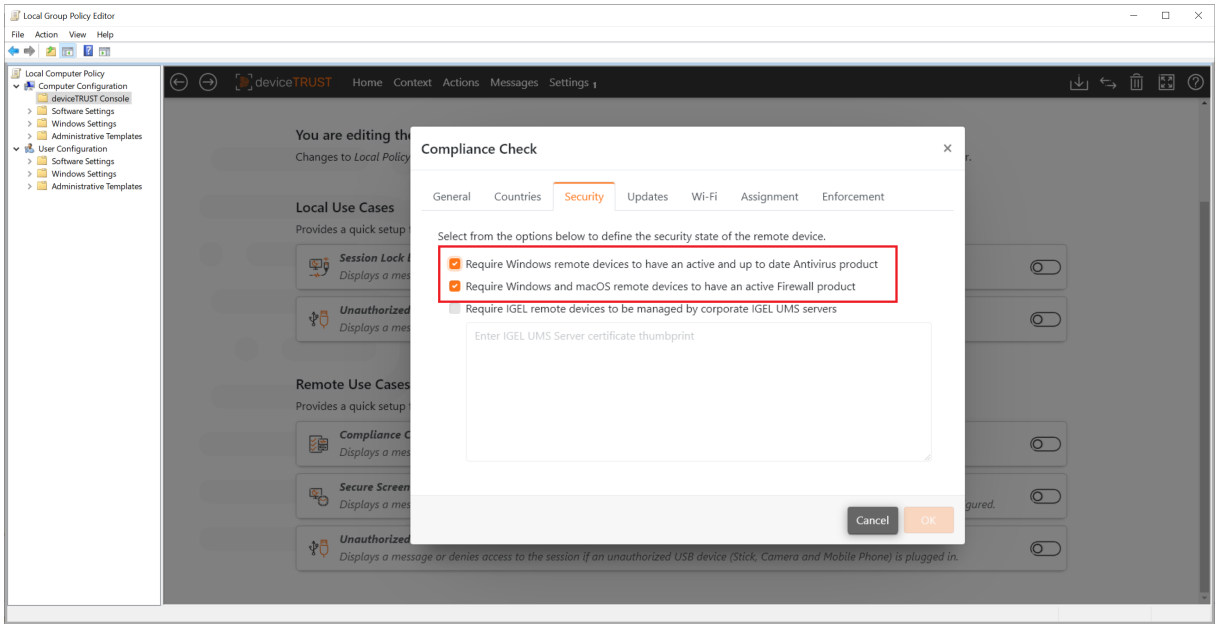


Click on the COUNTRY configuration tab and add all authorized countries using ISO 3166-1 Alpha-2 code.

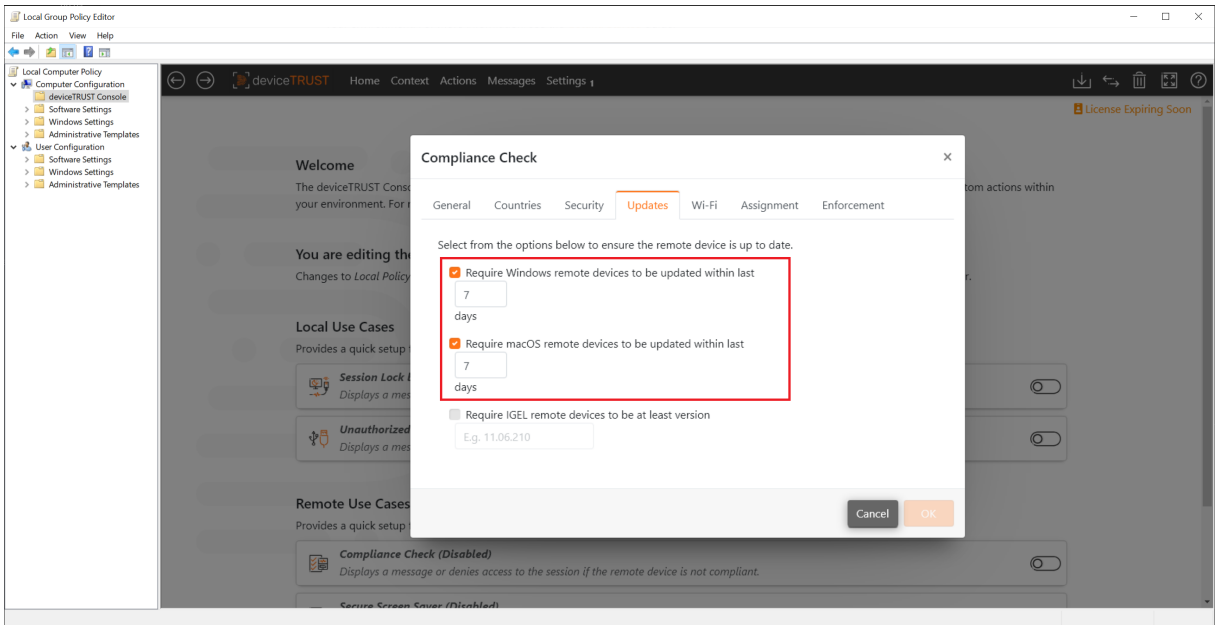


Click on the SECURITY configuration tab and enable the REQUIRE WINDOWS REMOTE DEVICES TO HAVE AN ACTIVE AND UP TO DATE ANTIVIRUS PRODUCT and REQUIRE WINDOWS AND MACOS REMOTE DEVICES TO HAVE AN ACTIVE FIREWALL PRODUCT options.

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

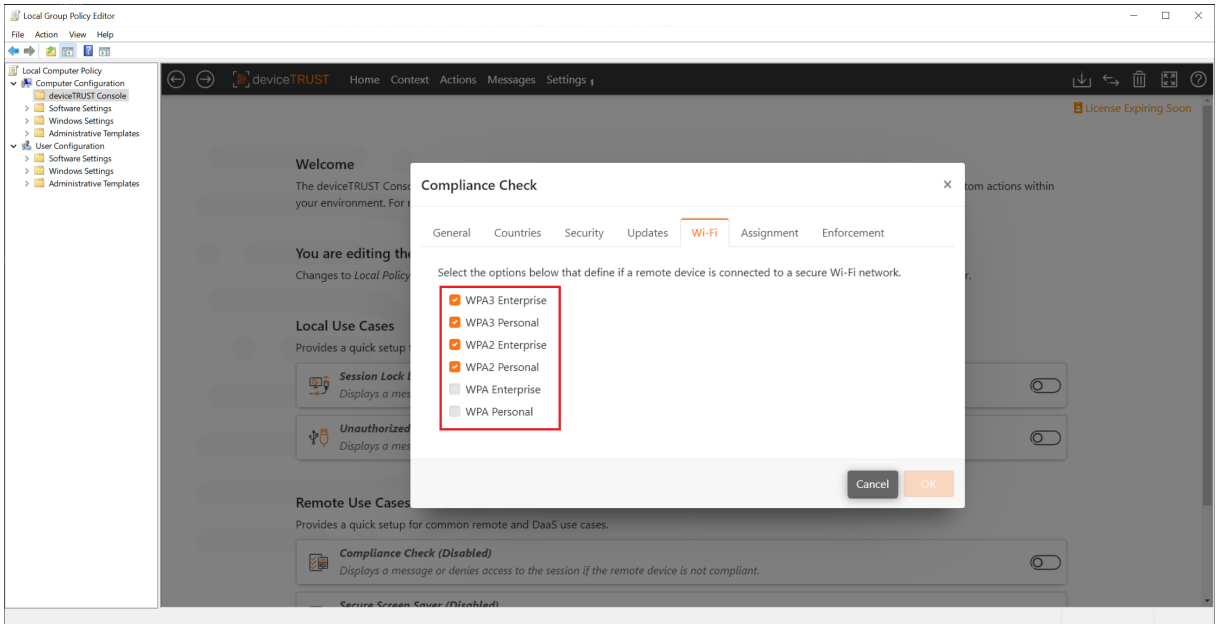


Click on the `UPDATES` configuration tab and enable the `REQUIRE WINDOWS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` and `REQUIRE MACOS REMOTE DEVICES TO BE UPDATED WITHIN THE LAST 7 DAYS` options.

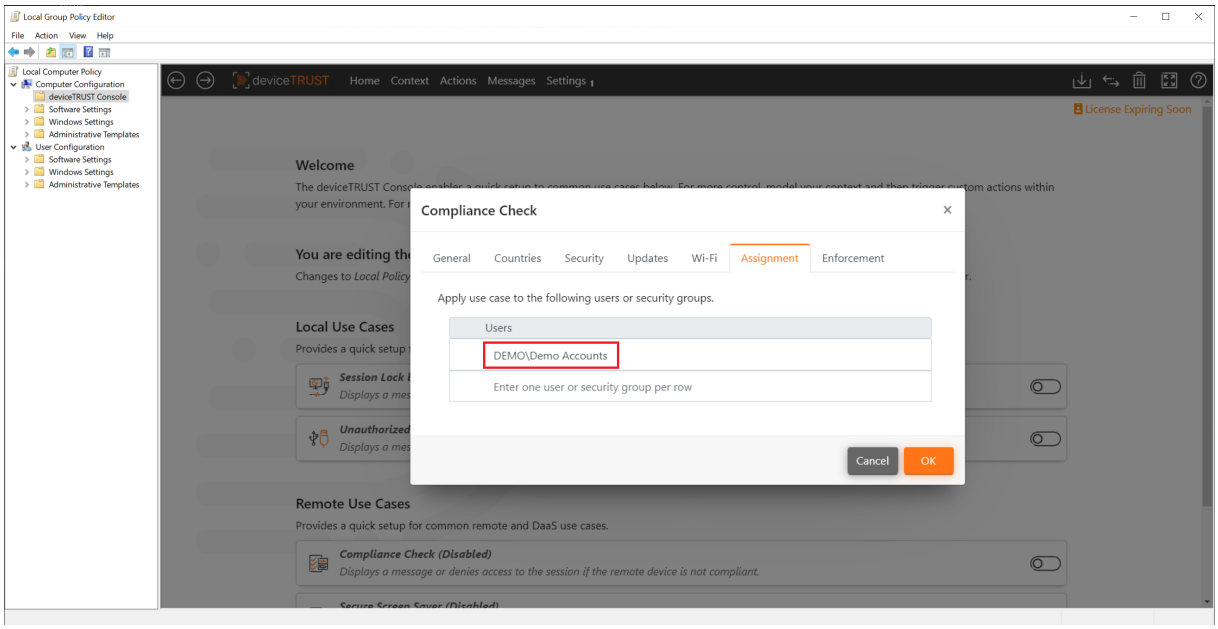


Click on the `WI-FI` configuration tab and enable the `WPA3 ENTERPRISE`, `WPA3 PERSONAL`, `WPA2 ENTERPRISE` and `WPA2 PERSONAL` options.

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

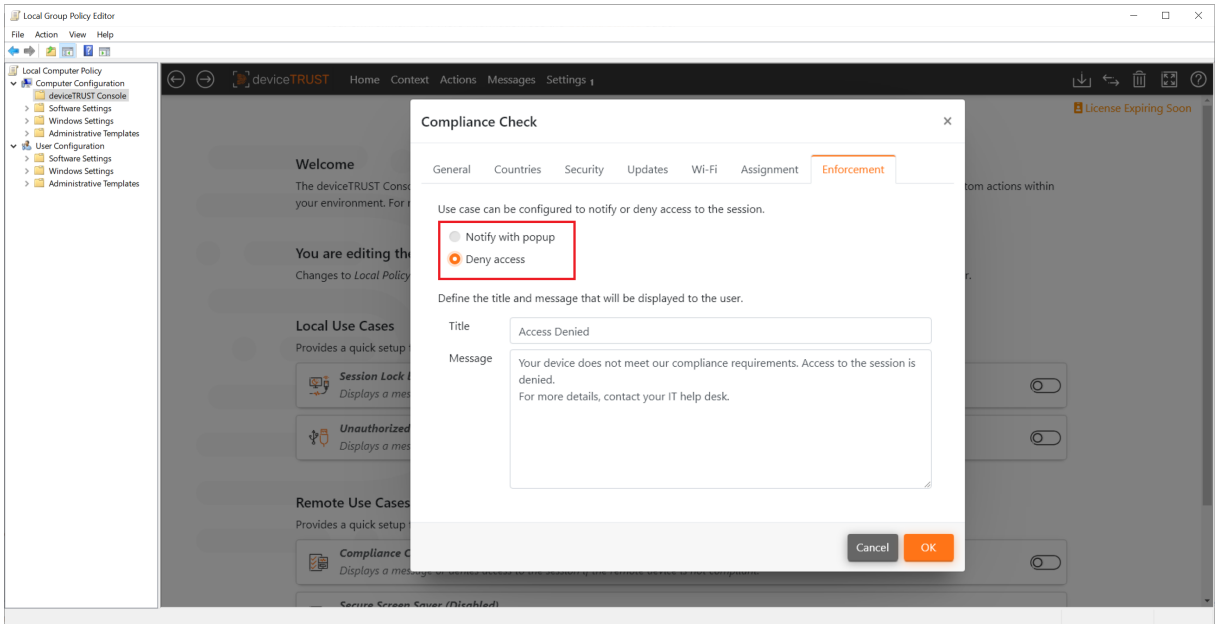


Click on the `ASSIGNMENT` configuration tab and add `USERS` and / or `SECURITY GROUPS` to apply the use case for.

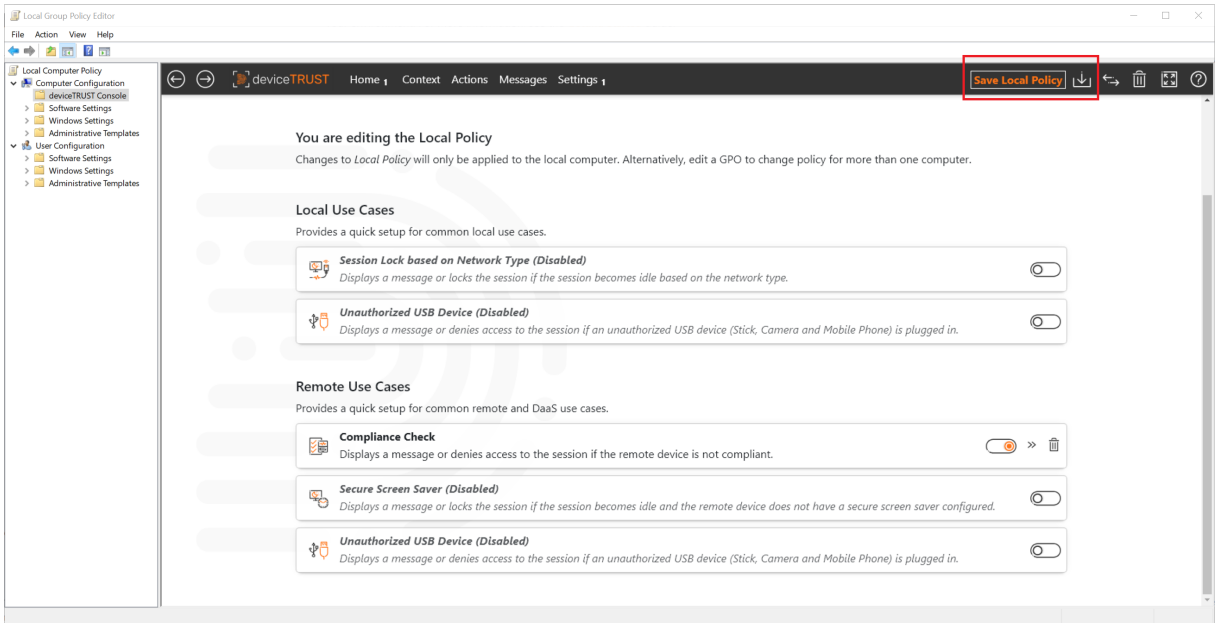


Click on the `ENFORCEMENT` configuration tab and select `DENY ACCESS`.

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



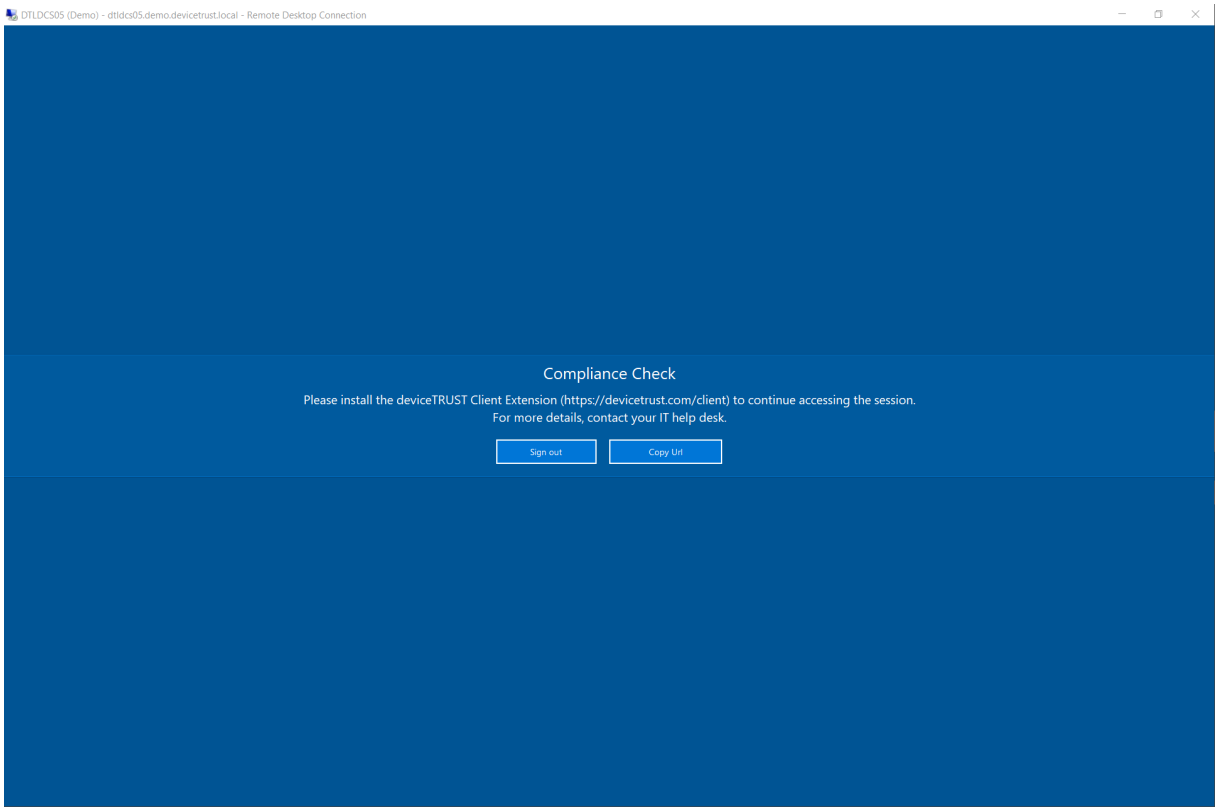
Click on `SAVE TO LOCAL COMPUTER POLICY` in the top right toolbar to save the complianc check use case to the local computer policy.



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

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

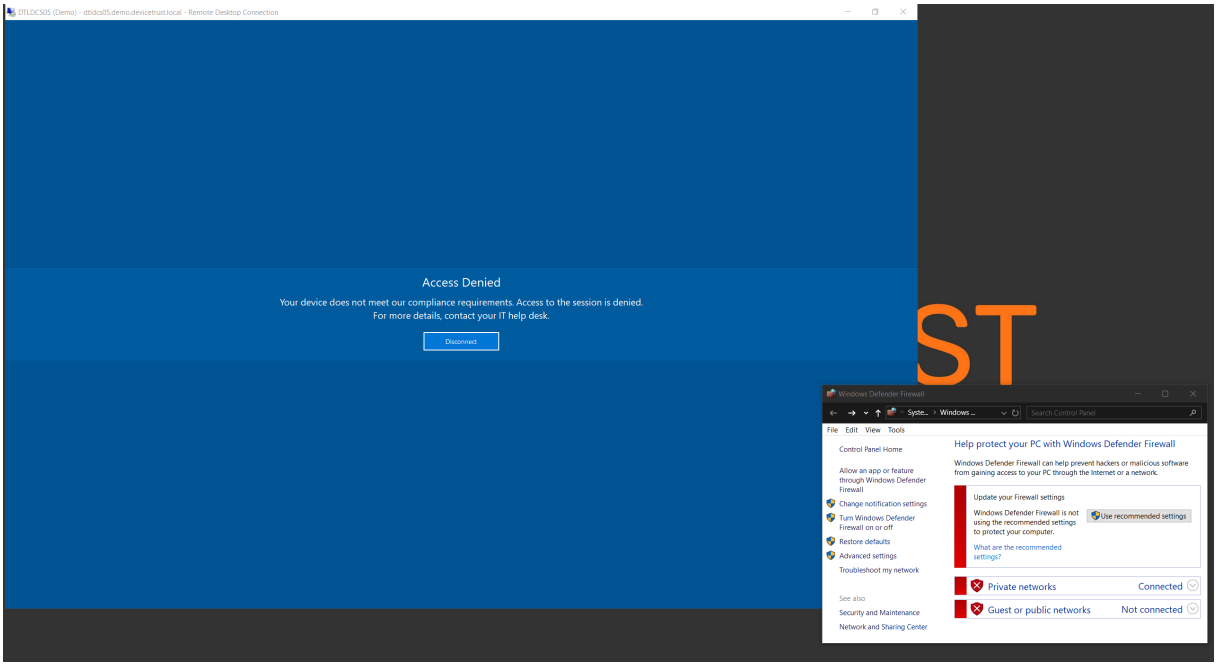
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

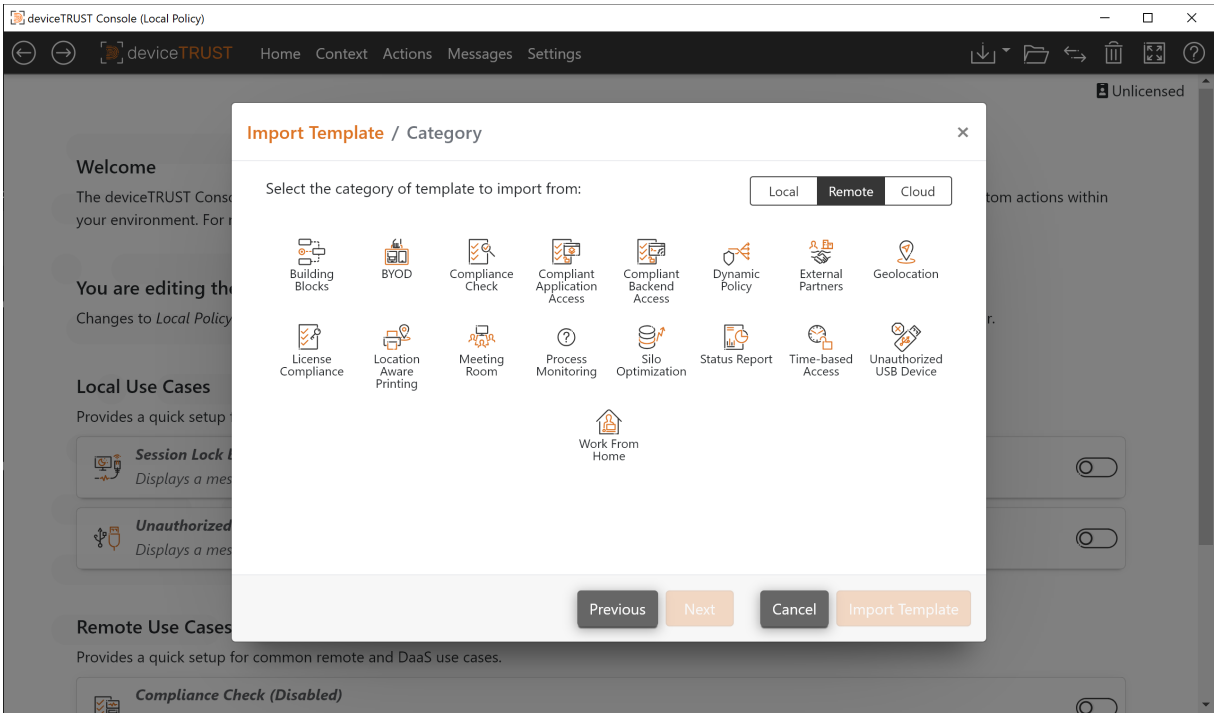
From a Microsoft Windows device with the deviceTRUST Client Extension installed, connect to your remoting or DaaS host system. Toggle the state of the Windows Defender Firewall to see how deviceTRUST can simply and dynamically control access to the session depending on the firewall state of the remote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

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



Next steps

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



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

Troubleshooting

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

Download deviceTRUST 23.1 for Windows

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

Version	23.1.410
Release Date	21st October 2024
URL	https://storage.devicetrust.com/download/deviceTRUST-23.1.410.zip
SHA256 Hash	04F5F434178FBE97D25F965A5F29239FF4EB117F04A5140C9D

Previous releases of these components can be downloaded download.

Download deviceTRUST® Client Extensions

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

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

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

Version	23.1.100
Release Date	19th May 2023
NoTouch Citrix URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient%5Fica.so
NoTouch Citrix SHA256	B5AF15C3338646A62EA4090AEB41C2DD2609B7B9228085C6B
NoTouch RDP URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient%5Frdp.so
NoTouch RDP SHA256	1E4F5DF9ABBA115BF9E0FD62A7EDA54C46C8C47ABE9EC12B

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

NoTouch VMware URL	https://storage.devicetrust.com/client/dtclient-notouch-amd64-release-23.1.100.0/libdtclient%5Fvmware.so
NoTouch VMware SHA256	27B80D37F28DC90727560527FD04BDA56F33C919EEE17C9E8

Note:

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

Software components

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

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

Note:

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

Installation

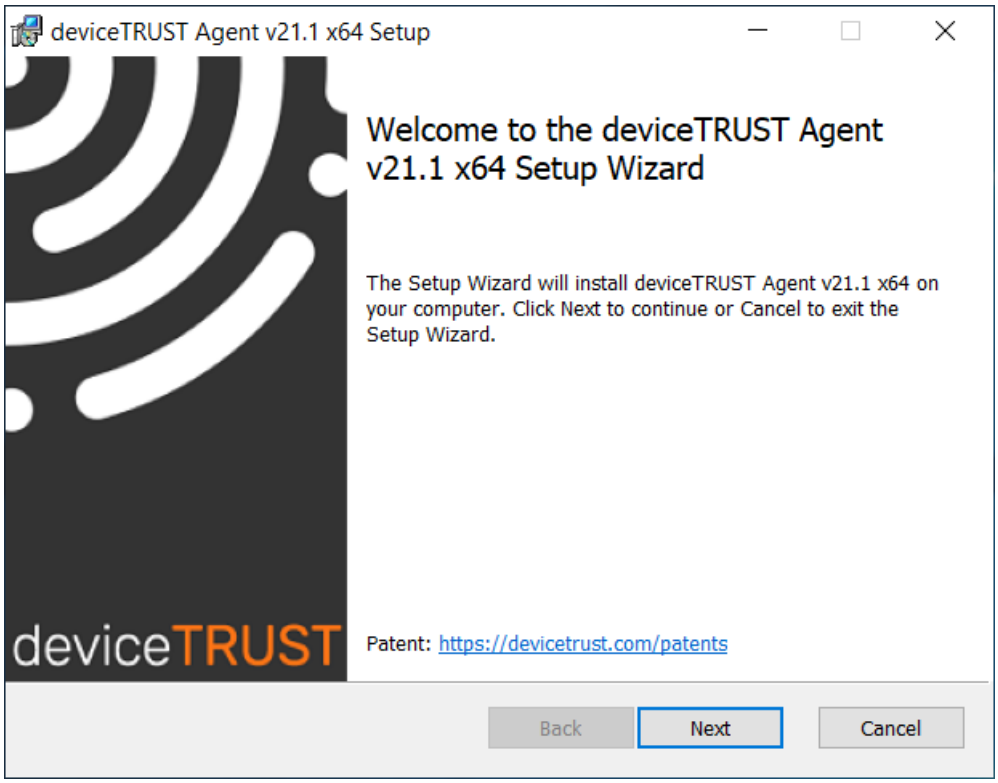
TABLE OF CONTENTS

- Agent
- Console
- Client Extension

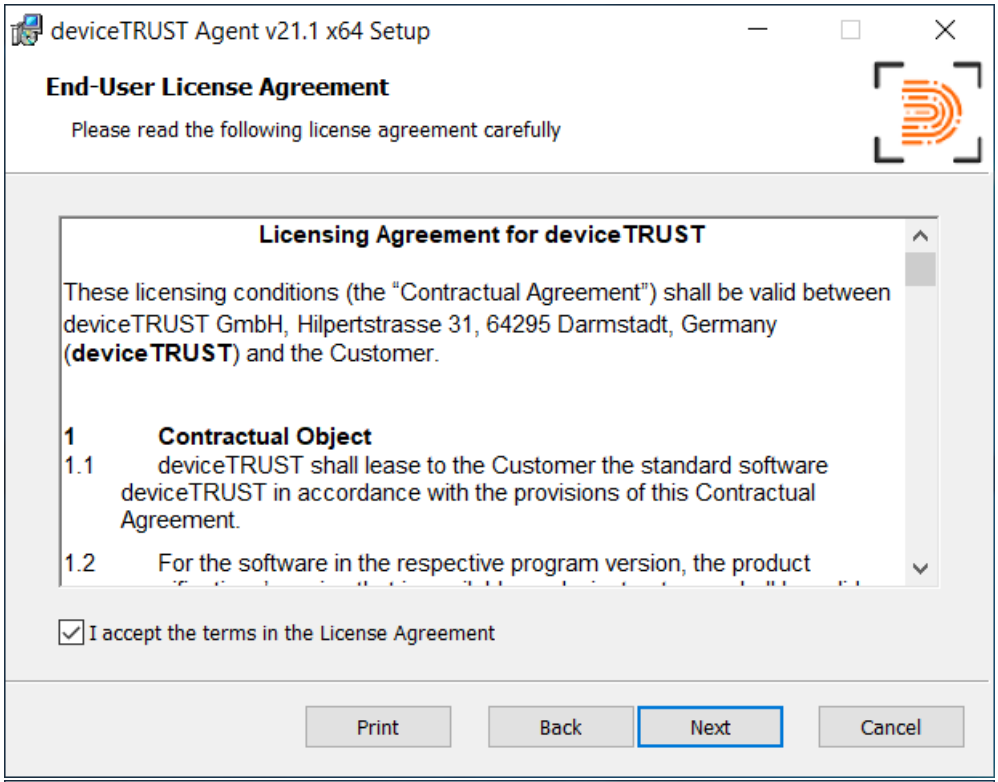
© 1997–2026 Citrix Systems, Inc. All rights reserved.

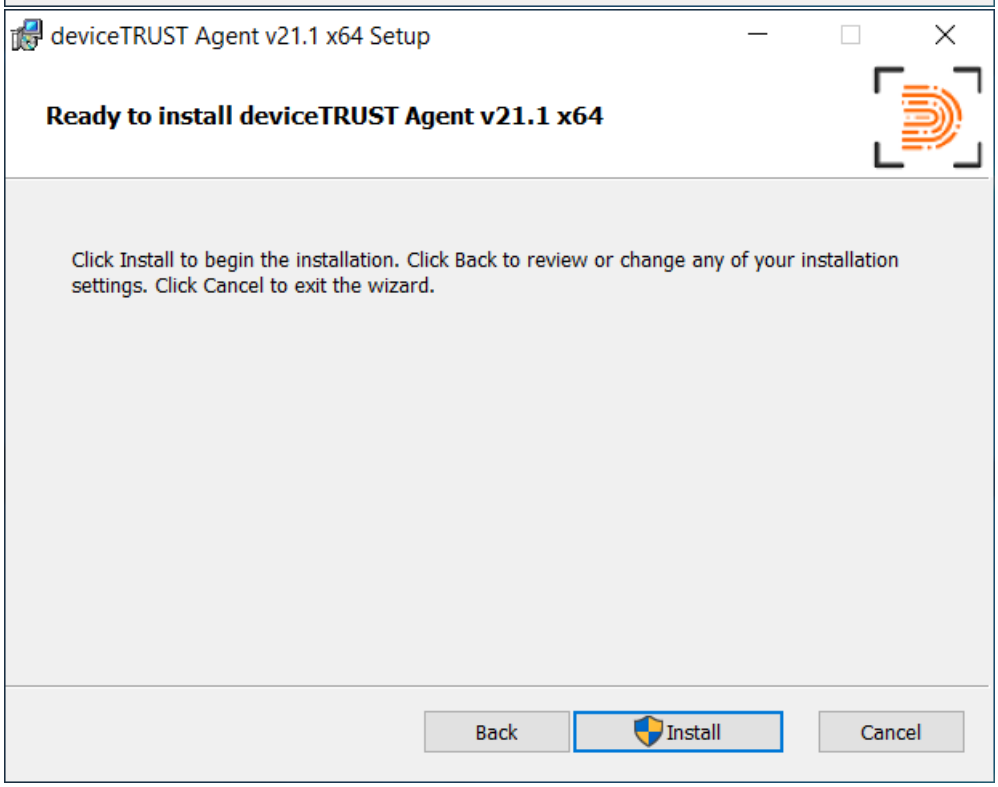
Installing the deviceTRUST® Agent

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

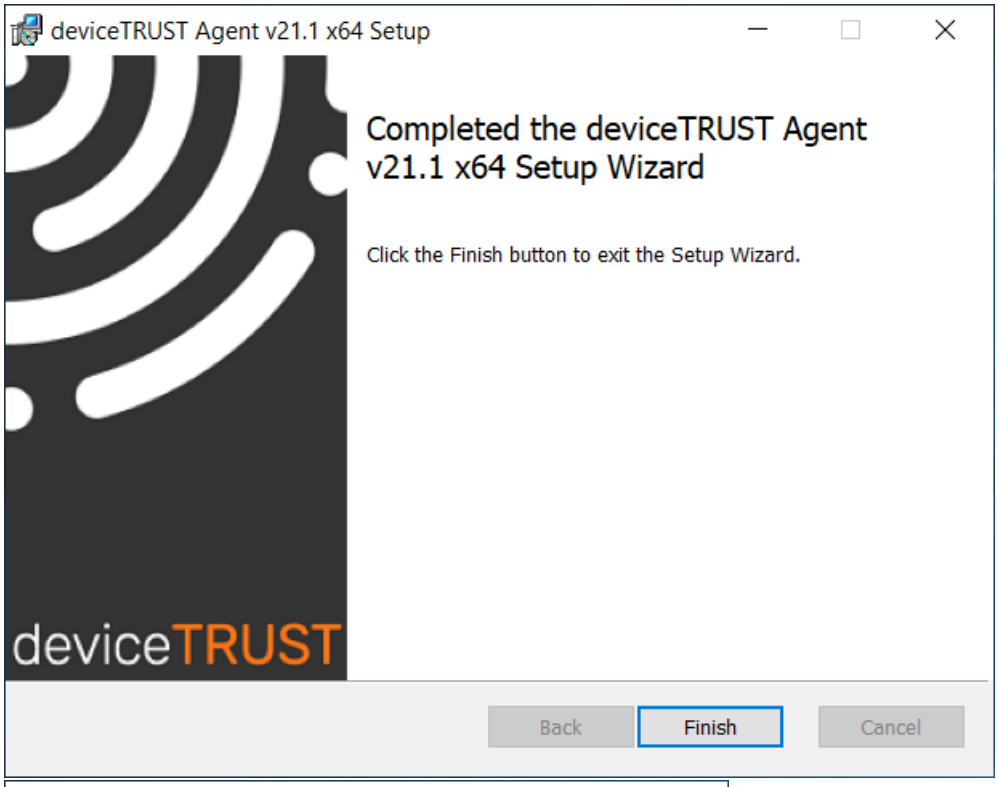


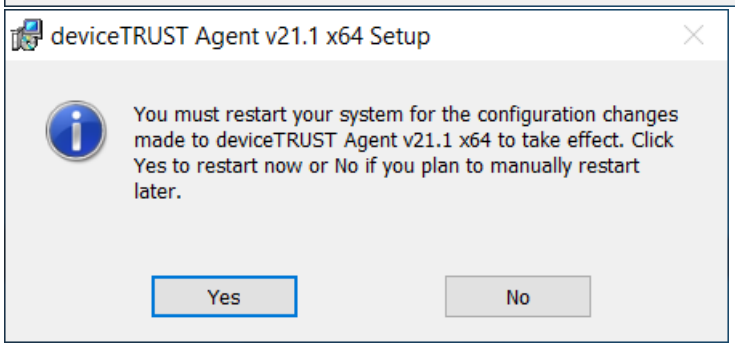
© 1997–2026 Citrix Systems, Inc. All rights reserved.





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





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

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.

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

More details can be found on the Knowledge Base.

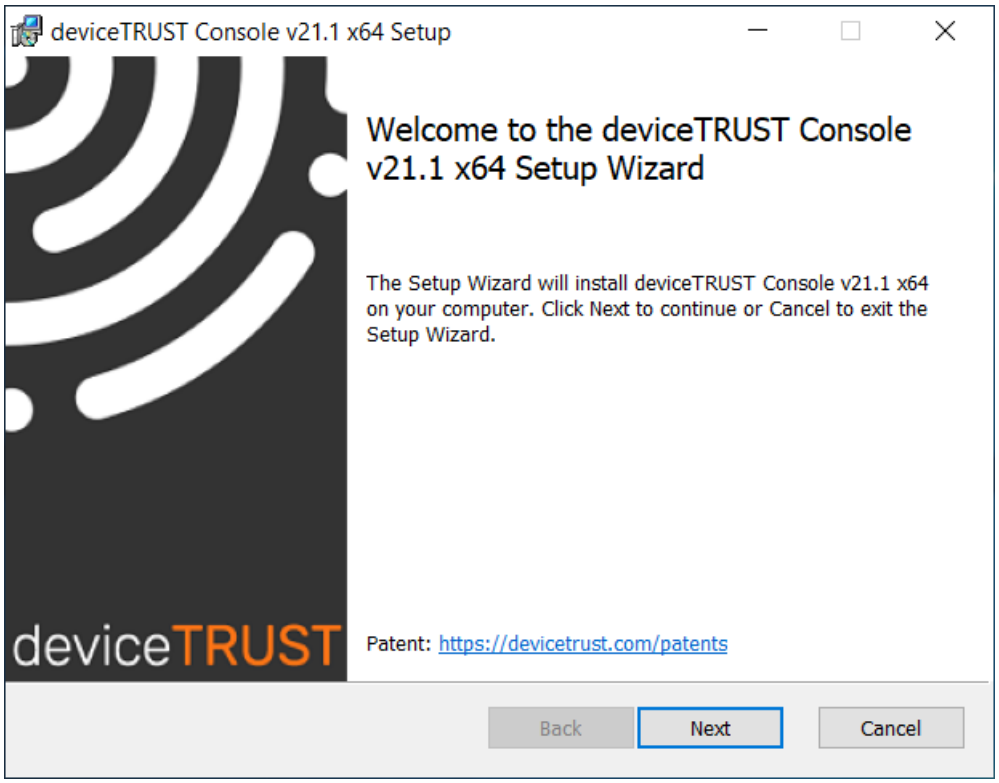
Unattended Installation

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

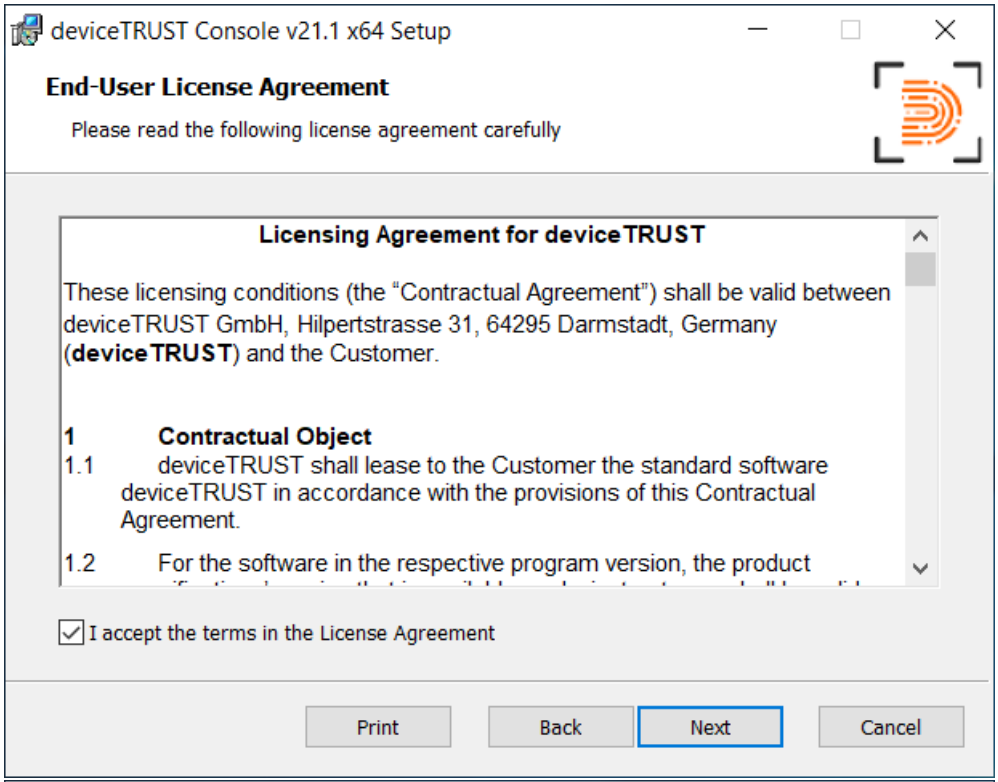
Component	Commandline
dtagent-x64-release-x.x.x.x.msi	The deviceTRUST Agent installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters `MSIEXEC.EXE /I DTAGENT-X64-RELEASE-X.X.X.X.MSI /PASSIVE /FORCERESTART`

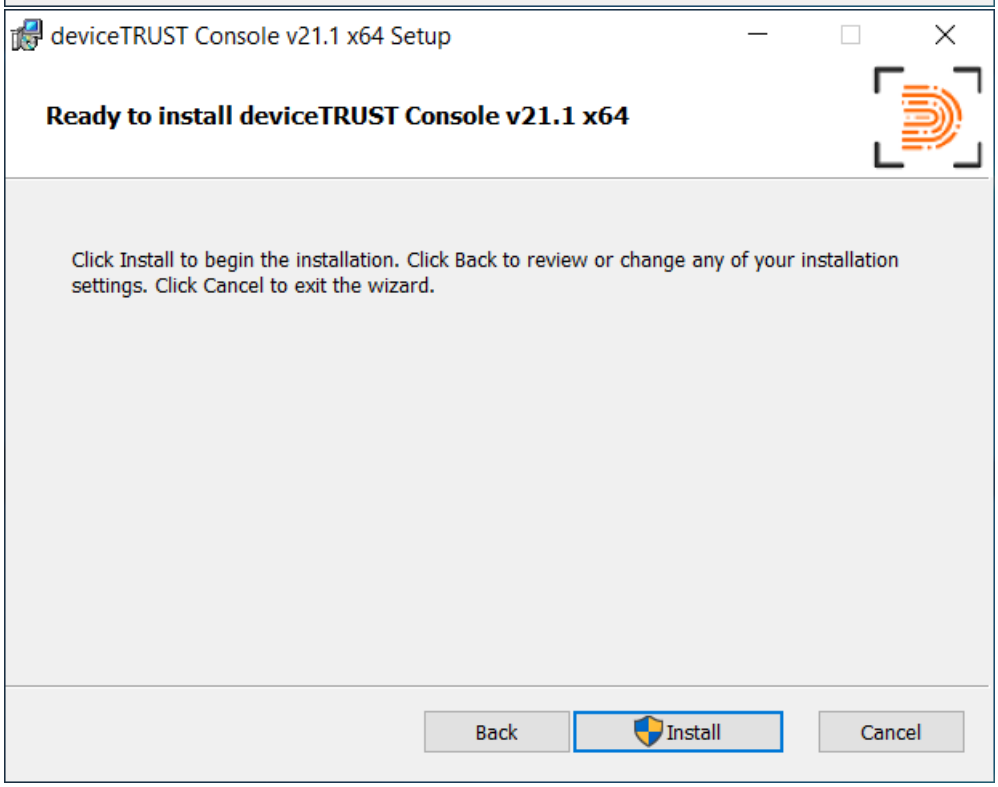
Installing the deviceTRUST® Console

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

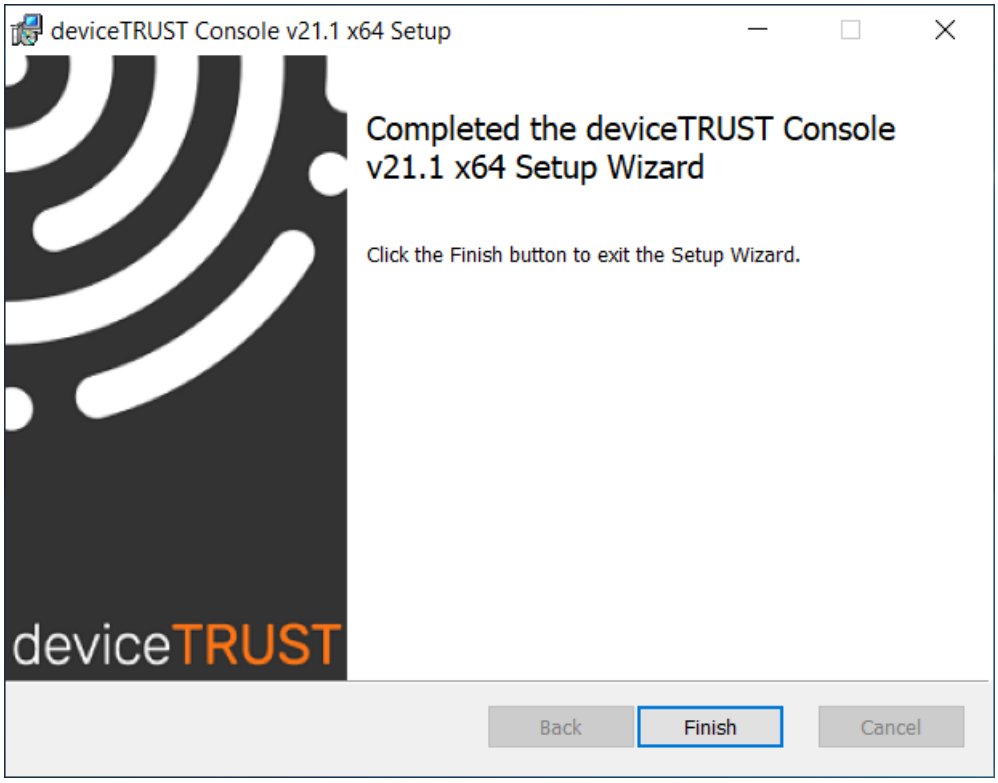


© 1997–2026 Citrix Systems, Inc. All rights reserved.





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



> **Note**
>
> Installation path: `%PROGRAMFILES%\DEVICETRUST\CONSOLE`

Unattended Installation

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

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

Installing the deviceTRUST® Client Extension

TABLE OF CONTENTS

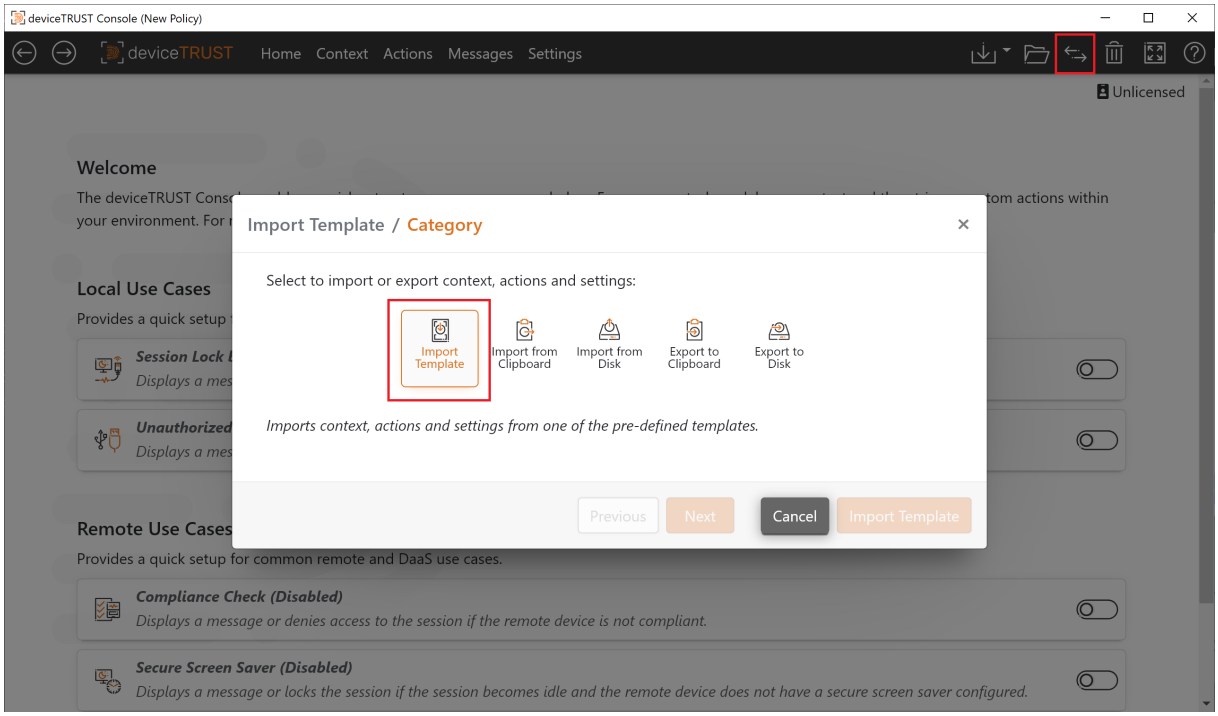
- Microsoft Windows

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

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

Templates

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



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

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

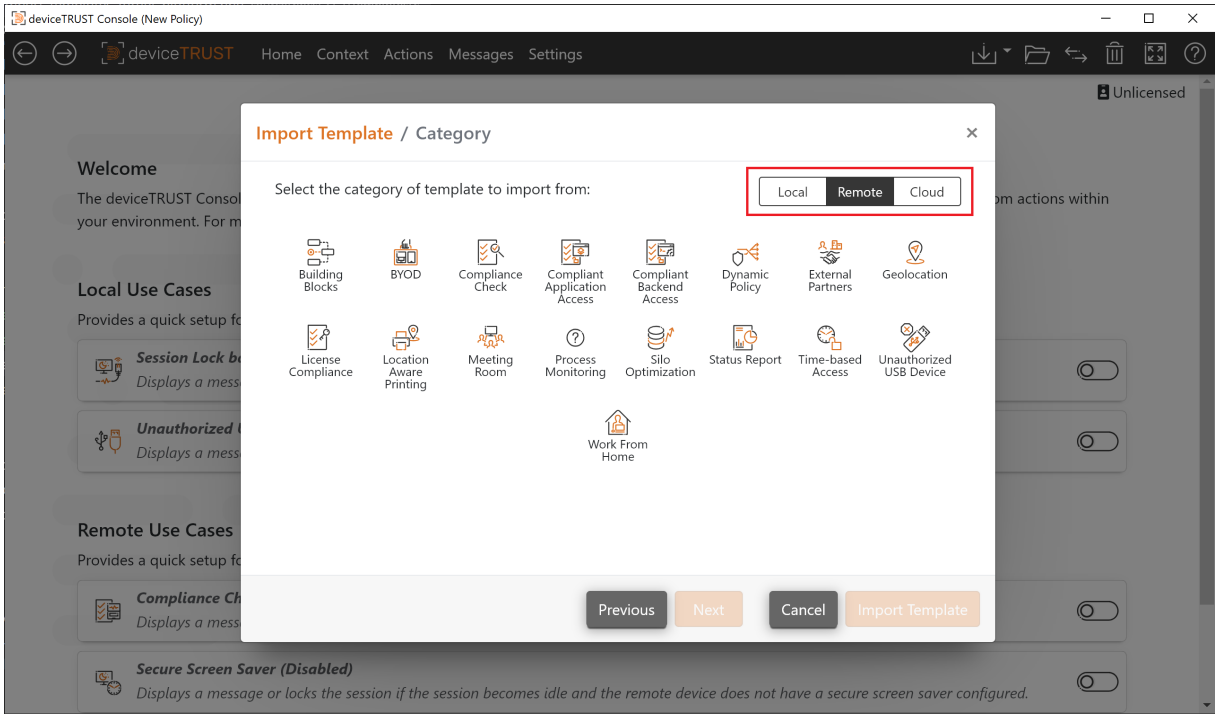


Table of Contents

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

Local Templates

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

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

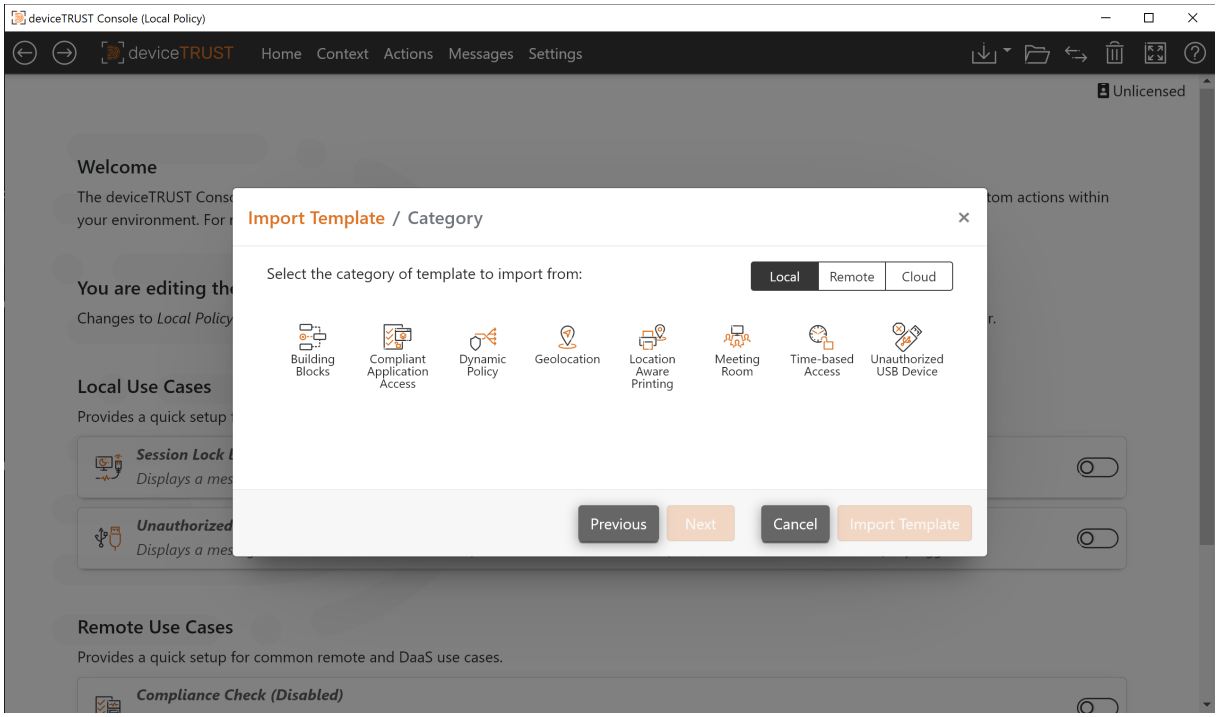


Table of Contents

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

Remote Templates

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

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

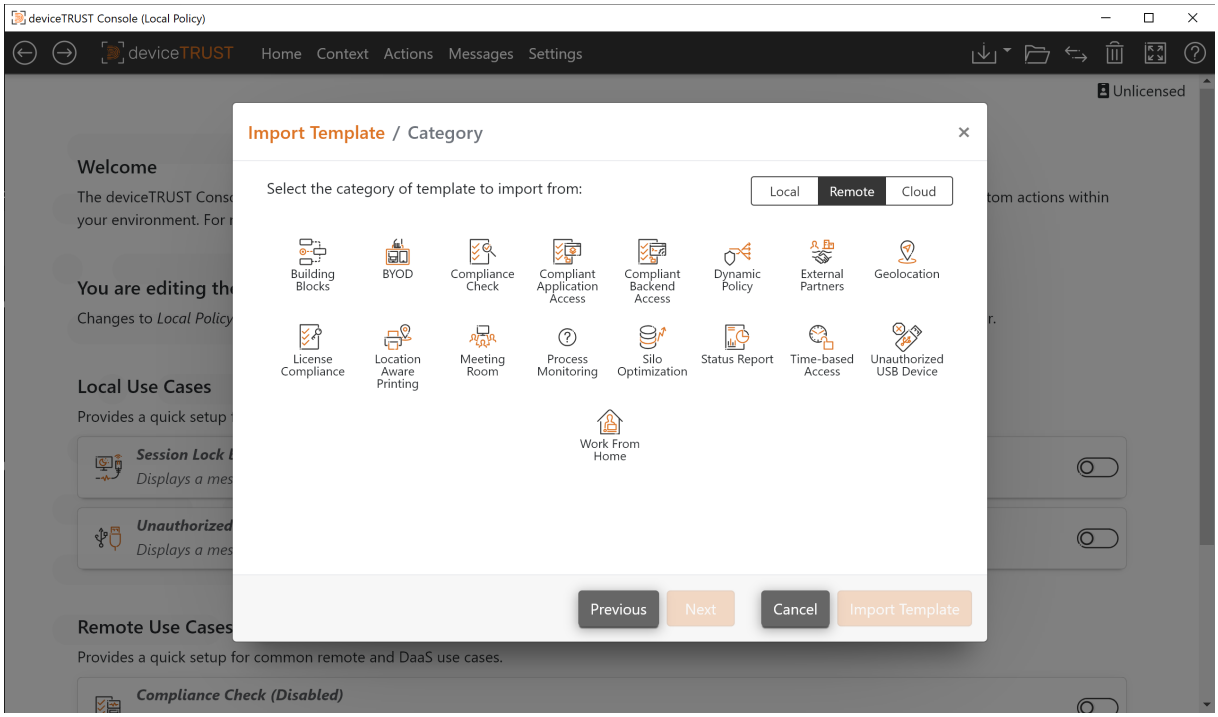


Table of Contents

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

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

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

SaaS Templates

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

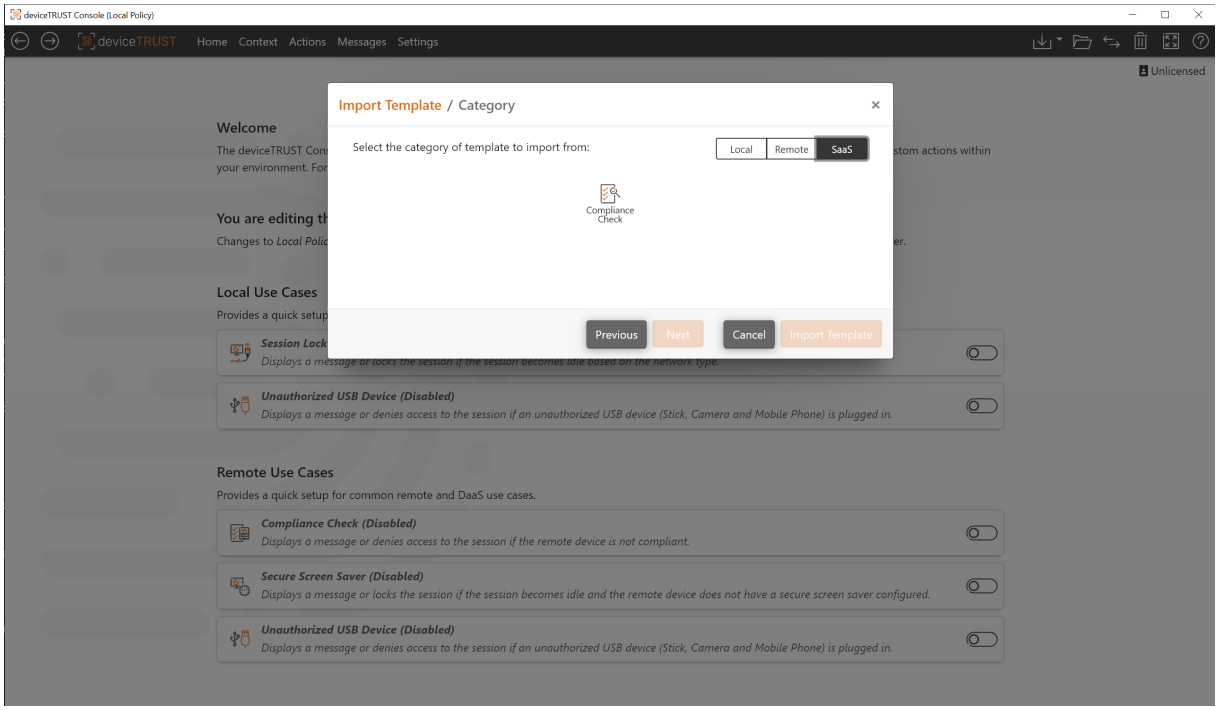


Table of Contents

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

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

Compliance Check

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

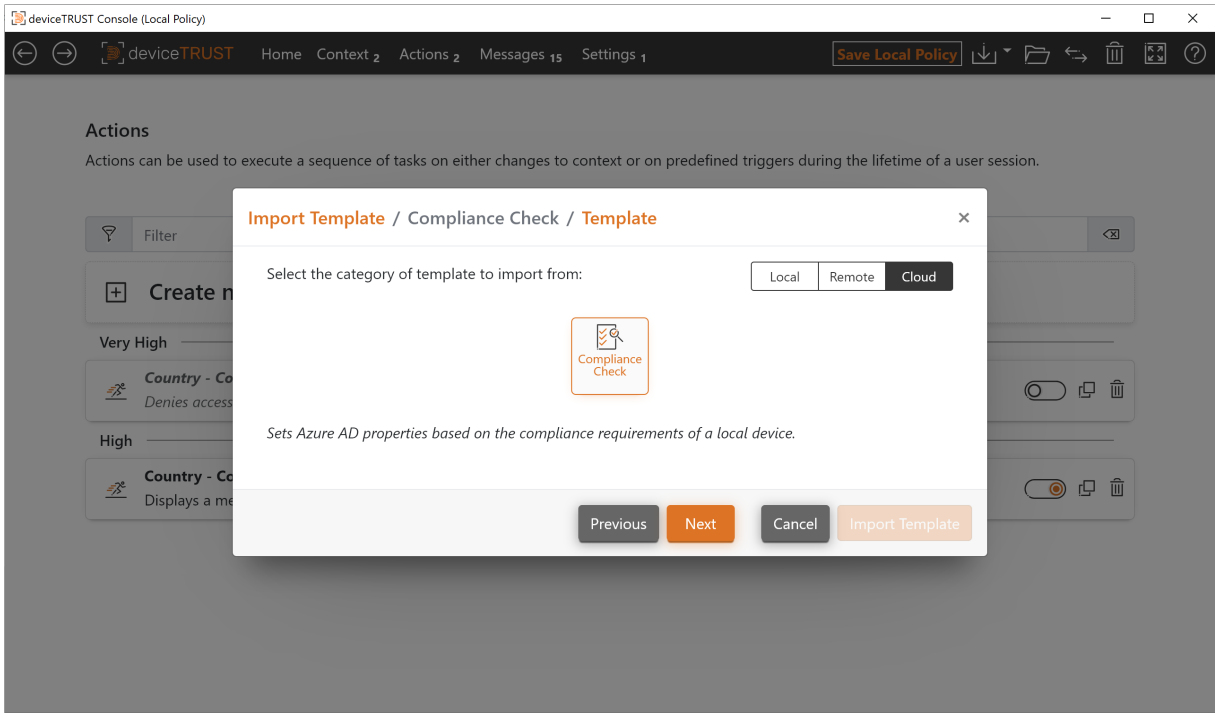


TABLE OF CONTENTS

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

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

Reporting

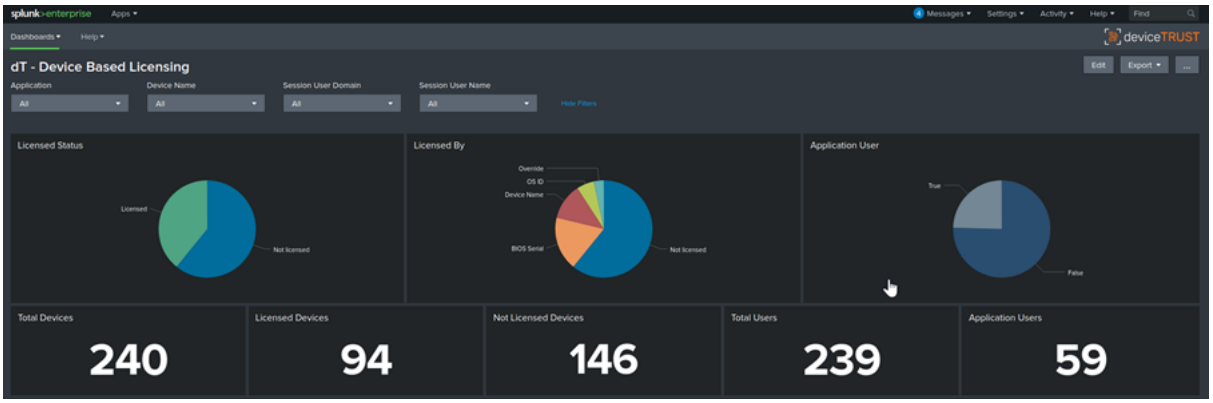
Table of Contents

- Splunk Dashboards
- ELK Stack Dashboards

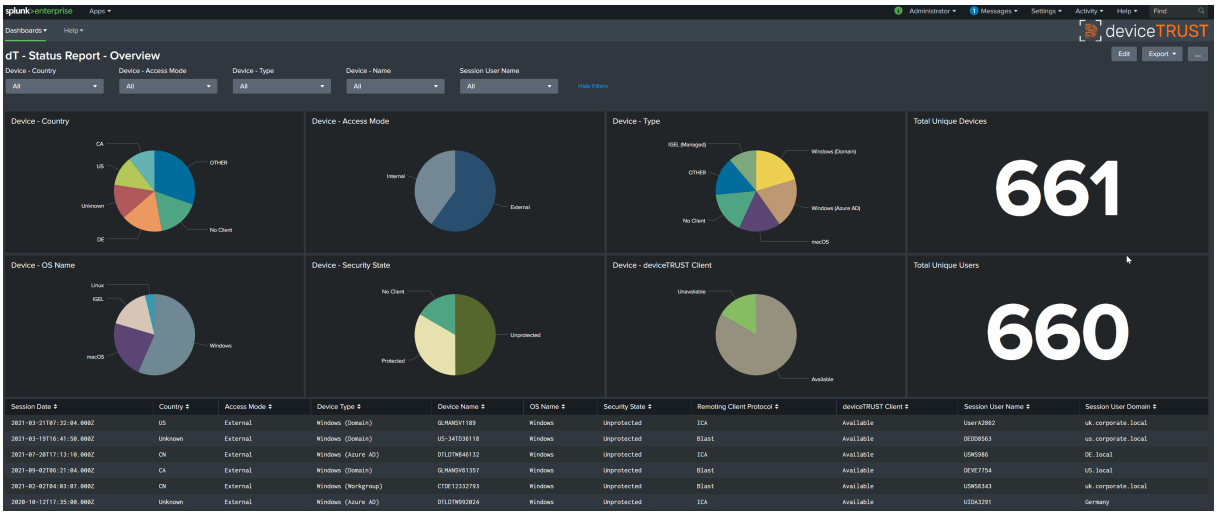
Splunk Dashboards

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

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



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



The following steps will be performed:

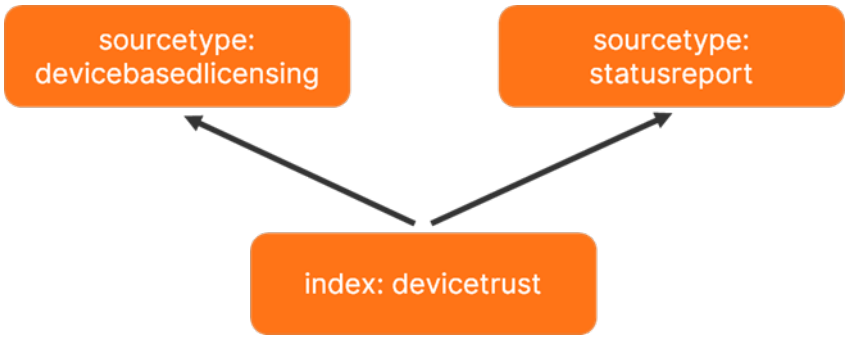
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

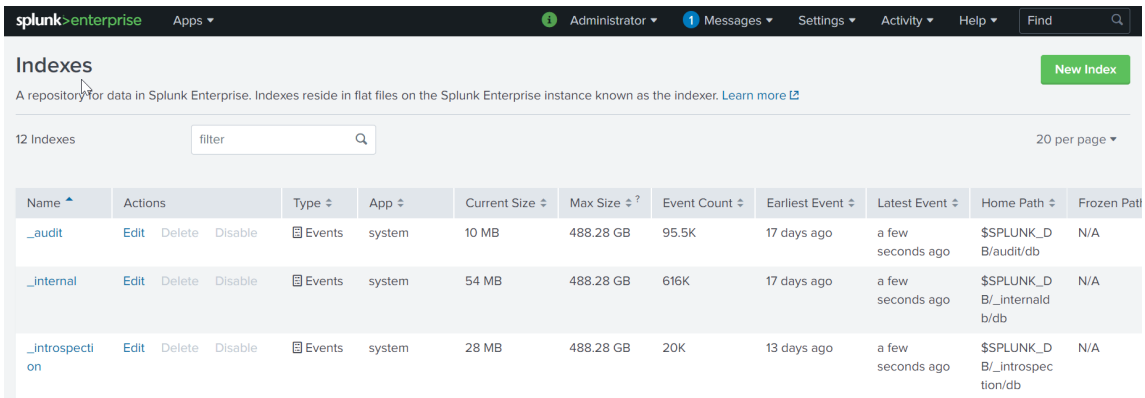


You can either create the index `devicetrust` manually or by importing our prepared app `dt_index`.

Step 1.1: Manually creating the Splunk Index

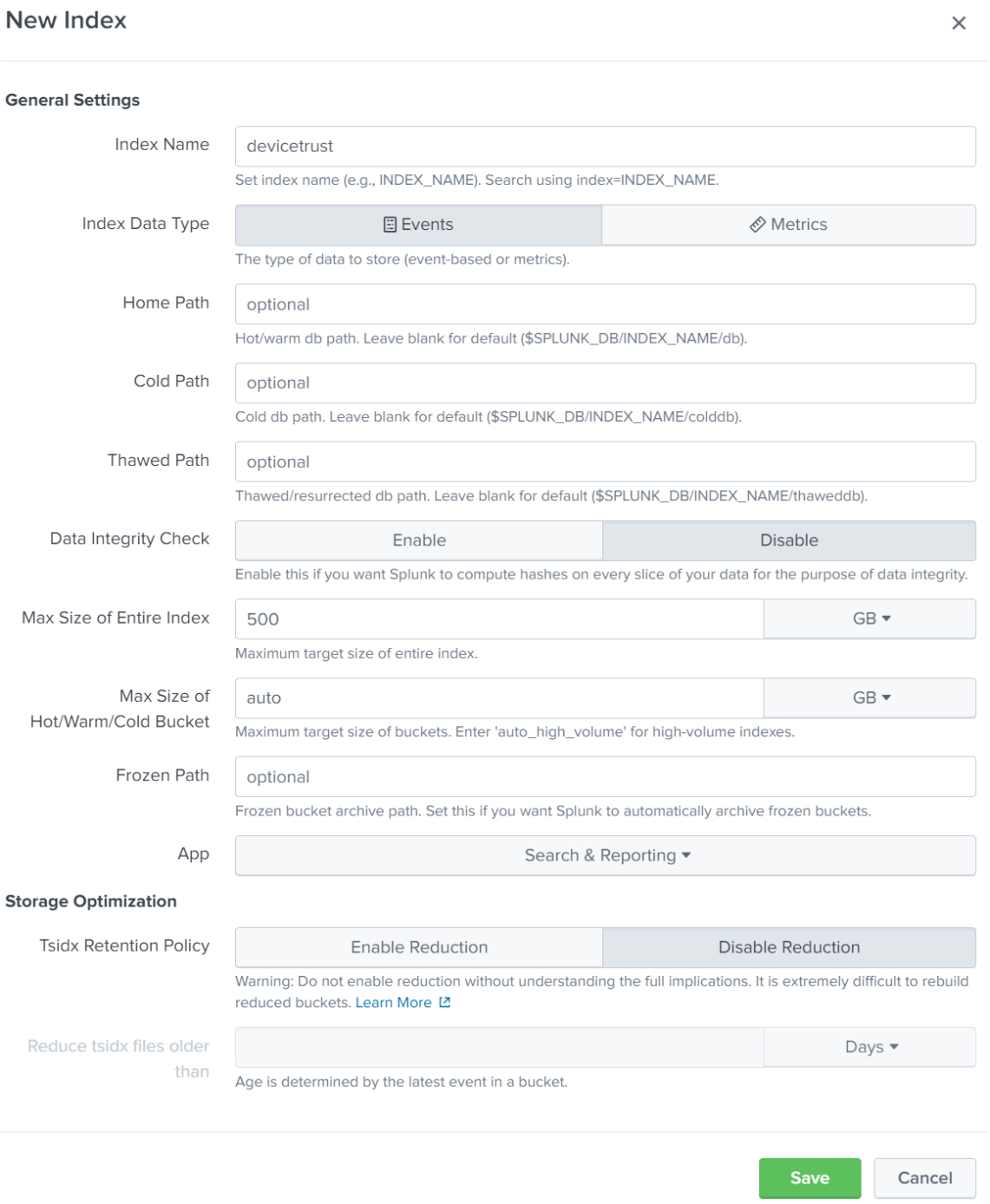
Implementing the index manually does not require any special configuration.

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



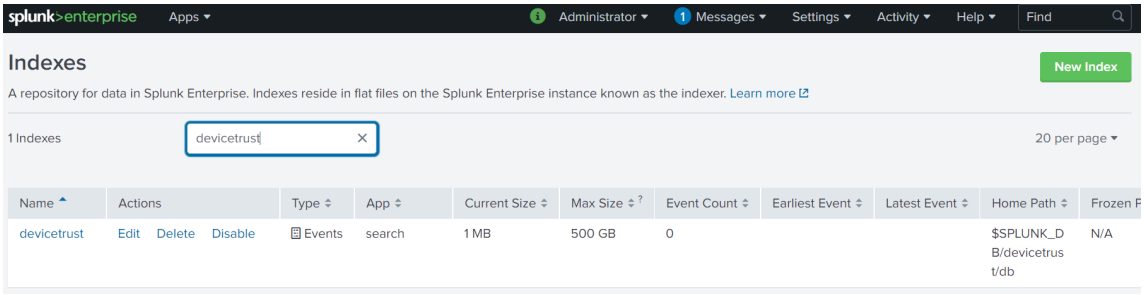
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



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

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



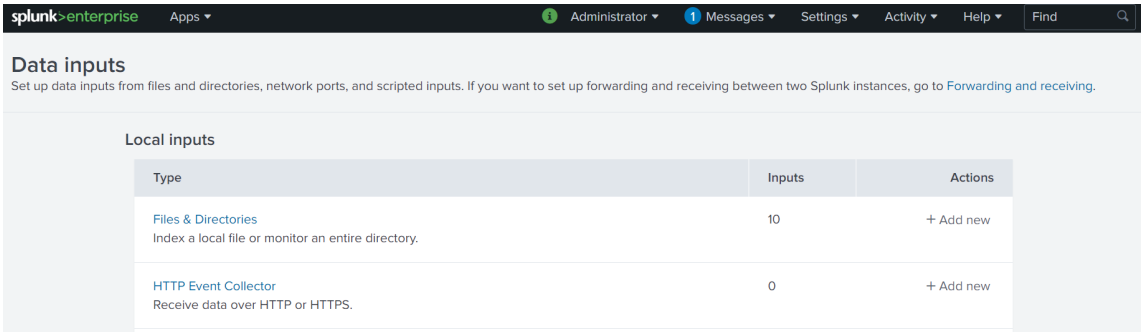
Step 1.2: Creating the Splunk Index by installing the app

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`.

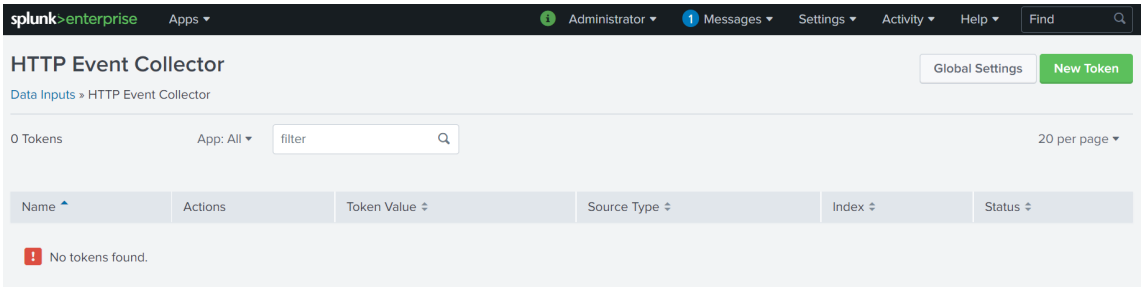
Step 2: Creating the Splunk Data Inputs

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`.



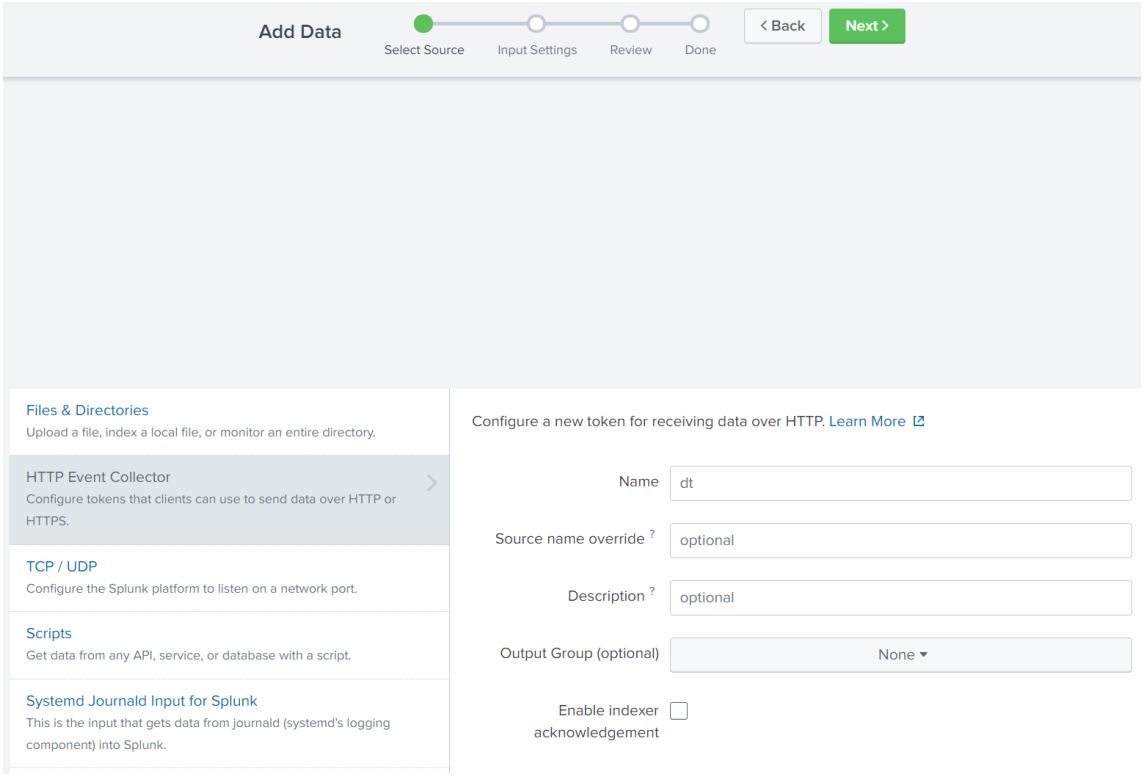
- Select `HTTP Event Collector`
- Click ‘New Token



- Set a `name` of your choice.

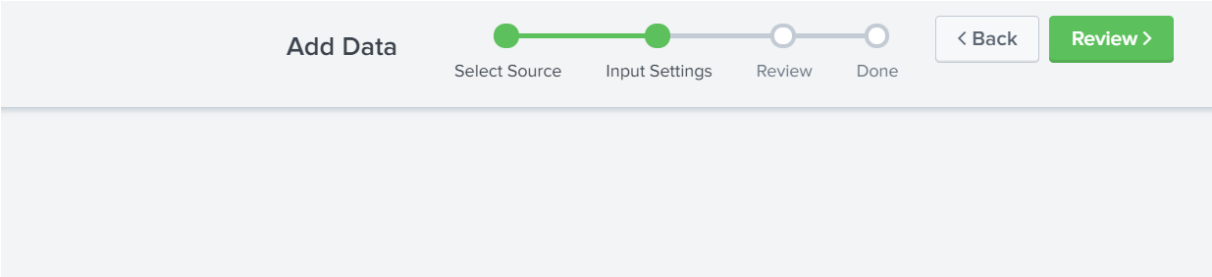
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: App Exporter (app_exporter)

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Select Allowed Indexes

Available item(s) — add all »

- devicetrust
- history
- main
- summary

Selected item(s) « remove all

Select indexes that clients will be able to select from.

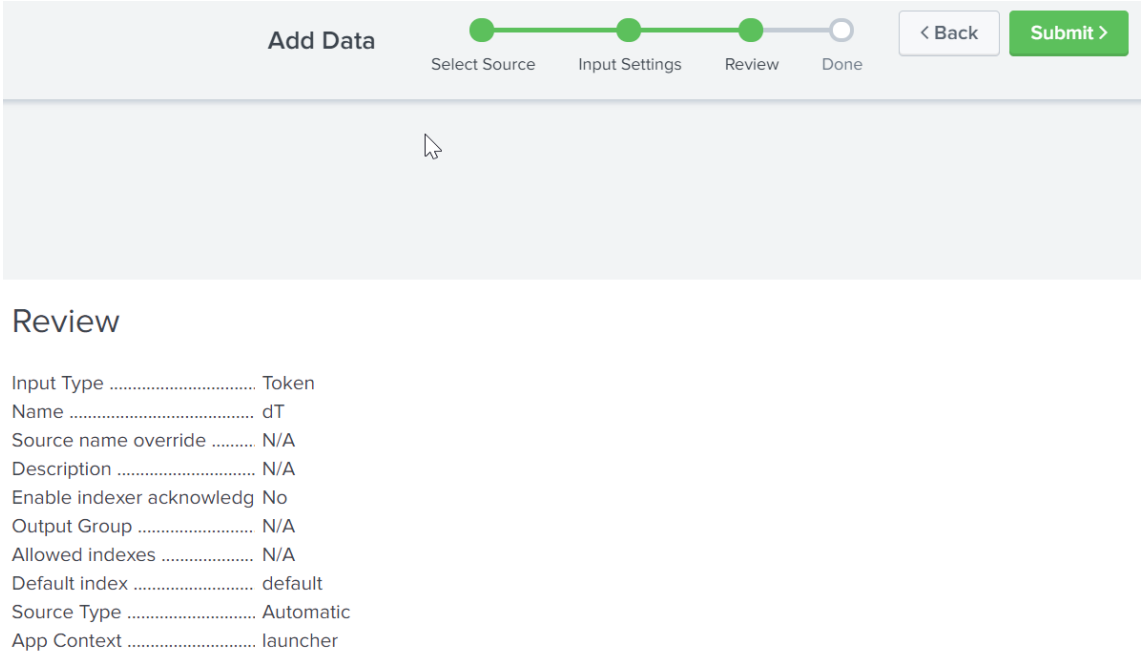
Default Index: Default — Create a new index

FAQ

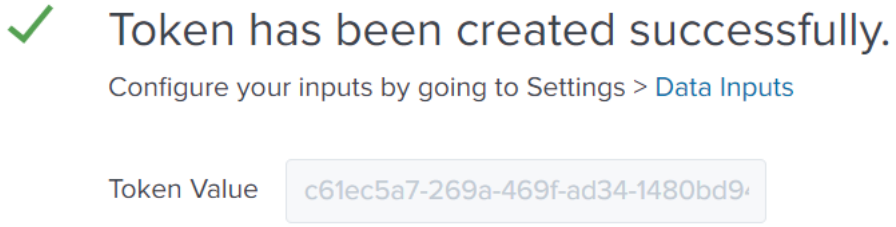
- How do indexes work?
- How do I know when to create or use multiple indexes?

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

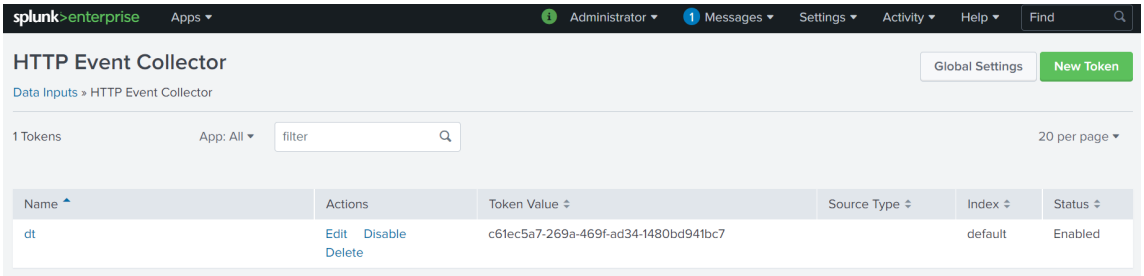
- Review the Settings.
- Click `Submit`.



- The created token is shown.



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

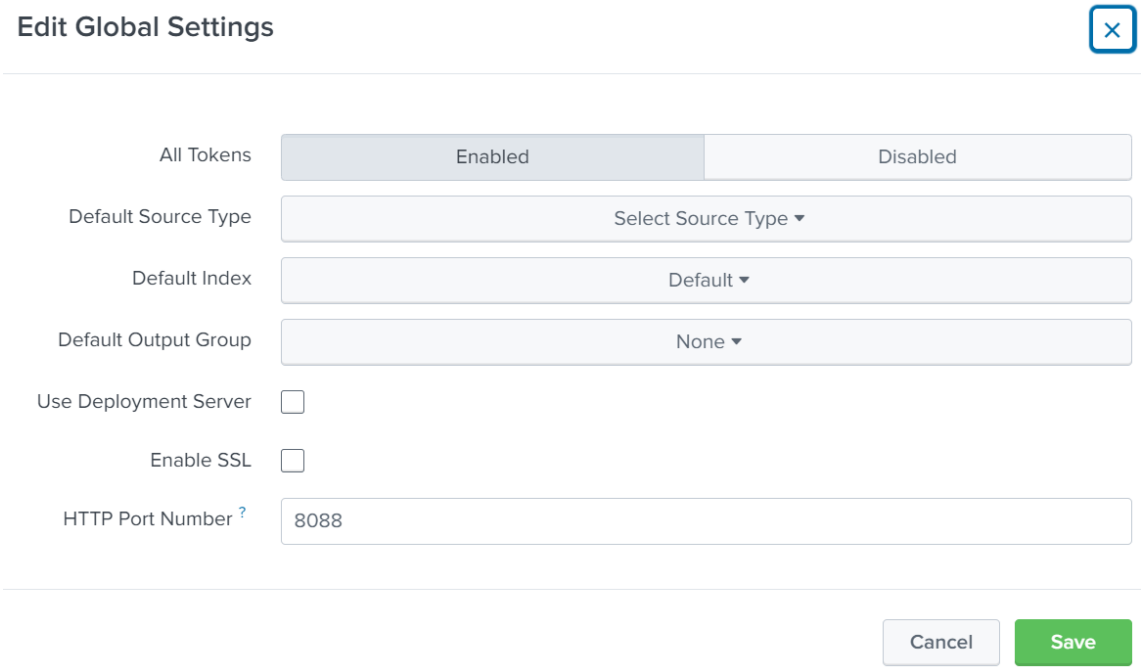


Additionally, the http input method has to be configured. In the most basic configuration, we make sure SSL is not active and all tokens are enabled.

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

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

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



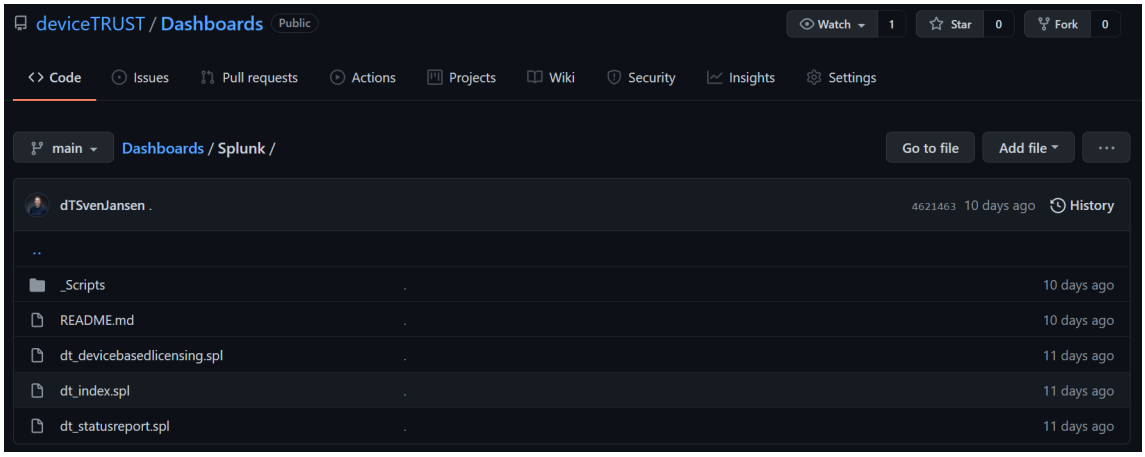
Step 3: Importing the Splunk app

Step 3.1: Downloading the Splunk app

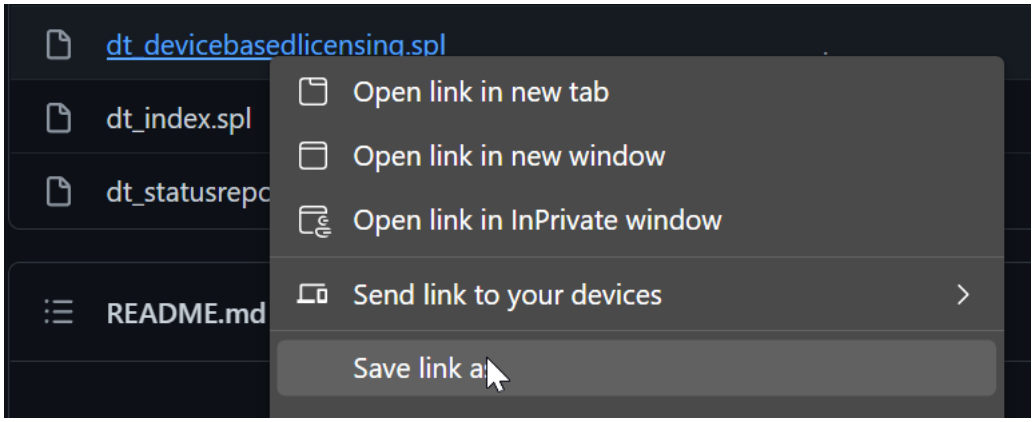
The deviceTRUST reports are delivered as Splunk apps. The apps is available from the deviceTRUST GitHub repository.

- Navigate to the repository and find the Splunk apps.

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



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



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

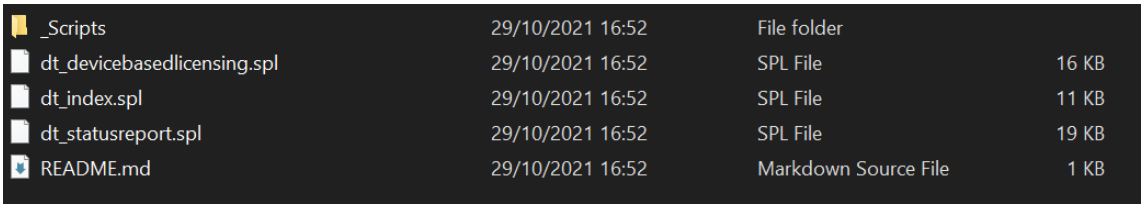
```
PS C:\_Data\GIT> git clone https://github.com/deviceTRUST/Dashboards.git
Cloning into 'Dashboards'...
remote: Enumerating objects: 205, done.
remote: Counting objects: 100% (205/205), done.
remote: Compressing objects: 100% (140/140), done. eceiving objects:  13% (27/205)
remote: Total 205 (delta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


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


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

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

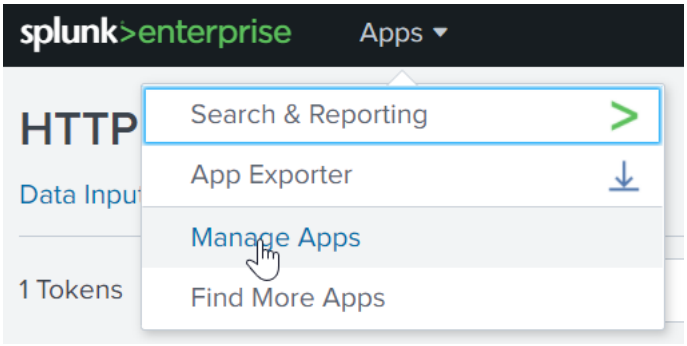
- With the apps available locally, they can be imported into Splunk.



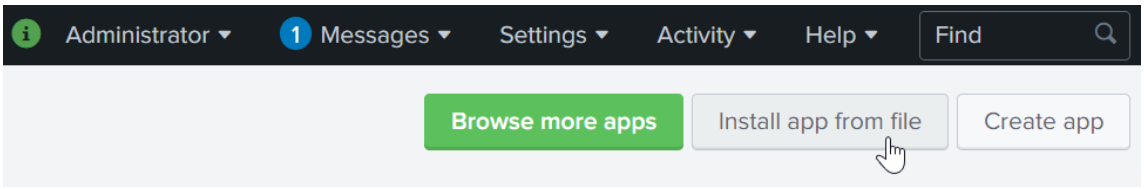
Step 3.2: Installing the Splunk app

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

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

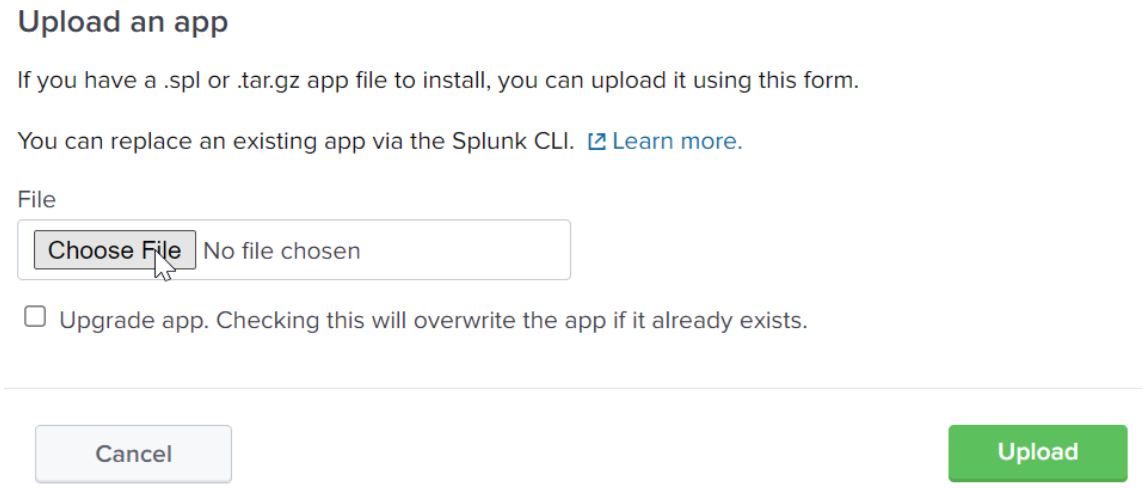


- Click `Install app from file`.

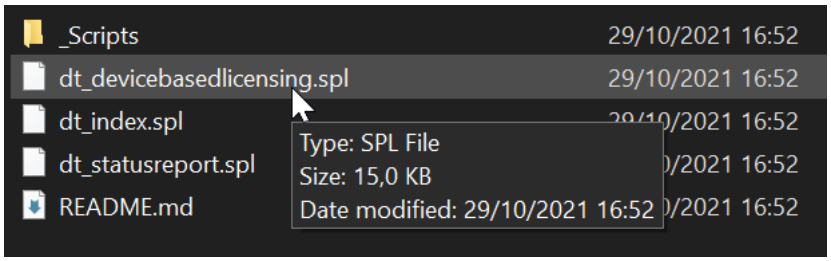


- Click `Choose File`.

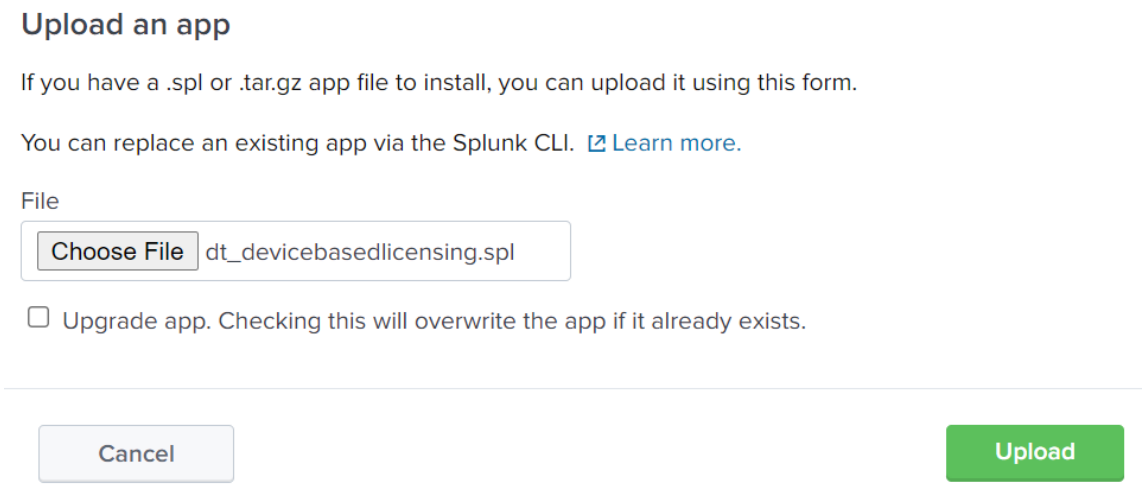
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Select your app file.

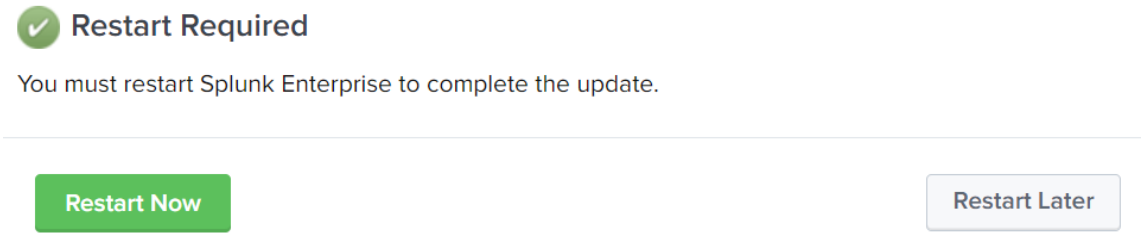


- Confirming your selection.
- Optionally select to upgrade apps, if applicable.
- Click `Upload`.

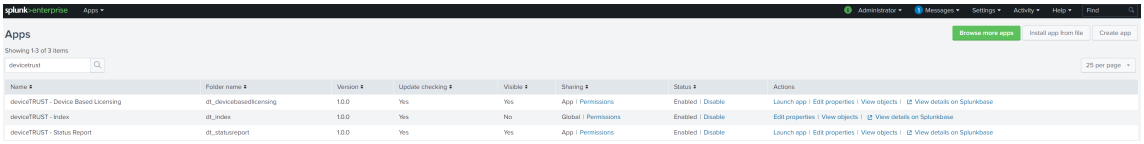


- Splunk will ask to restart the service. This is only required after importing the last app.
- Choose `Restart Now` or `Restart Later` accordingly.

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



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



Step 4: Configuring deviceTRUST

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

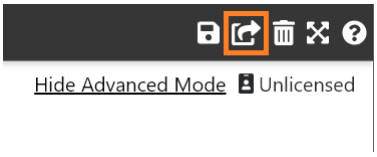
As both reports `Device-Based Licensing` and `Status Report` differ in their details, both are described here separately.

Step 4.1: The Device-Based Licensing Report

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

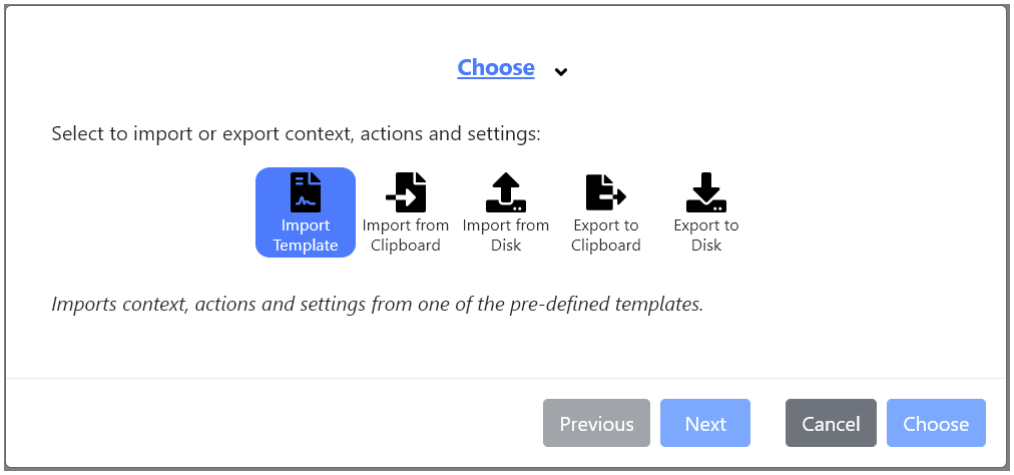
The integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. These five example applications can be easily edited for your own applications, or cloned to represent new applications. The elements are contexts,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

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

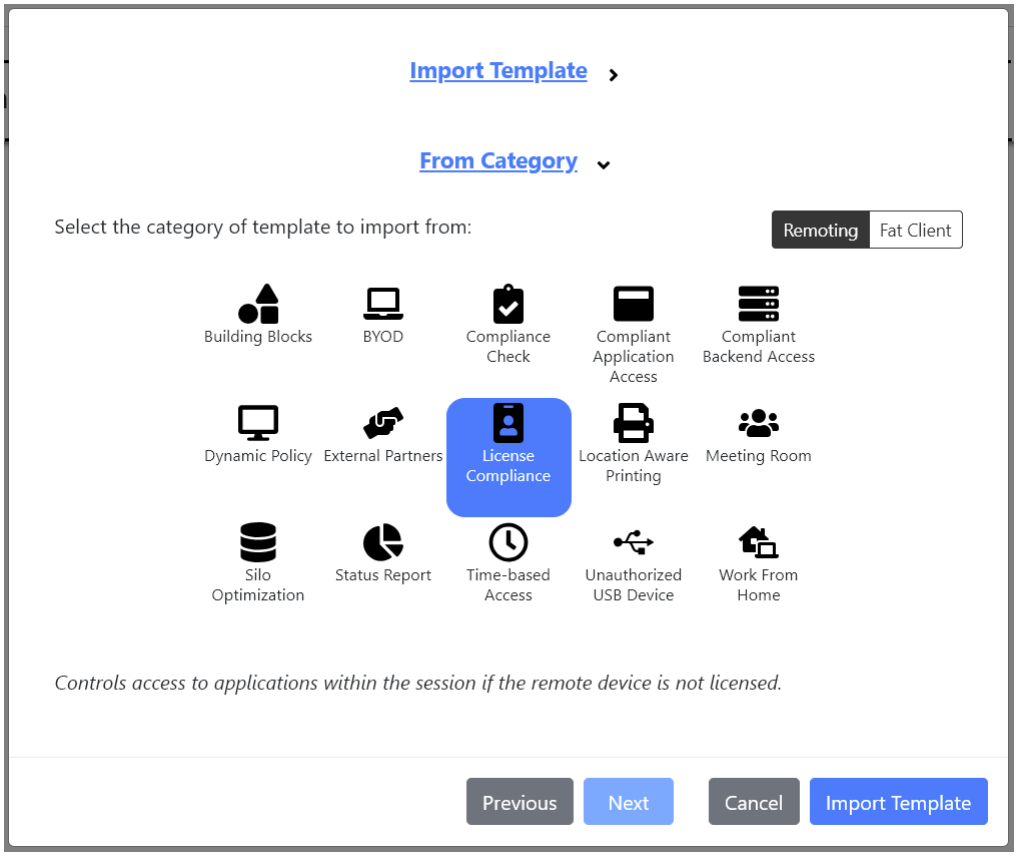


- Select `Import Template`

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

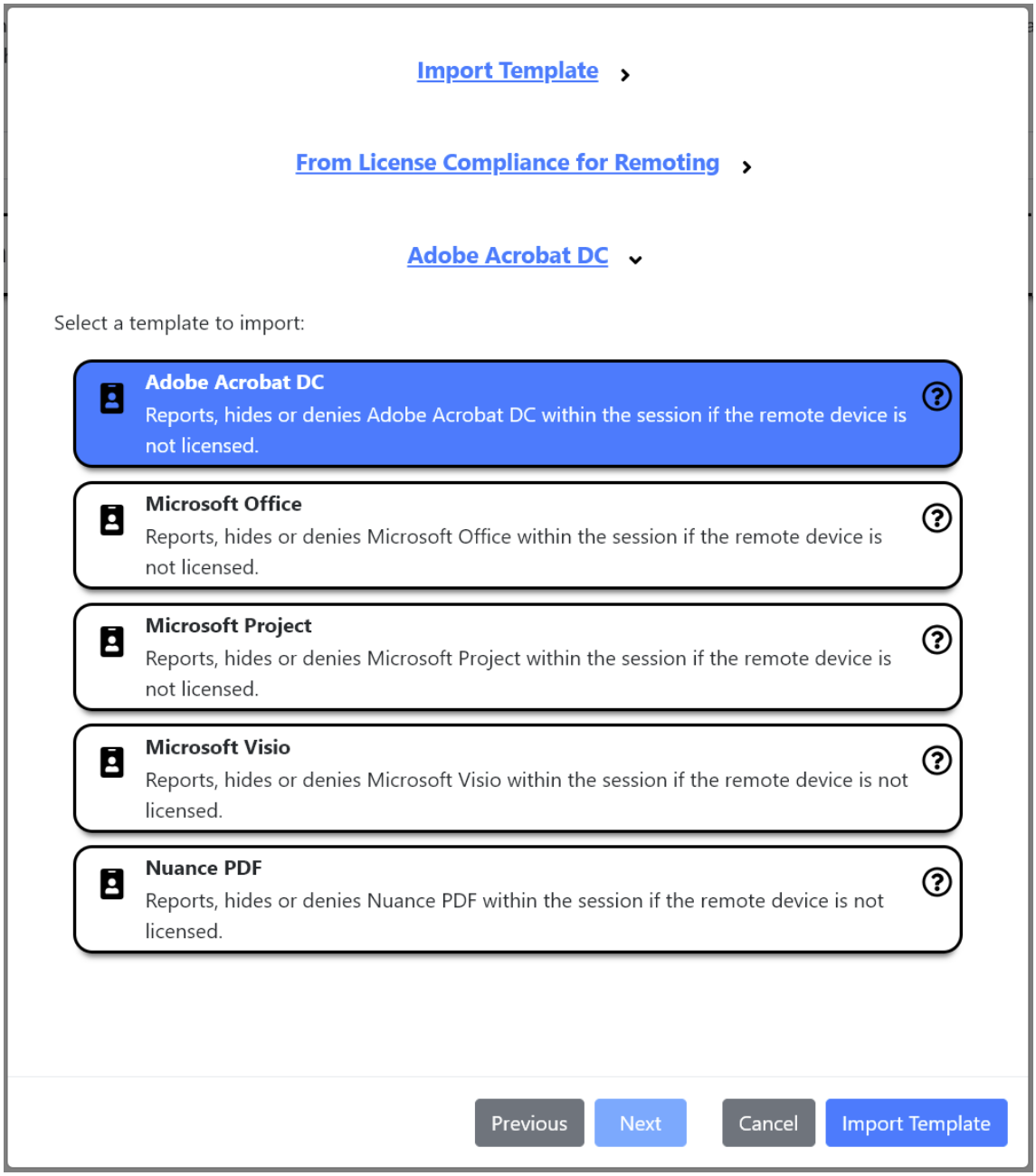


- The report `Device-Based Licensing` can be found within the template category `License Compliance` when `Remoting` is selected.



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

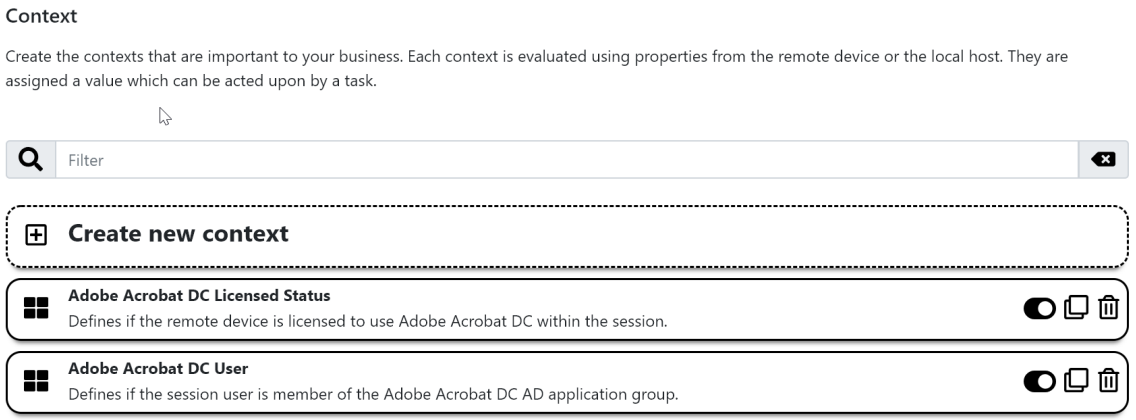
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Two contexts are included within the template:

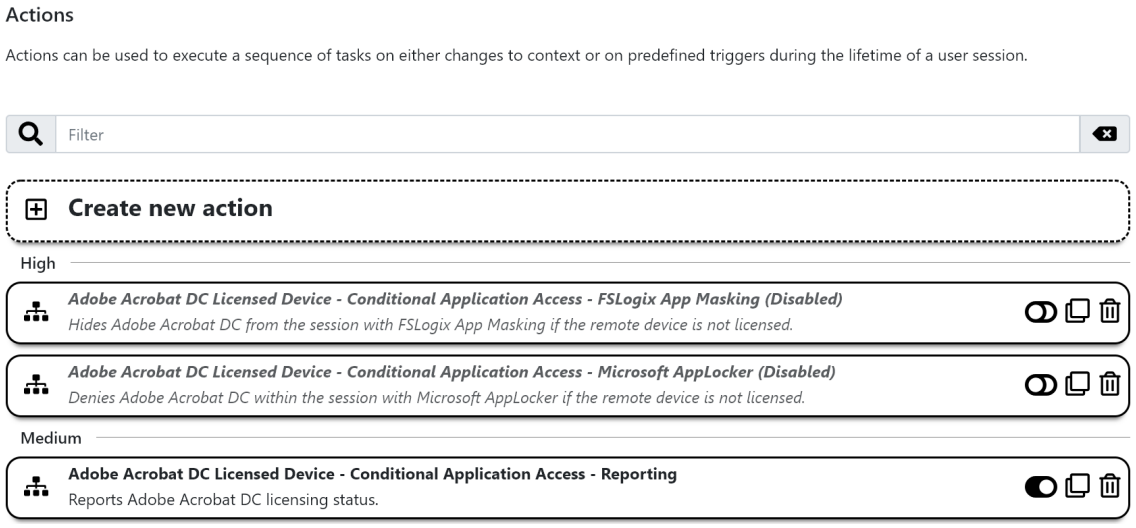
- `Adobe Acrobat DC Licensed Status` to evaluate the device license status.
- `Adobe Acrobat DC User` to define if the accessing user is licensed to use the software.

© 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.

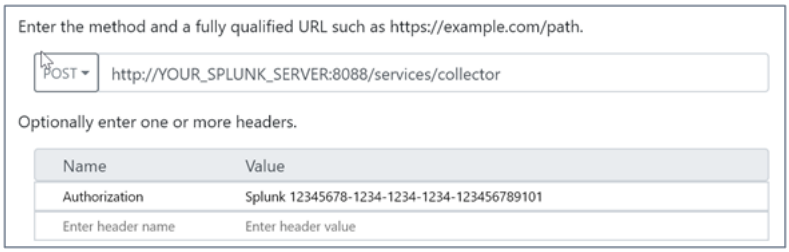
Adobe Acrobat DC Licensed Device - Conditional Application Access - Reporting

Reports Adobe Acrobat DC licensing status.

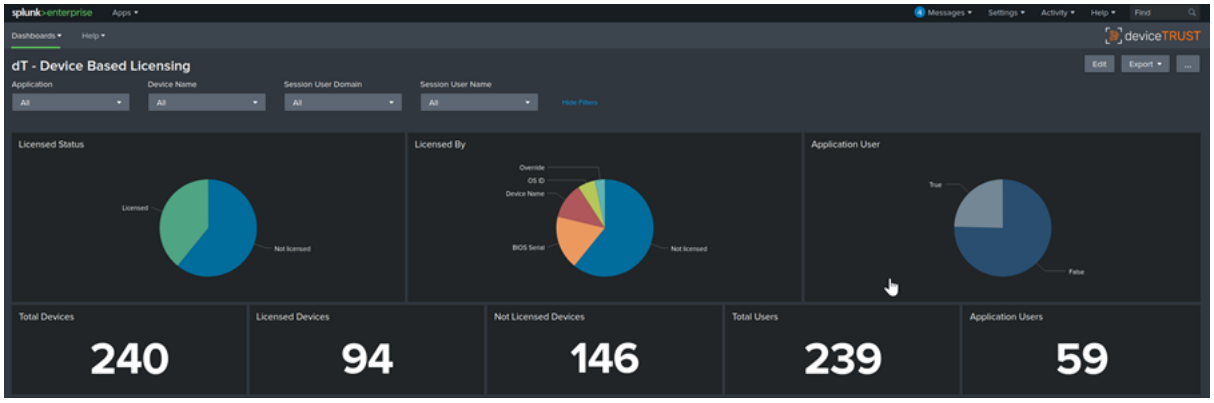


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



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

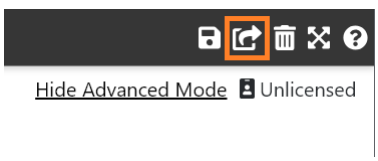


Step 4.2: The Status Report

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

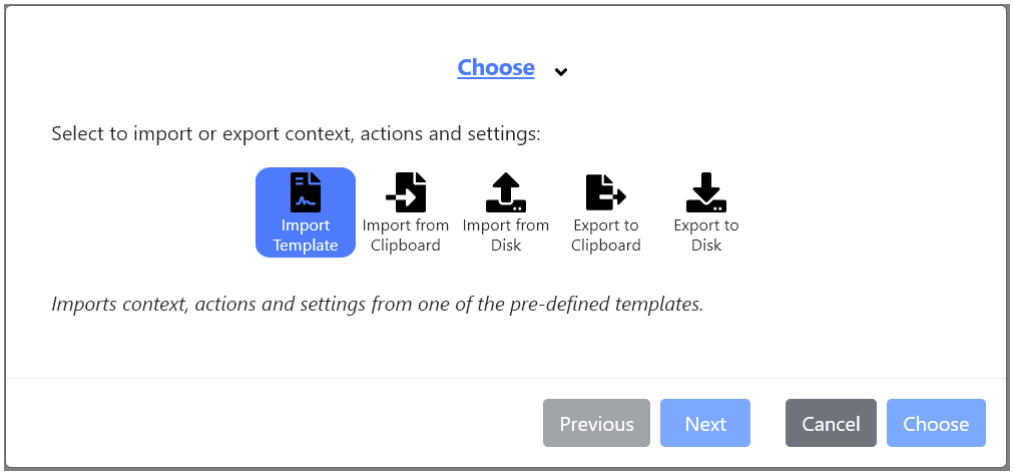
Our integrated templates contain all elements that are required to fully configure the agent for the Device-Based Licensing of five example applications. The elements are contexts, actions, messages and settings.

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

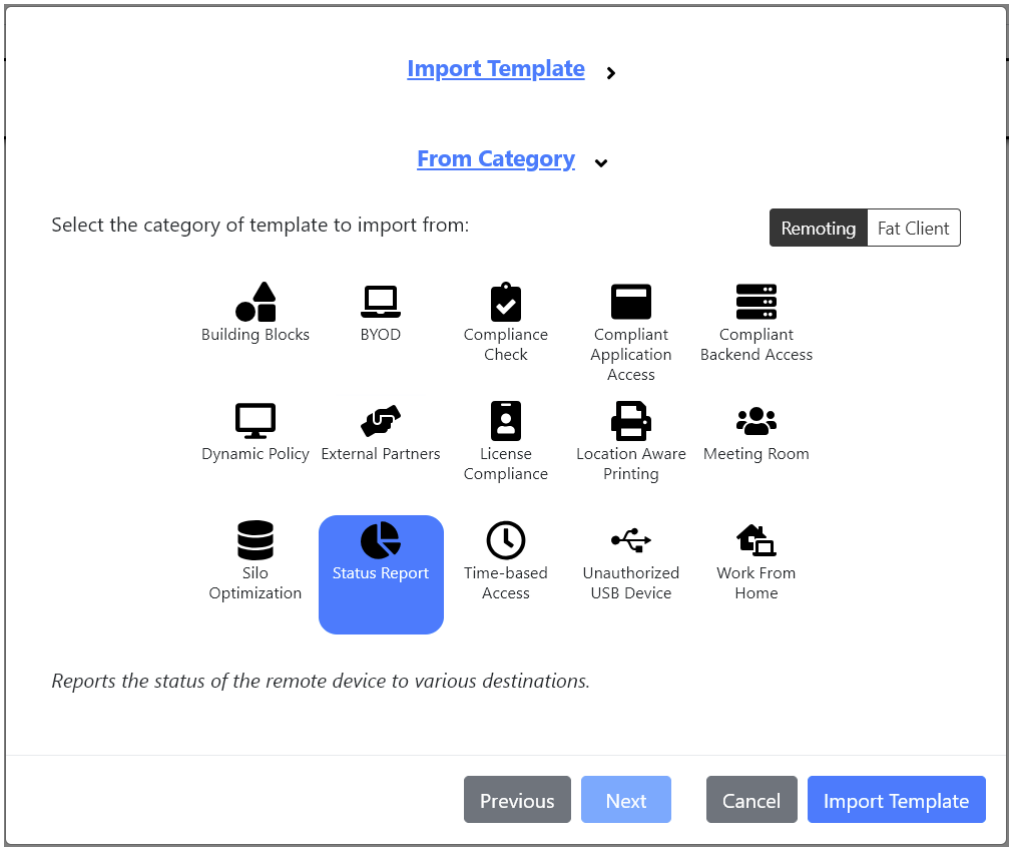


- Select `Import Template`

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

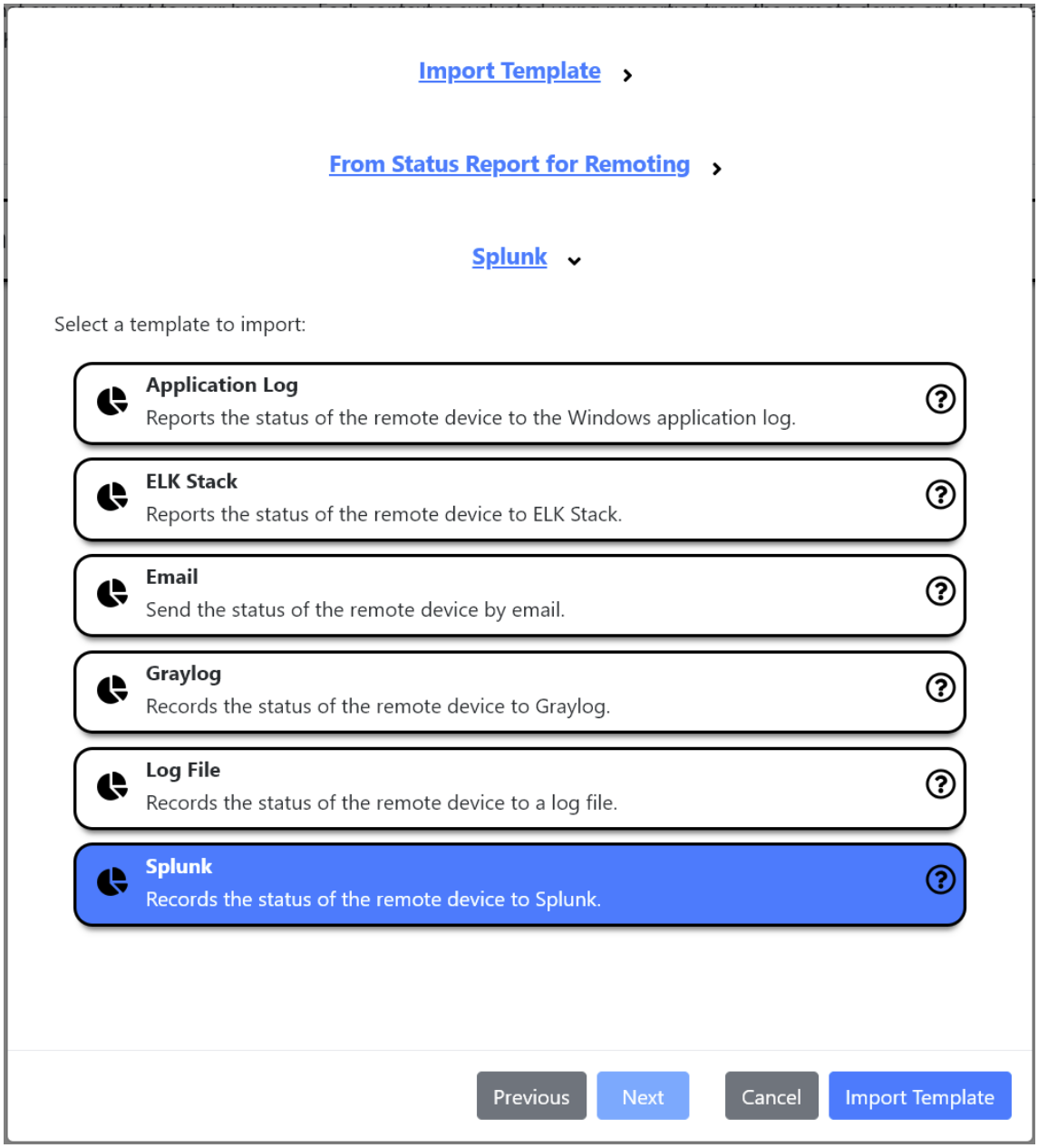


- The `Status Report` template can be found within the template category `Status Report` when `Remoting` is selected.



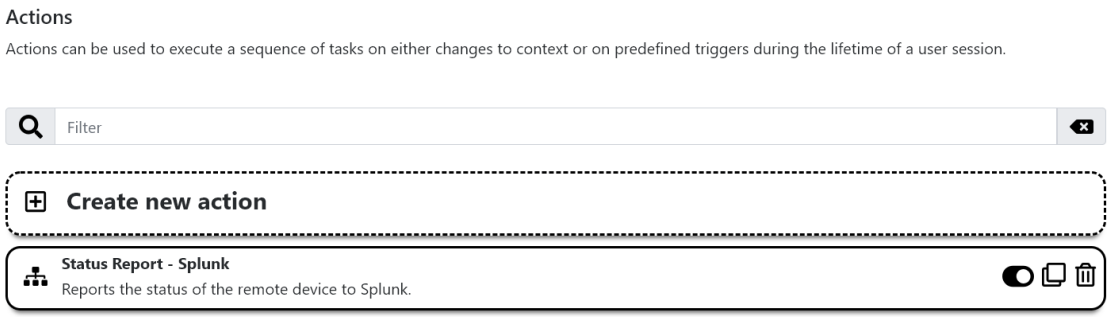
- This category contains templates for several ways of storing data. Choose `Splunk`.

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

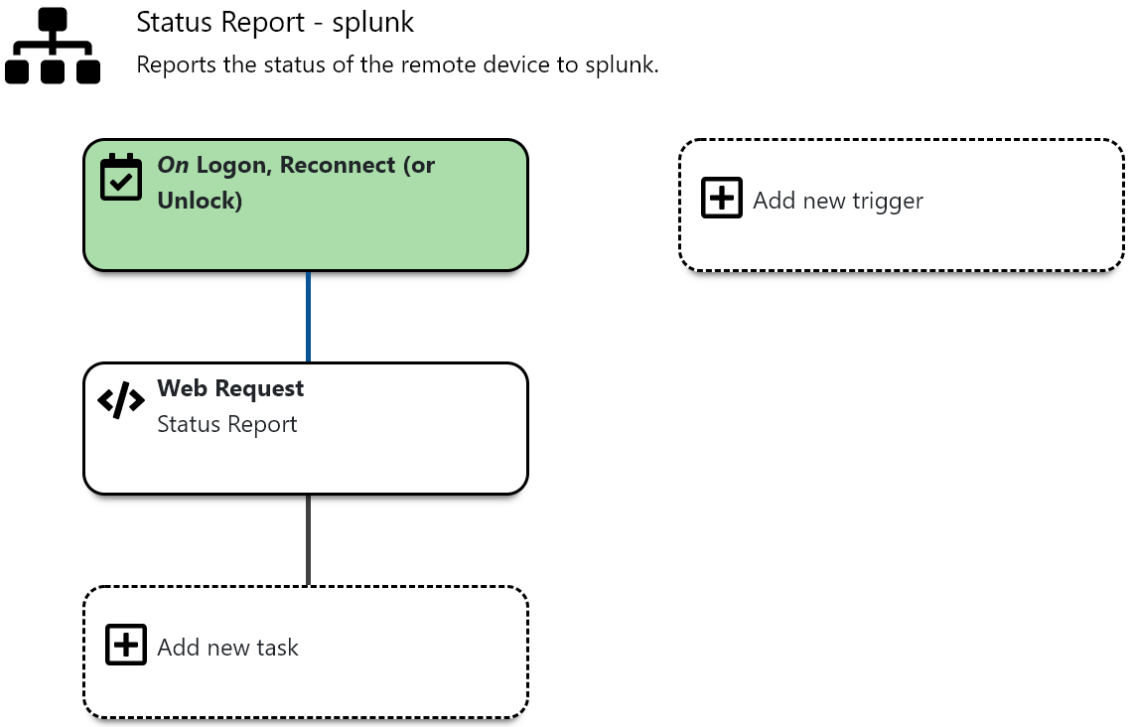


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – Splunk` collects all relevant data and sends them over to Splunk.

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

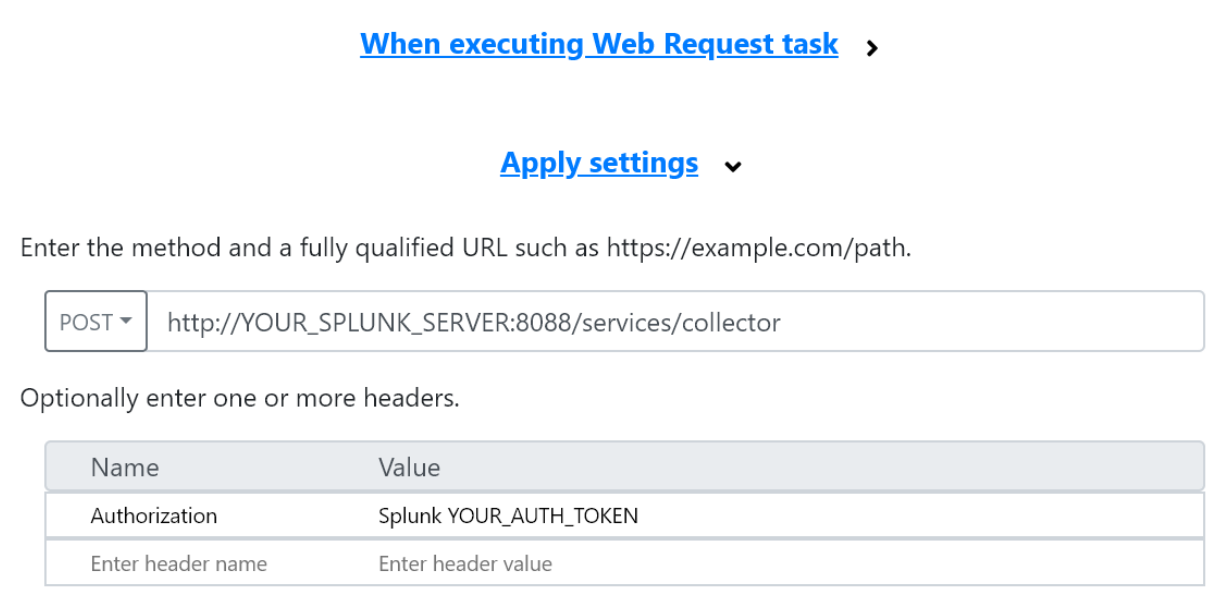


- Sending data to Splunk is configured by using a `Web Request` task.

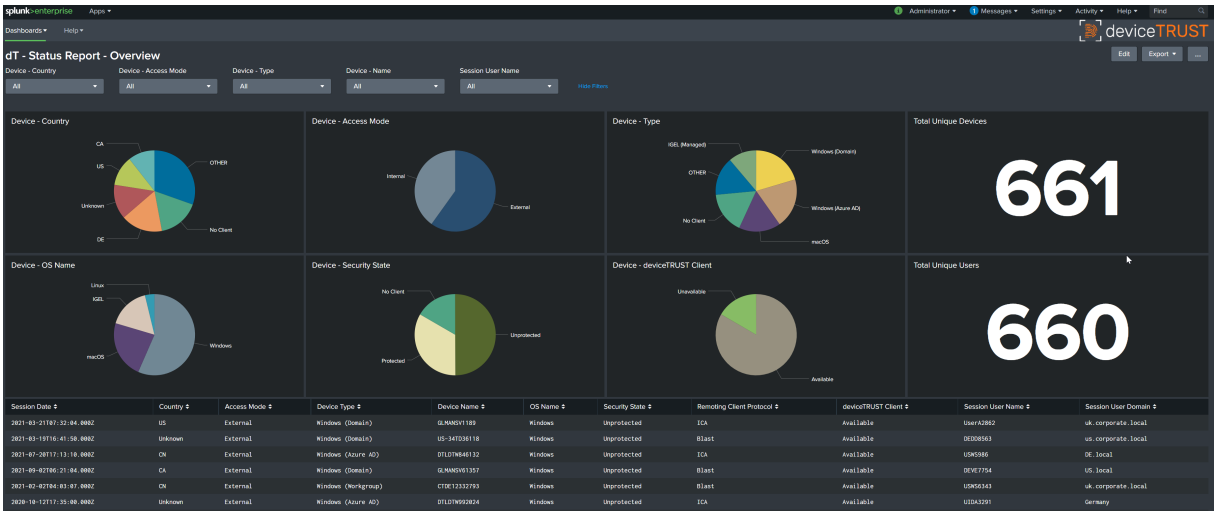


The Web Request task needs to be edited to suit your environment. If you do not require SSL transport, you'll only have to configure your `server's fqdn` and the `authorization token` (http data input). Make sure to leave the keyword `splunk` and only change your authorization token's GUID.

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



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

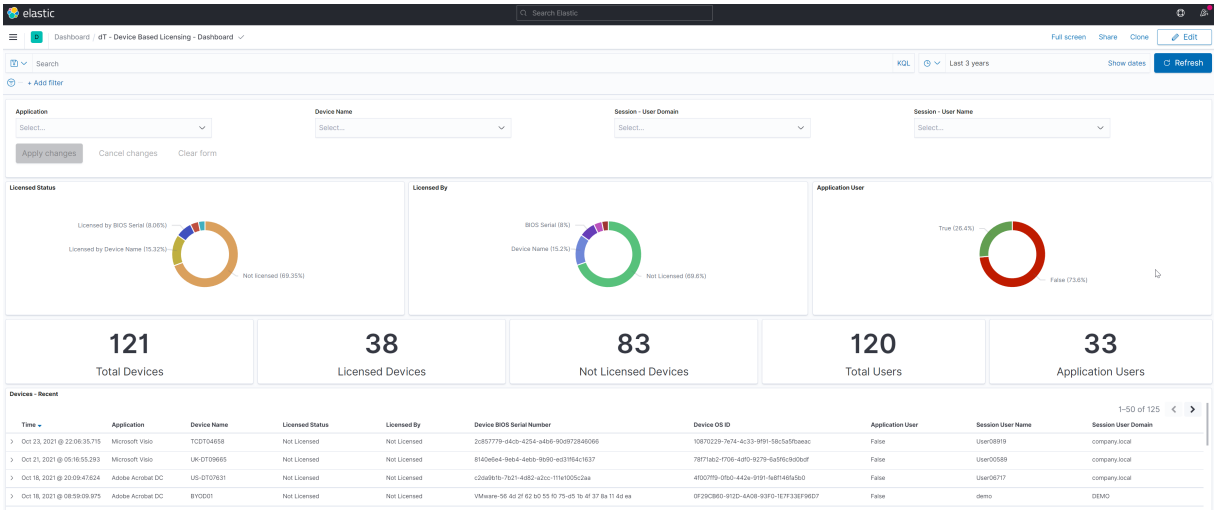


ELK Stack Dashboards

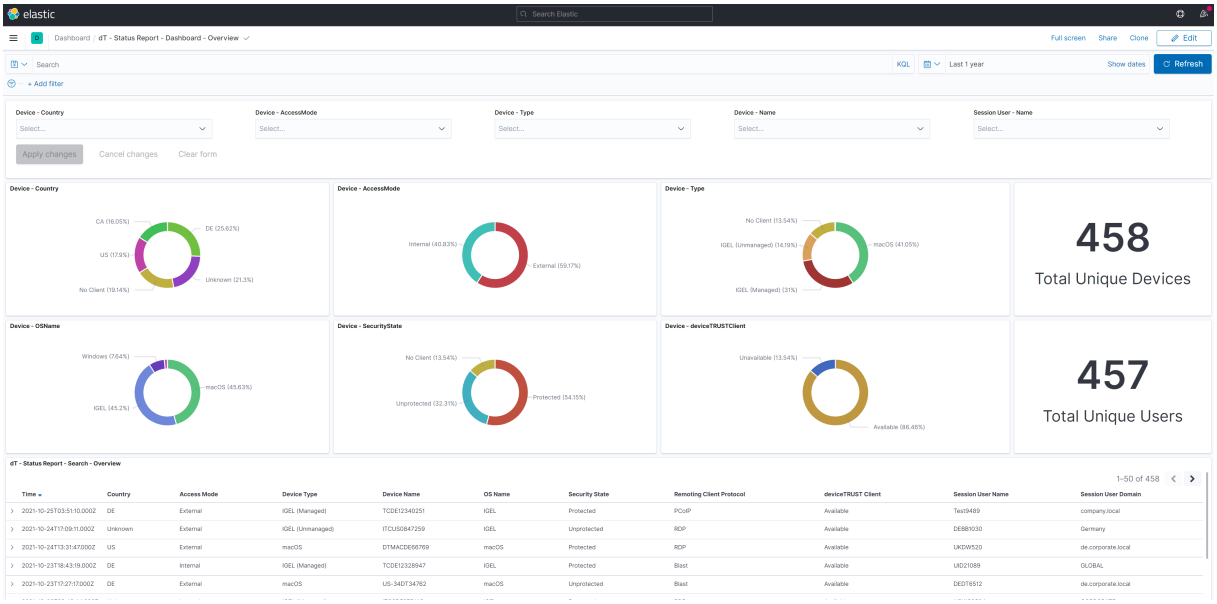
deviceTRUST® includes components for an ELK Stack to easily create a dashboard to monitor the contextual status of your remoting and DaaS environment.

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

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



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



Step 1: Components

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

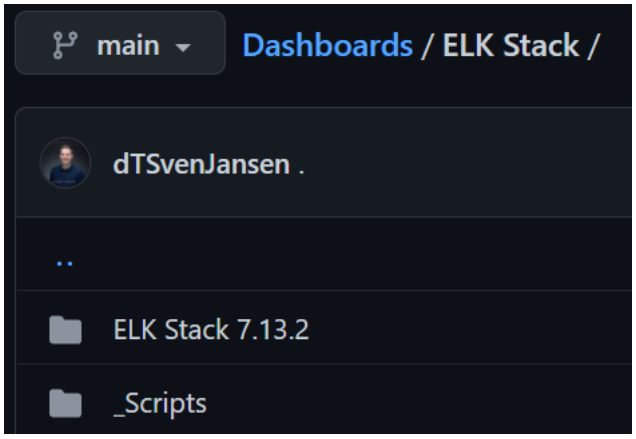
Step 1.1: Components - GitHub

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

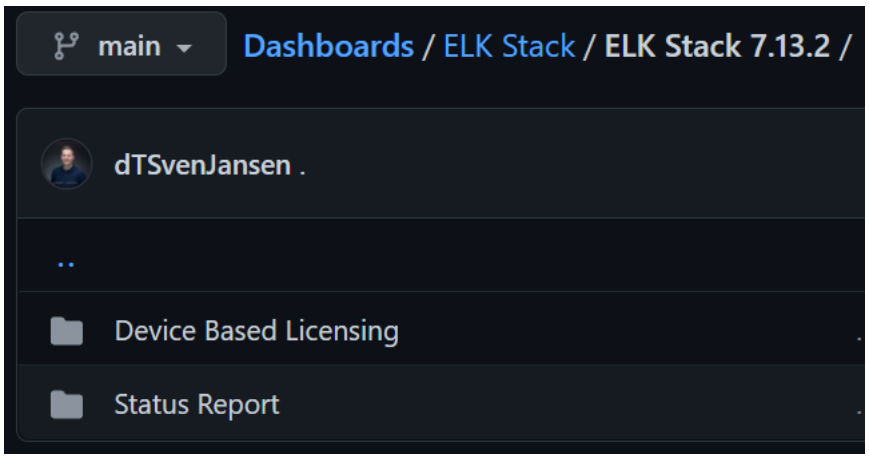
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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



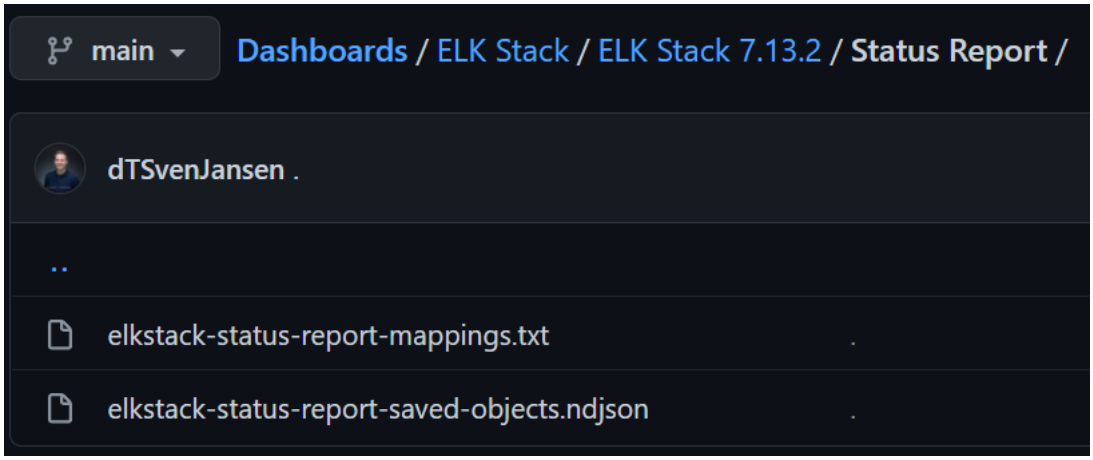
  Every version folder contains folders for each use case. Each of these use case folders contains the relevant stored object and mapping files.



Each use case folder contains the following files:

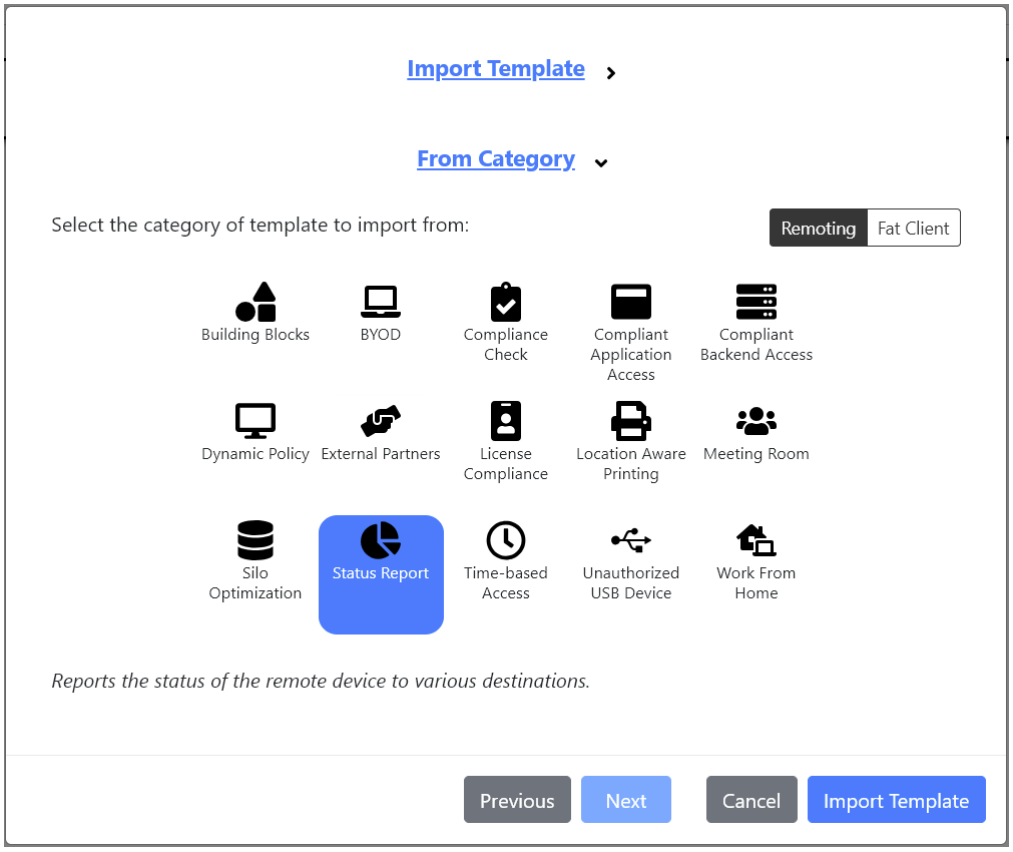
- `elkstack-<use case>-mappings.txt` contains data definitions for the data being sent to ELK Stack index mapping.
- `elkstack-<use case>-saved-objects.ndjson` contains all objects that are required to store, search and visualize data, such as indexes, scripted fields, dashboards and searches.

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



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.

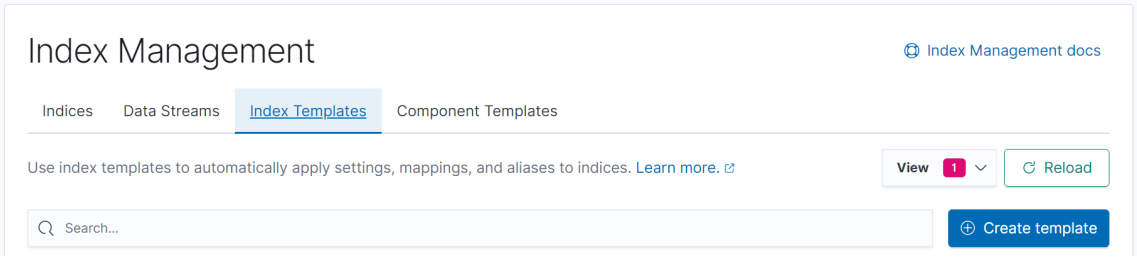
Step 2: The Device-Based Licensing Report

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.

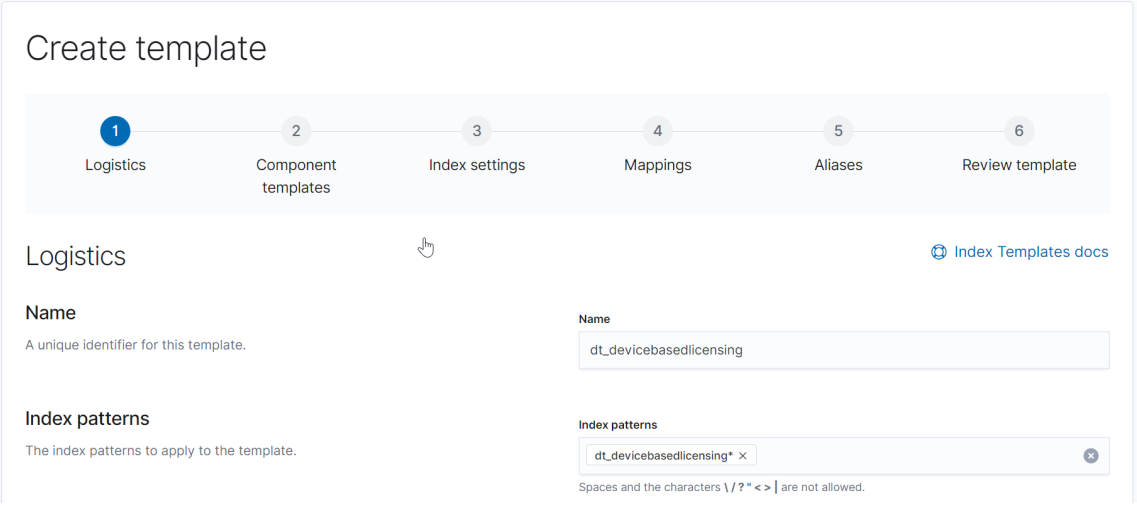
Step 2.1: Add Index Template to ELK Stack

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`.

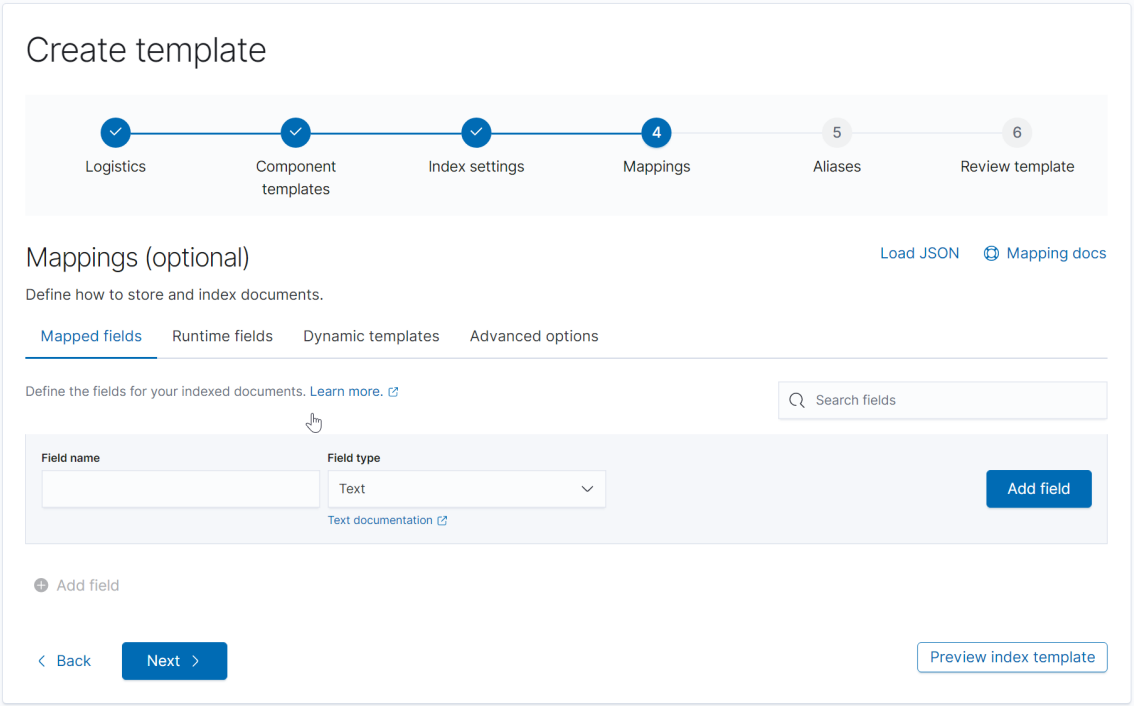


- Set `Name` to `dt_devicebasedlicensing`.
- Set `Index Patterns` to `dt_devicebasedlicensing*`.



- 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`.

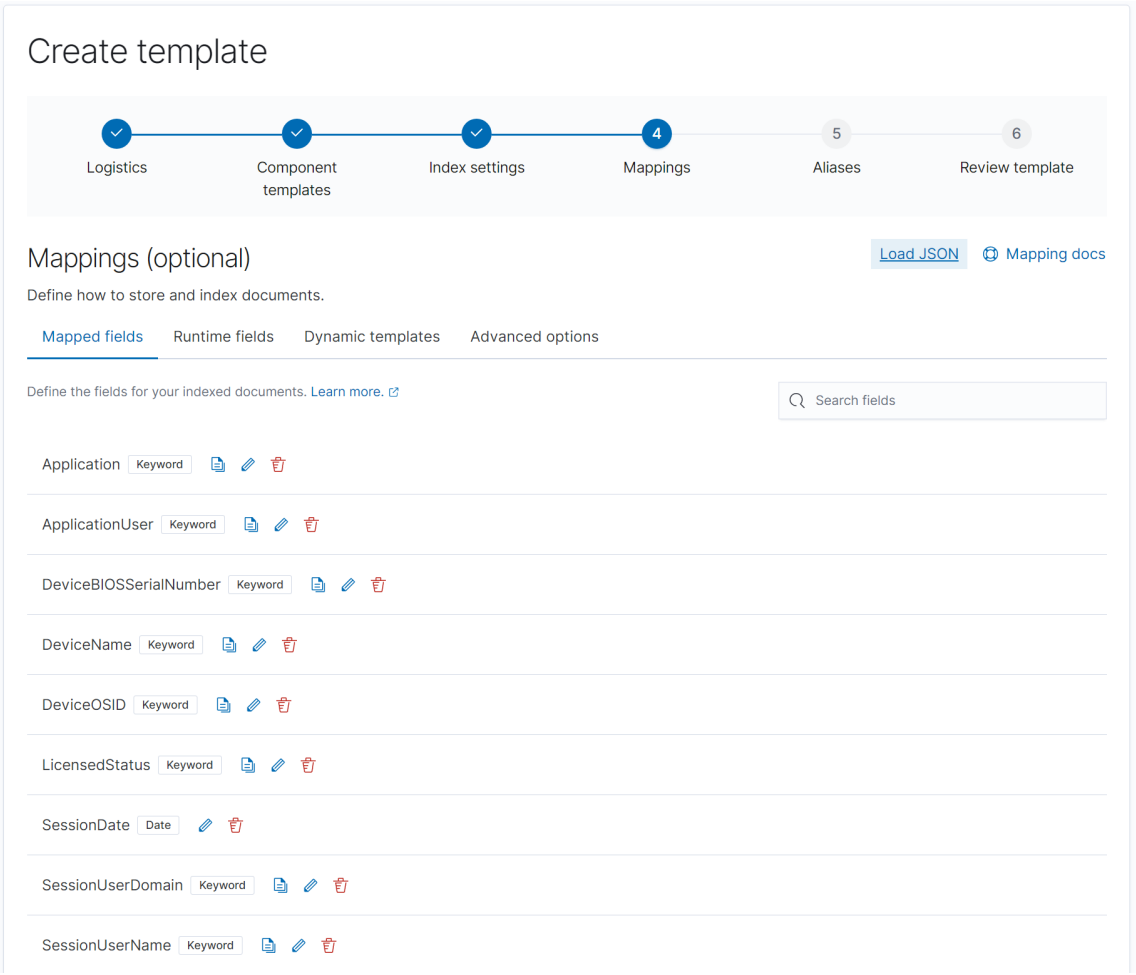
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The imported mappings are displayed. Please review them carefully.

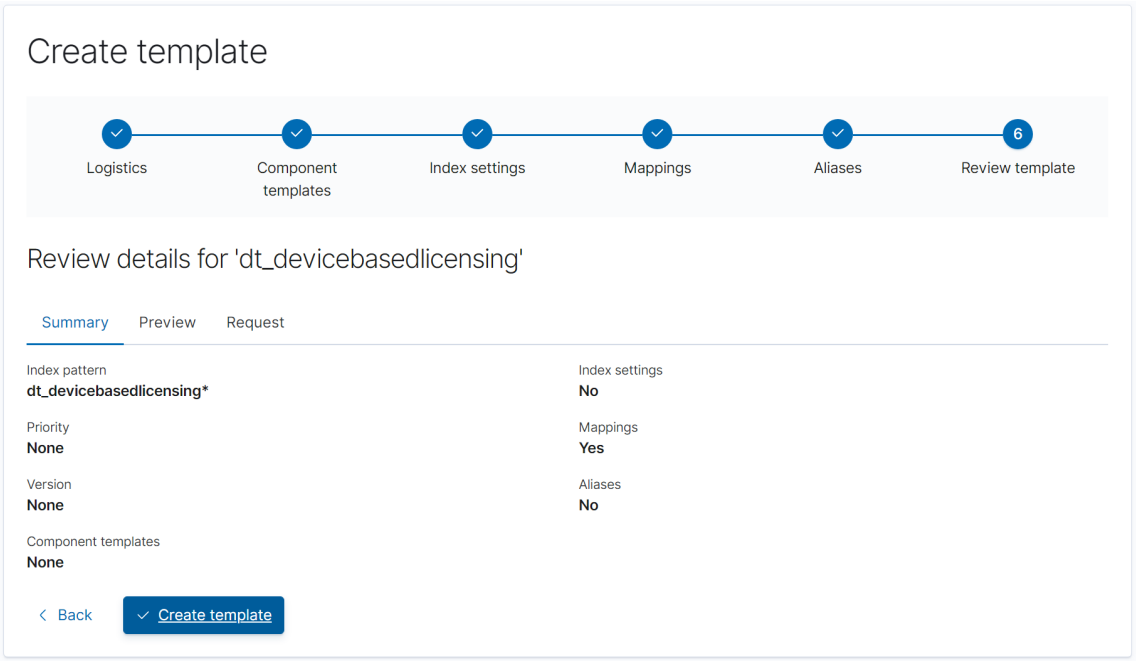
- `SessionDate` needs to be recognized as type `Date` for the report to function properly.

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

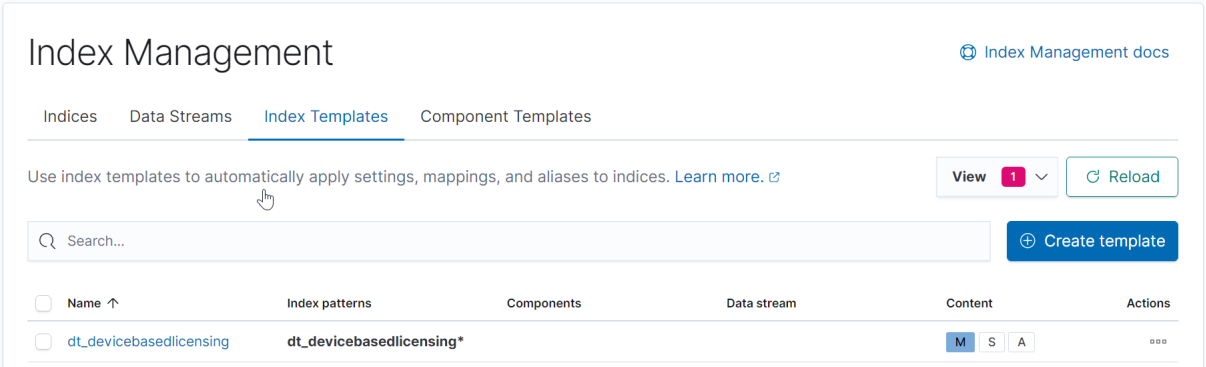


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.

© 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.

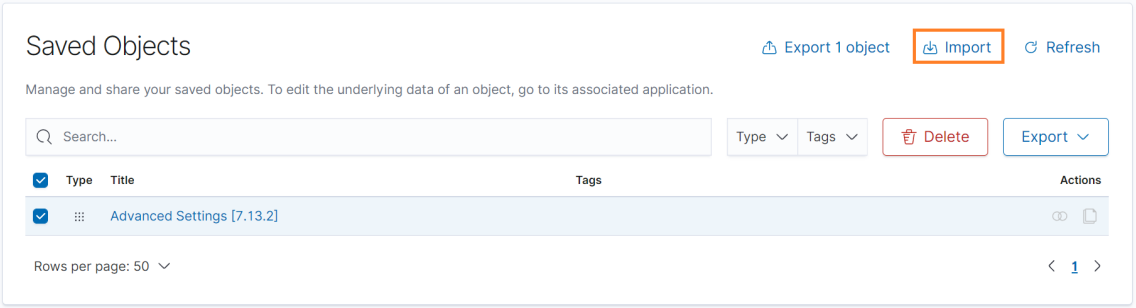


Step 2.2: Import Saved Objects to ELK Stack

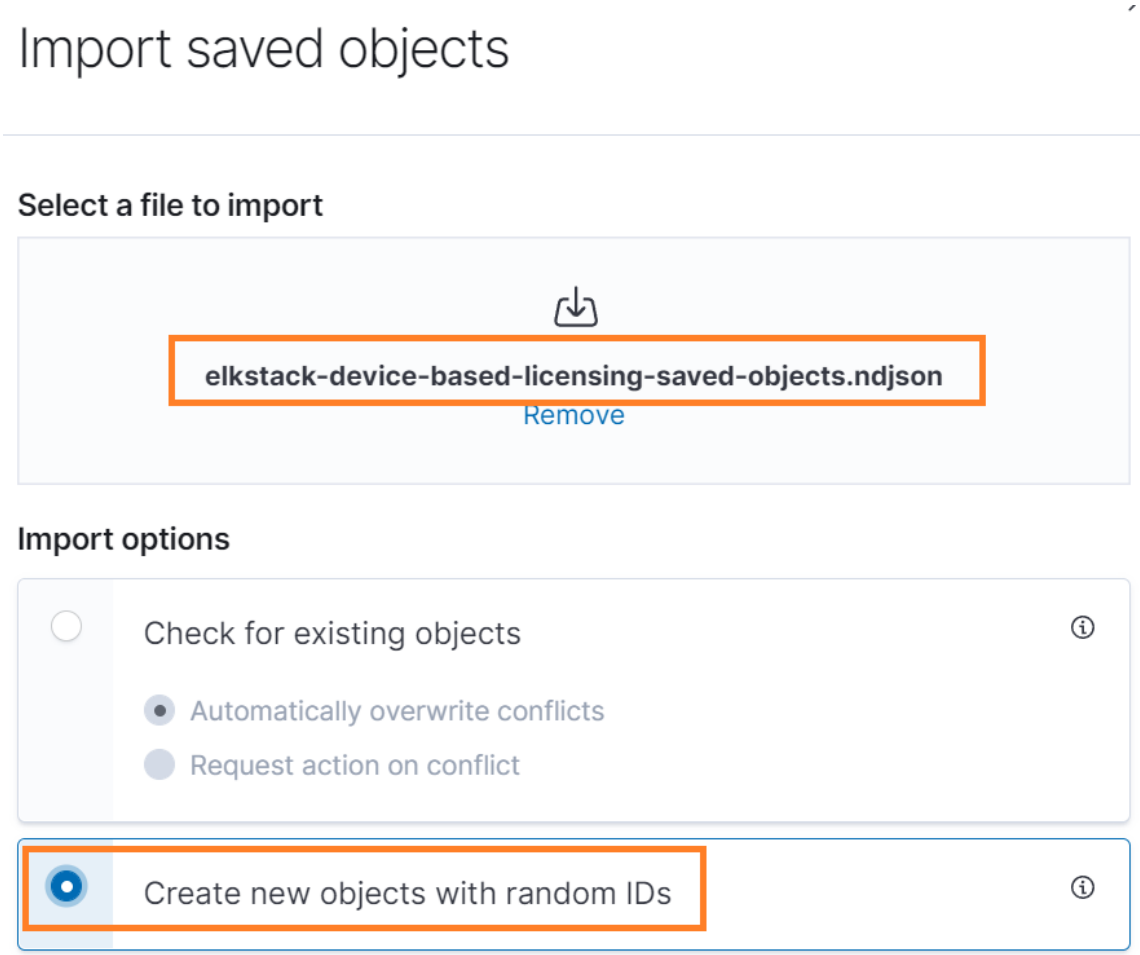
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

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

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

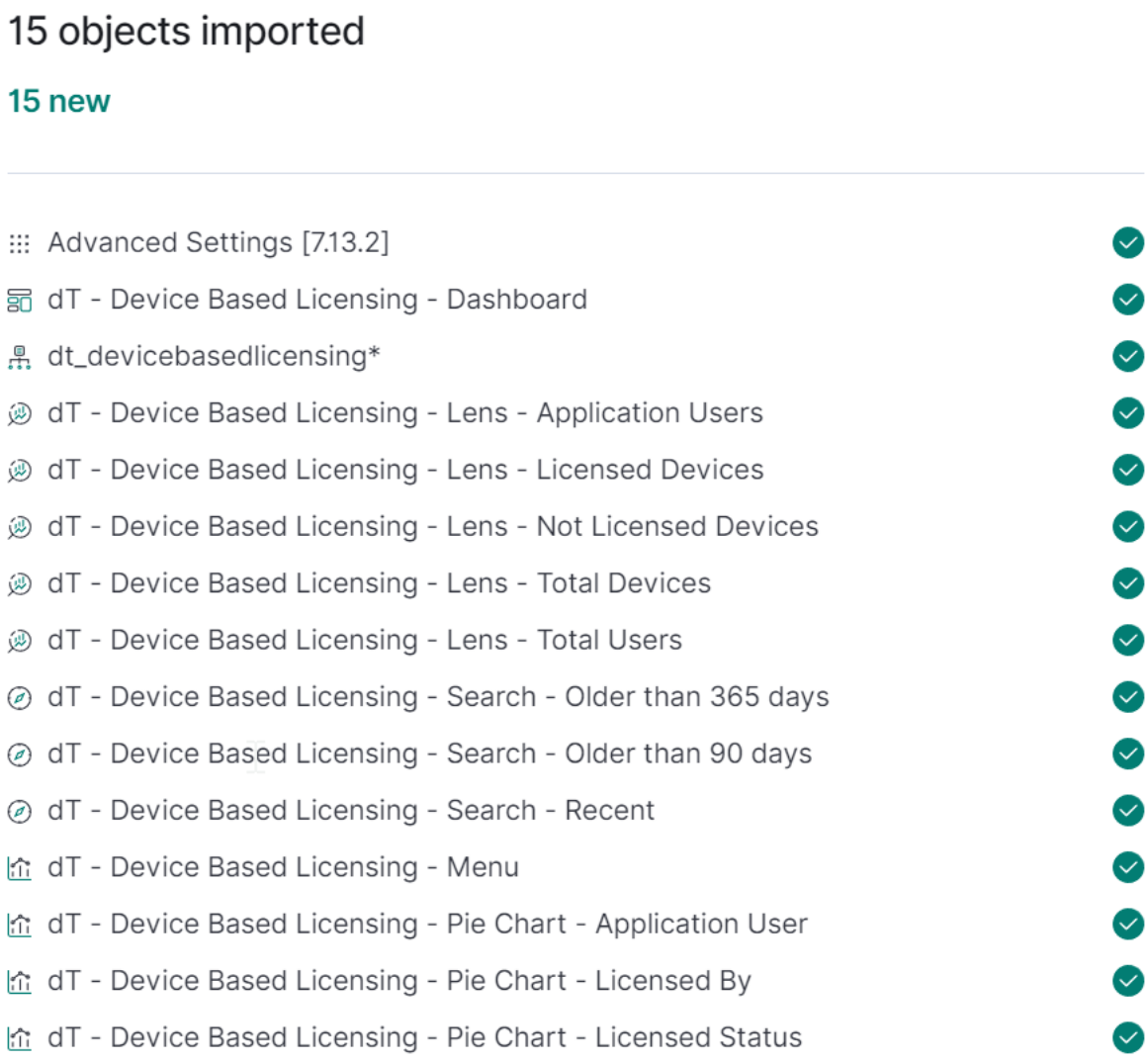


- Select the file `elkstack-device-based-licensing-saved-objects.ndjson`.
- Check `Create new objects with random IDs` to make sure no existing objects are altered.



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

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



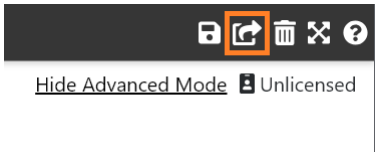
Step 2.3: Configuring deviceTRUST

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.

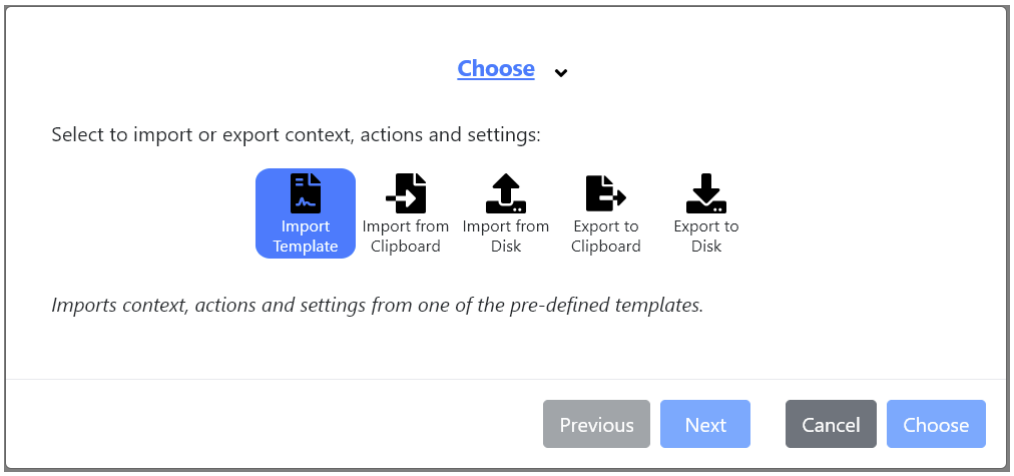
The final step is to create the deviceTRUST configuration that will make sure all the required data is provided.

- 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.

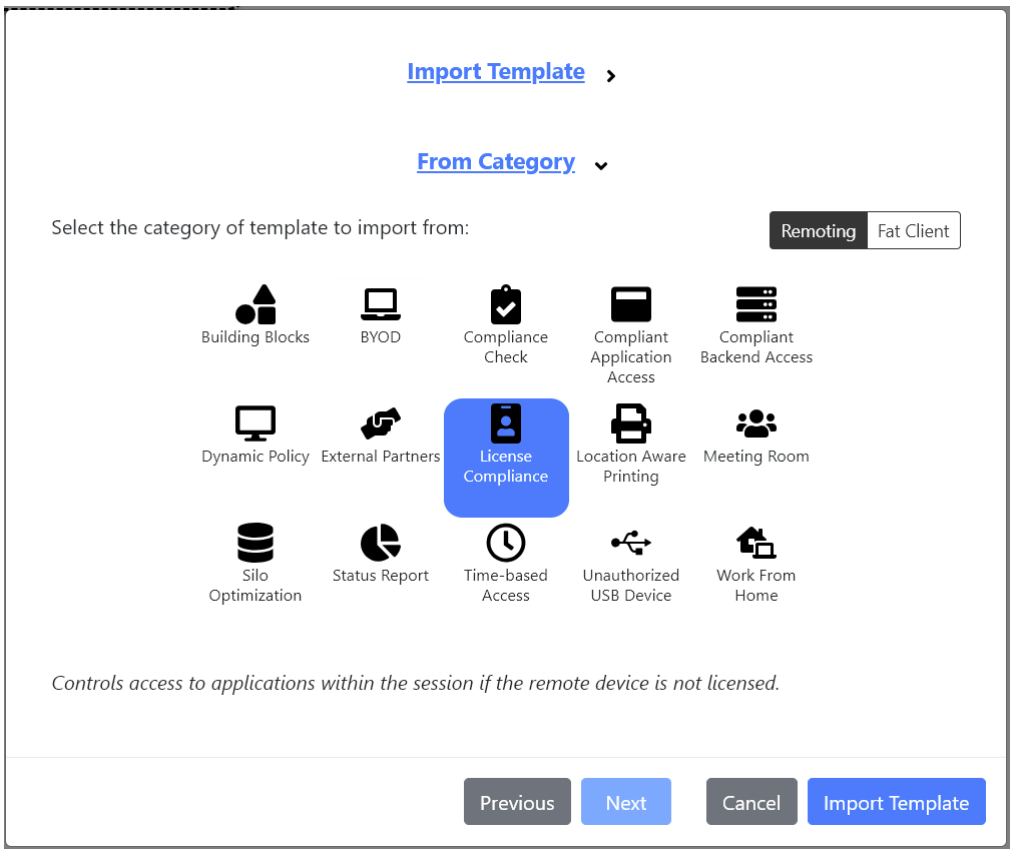
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Select `Import Template`.



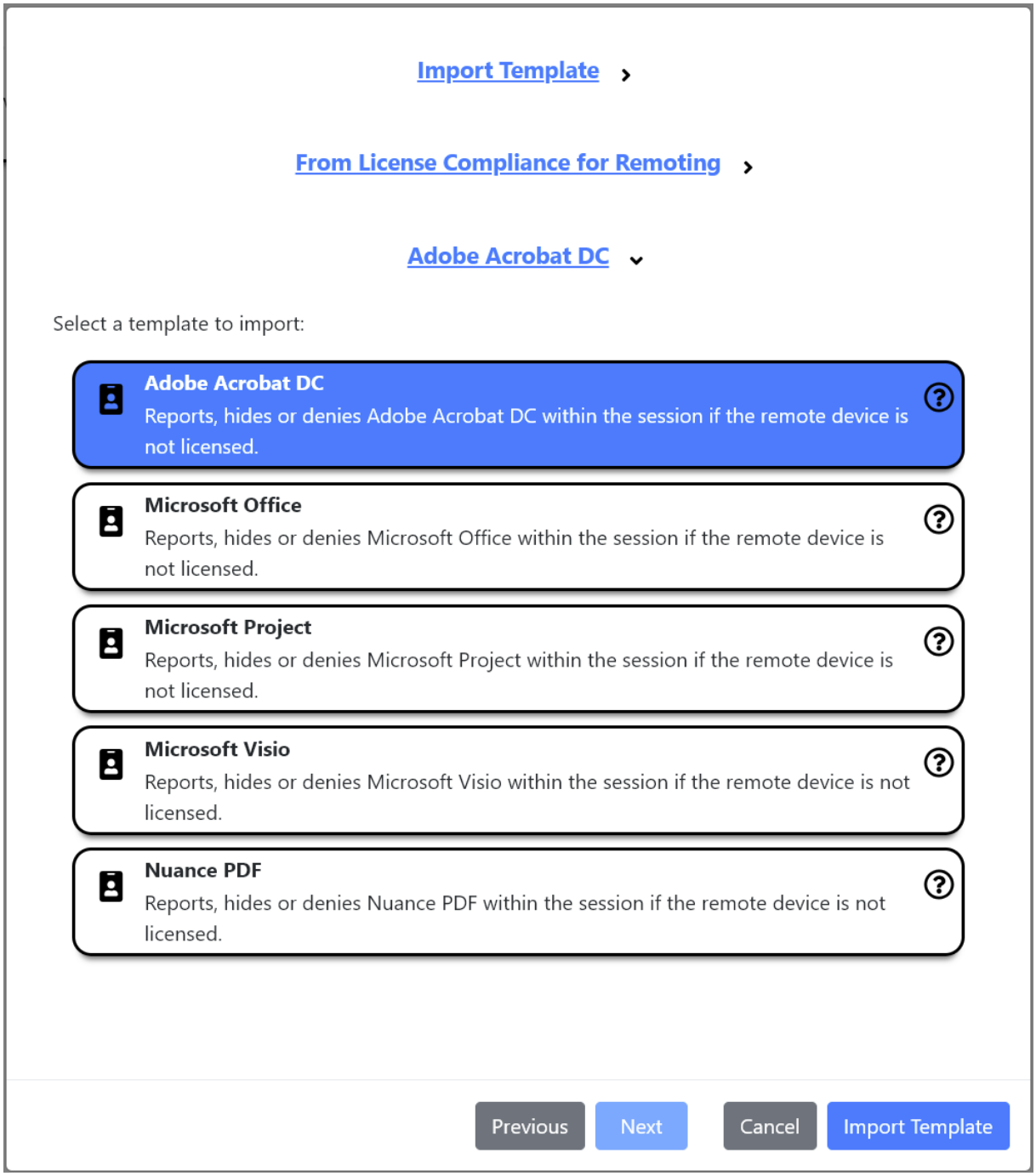
- For `Device-Based Licensing`, the template category `License Compliance` is used.



This category contains templates for several software products. This example uses `Acrobat DC`, but

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

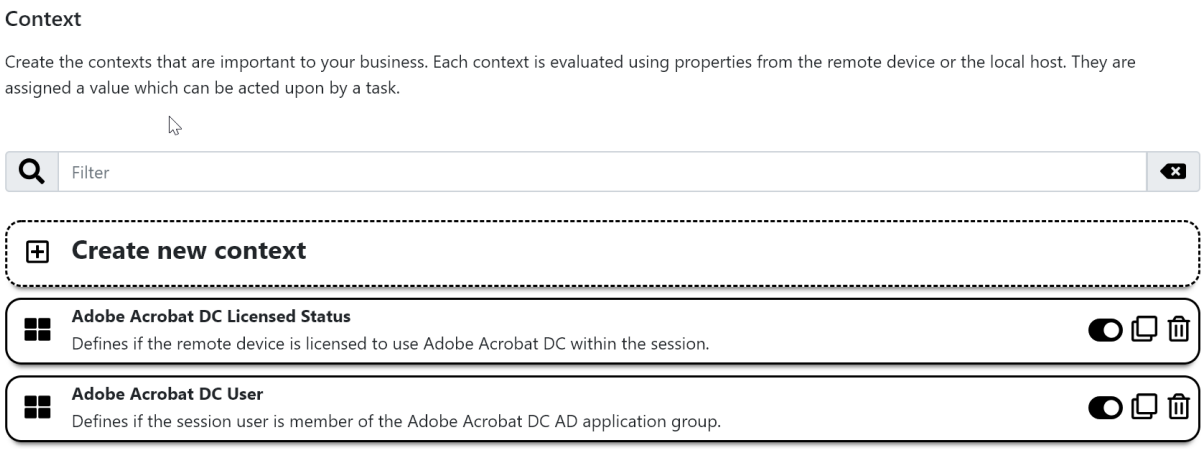
can easily be customised for other applications.



Two contexts are included:

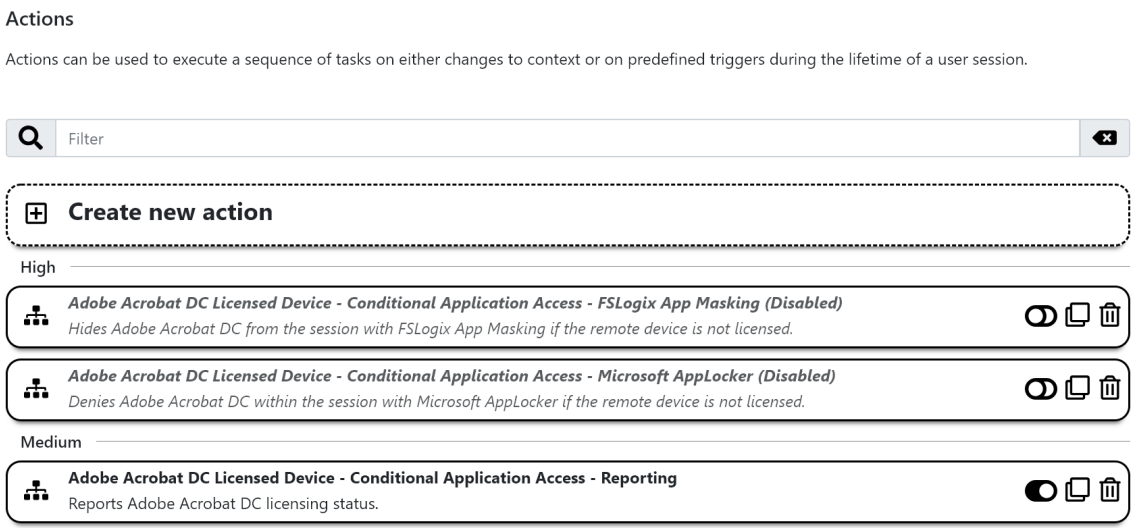
- `Adobe Acrobat DC Licensed Status` to evaluate the device's license status.
- `Adobe Acrobar DC User` to define if the accessing user shall or shall not be using the software.

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



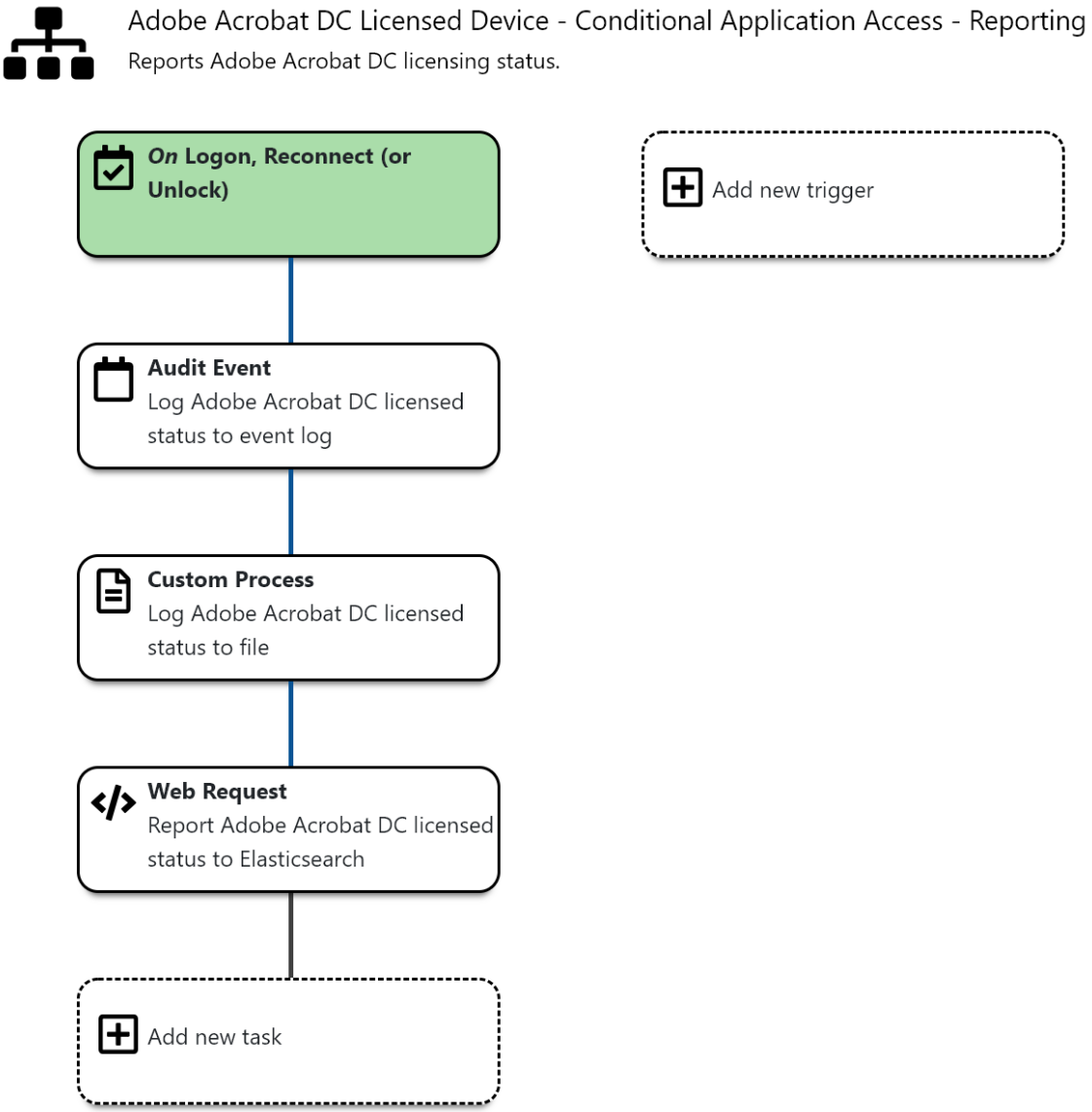
Three actions are included:

- `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.



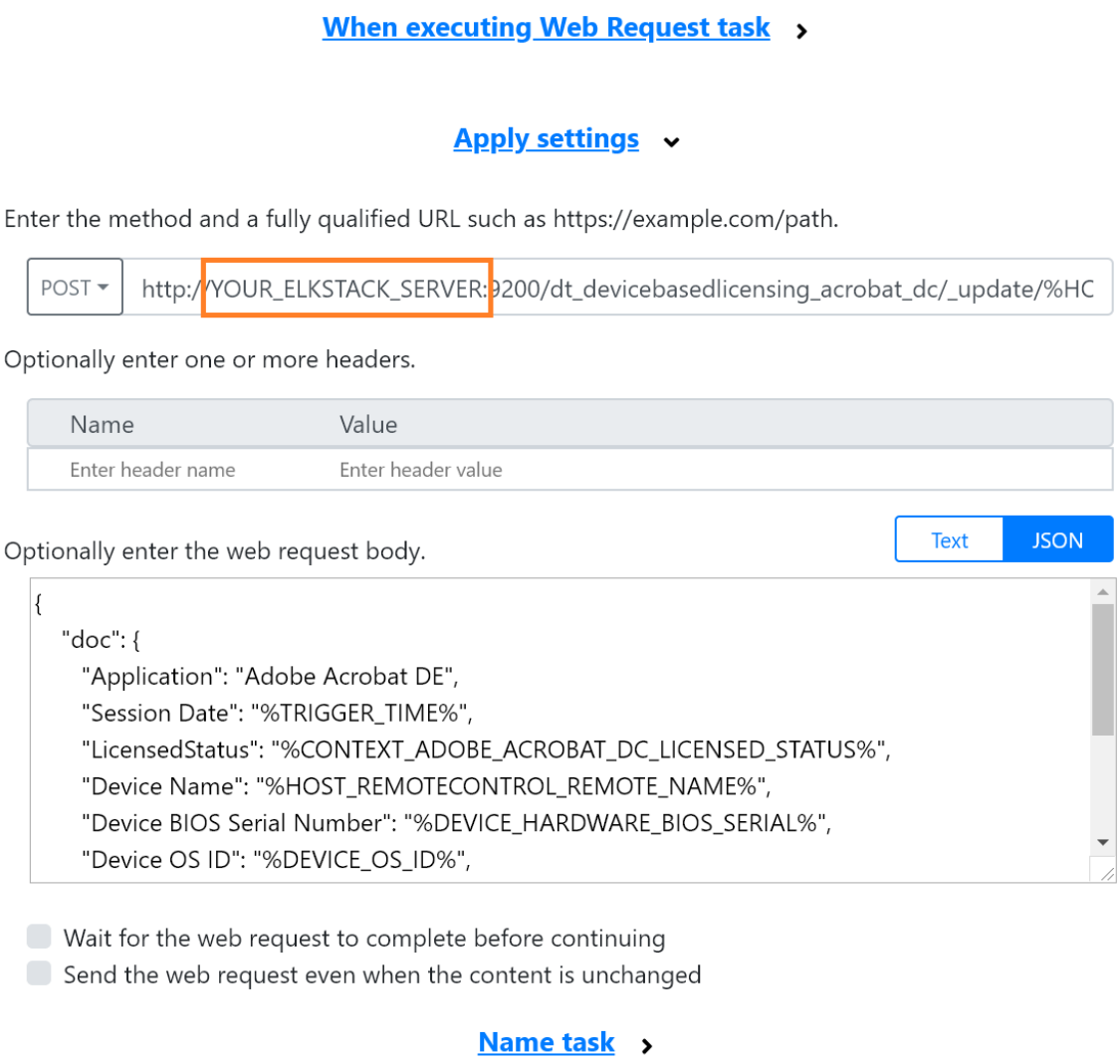
- The action contains multiple ways to store the data. Sending data to ELK Stack is configured by using a `Web Request` task. The `Audit Event`, `Custom Process`, as well as the `Web Request` Tasks for Splunk and Graylog can be deleted, as we are looking at ELK Stack here.

© 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.

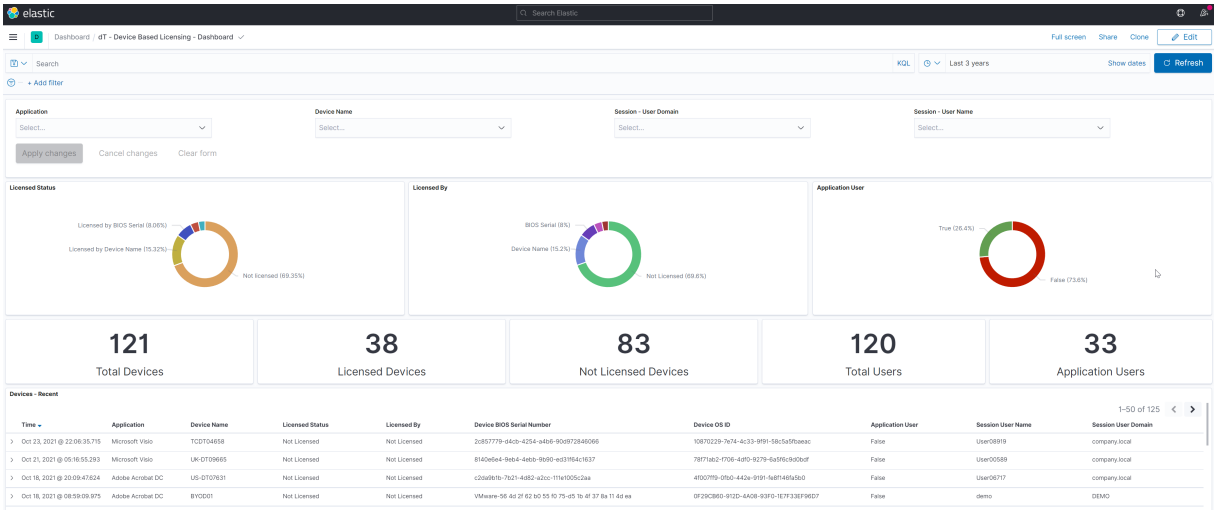
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



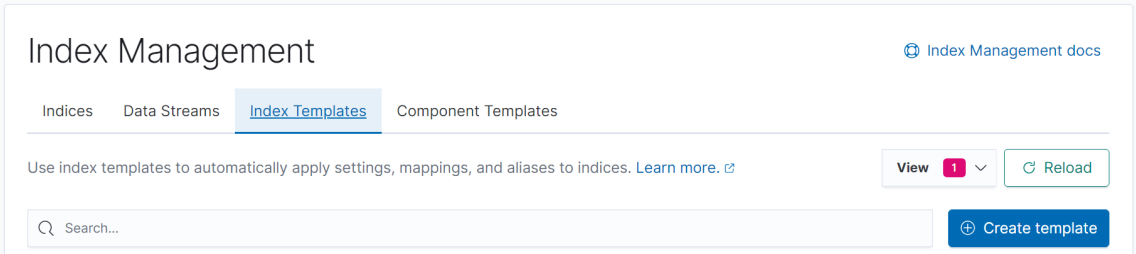
Step 3: The Status Report

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

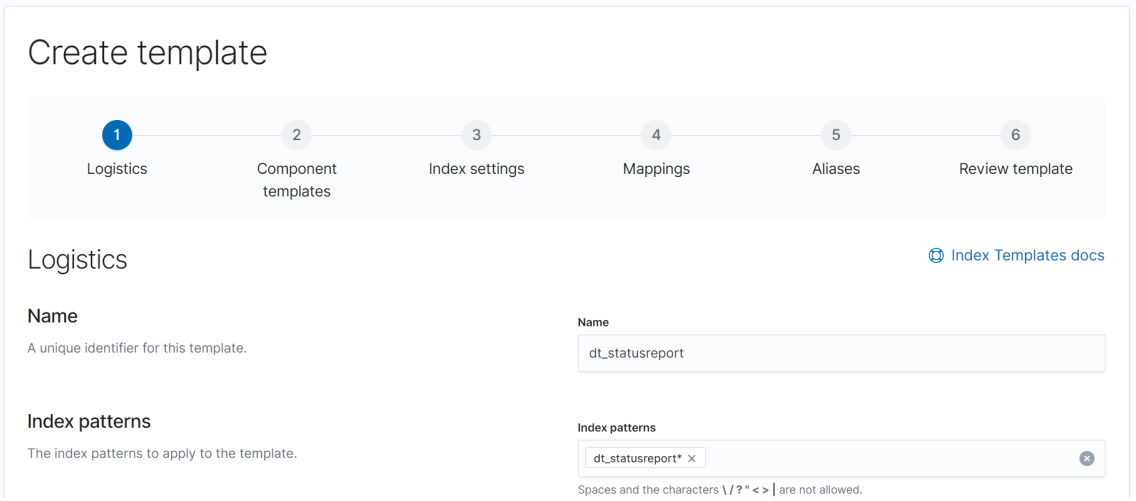
The first step is to create an `Index Template`. Index Templates describe the data that is being sent to an index. They make sure, that every date is treated according to its type.

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

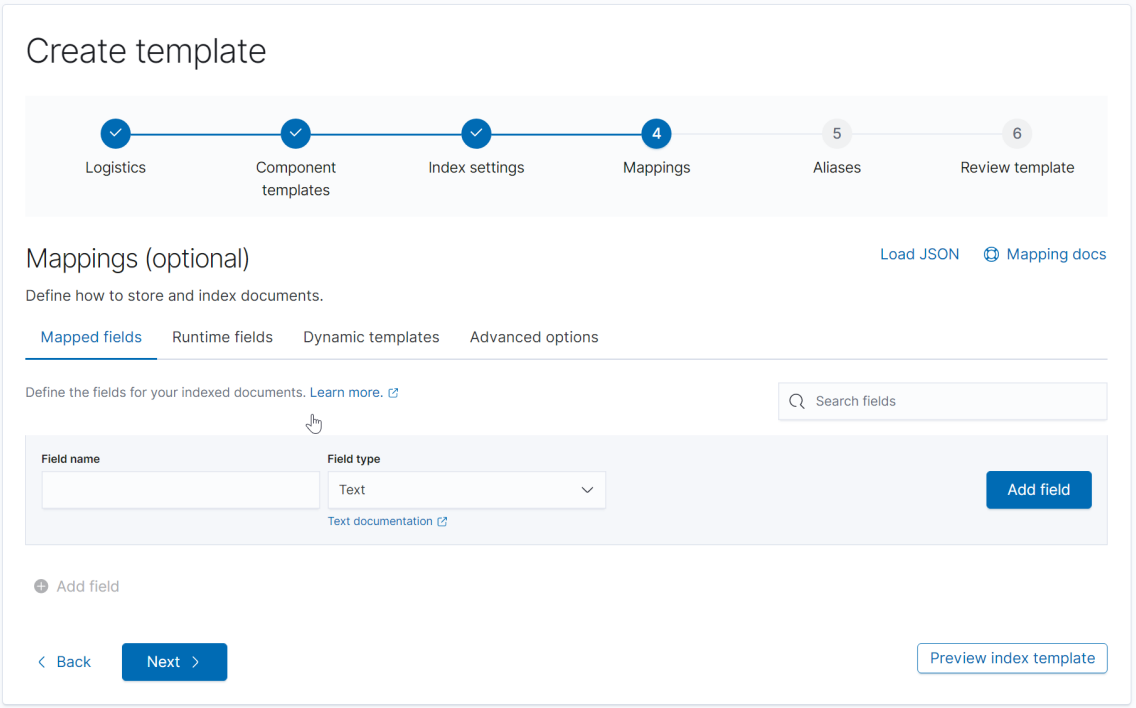


- Set `Name` to `dt_statusreport`.
- Set `Index Patterns` to `dt_statusreport*`.

© 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.

Load JSON

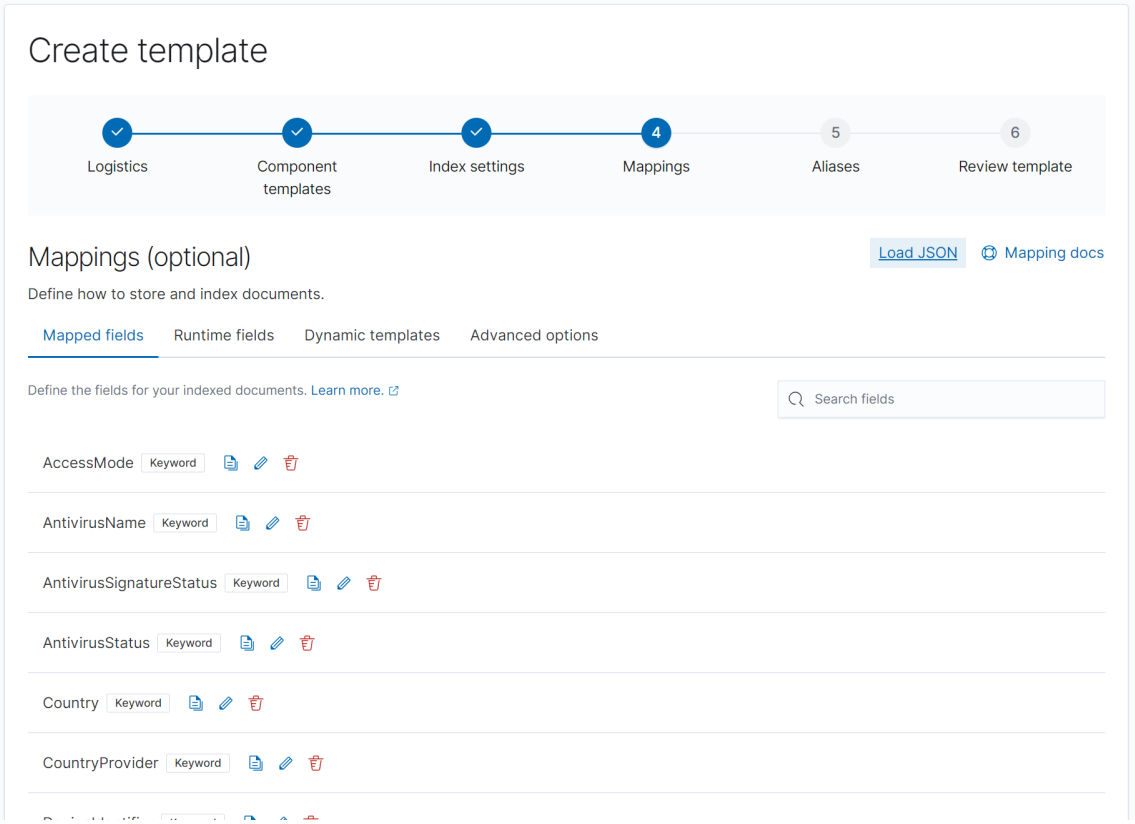
Provide a mappings object, for example, the object assigned to an index `mappings` property. This will overwrite existing mappings, dynamic templates, and options.

Mappings object

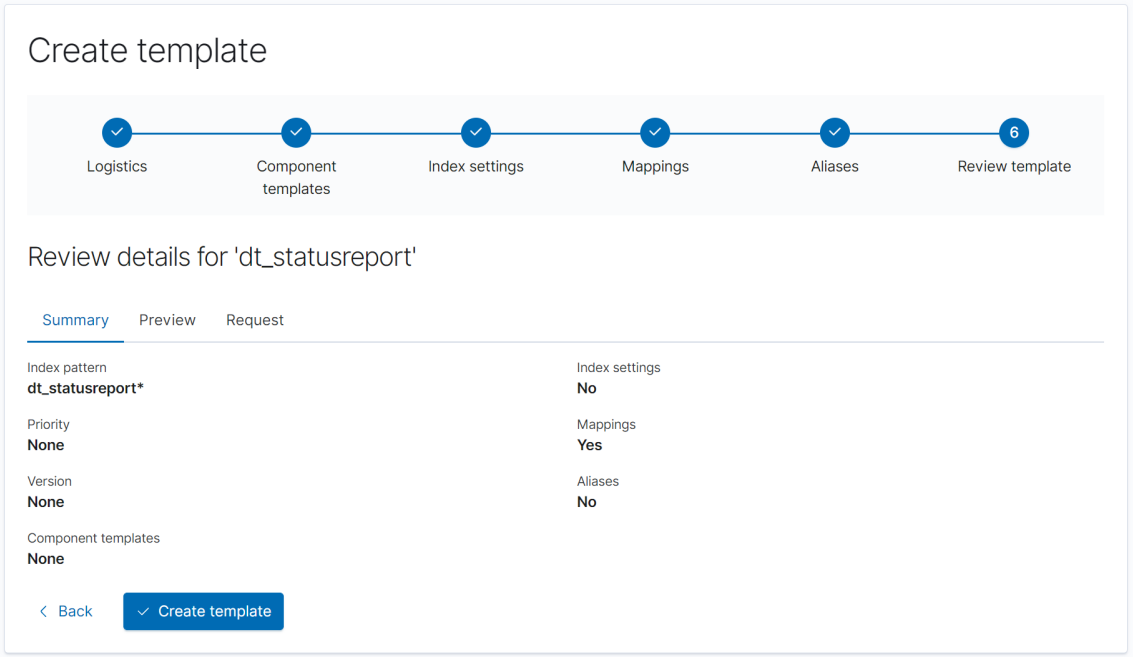


- The imported mappings are displayed. Please review them carefully. `Session Date`, `Anti-Virus Timestamp` and `Hardware BIOS Release Date` need to be recognized as type `Date` for the report to function properly.

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

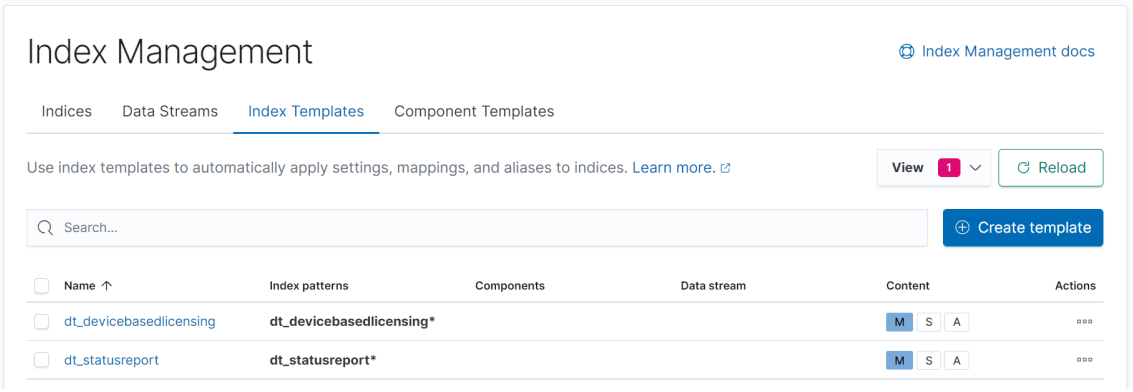


- Skip all options until `Review Template`.
- Generate the template with `Create Template`.



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

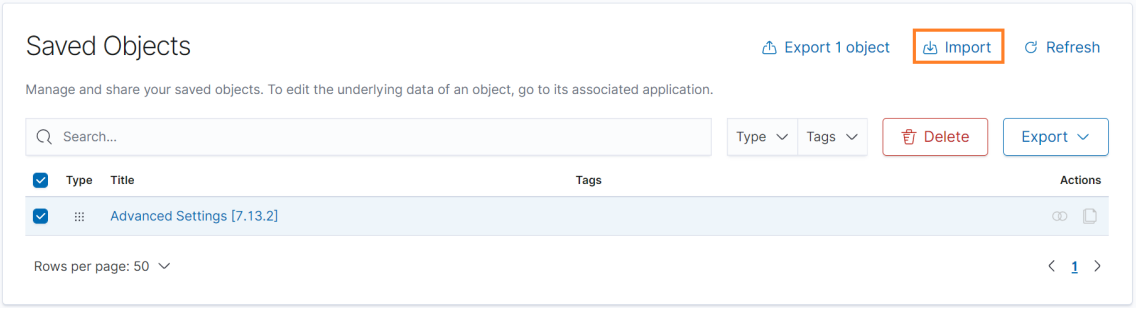
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3.2: Import Saved Objects to ELK Stack

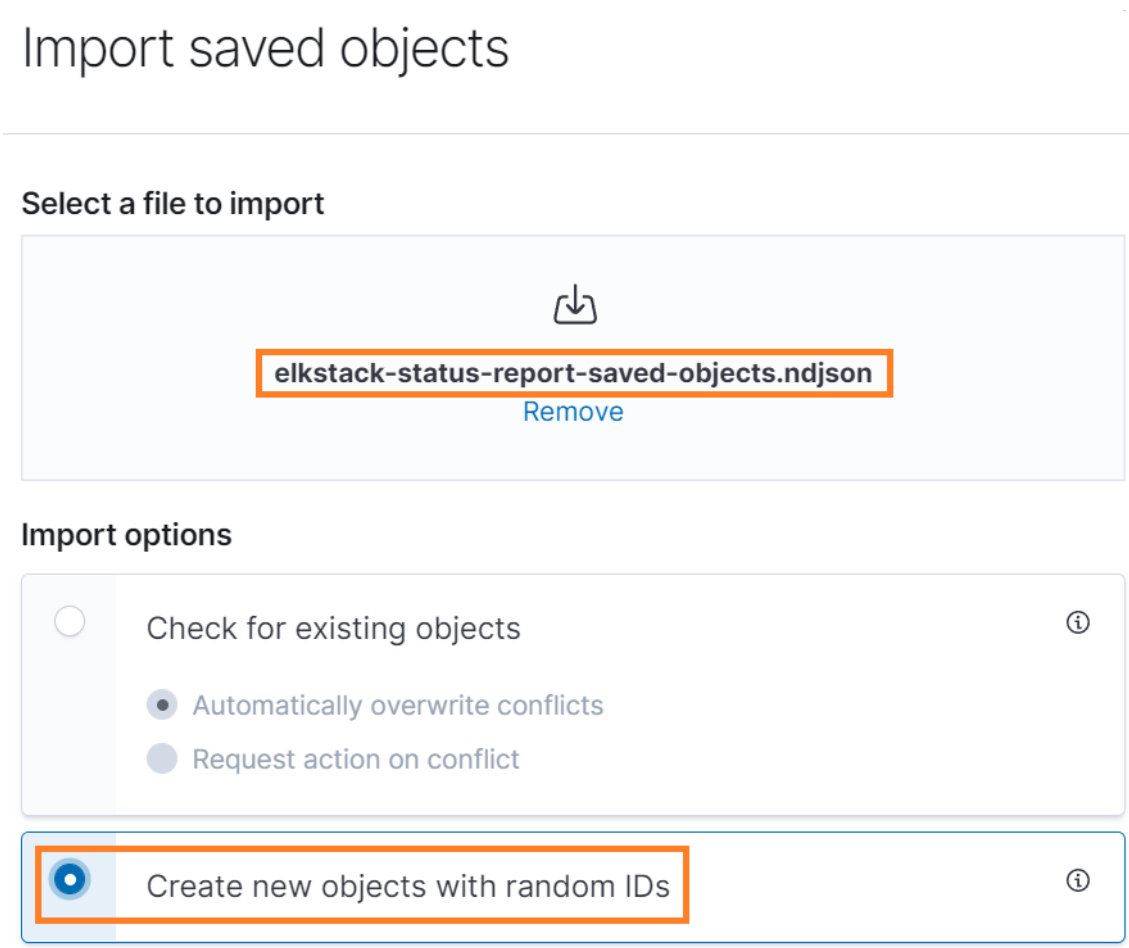
All other parts of the report are to be imported as `Saved Objects`. The Saved Objects consist of Index Patterns with Scripted Fields, Visualizations and Dashboards.

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



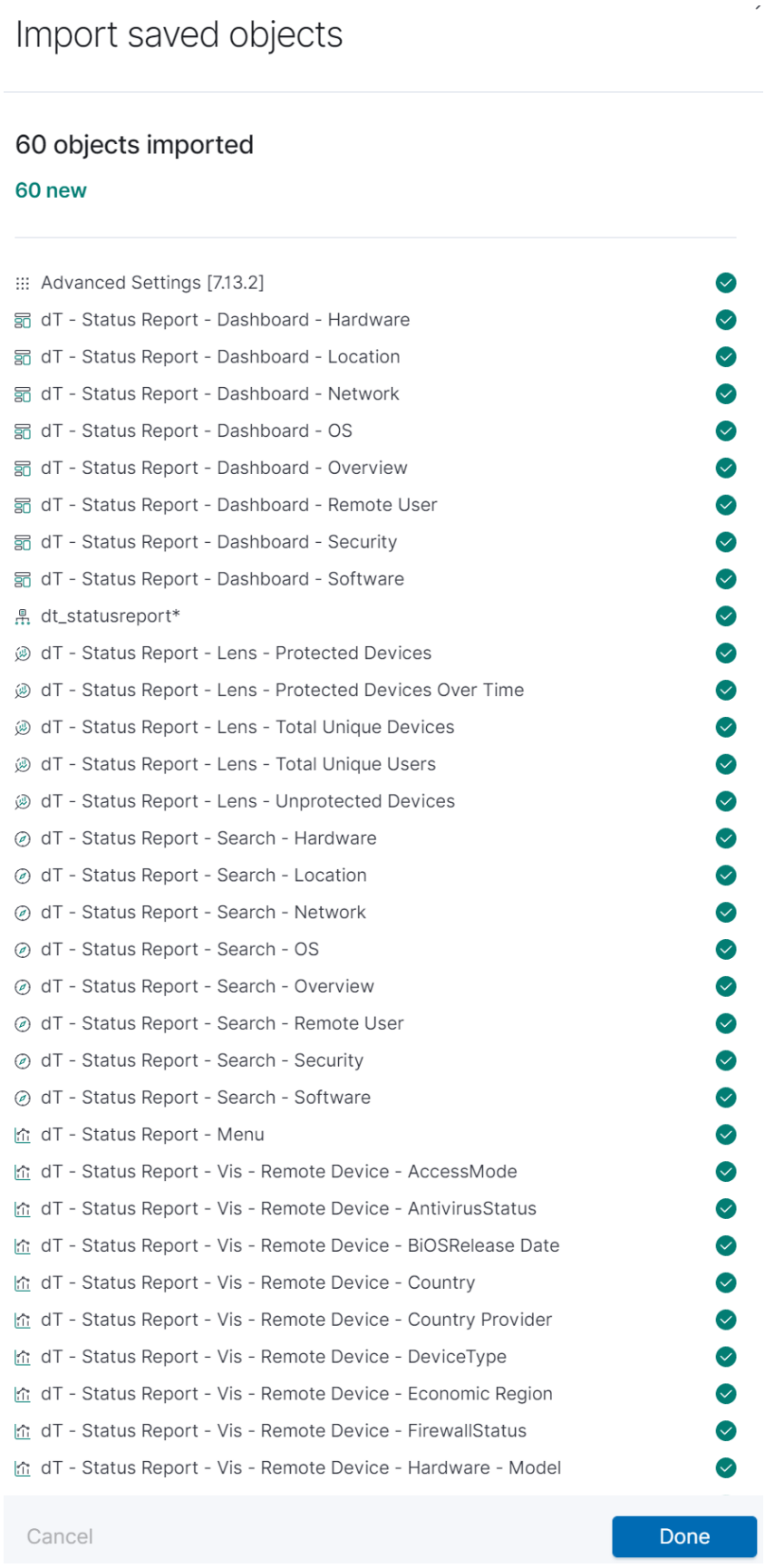
- Select the file `elkstack-status-report-saved-objects.ndjson`.
- Check `Create new objects with random IDs` to make sure no existing objects are altered.

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



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

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



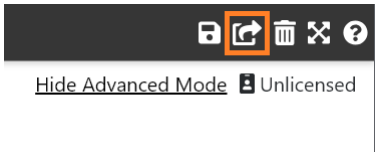
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3.3: Configuring deviceTRUST

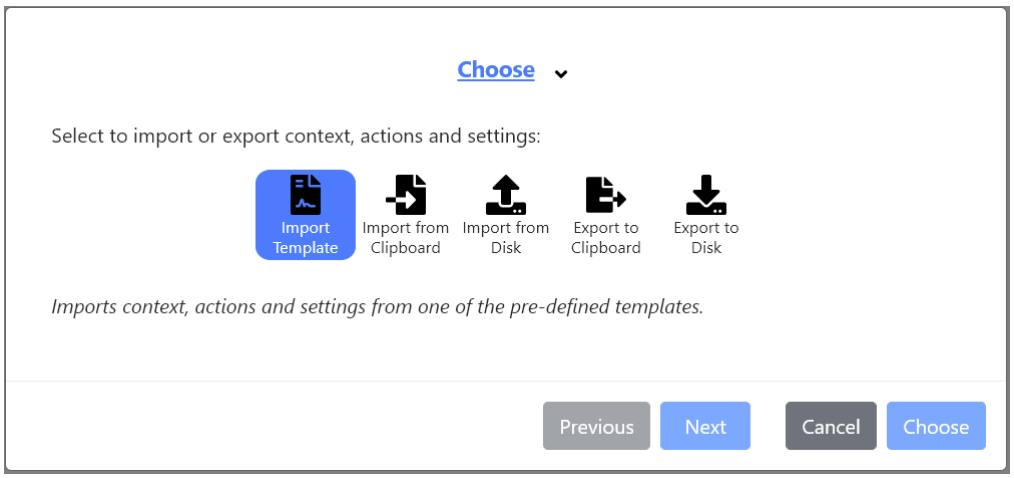
After the Index Mapping has been created, the Saved Objects are included the index has been edited and the agent-side has been configured, the ELK Stack is prepared for storing, sorting, and displaying your data.

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

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



- Select `Import Template`.



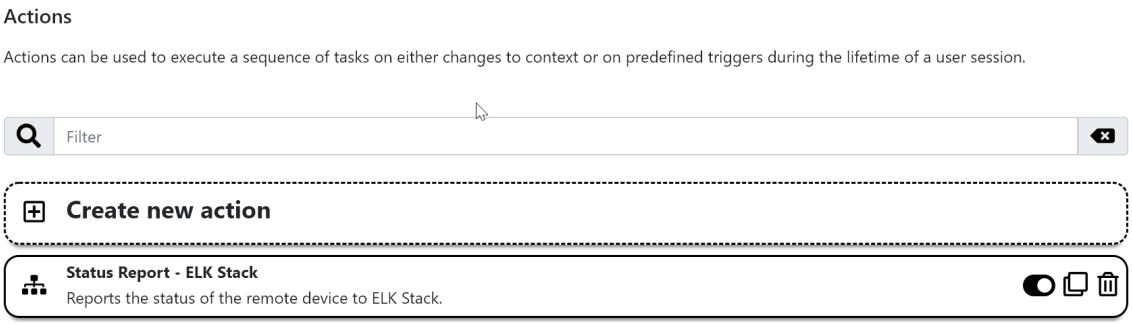
- For `Status Report`, the template category `Status Report` is used.
- This category contains templates for several ways of storing data. Choose `ELK Stack`.

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

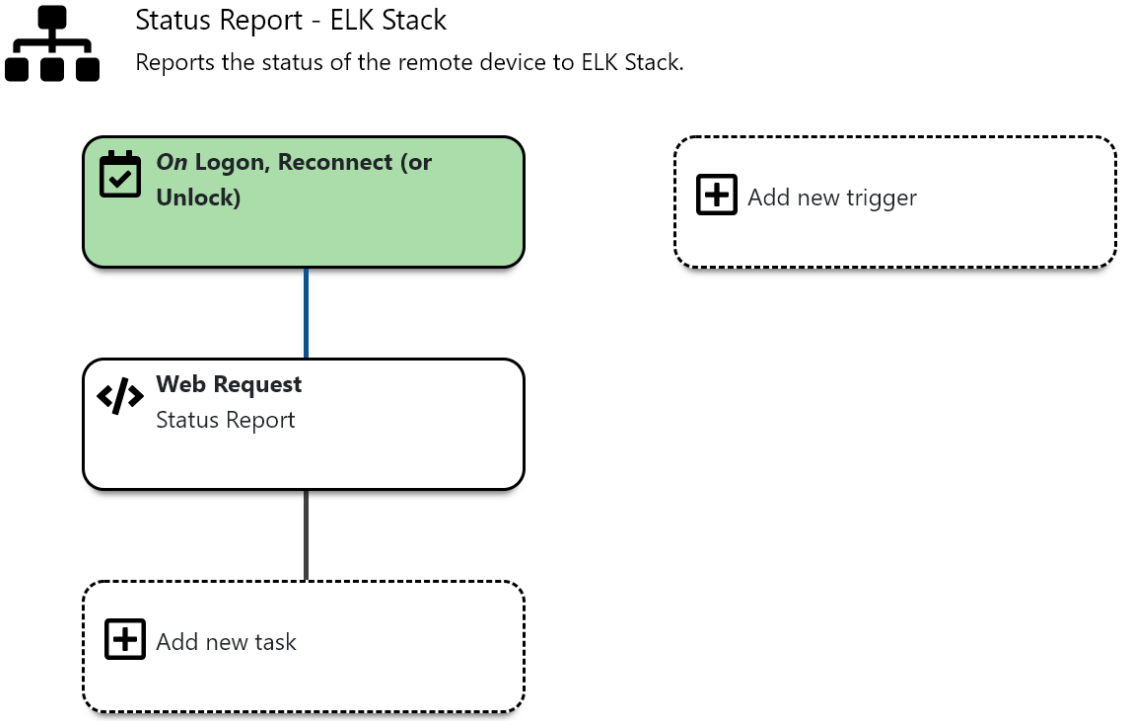


- The imported template consists of 50 contexts and one action.
- The Action `Status Report – ELK Stack` collects all relevant data and sends them over to the ELK Stack.

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

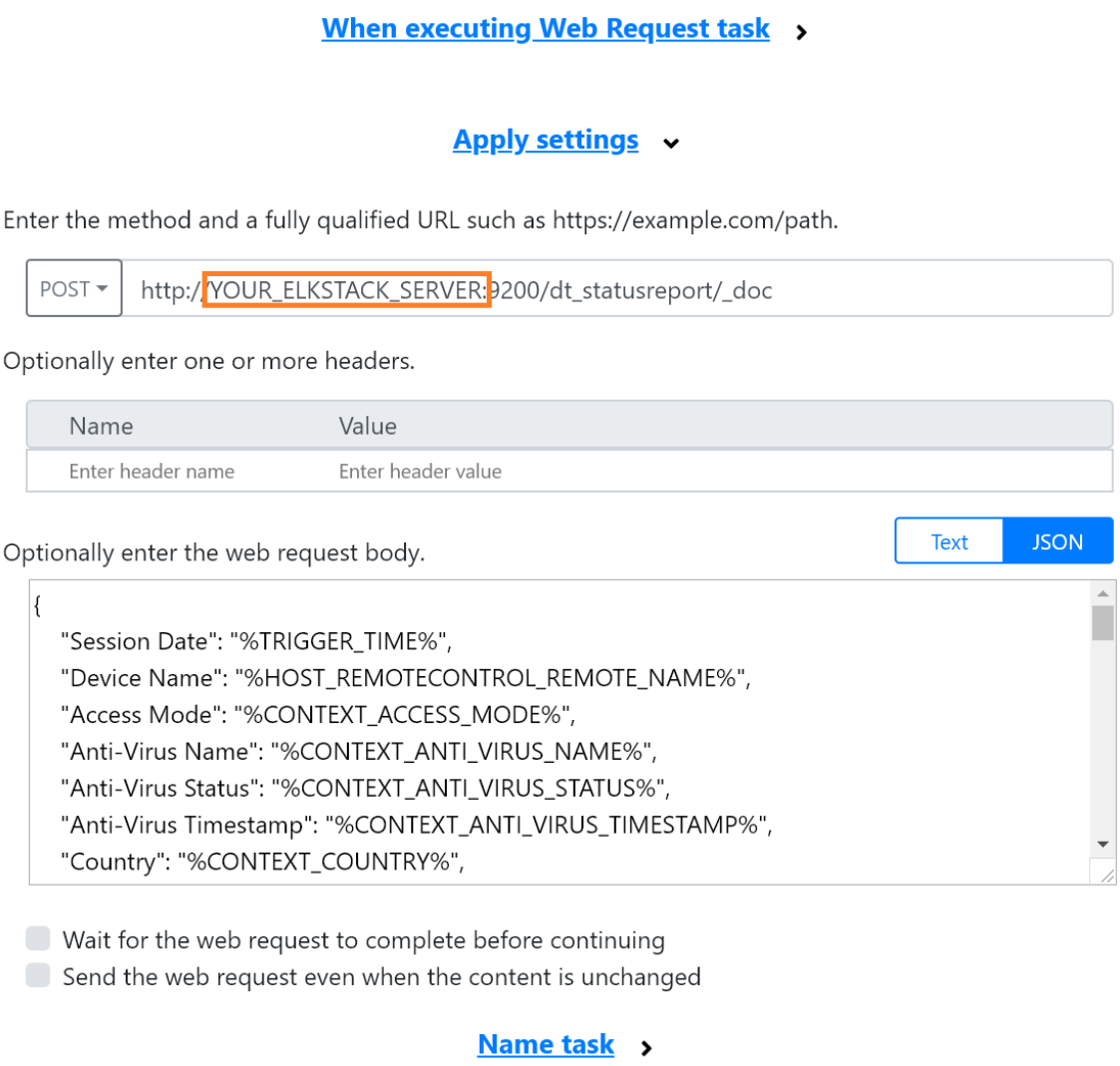


- Sending data to ELK Stack is configured by using a `Web Request` task.



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

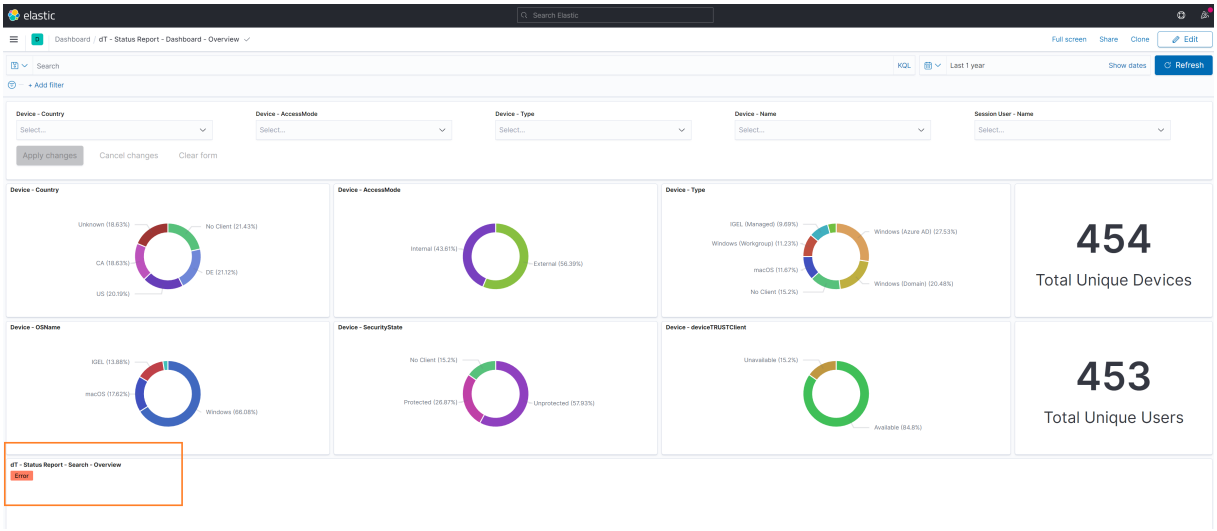
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3.4: Edit index settings

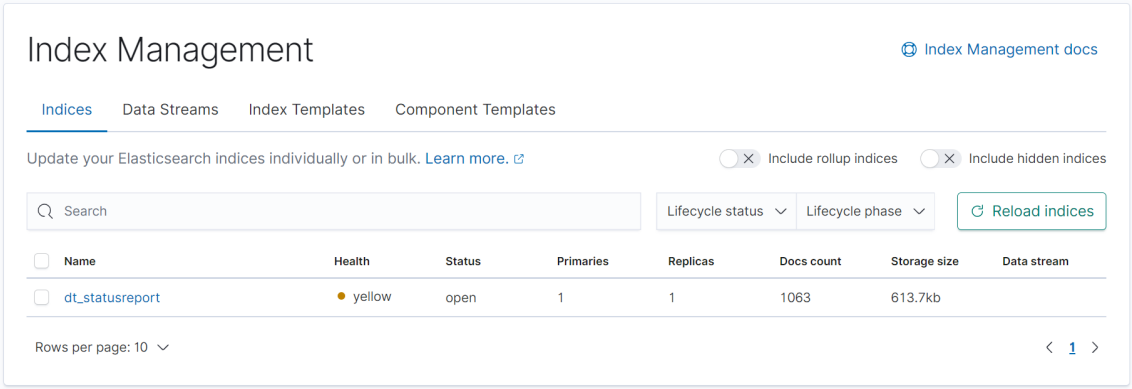
For the Status Report Dashboards to work properly, a configuration needs to be made at the index level: In a basic setting, ELK Stack allows to use 25 "calculated fields" per index. For the Status Report Dashboard, 48 calculated fields are used. Thus, the `allowed number of calculated fields` needs to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

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



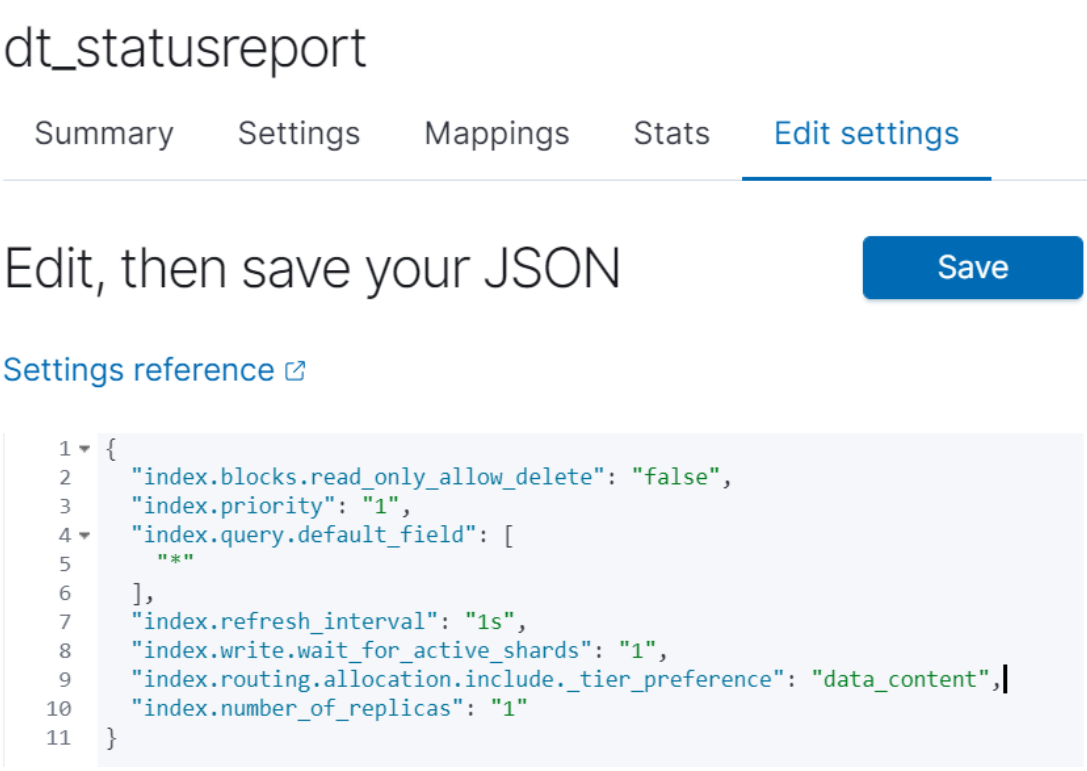
You need to send data to ELK Stack first. Sending data will create the index with basic settings. It can then be edited.

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



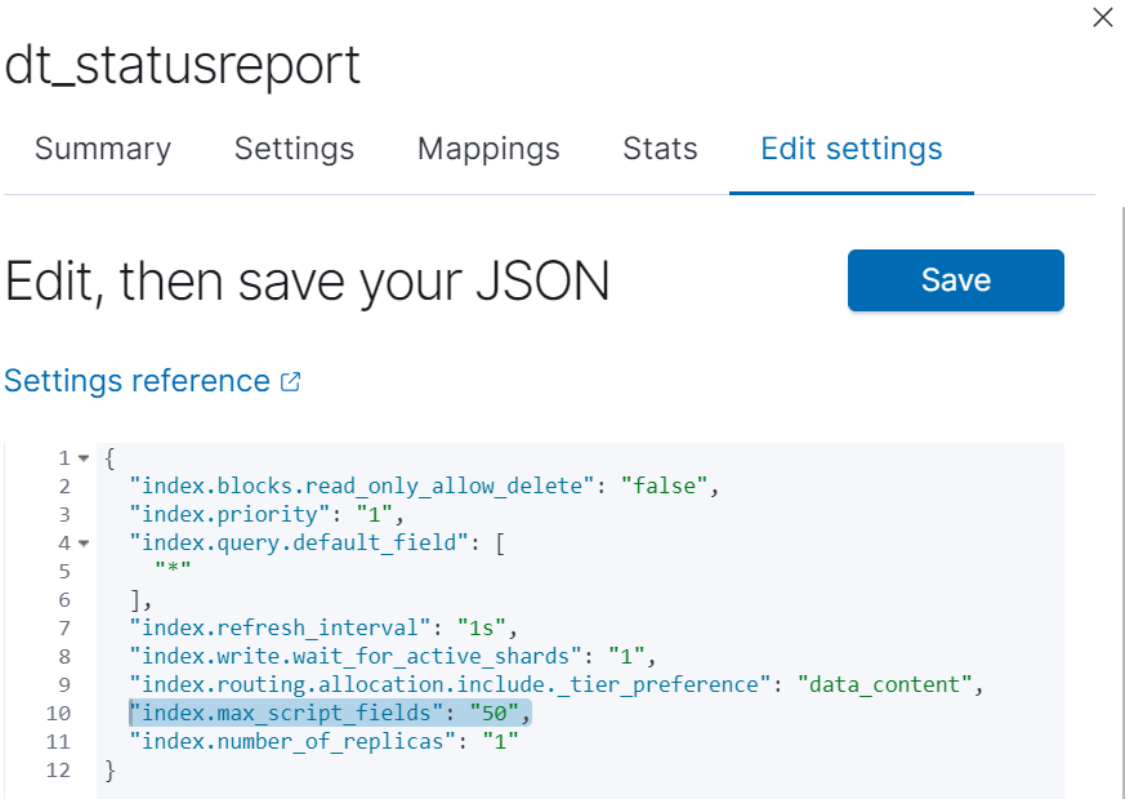
- Select the Index and chose `Edit Settings`. You'll be presented a json configuration view.

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



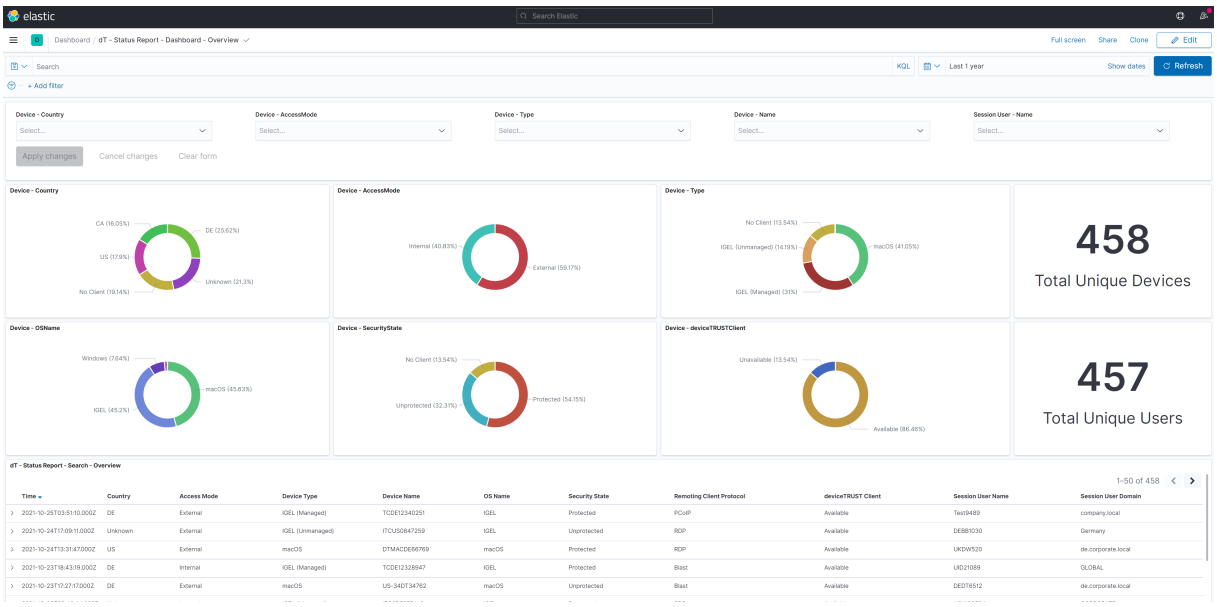
- Add `"index.max_script_fields": "50"` as a new line, making sure to keep the correct json formatting.
- Save your changes.

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



Your Dashboard will now be displayed without errors.

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



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

Reference

TABLE OF CONTENTS

- Properties
- Agent
- Client Extension
- Console

Properties

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

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

- Multihop Properties - Describes the number of hops taken by the user over deviceTRUST connected sessions.
- Name Properties - Identifies the endpoint.
- Network Properties - Describes the network adapters and their bound network addresses.
- NoTouch Properties - Provides properties unique to a Stratodesk NoTouch device.
- OS Properties - Provides information about the operating system installed on the endpoint.
- Password Policy Properties - Describes the password policy of the logged in user.
- Performance Properties - Describes the performance of the remoting protocol.
- Power Properties - Describes the power profile of the endpoint.
- Printer Properties - Describes the printers available to the user session.
- Region Properties - Describes the regional information of the user session.
- Remote Control Properties - Determines whether the user session is being remote controlled and provides information about the remote controlling endpoint.
- Remoting Client Properties - Provides properties about the remoting client used to remote control the user session.
- Screen Saver Properties - Describes the screen saver applied to the user session.
- Security Product Properties - Provides real-time properties describing the state of the installed Antivirus, Antispyware and Firewall security products.
- Session Properties - Provides information describing the user's logon session.
- Smartcard Reader Properties - Describes the connected smart-card readers available to the user.
- User Properties - Identifies the logged in user.
- WHOIS Properties - Provides the results of a WHOIS lookup of the endpoint.
- Windows Properties - Provides real-time properties unique to a Microsoft Windows device.
- Windows Defender Properties - Provides real-time properties describing the state of Microsoft Windows Defender Antivirus.
- Windows Firewall Properties - Provides real-time properties describing the state of the Microsoft Windows Firewall.
- Windows Registry Properties - Provides access to Windows Registry entries.
- Windows Update Properties - Describes the status of Microsoft

Agent Reference

TABLE OF CONTENTS

- Policy Loading
- Product Events

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

Client Extension Reference

TABLE OF CONTENTS

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

Console Reference

TABLE OF CONTENTS

- Actions - Actions Reference
- Settings - Settings Reference

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

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

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
- 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.

Knowledge Base

TABLE OF CONTENTS

- Features
- General
- Properties
- Reporting

General

TABLE OF CONTENTS

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

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

Configuration

Table of Contents

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

Connectivity

Table of Contents

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

Diagnostics

Table of Contents

- deviceTRUST debug log locations

Installation

TABLE OF CONTENTS

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

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

Licensing

TABLE OF CONTENTS

- Make sure that you have a valid license

Support

TABLE OF CONTENTS

- IGEL OS 12 - No IGEL Properties

Compatibility

Table of Contents

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

Properties

TABLE OF CONTENTS

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

Reporting

TABLE OF CONTENTS

- Log data to Microsoft Teams

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

Features

Table of Contents

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

Releases

TABLE OF CONTENTS

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

TABLE OF CONTENTS

June 20, 2025

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

IGEL OS 11 Client Extension 23.1.400

This release includes minor enhancements to the deviceTRUST Client Extension for IGEL OS 11. This release has been submitted to IGEL for native integration into IGEL OS 11, however this has not been

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

released yet. To integrate into currently available IGEL OS releases, please consult our Updating the deviceTRUST Client Extension in IGEL OS 11 Knowledge Base article.

Support for third party WHOIS providers in 23.1.300

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

Compatibility

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

IGEL OS 12 Client Extension 23.1.400

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

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

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

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

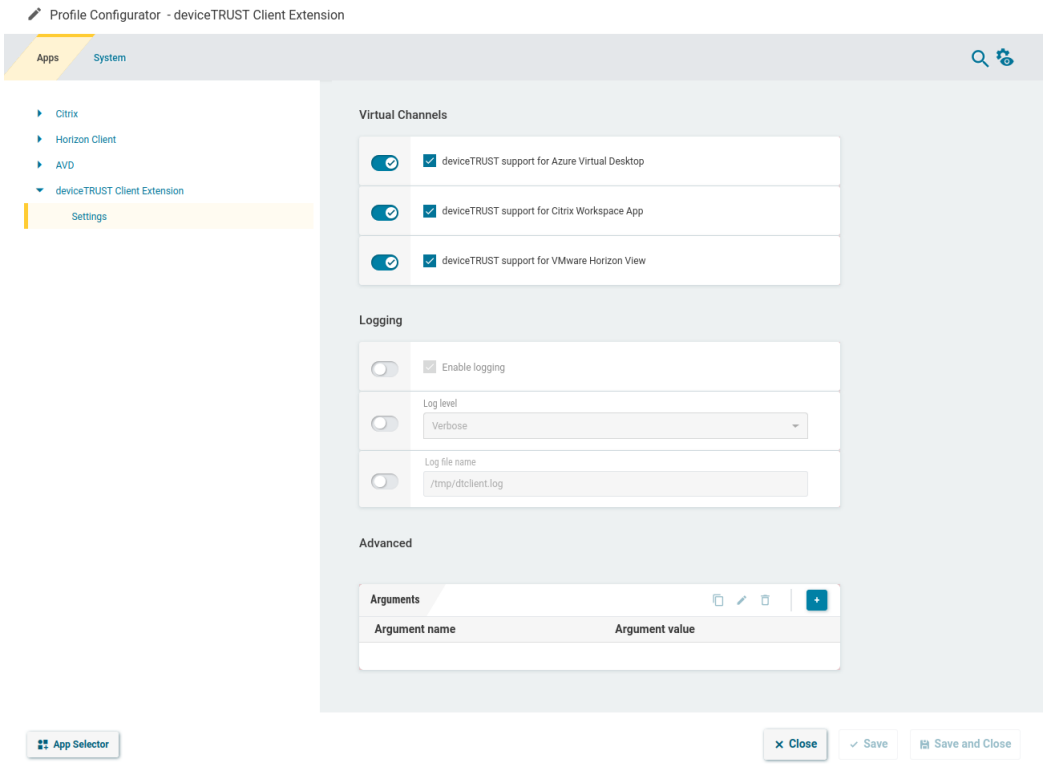
Remoting Clients

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

UMS Configuration

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

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



New COSMOS Properties

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

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

More information can be found at IGEL Properties.

WHOIS proxy, proxy type and usage in 23.1.400

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

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

Bug fixes in 23.1.200

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

Minor enhancements in 23.1.200

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

Bug fixes in 23.1.210

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

Compatibility

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

iOS Client Extension 23.1.400

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

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

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

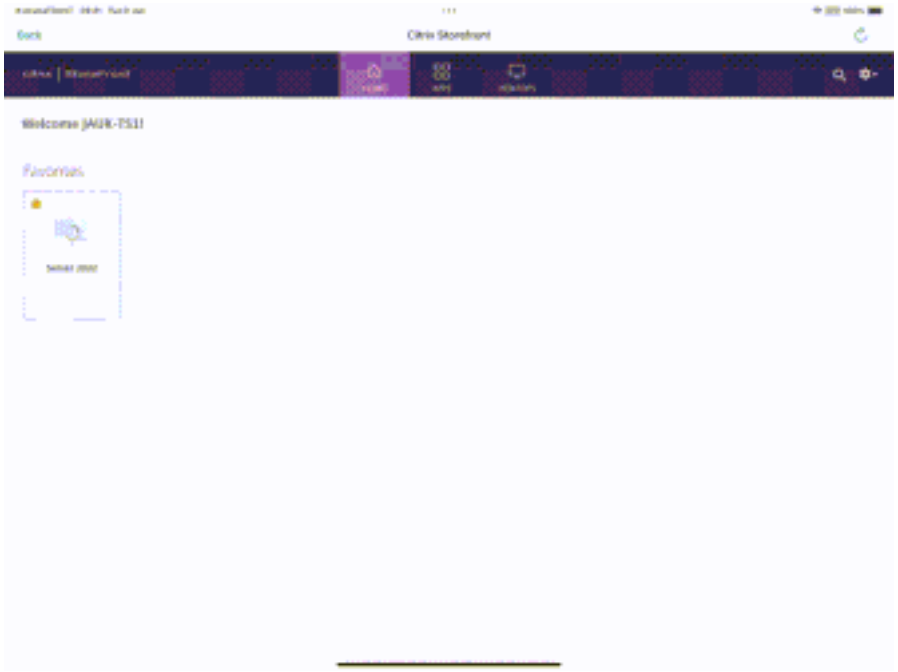
Passcode authentication for iOS 17

Previously when connecting to a virtual session with an iOS device, the deviceTRUST Agent matched the *client name* taken from the remoting protocol with the name of the registered iPhone or iPad

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

within the deviceTRUST Portal. However with Apple's continued push towards user privacy, the ability to query the name of the device is now limited to apps meeting specific criteria and requesting the necessary entitlement. Neither the deviceTRUST Client Extension for iOS, or any of the popular remoting clients, have been granted this entitlement. Having lost the only information we have that identifies the remote iOS device, a new approach to matching the remote device is required.

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



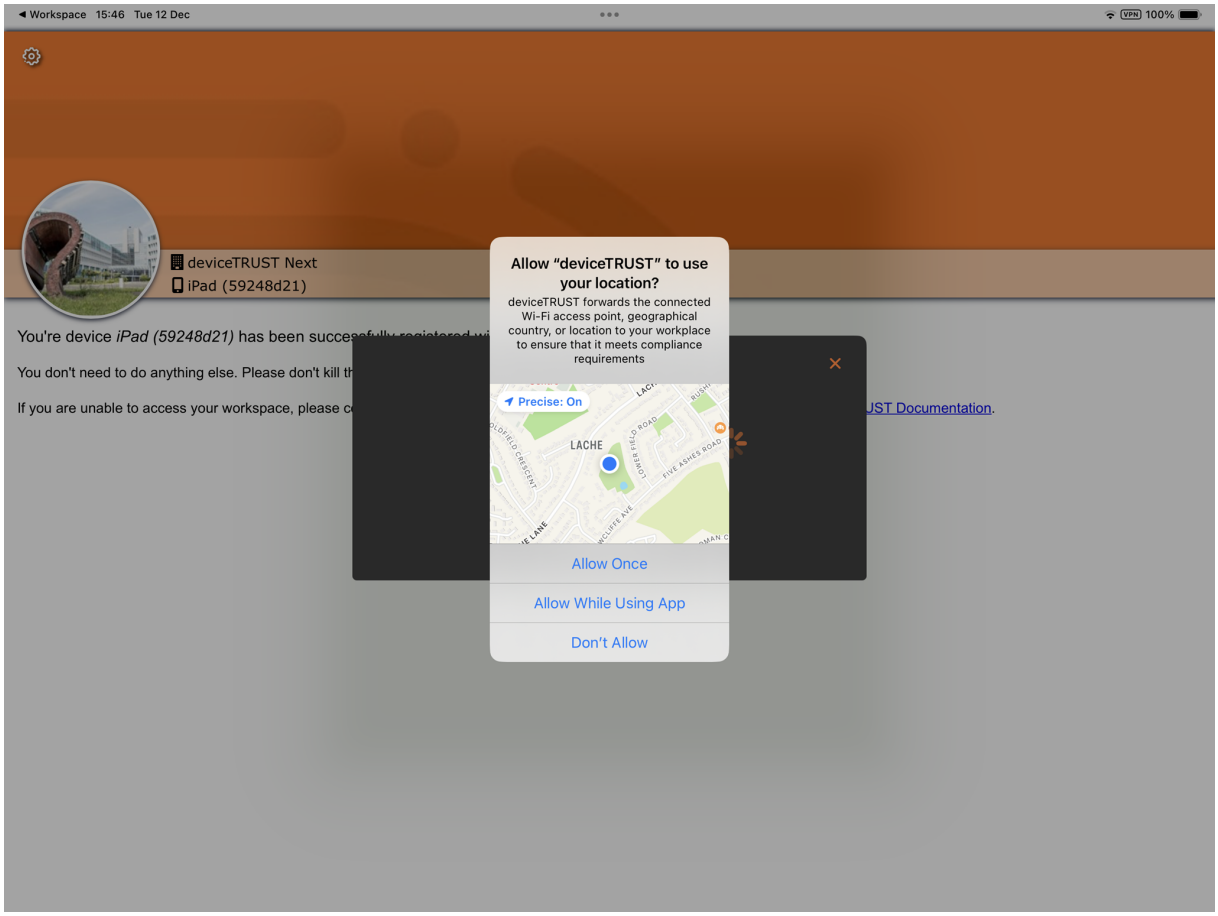
By using passcodes, we now support iOS as a remote device on Citrix Virtual Apps and Desktops, Citrix Cloud, Microsoft Remote Desktop Services and VMware Horizon View. For more information, see OS Compatibility.

More information can be found in the iOS Passcodes reference.

Location and Network Wi-Fi SSID/BSSID

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

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



Compatibility

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

macOS Client Extension 23.1.410

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

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

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

Release 23.1.300 includes compatibility with third party WHOIS providers.

Release 23.1.400 includes bug fixes to address compatibility issues with macOS 15.0 Sequoia, as well

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

as support for new Microsoft Intune and WHOIS properties introduced in release 23.1.400 of the deviceTRUST Agent and Console.

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

Support for third party WHOIS providers in 23.1.300

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

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

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

Nice DCV extension support including Amazon WorkSpaces WSP

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

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

Bug Fixes in 23.1.100

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

Bug Fixes in 23.1.110

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

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

Bug Fixes in 23.1.200

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

Bug Fixes in 23.1.400

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

Bug Fixes in 23.1.410

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

Known Issues

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

Compatibility

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

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

Stratodesk NoTouch OS Client Extension 23.1.100

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

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

Available Properties

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

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

NoTouch Properties

The following properties are available within the NoTouch category:

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

Custom Properties for NoTouch Devices

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

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

Ubuntu Client Extension 23.1.400

September 6, 2025

Release 23.1.300 includes support for third party WHOIS providers.

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

Support for third party WHOIS providers in 23.1.300

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

Support for WHOIS proxy, proxy type and usage in 23.1.400

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

Bug Fixes in 23.1.300

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

Bug Fixes in 23.1.400

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

Compatibility

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

deviceTRUST 23.1.410

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

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

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

Microsoft Intune Detection

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

WHOIS Proxy Detection

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

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

Proxy Detection with IP2Location Web Services

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

Property	Response Field	Free Plan	Starter Plan	Plus Plan	Security Plan
Proxy	`is_proxy<sup>1</sup>`	✓	✓	✓	✓
Proxy Type	`proxy.proxy_type`				✓
Usage	`usage_type`		✓	✓	✓

> **Note:**
>
> The accuracy of the `is_proxy` field is dependent upon the selected plan.

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

Proxy Detection with MaxMind GeoIP2 Insights Web Service

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

Property	Response Field	GeoIP2 Country	GeoIP2 City Plus	GeoIP2 Insights	GeoLite Country	Geolite City
Proxy	`is_anonymous`			✓		
Proxy Type	`is_hosting_provider`, `is_anonymous_vpn`, `is_public_proxy`, `is_residential_proxy`, `is_tor_exit_node`			✓		
Usage	`user_type`			✓		

Minor enhancements to 23.1.400

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

Bug fixes in 23.1.400

- Fixed an issue where a virtual session could be logged off during a live reconnect to a session that had never shown the desktop to the user.
- Fixed an issue with the Logical Disk Identity operator where the None Of operator was shown as Not Equals.

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

Bug fixes in 23.1.410

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

Compatibility

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

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

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

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

June 20, 2025

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.