deviceTRUST® 2503 CR

Contents

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.
- Reference provides a set of reference material describing the more advanced features of deviceTRUST.
- Knowledge Base provides a useful resource for common problems and resolutions.
- Troubleshooting important steps are described to help troubleshoot the deviceTRUST installation and configuration.
- Releases contains the release notes detailing new features and bug fixes within the released deviceTRUST products.

Architecture

July 23, 2025

TABLE OF CONTENTS

Local Scenario

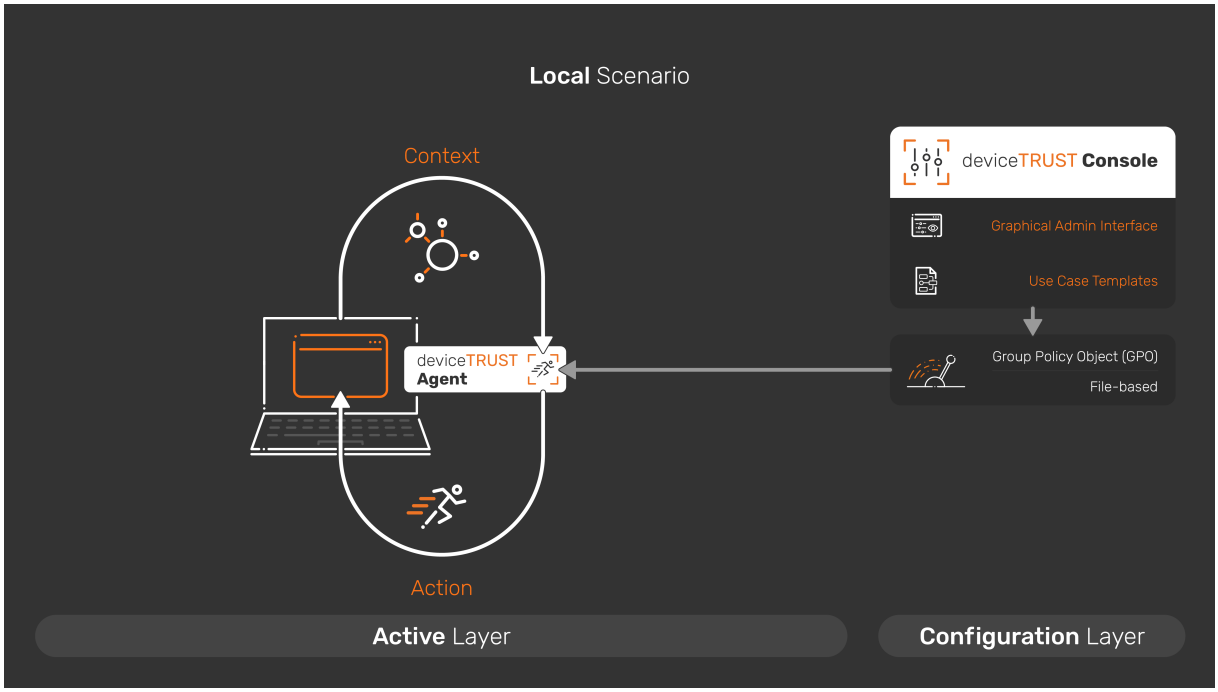
deviceTRUST requires only one main component when installing on local devices, the deviceTRUST Agent. The deviceTRUST component can be installed and configured within minutes and can be fully integrated with existing deployment processes and management tools. No additional infrastructure (e.g. a database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



Remote Scenario

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

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

deviceTRUST Agent

This component needs to be installed on the remoting host that delivers the remote session to the users.

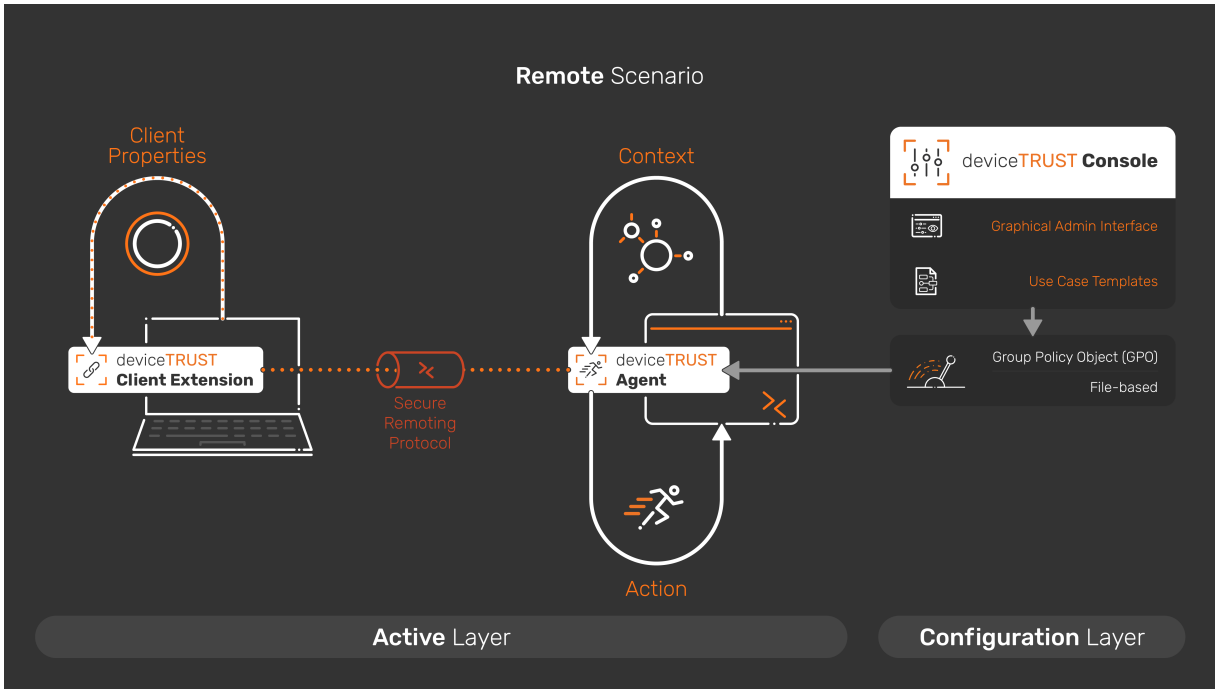
deviceTRUST Client Extension

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

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

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

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



Operating System Compatibility

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

Apple iOS and iPadOS

Compatible operating systems (deviceTRUST® Client Extension):

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

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

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

Apple macOS

Compatible operating systems (deviceTRUST Client Extension):

- Apple macOS 10.15 and later

Compatible technologies:

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

IGEL OS 10 and 11

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops natively integrated in IGEL OS 10.03.500 and later
- Citrix Cloud natively integrated in IGEL OS 10.03.500 and later
- Microsoft Azure Virtual Desktop (AVD) natively integrated in IGEL OS 11.08.200 and later
- Microsoft Remote Desktop natively integrated in IGEL OS 10.03.500 and later

IGEL OS 12

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops available for IGEL OS 12.01.120 and later -1.
- Citrix Cloud natively integrated available for IGEL OS 12.01.120 and later -1.
- Microsoft Azure Virtual Desktop (AVD) available for IGEL OS 12.01.120 and later -1.

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

Microsoft Windows

Compatible operating systems (deviceTRUST Agent and Console):

- Microsoft Windows 10 and later

- Microsoft Windows Server 2012 R2 and later

Compatible operating systems (deviceTRUST Client Extension):

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

Compatible technologies:

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

Stratodesk NoTouch

Compatible technologies (deviceTRUST Client Extension):

- Citrix Virtual Apps and Desktops on NoTouch OS 3.4.516 and later
- Citrix Cloud on NoTouch OS 3.4.516 and later
- Microsoft Remote Desktop on NoTouch OS 3.4.516 and later

Ubuntu Desktop

Compatible operating systems (deviceTRUST Client Extension):

- Ubuntu Desktop 18.04 LTS and later

Compatible technologies:

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

eLux®

Compatible technologies (deviceTRUST Client Extension):

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

Platform Compatibility

- Citrix Systems
- Microsoft

Citrix Systems

Compatible technologies:

- Citrix Virtual Apps and Desktops™
- Citrix Cloud™

Compatible operating systems:

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later
- Apple macOS 10.15 and later
- IGEL OS 10.03.500 and later
- Microsoft Windows 10 and later
- Microsoft Windows Server 2012 R2 and later
- Stratodesk NoTouch OS 3.4.516 and later
- Ubuntu Desktop 18.04 LTS and later
- eLux® 7

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

Microsoft

Compatible technologies:

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

Compatible operating systems:

- Apple iOS 13.x and later
- Apple iPadOS 13.x and later
- Apple macOS 10.15 and later (via FreeRDP 2)
- IGEL OS 11.08.200 or later
- Microsoft Windows 10 and later

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

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

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

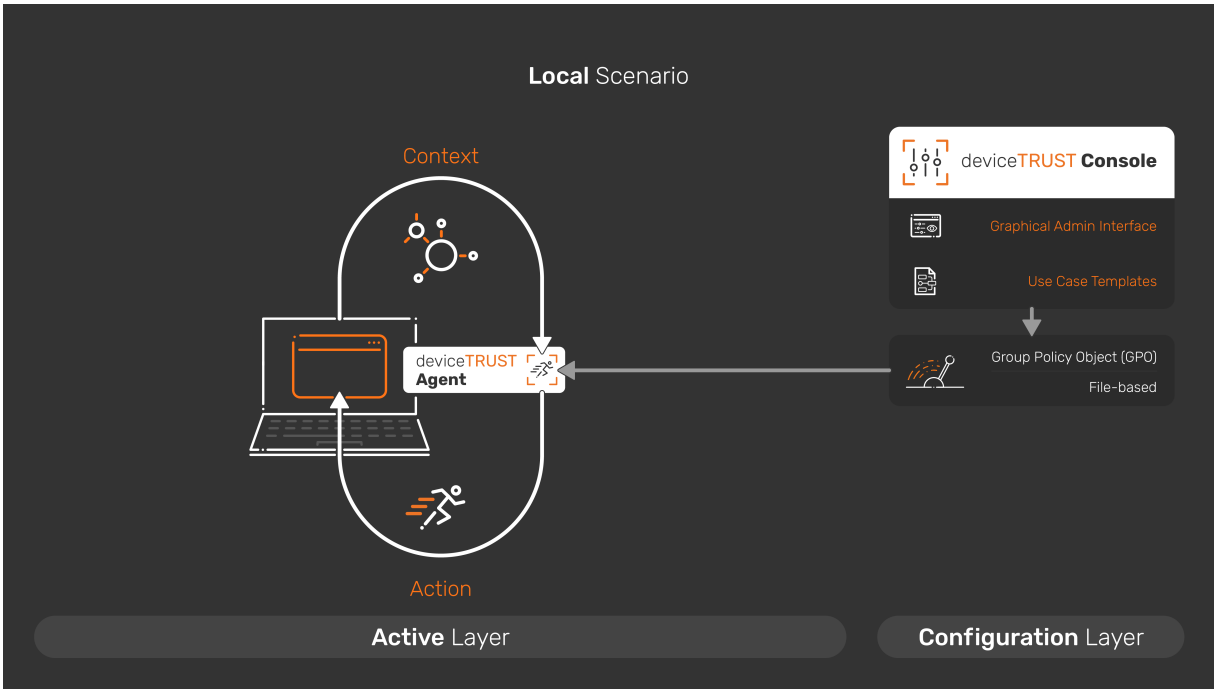
In remote scenarios, deviceTRUST transports the context information from the users remote device into the virtual session where the configuration is enforced. Please visit Getting Started for Remote Devices to begin the guide.

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.



We will perform the following steps:

- Step 1: Download the deviceTRUST setup binaries
- Step 2: Install the deviceTRUST Agent
- Step 3: Install the deviceTRUST Console
- Step 4: Enter your deviceTRUST License
- Step 5: Create and apply a file based configuration
- Step 6: Test the Unauthorized USB Device use case

Step 1: Download the deviceTRUST setup binaries

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

Step 2: Install the deviceTRUST Agent

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

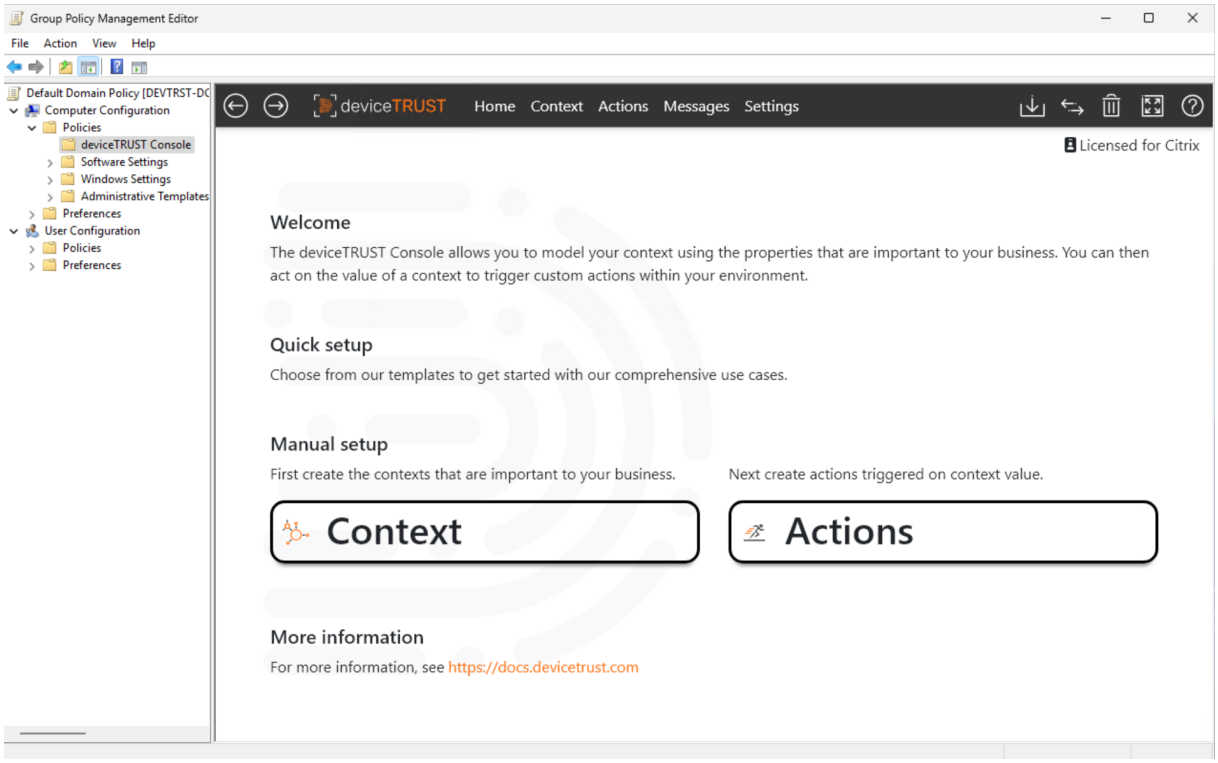
Step 3: Install the deviceTRUST Console

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

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

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

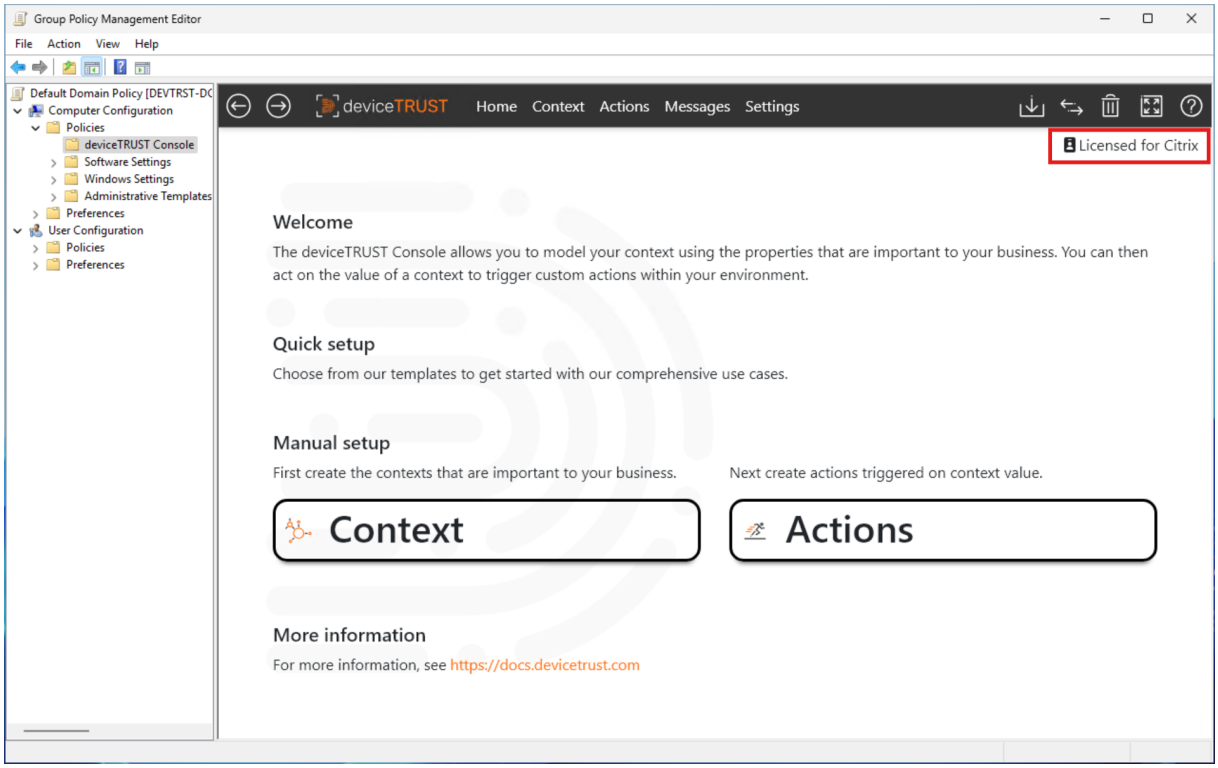
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



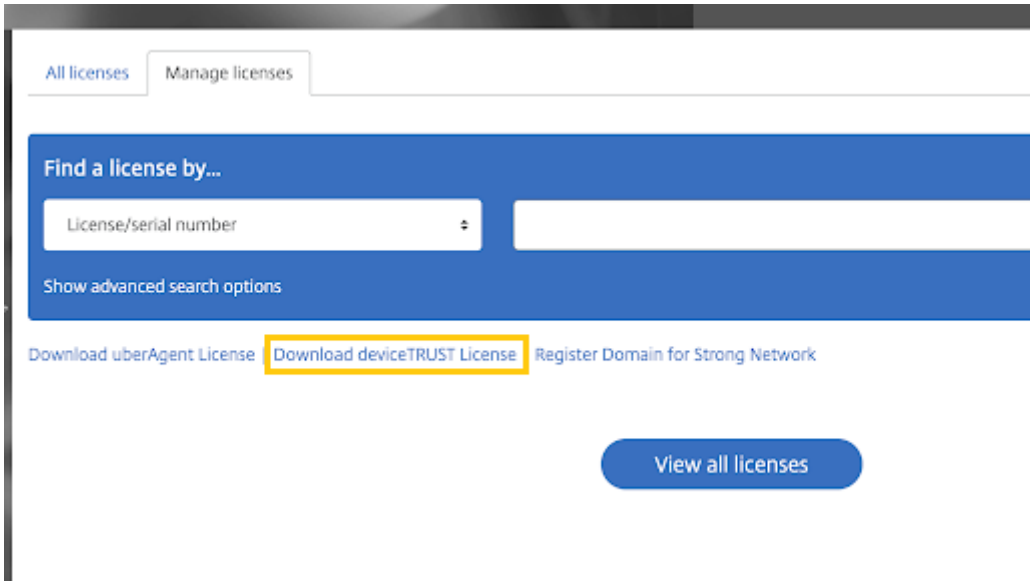
Step 4: Enter your deviceTRUST License

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

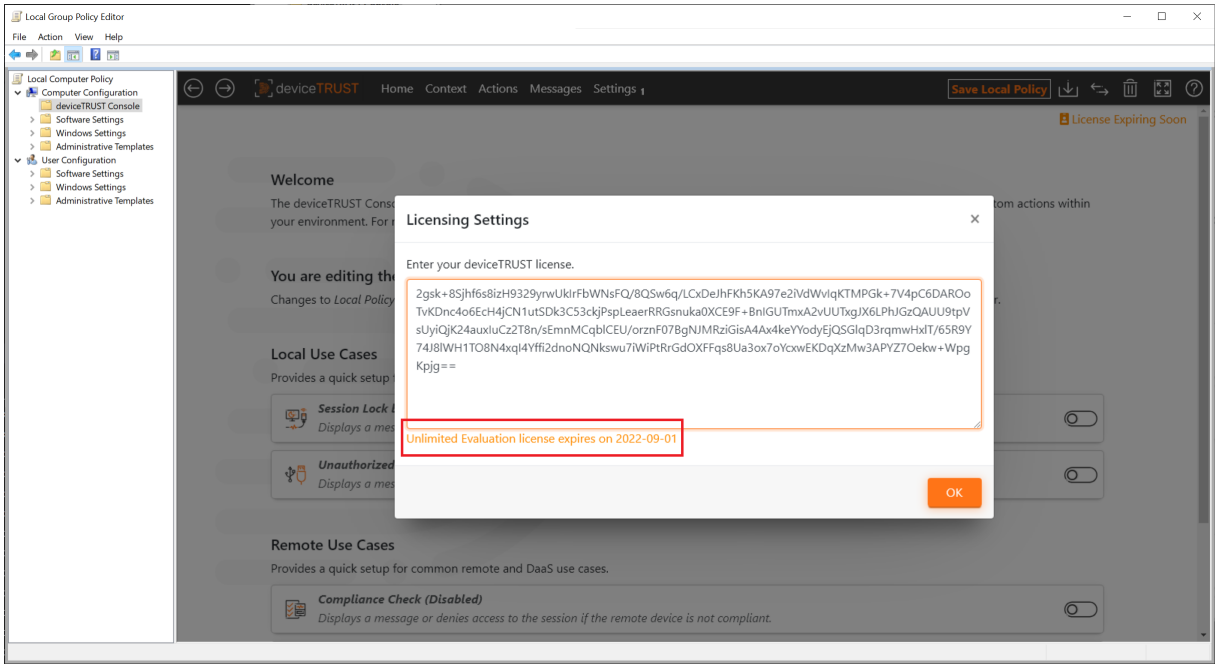
To add the license into the deviceTRUST contextual security policy open the Local Policy Editor and navigate to `DEVICETRUST CONSOLE` and click on the `LICENSED FOR CITRIX®` link on the homepage.



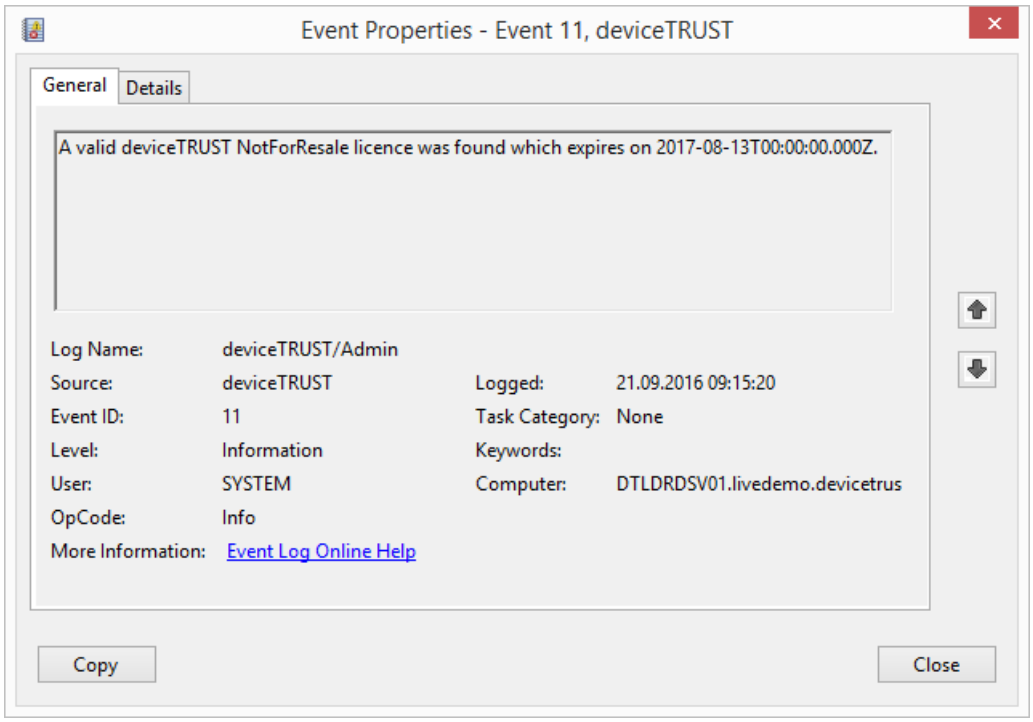
Dependent on your license, your individual deviceTRUST license can be found in your MyCitrix Portal.



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



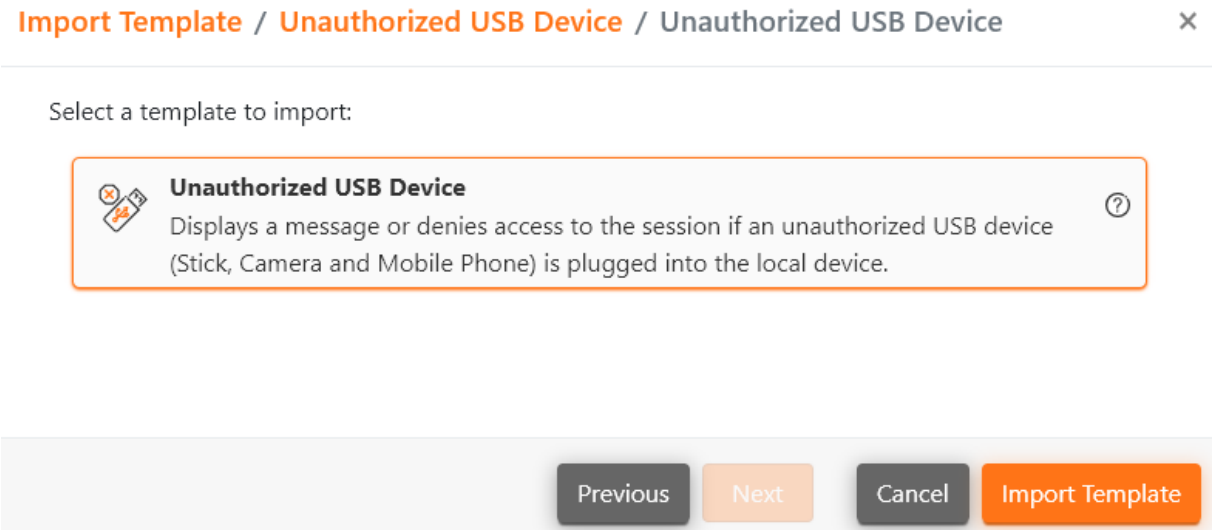
deviceTRUST is now enabled and will work for all users except local administrators connecting to that remoting or DaaS host system with deviceTRUST Agent installed. To check if you have added a valid deviceTRUST license, open the Windows Event Log and navigate to `APPLICATION AND SERVICE LOGS\DEVICETRUST\ADMIN`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



Step 5: Create and apply a file based configuration

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

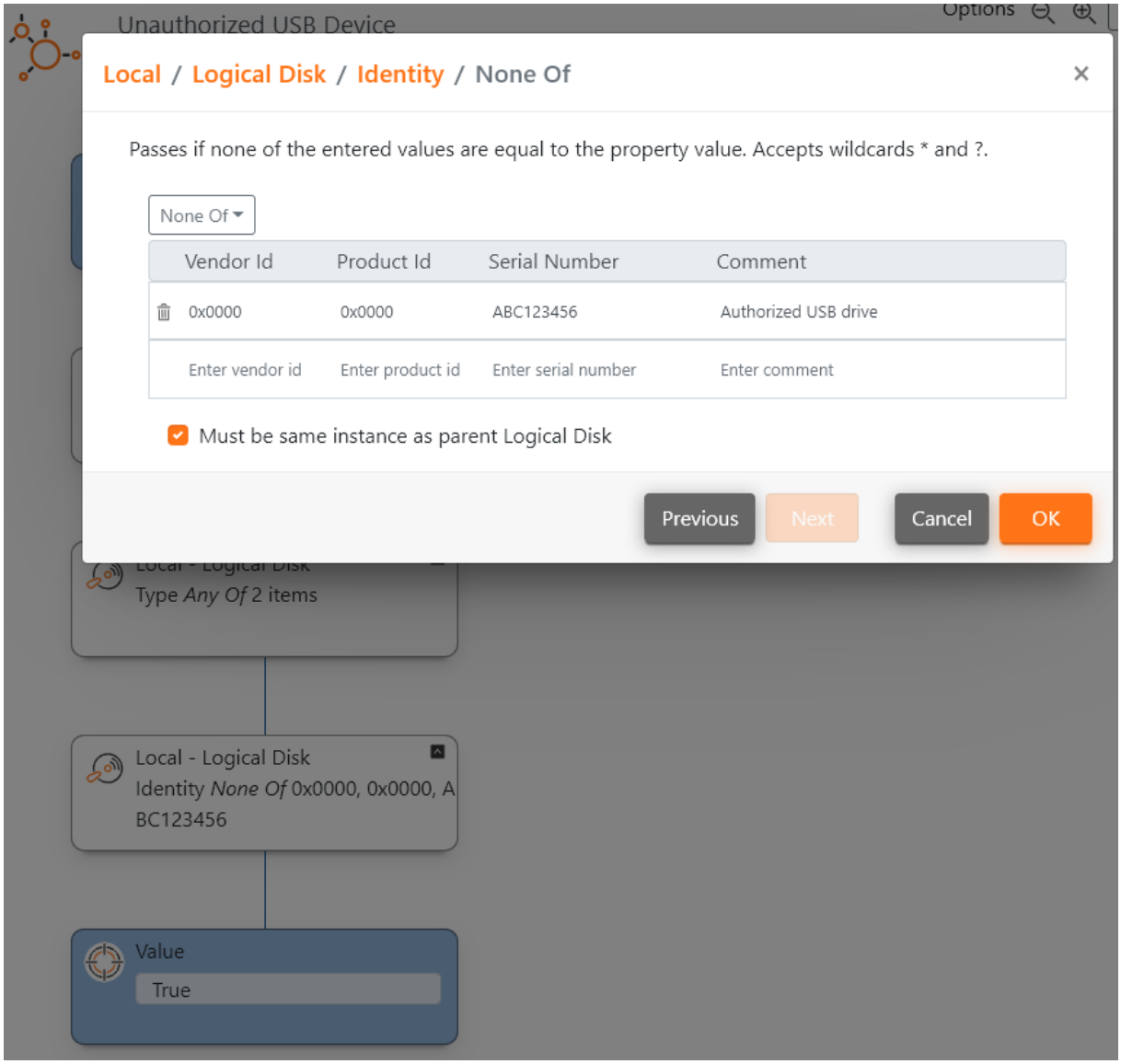
Select `Sharing` top right and click `Import Template`, `Local`, `Unauthorized USB Device`, `Unauthorized USB Device` and confirm with `Import Template` at the bottom.



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

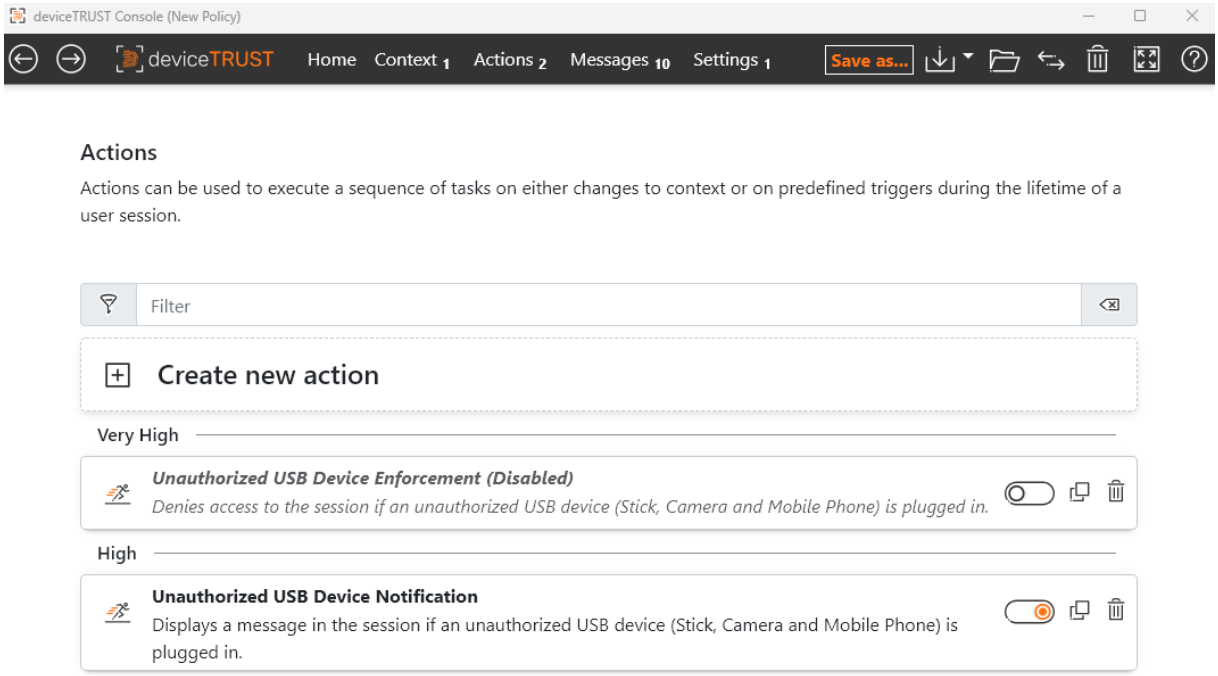
At the top of the console you´ll find the count of configured Context, Actions, Messages, Settings.

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



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

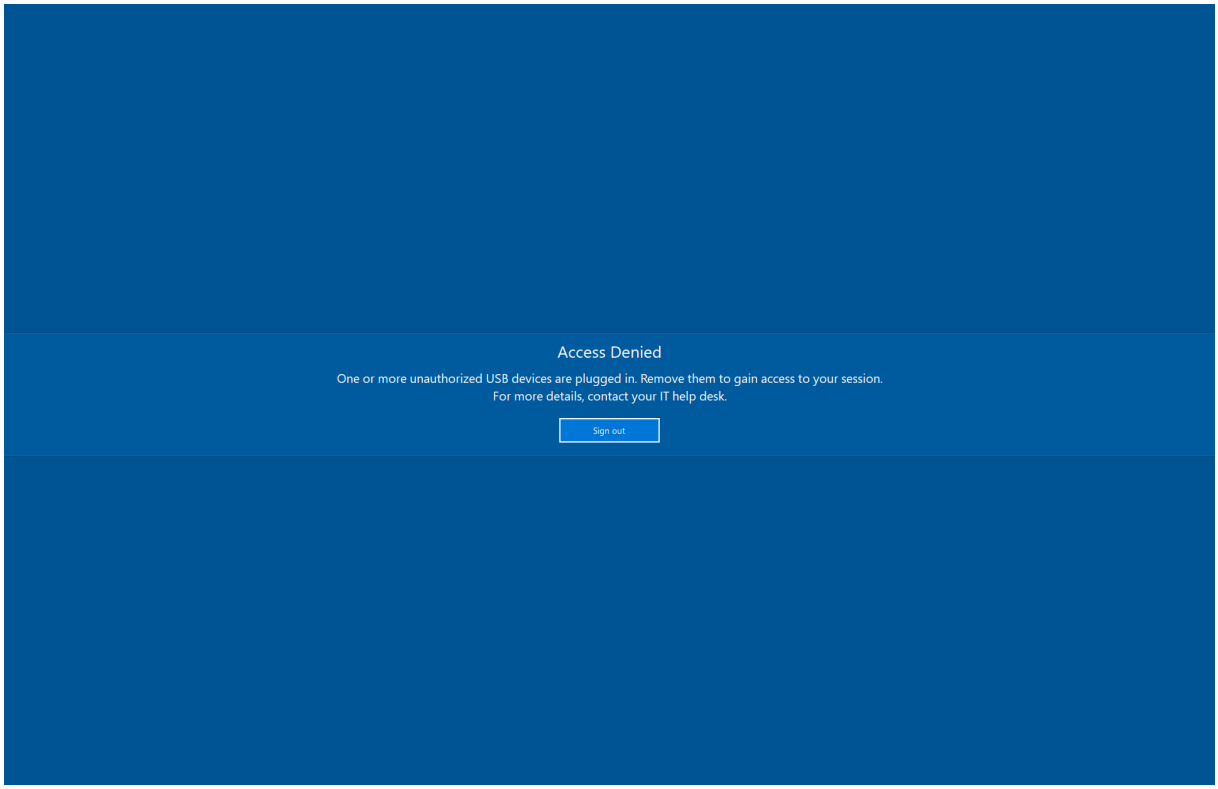
Select Actions and see one active (Unauthorized USB Device Notification) and one disabled (Unauthorized USB Device - Enforcement) action.
Depending on whether you only want to inform about the execution of the policy or block access, select what should be active using the Enable/Disable toggle on the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



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

Step 6: Test the Unauthorized USB Device use case

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

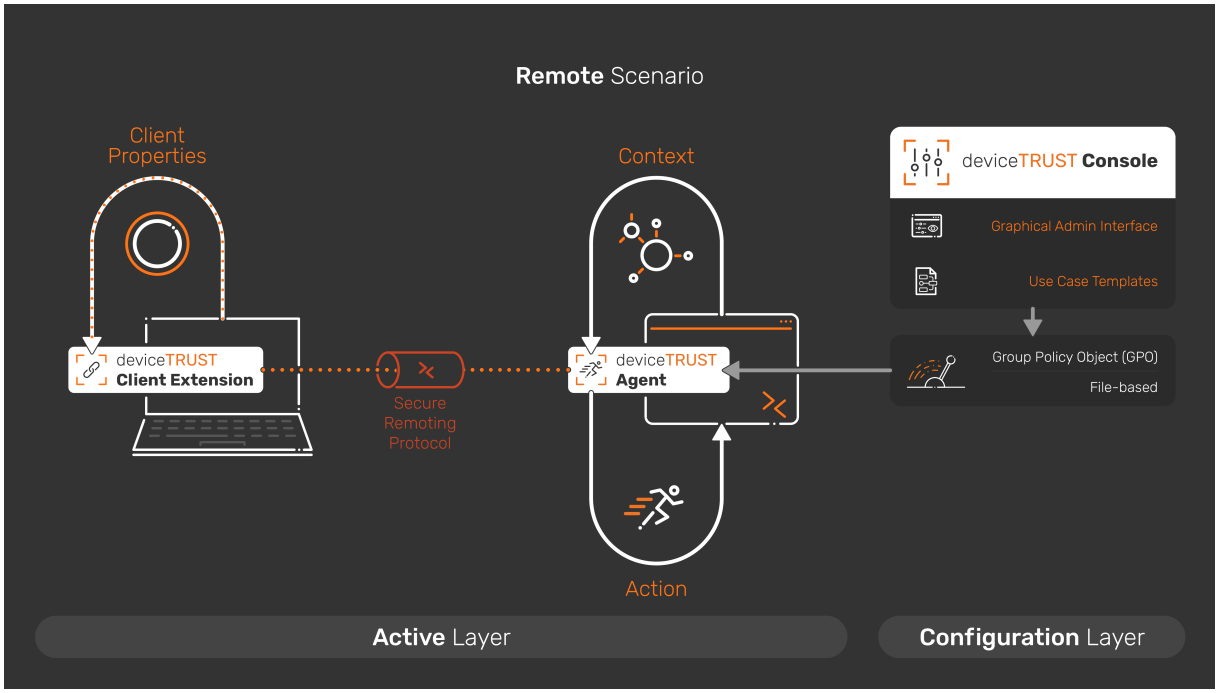


Troubleshooting

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

Getting Started for Remote

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



We will perform the following steps:

- Prerequisites
- Option 1: Citrix® installation packages
    - 1.1: Download the Citrix product software
    - Step 1.2: Install Citrix deviceTRUST
    - Step 1.3: Install the deviceTRUST Console
    - Step 1.4: Enter your deviceTRUST License
    - Step 1.5: Install the xdeviceTRUST Client Extension on a Microsoft Windows device
- Option 2: Manual installation
    - Step 2.1: Download the deviceTRUST setup binaries
    - Step 2.2: Install the deviceTRUST Agent
    - Step 2.3: Install the deviceTRUST Console
    - Step 2.4: Enter your deviceTRUST License
    - Step 2.5: Install the deviceTRUST Client Extension on a Microsoft Windows device
- Set up a simple use case
    - Step 1: Create and apply a file based configuration
    - Step 2: Check the access to your VDA when the deviceTRUST Client Extension is not installed
    - Step 3: Test the Compliance Check use case from a Microsoft Windows device

Prerequisites

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

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

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

- **Endpoint device:**

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

- **Policy management device:**

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

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

- **Citrix Policy Management:**

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

- **Test user account:**

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

If you plan to use deviceTRUST in combination with other tools (e.g. Microsoft AppLocker or FSLogix App Masking), ensure that these components are installed and working properly.
If deviceTRUST is intended to take over functionality previously managed by other tools (e.g. clipboard redirection via Citrix Policy), make sure those features are disabled or unconfigured to avoid conflicts.

Option 1: Citrix installation packages

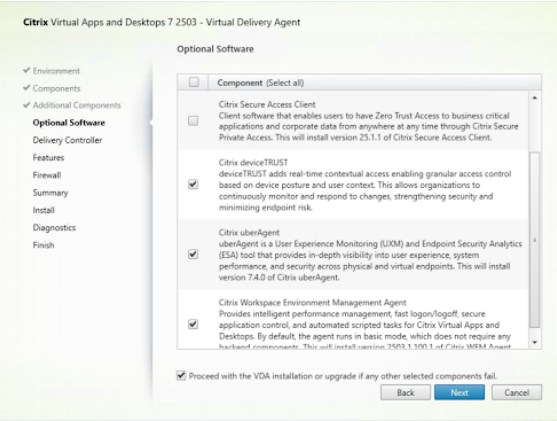
1.1: Download the Citrix product software

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

Follow the VDA installation guide to get the right version.

Step 1.2: Install Citrix deviceTRUST

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



Check the box and proceed with the installation.

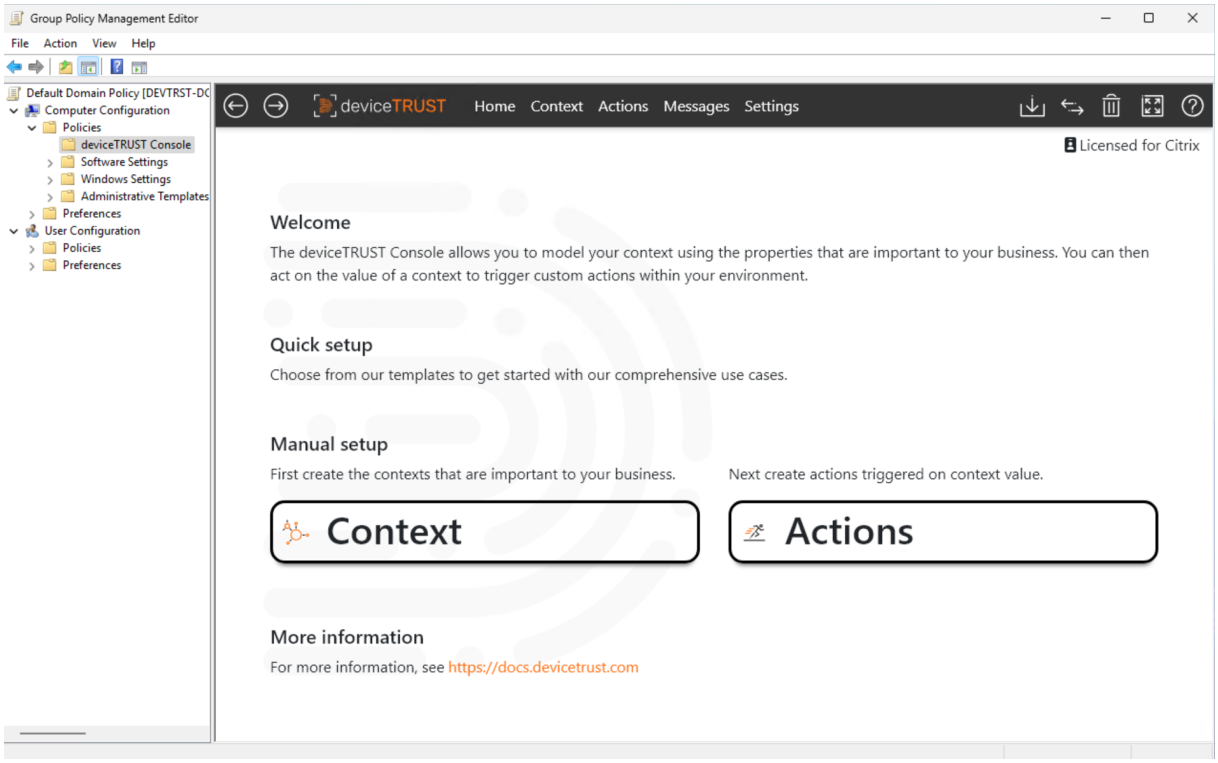
Step 1.3: Install the deviceTRUST Console

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

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

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

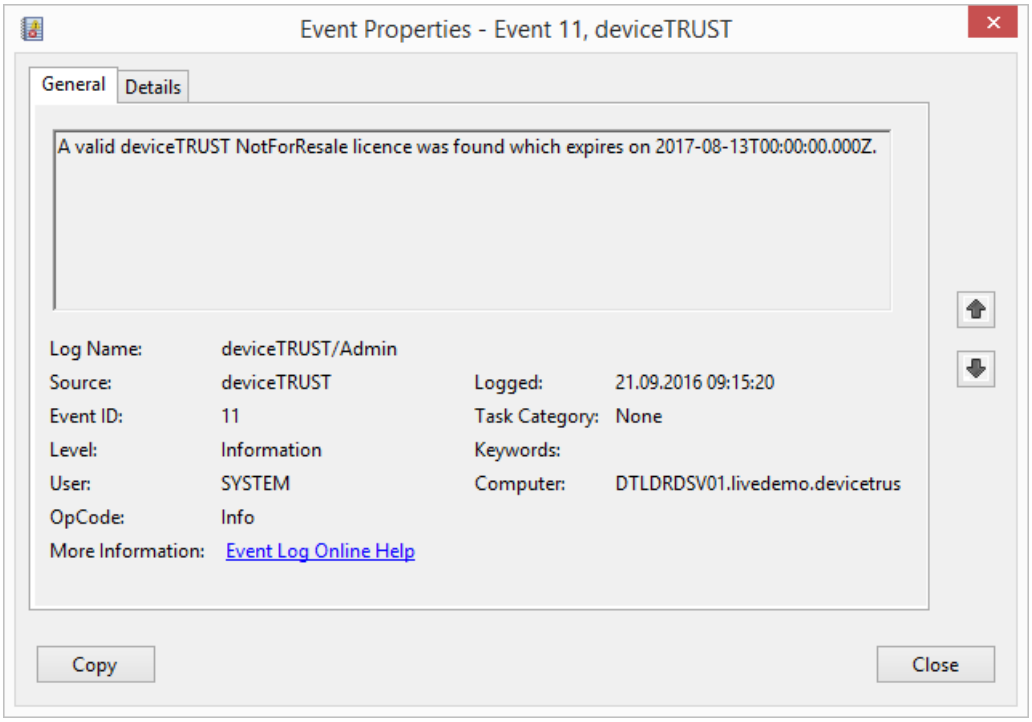
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION\DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



Step 1.4: Enter your deviceTRUST License

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

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



Step 1.5: Install the deviceTRUST Client Extension on a Microsoft Windows device

Follow the information on Installation Client Extension page.

Option 2: Manual installation

Step 2.1: Download the deviceTRUST setup binaries

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

Step 2.2: Install the deviceTRUST Agent

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

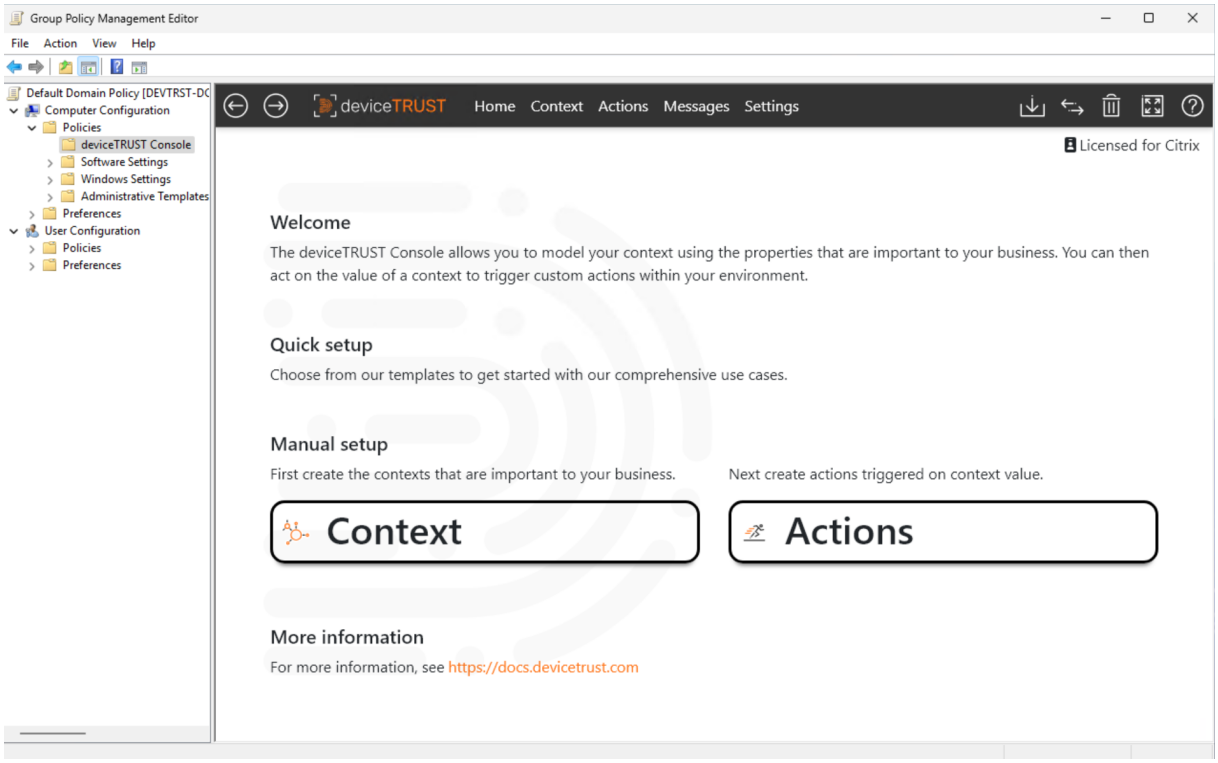
Step 2.3: Install the deviceTRUST Console

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

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

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

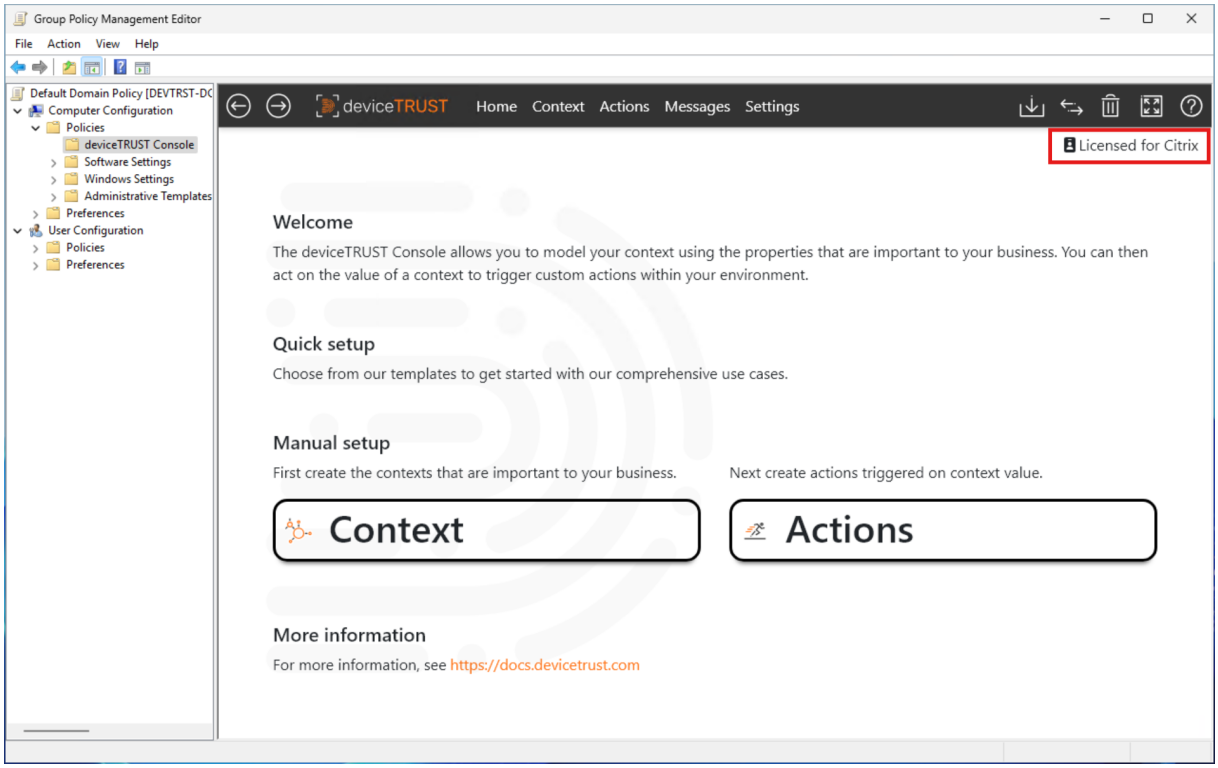
The deviceTRUST Console includes a node within the Local Policy Editor `COMPUTER CONFIGURATION \DEVICETRUST CONSOLE` which can be used to model the context of a user, and then act on changes to that context by triggering custom actions within your environment.



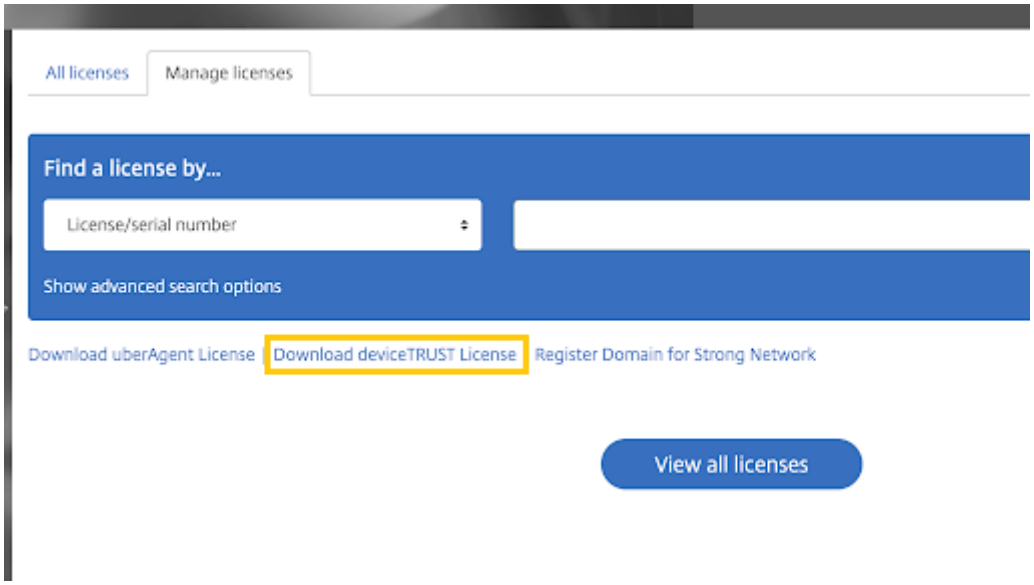
Step 2.4: Enter your deviceTRUST License

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

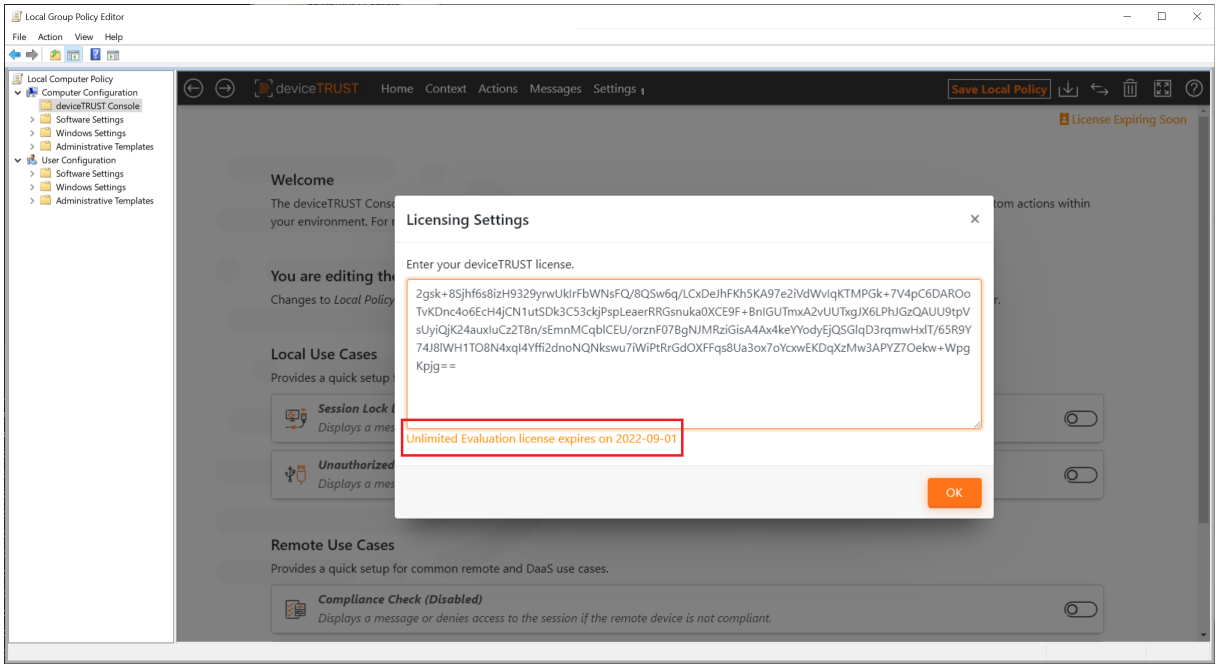
To add the license into the deviceTRUST contextual security policy open the Local Policy Editor and navigate to `DEVICETRUST CONSOLE` and click on the `UNLICENSED` link on the homepage.



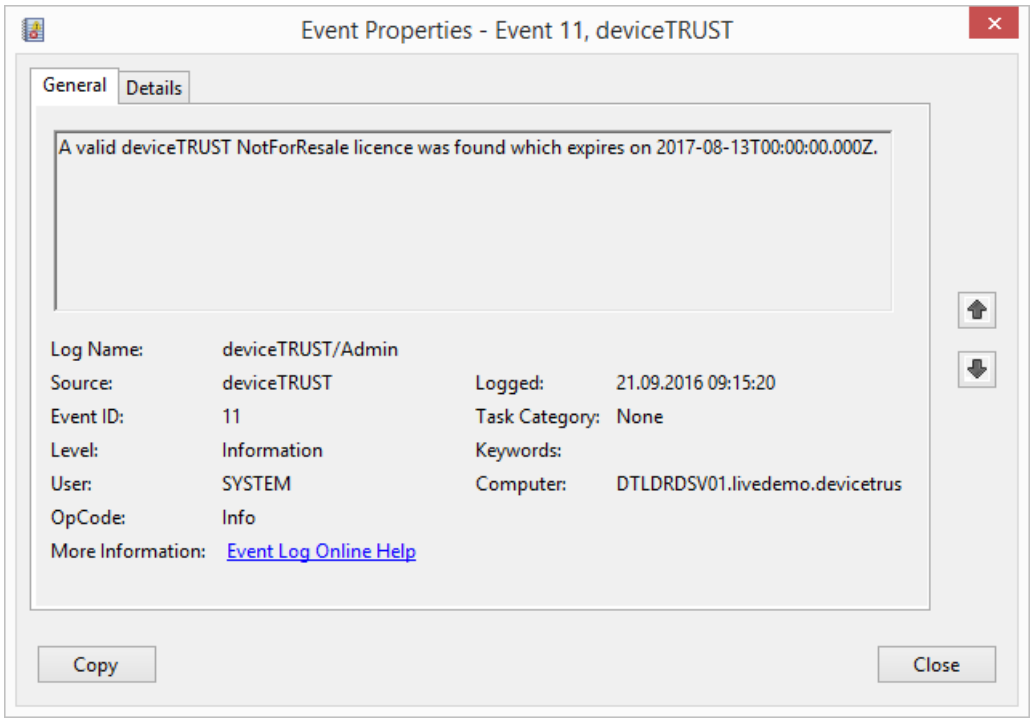
Dependent on your license, your individual deviceTRUST license can be found in your MyCitrix Portal.



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



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.



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

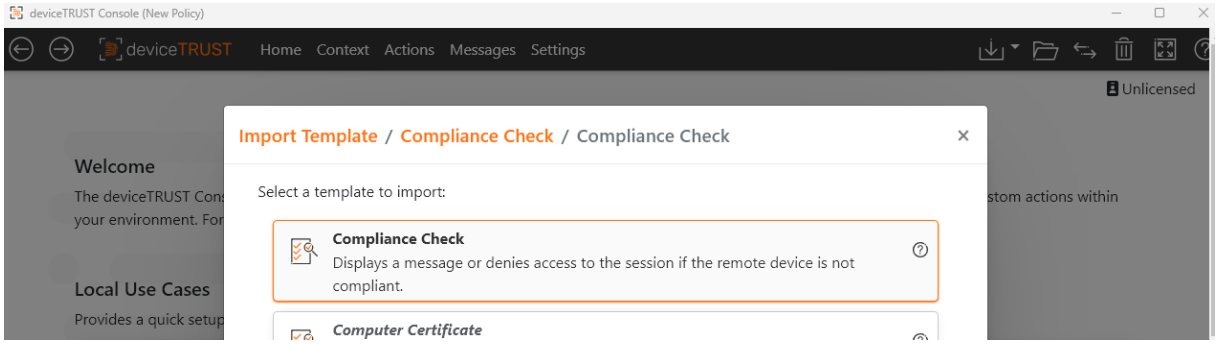
Within the Getting Started Guide, for simplicity, we will only install the deviceTRUST Client Extension on a Microsoft Windows device. Other device operating systems are also supported and an overview of how to install the deviceTRUST Client Extension on the particular operating system can be found on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

Set up a simple use case

Step 1: Create and apply a file based configuration

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

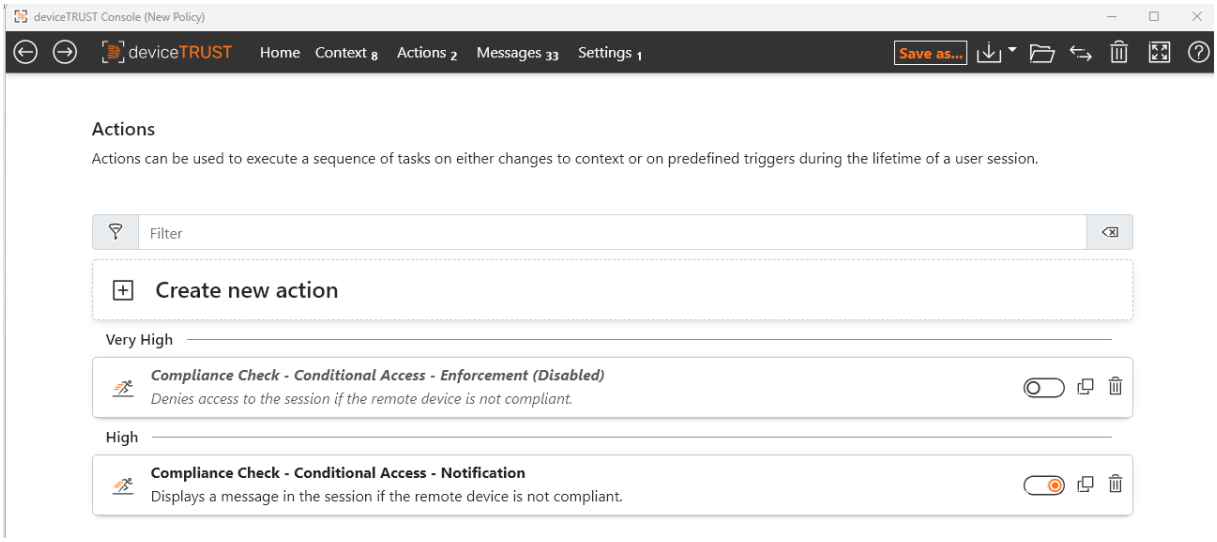
Select `Sharing` top right and click `Import Template`, `Compliance Check`, `Compliance Check` and confirm with `Import Template` at the bottom.



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

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

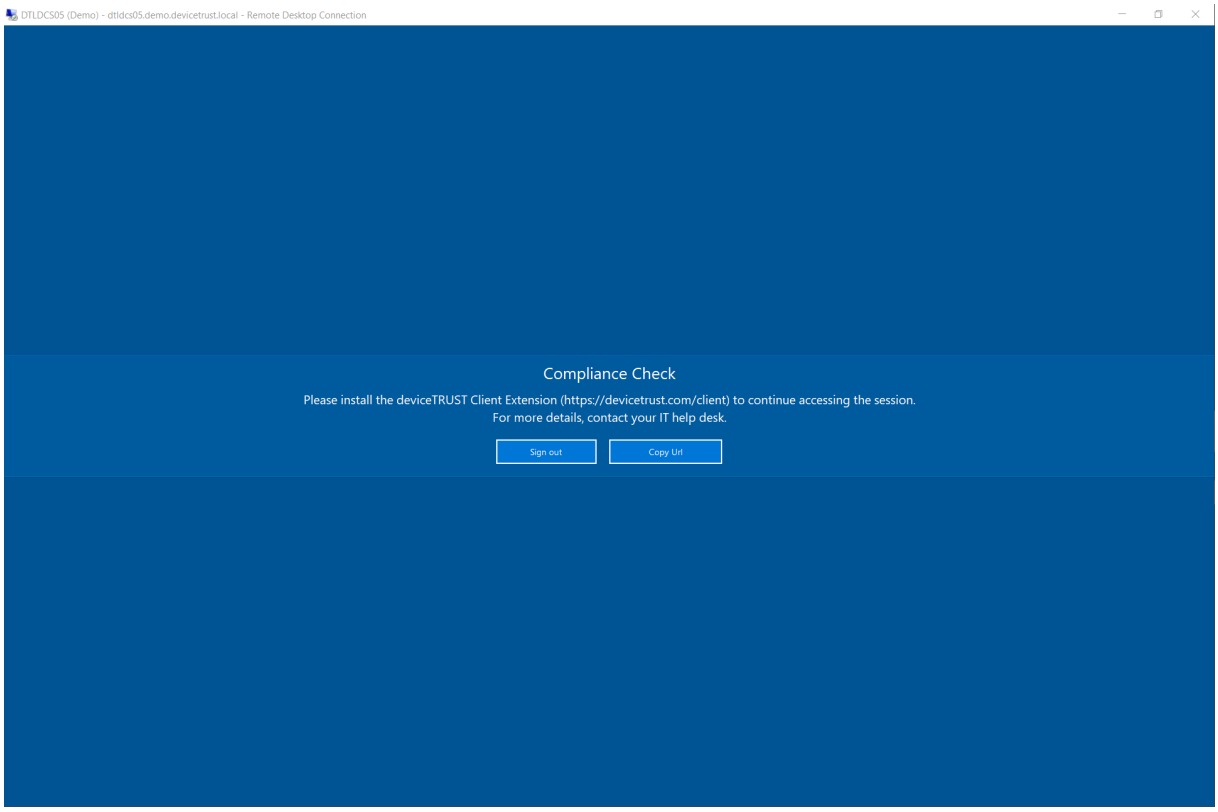
Select `Actions` and see one active (Compliance Check - Conditional Access - Notification) and one disabled (Compliance Check - Conditional Access - Enforcement) action.
Depending on whether you only want to inform about the execution of the policy or block access, select what should be active using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



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

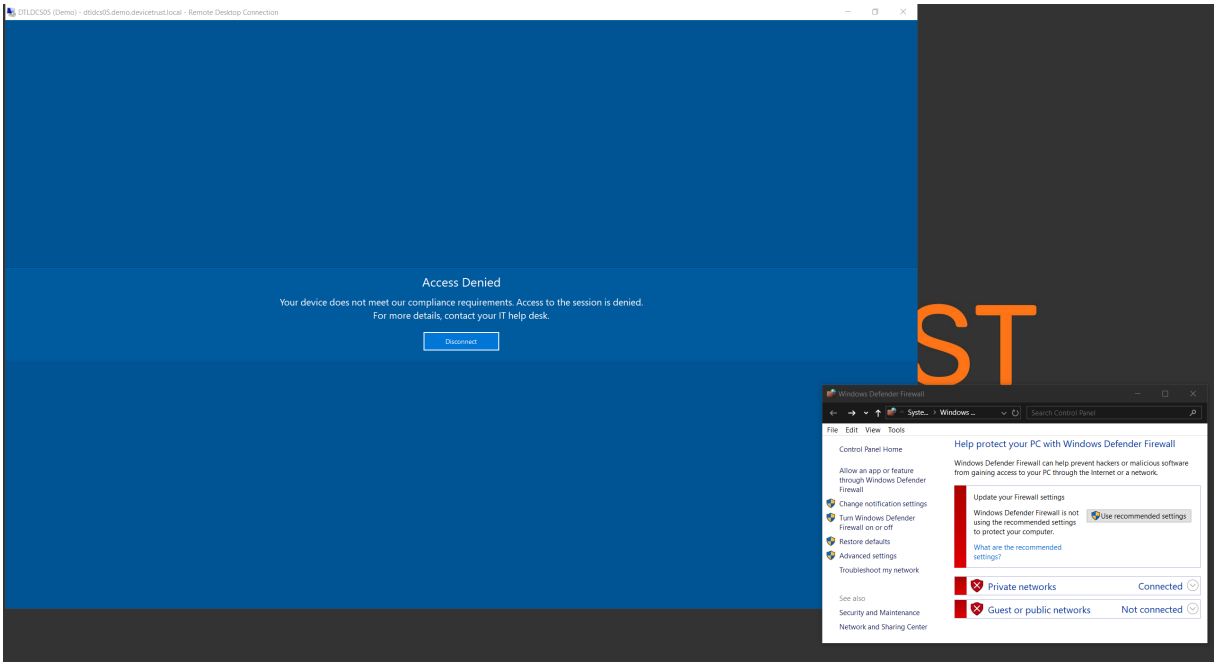
Step 2: Check the access to your VDA when the deviceTRUST Client Extension is not installed

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



Step 3: Test the Compliance Check use case from a Microsoft Windows device

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



Troubleshooting

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

Downloads

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

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

Download deviceTRUST Client Extension 2503 CR for eLux® 7

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

Download deviceTRUST Agent and Console 2503 CR

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

Installation

TABLE OF CONTENTS

Installing the deviceTRUST Agent

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

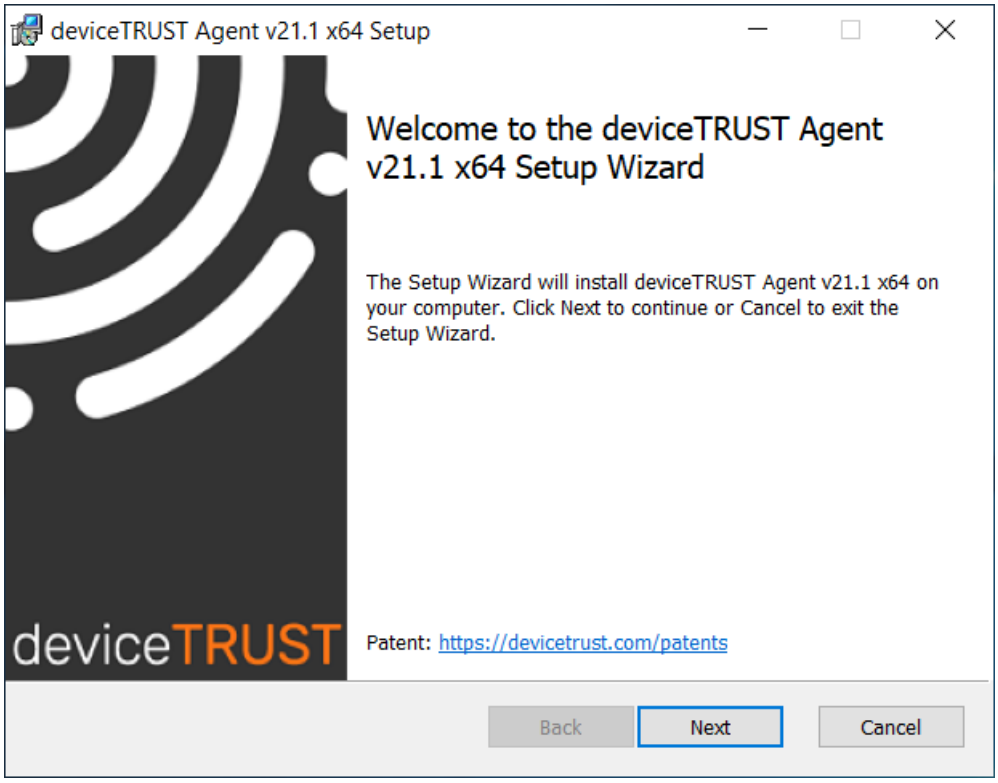
Option 1: Install Citrix VDA 2503 or later

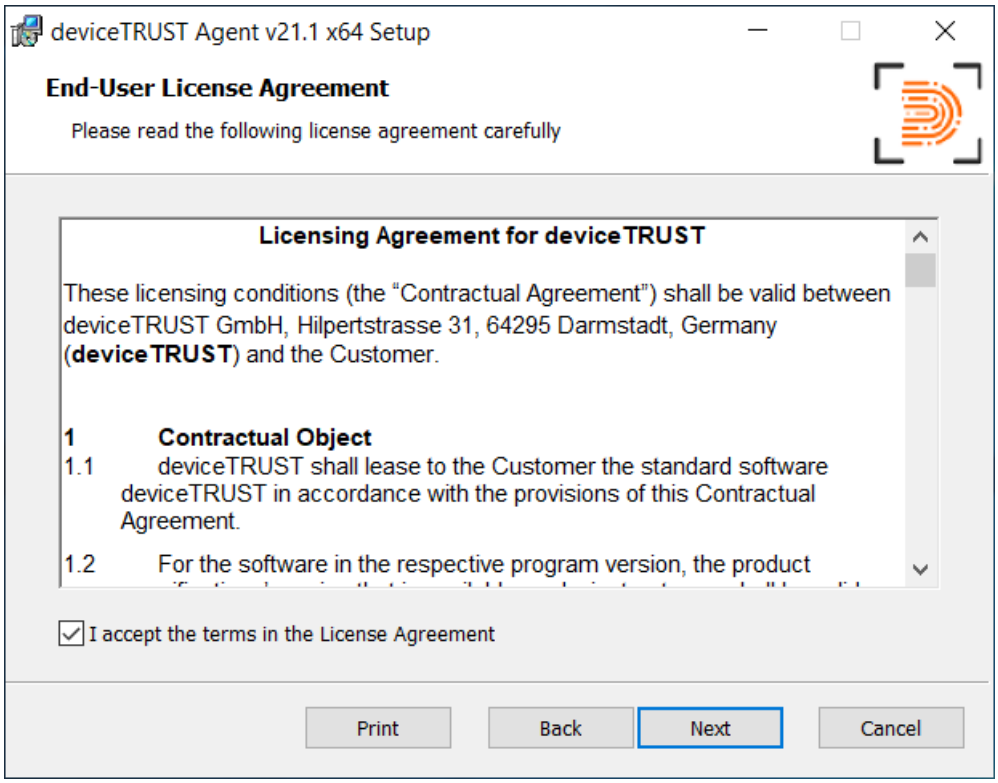
The deviceTRUST Agent is now installed by default as part of the Citrix Virtual Apps and Desktops VDA installation when using release 2503 or later. This can be downloaded from Citrix Downloads.

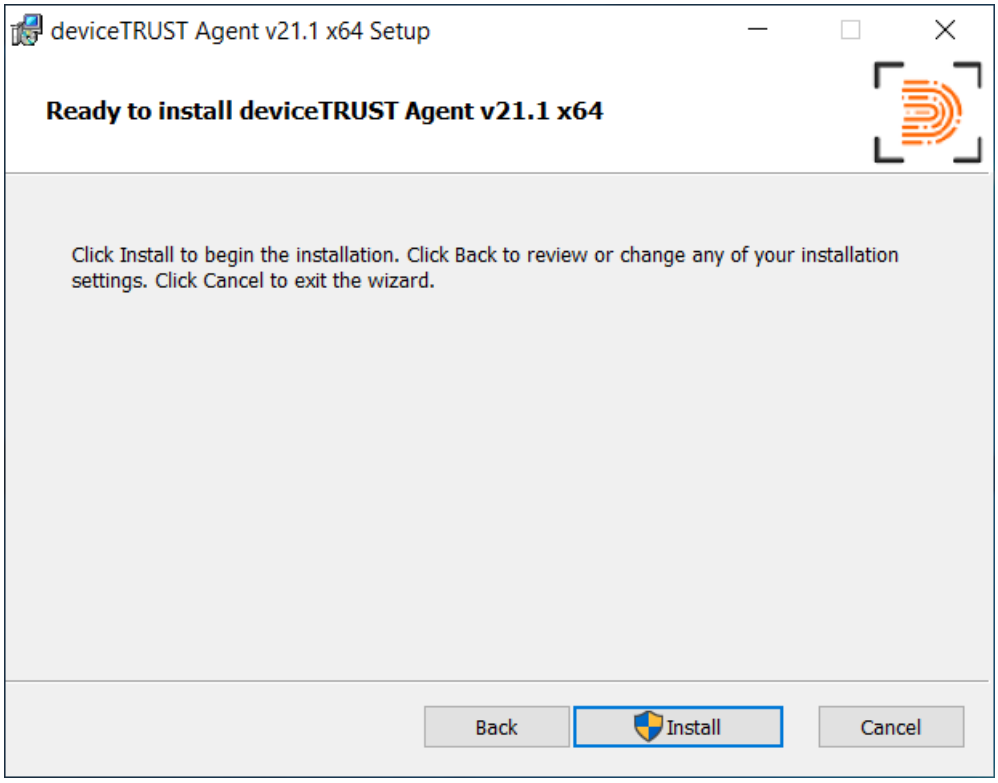
> **Important:**
>
> When using Citrix Virtual Apps and Desktops™, you may need to edit the Virtual channel allow list policy to allow the deviceTRUST Agent to open a virtual channel to the deviceTRUST Client Extension.

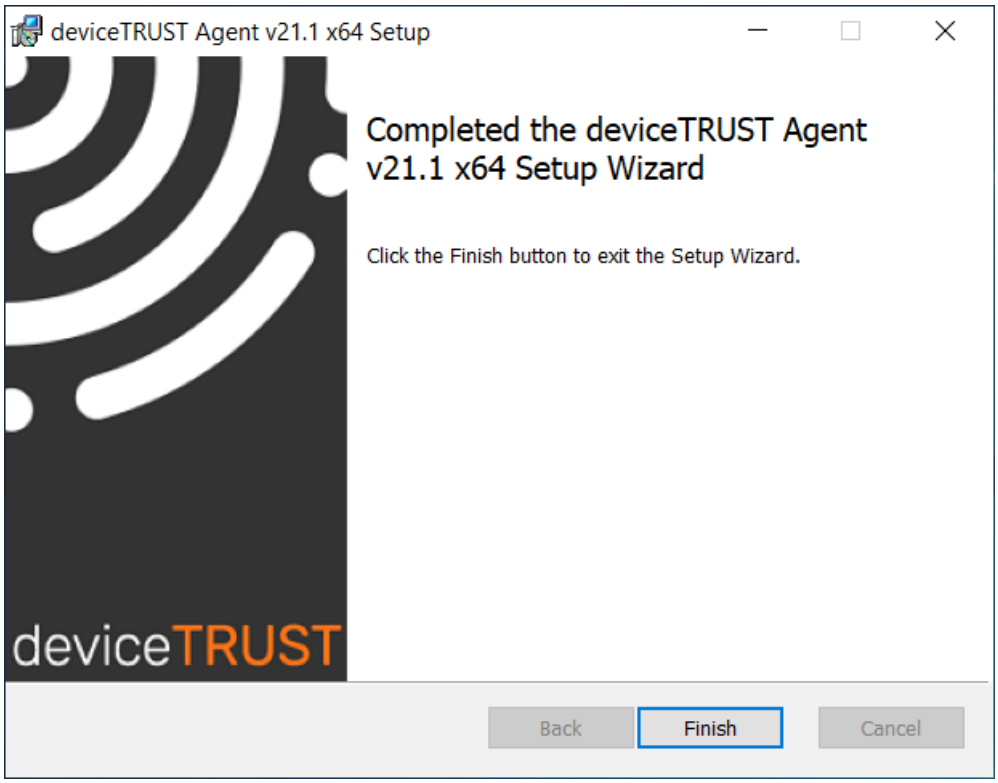
Option 2: Manual Installation

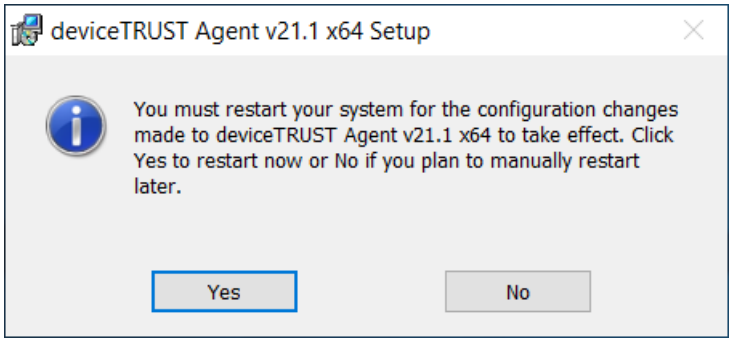
The deviceTRUST Agent requires a user account with local administrative privileges to install the deviceTRUST Agent on the target system. The installation can be performed by following the steps of the deviceTRUST Agent installer.











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

Note:

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

Option 3: Unattended Installation

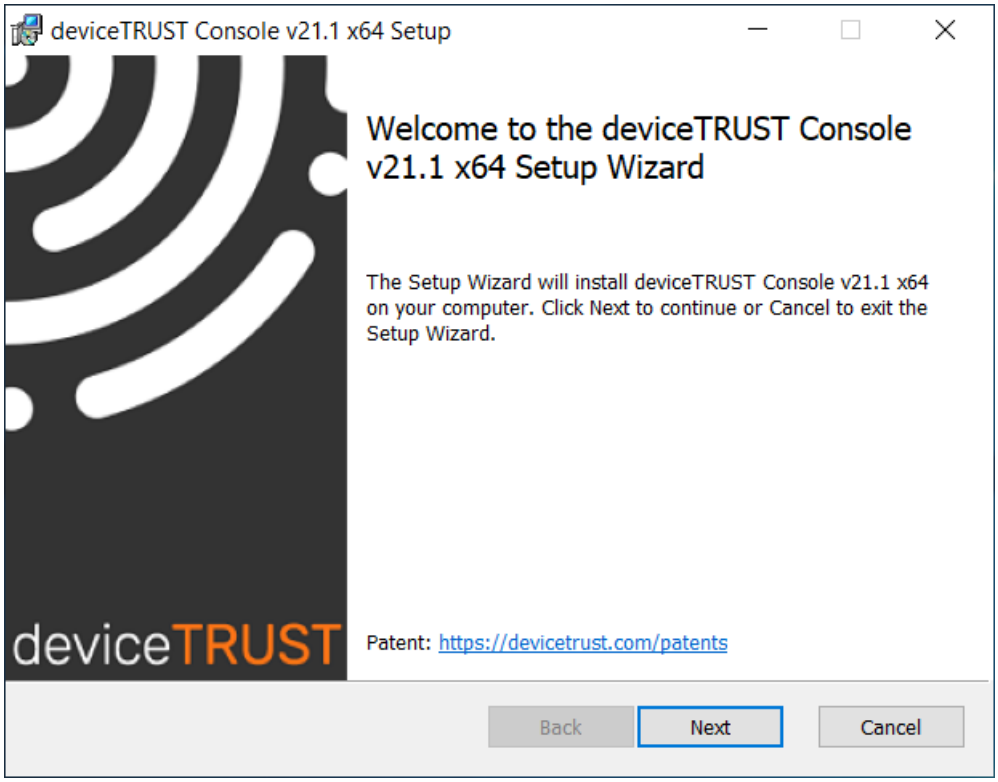
The deviceTRUST Agent can be installed unattended from the command line interface with the following options:

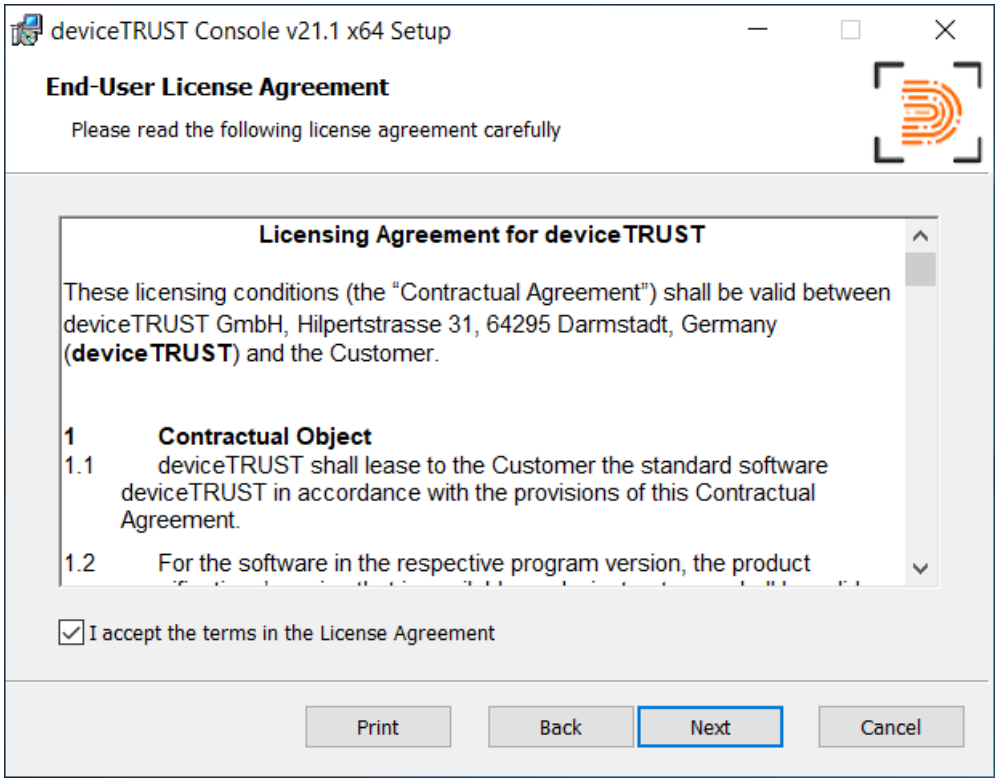
Component	Commandline
dtagent-x64-release-x.x.x.x.msi	The deviceTRUST Agent installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters: `MSIEXEC.EXE /I DTAGENT-X64-RELEASE-X.X.X.X.MSI /PASSIVE /FORCERESTART`

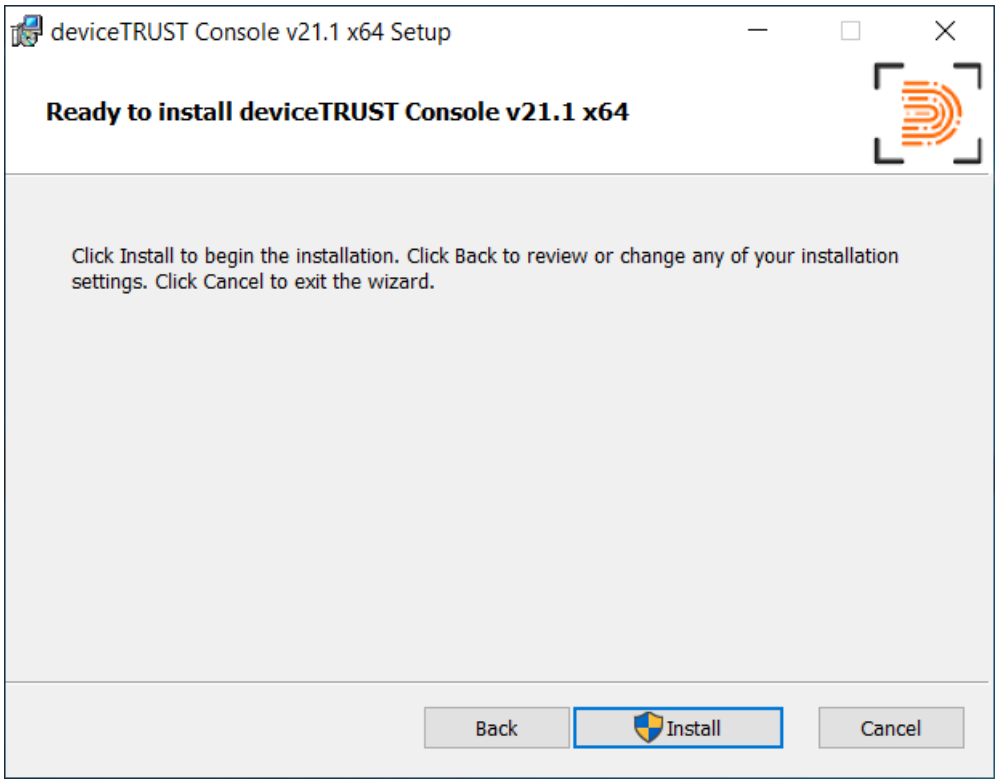
> **Note:**
>
> When using Citrix Virtual Apps and Desktops, you may need to edit the Virtual channel allow list policy to allow the deviceTRUST Agent to open a virtual channel to the deviceTRUST Client Extension.

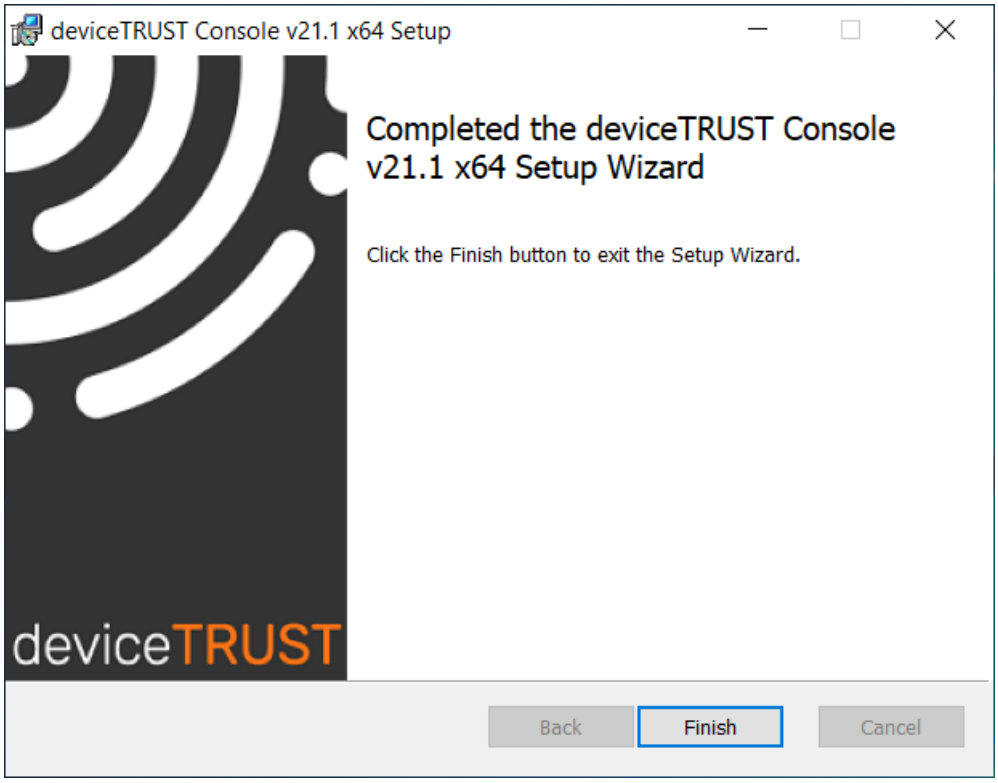
Installing the deviceTRUST Console

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









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

Unattended Installation

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

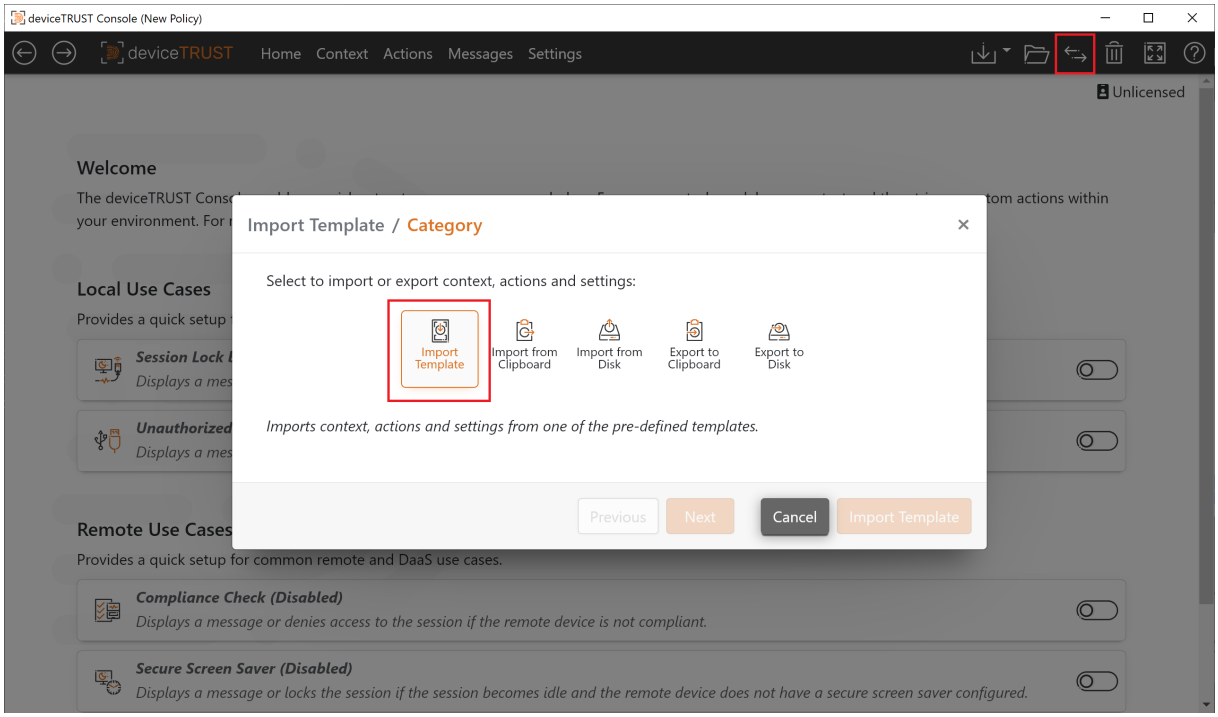
Component	Commandline
dtconsole-x64-release-x.x.x.x.msi	The deviceTRUST Console installer file can be customized by common Microsoft Windows Installer parameters. An unattended installation can be achieved with the following parameters: `MSIEXEC.EXE /I DTCONSOLE-X64-RELEASE-X.X.X.X.MSI /PASSIVE`

Installing the deviceTRUST Client Extension

TABLE OF CONTENTS

Templates

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



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

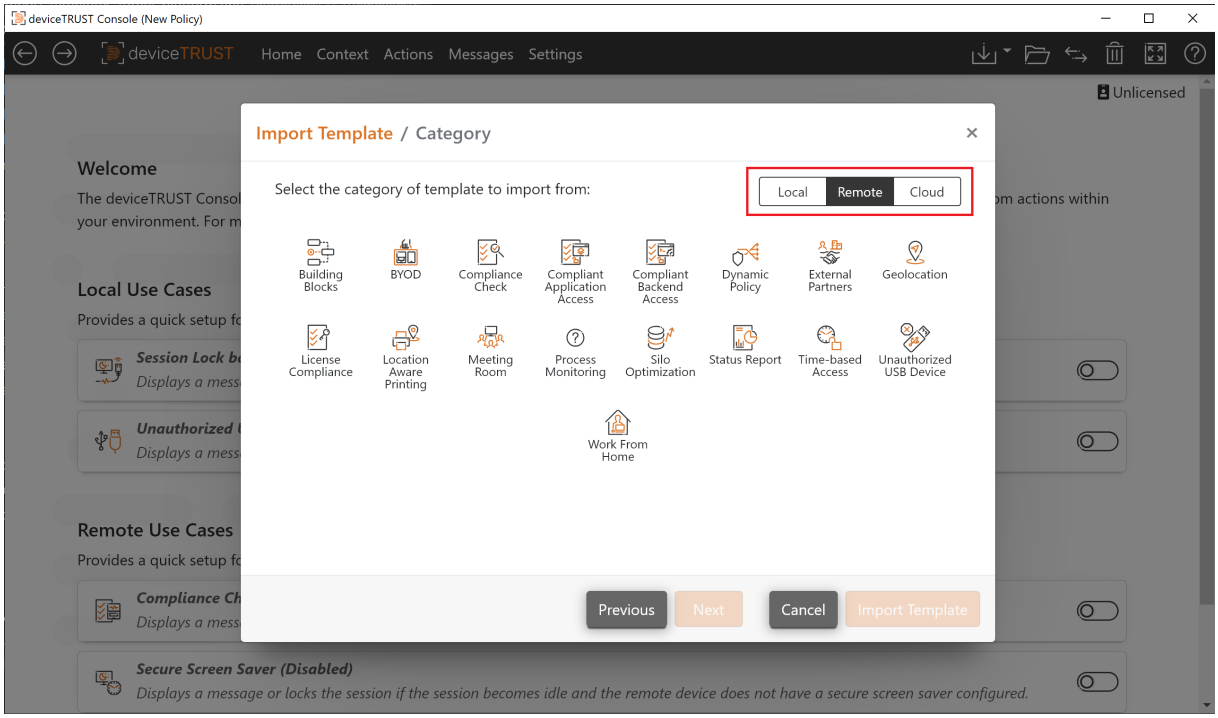


TABLE OF CONTENTS

Local Templates

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

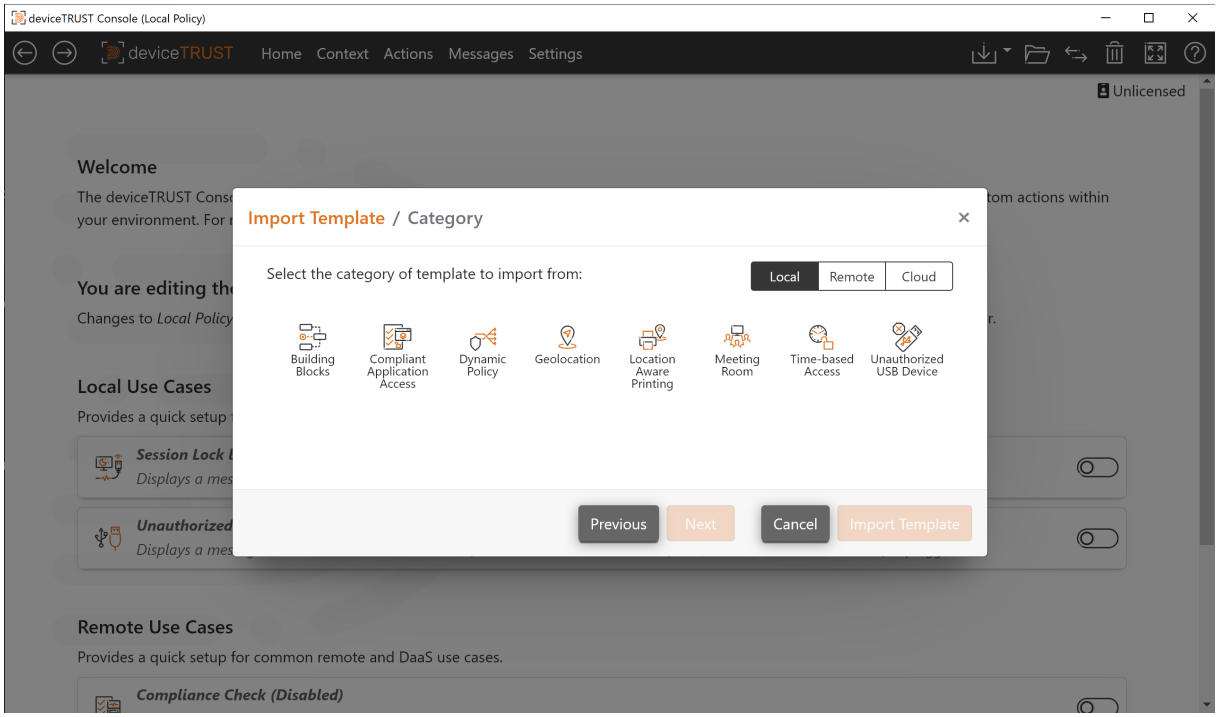


TABLE OF CONTENTS

Remote Templates

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

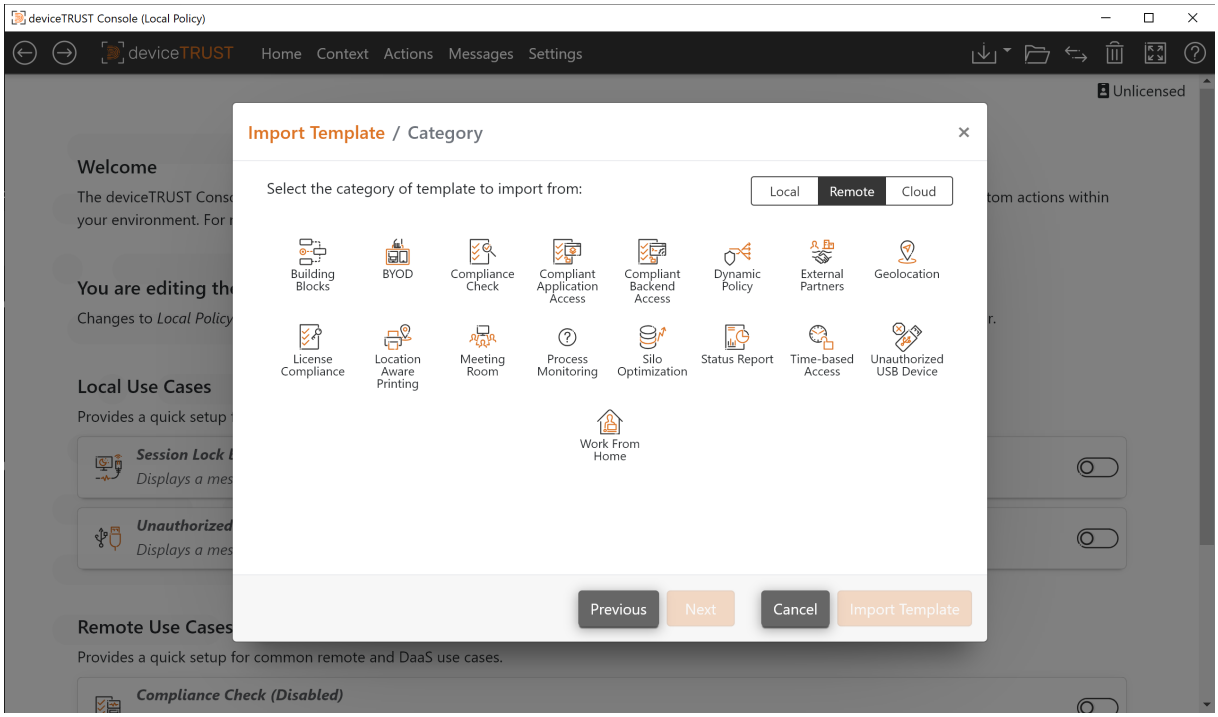


TABLE OF CONTENTS

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

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

SaaS Templates

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

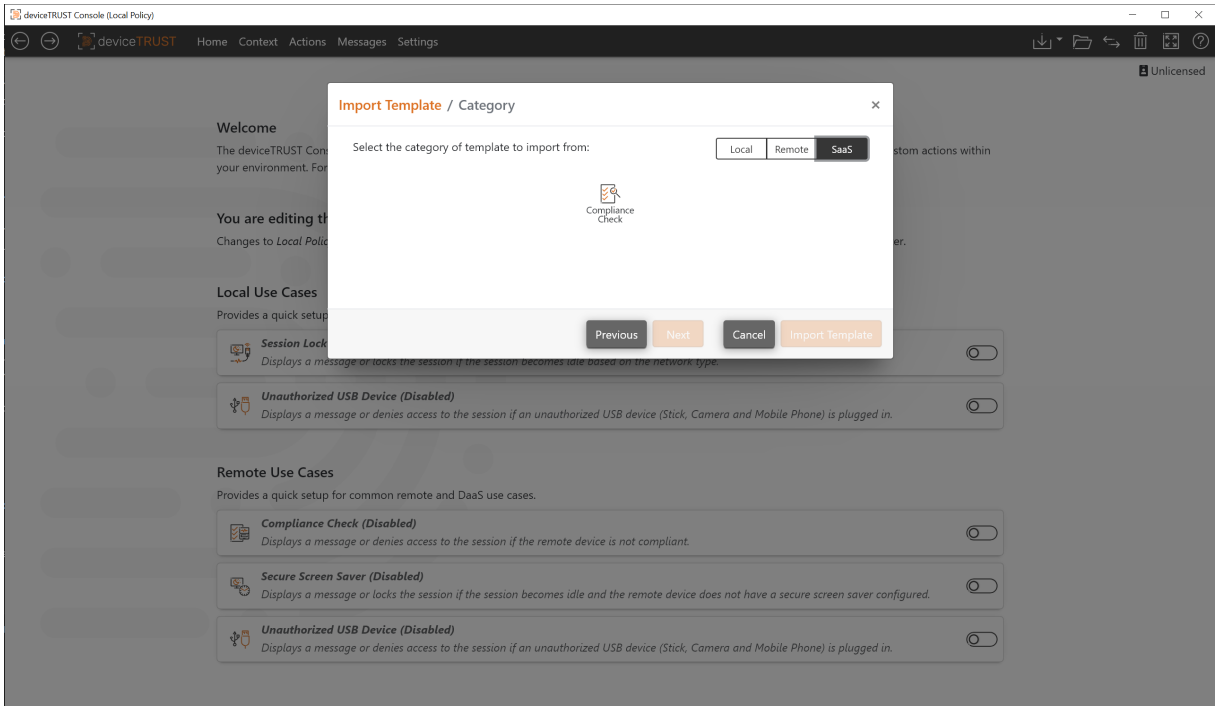


TABLE OF CONTENTS

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

Reference

TABLE OF CONTENTS

Property Reference

Table of contents

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

Agent Reference

TABLE OF CONTENTS

Client Extension Reference

TABLE OF CONTENTS

Console Reference

TABLE OF CONTENTS

Troubleshooting

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

Scenario: Remote

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

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

Scenario: Local

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

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

General

TABLE OF CONTENTS

Configuration

TABLE OF CONTENTS

Connectivity

Table of Contents

Diagnostics

TABLE OF CONTENTS

Installation

TABLE OF CONTENTS

Licensing

TABLE OF CONTENTS

Support

TABLE OF CONTENTS

Compatibility

TABLE OF CONTENTS

Properties

TABLE OF CONTENTS

Reporting

TABLE OF CONTENTS

Features

TABLE OF CONTENTS

Releases

TABLE OF CONTENTS

deviceTRUST Client Extension for macOS 2503 CR

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

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

Supported platforms

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

Compatibility with previous releases

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

Custom Properties and Custom Process Task

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

deviceTRUST® Client Extension for eLux 2503 CR

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

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

Supported platforms

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

Compatibility with previous releases

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

Custom Properties and Custom Process Task

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

deviceTRUST Client Extension for Ubuntu 2503 CR

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

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

Supported platforms

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

Compatibility with previous releases

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

Custom Properties and Custom Process Task

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

deviceTRUST 2503 CR

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

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

Supported platforms

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

Licensing

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

Citrix Virtual Channel Allow List

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

Custom Properties and Custom Process Task

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

Compatibility with previous clients

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

Compatibility

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

If upgrading from a previous release, be sure to check out the deviceTRUST 23.1.410 compatibility notes.

The deviceTRUST Agents can read policies created by previous releases of the deviceTRUST Console. However, they cannot read policies created by a newer console. Therefore, you must ensure that the deviceTRUST Agent 2503 CR is deployed before applying policy that has been written by the deviceTRUST Console 2503 CR.

Releases

August 19, 2025

TABLE OF CONTENTS