Device Posture

Contents

Device Posture overview

February 4, 2026

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

Prerequisites

- Licensing requirements: The Device Posture service is available as part of the Universal Hybrid Multi Cloud License (UHMC) and Platform License (CPL). For more information, see https://www.citrix.com/buy/licensing/product.html.
- Supported platforms:
  - Windows (10 and 11)
  - macOS 13 Ventura
  - macOS 12 Monterey
  - iOS
  - Linux

> **Note:**
>
> - A device running on a non-supported platform is marked as non-compliant by default. You can change the classification from **Non-compliant** to **Denied login** from the **Settings** tab on the Device Posture page. For the definitions of "compliant"and "non-compliant,"see Definitions.
> - A device that is running on a supported platform but does not match any pre-defined device posture policy is marked as non-compliant, by default. You can change the classification from **Non-compliant** to **Denied login** from the **Settings** tab on the Device Posture page.
> - For Device Posture service support on iOS, the EPA client is built in as part of the Citrix Workspace app for iOS. For details on the versions, see Citrix Workspace app for iOS.
> - For Linux support, reach out to Citrix Support to request enablement of Device Posture capabilities.

- Citrix Device Posture client (EPA client): A lightweight application that must be installed on the endpoint device to run device posture scans. This application does not require local admin rights to download and install on an endpoint.

  > **Note:**
  >
  > If you're using a device certificate check, then you must install the EPA client with administrative rights.

- Supported browsers: Chrome, Edge, and Firefox.
- Firewall configuration: To use the Device Posture service, ensure that the firewall or the proxy are configured to allow the following domains:
  - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
  - `https://productioniconstorage.blob.core.windows.net`
  - *.netscalergateway.net
  - *.nssvc.net
  - *.cloud.com
  - *.pendo.io
  - *.citrix.com
  - *.citrixworkspacesapi.net

Definitions

The terms "compliant"and "non-compliant"in reference to the Device Posture service are defined as follows:

- **Compliant devices** –A device that meets the pre-configured policy requirements and is allowed to log into the company's network with full or unrestricted access to Citrix Secure Private Access resources or Citrix DaaS resources.
- **Non-Compliant devices** - A device that meets the pre-configured policy requirements and is allowed to log in into the company's network with partial or restricted access to Citrix Secure Private Access resources or Citrix DaaS resources.

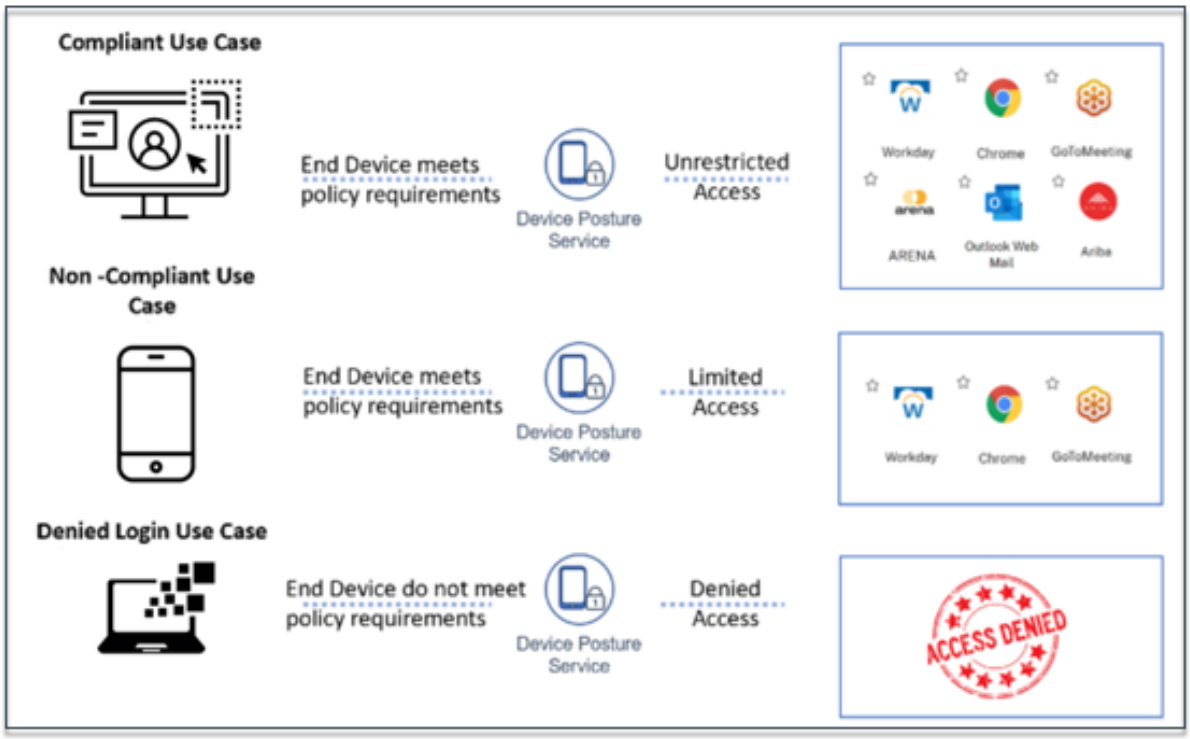
How it works

The admins can create device posture policies to check the posture of endpoint devices and determine whether an endpoint device is allowed or denied login. The devices, which are allowed to log in are further classified as compliant or non-compliant. Users can log in from a browser or the Citrix Workspace™ app.

The high-level conditions used to classify a device as compliant, non-compliant, and denied login are:

- **Compliant devices** –A device that meets the pre-configured policy requirements and is allowed to log in into the company's network with full or unrestricted access to Citrix Secure Private Access™ resources or Citrix DaaS resources.
- **Non-Compliant devices** - A device that meets the pre-configured policy requirements and is allowed to log in into the company's network with partial or restricted access to Citrix Secure Private Access resources or Citrix DaaS resources based on your DaaS and Secure Private Access configuration for Device Posture.
  - DaaS: Administrators can specify the delivery groups to restrict access for non-compliant devices. For details on how to configure restricted access to delivery groups, see Citrix DaaS configuration with Device Posture.
  - Secure Private Access: Administrators can choose specific applications to restrict access for these devices. For details on how to restrict access to specific applications, see Citrix Secure Private Access configuration with Device Posture.
- **Denied login:** - A device that fails to meet the policy requirements is denied login.

The classification of devices as **compliant**, **non-compliant**, and **denied login** is passed onto the Citrix DaaS and Citrix Secure Private Access service that in turn uses the device classification to provide smart access capabilities.



> **Note:**
>
> - The device posture policies must be configured specifically for each platform. For example, for macOS, an admin can allow access for the devices that have a specific OS version. Similarly, for Windows, the admin can configure policies to include a specific authorization file, registry settings, and so on.
> - Device posture scans are done only during pre-authentication/before logging in.
> - For definitions of "compliant"and "non-compliant,"see Definitions.

Scans supported by the Device Posture service

The following scans are supported by the Citrix Device Posture service:

Windows	macOS	iOS	Linux
Citrix Workspace App Version OS Version	Citrix Workspace App Version OS Version	Citrix Workspace App Version OS Version	- OS Version
File (Exists, Last Modified Time, MD5)	File (Exists, Last Modified Time, MD5)	-	File (Exists, Last Modified Time, MD5)
Geo Location	Geo Location	-	-
Network Location	Network Location	-	-
MAC Address	MAC Address	-	-
Process (Exists, MD5, SHA1)	Process (Exists, MD5, SHA1)	-	Process (Exists, MD5, SHA1)
Microsoft Endpoint Manager	Microsoft Endpoint Manager	-	-
CrowdStrike	CrowdStrike	-	-
Device Certificate	Device Certificate	-	-
Web Browser	Web Browser	-	-
Antivirus	Antivirus	-	-
Non-Numeric Registry (32 Bit)	-	-	-
Non-Numeric Registry (64 Bit)	-	-	-
Numeric Registry (32 Bit)	-	-	-

Windows	macOS	iOS	Linux
Numeric Registry (64 Bit)	-	-	-
Windows Update Installation Type	-	-	-
Windows Update Last Update Check	-	-	-
External Device Connected	-	-	-
Network Settings	-	-	-
-	-	-	Mount Point

> **Note:**
>
> - Starting from EPA library version 24.9.1.1, the **Windows Update Last Update Check** scan also includes updates installed through BigFix, Microsoft Intune, and other third-party tools, in addition to those installed through the Windows Auto Upgrade service.
> - For iOS support on Device Posture service, the EPA client is built in as part of the Citrix Workspace app for iOS. For details on the versions, see Citrix Workspace app for iOS.

Windows Update Last Update Check

The **Windows Update Last Update Check** enhancement is applicable from EPA library version 24.9.1.1. Starting from version 24.9.1.1, the scan includes updates installed through BigFix, Intune, and other third-party tools, in addition to those installed through the Windows Auto Upgrade service.

Starting from the EPA library version 24.11.1.1, the **Windows Update Last Update Check** scan lists the Windows updates in the following categories:

- **Generic updates:** This category includes updates installed using Windows update, Microsoft update, or automatic updates feature.
- **Security updates:** This category includes the patches for security-related vulnerabilities. The security updates are published on the second Tuesday of each month.
- **Critical updates:** This category includes the patches for critical and non-security-related bugs. The critical updates are published as and when required.
- **Definition updates:** This category includes updates that contain additions to a product's definition database. When definition updates are published only the differences between the latest update and the update that is currently installed are downloaded and applied to the device.

- **Update rollups:** This category includes tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. The update rollups are published on the second Tuesday of each month.

> **Note:**
>
> - While configuring the **Windows Update Last Update Check** scan, ensure that updates are scheduled within the configured period for each category. If updates are not installed within this timeframe, the scan fails.
> - The **Windows Update Last Update Check** scan is not applicable for manually installed updates where the update patch is downloaded and installed by the user.

Third-party integration with the Device Posture service

In addition to the native scans offered by the Device Posture service, the service can also be integrated with the following third-party solutions on Windows and macOS.

- Microsoft Intune. For details, see Microsoft Intune integration with Device Posture.
- CrowdStrike. For details, see CrowdStrike integration with Device Posture.

Known limitations

- The time taken for the device posture functionality to be enabled or disabled after the **Device Posture** toggle button is turned On or Off can take a few minutes to an hour.
- Any changes in the device posture configuration do not take effect immediately. It might take around 10 minutes for the changes to take effect.
- If you have enabled the Service Continuity option in Citrix Workspace and if the Device Posture service is down, users might be unable to sign in to Workspace. This is because Citrix Workspace enumerates apps and desktops based on local cache on the user device.
- If you have configured a long-lived token and password on Citrix Workspace, the Device Posture scan does not work for this configuration. The devices are scanned only when the users log in to Citrix Workspace.
- Each platform can have a maximum of 10 policies and each policy can have a maximum of 10 rules.
- Role-based access is not supported with the Device Posture service.
- The Device Posture service is not supported in Citrix Cloud™ Japan.

Quality of service

- Performance: Under ideal conditions, the Device Posture service adds an additional 2 seconds of delay during login. This delay might increase depending on additional configurations such as third-party integrations like Microsoft Intune.
- Resiliency: Device Posture service is highly resilient with multiple POPs to ensure that there's no downtime.

Integration with Chrome Enterprise Premium

By integrating the Device Posture service with Google Chrome Enterprise Premium, you can extend device compliance checks to Chrome browser-based access scenarios. This integration enables organizations to enforce device posture policies when users access applications through Chrome Enterprise Premium managed browsers.

To enable integration between the Device Posture service and Chrome Enterprise Premium, you must configure OpenID Connect (OIDC) authentication as the primary authentication method.

For more details, see the following topics:

- Integration with Google Chrome Enterprise
- Open ID Connect (OIDC) with Citrix Workspace

What's new

February 4, 2026

21 January 2026

- **Device Posture service and deviceTRUST - Better together**

  Securing access to enterprise applications and data now requires more than static policies. They require real-time, context-aware controls that continuously adapt throughout the user journey. Citrix's Device Posture Service (DPS) and deviceTRUST (dT) deliver this capability by collaborating to deliver comprehensive contextual access coverage across every phase; pre-authentication, enumeration, and in-session. For details, see Device Posture service and deviceTRUST - Better together.

26 September 2025

- **Scan to evaluate multiple registry key values**

  The Device Posture service now includes a new scan for Windows devices. Admins can configure the **Multi-Value Non Numeric Registry** scan to evaluate multiple registry key values and then determine the device's managed status. For details on configuring a device posture policy with multi-value non-numeric registry scan, see Configure Device Posture policies.

- **Troubleshoot Device Posture service transactions using Citrix Monitor**

  Administrators can now diagnose and troubleshoot Device Posture service transactions effectively through comprehensive monitoring capabilities integrated into the Citrix Monitor dashboard. This enhancement provides detailed insights into Device Posture policy evaluation, compliance checks, and error diagnostics. For details, see Diagnose Device Posture service transactions.

- **Automatic skipping of posture checks**

  The Device Posture service now supports automatic skipping of posture checks if the EPA client is not detected on the end-user devices. When configured for auto skip, the system performs real-time detection to determine if the EPA client is present on the end-user's device. If the client is not detected, the posture check process is automatically bypassed without requiring any user interaction thus streamlining the login process.

  Admins can also configure the settings to enable end users to manually click **Skip Posture Check** on every login attempt if the EPA client is not installed on their machines or the EPA client version is outdated. For details, see Skip device posture checks.

- **Integration of multiple Microsoft Intune accounts with Device Posture**

  The Device Posture service now supports integration with multiple Microsoft Intune accounts. This allows organizations with multiple Intune tenants (often a result of mergers, acquisitions, or departmental segmentation) to seamlessly manage device posture across all their environments. For details, see Microsoft Intune integration with Device Posture.

- **Device Posture support for Secure Private Access hybrid deployments**

  Device Posture is supported for Secure Private Access hybrid deployments, but is available only upon request. Contact Citrix Support or ATS to have the feature enabled. Device Posture service is not yet supported on gateway for Citrix Virtual Apps and Desktops.

  - For details on enabling Device Posture checks on NetScaler Gateway, see Device Posture checks on NetScaler Gateway.
  - In addition to enabling the Device Posture feature on NetScaler Gateway, you must add the URL of NetScaler Gateway accessing StoreFront™ in the Device Posture Settings page. For details, see Enable Device Posture for Secure Private Access hybrid solutions.

09 July 2025

- **Multi-workspace URLs support**

  Administrators can now apply distinct device posture policies to different Citrix Workspace™ access URLs, offering granular control and simplified security management. Previously, the Device Posture service was enabled globally across all workspace URLs, preventing administrators from applying specific requirements on a per-URL basis.

  With multi-workspace URLs support, you can now do the following:

  - Apply distinct device posture checks for specific workspace URLs.
  - Enforce varying levels of device compliance based on the workspace URL that users access.
  - Create and test the device posture checks on test workspace URLs before deploying to production URLs.

  For details, see Multi-workspace URLs support.

  > **Note:**
  >
  > This feature is in preview.

21 Feb 2025

- **Device compliance with event-driven posture checks**

  Starting with EPA Library version 24.11.1.1, Device Posture introduces enhanced checks to assess the compliance of your devices.

  The following two scans are added to provide more control over device compliance:

  - **External Device Connected:** This scan detects if an external USB storage device is connected to the endpoint.
  - **Network Settings:** This scan determines if the device is connected to a protected Wi-Fi network.

  When any of the following events occur, Device Posture re-evaluates the device's compliance status:

  - The **External Device Connected** scan is configured, and an external USB storage device is inserted or removed.
  - The **Network Settings** scan is configured, and a switch between an open network and a protected network is detected.
  - The **Windows Defender Firewall** scan is configured, and it's enabled or disabled.

Access to the resources is updated in accordance with the new compliance status. This ensures that access to resources is granted or revoked based on the device's real-time compliance status.

For details, see Device compliance with event-driven posture checks.

> **Note:**
>
> This feature is supported only on the Windows platform.

- **TCP/UDP active sessions terminated after a downgrade**

  For TCP/UDP applications launched from the Citrix Secure Access client, if a device posture scan results in a downgrade (for example from **Compliant** to **Non-compliant** or **Denied access**), users receive a notification, and after 5 minutes, the active sessions are terminated. For details, see Periodic scanning of devices.

  > **Note:**
  >
  > This feature is supported only on the Windows platform and is available from the End Point Analysis (EPA) client version 24.8.1.19 and library version 24.9.1.1.

- **Enhancements to the Windows Update Last Update scan**

  Starting from EPA library version 24.9.1.1, the **Windows Update Last Update** scan also includes updates installed through BigFix, Microsoft Intune, and other third-party tools, in addition to those installed through the Windows Auto Upgrade service.

04 Dec 2024

- **Jamf Pro integration with Device Posture**

  In addition to the native scans offered by the Device Posture service, the Device Posture service is also integrated with Jamf Pro. For details, see Jamf Pro integration with Device Posture.

29 May 2024

- **Availability of Device Posture service in test mode**

  The Device Posture service is also available in test mode wherein admins can test the Device Posture service before enabling it on their production environment. This enables the admins to analyze the impact of the device posture scans on the end user devices and then plan their course of action accordingly before enabling it on production. For details, see Device Posture service in test mode.

- **Periodic scanning of devices

  You can now enable periodic scanning of Windows devices for the configured checks every 30 minutes. For details, see Periodic scanning of devices.

14 May 2024

- **Skip device posture checks**

  Admins can allow the end users to skip the device posture checks on their devices. For details, see Skip device posture checks.

- **Device posture dashboard**

  The Device Posture service portal now has a dashboard for monitoring and troubleshooting logs. Admins can now use this dashboard for monitoring and troubleshooting purposes. For details, see Device posture logs.

- **General availability of browser and antivirus checks**

  The browser and antivirus checks are now generally available. For details, see Scans supported by device posture.

- **General availability of custom messages**

  The option to add customized messages when access is denied is now generally available. For details, see Customized messages for access denied scenarios.

26 March 2024

- **Custom workspace URLs support**

  Custom workspace URLs are now supported with the Device Posture service. You can use a URL that you own in addition to your cloud.com URL to access workspace. Ensure that you allow access to citrix.com from your network. For details on custom domains, see Configure a custom domain.

12 February 2024

- **Support for browser and antivirus checks - Preview**

  Device Posture service now supports browser and antivirus checks. For details, see Scans supported by device posture.

23 January 2024

- **General availability of device certificate check with Device Posture service**

  Device certificate check with the Device Posture service is now generally available. For details, see Device certificate check.

- **Device Posture service preview features**

  Device Posture service now supports the following checks:

  - Device Posture service is now supported on the IGEL platforms.
  - Device Posture service now supports geolocation and network location checks.

  For details, see Device Posture.

11 September 2023

- **General availability of Device Posture Integration with Microsoft Intune**

  Device Posture Integration with Microsoft Intune is now generally available. For details, see Microsoft Intune integration with Device Posture.

30 August 2023

- **Manage Citrix Endpoint Analysis Client for Device Posture service**

  The EPA client can be used together with NetScaler and Device Posture. Some configuration changes are required to manage EPA client when used with NetScaler and Device Posture. For details, see Manage Citrix Endpoint Analysis Client for Device Posture service.

28 August 2023

- **Device Posture service support on iOS platforms - Preview**

  Device Posture service is now supported on iOS platforms. For details, see Device Posture.

22 August 2023

- **Device Certificate check with Citrix Device Posture service - Preview**

  Citrix Device Posture service can now enable contextual access (Smart Access) to Citrix DaaS and Secure Private Access resources by checking the end device's certificate against a corporate certificate authority to determine if the end device can be trusted. For details, see Device certificate check.

17 August 2023

- **Device Posture events on Citrix DaaS™ Monitor**

  Device Posture service events and monitoring logs are now searchable on DaaS Monitor. For details, see Device posture events on Citrix DaaS Monitor.

23 January 2023

- **Device posture service**

  Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps). For details, see Device Posture.

  [AAUTH-90]

- **Microsoft Endpoint Manager integration with Device Posture**

  In addition to the native scans offered by the Device Posture service, the Device Posture service can also be integrated with other third-party solutions. Device Posture is integrated with Microsoft Endpoint Manager (MEM) on Windows and macOS. For details, see Microsoft Endpoint Manager integration with Device Posture.

  [ACS-1399]

Configure Device Posture policies

February 16, 2026

Device posture is a combination of policies and rules that a device must meet to gain access to the resources. Each policy is attached with one of the actions namely compliant, non-compliant, and denied login. In addition, each policy is associated with a priority and the policy evaluation stops if a policy evaluates to true and the associated action is taken.

1. Sign in to Citrix Cloud™, and then select **Identity and Access Management** from the hamburger menu.
2. Click the **Device Posture,** tab and then click **Manage**.

   > **Note:**
   >
   > - Secure Private Access service customers can directly click **Device Posture** on the left

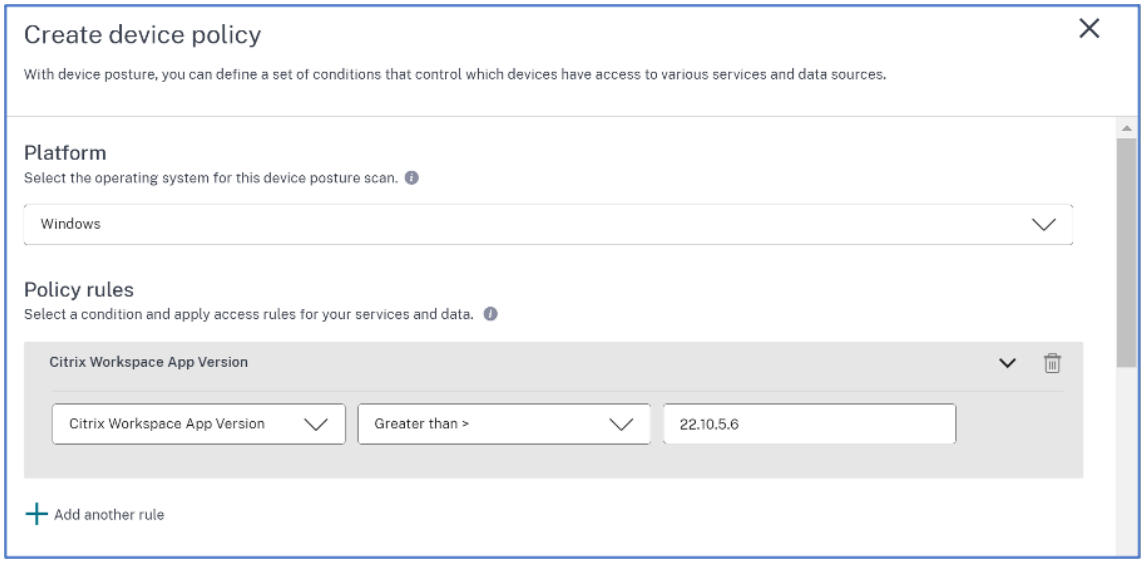
navigation in the admin user interface.
- For the first-time users, the Device Posture landing page prompts you to create a device posture policy. Device posture policy must individually be configured for each platform. Once you create a device posture policy, it gets listed under the appropriate platforms.
- A policy comes into effect only after device posture is enabled. To enable device posture, slide the **Device posture is disabled** toggle on the right hand top corner to **ON**.

3. Click **Create device policy**.
4. In **Platform**, select the platform for which you want to apply a policy. You can change the platform from Windows to macOS or conversely irrespective of the tab that you selected on the Device Posture home page.
5. In **Policy rules**, select the check that you want to perform as part of device posture and select the conditions that must be matched.

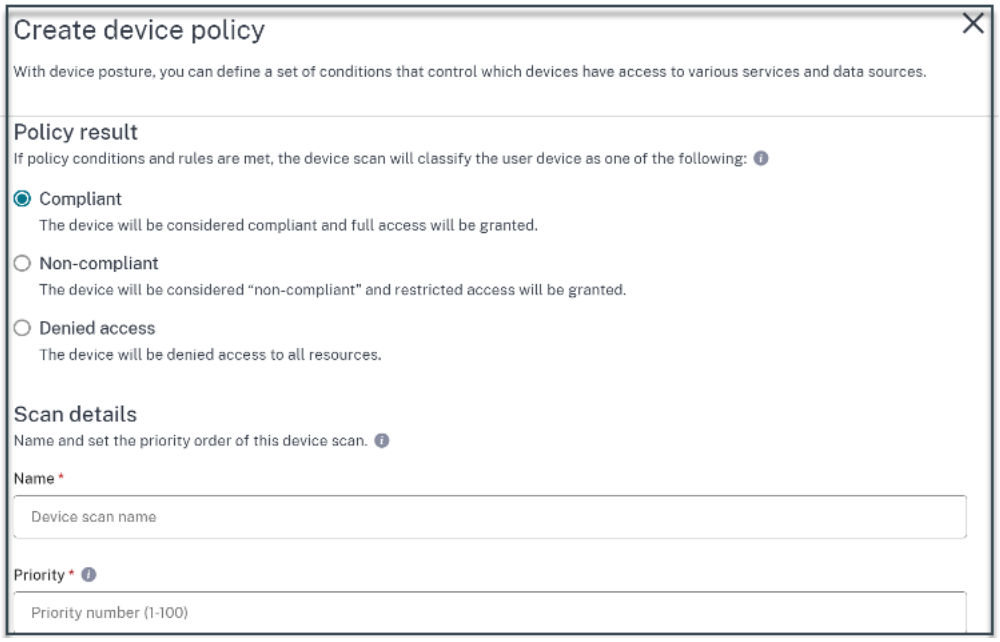
   Note:

   - The **Multi-Value Non Numeric Registry** scan allows administrators to determine if a device is managed or unmanaged. This is achieved by evaluating several registry key values.
   - Note the following points regarding **Device Certificate** check:
     - Ensure that the issuer certificate exists on the device. Else, you can import a device certificate while creating the device posture policy or upload the certificate from **Settings** on the Device Posture home page. For details, Device certificate check.
       - In environments where multiple device certificates share a common issuer name, the Device Posture service might evaluate the wrong certificate. To ensure the service identifies the exact certificate for a specific policy, you must explicitly enable the **Check Thumbprint** option. For details, see Configure device certificate check scans.
       - The EPA client on the end device must be installed with administrative rights.
       - The device certificate check with the Device Posture service does not support the **Certificate Revocation** check.
   - When creating a policy rule for network location check, you can add a network location directly from the Device Posture service console. However, to modify the network location, you must use the Network Location configuration on Citrix Cloud.

6. Click **Add another rule** to create multiple rules. An AND condition is applied on multiple rules.



7. In **Policy result** based on the conditions that you've configured, select the type under which the device scan must classify the user device.
    - Compliant
    - Non-compliant
    - Denied access
8. Enter a name for the policy.
9. In **Priority**, enter the order in which the policies must be evaluated.
    - You can enter a value between 1 through 100. It's recommended that you configure deny policies with higher priority, followed by non-compliant, and finally compliant.
    - The priority with the lower value has the highest preference.
    - Only the policies that are enabled are evaluated based on the priority.
10. Click **Create**.



> **Important:**
>
> You must turn the **Enable when created** toggle switch to **ON** for the device posture policies to take effect. Before you enable the policies, it's recommended that you ensure that the policies are correctly configured and you're performing these tasks in your test setup.

Configure contextual access (smart access) using device posture

After the device posture verification, the device is allowed to log in and classified as compliant or non-compliant. This information is available as tags to the Citrix DaaS service and Citrix Secure Private Access™ service and is used to provide contextual access based on device posture. Therefore, Citrix DaaS and Citrix Secure Private Access must be configured to enforce access control using device posture tags.

Citrix DaaS configuration with Device Posture

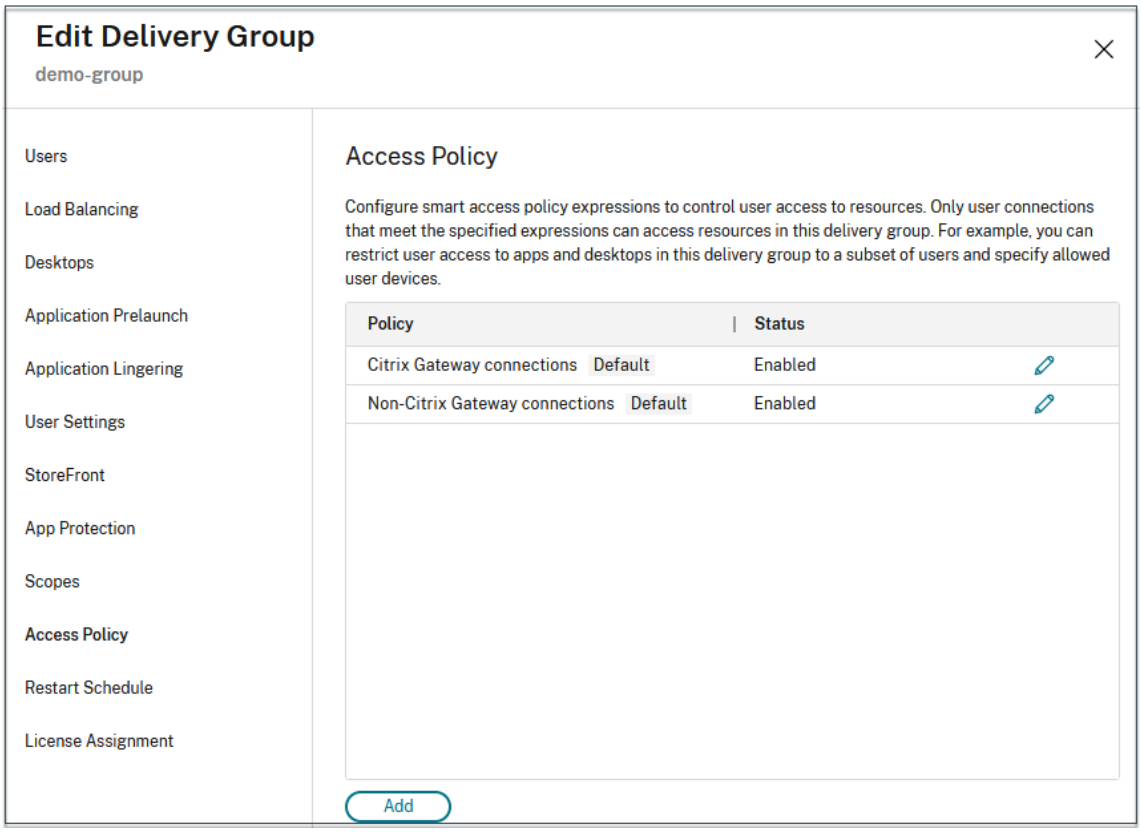
To restrict access to the DaaS resources, you can specify the delivery groups on which access restrictions must be enforced and configure the access control restrictions using the Device Posture tags.

Prerequisites:

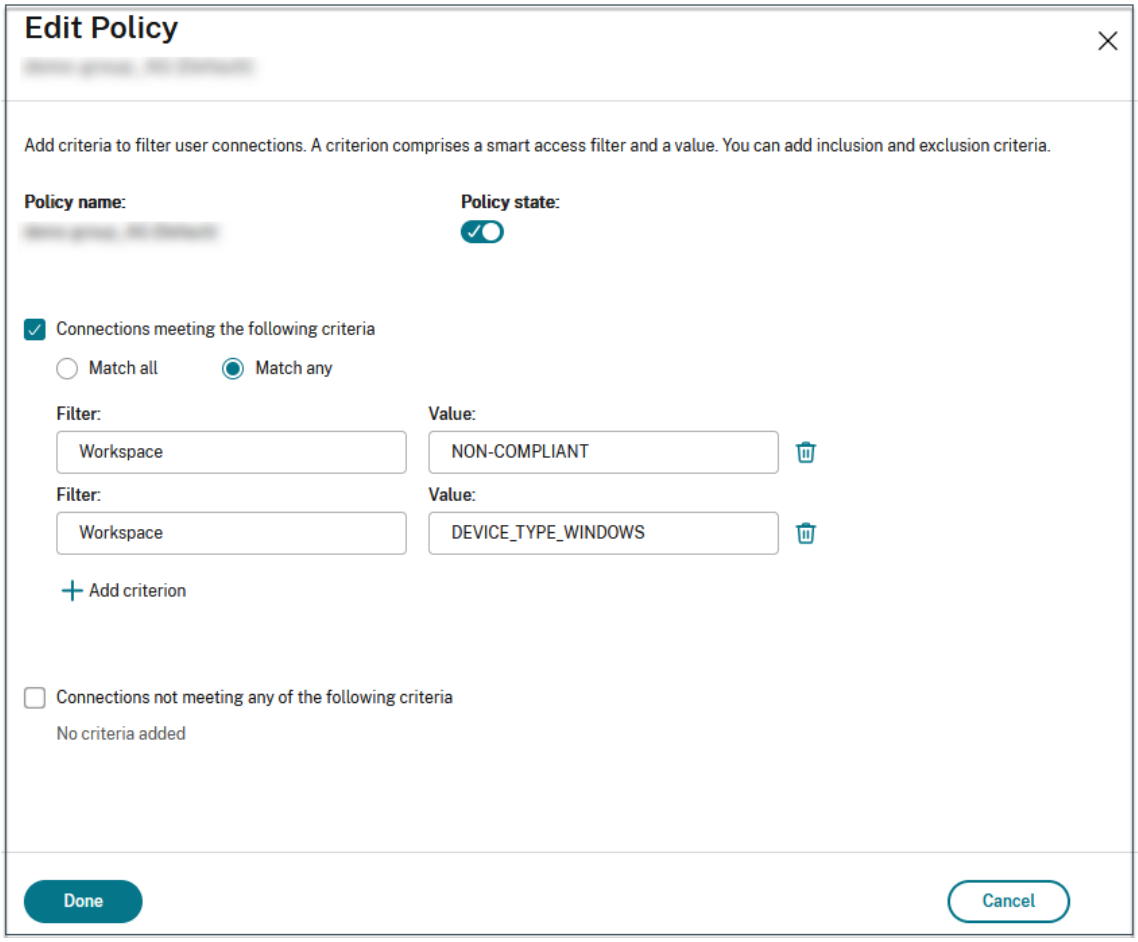
Ensure that the Adaptive Access feature is enabled (**Citrix Workspace > Access > Adaptive Access**). For details, see Enable the Adaptive Access feature.

1. Sign into Citrix Cloud.
2. On the **DaaS** tile, click **Manage**.

3. Go to the **Delivery Group** section from the left-hand menu.
4. Select the delivery group for which you want to configure access control based on device posture and click **Edit**.
5. In the **Edit Delivery Group** page, click **Access Policy**.
6. Click the edit icon on the **Citrix Gateway connections** row to edit the gateway connections policy.



   a) On the Edit policy page, select **Connections meeting the following criteria.**
   b) Select **Match any**, and then click **Add criterion**.
   c) Add criteria for all location tags you configured in Configure network locations: Type **Workspace** for **Filter** and **COMPLIANT** or **NON-COMPLIANT** for **Value**.



Note:

The syntax for the device classification tags must be entered exactly as captured earlier, that is all in uppercase (**COMPLIANT** and **NON-COMPLIANT**). Else the device posture policies do not work as intended.

In addition to the device classification tags, the Device Posture service also returns the operating system tag and the access policy tag associated with the device. The operating system tags and the access policy tags must be entered in uppercase only.

- DEVICE_TYPE_WINDOWS
- DEVICE_TYPE_MAC
- Exact policy name (uppercase)

Citrix Secure Private Access configuration with Device Posture

To restrict access to the Secure Private Access resources, you can select the applications on which access restrictions must be enforced and configure the access control restrictions using the Device Posture tags.

1. Sign into Citrix Cloud.
2. On the Secure Private Access tile, click **Manage**.
3. Click **Access Policies** on the left navigation and then click **Create policy**.
4. Enter the policy name and description of the policy.
5. In **Applications**, select the app or set of apps on which this policy must be enforced.
6. Click **Create Rule** to create rules for the policy.
7. Enter the rule name and a brief description of the rule, and then click **Next**.
8. Select the users' conditions. The **Users** condition is a mandatory condition to be met to grant access to the applications for the users.
9. Click **+** to add device posture condition.
10. Select **Device posture check** and the logical expression from the drop-down menu.
11. Enter one of the following values in the custom tags:

    - **Compliant** - For compliant devices
    - **Non-Compliant** - For non-compliant devices

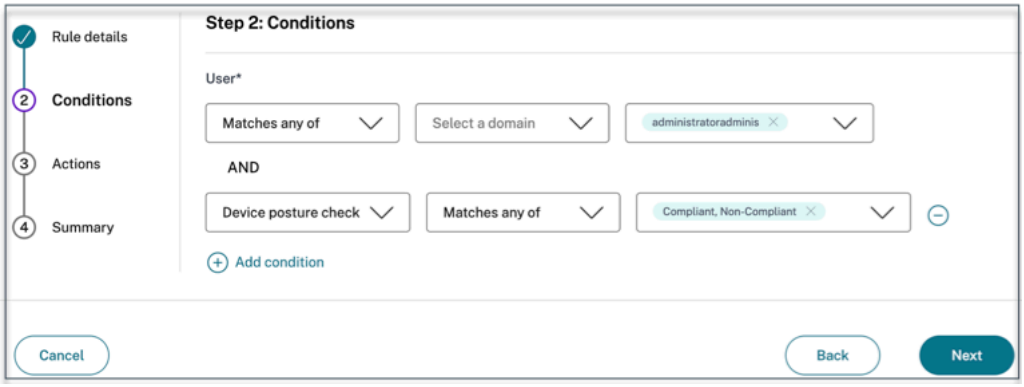
    > **Note:**
    >
    > The tags must be entered exactly as captured earlier, using initial caps (**Compliant** and **Non-Compliant**). Otherwise, the device posture policies do not function as intended.

12. Click **Next**.
13. Select the actions that must be applied based on the condition evaluation, and then click **Next**.

    The Summary page displays the policy details.
14. You can verify the details and click **Finish**.

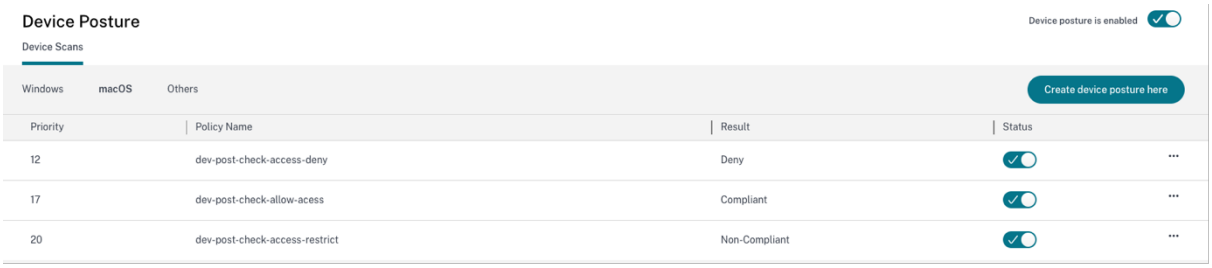
    For more details on creating access policies, see Configure an access policy with multiple rules.

> **Note:**
>
> Any Secure Private Access application, which isn't tagged as compliant or non-compliant in the access policy is treated as the default application and is accessible on all the endpoints regardless of device posture.



Edit a device posture policy

The configured device posture policies are listed under the specific platform in the **Device Scans** page. You can search for the policy you want to edit from this page. You can also enable, disable, or delete a policy from this page.



Configure Device Posture global settings

February 16, 2026

The following are some of the global Device Posture settings that you can configure as required.

- Device compliance with event-driven posture checks
- Periodic scanning of devices
- Customized messages for access denied scenarios
- Skip device posture checks
- Custom workspace URLs support
- Session Recording configuration with Device Posture
- Device certificate check

Device compliance with event-driven posture checks

Starting with EPA Library version 24.11.1.1, Device Posture introduces enhanced checks to assess the compliance of your devices.

The following two scans are added to provide more control over device compliance:

- **External Device Connected:** This scan detects if an external USB storage device is connected to the endpoint.
- **Network Settings:** This scan determines if the device is connected to a protected Wi-Fi network.

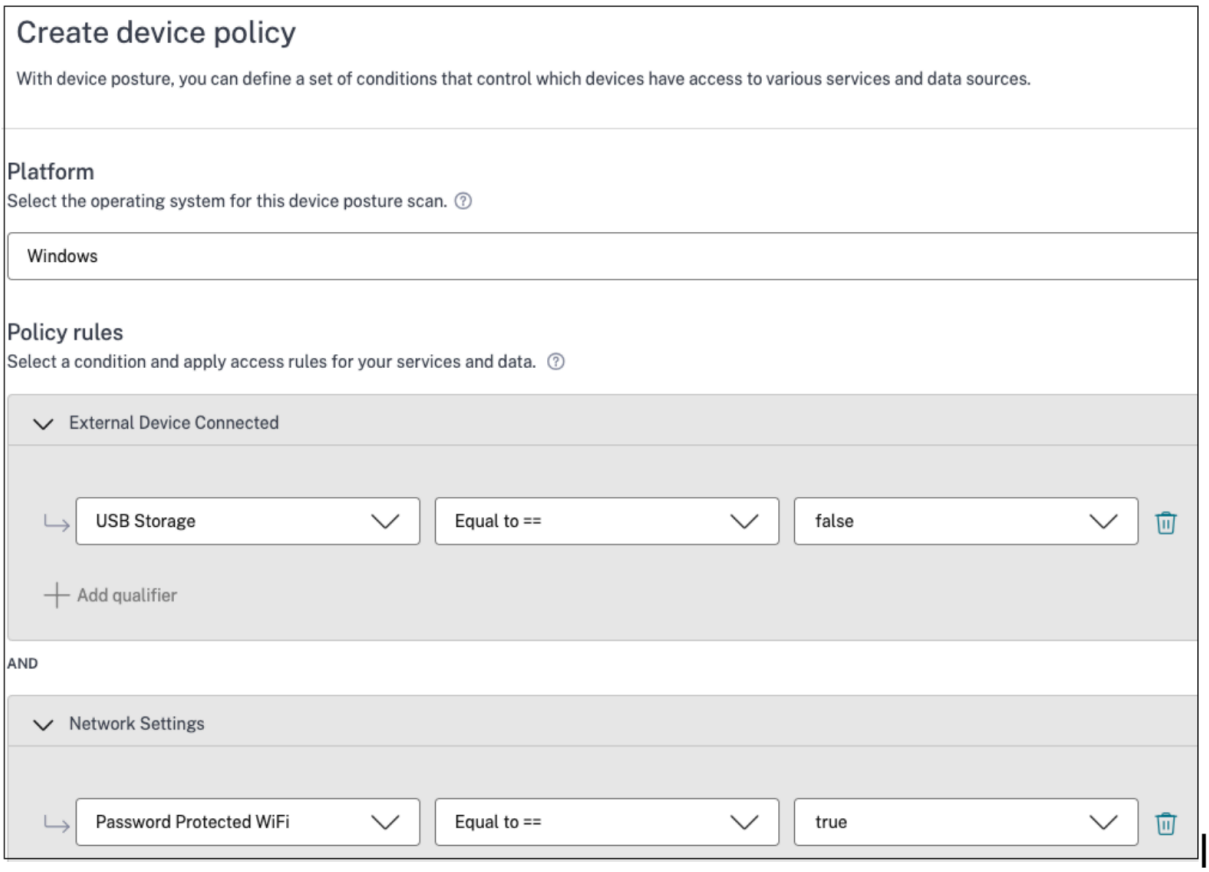
When any of the following events occur, Device Posture re-evaluates the device's compliance status:

- The **External Device Connected** scan is configured, and an external USB storage device is inserted or removed.
- The **Network Settings** scan is configured, and a switch between an open network and a protected network is detected.
- The **Windows Defender Firewall** scan is configured, and it's enabled or disabled.

Access to the resources is updated in accordance with the new compliance status. This ensures that access to resources is granted or revoked based on the device's real-time compliance status.

> **Note:**
>
> - Event-driven posture checks are currently supported only on the Citrix Secure Access client for Windows version 24.8.1.19 and later.
> - While both user and administrator installations can utilize the posture scans, real-time re-evaluation of device compliance based on events requires administrator privileges.

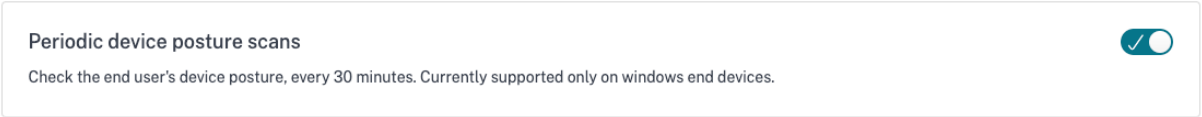
The following figure displays the **External Device Connected** and **Network Settings** scans configured in the Device Posture admin console.



Periodic scanning of devices

You can enable periodic scanning of Windows devices for the configured checks every 30 minutes. The EPA client on the end device must be installed with administrative rights to enable periodic scanning of devices. To enable periodic scanning, do the following:

1. Navigate to **Device Posture > Device Scans** and click **Settings**.
2. In **Periodic device posture scans** section, slide the toggle switch to ON to enable periodic scanning of devices.



- For HTTP/HTTPS applications, if a device posture scan result changes from **Compliant** to **Non-compliant** or **Denied access**, access to the resources is updated in accordance with the new compliance status.
- For TCP/UDP applications launched from the Citrix Secure Access client, if a device posture scan results in a downgrade (for example from **Compliant** to **Non-compliant** or **Denied access**),

users receive a notification, and after 5 minutes, the active sessions are terminated.

Customized messages for access denied scenarios

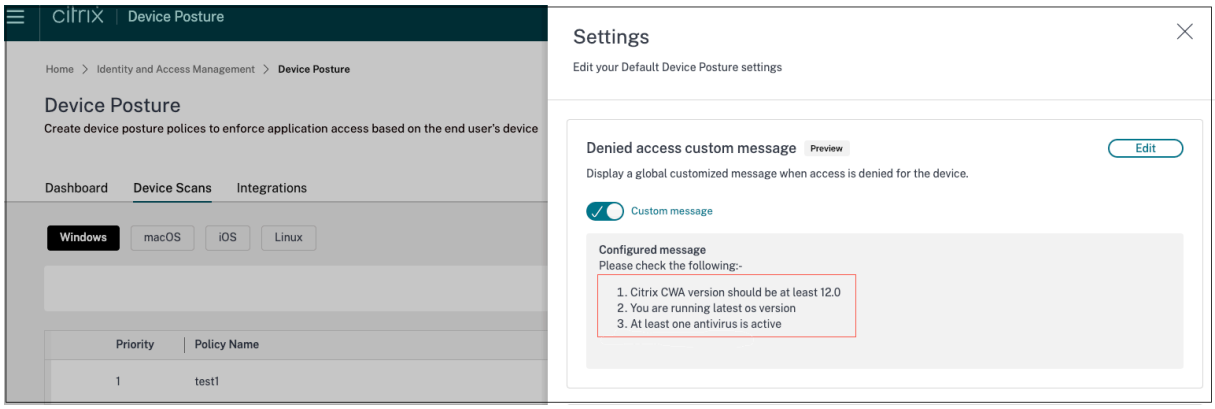
Admins can customize the message that is displayed on the end device when access is denied.

Perform the following steps to add customized messages:

1. Navigate to the **Device Posture > Device Scans** page.
2. Click **Settings**.
3. Click **Edit** and in the **Message** box, enter the message that must be displayed in access denied scenarios. You can enter a maximum of 256 characters.
4. Click **Enable custom message on save** to enforce the option of displaying the custom message. If you do not select this checkbox, the custom message is created but not displayed on the devices in access denied scenarios.

   Alternatively, you can enable the **Custom message** toggle switch on the **Settings** page to display the message on the devices.
5. Click **Save**.

The following image displays a sample message added by the admin.



The following image displays the custom message that appears on the end user device when access is denied.

The message that you have entered appears whenever access is denied for the end device.

Skip device posture checks

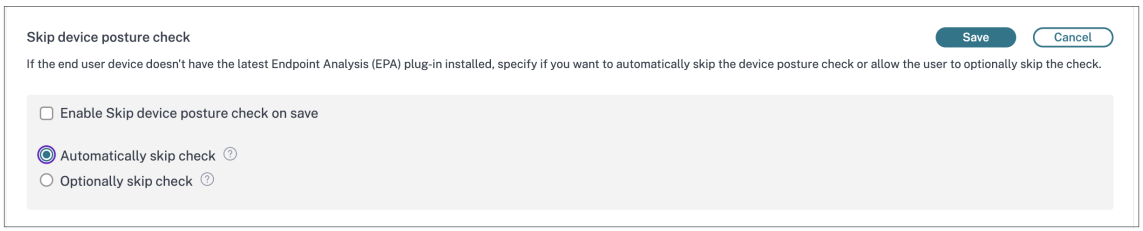
Admins can configure device posture checks to be skipped automatically or allow end users to skip them in the following scenarios:

- The EPA client is not installed on the device.
- The EPA client installed on the device is outdated.

When the skip check feature is enabled, the default policy result (non-compliant) is enforced and the device is classified as non-compliant. End users are provided with partial or restricted access to the Citrix Secure Private Access™ or Citrix DaaS resources.

Enable skipping of the device posture checks

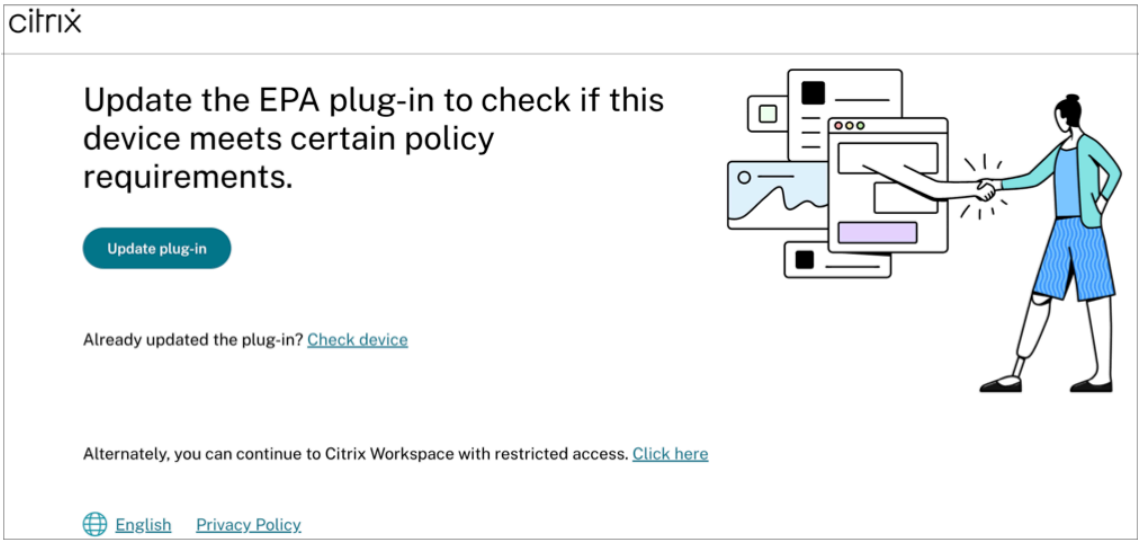
1. Navigate to **Device Posture > Device Scans**.
2. Click **Settings**.
3. In the **Skip device posture check** section, slide the toggle switch to ON to enable skipping of the device posture checks and then click **Edit**.



4. Select one of the following options:

   - **Automatically skip check** - The system automatically bypasses posture checks when the EPA client is missing or outdated, thus streamlining the login process for users accessing Citrix Workspace from devices without the EPA client.
   - **Optionally skip check** - When logging into Citrix Workspace from devices without the EPA client, the users are prompted to manually skip the posture checks by clicking **Skip Posture Check**.

   When the **Optionally skip check** option is enabled and the end user logs on to Citrix Workspace, the following message appears when the end user tries to download the client or upgrade the EPA version.



5. Click **Save**.

Custom workspace URLs support

Custom workspace URLs are supported with the Device Posture service. You can use a URL that you own in addition to your cloud.com URL to access workspace. Ensure that you allow access to citrix.com from your network. For details on custom domains, see Configure a custom domain.

Session Recording configuration with Device Posture

Session Recording allows organizations to record on-screen user activity in virtual sessions. You can specify tags when creating a custom session recording policy, event detection policy, or event response policy. For an example, see Create a custom recording policy.

Device certificate check

To configure device certificate checks with the Device Posture service, admins must import an issuer certificate from their device. Once a valid issuer certificate is present in the Device Posture service, admins can use device certificate checks as part of device posture policies.

> **Points to note:**
>
> - Device Posture service supports only PEM issuer certificate type.
> - For the device certificate check on Windows, the EPA client on the end device must be installed with administrative rights. For other checks, you do not require the local administrative rights. For details on the supported scans, see Scans supported by device posture.

- To install the EPA client with administrative rights on Windows, run the following command in the location where the EPA client plug-in is downloaded.

  ```
  msiexec /i epasetup.msi
  ```

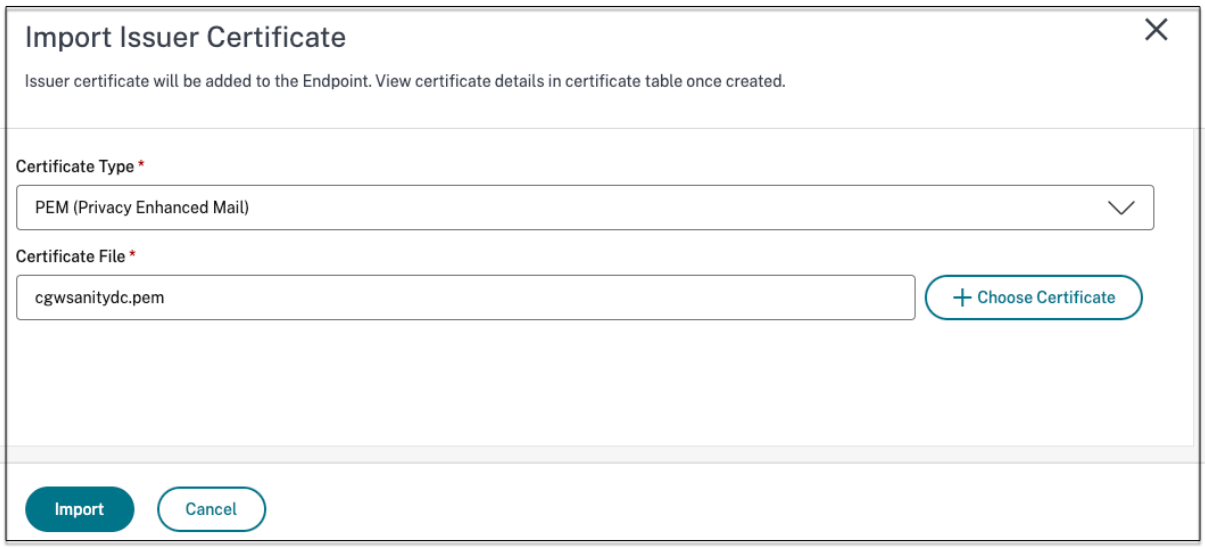
- The device certificate check with the Device Posture service does not support the certificate revocation check.
- If a device certificate is signed by an intermediate certificate, then you must upload the complete chain containing the root and the intermediate certificates in a single PEM file.

  ```
  Example: chain.pem

  -----BEGIN CERTIFICATE-----
  ******************************
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  ******************************
  -----END CERTIFICATE
  ```

Upload device certificate

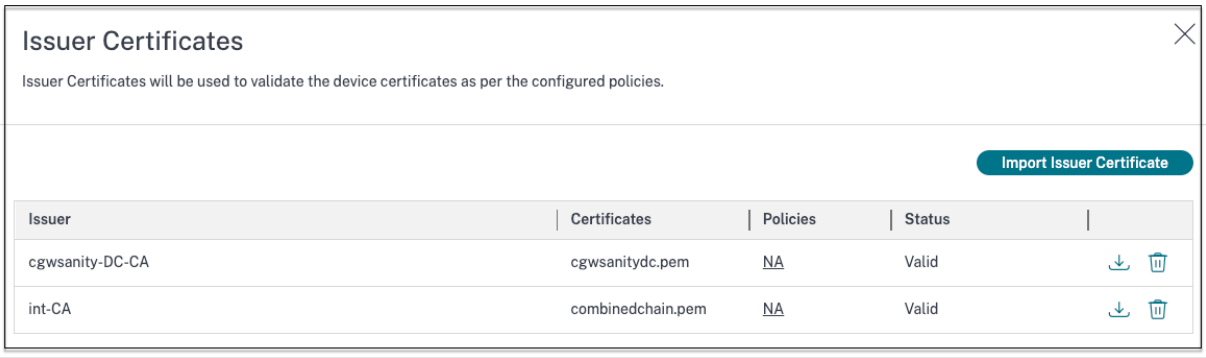
1. Click **Settings** on the Device Posture home page.
2. Click **Manage**, and then click **Import Issue Certificate**.
3. In **Certificate Type**, select the certificate type. Only the PEM type is supported.
4. In **Certificate File**, click **Choose Certificate** to select the issuer certificate.
5. Click **Open**, and then click **Import**.



The selected certificate is listed in **Settings > Issuer Certificates**. You can import multiple certificates.

View imported certificates

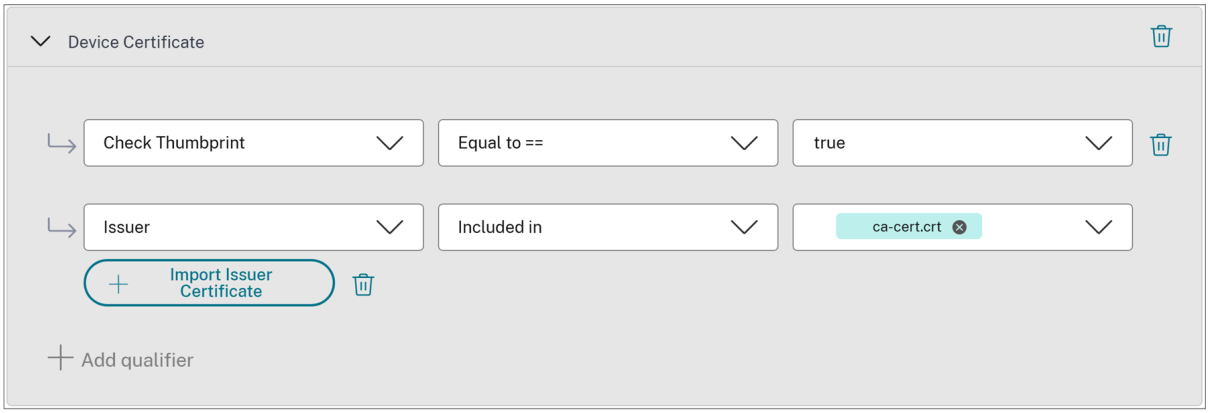
1. Click **Settings** on the Device Posture home page.
2. In **Issuer Certificates**, click **Manage**.
3. The Issuer Certificates page lists the imported issuer certificates.



Configure device certificate check scans

1. Configure the device posture policy. For details, see Configure Device Posture policies.
2. When adding a policy rule for the device certificate check, specify both the **Check Thumbprint** and **Issuer** conditions.

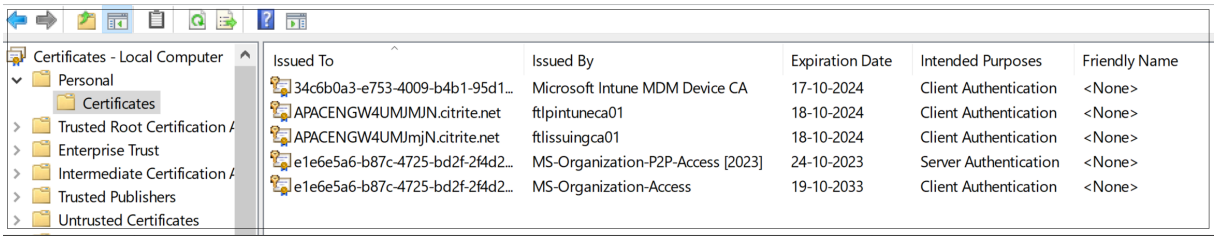
> **Important:**
>
> If multiple device certificates in your environment share the same issuer name, you must enable the **Check Thumbprint** option to prevent the service from matching the wrong certificate. Without this option enabled, the service matches certificates by issuer name only, which can cause policy conflicts when duplicate issuer names exist.



Install the device certificate on the end device

Windows:

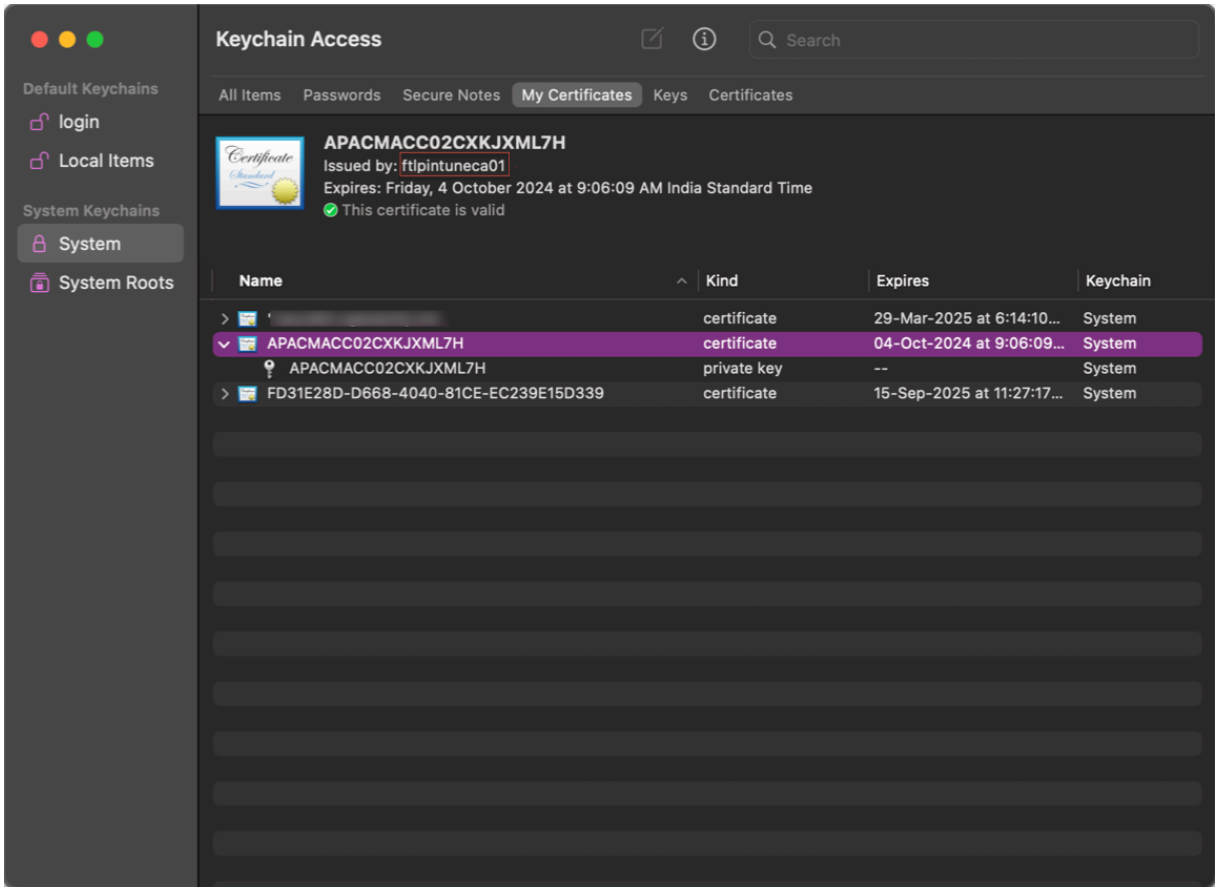
1. From the **Start** menu, open **Computer Certificate manager**.
2. Ensure that the certificate is installed in `Certificates - Local Computer\Personal\Certificates`.
    - The **Intended Purposes** must include **Client Authentication**.
    - The **Issued By** column must match the issuer name configured on the admin GUI.



macOS:

1. Open **Keychain Access** and then select **System**.
2. Click **File > Import items** to import the certificate.

   The **Issued by** field must display the certificate issuer name.



Third-party integration with device posture

September 26, 2025

In addition to the native scans offered by the Device Posture service, the Device Posture service can also be integrated with the following third-party solutions on Windows and macOS.

- Jamf Pro
- Microsoft Intune
- CrowdStrike

Jamf Pro integration with Device Posture

Jamf Pro, an Apple mobile device management (MDM) software and security provider, helps organizations configure and secure their Apple devices.

> **Important:**
>
> - The Citrix Secure Access client for macOS version 24.9.6 supports the Jamf Pro integration.
> - For the Jamf Pro integration with Device Posture to work on iOS devices, administrators must push the Citrix Workspace app from the Jamf Pro portal. For details, see Push the Citrix Workspace app from the Jamf Pro portal.

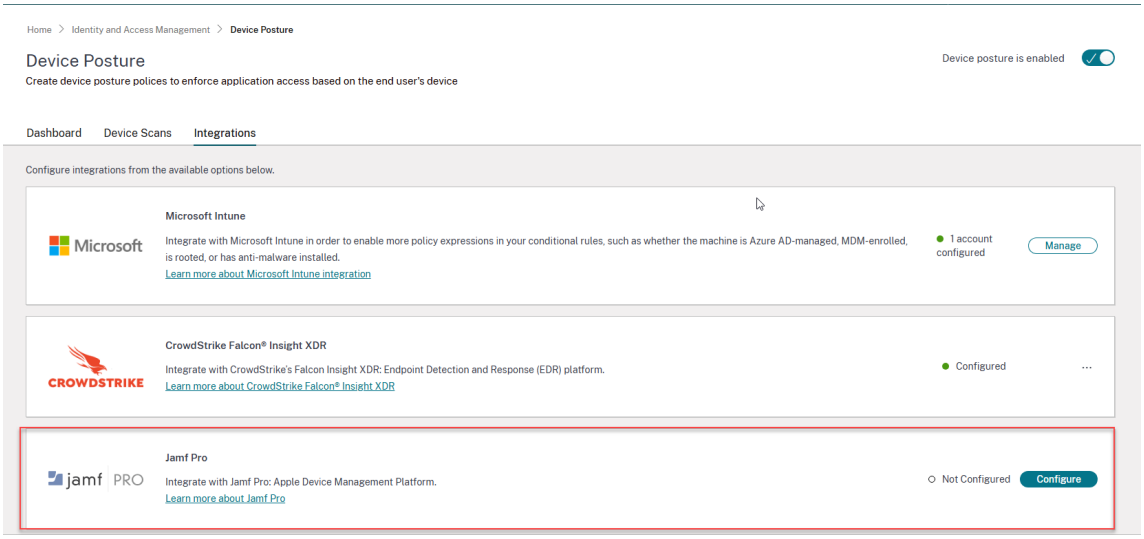
Configure Jamf Pro integration

Jamf Pro integration configuration is a two-step process.

1. Establish trust between Citrix Device Posture service and Jamf Pro service.
2. Configure policies to use Jamf Pro information.

Establish trust between Citrix Device Posture service and Jamf Pro service Perform the following steps to establish trust between Citrix Device Posture service and Jamf Pro service.

1. Sign into Citrix Cloud™, and then select **Identity and Access Management** from the menu.
2. Click the **Device Posture** tab, and then click **Manage**.
3. Click the **Integrations** tab.



> **Note:**
>
> Alternatively, customers can navigate to the **Device Posture** option on the left navigation pane of the Secure Private Access service GUI, and then click the **Integrations** tab.

4. Click the ellipsis button in the Jamf Pro box, and then click **Connect**. The **Configure Jamf Pro Integration** pane appears.

5. Enter the client ID, client secret, and Jamf Pro URL and then click **Save**.

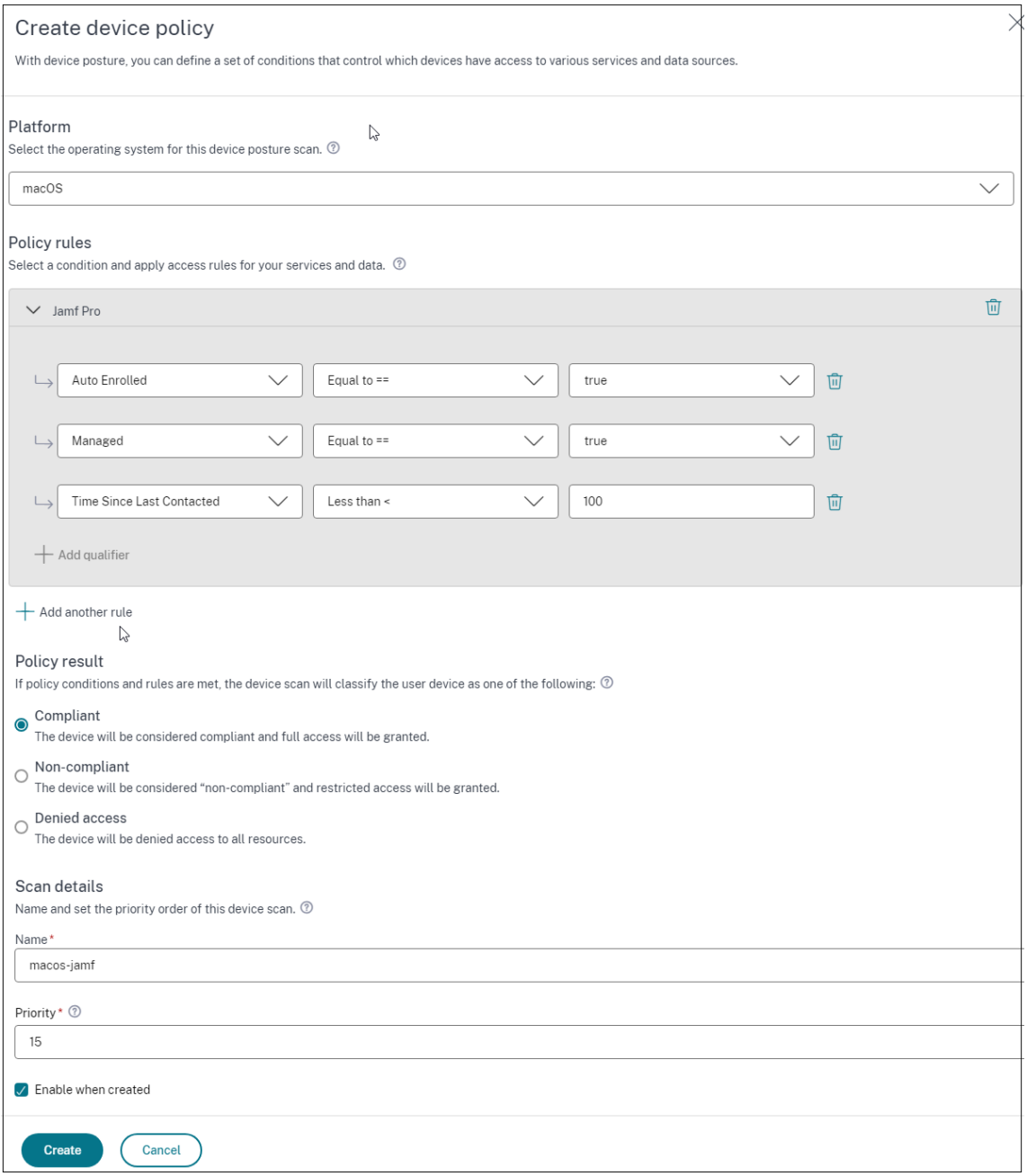
> **Note:**
>
> - You can obtain the API client ID from the Jamf Pro portal.
> - Ensure that you select the **Read Computers** and **Read Mobile Devices** scopes with read permissions for establishing the trust.
> - The Jamf Pro URL is provided by Jamf for each customer account. The Jamf Pro URL is in the format `https://<organization name>.jamfcloud.com`.

The integration is considered successful after the status changes from **Not Configured** to **Configured**.

If the integration is not successful, the status appears as **Pending**. You must click the ellipsis button, and then click **Reconnect**.

Configure device posture policies

1. Click the **Device Scans** tab and select the platform (**macOS/iOS**) for which this policy is created.
2. Click **Create device policy**.



3. In **Policy rules**, select **Jamf Pro**.
4. Select a condition, and then select the values to be matched.

    - **Auto Enrolled** - To check if the Apple device is automatically enrolled into the Jamf system during the initial setup.
    - **Managed** - To check if the device is managed by Jamf Pro.
    - **Time Since Last Contacted** - Applicable for macOS only. To check the time (in minutes) since the device last communicated with the Jamf Pro server.
    - **Time Since Last Inventory Updated** - Applicable for iOS only. To check the time (in min-

utes) since the device last communicated with Jamf Pro to update its inventory data.

5. Click **+** to add additional qualifiers.

> **Note:**
>
> You can use this rule with other rules that you configure for Device Posture.

6. In **Policy result** based on the conditions that you have configured, select one of the following.
   - **Compliant**
   - **Non-compliant**
   - **Denied login**
7. Enter the name for the policy and set the priority.
8. Click **Create**.

Push Citrix Workspace™ app from Jamf Pro portal to iOS devices

To support Jamf Pro integration with Device Posture on iOS devices, admins must push the Citrix Workspace app from the Jamf Pro portal to the iOS devices. Perform the following steps:

1. Sign in to your Jamf Pro MDM.
2. Add the Citrix Workspace app that you want to manage.
3. Link the app in the App store.
4. Create an app configuration policy for the app.
5. Add the following XML to the app configuration.

```
<dict>

<key>UDID</key>

<string>$UDID</string>

</dict>
```

Microsoft Intune integration with Device Posture

Microsoft Intune classifies a user's device as compliant or registered based on its policy configuration. During user login into Citrix Workspace, device posture can check with Microsoft Intune about the user's device status and use this information to classify the devices within Citrix Cloud as compliant, non-compliant (partial access), or even deny access to the user login page. Services like Citrix DaaS

and Citrix Secure Private Access™ in turn use device posture's classification of devices to provide contextual access (Smart Access) to virtual apps and desktops, and SaaS and Web apps respectively.

> **Important:**
>
> The Device Posture administrator must use an Intune account with the **Global Administrator** role to configure the Intune integration.

Integration of multiple Microsoft Intune accounts with Device Posture

The Device Posture service supports integration of up to five Microsoft Intune accounts. This allows organizations with multiple Intune tenants (often a result of mergers, acquisitions, or departmental segmentation) to seamlessly manage device posture across all their environments.

Some of the key benefits of integrating multiple Intune accounts with the Device Posture service are:

- Centralized device posture management: Manage the posture of devices across multiple Intune tenants from a single Device Posture console.
- Streamlined administration: Eliminates the need to switch between different Device Posture instances or manage separate configurations for each Intune account.
- Improved visibility: Gain a consolidated view of the security posture of all devices, regardless of which Intune tenant they are managed by.
- Enhanced flexibility: Supports organizations with complex IT environments and multiple Intune deployments.

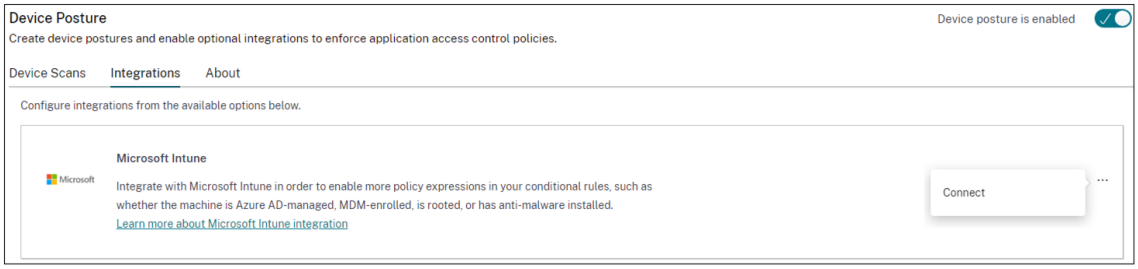
Configure Microsoft Intune integration

Intune integration configuration is a two-step process.

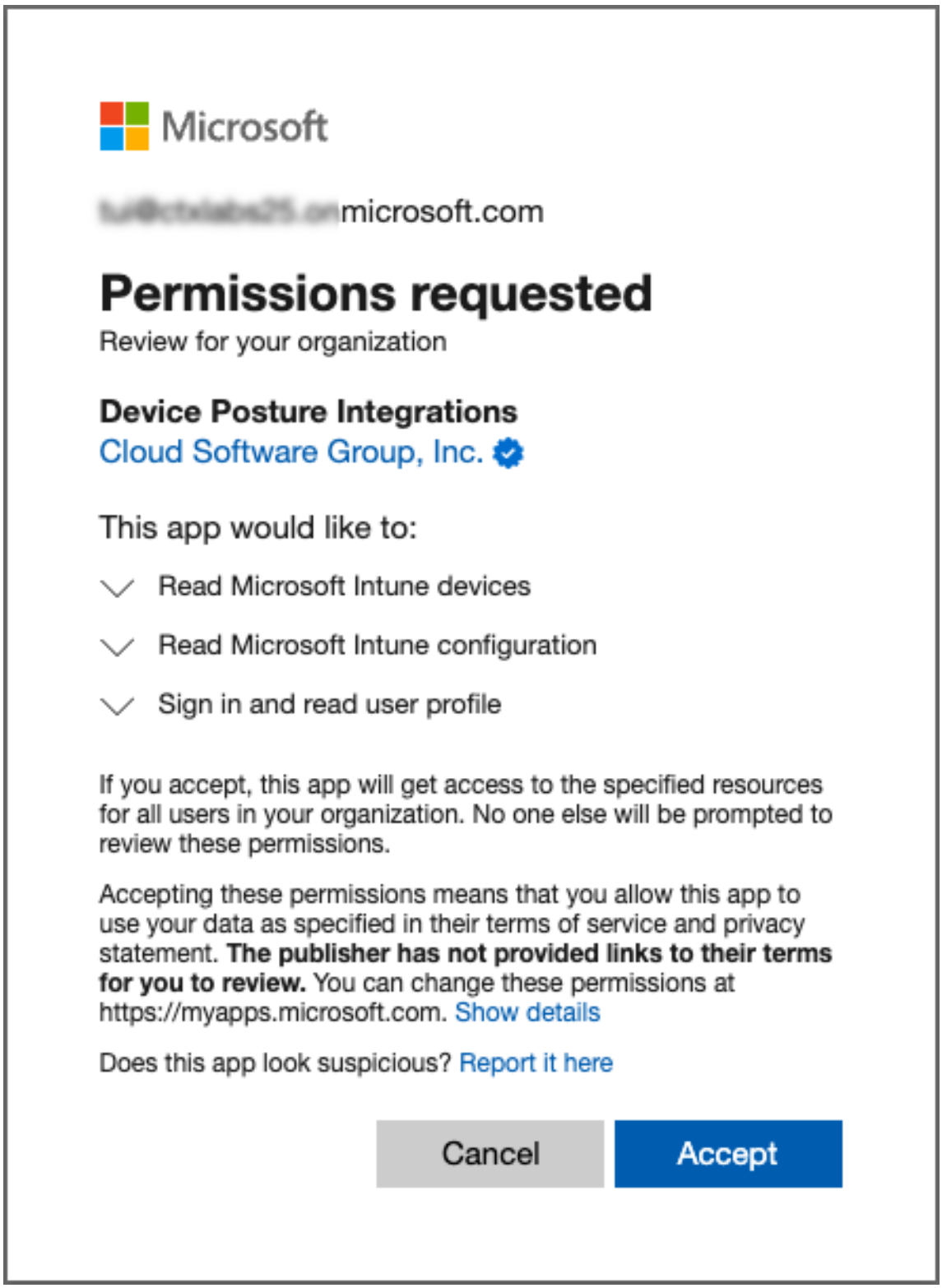
1. Integrate device posture with Microsoft Intune service. This is a one-time activity that you do to establish trust between Device Posture and Microsoft Intune.
2. Configure policies to use Microsoft Intune information.

Integrate device posture with Microsoft Intune

1. To access the **Integrations** tab, use one of the following methods:
    - Access the URL https://device-posture-config.cloud.com on your browser, and then click the **Integrations** tab.
    - Secure Private Access customers - On the Secure Private Access GUI, on the left side navigation pane, click **Device Posture,** and then click the **Integrations** tab.



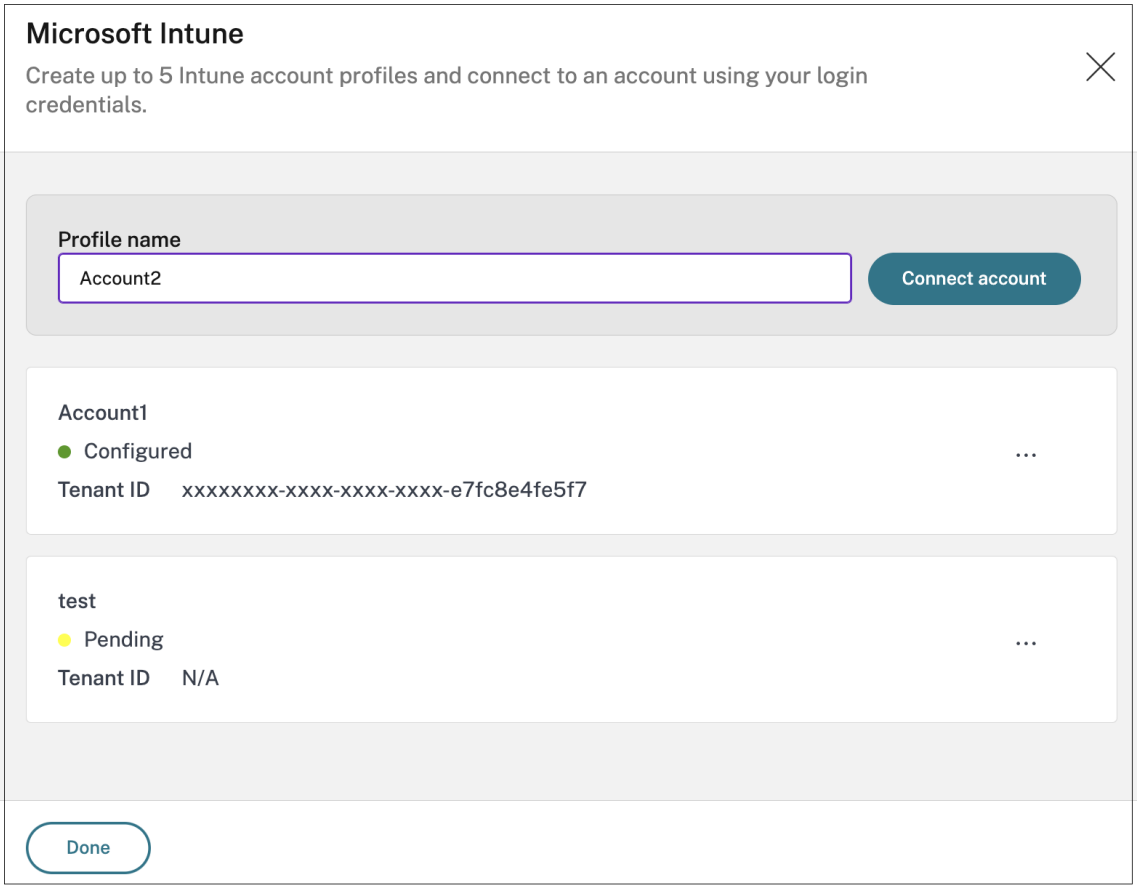
2. Click the **ellipsis** button, and then click **Connect**. The admin is redirected to Azure AD to authenticate.



Integrate multiple Microsoft Intune accounts with Device Posture

1. In the **Integrations** page, click **Manage** in the Microsoft Intune section.

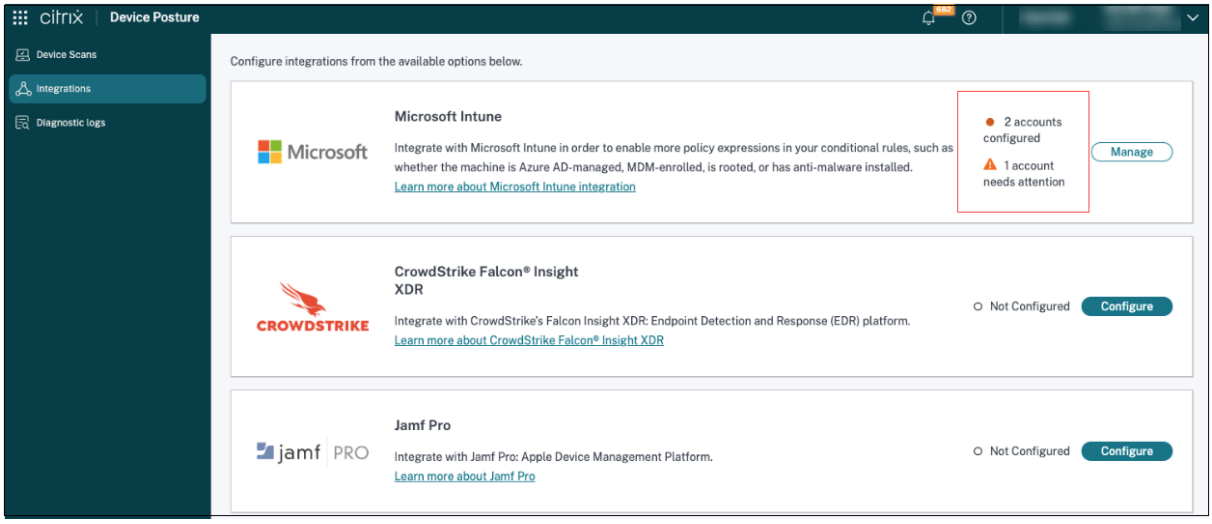
2. In **Profile name**, enter a profile name to connect to your Microsoft Intune account.
3. Click **Connect account**.



Once the connection is established, the status appears as **Configured** and the tenant ID associated with the account is displayed.

4. Click **Done**.

The Microsoft Intune section displays the number of successfully configured accounts and accounts with issues. To resolve an issue, select the affected profile from the **Profile name** drop-down list and reconnect the account.



Microsoft Intune API permissions

The following table lists the Microsoft Intune API permissions for integration with the Device Posture service.

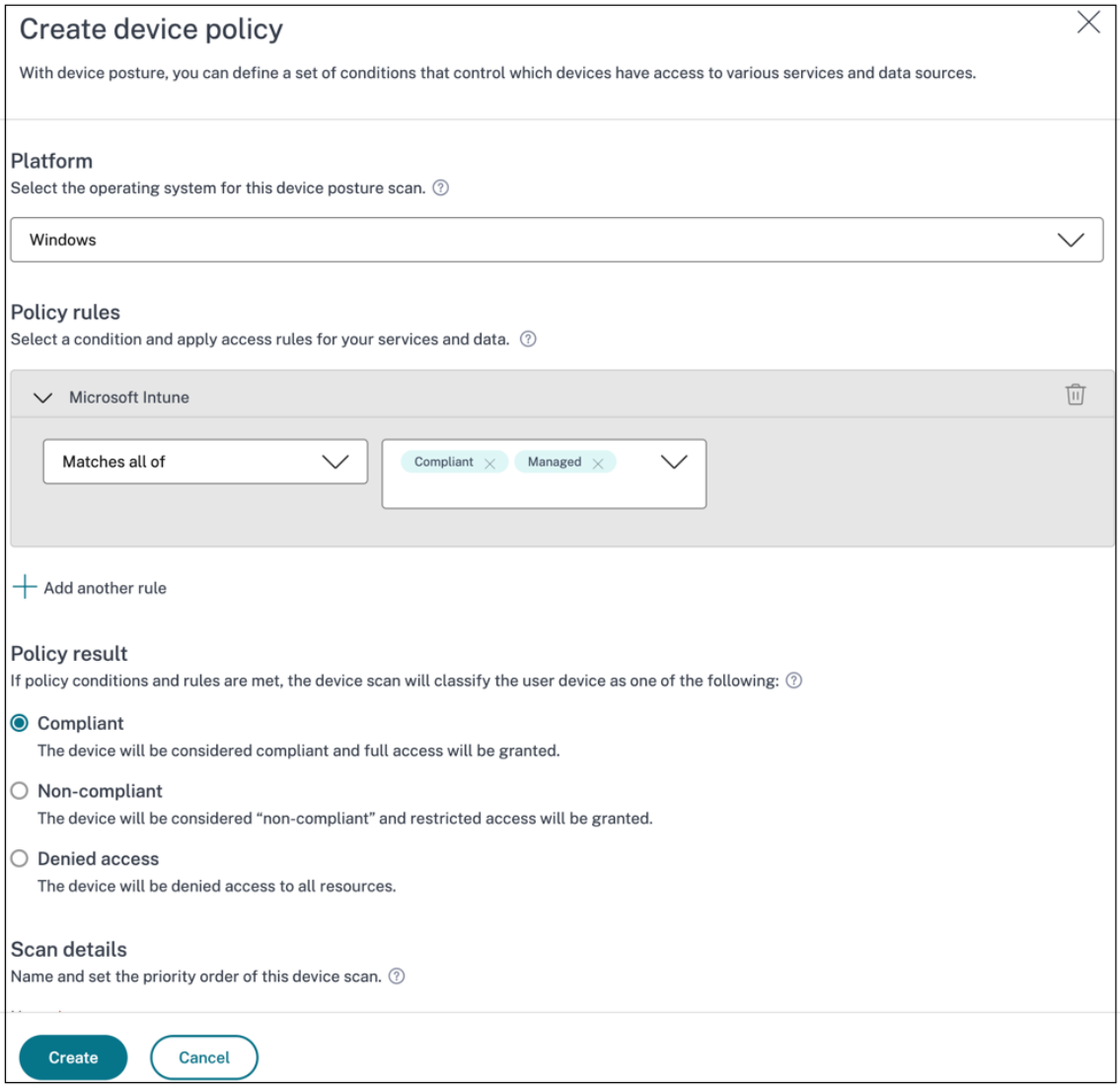
API name	Claim value	Permission name	Type
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Read Microsoft Intune devices	Application
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Read Microsoft Intune devices	Application

After the integration status changes from **Not Configured** to **Configured**, admins can create a device posture policy.

If the integration is not successful, the status appears as **Pending**. You must click the **ellipsis,** button and then click **Reconnect**.

Configure device posture policies

1. Click the **Device Scans** tab and then click **Create device policy**.



2. Enter the name for the policy and set the priority.
3. Select the platform for which this policy is created.
4. In **Policy rules**, select **Microsoft Endpoint Manager**.
5. Select the condition to be applied.
    - **Matches any of** - An OR condition is applied.
    - **Matches all of** - An AND condition is applied.
6. Select the Microsoft Intune tags to be matched.
    - **Managed** - Indicates that the device is enrolled in Intune.
    - **Compliant** - Indicates that the device meets the compliance policies set by the Intune administrator in the Intune admin center.

> **Note:**
>
> You can use this rule with other rules that you configure for device posture.

7. In **Then the device is:** based on the conditions that you have configured, select one of the following.
   - **Compliant (full access is granted)**
   - **Non-compliant (Restricted access is granted)**
   - **Denied login**

For more details about creating a policy, see Configure device posture policy.

CrowdStrike integration with Device Posture

CrowdStrike Zero Trust Assessment (ZTA) delivers security posture assessments by calculating a ZTA security score from 1 to 100 for each end device. A higher ZTA score means that the posture of the end device is better.

Citrix Device Posture Service can enable contextual access (Smart Access) to Citrix Desktop as a Service (DaaS) and Citrix Secure Private Access (SPA) resources by using the ZTA score of an end device.

Device Posture administrators can use ZTA score as part of policies and classify the end devices as compliant, non-compliant (partial access), or even deny access. This classification can in turn be used by organizations to provide contextual access (Smart Access) to virtual apps and desktops, and SaaS and Web Apps. ZTA score policies are supported for Windows and macOS platforms.

Configure CrowdStrike integration

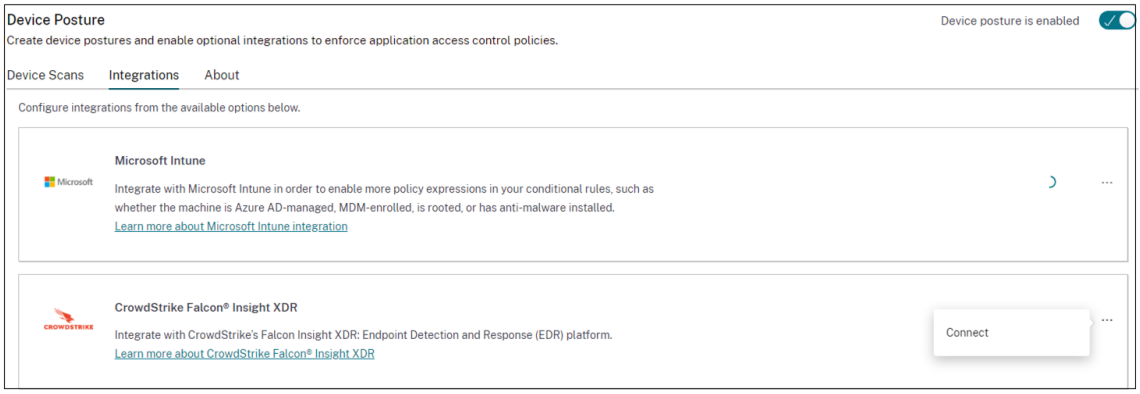
CrowdStrike integration configuration is a two-step process.

1. Establish trust between Citrix Device Posture service and CrowdStrike ZTA service. This is a one-time activity.
2. Configure access policies. The access policies use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS and Citrix Secure Private Access resources.

Establish trust between Citrix Device Posture service and CrowdStrike ZTA service Perform the following steps to establish trust between Citrix Device Posture service and CrowdStrike ZTA service.

1. Sign into Citrix Cloud, and then select **Identity and Access Management** from the hamburger menu.

2. Click the **Device Posture** tab, and then click **Manage**.
3. Click the **Integrations** tab.



> **Note:**
>
> Alternatively, customers can navigate to the **Device Posture** option on the left navigation pane of the Secure Private Access service GUI, and then click the **Integrations** tab.

4. Click the ellipsis button in the CrowdStrike box, and then click **Connect**. The CrowdStrike Falcon Insight XDR integration pane appears.
5. Enter the client ID and client secret and then click **Save**.

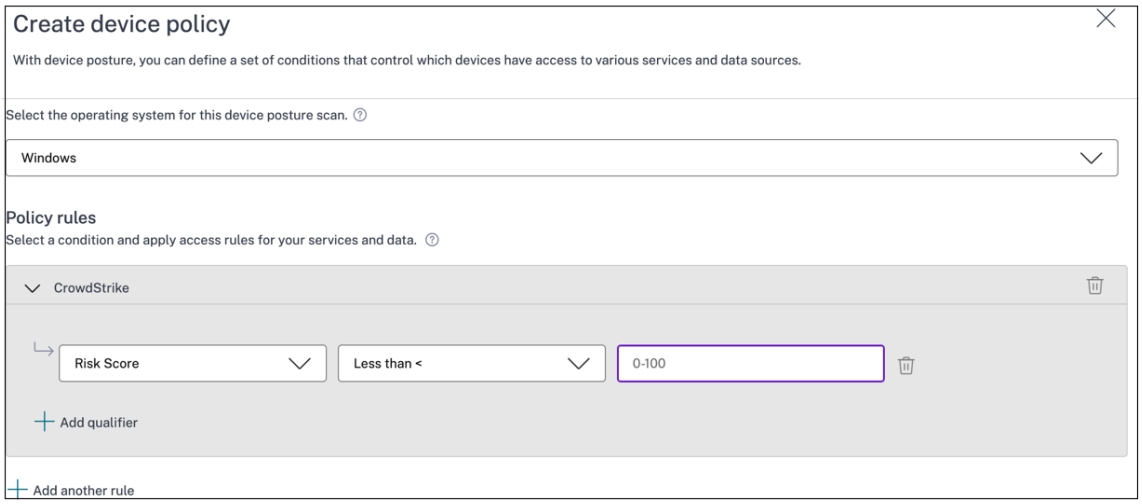
> **Note:**
>
> - You can obtain the ZTA API client ID and client secret from the CrowdStrike portal (**Support and resources > API clients and keys**).
> - Ensure that you select the **Zero Trust Assessment** and **Host** scopes with read permissions for establishing the trust.

The integration is considered successful after the status changes from **Not Configured** to **Configured**.

If the integration is not successful, the status appears as **Pending**. You must click the ellipsis button, and then click **Reconnect**.

Step 2 - Configure device posture policies Perform the following steps to configure policies to use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS™ and Citrix Secure Private Access resources.

1. Click the **Device Scans** tab and then click **Create device policy**.

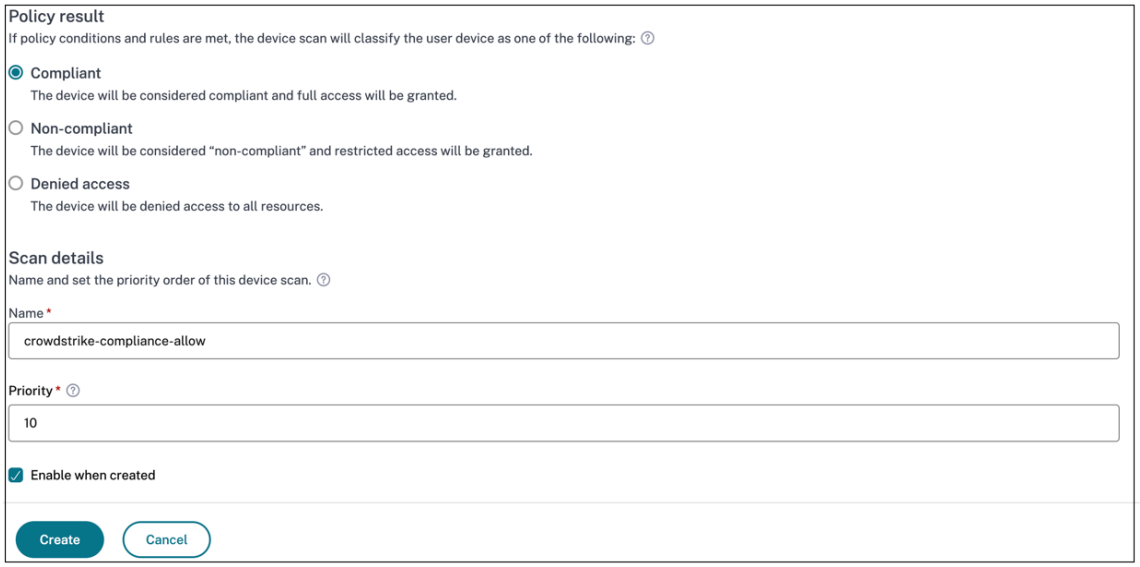


2. Select the platform for which this policy is created.
3. In **Policy Rule**, select **CrowdStrike**.
4. For the **Risk Score** qualifier, select the condition, and then enter the risk score.
5. Click **+** to add a qualifier that checks if the CrowdStrike Falcon sensor is running.

   > **Note:**
   >
   > You can use this rule with other rules that you configure for device posture.

6. In **Policy result** based on the conditions that you have configured, select one of the following.

   - **Compliant**
   - **Non-compliant**
   - **Denied login**



7. Enter the name for the policy and set the priority.
8. Click **Create**.

End user flow

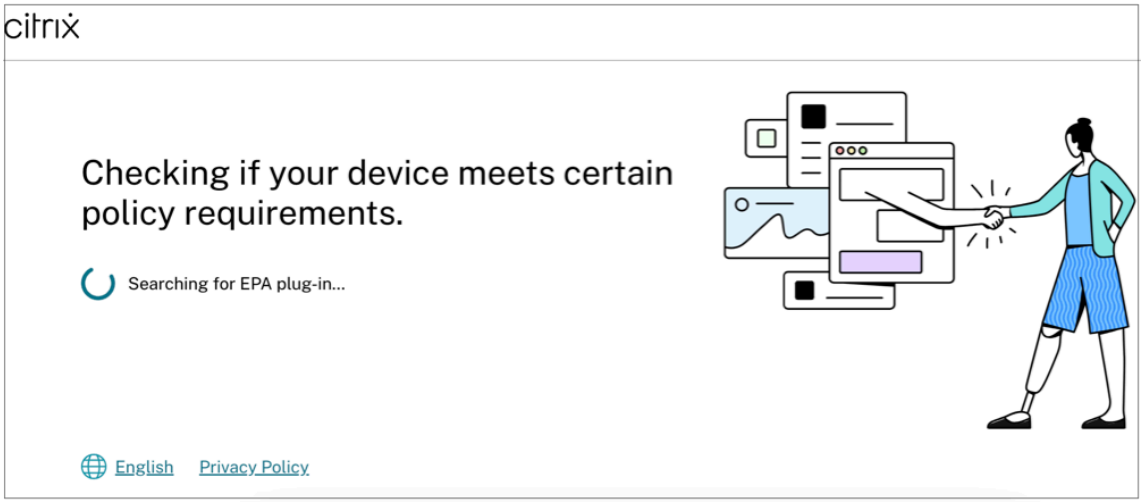
September 6, 2025

Once the device posture policies are set and device posture is enabled, the following are the end-user flows based on how the end user is logging into Citrix Workspace.

End-user flow via browser access

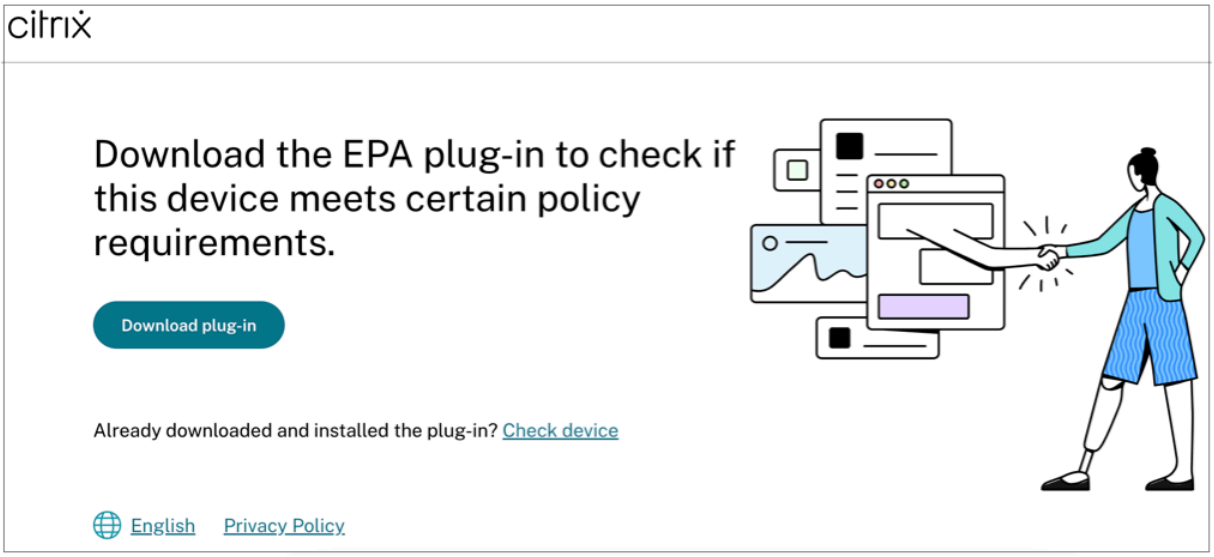
> **Note:**
>
> The macOS client and Chrome browser are used as an example for illustration purposes. The screens and the notifications vary depending on the client and the browser that you use for accessing the Citrix Workspace URL.

- When an end-user logs on to the Citrix Workspace URL `https://<your-workspace-URL` through a browser, the end user is prompted to run the Citrix EndPointAnalysis application.

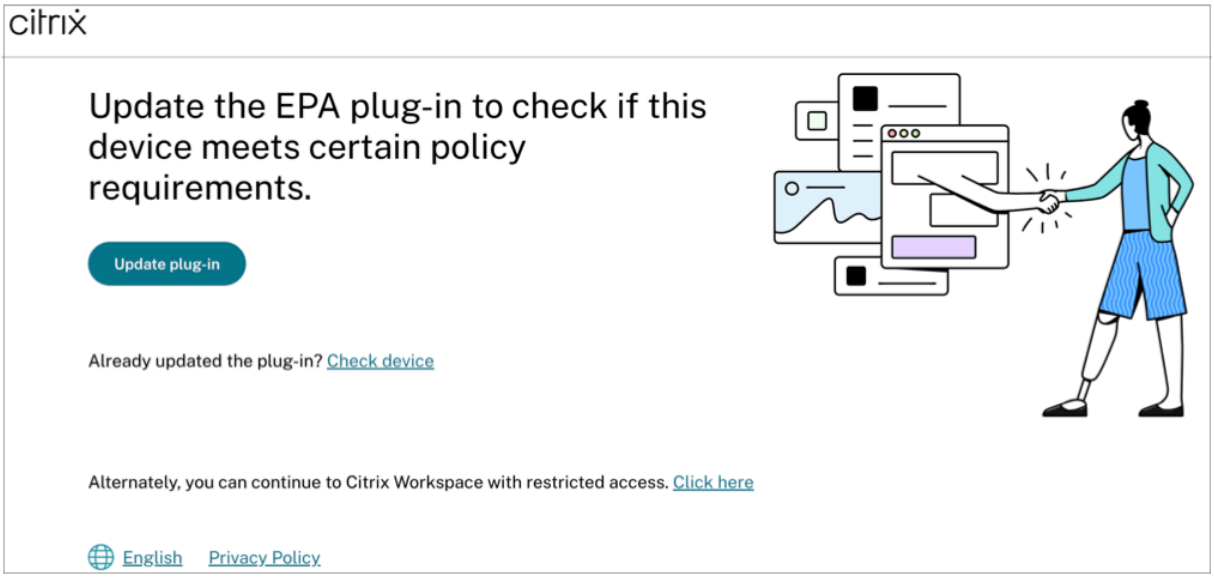


- When the end user clicks **Open Citrix End Point Analysis**, the device posture client runs and scans the endpoint parameters based on device posture policy requirements.
- If the device posture client is not installed on the device, the users are redirected to a page that displays the **Download plug-in** option. If the latest device posture client is already installed on the endpoint, the user must click **Check device** to confirm the same. Similarly, if the EPA installed on the device is not the latest version, the users are redirected to a page that displays

the **Update plug-in** option. If the EPA client is already updated, then the user must click **Check device** to confirm the same.



In both scenarios, if the skip check feature is enabled, the message *Alternately, you can continue to Citrix Workspace with restricted access.* is displayed on the **Download plug-in** or the **Update plug-in** pages.



End-user flow via Citrix Workspace application

- When an end-user logs on to the Citrix Workspace URL `https://your-workspace-url` through the Citrix Workspace application, the device posture client installed on the endpoint runs and scans the endpoint parameters based on device posture policy requirements.

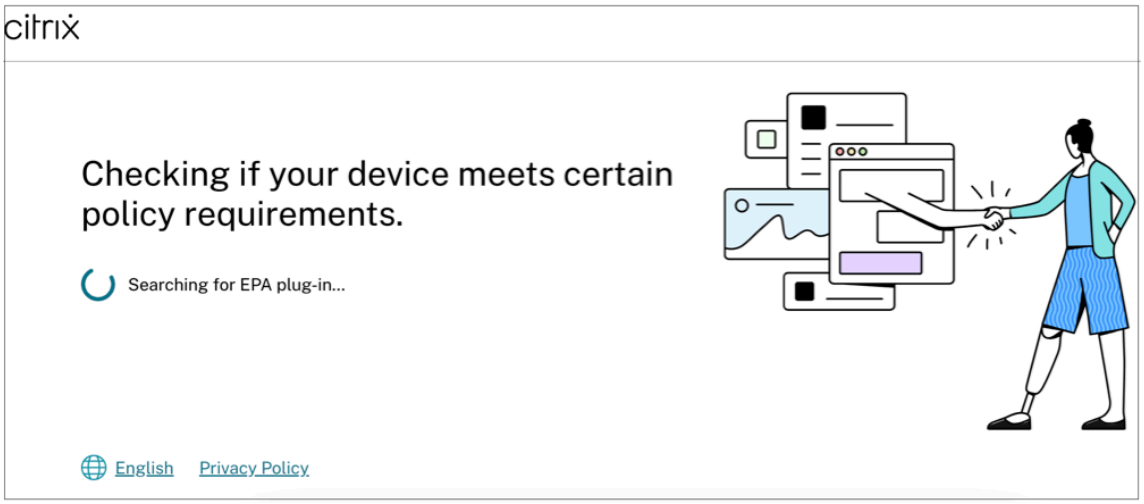
- If the latest device posture client isn't installed on the endpoint, the users are redirected to the page that displays the options **Check again** and **Download Client**. The user must click **Download Client**.
- If the latest device posture client is already installed on the endpoint, the user must click **Check again**.

End-user flow - Device posture results

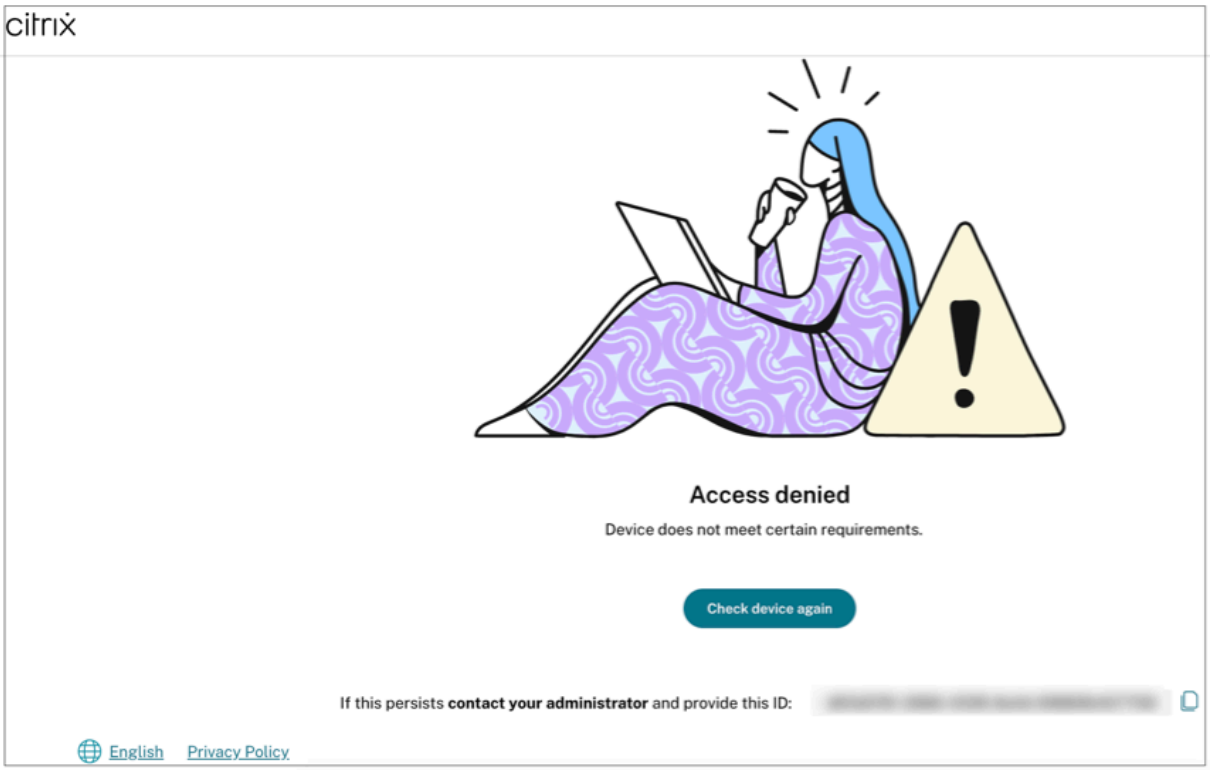
Based on the device posture policy conditions, three possibilities can occur.

If an endpoint meets the policy conditions such that the device is categorized as;

- **Compliant** - The end user is allowed to log in with unrestricted access to Secure Private Access or Citrix DaaS resources.
- **Non-compliant** - The end user is allowed to log in with restricted access to Secure Private Access or Citrix DaaS resources.



If an endpoint meets the policy conditions such that the device is categorized as **Denied access**, the **Access denied** message appears.



Device Posture service in test mode

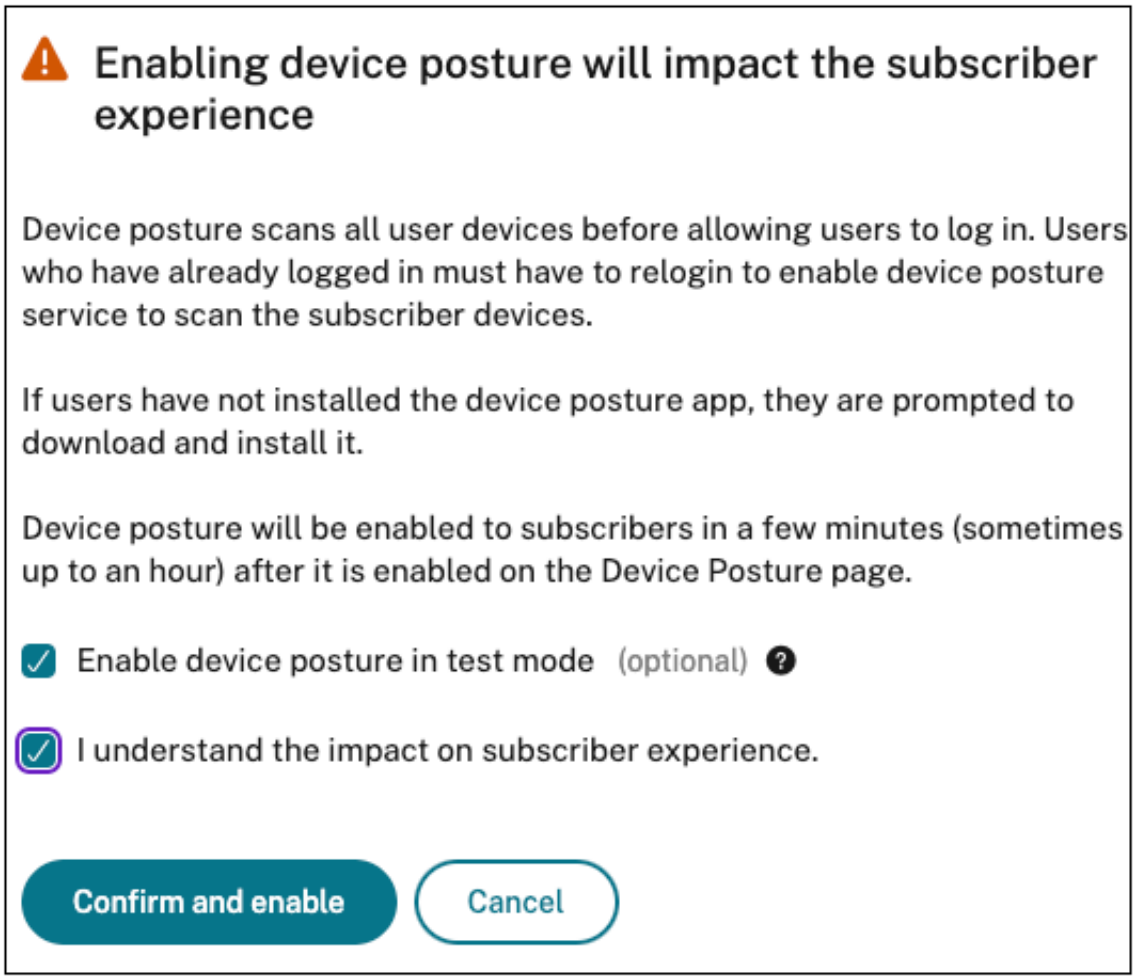
September 6, 2025

The Device Posture service is also available in test mode wherein admins can test the Device Posture service before enabling it on their production environment. This enables the admins to analyze the impact of the device posture scans on the end user devices and then plan their course of action accordingly before enabling it on production. The Device Posture service in test mode collects data of the end user devices and classifies the devices into the three categories namely, compliant, non-compliant, and denied. However this classification does not enforce any actions on the end user devices. Instead, it empowers administrators to evaluate their environments and enhance security. Admins can view this data on the Device Posture dashboard. Admins can also disable the test mode, if necessary.

> **Note:**
>
> The EPA client must be installed on the devices. In case an end device does not have the EPA client installed, the Device Posture service presents a download page to the end user to download and install the client, without which the end user cannot log on.

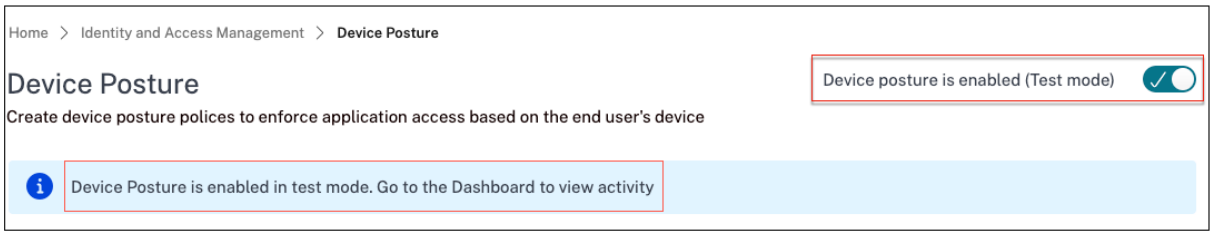
Enable test mode

1. Sign in to Citrix Cloud™, and then select **Identity and Access Management** from the hamburger menu.
2. Click the **Device Posture** tab and then click **Manage**.
3. Slide the **Device posture is disabled** toggle switch ON.
4. In the confirmation window, select both the checkboxes.



5. Click **confirm and enable**.

When the Device Posture service is enabled in test mode, the Device Posture home page displays a note confirming the same.



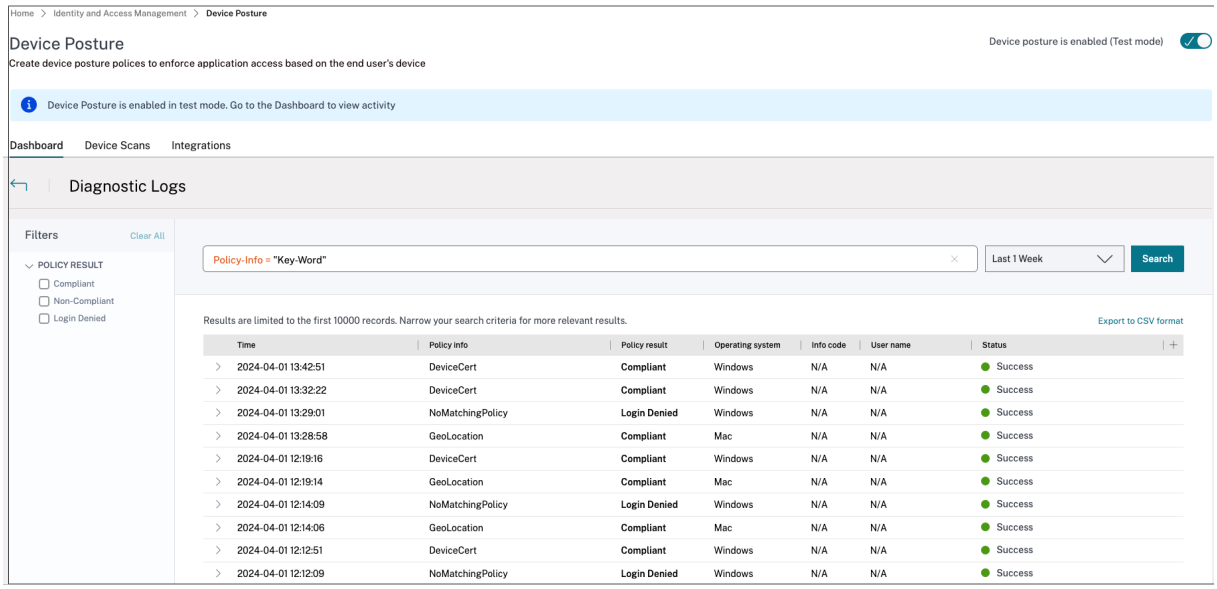
Admins can configure the policies and rules for device posture scans. For details, see Configure device posture. Based on the scan results, the end user devices are classified as compliant, non-compliant, and denied. Admins can view this data on the dashboard.

View the test mode activities on the dashboard

1. Click the **Dashboard** tab on the Device Posture page.

   The **Diagnostic logs** chart displays the number of devices classified as compliant, non-compliant, and login denied.

2. To view the details, click the **See more** link.



Admins can download the monitoring logs from the UI.

Enable test mode in production

If the Device Posture service is already enabled on production, perform the following steps to enable the test mode:

1. On the home page, slide the **Device Posture is enabled** toggle switch OFF.

2. Select **I understand all device posture checks will be disabled**.
3. Click **confirm and disable**.
4. Now enable the device posture by sliding the **Device Posture is disabled** toggle switch ON.
5. In the confirmation window, select both of the following options.
    - **Enable device posture in test mode**
    - **I understand the impact on subscriber experience**
6. Click **confirm and enable**.

Transition from test mode to production

To transition from test mode to production, you must first disable Device Posture in the test mode and then enable Device Posture again without selecting the option **Enable device posture in test mode**.

> **Important:**
>
> - It is important to thoroughly review your policies before transitioning from test mode to production. Policies that were set up in test mode might behave differently when enforced in production, potentially impacting user access specifically **Deny Access**. In test mode, **Deny Access** is effectively treated as **Non-Compliant,** allowing users to continue accessing the system without disruption. However, in production, this outcome directly blocks access, potentially impacting user experience and operations.
> - Also, when transitioning from test mode to production, there might be potential downtime. It is recommended to plan your transition carefully to minimize disruptions.

Multi-workspace URLs support - Preview

October 24, 2025

Administrators can apply distinct device posture policies to different Citrix Workspace™ access URLs, offering granular control and simplified security management.

Previously, the Device Posture service was enabled globally across all workspace URLs, preventing administrators from applying specific requirements on a per-URL basis.

With multi-workspace URLs support, you can now do the following:

- Apply distinct device posture checks for specific workspace URLs.
- Enforce varying levels of device compliance based on the workspace URL that users access.

- Create and test device posture checks on test workspace URLs before deploying to production URLs.

Important considerations

Before implementing multi-workspace URLs, note the following:

- Service continuity might be interrupted during initial setup or due to misconfiguration. We recommend testing this feature in a controlled test environment before deploying to production.
- Use a phased approach to minimize end-user impact during rollout:
  - Create a new workspace URL specifically for a small group of test users.
  - Keep your existing production workspace URL operational with its current configuration.

  This approach allows you to validate the multi-workspace URLs feature without disrupting the broader user base.

Prerequisites

- Supported platforms: Windows, macOS and iOS
- Multi-workspace URLs support is available in the following EPA clients:
  - Windows: Version 25.2.1.18 and later. Download link.
  - macOS: Version 25.6.10 and later. Download link.
  - iOS: Citrix Workspace app (CWA) version 25.5.0 and later (installed from App Store).

> **Note:**
>
> - Users accessing from devices running on platforms other than Windows, macOS, or iOS are treated as non-supported and follow the default behavior configured by the administrator in the Device Posture service console:
>
>   > - Devices on non-supported platforms are marked as **Non-compliant** by default.
>   > - You can change the classification from **Non-compliant** to **Denied login** from the **Settings** tab on the Device Posture page.
>   > - For the definitions of “compliant”and “non-compliant,”see Definitions.
>
> - The EPA clients on endpoints must use the versions specified in the prerequisites section. If clients use older versions, device scans fail to start. For Windows administrators, this requirement is simplified because the EPA client is bundled with Citrix Secure Access™ Client for Windows 2505.

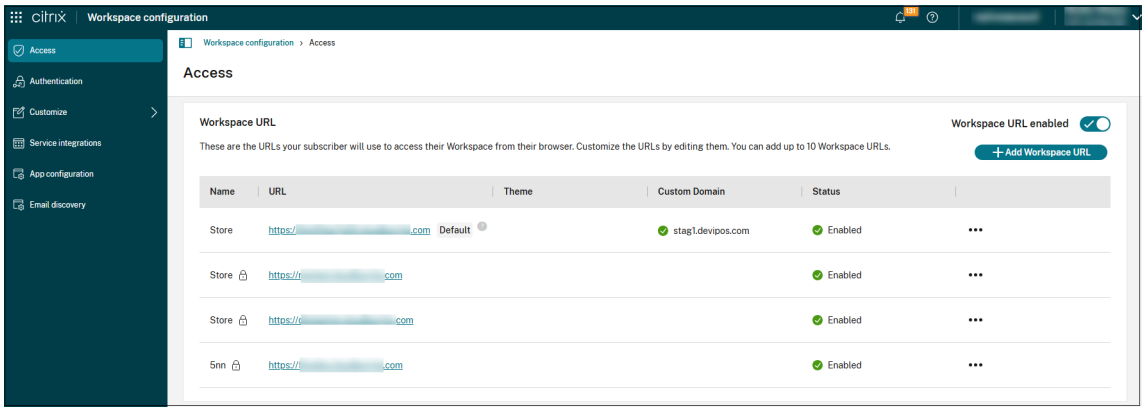
> - You can also skip device posture checks for non-supported devices. For details, see Skip device posture checks.

Enable the feature

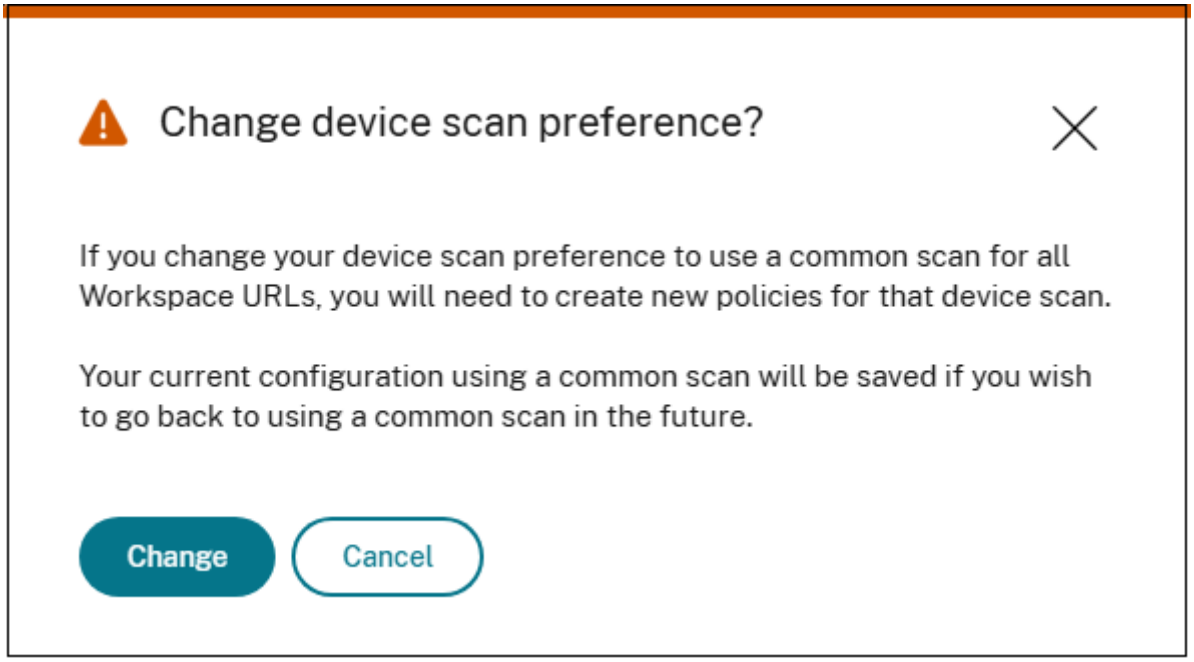
To enable multi-workspace URLs support for your organization, complete the enablement request form. Once submitted, the Citrix team will enable this feature for your environment.

Configure multi-workspace URLs

1. Ensure workspace URLs are configured via **Workspace configuration > Access**.



2. To access Device Posture, log in to Citrix Cloud™ and navigate to **Identity and Access Management > Device Scans** in the Device Posture navigation bar.
3. Click **Configure Device Posture** and then click **Settings**.
4. Select **Use different device scans per Workspace URL**.
5. To modify the device posture preference, click **Change**.



Note:

- When the **Use different device scans per Workspace URL** option is enabled, all existing global scans become inactive. You must configure new scans individually for each workspace URL.
- After configuring and saving new scans, users are prompted to re-authenticate within 1-2 hours to ensure that their login sessions are evaluated using the new configuration.

Export of Device Posture user events into SIEM systems

September 6, 2025

The Device Posture service events are exported to Security Information and Event Management (SIEM). This allows you to view the following user events associated with the Device Posture service in your SIEM:

- All event types related to Device Posture service.
- Device Posture evaluation events, which provide information about the evaluation of a device's posture against the defined policies.

The following are the benefits of exporting events into SIEM systems:

- Enables your Security Operations teams to correlate, analyze, and search data from disparate logs.

- Helps your Security Operations teams to identify and quickly remediate the security risks.
- Visibility of security alerts in a centralized place.
- Centralized approach to detect potential security threats for organizational risk analysis capabilities such as risk indicators, user profiles, and risk scores.
- Ability to combine and correlate the Citrix Analytics risk intelligence information of a user account with the external data sources connected within your SIEM.

For more information, see the following topics:

- Device Posture service events
- Diagnose Device Posture service events failure
- Security Information and Event Management (SIEM) integration

Troubleshoot Device Posture issues using DaaS Monitor

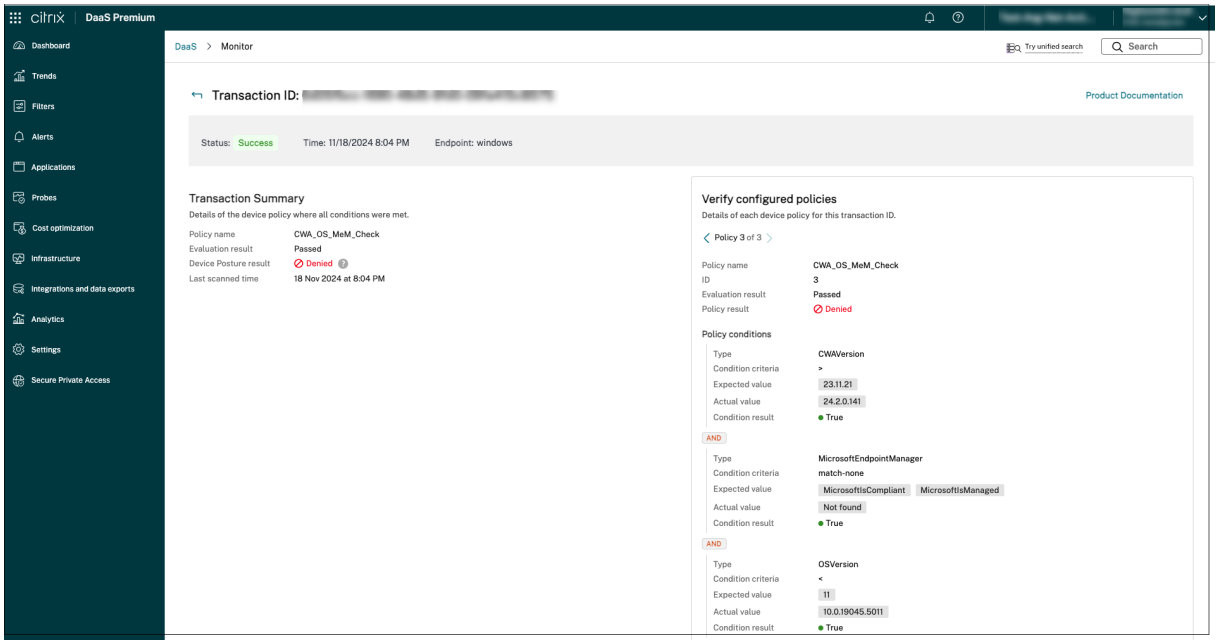
September 6, 2025

You can troubleshoot the Device Posture issues/errors in DaaS Monitor using the transaction ID that is generated for each session when a user connects through Secure Private Access or DaaS. When you locate the transaction ID, the DaaS Monitor displays information about the session and the associated Device Posture policy that was applied. Monitor also displays the policy results, including whether the device passed or failed the posture checks.

Device posture events on Citrix DaaS™ Monitor

Perform the following steps to view the events logs for the Device Posture service.

1. Copy the transaction ID of the failed or access denied session from the end user device.
2. Sign into Citrix Cloud.
3. On the DaaS tile, click **Manage**, and then click the **Monitor** tab.
   In the Monitor UI, search for the 32-digit transaction ID and click **Details**.



For more information, see the following topics:

- Troubleshoot Device Posture service policies and transactions with Monitor
- Review SIEM data exports format for device posture events

Device Posture logs and events

January 9, 2026

Administrators can monitor device compliance through the device posture dashboard. They can view all configured device posture policies that define compliance requirements for endpoints accessing organizational resources. They can also view real-time compliance status for all devices, including detailed evaluation results categorized as follows:

- **Compliant:** Devices that meet all specified security requirements and policy criteria.
- **Non-compliant:** Devices that fail to meet one or more security requirements but might still have limited access.
- **Access denied:** Devices that pose significant security risks and are blocked from accessing resources.

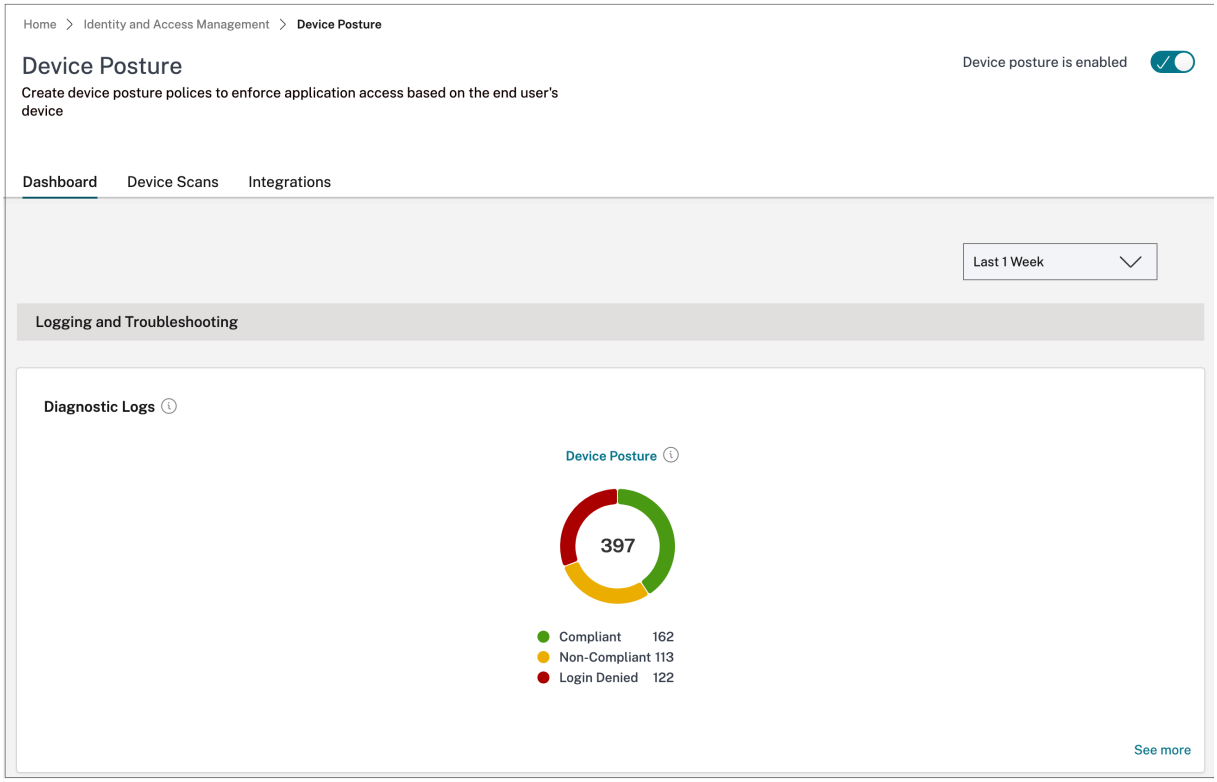
You can view the Device Posture logs and events in the Secure Private Access dashboard and in the Device Posture dashboard in the Identity and Access Management console.

Device Posture dashboard in Identity and Access Management console

Perform the following steps to view the logs and events for the Device Posture dashboard in the Identity and Access Management console.

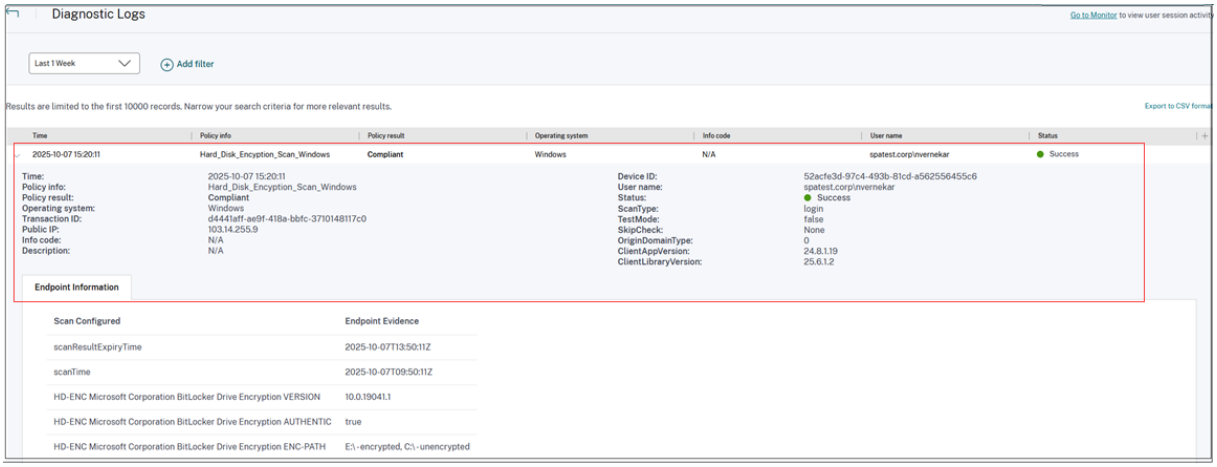
1. Sign into Citrix Cloud.
2. From the Citrix Cloud menu, select **Identity and Access Management**,
3. Click **Device Posture > Manage** and then click **Dashboard.**

   The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service.
4. Click the **See more** link to view the details of the logs. You can refine your search based on the policy results (**Compliant**, **Non-Compliant**, and **Login Denied**).



You can use the **Add filter** option to refine your search based on various criteria such as policy info, policy result, operating system, transaction ID, info code, or device ID. For example, in the search field, you can click **Device-ID**, select **~ (contains some value)**, and enter 6273. All logs related to device IDs containing 6273 are displayed.

Click the expand icon next to each log entry to view comprehensive details, such as scan type, client app version, client library version, and endpoint information.



Note:

- The **ClientAppVersion** and the **ClientLibraryVersion** fields display the EPA client version and library version respectively.
- The transaction ID is also displayed to the end user whenever access is denied.
- If there's an error or a scan failure, the Device Posture service displays a transaction ID. This transaction ID is available in the Secure Private Access service dashboard. If the logs do not help resolve the issue, end users can share the transaction ID with Citrix Support to resolve the issue.

Logs location

The Windows client logs can be found at:

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

The macOS client logs can be found at:

- ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

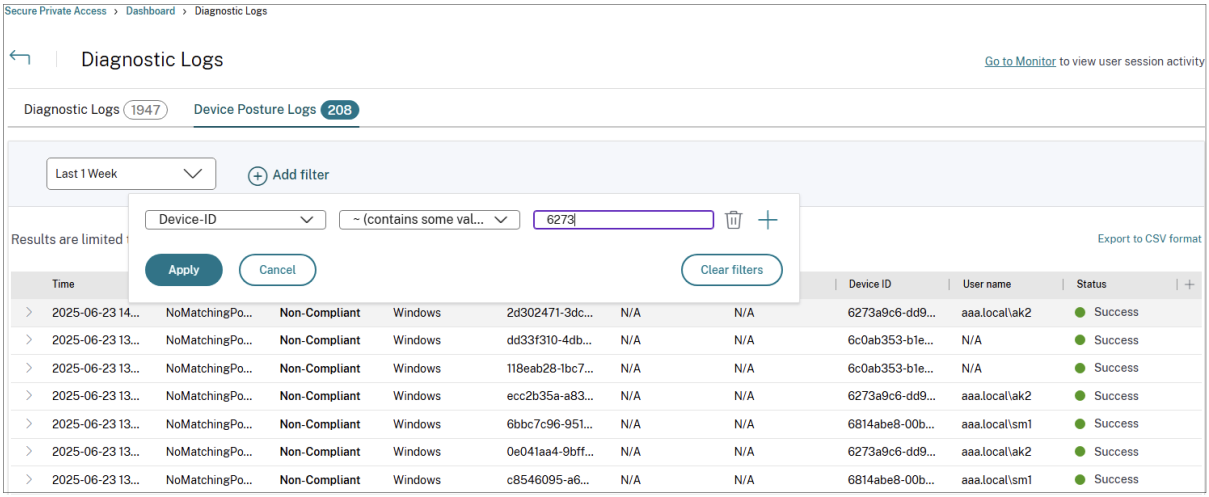
Secure Private Access dashboard

Perform the following steps to view the logs and events for the Device Posture service.

1. Sign into Citrix Cloud.
2. On the Secure Private Access tile, click **Manage** and then click **Dashboard**.

   The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service.

3. Click the **See more** link to view the details of the logs. You can refine your search based on the policy results (**Compliant**, **Non-Compliant**, and **Login Denied**).



Device posture error logs

The following logs related to the Device Posture service can be viewed on the Citrix Monitor and Secure Private Access dashboard. For all these logs, it's recommended that you contact Citrix Support for resolution.

- Failed to read configured policies
- Failed to evaluate endpoint scans
- Failed to process policies/expression
- Failed to save endpoint details
- Failed to process scan results from endpoints

Device posture data export

The Device Posture service events (such as device posture results and event types) can be exported to the Security Information and Event Management (SIEM) service. These events are generated when the Citrix Endpoint Analysis (EPA) client performs a posture check on a device attempting to access Citrix Virtual Apps and Desktops™ or Citrix Secure Private Access resources.

- To understand how to set up, configure, and export your Device Posture service logs to SIEM, see Security Information and Event Management (SIEM) integration.
- To know more about what events and logs you can export from the Device Posture service, see Device Posture service events.
- To understand how to diagnose and troubleshoot Device Posture service transactions, see Diagnose Device Posture service transactions.

Diagnose Device Posture service transactions

September 9, 2025

Administrators can now diagnose and troubleshoot Device Posture service transactions effectively. This update enhances troubleshooting capabilities in Citrix Monitor, providing detailed insights into Device Posture policy evaluation, compliance checks, and error diagnostics.

Understanding the Device Posture service evaluation flow

A typical Secure Private Access or VDI app access launch involves the following three stages:

1. **Pre-authentication**: A basic endpoint hygiene check is conducted using Device Posture service. Access is blocked before authentication if a device fails to meet compliance policies.
2. **Authentication**: Authenticates the user in this stage. Authentication fails if there is credential mismatches or identity provider errors.
3. **Application access**: The following two sub stages are involved in this stage:
    - **Policy brokering and enumeration stage**: When a user's device context violates policy settings, access to applications is restricted.
    - **Application launch stage**: The final stage, where an application transaction completes using Citrix Enterprise Browser™, Secure Private Access client, or native endpoint client.

Troubleshooting enhancements in Citrix Monitor

With this update, Citrix Monitor provides search-based Device Posture service troubleshooting, allowing IT teams to:

- Filter transactions by a user ID or transaction ID for targeted debugging.
- Analyze policy evaluation outcomes such as whether a device is compliant, non-compliant, or blocked due to policy violations.
- Pinpoint policy failures by examining detailed compliance checks, expected values, and real-time contextual values.
- Review device metadata, policy configurations, and logs for deeper diagnostics.
- Identify failed transactions due to system errors, with error messages linked to knowledge-base articles for quick resolution.

How IT teams can use the troubleshooting enhancement

Triaging Device Posture issues

Search a user-reported transaction ID to locate relevant Device Posture service logs quickly. Review whether compliance checks passed or failed and determine root causes.

For example, when searching for a transaction ID, you can review the Device Posture check policy outcome—whether it was successful (compliant or non-compliant) or failed due to an error. The system provides the full context of the Device Posture service evaluation, including client metadata, policy details, and other transaction details.

Investigating policy-based access blocks

When a device is non-compliant, IT can inspect the exact policy parameters that failed. The system provides side-by-side comparisons of the configured expected value to the device's real-time data.

Debugging large policy sets with precision search

Admins can search for specific parameters in complex environments with multiple policies and verify whether the expected user context is present. The system visually highlights the failing condition if a parameter value mismatch occurs, accelerating root cause identification. Also, admins can navigate through policies to see which ones were evaluated and which ones generated the current transaction outcome.

To troubleshoot large working sets of policy parameters, you can search the parameters and see if the desired user context is present in real time.

For example, in the preceding screenshot, the highlighted field, when searched, resulted in no outcome (mentioned in the following image), suggesting that the parameter value did not match. This mismatch caused the condition result to be false and, failing that, the overall policy outcome to be denied.

Handling transaction failures and errors

If a policy evaluation fails due to a system error, the following details are displayed in Citrix Monitor:

- Error descriptions with contextual details.
- Links to troubleshooting documentation, enabling faster resolution.

Steps to Diagnose Device Posture service transactions

1. Copy the transaction ID of the failed or access-denied session from the end-user device.
2. Sign into Citrix Cloud.
3. On the DaaS tile, click **Manage**, and then click the **Monitor** tab.
4. Enter the transaction ID in the **Search** field and click **Details**.

You can view the transaction summary and the verification details of the configured Device Posture policies. The different values for policy evaluation are compliant, non-compliant, and deny.

Transaction summary

The **Transaction Summary** page provides the outcome of the Device Posture policy. For compliant, non-compliant, and denied results, the summary includes:

- **Platform**: The OS of the client device.
- **Policy name**: Name of the Device Posture policy.
- **Evaluation result**: Indicates whether the Device Posture policy passed or failed.
- **Device Posture result**: Indicates whether the Device Posture outcome is compliant, non-compliant, or denied.
- **Last scanned time**: The time when the device was last scanned.

Verify configured policies

The **Verify Configured Policies** section provides comprehensive details of policy evaluation, including:

- Reasons for failure.
- The specific rule that failed.
- Evidence collected.

This information allows admins to troubleshoot and take appropriate actions based on the policy details.

Device posture policy evaluation process

1. **Policy failure and rule identification**:
    - Identify which rule failed and why it failed.
    - Collect evidence related to the failure.

2. **Outcome determination**:
    - Depending on the policy evaluation, the outcome can be compliant, non-compliant, or denied.
    - If no policies match, the outcome is "no matching policy."
3. **Viewing policy details**:
    - Admins can view the details of each device policy for a specific transaction ID.
    - Use the backward and forward arrows to navigate through different policies.

    In cases of compliant, non-compliant, and denied results, the Device Posture policy evaluation includes the following information in the Verify Configured Policies section:

    - **Policy name**: Name of the device policy.
    - **ID**: The order in which the policy is evaluated.
    - **Evaluation result**: Indicates whether the Device Posture policy passed or failed.
    - **Policy result**: Indicates whether the Device Posture outcome is compliant, non-compliant, or denied.
    - **Policy Conditions**:
        - **Type**: The device scan type.
        - **Condition criteria**: The condition to evaluate the policy rule.
        - **Expected value**: The configured value of the policy condition.
        - **Actual value**: The evidence collected from the endpoint.
        - **Condition result**: Indicates whether the condition passed or failed.

Error code

When there is an issue and Device Posture fails to evaluate the policy, the error code is displayed.

If there is a failure, copy the error code and contact Citrix support.

The policy details and error codes simplify the triage and troubleshooting of user issues.

The following table provides the error code, error message, and solution for the error:

#	Error message	Error code	Action
1	Failed to read configured policies.	0x0050001	Contact Citrix Support
2	Failed to evaluate endpoint scans.	0x0050002	Contact Citrix Support

#	Error message	Error code	Action
3	Failed to process policies or expression.	0x0050003	Contact Citrix Support
4	Failed to save endpoint details.	0x0050004	Contact Citrix Support
5	Failed to process scan results from endpoints.	0x0050005	Contact Citrix Support
6	Failed to read Device Posture mode configuration.	0x0050006	Contact Citrix Support

Manage Citrix Endpoint Analysis client for Device Posture service

February 4, 2026

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access™ resources (SaaS, Web apps, TCP, and UDP apps).

To run device posture scans on an end device, you must install the Citrix EndPoint Analysis (EPA) client, which is a lightweight application, on that device. Device Posture service always runs with the latest version of the EPA client released by Citrix.

Installation of the EPA client

During runtime, the Device Posture service prompts the end user to download and install the EPA client during run-time. For details, see End-user flow.
Usually, an EPA client does not require local admin rights to download and install on an endpoint. However, to run device certificate check scans on an end device, the EPA client must be installed with administrator access. For details about installing an EPA client with administrator access, see Install device certificate on the end device.

Upgrade of the EPA client for Windows

When a new version of the EPA client is released, the EPA clients for Windows are upgraded by default after the first installation. Auto-upgrade ensures that the end-user devices are always running

on the latest version of the EPA client that is compatible with the Device Posture service. For the auto-upgrade, the EPA client must have been installed with administrator access.

Distribution of the EPA client

EPA clients can be distributed using Global App Configuration service (GACS) or EPA integrated with Citrix Workspace™ app installer, or using software deployment tools.

- **EPA client installer integrated with Citrix Workspace app:** The EPA client installer is integrated with Citrix Workspace app 2402 LTSR for Windows and macOS. This integration eliminates the need for the end users to install EPA client separately after installing Citrix Workspace app.
  - To install the EPA client as part of Citrix Workspace app for Windows, use the command line option `InstallEPAClient`. For example, `./CitrixworkspaceApp.exe InstallEPAClient`.
  - For macOS, the EPA client installer is installed by default.

  > **Note:**
  >
  > - EPA client installation as part of Citrix Workspace app is disabled by default. It must be explicitly enabled by using the command line option `InstallEPAClient`.
  > - If an end device already has an EPA client installed and the end user installs Citrix Workspace app, the existing EPA client is upgraded.
  > - If an end user uninstalls Citrix Workspace app, then the integrated EPA client is also removed from the device, by default. However, if the EPA client was not installed as part of the integrated Citrix Workspace app installation, then the existing EPA client is retained in the device.
  > - The EPA client installer integrated with Citrix Workspace app can also be used with NetScaler. For details, see Manage EPA client when used with NetScaler and Device Posture.

- **Distribute the client using GACS**: GACS is a Citrix provided solution to manage the distribution of client-side agents (plug-ins). The Auto update service available in GACS ensures that the end devices are on the latest EPA versions without end user intervention. For more information on GACS, see How to use the Global App Configuration service.

> **Note:**
>
> - GACS is supported on Windows devices only for distributing the EPA client.
> - To manage an EPA client through GACS, install Citrix Workspace Application (CWA) on the end devices.

> - If CWA is installed with administrator privileges on an end user device, then GACS installs the EPA client with the same administrator privileges.
> - If CWA is installed with user privileges on an end user device, then GACS installs the EPA client with the same user privileges.

Distribute the client using Software deployment tools: The latest EPA client can be distributed by admins through software deployment tools like Microsoft SCCM.

Manage EPA client when used with NetScaler and Device Posture

The EPA client can be used together with NetScaler and Device Posture in the following deployments:

- NetScaler based adaptive authentication with EPA
- NetScaler based on-premises gateway with EPA

The Device Posture service pushes the latest version of the EPA client to the end devices. However, on NetScaler, administrators can configure the following version control for the EPA scans on gateway virtual servers:

- **Always**: The EPA client on the end device and NetScaler must be on the same version.
- **Essential**: The EPA client version on the end device must be within the range configured on NetScaler.
- **Never**: The end device can have any version of the EPA client.

For more information, see Plug-in behaviors.

Considerations when EPA client is used with NetScaler and Device Posture

When an EPA client is used together with Device Posture Service and NetScaler, there might be scenarios where the end device is running the latest EPA client version whereas NetScaler is on a different version of the EPA client. This might result in a mismatch of the EPA client version on NetScaler and the end device. As a result, NetScaler might prompt the end user to install the EPA client version which is present on NetScaler. To avoid this conflict, we recommend the following configuration changes:

- If you have configured EPA with Adaptive Authentication or on-premises authentication or gateway virtual server, it is recommended that you disable version control of the EPA client on NetScaler. This is done to ensure that the GACS or Device Posture service does not push the latest version of the EPA client to the end devices.
- The EPA version control can be set to **Never** by using the CLI or the GUI. These configuration changes are supported on NetScaler 13.x and later versions.

- CLI: Use the CLI commands for Adaptive Authentication and on-premises authentication virtual server.
- GUI: Use the GUI for the on-premises gateway virtual server. For details, see Control upgrade of Citrix Secure Access clients.

Sample CLI commands:

```
add rewrite action <rewrite_action_name> insert_http_header Plugin-Upgrade "\"epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:Never;vpn_mac:Always;vpn_linux:Always;\""

add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS(\"pluginlist.xml\")" <rewrite_action_name>

bind authentication vserver <Authentication_Vserver_Name> -policy <rewrite_action_policy> -priority 10 -type RESPONSE
```

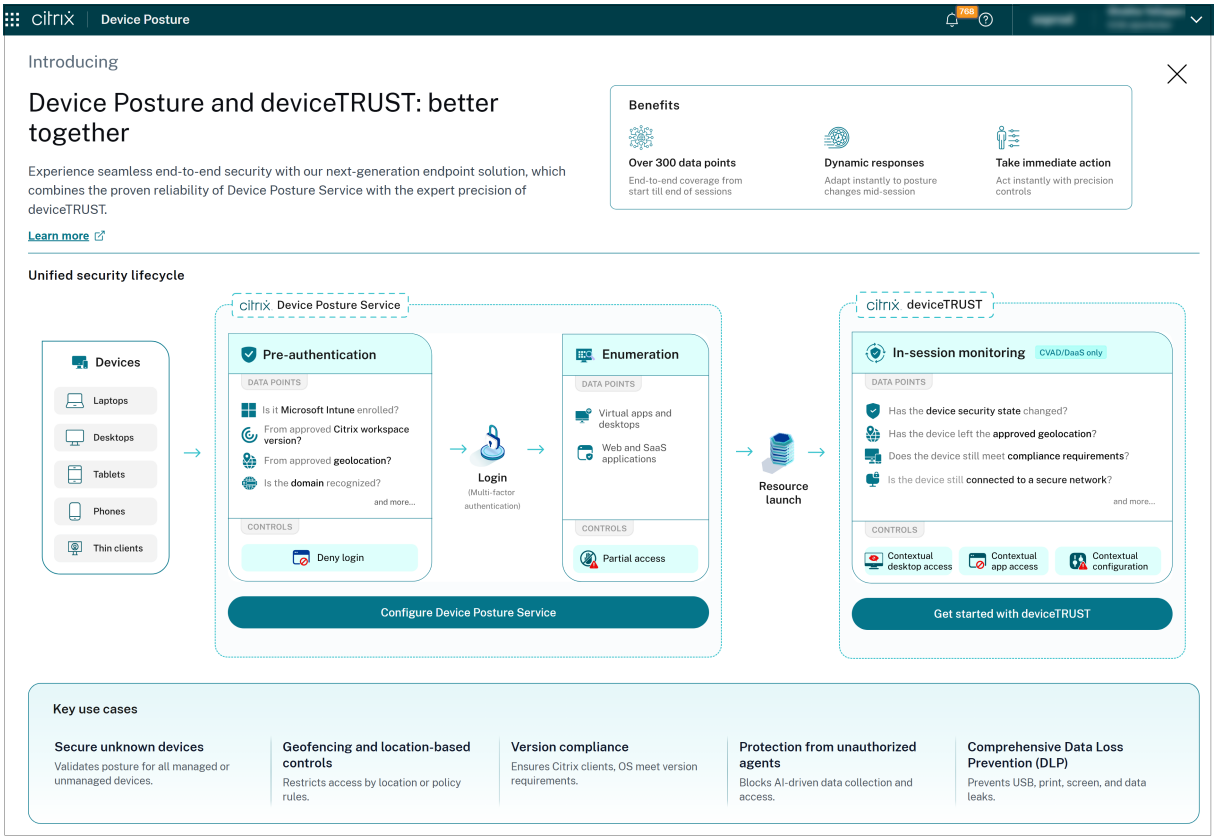
Device Posture service and deviceTRUST - Better together

February 6, 2026

Securing access to enterprise applications and data now requires more than static policies. They require real-time, context-aware controls that continuously adapt throughout the user journey. The Citrix Device Posture service and deviceTRUST integration delivers comprehensive contextual access coverage across every phase; pre-authentication, enumeration, and in-session.

To configure Device Posture service and deviceTRUST for your specific environment, see the following topics:

- Configure contextual access (smart access) using device posture
- deviceTRUST Quick setup



How Device Posture service and deviceTRUST work together

Pre-authentication: Establishing trust before login

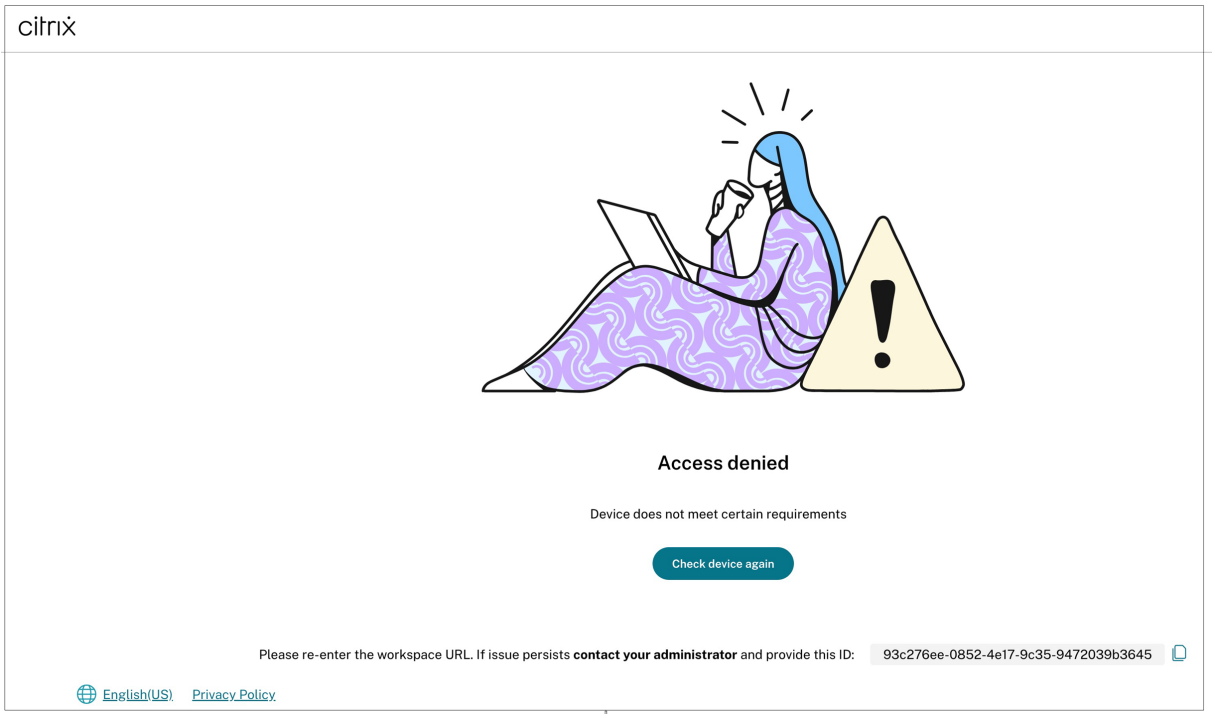
The Device Posture service acts as the first line of defense, performing endpoint hygiene checks before a user is allowed to authenticate. Administrators can define policies that inspect device properties such as;

- Citrix Workspace app version
- OS version
- Security software status (Antivirus)
- Corporate enrollment via MDM solutions
- Device certificate
- Compliance with corporate standards

If a device fails to meet these requirements, access is blocked before authentication even begins.

Example:

When a user attempts to log in from a personal device, the Device Posture service verifies that the antivirus software is installed and running. If the device fails to meet the policy requirements created by the administrator, login is denied, ensuring only trusted devices can access sensitive resources.

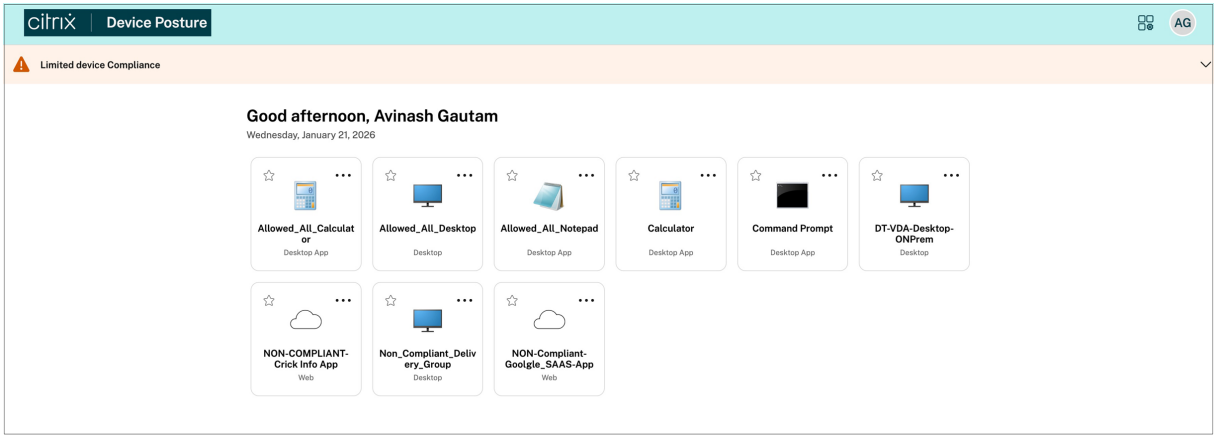


Enumeration: Contextual access to applications

During the enumeration phase, the Device Posture service continues to enforce policies by evaluating device posture when users browse or enumerate applications in the store. Administrators can restrict which applications or desktops are visible or accessible based on context.

Example:

If a device is compliant, the user sees all entitled applications. If not, certain apps might be hidden or access might be limited, such as disabling clipboard or file transfer features.



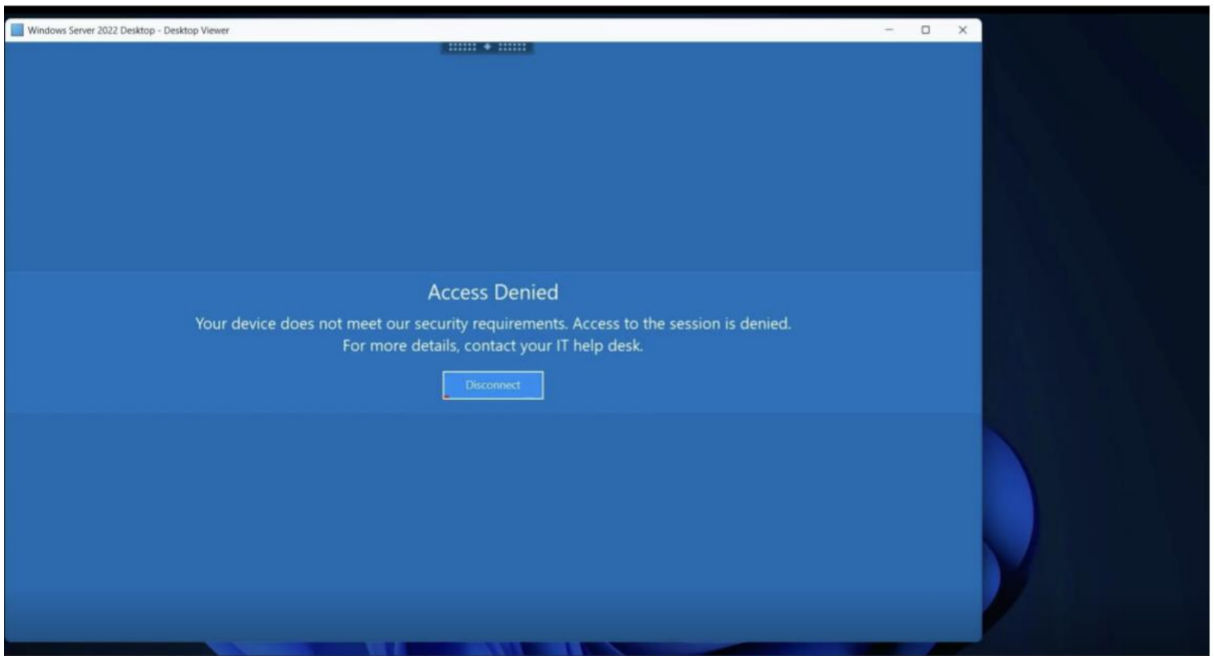
In-Session: Continuous contextual access evaluation

Once a session is established, deviceTRUST takes over to provide continuous, in-session contextual access controls. Unlike traditional solutions that only check device posture at login, deviceTRUST monitors device context throughout the session, enabling dynamic enforcement of policies as conditions at the endpoint change.

Granular Controls: Administrators can configure actions such as session disconnects, pop-up notifications, or auditing when device context changes (for example, plugging in an unauthorized USB stick, disabling firewall, connecting to an unencrypted Wi-Fi, changing network location).

Example:

A user starts a session from a compliant device. During the session, deviceTRUST detects a change —for example, the device connects to an unsecured network or a prohibited peripheral is attached. The system can automatically restrict access, disconnect the session, or notify the user of required actions, maintaining continuous compliance.



Use case of the Device Posture service and deviceTRUST integration

The Device Posture service and deviceTRUST integration support a range of critical use cases, such as;

- Version compliance (restricting access to approved operating system and application versions)
- Geofencing (controlling access based on device location)
- Continuous monitoring of security states such;

- Antivirus status
- Protection against unauthorized software agents - Comprehensive data loss prevention (DLP) through dynamic restriction of clipboard, file transfer, and printing
- Securing unknown or unmanaged devices in BYOD scenarios.

These capabilities empower administrators to maintain continuous compliance, reduce risk, and protect enterprise data in dynamic, hybrid environments.

Version compliance

Ensure that only devices running approved versions of operating systems and Citrix Workspace app (CWA) can access resources. This prevents outdated or vulnerable endpoints from connecting, reducing risk from unpatched systems.

For detailed policy configuration steps, see this tutorial.

Geofencing

Restrict access to applications and desktops based on the physical location of the device. For example, allow access only from approved countries or corporate offices, and revoke access if a device crosses a border.

For detailed policy configuration steps, see this tutorial.

Monitoring security state of device

Antivirus checks: Checking for antivirus is a foundational security measure that helps ensure only trusted, protected devices can access enterprise resources, both at the point of log in and throughout the user session. This is especially important in dynamic, hybrid, or BYOD environments where device compliance cannot be assumed.

For detailed policy configuration steps, see this tutorial.

Data Governance

September 6, 2025

This topic provides information regarding the collection, storage, and retention of logs by the Device Posture service. Any capitalized terms not defined in the Definitions sections carry the meaning specified in the Citrix End User Services Agreement.

Data residency

The Citrix Device Posture customer content data resides in the AWS and Azure Cloud Services. They are replicated to the following regions for availability and redundancy:

- AWS
  - East US
  - West India
  - Europe (Frankfurt)
- Azure
  - West US
  - West Europe
  - Asia (Singapore)
  - South Central US

The following are the different destinations for the service configuration, runtime logs and events.

- Splunk service for system monitoring and debug logs, in the US location only.
- Citrix Analytics Service for the diagnostics and user access logs, see Citrix Analytics Service Data Governance for more information.
- Citrix Cloud System Logs service for admin audit logs. For details, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

Data collection

Citrix Device Posture service allows the customer administrators to configure the service through the Device Posture UI. The following customer content is collected based on the device posture policy configuration and the platform:

- Operating system version
- Citrix Workspace™ app version
- MAC addresses
- Running processes
- Device certificate
- Registry details
- Windows installation update details
- Last Windows update details
- File system –file names, file hashes and modified time
- Domain name

For runtime logs collected by the service components, the key information consists of the following:

- Customer/tenant ID
- Device ID (Citrix generated unique identifier)
- Device posture scan output
- Public IP address of the endpoint device

Data transmission

Citrix Device Posture service sends logs to destinations protected by transport layer security.

Data control

Citrix Device Posture service does not currently provide options for the customers to turn off sending logs or prevent customer content from being replicated globally.

Data retention

Based on the Citrix Cloud™ data retention policy, the customer configuration data are purged from the service 90 days after subscription has expired.

The log destinations maintain their service-specific data retention policy.

- For details, see Data Governance for the retention policy for the Analytics logs.
- The Splunk logs are archived and eventually removed after 90 days.

Data export

There are different data export options for different types of logs.

- The admin audit logs are accessible from the Citrix Cloud System Log console.
- The Device posture service diagnostics logs can be exported from the Citrix Analytics Service or Secure Private Access service dashboard as a CSV file.

Definitions

- Customer Content means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform Services.
- Log means a record of events related to the services, including records that measure performance, stability, usage, security, and support.
- Services mean that the Citrix Cloud services outlined earlier for the purposes of Citrix Analytics.