Device Posture

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

Contents

Device Posture overview 2

What's new 8

Endpoint analysis release notes 17

Configure Device Posture policies 23

Configure Device Posture global settings 30

Device Posture service integration with Chrome Enterprise device trust connector 41

Third-party integration with Device Posture service 49

Third-party integration failure notifications 61

End user flow 63

Device Posture service in test mode 67

Manage Citrix Secure Access Endpoint Analysis (EPA) client versions by setting minimum supported versions 70

Multiple cloud store support 73

Export of Device Posture user events into SIEM systems 77

Troubleshoot Device Posture issues using DaaS Monitor 77

Device Posture logs and events 78

Diagnose Device Posture service transactions 82

Citrix Secure Access Endpoint Analysis (EPA) client distribution and upgrade 86

Device Posture service and deviceTRUST - Better together 93

Data Governance 98

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

Device Posture overview

September 29, 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 Licensing.
- Supported platforms:
  - Windows (10 and 11)
  - macOS 26 Tahoe
  - macOS 15 Sequoia
  - macOS 14 Sonoma
  - iOS
  - Linux (Ubuntu 22.04/24.04 and eLux 7)

  > **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.

- 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.

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

> **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

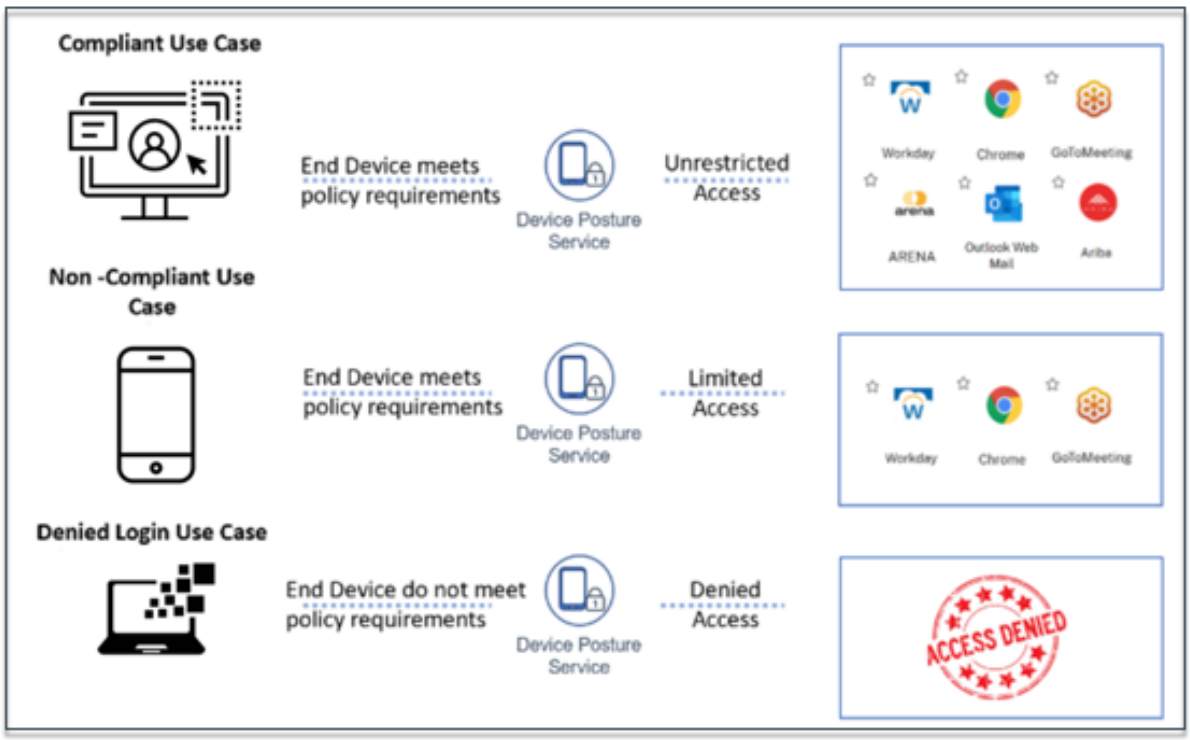
The admins can create device posture policies to check the posture of endpoint devices and determine whether an endpoint device is allowed or denied login. The devices, which are allowed to log in are further classified as compliant or non-compliant. Users can log in from a browser or the Citrix Workspace™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

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

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

- **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 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,

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

> 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.
> - Linux users see the Device Posture scan in the flow, but the posture is evaluated only when a Linux scan is configured in admin policies. If no Linux rules are configured, posture evaluation falls back to the default outcome.
> - 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)	-	-	-

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

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.

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

- **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.

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

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

September 29, 2026

This topic captures details about the enhancements and new features in the Device Posture service.

09 September 2026

- **General availability of multiple cloud store support**

  The multiple cloud store support is now generally available. For more information, see Multiple cloud store support.

22 June 2026

- **Microsoft Entra ID integration with Device Posture service**

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

Device Posture integration with Microsoft Entra ID is now generally available for the Windows platform.

For details, see Microsoft Entra ID integration with Device Posture service.

15 June 2026

- **Device Posture service integration with Chrome Enterprise device trust connector**

  The Device Posture service now integrates with the Chrome Enterprise device trust connector. With this integration, Citrix® administrators can share device posture results with Google Workspace, enabling Chrome to enforce context-aware access and Data Loss Prevention (DLP) policies based on the posture of managed devices. For details, see Device Posture service integration with Chrome Enterprise device trust connector.

05 June 2026

- **Endpoint Analysis (EPA) client version management through Device Posture service**

  Administrators can manage EPA client versions through the Device Posture service by maintaining a minimum supported EPA version. Administrators must set a minimum version that all users must comply with. Users with this minimum version or higher can perform Device Posture scans. For details, see EPA client version management through Device Posture service.

01 June 2026

- **General availability of Device Posture service for Linux**

  The Device Posture service is now generally available for the Linux platforms. Previously offered as a Technical Preview, it now supports full policy configuration and enforcement for endpoints running supported Linux distributions.

  With this release, the Device Posture service evaluates Linux endpoints for compliance, including managed or BYOD status and overall security posture, before allowing user to sign in. This strengthens a zero-trust access model.

  The integration provides the following benefits:

  - Comprehensive access enforcement: Dynamically grant, restrict, or deny access to Citrix DaaS (virtual apps and desktops) and Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps) based on the Linux endpoint scan results.
  - Streamlined security checks: Pre-authentication contextual scans on Linux endpoints now integrate seamlessly with existing policies for Windows, macOS, and iOS.

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

Administrators can configure Device Posture policies for Linux devices using the following supported scans:

- OS Version
- File (Exists, Last Modified Time, MD5)
- Process (Exists, MD5, SHA1)
- Mount Point

> **Note:**
>
> Linux users see the Device Posture scan in the flow, but the posture is evaluated only when a Linux scan is configured in admin policies. If no Linux rules are configured, posture evaluation falls back to the default outcome.

For details on configuring posture policies for endpoint devices, see Configure Device Posture policies.

09 April 2026

- **Availability of Windows Citrix Endpoint Analysis (EPA) client version 26.3.1.10**

  This update for the Citrix Endpoint Analysis (EPA) client introduces significant performance optimizations and critical bug fixes designed to improve scan reliability and policy handling across Windows environments.

  Availability: Citrix Downloads.

  Key enhancements and fixes:

  - Improved policy scalability: The EPA client is now optimized to handle complex enterprise environments, providing efficient data processing and improved stability.
  - Improved Windows Update scanning: Added an automatic UpdateSearcher fallback mechanism to ensure accurate patch detection.
  - User-Agent modernization: Replaced legacy IE7-based User-Agent strings with a modern, product-specific format to improve compatibility with current web gateways and security filters.

17 March 2026

- **Email notifications for third-party integration failures**

  Administrators now receive email notifications when third-party integration failures occur. These errors are also visible in the Secure Private Access and Device Posture service dashboards, enabling direct contact with third-party service support with relevant error details

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

and minimizing resolution time. For more information, see Third-party integration failure notifications.

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**

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

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.

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

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**

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

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**

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

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.

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

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]

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

Endpoint analysis release notes

September 28, 2026

The endpoint analysis (EPA) release note captures the enhancements, new features, fixed issues, and known issues in the EPA client for various platforms.

V26.07.20 for macOS (18 September 2026)

- **Continuous scanning support for macOS**

  Endpoint Analysis for Mac now supports continuous scanning. Previously, device posture on macOS was evaluated only when users connected, so changes after sign-in, such as disabling the firewall or stopping antivirus protection, were not detected until the next connection attempt. With continuous scanning, Endpoint Analysis continuously re-evaluates device posture throughout the session and reports its current state, enabling contextual access policies to respond to the device's live posture rather than a one-time snapshot. This feature aligns macOS with Windows' continuous scanning, strengthening conditional access for Mac users.

  > **Note:**
  >
  > - This feature is being rolled out in phases and will become available to customers progressively.
  > - No client-side configuration changes are required.

V26.7.1.15 for Windows (11 September 2026)

What's new

- **Native ARM64 support for Endpoint Analysis on Windows**

  Endpoint Analysis now supports native installation on ARM64 Windows devices. The separate epasetup_ARM64.exe package is provided alongside the x64 client, eliminating the need to run the client through x64 emulation.

  Deploy the package that matches the device architecture: epasetup.exe for x64 devices or epasetup_ARM64.exe for ARM64 devices. Native ARM64 support improves performance on ARM64 devices.

  Limitations:

  - Keylogger detection is not supported on ARM64.

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

- The ARM64 client requires a clean installation, so uninstall any existing Endpoint Analysis client before installing it.

[DPS-2775]

- **Keylogger detection in Endpoint Analysis (Preview)**

  Endpoint Analysis can now detect keylogging software running on an endpoint and report the detection details in Monitor for administrator visibility.

  This feature helps administrators identify keylogging risks on managed endpoints. It is for visibility only and does not affect posture evaluation or access decisions. Enabling it cannot block users from accessing resources.

  > **Note:**
  >
  > - This feature is currently in preview and is enabled per customer upon request.
  > - This feature is not supported on ARM64 devices.

  [DPS-2737]

- **Bundled scan engine for Endpoint Analysis**

  The scan engine and its libraries are now included in the Endpoint Analysis client package and are installed together with the client. Packaging the client and scan engine as a single release ensures version alignment and removes the dependency on downloading scan engine components at runtime. The client application upgrade process remains unchanged.

  [DPS-4580]

- **Endpoint Analysis is now 64-bit only**

  Endpoint Analysis is now available only as a 64-bit client. 32-bit (Win32/x86) binaries and installers are no longer produced or supported, and the installer does not run on 32-bit versions of Windows.

  - Update any deployment scripts or software-distribution packages that reference a 32-bit Endpoint Analysis package.
  - Both supported 64-bit architectures are available: `epasetup.exe` for x64 devices and `epasetup_ARM64.exe` for ARM64 devices.

  [DPS-2707]

- **Endpoint Analysis uses dedicated installation paths**

  Endpoint Analysis now installs in a product-specific folder and registry location instead of using the shared Secure Access Client location.

  The installation paths are:

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

- Per-machine: C:\Program Files\Citrix\Secure Access Endpoint Analysis
- Per-user: %LocalAppData%\Citrix\Secure Access Endpoint Analysis
- Product registry key: HKLM\SOFTWARE\Citrix\Secure Access Endpoint Analysis

[DPS-5131]

- **Endpoint Analysis retention during uninstallation**

  Uninstalling a Citrix product no longer removes Endpoint Analysis when another installed Citrix product still depends on it. This applies when Endpoint Analysis is shared by multiple Citrix products on the same device, such as Citrix Workspace app, Citrix Enterprise Browser, and Citrix Secure Access. Previously, uninstalling one product can remove Endpoint Analysis and leave the other products without a posture client.

  When an interactive uninstall would remove a still-needed client, the maintenance page lists the dependent applications that are keeping Endpoint Analysis installed.

  > **Note:**
  >
  > - For scripted removal, a silent uninstall that correctly retains Endpoint Analysis returns exit code `1000`. Configure `1000` as a success code in your deployment system.
  > - To remove Endpoint Analysis despite the dependency, rerun the uninstall command from an elevated prompt with `/SkipConsumerCheck`.

  [DPS-5095]

- **Endpoint Analysis supports unattended deployment**

  Endpoint Analysis setup now supports unattended installation and uninstallation through software-distribution tools such as Configuration Manager and Intune. Use `/quiet` for silent operations and `/log <path>` to specify the log location, on both installation and uninstallation.

  > **Note:**
  >
  > - These options are intended for centrally managed deployments. If the setup cannot write to the specified log path, it stops with exit code `1622` instead of silently writing the log elsewhere.
  > - During uninstallation, use the elevated-only `/SkipConsumerCheck` option to remove Endpoint Analysis even when another Citrix product depends on it.
  > - Configure exit code `1000` as a success code in your deployment tool. This code indicates that Endpoint Analysis was intentionally retained because another Citrix product still requires it.

  [DPS-5493]

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

- **Modernized Endpoint Analysis installer**

  The Endpoint Analysis installer interface is now enhanced for installation, repair, and maintenance. The enhanced interface appears when users interactively install, repair, or remove the client, such as from the downloads page or the maintenance page.

  > **Note:**
  >
  > Silent and scripted deployments remain supported. As MSI-based deployment is no longer supported, use the following epasetup.exe command-line switches as needed.
  >
  > - /quiet, /silent, /q - Silent installation with no user interface.
  > - /passive - Displays progress only, with no interactive prompts.
  > - /uninstall - Uninstalls the product.
  > - /repair - Repairs an existing installation.
  > - /log "<file>"- Writes the installer log to the specified path.
  > - /norestart - Suppresses automatic restart after installation or uninstallation.
  > - /?, /h, /help - Displays installer help information.

  [DPS-2645]

Fixed issues

- Windows Update posture was reported from the wrong source: hot patched machines showed the age of a superseded baseline, patch ages were based on unrelated installations, and unmeasurable values were reported instead of being identified as unavailable.

  [DPS-5465]

- Posture signals from the third-party scanning engine are intermittently unavailable while the Windows Update service is starting.

  [DPS-5379]

- A scan-engine failure is reported as if no security product was installed on the device, making an engine fault indistinguishable from a genuinely unprotected device resulting in the same access denial.

  [DPS-5121]

- Signature verification now requires the signer to chain to a root certificate in the machine trust store. Roots trusted only in a per-user store are no longer accepted. Administrators using a custom trusted signing certificate must deploy it machine-wide.

  [DPS-2038]

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

- The `devicePostureNativeBridge.exe` process can clear config.js, erasing saved connections. As a result, saved connections disappear from the client.

  [DPS-4701]

- Repeated scans can cause memory and handle leaks.

  [DPS-4552]

- Users cannot retry an uninstall or remove a damaged installation.

  With this fix, the maintenance page now offers the same deep-clean option as the silent path, allowing recovery when an uninstall fails on a damaged installation.

  [DPS-3933]

- Uninstalling Endpoint Analysis leaves behind an orphaned service registry key.

  [DPS-5226]

- The browser Endpoint Analysis flow fails when global server load balancing, HSTS, httpOnly cookies, and content security policy are all enabled on NetScaler Gateway.

  [DPS-3684]

- Users might remain indefinitely on the "Checking your device…"screen because large service responses can be truncated or over-read, preventing the device check from completing.

  [DPSHELP-118]

- The browser native-messaging host previously accepted connections from a process other than the verified browser because it checked only one end of the connection. With this fix, it now verifies that both ends belong to the same browser process.

  [CTXBR-14824]

- The clipboard handshake with the broker fails when the receiver process is closed.

  [CTXBR-14570]

V26.6.1.4 for Windows (24 August 2026)

The following sections provide more information about the V26.6.1.4 for Windows release.

What's new

- **Updated OPSWAT libraries that resolve memory leaks during device posture scans**

  The EPA client now includes updated OPSWAT (OESIS) libraries that resolve memory leaks during third-party product detection. Devices that perform frequent or continuous device posture

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

scans no longer experience gradual memory buildup in the scanning process. The update also expands detection support for third-party security products, including ALYac, WatchGuard Endpoint Security Prime, and Trellix EDRF.

Fixed issues

- Launching Citrix Secure Access from a browser might fail to load the home page when Full tunnel is selected on the Client Choices page. This issue occurs because EPA sends an incorrectly terminated HTTP header that is rejected by NetScaler Gateway.

  [DPS-5100]

- The device posture scan might not complete, leaving the client stuck on the "Checking your device…"message. This issue occurs when the scan configuration returned by the Device Posture service exceeds the client's capacity, such as when an administrator enables a registry scan policy.

  [DPS-4639]

- Users might be denied access to resources during each scan cycle. This issue occurs when the local Device Posture admin service cannot consistently resolve the signed-in user while saving and reading context during periodic scans.

V26.5.1.7 for Windows (08 Jul 2026)

The following sections provide more information about the V26.5.1.7 for Windows release.

Fixed issues

- On some devices, the EPA client incorrectly reports the Windows version. For example, a Windows 11 device was reported as an older Windows version, causing OS-based scan checks to evaluate incorrectly. This issue affects the EPA v1 (classic, on-premises) scan flow on certain Windows 10 and Windows 11 devices.

  [DPS-3919]

- In admin mode deployments, device certificate posture checks might fail because the EPA admin service does not automatically select a device certificate during evaluation. On affected setups, this causes periodic (continuous) device-certificate checks to fail repeatedly.

  [DPSHELP-154]

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

- For certain security products, such as CrowdStrike Falcon and OPSWAT-based products, scans do not correctly apply the Ignore Internet Check setting. As a result, checks such as virus-definition last-update time might fail even when the product is healthy.

  This issue occurs in OPSWAT-based antivirus and definition scans for affected products.

  [DPSHELP-153]

- Users might experience device posture context read failures. For example, a browser extension might report that it cannot fetch device posture context because the stored EPA context file is not decrypted and read back reliably. This issue occurs when the Device Posture service writes and later re-reads encrypted posture context and periodic scan files.

  [DPSHELP-144]

V26.03.31 for macOS (14 May 2026)

The following sections provide more information about the V26.03.31 for macOS release.

What's new

- **Deprecation of independent library update**

  Starting with this release, runtime-dependent library updates are no longer supported. All future updates to these components will be delivered exclusively through new versions of the CitrixEndpointAnalysis application.

- **Static library integration with EPA appliaction**

  The core libraries required for system scanning are now bundled directly with the CitrixEndpointAnalysis application for both cloud and on-premises deployments.

  This integration provides the following benefits:

  - The integrated libraries now subjected to rigorous signature verification during application launch.
  - By bundling these assets, the application no longer needs to download and extract libraries at runtime, resulting in faster initialization and more reliable startup.

Configure Device Posture policies

September 29, 2026

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

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 that the service identifies the exact certificate for a specific policy, you must explicitly enable the **Check Thumbprint** option. For details, see Configure device certifi-

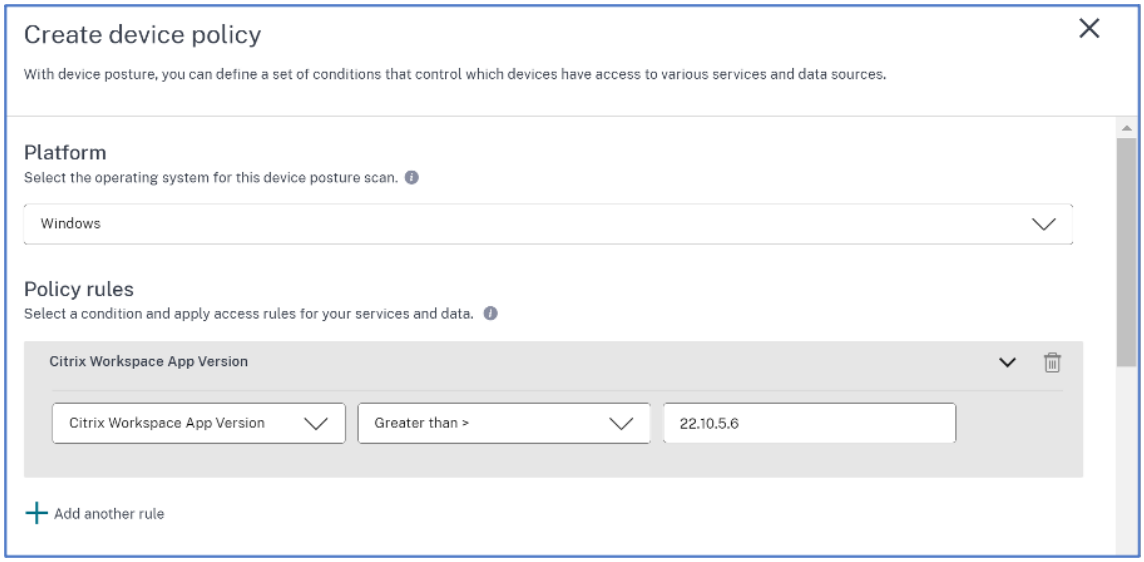
© 1997–2026 Citrix Systems, Inc. All rights reserved.

cate 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.

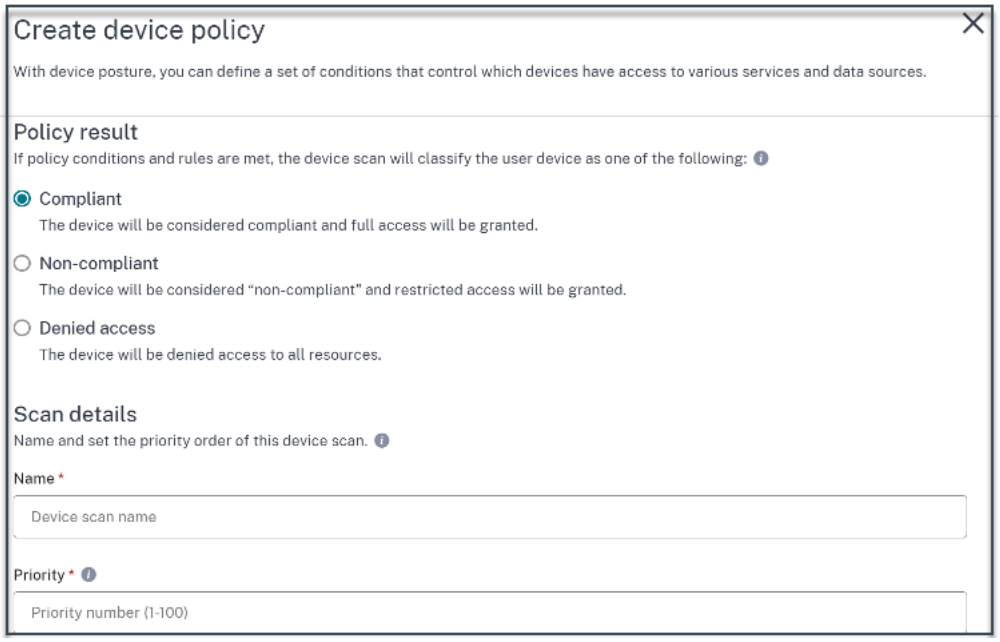
- When creating a policy rule for network location check, you can add a network location directly from the Device Posture service console. However, to modify the network location, you must use the Network Location configuration on Citrix Cloud.

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**.

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



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.
- Linux users see the Device Posture scan in the flow, but the posture is evaluated only when a Linux scan is configured in admin policies. If no Linux rules are configured, posture evaluation falls back to the default outcome.

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

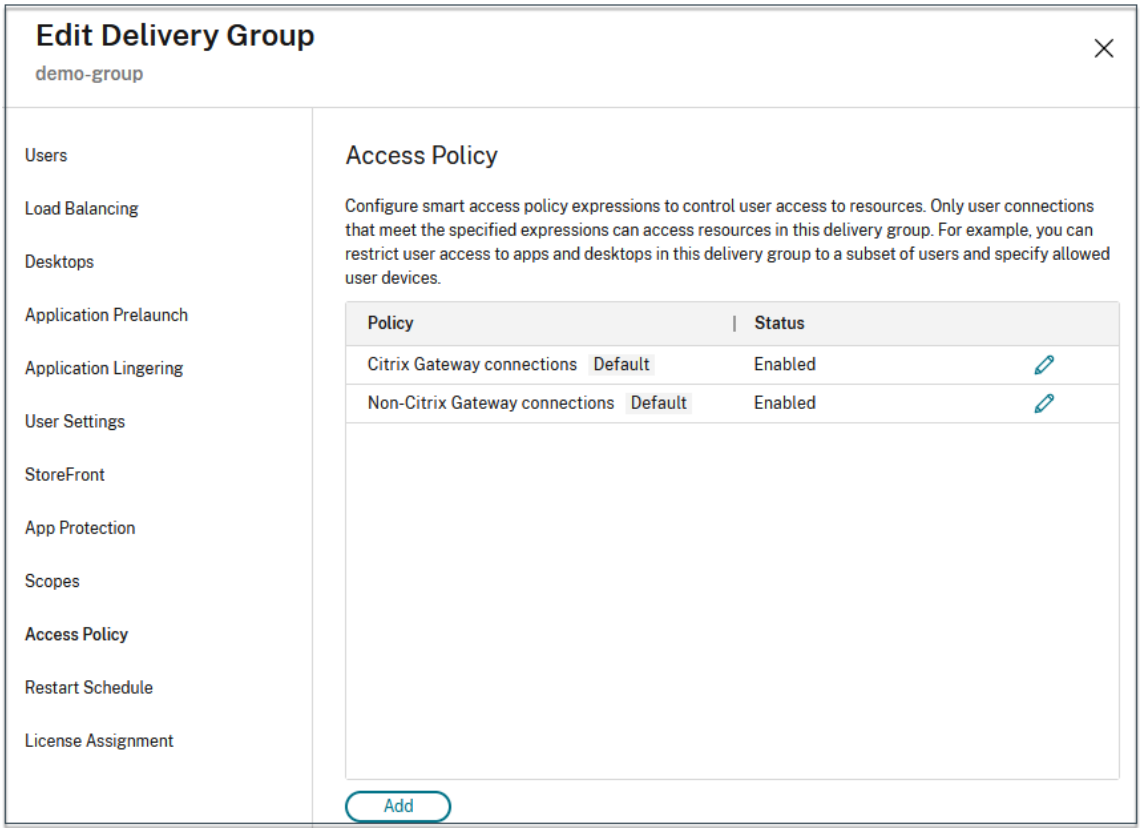
To restrict access to the DaaS resources, you can specify the delivery groups on which access restrictions must be enforced and configure the access control restrictions using the Device Posture tags.

Prerequisites:

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

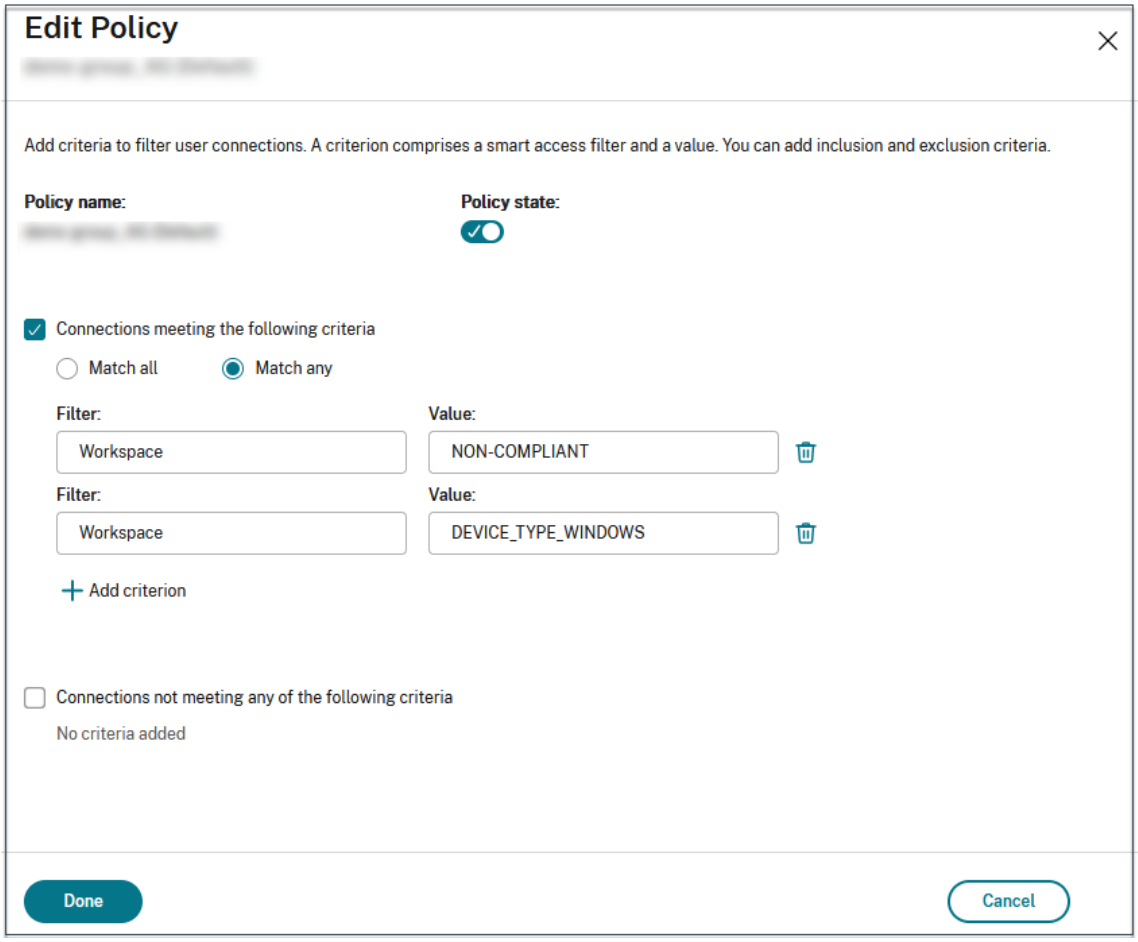
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

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



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.

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

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.

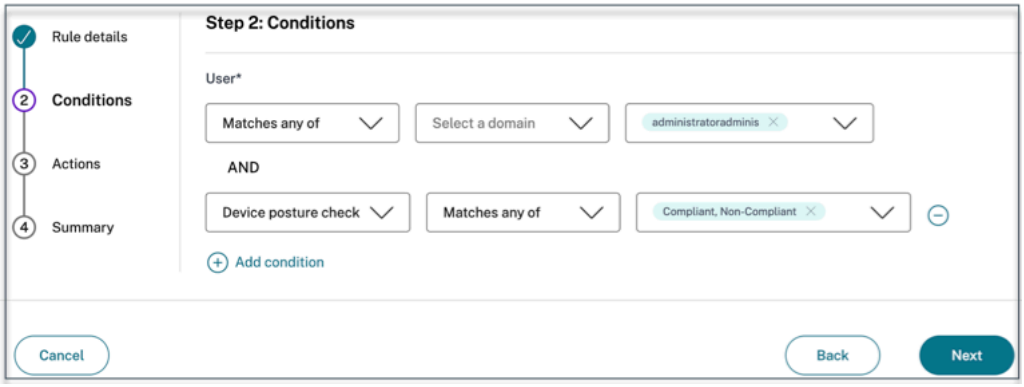
12. Click **Next**.
13. Select the actions that must be applied based on the condition evaluation, and then click **Next**.

    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.

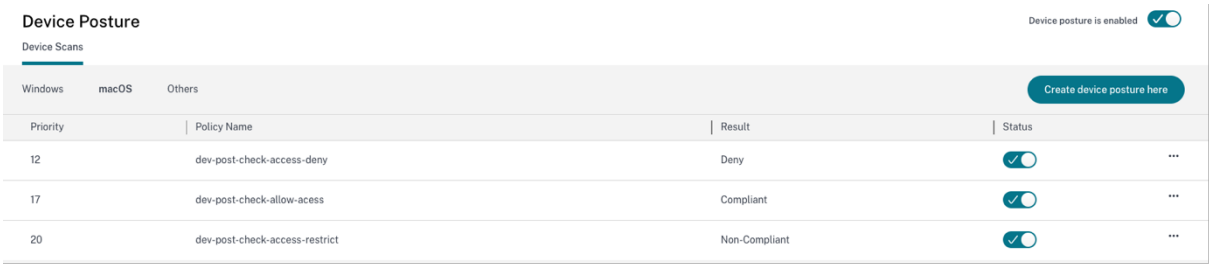
> **Note:**
>
> Any Secure Private Access application, which isn't tagged as compliant or non-compliant in the access policy is treated as the default application and is accessible on all the endpoints regardless of device posture.

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



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

September 11, 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
- Configure the list of allowed domains

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

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:

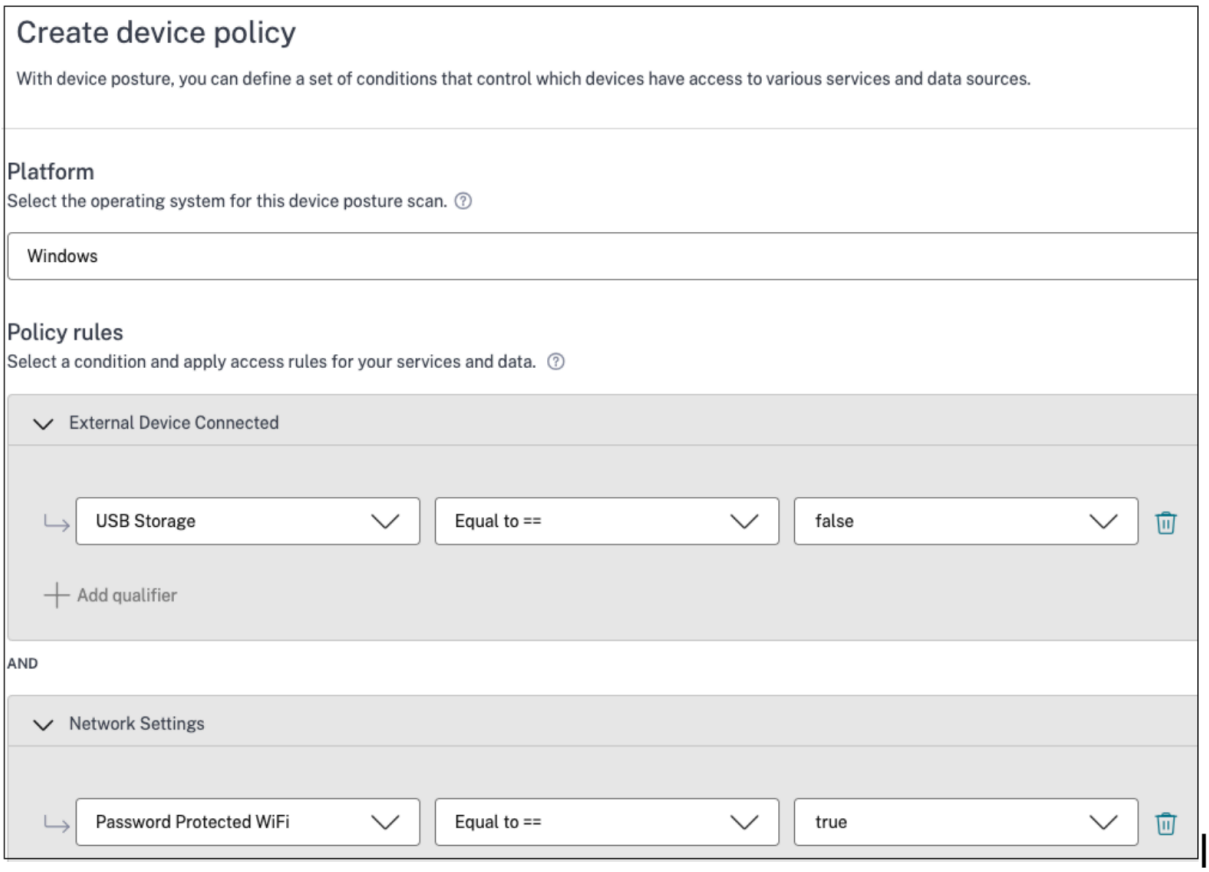
- The **External Device Connected** scan is configured, and an external USB storage device is inserted or removed.
- The **Network Settings** scan is configured, and a switch between an open network and a protected network is detected.
- The **Windows Defender Firewall** scan is configured, and it's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

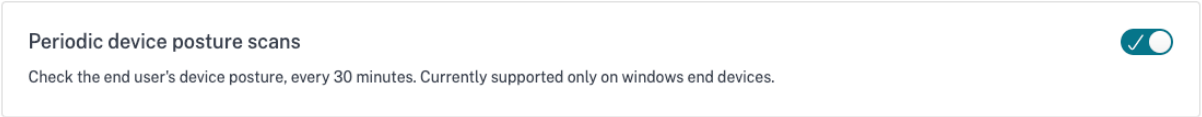
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**),

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

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.

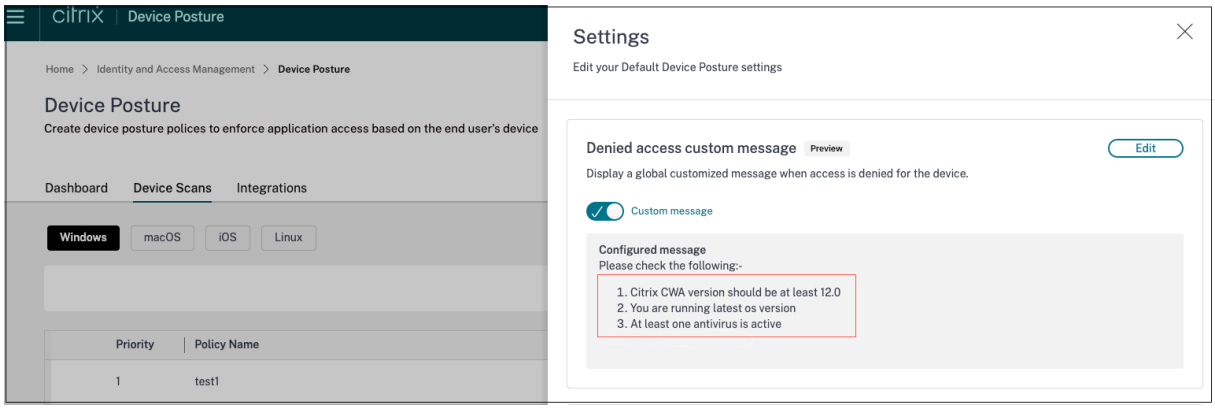
Perform the following steps to add customized messages:

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**.

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

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.

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

Skip device posture checks

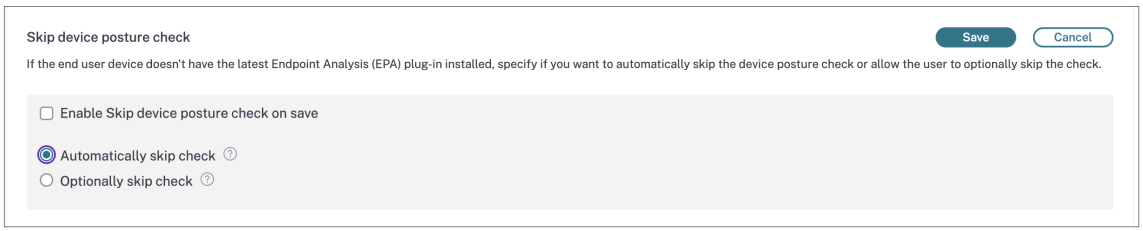
Admins can configure device posture checks to be skipped automatically or allow end users to skip them in the following scenarios:

- 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**.

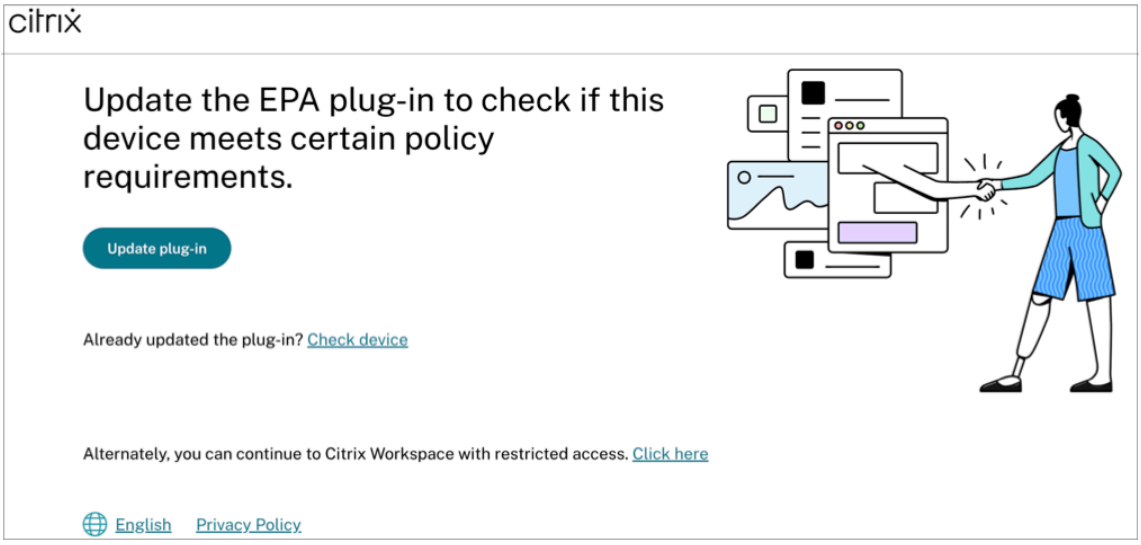


4. Select one of the following options:

   - **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.

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



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.

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

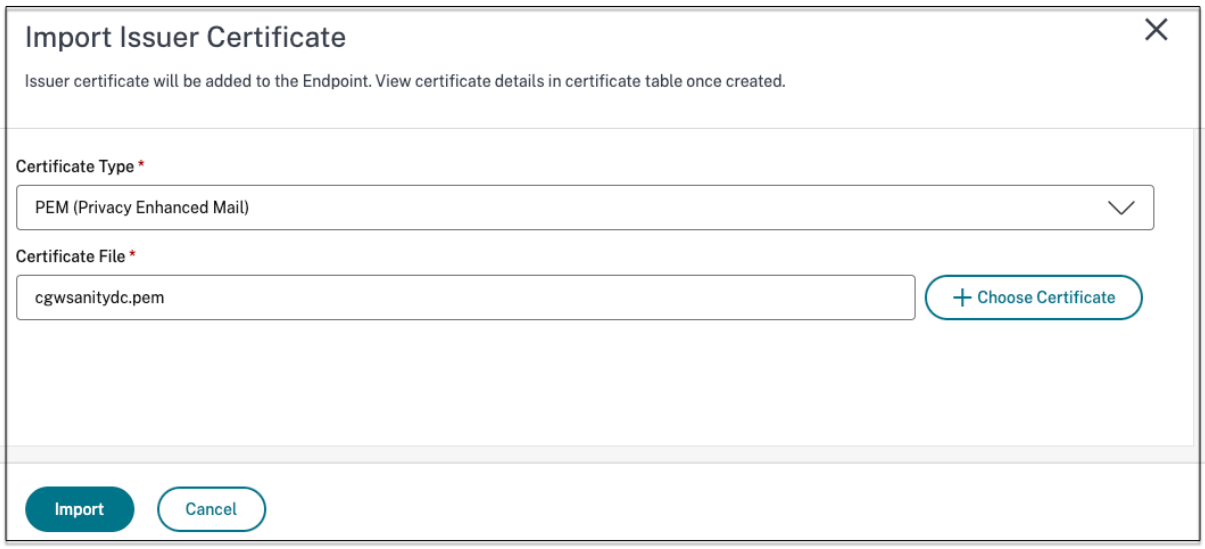
- To install the Endpoint Analysis client with administrative rights on Windows, run the command `epasetup.exe /quiet` from an elevated command prompt, in the folder where the client was downloaded. On ARM64 devices, run `epasetup_ARM64.exe /quiet` instead.
- The device certificate check with the Device 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**.

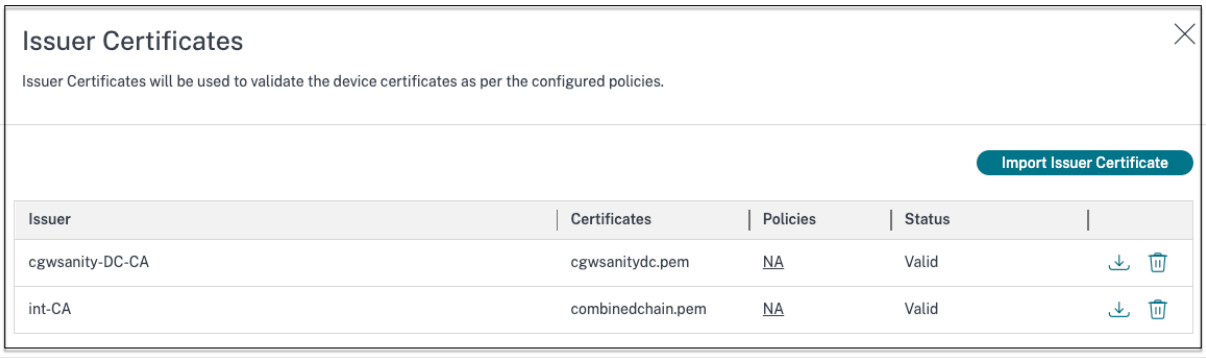


The selected certificate is listed in **Settings > Issuer Certificates**. You can import multiple certificates.

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

View imported certificates

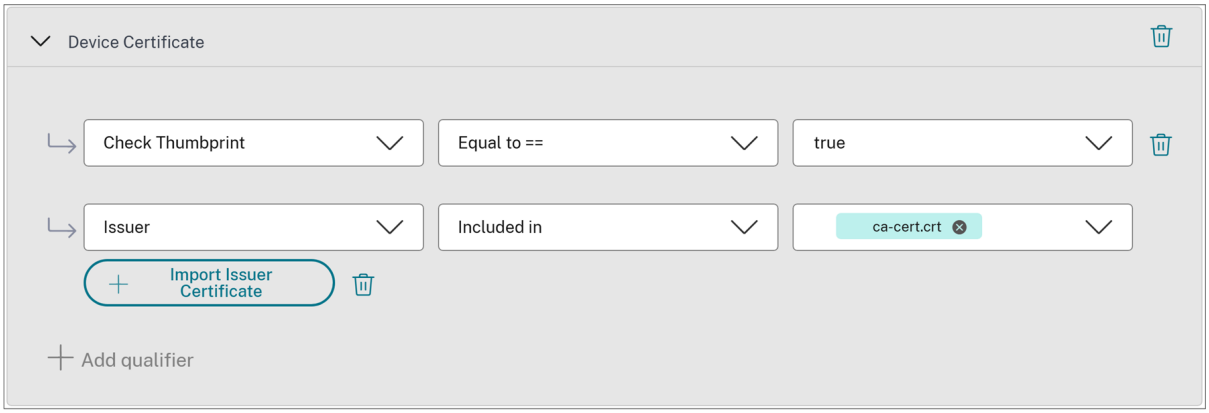
1. Click **Settings** on the Device Posture home page.
2. In **Issuer Certificates**, click **Manage**.
3. The Issuer Certificates page lists the imported issuer certificates.



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.

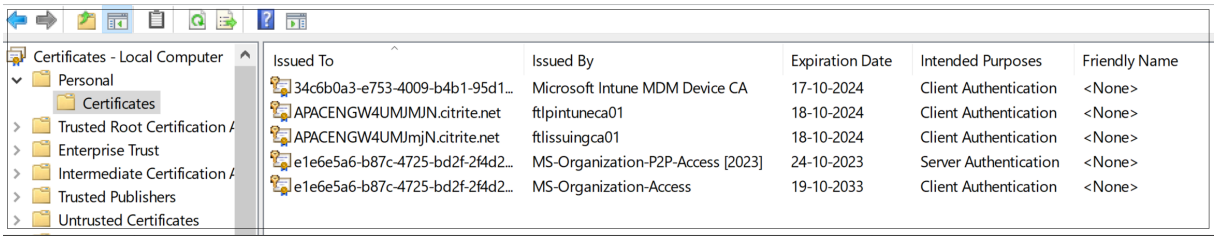


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

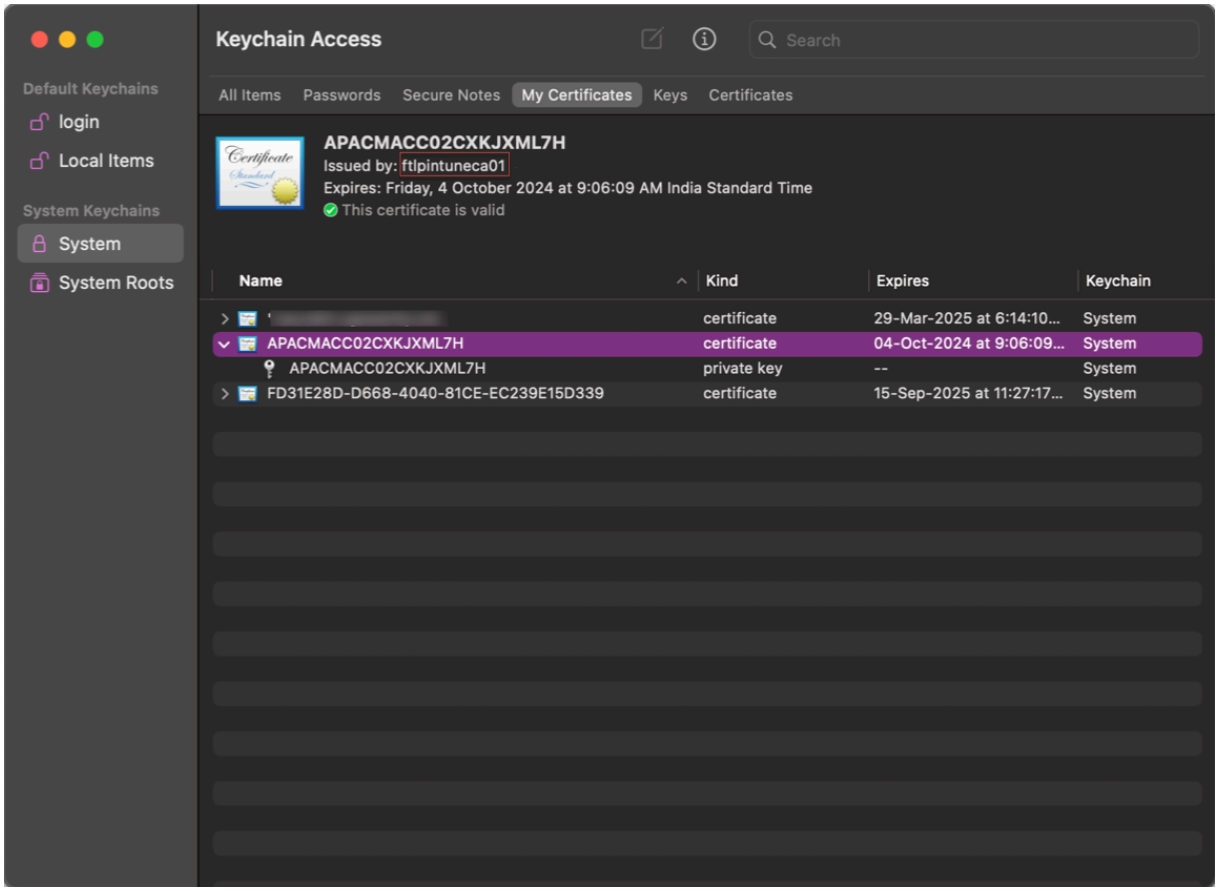


macOS:

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.

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



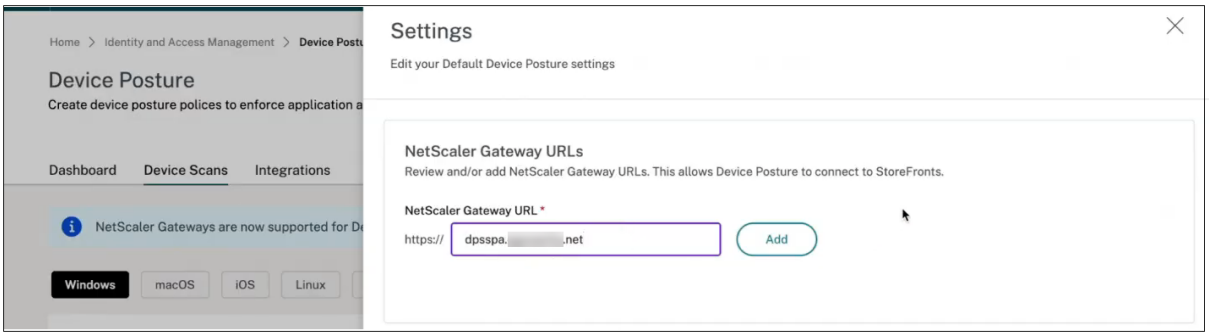
Configure the list of allowed domains

You can configure FQDNs of NetScaler Gateway virtual servers from which the Device Posture service scans can be initiated.

> **Note:**
>
> - This feature is only applicable for Secure Private Access deployments.
> - To get this feature enabled for your Secure Private Access deployment, contact Citrix Support.

1. Navigate to **Device Posture > Device Scans**, and then click **Settings**.
2. In **NetScaler Gateway URL**, enter the FQDN of the virtual server for which the Device Posture checks must be enabled. For example, `https://gw.example.net`.

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



For a sample use case of this feature, see Enable Device Posture for Secure Private Access hybrid solutions.

To configure device posture scans on NetScaler, see Device Posture checks on NetScaler Gateway.

Device Posture service integration with Chrome Enterprise device trust connector

September 29, 2026

The Device Posture service integrates with the Chrome Enterprise device trust connector. With this integration, Citrix® administrators can share device posture results with Google Workspace, enabling Chrome to enforce context-aware access and Data Loss Prevention (DLP) policies based on the posture of managed devices.

Posture signals shared by Citrix can be consumed by Chrome to make access decisions for:

- Managed Chrome browsers
- Managed Chrome profiles

For the list of signals that Chrome can receive from third-party connectors, see Google's Endpoint Verification documentation.

> **Note:**
>
> Integration with the Chrome Enterprise device trust connector is supported only when the Device Posture service is in global mode.

Supported platforms and deployments

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

Item	Support
Supported platforms	Windows with EPA client version 26.5.1.7 or later
Deployment	Secure Private Access service with Citrix Enterprise Premium

Prerequisites

- A Citrix Cloud tenant with Device Posture service entitlement and configured.
- A Google Workspace tenant with Chrome Enterprise Premium (CEP) license and super admin privileges to the Google Admin console.
- Chrome Enterprise Premium is deployed for the customer.
- The **Context-Aware Access** access level is set to ON in the Google Admin console. For details, see Apply recommended access levels.

Configuration

The Citrix Device Posture service integration with the Chrome Enterprise Device Trust Connector involves the following high-level steps:

1. Configure Chrome Enterprise Premium and Device Posture service
2. Integrate Citrix Device Posture service with Chrome device trust connector
3. Define context-aware rules for Citrix signals

Configure Chrome Enterprise Premium and Device Posture service

Before integrating with Chrome, ensure that the following configurations are complete:

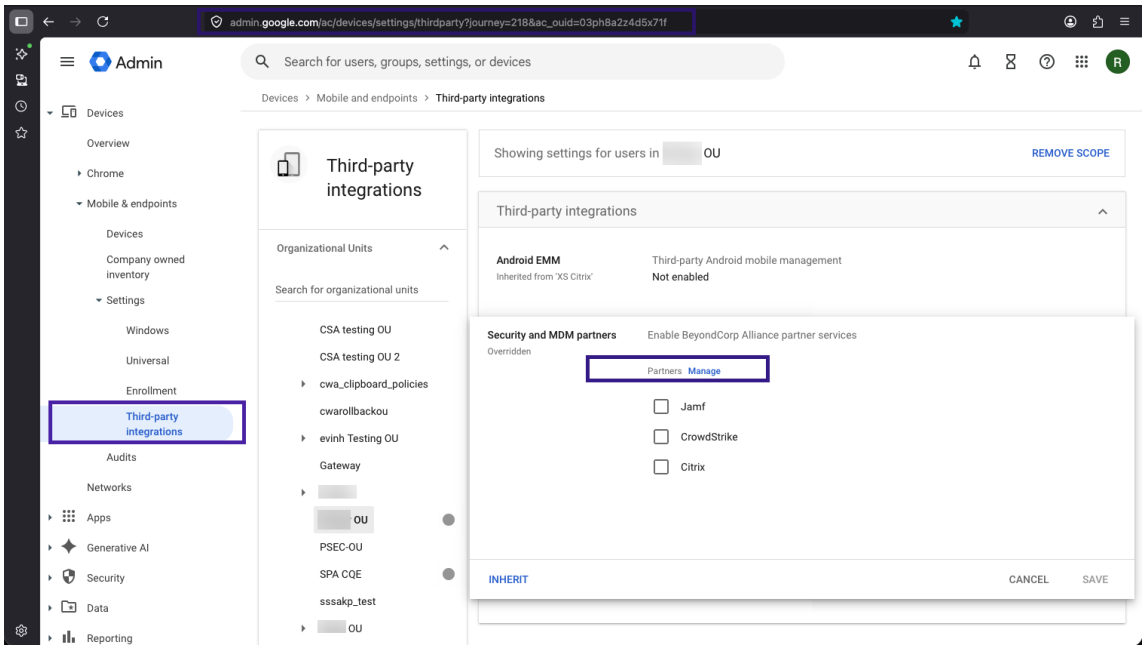
1. Deploy and configure Chrome Enterprise Premium (CEP) on managed Windows endpoints. For details, see Integration with Google Chrome Enterprise Premium.
2. Configure Device Posture service policies that produce the signals you intend to share with Chrome (for example, OS version, antivirus state, geo or authorized country, custom checks). For details, see Configure Device Posture policies.
3. Confirm that your Google Workspace tenant has Chrome Enterprise Premium (CEP) licensing, which is required to use the Device Trust Connector and context-aware access rules. For details, see Licenses, app versions, and extensions.

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

Integrate Citrix Device Posture service with Chrome device trust connector

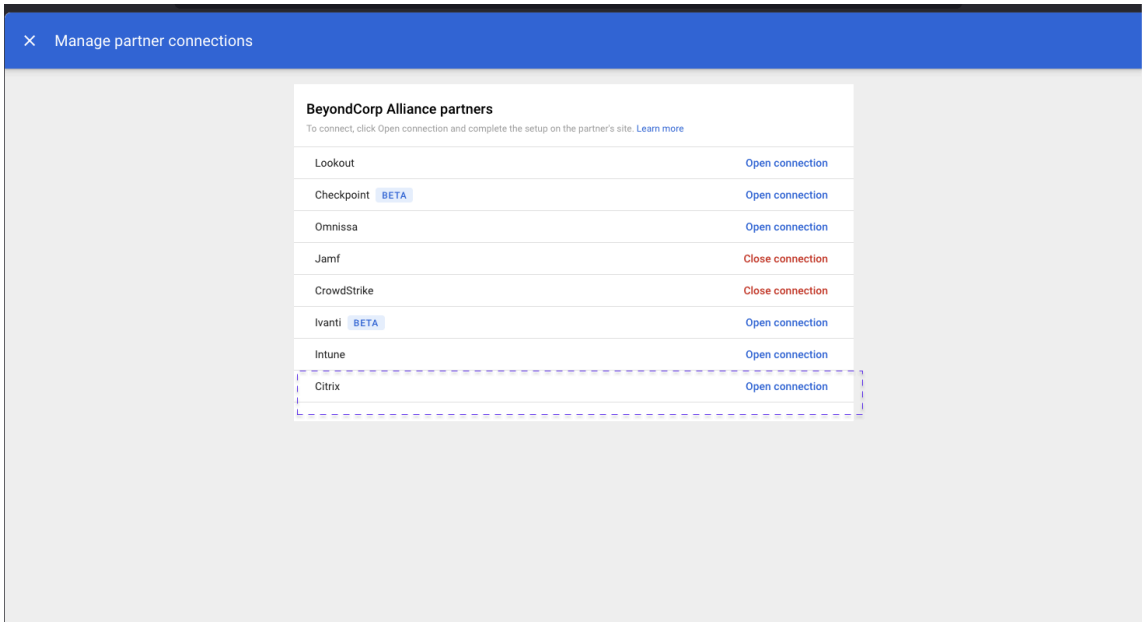
To integrate Citrix Device Posture service with the Chrome device trust connector, you must enable the third-party connector in the Google Admin console.

1. Sign in to the Google Admin console as a super admin.
2. Navigate to **Devices > Mobile and endpoints > Settings > Third-party integrations**.

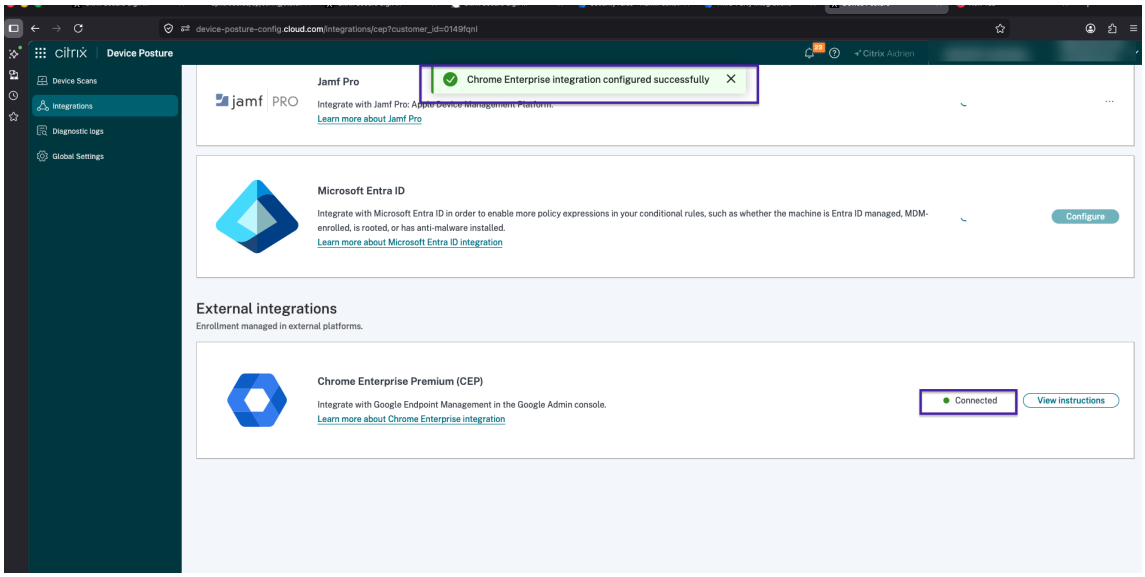


3. Locate **Citrix** in the partner list and click **Manage**.
4. Follow the on-screen prompts to authorize the connection between your Citrix Cloud tenant and Google Workspace.

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



When the handshake succeeds, the integration status for Citrix changes to **Connected**.



For details, see Setup third-party partner integrations.

Define context-aware rules for Citrix signals

Context-aware access and DLP rules in Google Workspace are written using the Common Expression Language (CEL). Citrix posture data is exposed under the `device.vendors["Citrix"].data[...]` namespace.

For details, see the following topics:

- Set up third-party partner integrations

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

- Combine DLP rules with context-aware access conditions

Citrix signal keys

The following keys are published by the Citrix Device Posture service to Chrome device trust connector:

Key	Description	Example values
OVERALL_OUTCOME	Aggregate posture result returned by the Device Posture service for the endpoint.	Compliant, Non-Compliant, Deny **Note:** Values are case-sensitive. Enter them exactly as listed above.
OVERALL_OUTCOME_CONTEXT_NAME	Name of the Device Posture service policy or context that drove the overall outcome.	AUTHORIZED_COUNTRY, AV_STATUS, OS_VERSION, Google-DTC-Demo-Deny, (custom policy name)
Citrix-DeviceId	The unique identifier of the endpoint registered with the Citrix Device Posture service.	6c813458-c27b-4299-87c6-55832a95ae7e
Citrix-TransactionId	The unique identifier of the posture evaluation transaction that produced the signal.	75b1e3f6-4224-484a-8c47-9a35c4e5eabd

> **Note:**
>
> - The exact context names depend on the policies you defined in the Device Posture service in step 1.
> - Citrix-DeviceId and Citrix-TransactionId are correlation identifiers. They are not intended for use in policy decisions. Use them when troubleshooting on the Citrix Device Posture dashboard to look up the exact scan that produced a given outcome.

Common Expression Language (CEL) examples for Citrix

Example 1 —Block access when Citrix reports Non-Compliant:

Deny access to a Google Workspace app when the Citrix overall outcome is Non-Compliant.

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

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

Use this expression in a context-aware access level with the action set to **Block**.

Example 2 —Block only when non-compliance is caused by an unauthorized country:

Combine the outcome with the context name to scope the rule to geographic violations.

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"&&
 device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "
AUTHORIZED_COUNTRY"
```

Example 3 —Allow access only when Citrix reports Compliant:

Grant access only when the Device Posture service explicitly returns a compliant result (fail-closed).

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant"
```

Example 4 —DLP: prevent file download on Non-Compliant devices:

In a DLP rule for Google Drive, attach the following condition to the Download / Print / Copy trigger to block exfiltration from a Non-Compliant endpoint:

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

Example 5 —Tiered policy with multiple Citrix contexts:

Block when posture failed for either antivirus or OS version, but allow other non-compliance reasons to be handled by a separate, less restrictive rule.

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"&&
 ( device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "
AV_STATUS"|| device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME
"] == "OS_VERSION")
```

Example 6 —Block an explicit Deny outcome from a named Device Posture service policy:

Match the exact Deny outcome produced by a specific Device Posture service policy (for example, the `Google-DTC-Demo-Deny` policy used during proof-of-concept):

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Deny"&& device.
vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "Google-DTC
-Demo-Deny"
```

Example 7 —Combine Citrix posture with Google native signals:

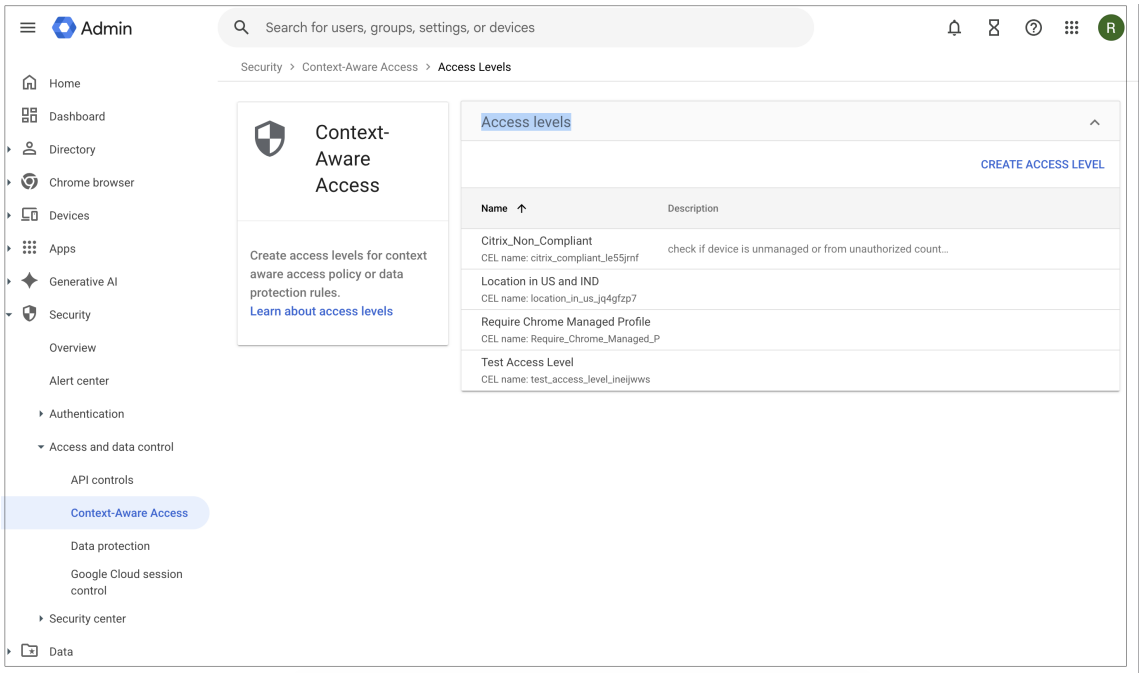
Citrix signals can be combined with built-in Chrome / Endpoint Verification attributes.

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant"&&
device.encryption_status == ENCRYPTED && device.os_version.major >=
10
```

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

To apply the rule

1. In the Google Admin console, go to **Security > Access and data control > Context-Aware Access (or Data protection for DLP)**.
2. Create an **Access level** (or **DLP rule**) and paste the CEL expression into the **Advanced / conditions** editor.



3. Assign the access level to the target Google Workspace app (Drive, Gmail, and so on) and the relevant organizational unit or group.
4. Save and roll out. Allow a few minutes for the propagation.

Validate the integration

1. From a managed Windows endpoint running CEP, deliberately fail a Device Posture service scan (for example, sign in from an unauthorized country or disable antivirus).
2. Attempt to access the protected Google Workspace app from the Chrome browser or profile on that endpoint.
3. Confirm that Chrome enforces the action defined by your CEL rule (block, warn, or allow).
4. Review the audit log under **Reporting > Audit and investigation > Access transparency / Rule log events** to confirm the Citrix signals were evaluated.

Troubleshooting

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

Symptom	Likely cause	Resolution
Integration status stays Not connected	OAuth/admin consent not completed	Re-run step 2 with a super-admin account
Rule never matches	CEL key name typo or policy not enabled in Device Posture service	Verify the key in the Admin console Rule log events. Confirm that the policy is active in the Device Posture service
Signals missing on endpoint	CEP not installed or user not signed in	Verify CEP deployment and Device Posture service enrollment on the endpoint
Unexpected Non-Compliant or Deny	A different Device Posture service policy is failing	Inspect OVERALL_OUTCOME_CONTEXT_NAME to identify the failing check

> **Note:**
>
> If you need to investigate a specific access decision, capture `Citrix-DeviceId` and `Citrix-TransactionId` from the Chrome / Workspace audit log and look them up on the Citrix Device Posture dashboard to view the full scan result, policy hits, and timestamps.

Using Citrix-DeviceId and Citrix-TransactionId for troubleshooting

When a Chrome access or DLP decision needs investigation:

1. Open **Google Admin console > Reporting > Audit and investigation > Rule log events (or the Access transparency log)** and locate the relevant event.
2. Copy the `Citrix-DeviceId` and `Citrix-TransactionId` values reported in the event payload.
3. Sign in to **Citrix Cloud > Device Posture > Dashboard**.
4. Search by Device ID to view the endpoint's enrollment, OS, and recent scan history.
5. Search by Transaction ID to view the exact scan instance —including which policies were evaluated, which signals were collected, and the resulting OVERALL_OUTCOME and OVERALL_OUTCOME_CONTEXT_NAME that were sent to Chrome.

This correlation lets you confirm whether an unexpected Chrome decision was caused by the Citrix posture result, by the CEL expression, or by the Workspace policy binding.

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

Limitations

A maximum of 10 Google resource IDs per host can be pushed from the Citrix Device Posture service to the Chrome device trust connector.

To push device posture signals to more than 10 Google resource IDs per host, contact Citrix Support to request an extension.

Third-party integration with Device Posture service

September 1, 2026

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.

- Microsoft Entra ID
- Jamf Pro
- Microsoft Intune
- CrowdStrike

Microsoft Entra ID integration with Device Posture service

With the Microsoft Entra ID integration, Citrix® supports a unified compliance workflow that works consistently across all Microsoft Entra ID-registered devices, regardless of which Mobile Device Management (MDM) solution is integrated with Microsoft Entra ID.

System requirements

- Supported platforms: Windows
- Supported EPA client version for Windows: 26.3.1.10 or later

Microsoft Entra ID API permissions

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

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

API name	Claim value	Permission name	Type
Microsoft Graph	Devices.Read.All	Read all devices	Application
Microsoft Graph	User.Read	Sign in and read the user profile	Delegated

> **Note:**
>
> - Only Privileged Role Administrator and Global Administrator can grant application permissions.
> - While the Device Posture service only requires Application Permissions to fetch Entra ID device details, the initial admin grant flow is an interactive process performed by an individual.
> - The `User.Read (Delegated)` permission included by default in Microsoft Entra ID verifies the administrator's identity during the grant flow. This ensures only authorized roles (Global Administrator or Privileged Role Administrator) grant the application-level access needed for the Device Posture service.

Configure Entra ID integration

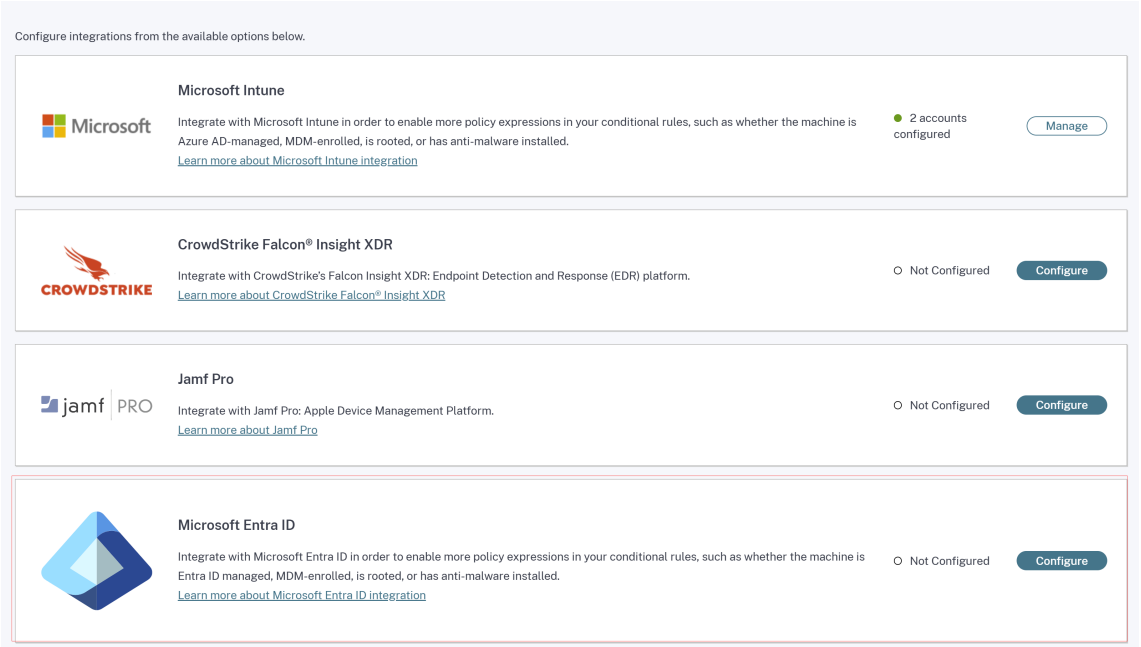
The Entra ID integration configuration is a two-step process.

1. Establish trust between Citrix Device Posture service and Microsoft Entra ID. This is a one-time activity that you do to establish trust between Device Posture and Microsoft Entra ID.
2. Configure policies to use Microsoft Entra ID compliance information.

Establish trust between Citrix Device Posture service and Microsoft Entra ID Perform the following steps to establish trust between the Citrix Device Posture service and Microsoft Entra ID.

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.

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



> **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 Microsoft Entra ID box, and then click **Configure**. The **Microsoft Entra ID** pane appears.
5. Enter the name for the profile and then click **Connect account**.
6. Click **Done**.

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

Configure device posture policies for Microsoft Entra ID integration

1. Configure a device posture policy. For details, see Configure Device Posture policies.
2. In **Policy rules**, select **Microsoft Entra ID**.
3. Select a condition, and then select the values to be matched.
   - **Compliant** - To check if the device meets the compliance policies configured in Microsoft Entra ID.
   - **Managed** - To check if the device is registered with Microsoft Entra ID.

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

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

4. Complete the policy configuration and then click **Create**.

Jamf Pro integration with Device Posture service

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

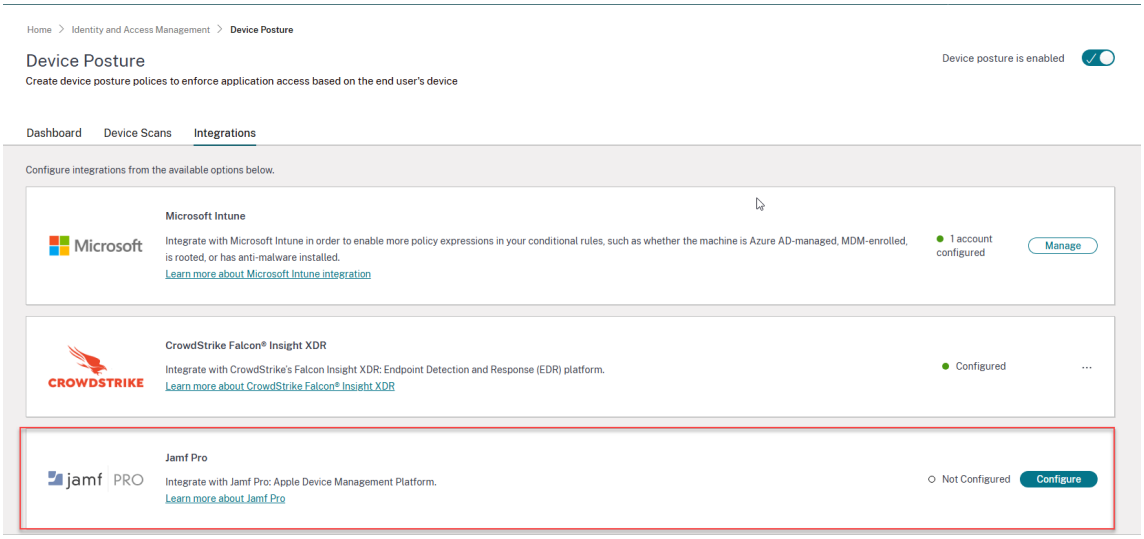
Jamf Pro integration configuration is a two-step process.

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.

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



> **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 for Jamf Pro integration

1. Configure a device posture policy. For details, see Configure Device Posture policies.
2. In **Policy rules**, select **Jamf Pro**.
3. Select a condition, and then select the values to be matched.

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

- **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 minutes) since the device last communicated with Jamf Pro to update its inventory data.

4. Click + to add additional qualifiers.

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

5. Complete the policy configuration and then 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 service

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.

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

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.

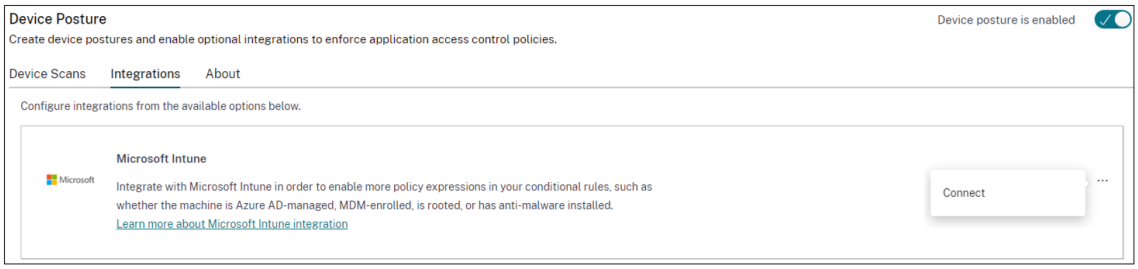
Configure Microsoft Intune integration

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.

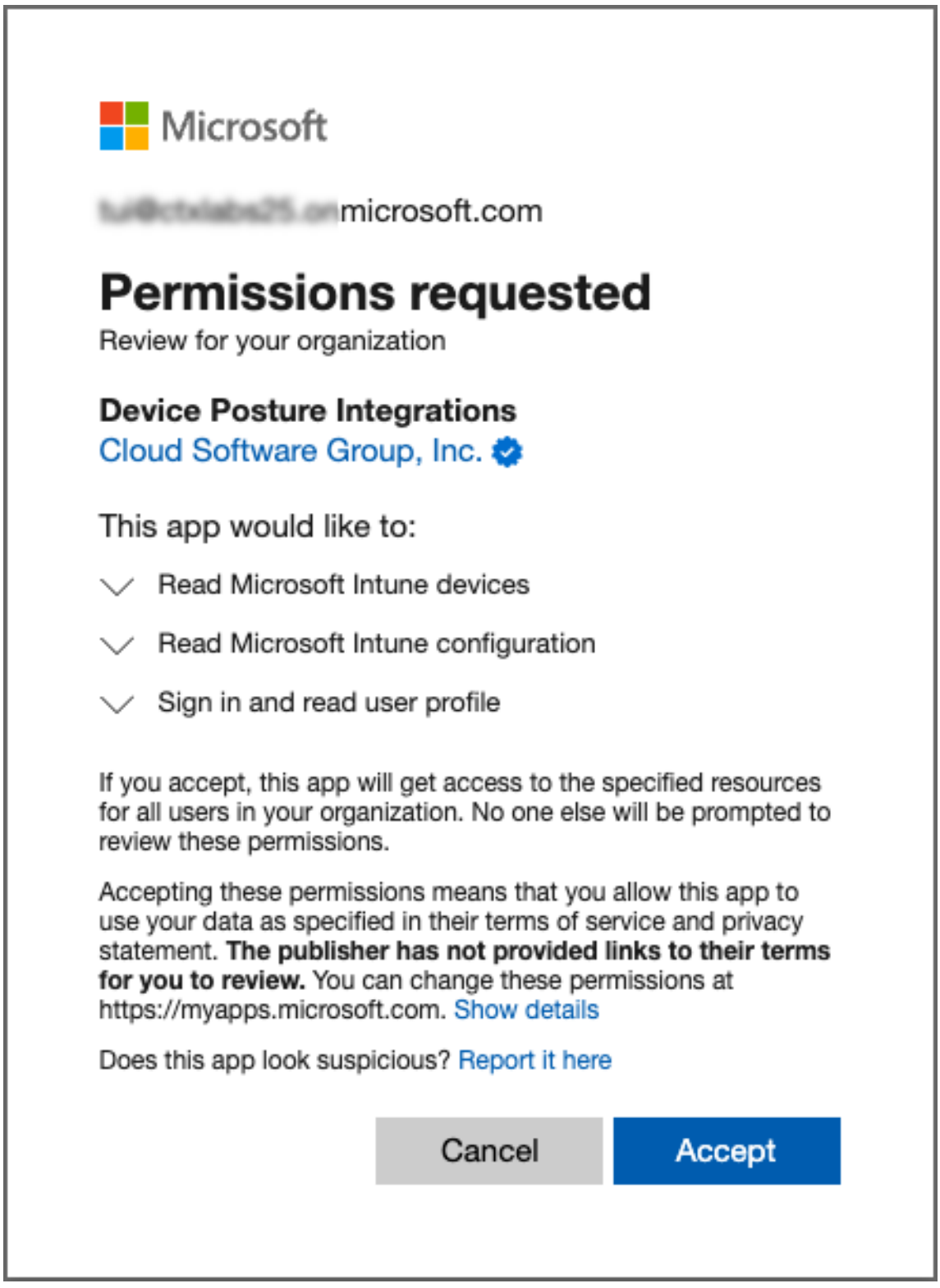
Integrate device posture with Microsoft Intune

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.



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

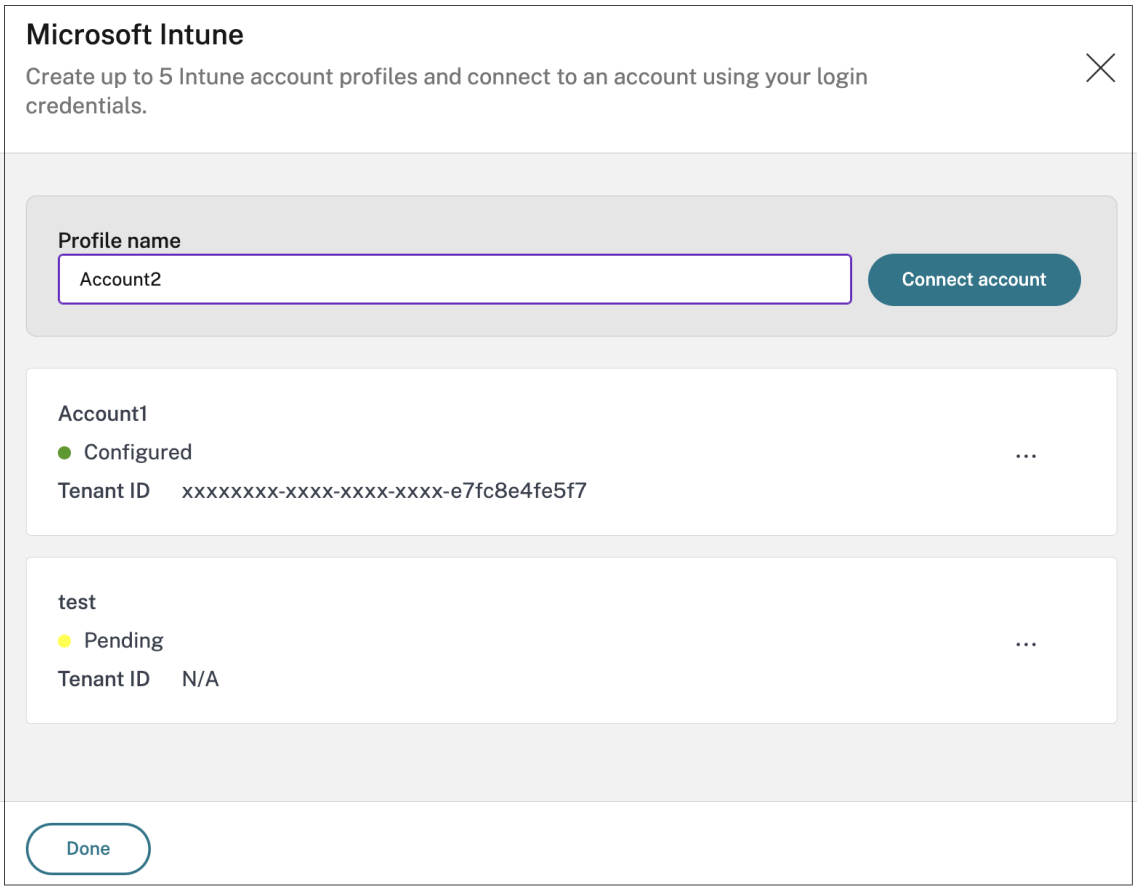
2. Click the **ellipsis** button, and then click **Connect**. The admin is redirected to Azure AD to authenticate.



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

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**.

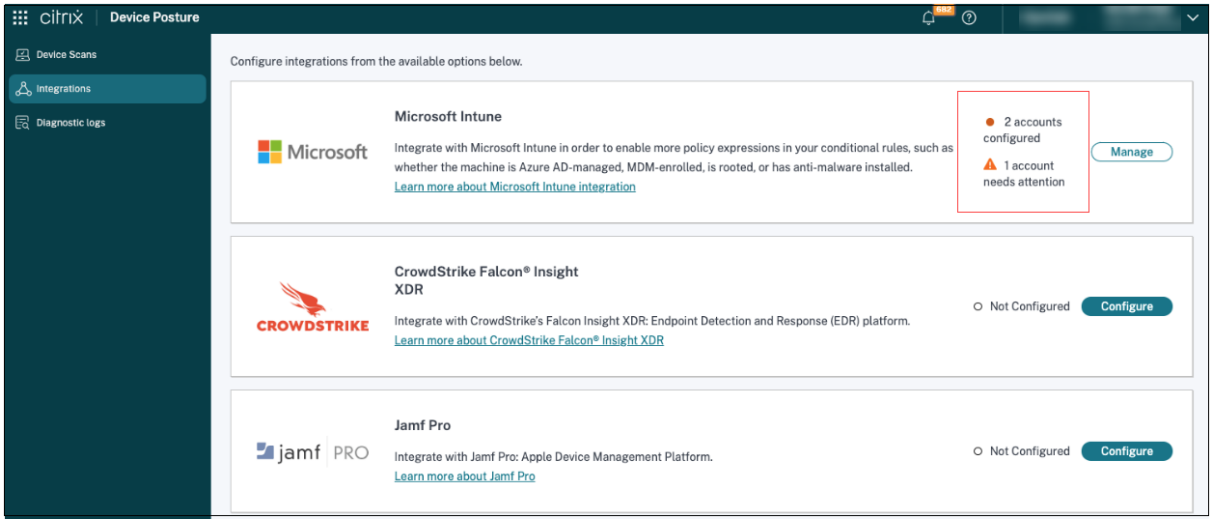


   Once the connection is established, the status appears as **Configured** and the tenant ID associated with the account is displayed.

4. Click **Done**.

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

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



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**.

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
Microsoft Graph	User.Read	Sign in and read user profile	Delegated

> **Note:**
>
> - Only Privileged Role Administrator and Global Administrator can grant application permissions.
> - While the Device Posture service only requires Application Permissions to fetch Entra ID device details, the initial admin grant flow is an interactive process performed by an individual.
> - The `User.Read (Delegated)` permission included by default in Microsoft Entra ID ver-

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

> ifies the administrator's identity during the grant flow. This ensures only authorized roles (Global Administrator or Privileged Role Administrator) grant the application-level access needed for the Device Posture service.

Configure device posture policies for Intune integration

1. Configure a device posture policy. For details, see Configure Device Posture policies.
2. In **Policy rules**, select **Microsoft Intune**.
3. Select a condition, and then select the values 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.

4. Complete the policy configuration and then click **Create**.

CrowdStrike integration with Device Posture service

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

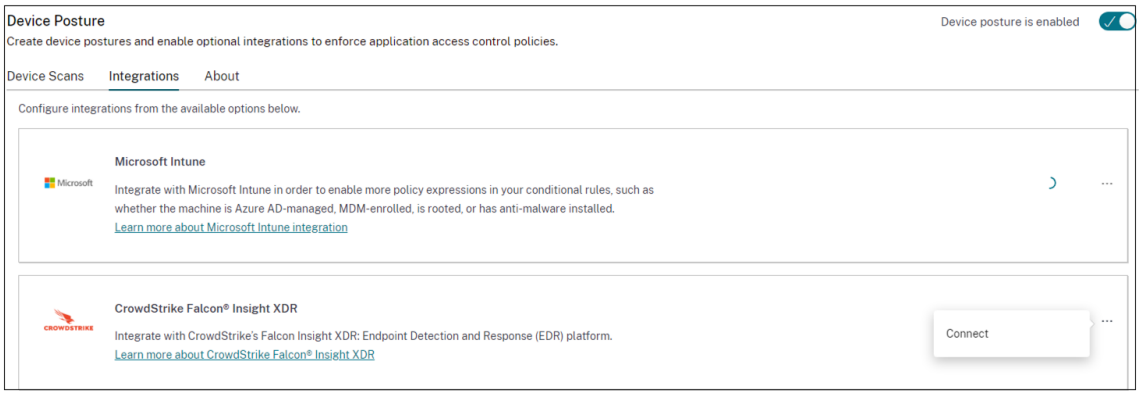
CrowdStrike integration configuration is a two-step process.

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.

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

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**.

Configure device posture policies for CrowdStrike integration Perform the following steps to configure policies to use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS

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

and Citrix Secure Private Access resources.

1. Configure a device posture policy. For details, see Configure Device Posture policies.
2. In **Policy rules**, select **CrowdStrike**.
3. For the **Risk Score** qualifier, select the condition, and then enter the risk score.
4. 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.

5. Complete the policy configuration and then click **Create**.

Third-party integration failure notifications

March 17, 2026

The Device Posture service integrates with third-party solutions such as Microsoft Intune, CrowdStrike, and Jamf Pro. Downtime or errors from these third-party cloud services can lead to unexpected device posture scan outcomes. This feature provides email notifications to administrators when third-party integration failures occur. These errors are also displayed in the Secure Private Access and Device Posture service dashboards. This allows customers to contact third-party service support directly with relevant error information, bypassing Citrix Support and reducing downtime.

Use case

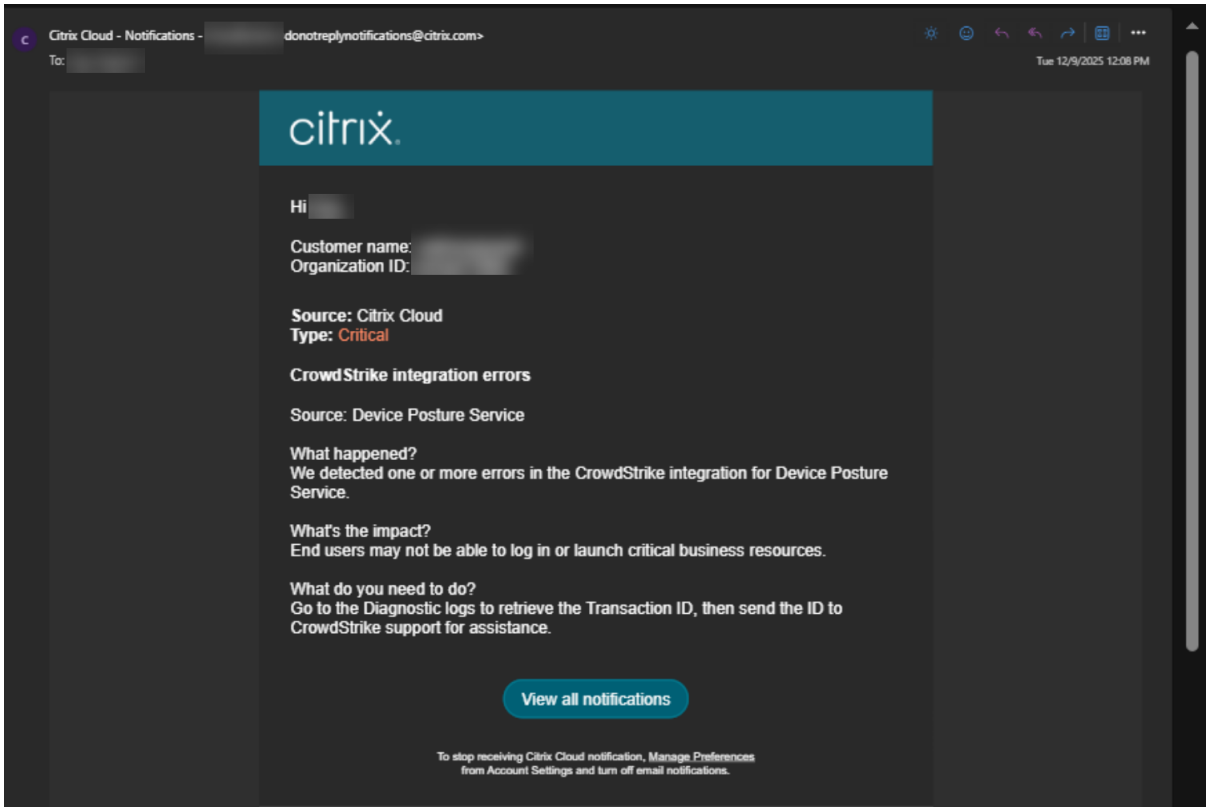
Consider a customer who has configured a CrowdStrike scan to mark a device as compliant. Otherwise, the device is marked as non-compliant.

If a CrowdStrike outage occurs, the Citrix Device Posture service cannot contact CrowdStrike to retrieve device compliance details. As a result, the end-user device is automatically marked as non-compliant.

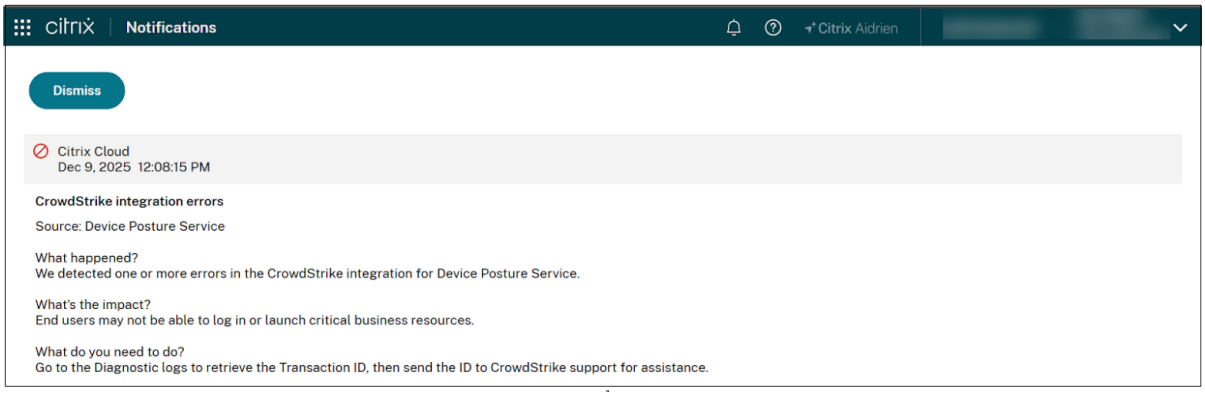
When this failure occurs, customers receive email notifications and can view detailed error information in both the Device Posture and Secure Private Access diagnostics dashboards. This visibility enables customers to contact the third-party support teams directly to resolve the issue, thereby reducing the downtime.

The following figure displays a sample email notification:

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



The following figure displays a notification on the dashboard:

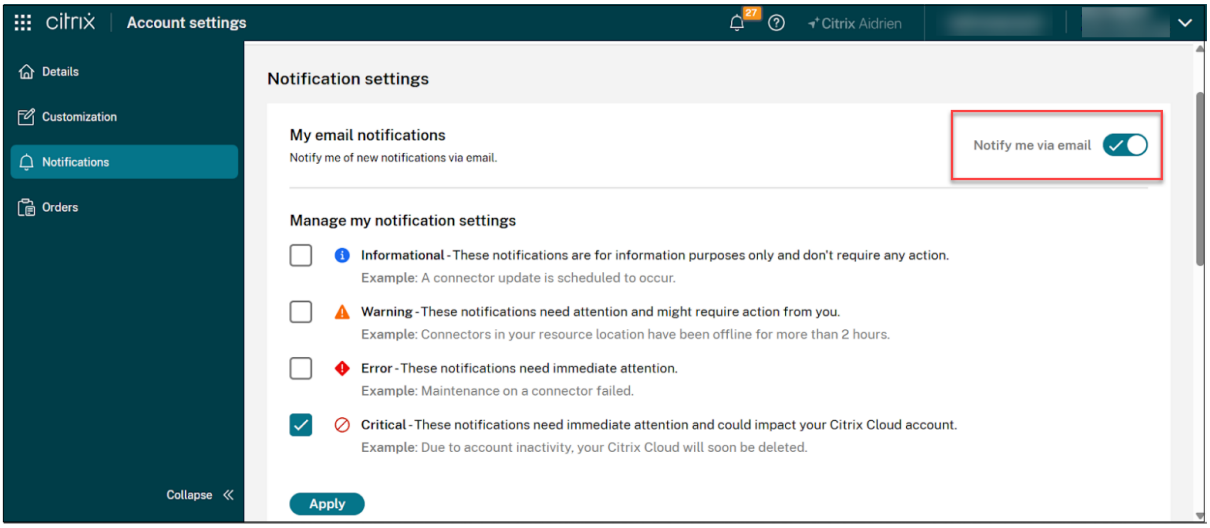


Prerequisites

The Citrix administrator must enable the following in the Citrix **Account settings > Notifications** page and the click **Apply**.

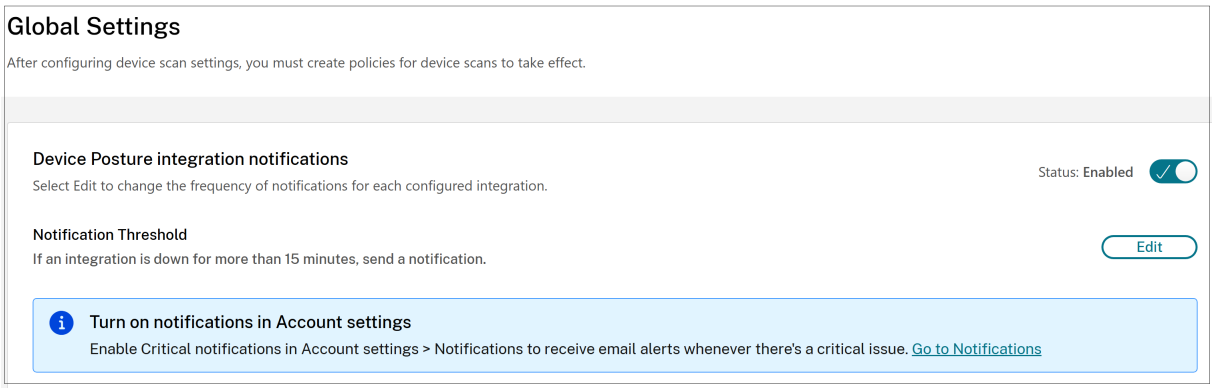
- Turn the **Notify me via email** toggle switch to ON.
- Select the **Critical** notification setting.

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



Configure for notifications in the Device Posture service admin console

1. Navigate to **Global settings**.
2. In the **Device Posture integration notifications** box, enable the toggle switch to ON.



By default, a notification is sent after 15 minutes if an integration is down. You can customize the notification frequency based on your requirements.

To change the frequency, click **Edit**, select the required frequency, and then click **Save**.

End user flow

September 6, 2025

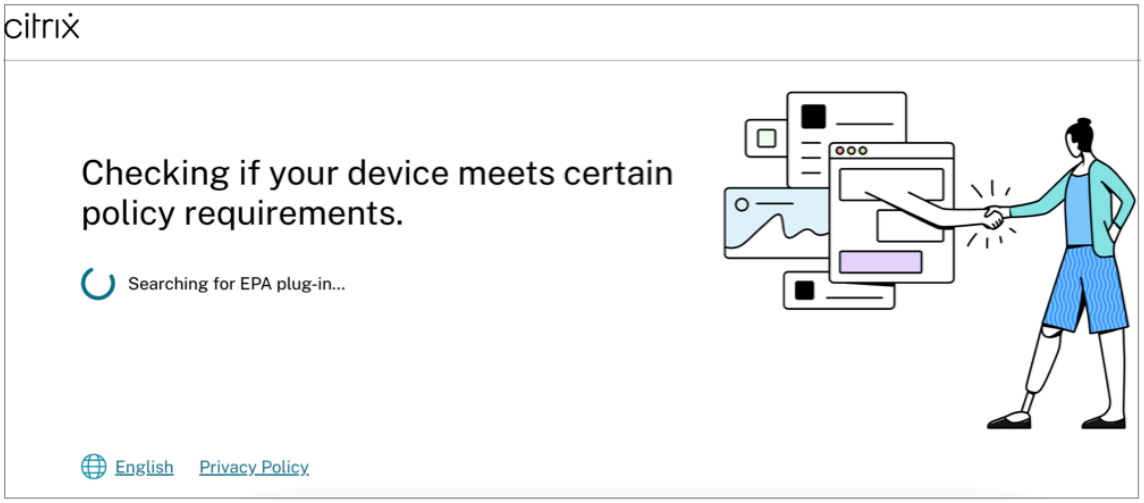
Once the device posture policies are set and device posture is enabled, the following are the end-user flows based on how the end user is logging into Citrix Workspace.

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

End-user flow via browser access

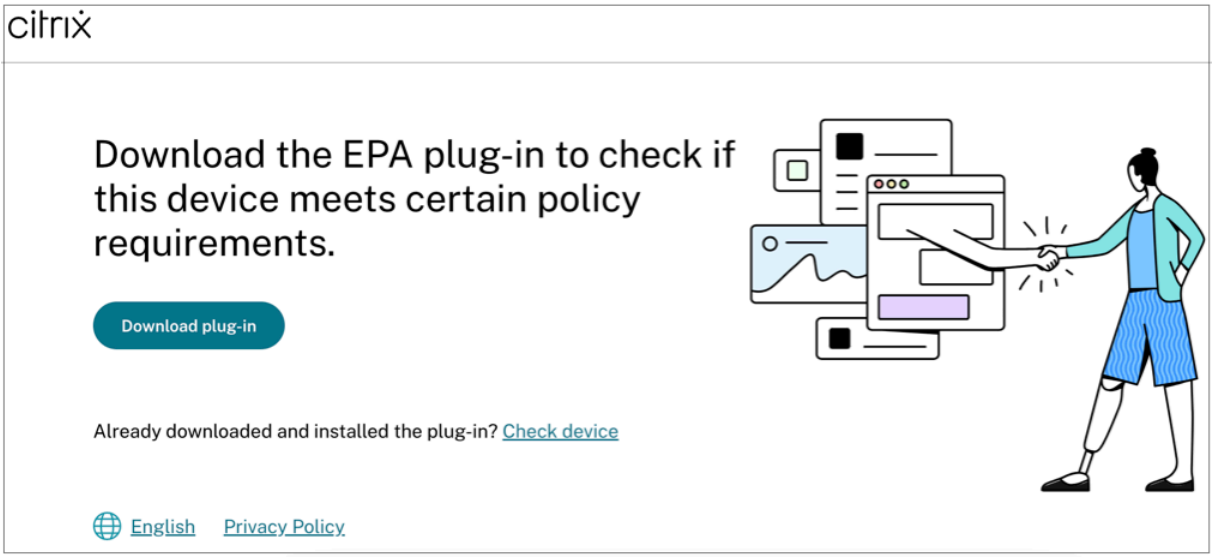
> **Note:**
>
> The macOS client and Chrome browser are used as an example for illustration purposes. The screens and the notifications vary depending on the client and the browser that you use for accessing the Citrix Workspace URL.

- 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.

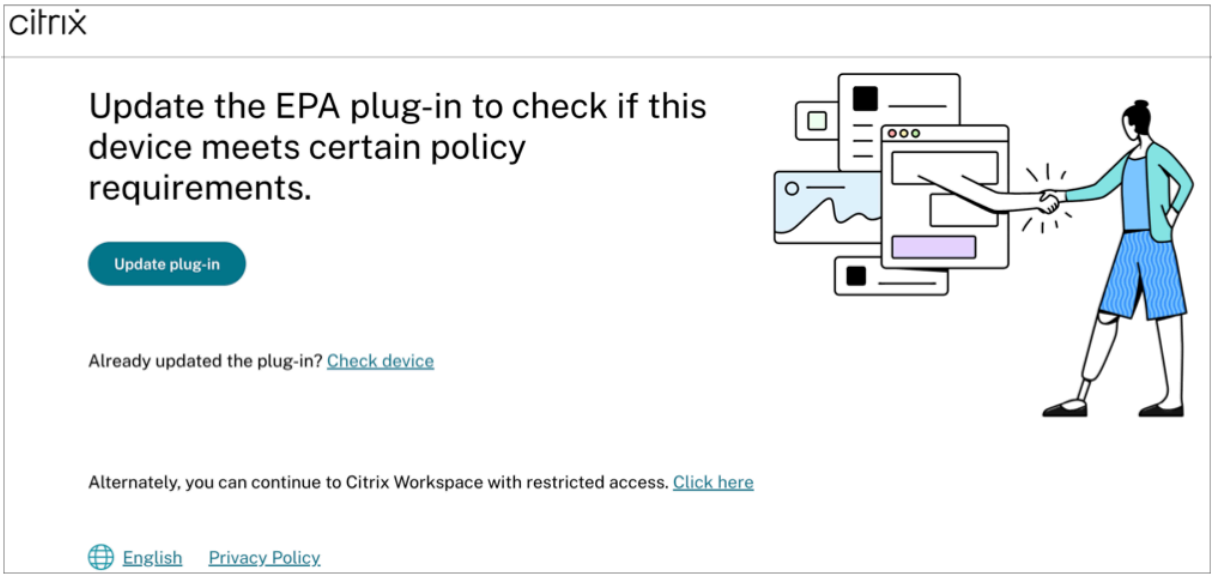


- When the end user clicks **Open Citrix End Point Analysis**, the device posture client runs and scans the endpoint parameters based on device posture policy requirements.
- If the device posture client is not installed on the device, the users are redirected to a page that displays the **Download plug-in** 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.

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



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**.

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

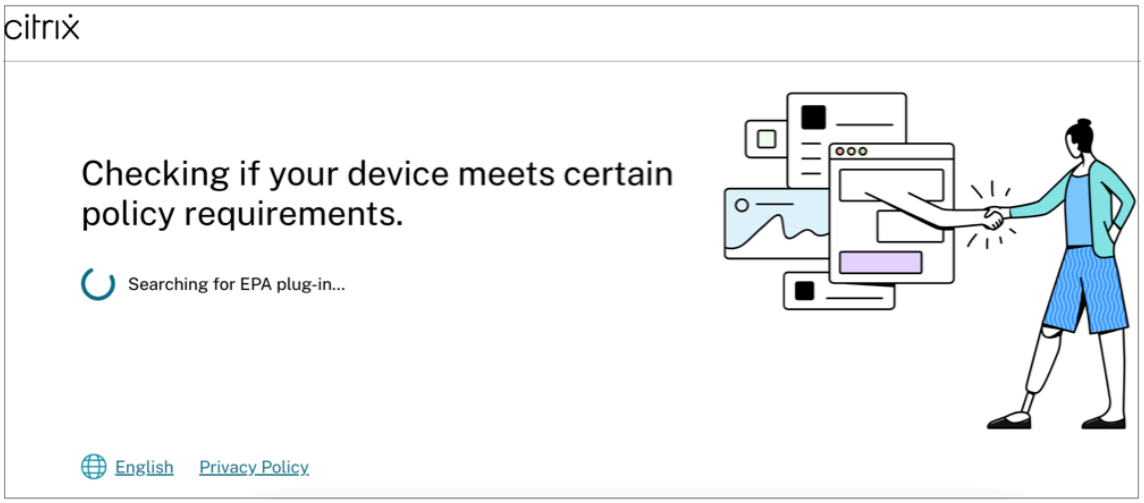
- If the latest device posture client is already installed on the endpoint, the user must click **Check again**.

End-user flow - Device posture results

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

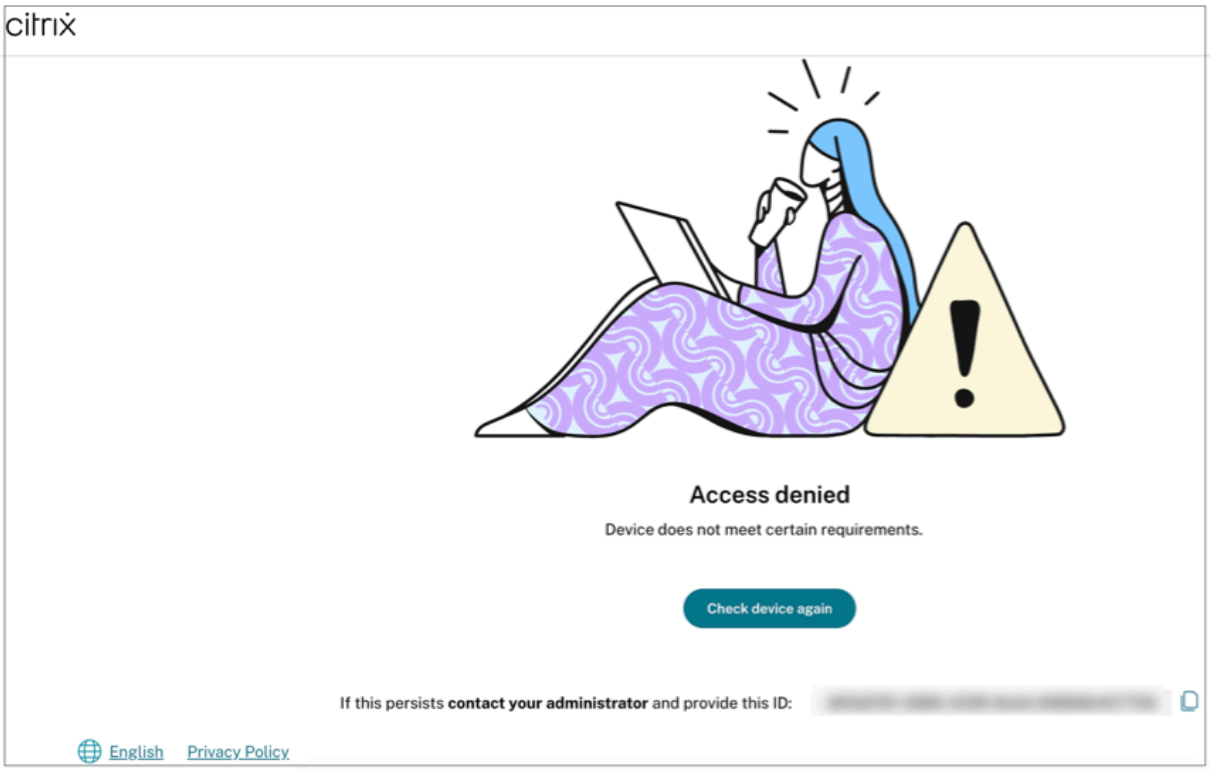
If an endpoint meets the policy conditions such that the device is categorized as;

- **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.

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



Device Posture service in test mode

September 6, 2025

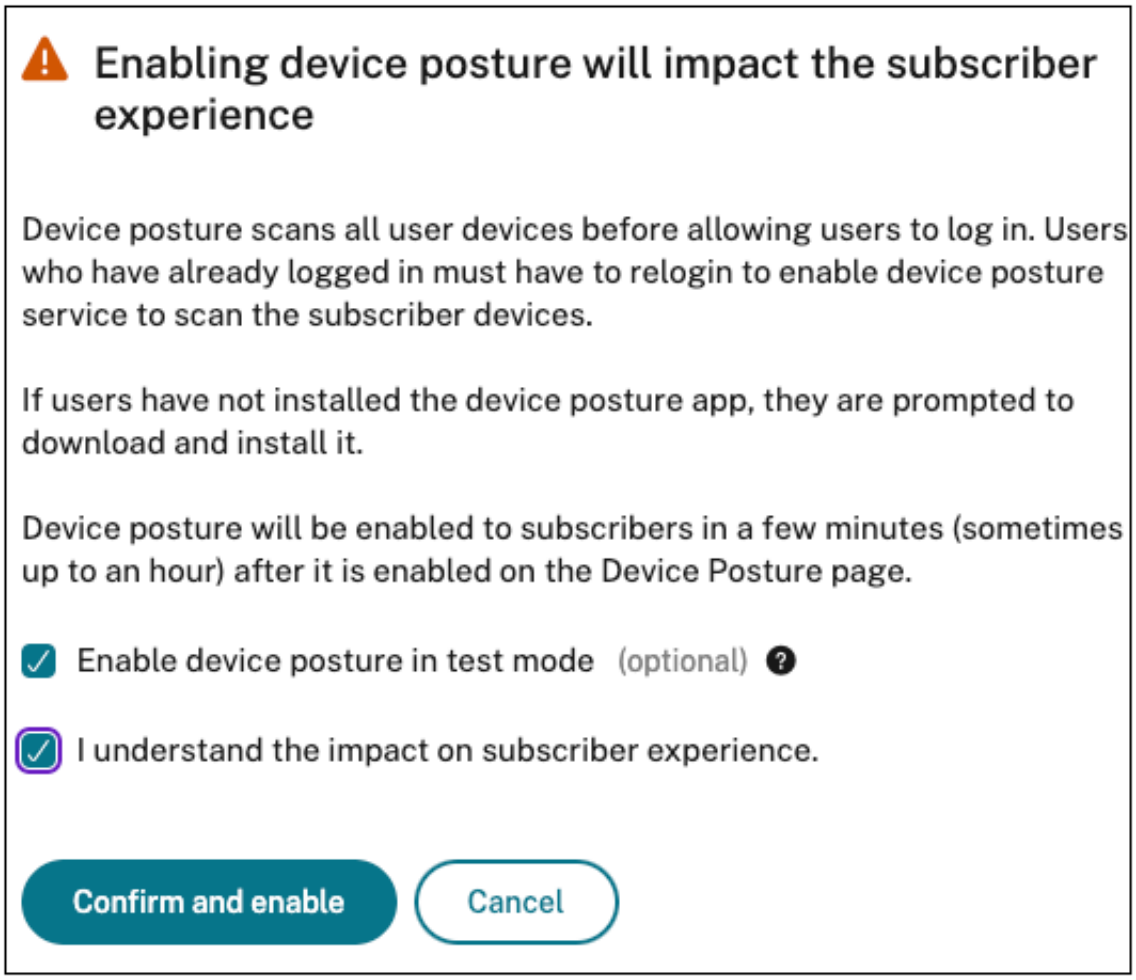
The Device Posture service is also available in test mode wherein admins can test the Device Posture service before enabling it on their production environment. This enables the admins to analyze the impact of the device posture scans on the end user devices and then plan their course of action accordingly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

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

Enable test mode

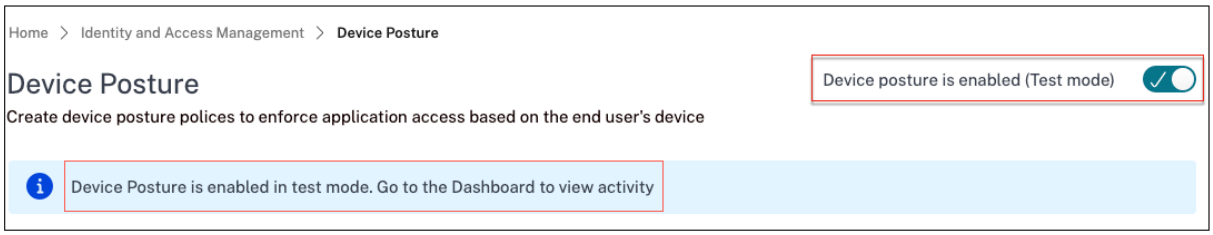
1. Sign in to Citrix Cloud™, and then select **Identity and Access Management** from the hamburger menu.
2. Click the **Device Posture** tab and then click **Manage**.
3. Slide the **Device posture is disabled** toggle switch ON.
4. In the confirmation window, select both the checkboxes.



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.

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



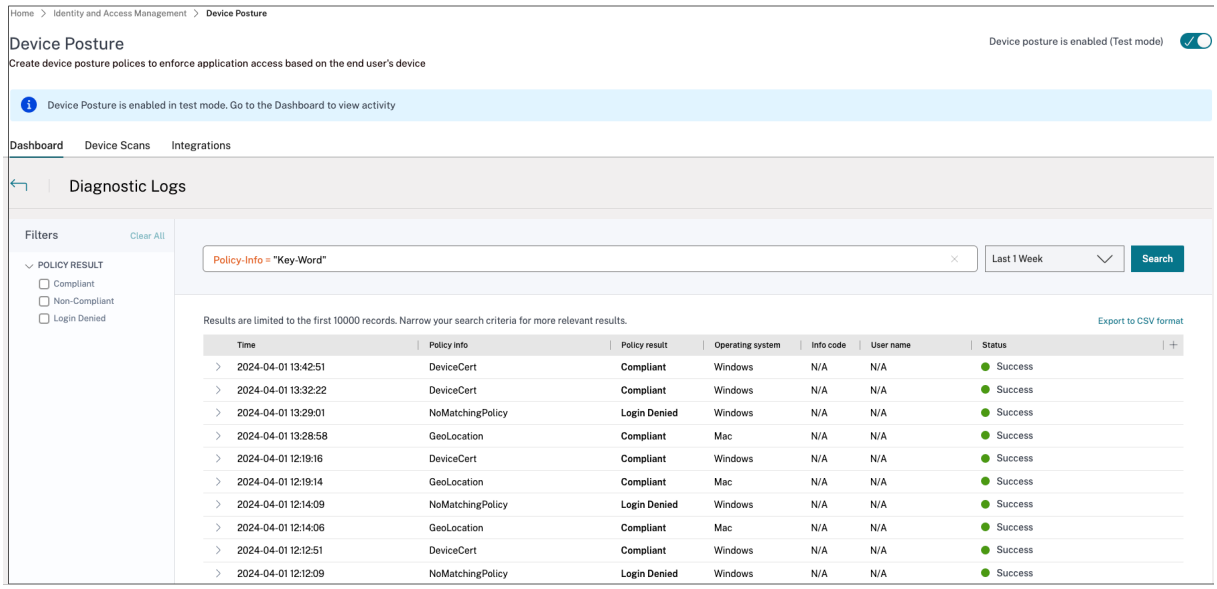
Admins can configure the policies and rules for device posture scans. For details, see Configure device posture. Based on the scan results, the end user devices are classified as compliant, non-compliant, and denied. Admins can view this data on the dashboard.

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.

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

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.

Manage Citrix Secure Access Endpoint Analysis (EPA) client versions by setting minimum supported versions

August 13, 2026

> **Note:**
>
> In this topic, EPA refers to the Citrix Secure Access Endpoint Analysis client. The two terms are used interchangeably.

Administrators can manage the Citrix Secure Access Endpoint Analysis (EPA) client versions through the Device Posture service by maintaining a minimum supported EPA version.

Previously, Device Posture service required a single fixed EPA client version across all endpoints.

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

Benefits:

EPA client version management through Device Posture service solution offers the following benefits:

- Streamlined version control
- Reduced support overhead
- Ensured endpoint compliance with Device Posture service requirements

How it works

Device Posture service prompts the users to either install or upgrade the client versions based on the platform-specific settings in the Device Posture admin console.

- **Minimum supported version:** When an administrator sets the minimum supported version, the Device Posture service behaves as follows:

Client devices	Device Posture service behavior
Devices with no client installed	The users are prompted to install the latest EPA client.
Devices with client version lower than the minimum	The portal presents a download option. The end users install or upgrade the client manually. Install with administrator privileges. Otherwise the install runs in user mode and some features might not be available.
Devices with version equal to or greater than the minimum version	No changes.

- **Always use latest version:** When an administrator sets the **Always use latest version** option, all endpoints run the latest available EPA client version.

  In case where the EPA client is not installed or is outdated, the Device Posture service behaves as follows:

Client devices	Device Posture service behavior
Devices with no client installed	The users are prompted to install the latest EPA client.

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

Client devices	Device Posture service behavior
Devices with older versions	The portal presents a download option. The end users install or upgrade the client manually. Install with administrator privileges. Otherwise the install runs in user mode and some features might not be available.

Example:

Consider the following example for a specific platform where the minimum supported version is 24.8 and the latest version is 25.8.

The following table summarizes the Device Posture service behavior based on the settings configured in the admin console:

Client devices	Minimum supported version selected as 24.8	Always use the latest version selected
No EPA client installed	Prompted to install the latest EPA client.	Prompted to install the latest EPA client.
EPA version < 24.8	Prompted to upgrade to latest	Prompted to upgrade to latest
EPA version ≥ 24.8 (but not latest)	Remains as is	Prompted to upgrade to latest
EPA version == latest	Remains as is	Remains as is

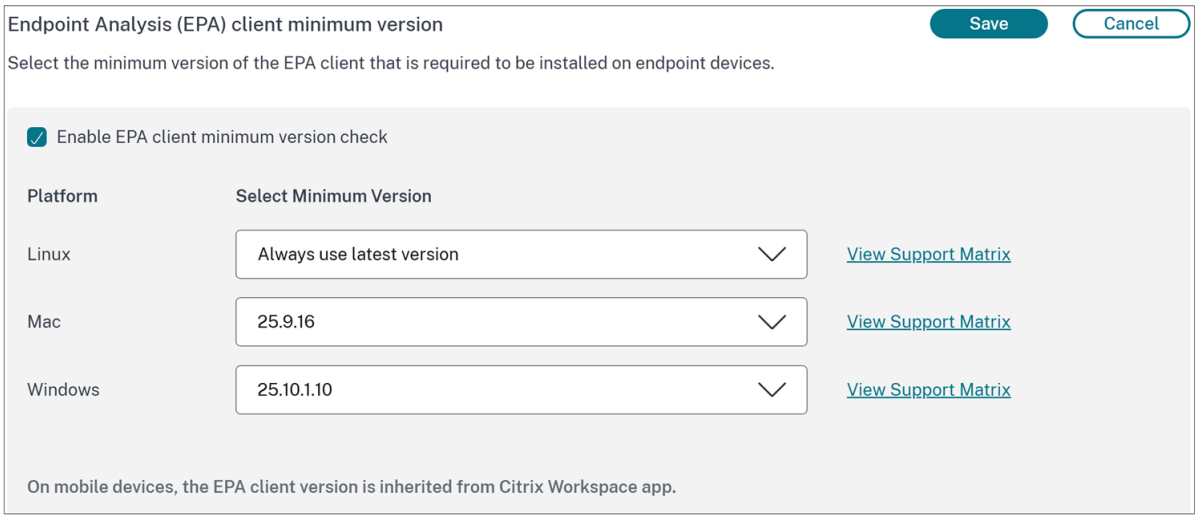
> **Note:**
>
> When the Device Posture service introduces a new feature requiring an updated EPA client, administrators must revise the minimum supported version to ensure compatibility and optimal functionality.

Set the EPA client version management option

1. Navigate to **Device Posture > Device Scans** and click **Settings**.
2. Enable the EPA client minimum version toggle and click **Edit**.
3. For each platform, choose one of the following options for client version management:
    - **Always use latest version**
    - **Minimum version listed** (for example 24.8.1.19 for Windows)

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

4. Click **Save**.



> **Important:**
>
> - EPA client version management supports the versions listed in the drop-down list. We recommend that your end users use these or higher versions. Any version not listed in the drop-down menu is not recommended for a production environment.
> - For the latest client versions, see Citrix Endpoint Analysis.

EPA client distribution and version management considerations

Consider the following points for EPA client distribution and version management:

- **Distribution strategy:** Use standard Endpoint Management tools (for example, SCCM for Windows, Jamf for macOS) to deploy or patch the EPA client.
- **Standardized rollouts:** Gradually roll out client updates by setting a minimum supported version aligned with your deployment schedule.
- **Immediate feature rollout:** Ensure that the Always use latest version setting is enabled so that all users receive the latest EPA version when it is released.
- **Compatibility assurance:** Update the minimum supported version whenever new Device Posture service dependent features are released to avoid unsupported client versions.

Multiple cloud store support

September 9, 2026

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

Administrators can apply distinct device posture policies to different cloud stores, offering granular control and simplified security management.

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

With multiple store support, you can now do the following:

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

Important considerations

Before implementing different rules per store, note the following:

- Multi-workspace URL support is not available with Chrome Extension Premium (CEP).
- Multi-workspace URLs are not supported with NetScaler Gateway URLs.
- When you switch to multi-workspace mode, the existing device posture configuration is cloned for each workspace URL.
- Existing customers can set up a test URL and then enable multiworkspace URL support for the Device Posture service. They can trial changes on the test URL while keeping the Device Posture service active on their production URLs. This approach allows you to validate the changes in posture check without disrupting the broader user base.

> **Note:**
>
> Service continuity for Device Posture service in multi-workspace deployments is supported from Delivery Controller™ (DDC) version 26.03.

Prerequisites

- Supported platforms: Windows, macOS and iOS
- Multi-workspace URLs support is available in the following EPA clients:
  - Windows: Version 25.7.1.11 and later. Download link.
  - macOS: Version 25.11.19 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 platforms other than Windows, macOS, or iOS are treated as using unsupported devices and follow the default behavior configured by the ad-

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

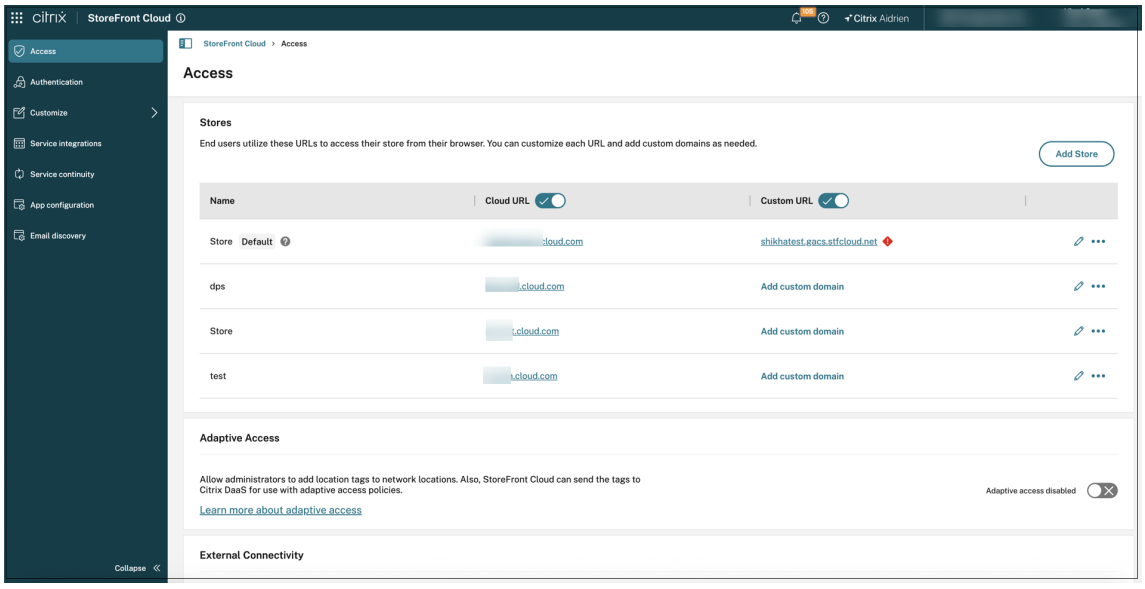
ministrator in the Device Posture service console. This is applicable only when **Skip check** is configured. Otherwise, users are prompted to download the latest client.

- 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.

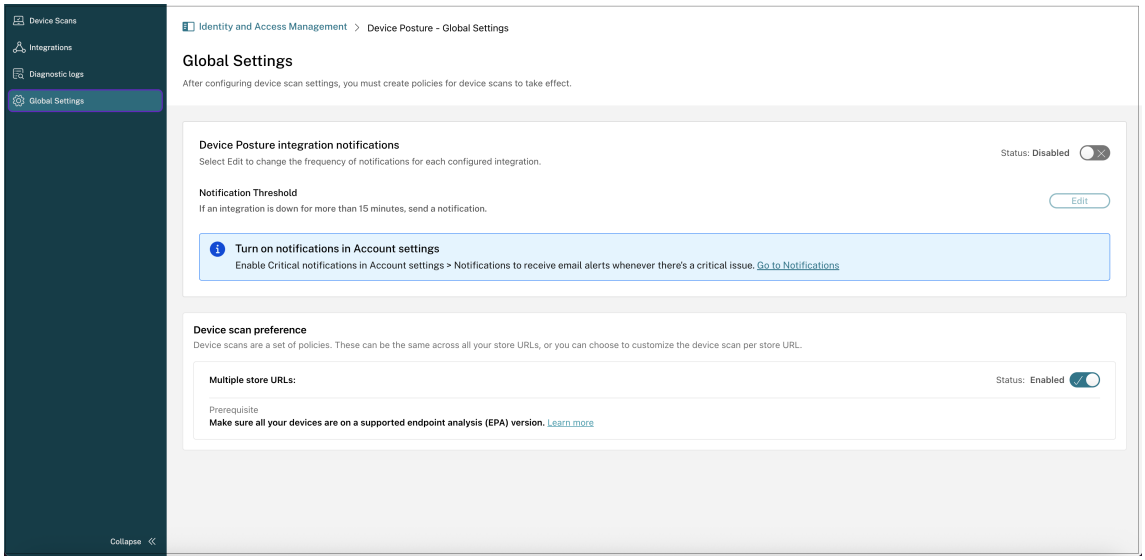
Configure store URLs

1. Ensure workspace URLs are configured via **StoreFront Cloud > Access**.

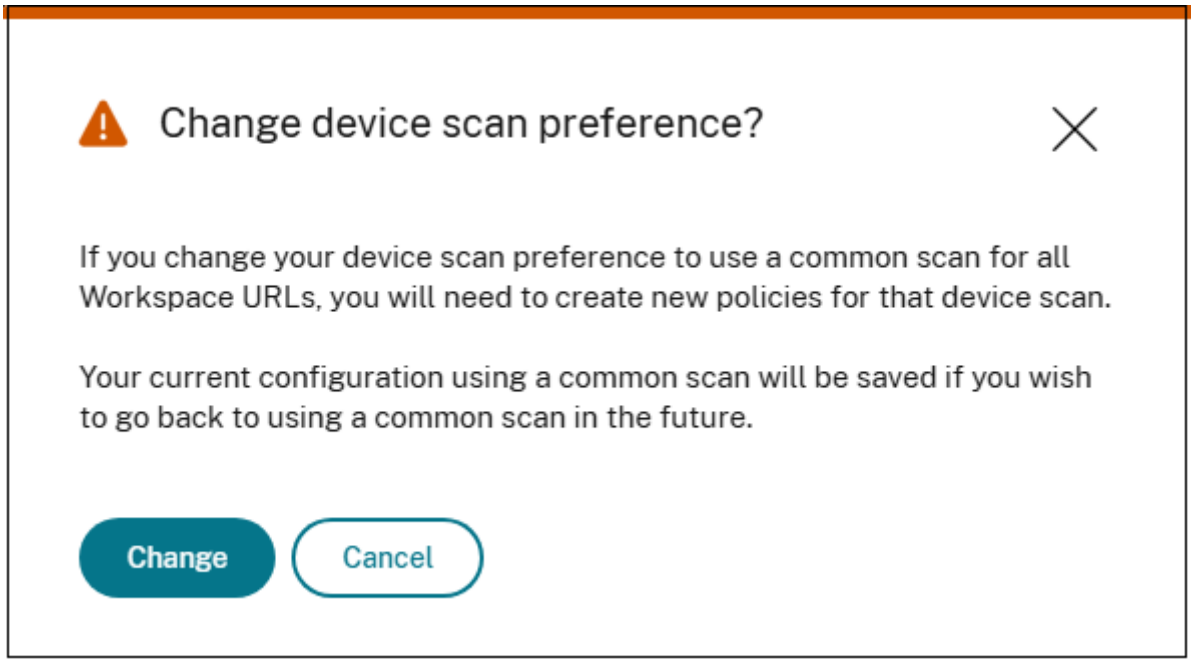


2. To access Device Posture, log in to Citrix Cloud™ and navigate to **Identity and Access Management > Device Posture > Global Settings** in the Device Posture navigation bar.

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



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, you must configure new scans individually for each workspace URL.
- After configuring the new scans, users are prompted to re-authenticate within 1-2 hours to ensure that their login sessions are evaluated using the new configuration.

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

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

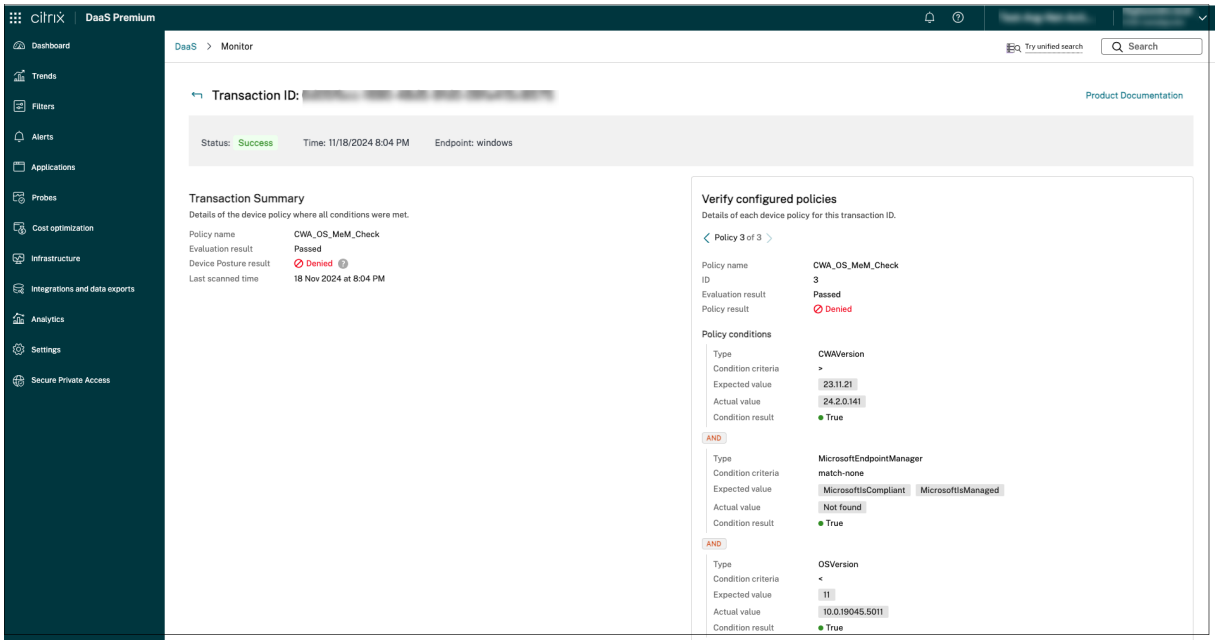
You can troubleshoot the Device Posture issues/errors in DaaS Monitor using the transaction ID that is generated for each session when a user connects through Secure Private Access or DaaS. When you locate the transaction ID, the DaaS Monitor displays information about the session and the associated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

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

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

September 1, 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.

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

- **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.

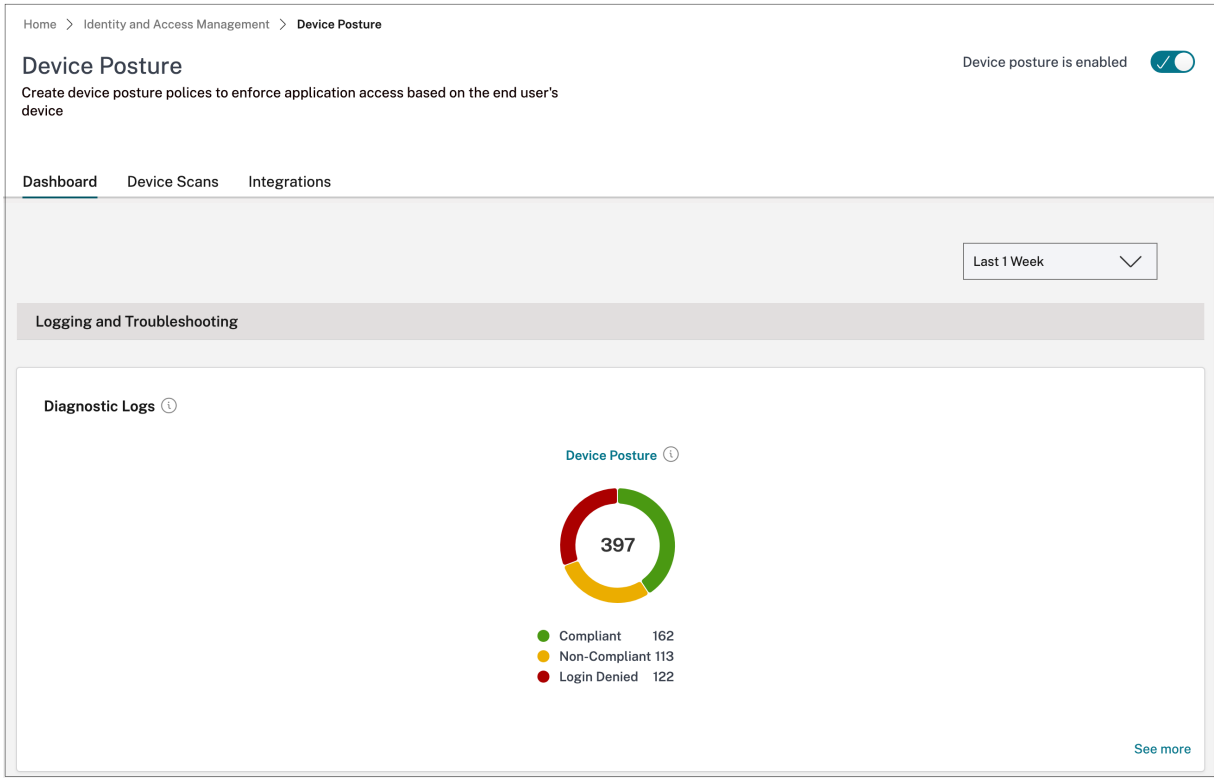
You can view the Device Posture logs and events in the Secure Private Access dashboard and in the Device Posture dashboard in the Identity and Access Management console.

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.**

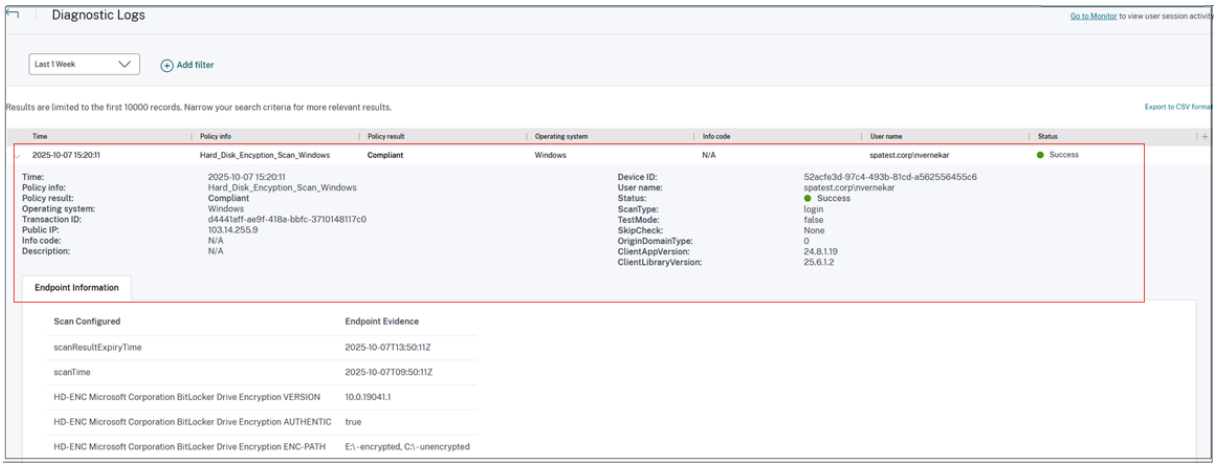
   The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service.
4. Click the **See more** link to view the details of the logs. You can refine your search based on the policy results (**Compliant**, **Non-Compliant**, and **Login Denied**).



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

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

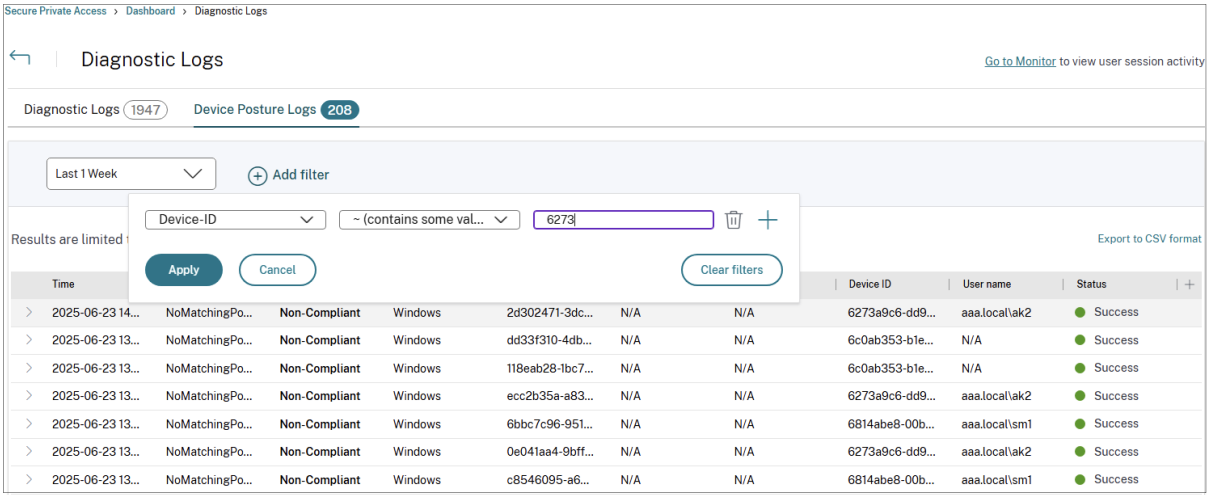
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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 22, 2026

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:

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

- 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

The following sections provide more information about trobleshooting the issues:

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

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

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.

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

- 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.

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

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
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

Citrix Secure Access Endpoint Analysis (EPA) client distribution and upgrade

September 28, 2026

This topic describes the supported ways to distribute and upgrade the Citrix Secure Access Endpoint Analysis client. The information captured here applies to both managed and unmanaged Windows devices, and to both cloud (Device Posture service) and on-premises (NetScaler® Gateway) deployments.

> **Note:**
>
> In this topic, EPA refers to the Citrix Secure Access Endpoint Analysis (EPA) client. The two terms are used interchangeably.

Citrix Secure Access Endpoint Analysis (EPA) client distribution and upgrade methods

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

Method	Deployment	Managed	Unmanaged	Trigger	How to configure
Bundled with the Citrix Workspace™ app release	Cloud and on-premises	Yes	Yes	Automatic (with the Citrix Workspace app update)	The Citrix Workspace app installer carries the Citrix Secure Access Endpoint Analysis client and installs or upgrades it together with Citrix Workspace app by default. See Download Citrix Workspace app. For detailed configuration steps, see Bundled with the Citrix Workspace app release.
Citrix Workspace app auto-update (Client App Management)	Cloud and on-premises	Yes	Yes	Automatic (Citrix Workspace app updater service)	Enable the **Citrix Endpoint Analysis plug-in** in the Client App Management (GACS) console to auto-upgrade the client.

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

Method	Deployment	Managed	Unmanaged	Trigger	How to configure
					For details on GACS setup, see Cloud: Configure GACS (Cloud). On-premises: Configure GACS (StoreFront). For detailed configuration steps, see Citrix Workspace app auto-update (Client App Management)
Push the installer using SCCM, Intune, Jamf, or another endpoint management tool	Cloud and on-premises	Yes	Not applicable	Manual or admin-managed	The administrator downloads the installer from Citrix Downloads. For detailed configuration steps, see Push the installer using SCCM, Intune, Jamf, or another endpoint management tool.

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

Method	Deployment	Managed	Unmanaged	Trigger	How to configure
Set a minimum EPA client version in the Device Posture service console	Cloud only	Yes	Yes	Prompt only (not enforced)	Clients running a lower version are shown a download option in the portal. This is not a silent or enforced upgrade. The end users install or upgrade the client manually. Install with administrator privileges. Otherwise the install runs in user mode and some features might not be available. For detailed configuration steps, see Set a minimum EPA client version in the Device Posture service console.

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

Method	Deployment	Managed	Unmanaged	Trigger	How to configure
Upload the plug-in to the NetScaler Gateway portal	On-premises	Yes	Yes	Prompt only (not enforced)	The portal presents a download option. The end users install or upgrade the client manually. Install with administrator privileges. Otherwise the install runs in user mode and some features might not be available. For detailed configuration steps, see Upload the plug-in to the NetScaler Gateway portal.

Detailed configuration steps

The following sections capture the detailed configuration steps:

Bundled with the Citrix Workspace app release

The Citrix Secure Access Endpoint Analysis client is bundled with Citrix Workspace app. Therefore, installing or upgrading Citrix Workspace app automatically installs or upgrades the EPA client.

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

1. Track the availability of Citrix Workspace app in the Citrix Workspace app release notes.
2. Distribute Citrix Workspace app through your usual channel: Citrix Workspace app auto-update, manual download, or a mobile device management (MDM) tool.

   During installation, the bundled Citrix Secure Access Endpoint Analysis client is installed or upgraded. No separate action is required.

Applicability: Cloud and on-premises. Managed and unmanaged devices, where end users install or update Citrix Workspace app themselves.

Citrix Workspace app auto-update (Client App Management)

The Citrix Workspace app auto-update service upgrades the Citrix Secure Access Endpoint Analysis client when the **Citrix Endpoint Analysis plug-in** is enabled in Client App Management. The Client App Management control is named **Citrix Endpoint Analysis plug-in**, and the client that it upgrades appears in the Windows control panel as **Citrix Secure Access Endpoint Analysis**.

1. Open the Client App Management console. For cloud, see Configure the Global App Configuration service (cloud). For on-premises, see Configure the Global App Configuration service (StoreFront).
2. Enable the **Citrix Endpoint Analysis plug-in** for auto-update.
3. Ensure that the configured version targets the required Citrix Secure Access Endpoint Analysis version.

   The Citrix Workspace app auto-update service automatically upgrades the EPA client on eligible endpoints through the Citrix Workspace app updater service.

   The configured versions are shown in the download option in the portal, and the end users download and install or upgrade the client themselves.

Applicability: Cloud and on-premises. Managed and unmanaged devices.

Push the installer using SCCM, Intune, Jamf, or another endpoint management tool

For managed endpoints, administrators can distribute the Citrix Secure Access Endpoint Analysis installer by using SCCM, Intune, Jamf, or another endpoint management tool.

1. Download the Citrix Secure Access Endpoint Analysis installer from Citrix Downloads.
2. Package the installer in your endpoint management platform.
3. Deploy the package to the required managed Windows devices by using your standard software distribution process.

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

4. Validate the installed version from the Windows Control Panel or from your management inventory.

Applicability: Cloud and on-premises. Managed devices only.

Set a minimum EPA client version in the Device Posture service console

In the Device Posture service console, you can set a minimum EPA client version. Clients running a lower version see a download option in the portal, allowing end users to install or upgrade the client.

1. In the Device Posture service console, set the Endpoint Analysis (EPA) client minimum version to your target version (for example, 26.5.1.7). For details, see EPA client version management through Device Posture service.

   At the next posture evaluation, clients running a lower version see a download option in the portal.

2. The end users download and install or upgrade the client.

   > **Note:**
   >
   > Install with administrator privileges. Otherwise the install runs in user mode and some features might not be available.

> **Note:**
>
> This method prompts the end user to update the client. It does not enforce a silent or automatic upgrade.

Applicability: Cloud only. Managed and unmanaged devices, where the end user is typically the administrator.

Upload the plug-in to the NetScaler Gateway portal

You can upload the Citrix Secure Access Endpoint Analysis plug-in to the NetScaler Gateway portal. At logon, the gateway prompts users to download or upgrade the client.

For the configuration steps, see How users connect with the NetScaler Gateway plug-in.

> **Note:**
>
> This method only detects and prompts. End users can decline the action, and it does not enforce a silent self-install.
>
> Install with administrator privileges. Otherwise, the client installs in user mode, and some fea-

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

> tures might not be available.

Applicability: On-premises. Managed and unmanaged devices, with the same detect-and-prompt behavior.

Considerations when the EPA client is used with NetScaler and Device Posture service

When an EPA client is used together with the 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 mismatch might cause NetScaler to prompt the end user to install the EPA client version that is present on NetScaler. To avoid this conflict, we recommend the following configuration changes:

- If you have configured EPA with adaptive authentication, on-premises authentication, or a gateway virtual server, we recommend that you disable version control of the EPA client on NetScaler. This ensures that the Client App Management (GACS) or Device Posture service does not push the latest version of the EPA client to the end devices.
- You can set the EPA version control 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 the adaptive authentication and on-premises authentication virtual servers.
    - 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

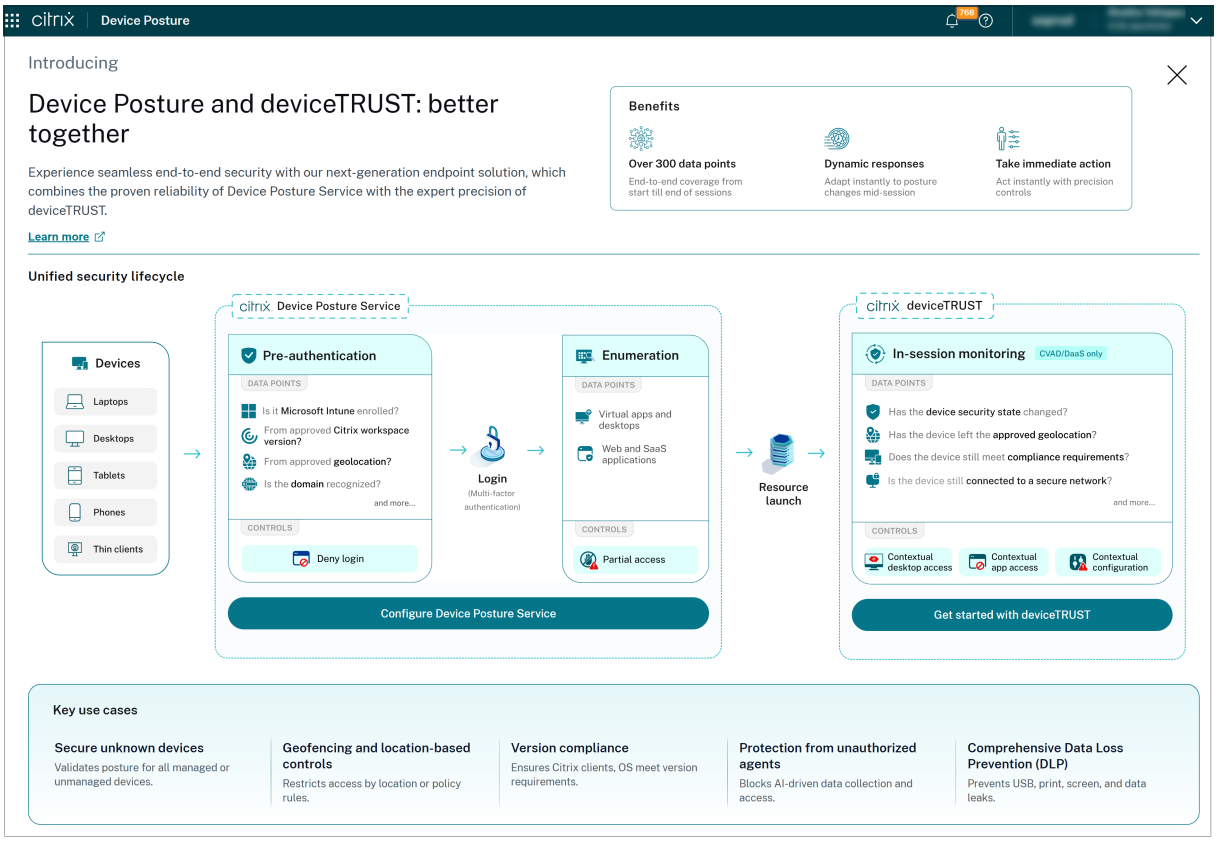
September 22, 2026

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

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

The following sections provide information about 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;

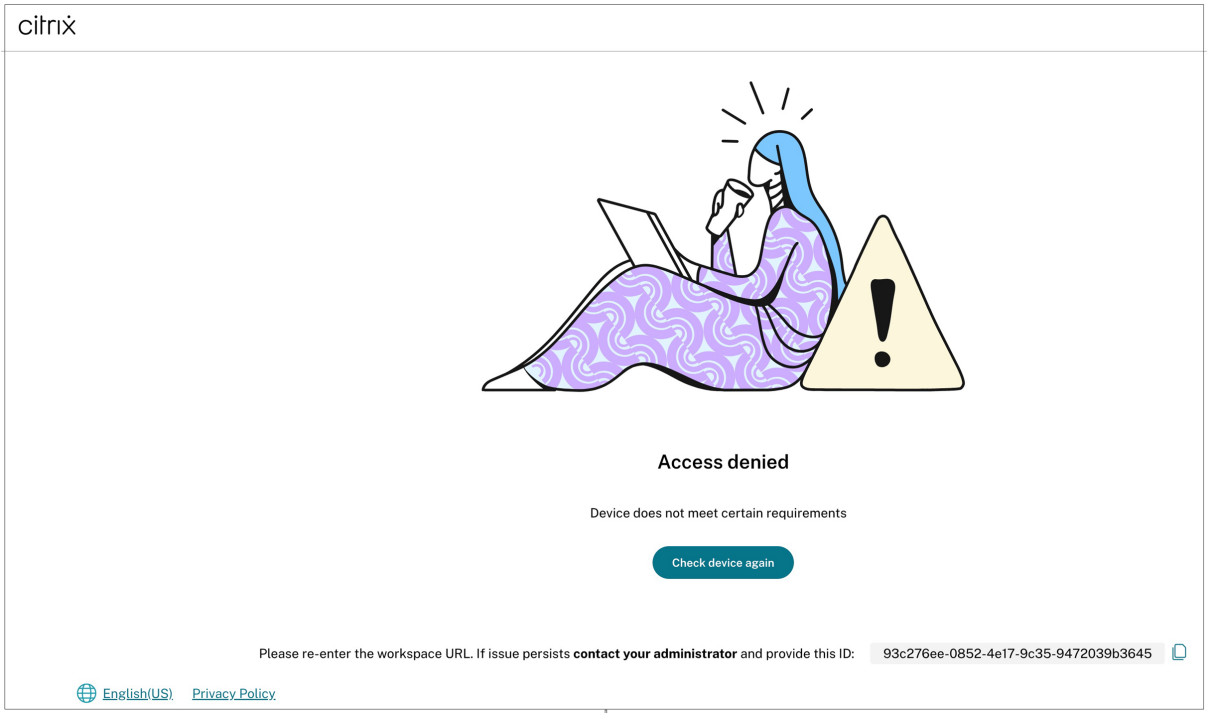
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.



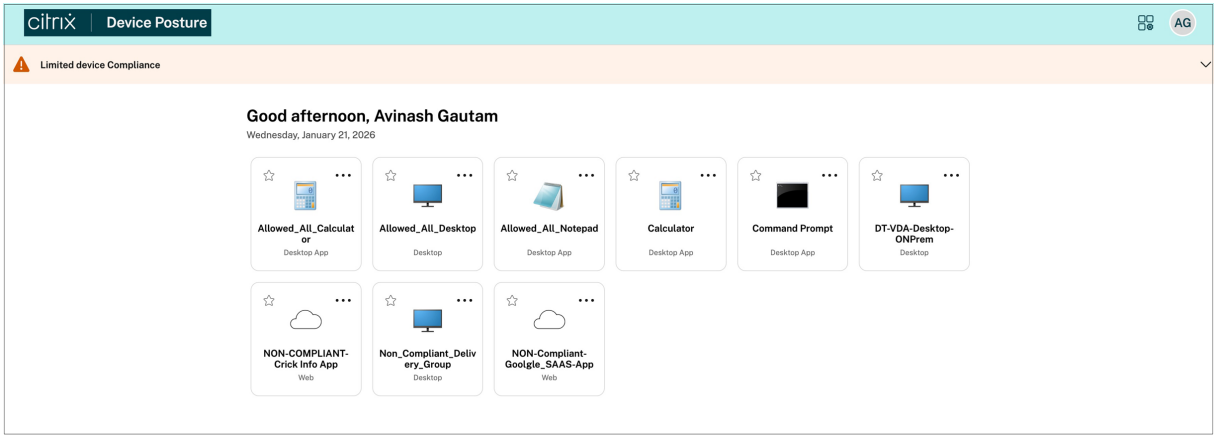
Enumeration: Contextual access to applications

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.

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



In-Session: Continuous contextual access evaluation

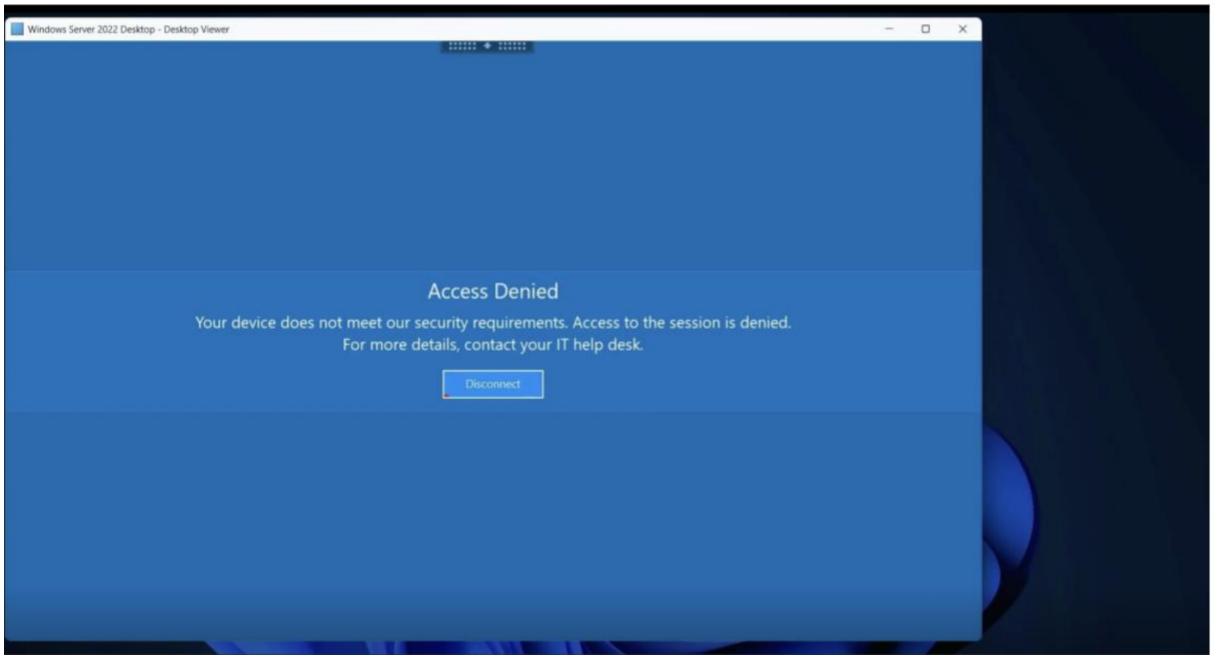
Once a session is established, deviceTRUST takes over to provide continuous, in-session contextual access controls. Unlike traditional solutions that only check device posture at login, deviceTRUST monitors device context throughout the session, enabling dynamic enforcement of policies as conditions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

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



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.

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

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)

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

- 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.

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

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.

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