



Device Posture

Contents

What's new	2
Device Posture service in test mode - Preview	5
CrowdStrike integration with Device Posture	7
Microsoft Intune integration with Device Posture	10
Device certificate check with Device Posture service	15
Enforce smart controls on DaaS using Device Posture	18
Monitor and troubleshoot	20
Device posture logs	22
Manage Citrix Endpoint Analysis client for Device Posture service	23
Data Governance	26

What's new

May 30, 2024

29 May 2024

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

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 - Preview](#).

- **Periodic scanning of devices - Preview**

You can now enable periodic scanning of Windows devices for the configured checks every 30 minutes. For details, see [Periodic scanning of devices - Preview](#).

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 an access is denied is now generally available. For details, see [Customized messages for access denied scenarios](#).

26 March 2024

- **Custom workspace URLs support**

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

12 February 2024

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

Device Posture service now supports browser and antivirus checks. For details, see [Scans supported by device posture](#).

23 January 2024

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

Device certificate check with the Device Posture service is now generally available. For details, see [Device certificate check with Device Posture service](#).

- **Device Posture service preview features**

Device Posture service now supports the following checks:

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

For details, see [Device Posture](#).

11 September 2023

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

Device Posture Integration with Microsoft Intune is now generally available. For details, see [Microsoft Intune integration with Device Posture](#).

30 August 2023

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

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

28 August 2023

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

Device Posture service is now supported on iOS platforms. For details, see [Device Posture](#).

22 August 2023

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

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

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]

Device Posture service in test mode - Preview

May 24, 2024


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 required.

Note:

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

Enable test mode


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

**Enabling device posture will impact the subscriber experience**

Device posture scans all user devices before allowing users to log in. Users who have already logged in must have to relogin to enable device posture service to scan the subscriber devices.

If users have not installed the device posture app, they are prompted to download and install it.

Device posture will be enabled to subscribers in a few minutes (sometimes up to an hour) after it is enabled on the Device Posture page.

☒ Enable device posture in test mode (optional) 

☒ I understand the impact on subscriber experience.

Confirm and enable


Cancel

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.

Home > Identity and Access Management > Device Posture

Device Posture

Device posture is enabled (Test mode) 

Create device posture policies to enforce application access based on the end user's device

 Device Posture is enabled in test mode. Go to the Dashboard to view activity

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 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.

Test mode diagnostics

Admins can download the monitoring logs from the UI.

Enable test mode in production

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

1. On the home page, slide the **Device Posture is enabled** toggle switch OFF.
2. Select **I understand all device posture checks will be disabled**.
3. Click **confirm and disable**.
4. Now enable 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**.

CrowdStrike integration with Device Posture

February 22, 2024

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.

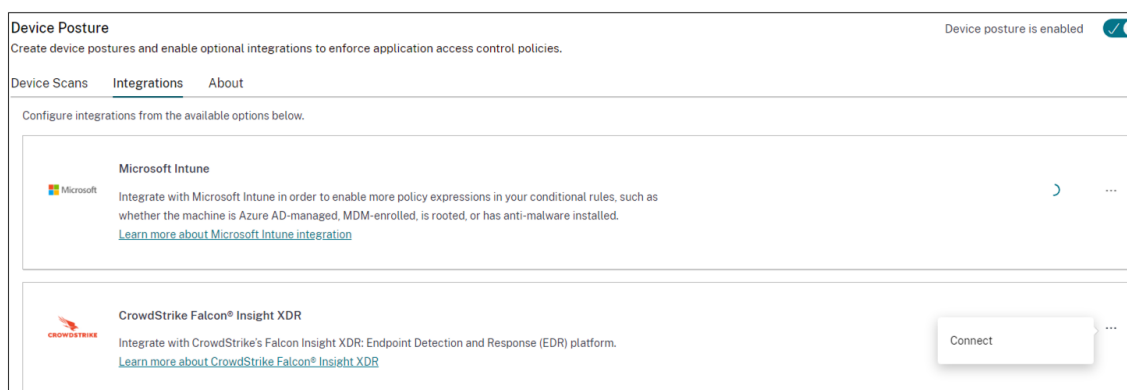
Step 1: Establish trust between Citrix Device Posture service and CrowdStrike ZTA service. This is a one-time activity.

Step 2: Configure policies to use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS and Citrix Secure Private Access resources.

Step 1: Establish trust between Citrix Device Posture service and CrowdStrike ZTA service

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

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



Note:

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

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

Note:

- You can obtain the ZTA API client ID and client secret from the CrowdStrike portal (**Support and resources > API clients and keys**).

- Ensure that you select the **Zero Trust Assessment** and **Host** scopes with read permissions for establishing the trust.

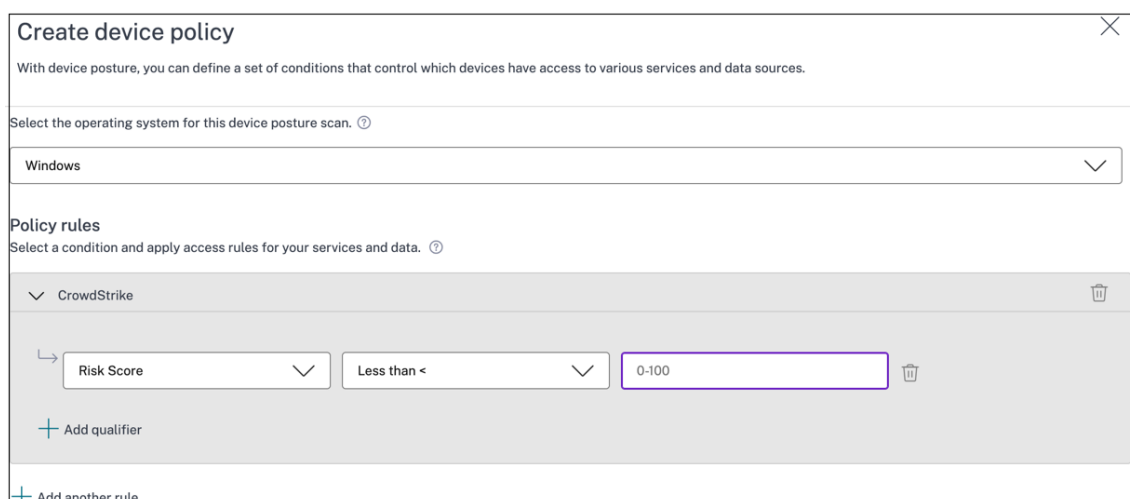
The integration is considered successful after the status changes from **Not Configured** to **Configured**.

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

Step 2: Configure device posture policies

Perform the following to configure policies to use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS and Citrix Secure Private Access resources.

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



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

Note:

You can use this rule with other rules that you configure for device posture.

6. In **Policy result** based on the conditions that you have configured, select one of the following.
 - **Compliant**
 - **Non-compliant**
 - **Denied login**

Policy result
If policy conditions and rules are met, the device scan will classify the user device as one of the following: ?

☒ **Compliant**
The device will be considered compliant and full access will be granted.

☐ **Non-compliant**
The device will be considered "non-compliant" and restricted access will be granted.

☐ **Denied access**
The device will be denied access to all resources.

Scan details
Name and set the priority order of this device scan. ?

Name *

crowdstrike-compliance-allow

Priority * ?

10

☒ Enable when created

Create

Cancel

7. Enter the name for the policy and set the priority.

8. Click **Create**.

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

References

[Device Posture service](#)

Microsoft Intune integration with Device Posture

February 26, 2024

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.

To configure Microsoft Intune integration

Intune integration configuration is a two-step process.

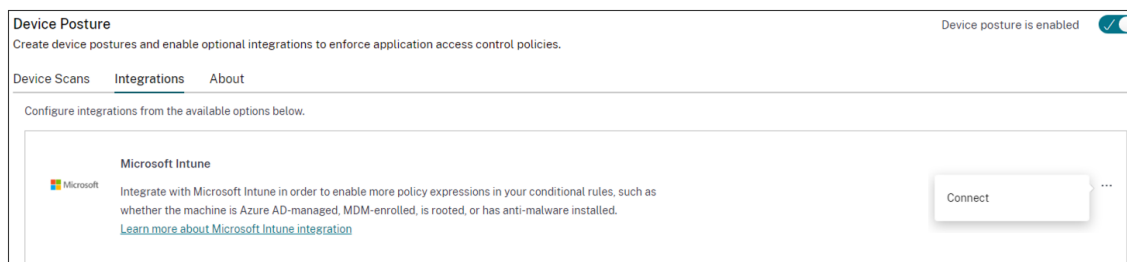
Step1: Integrate device posture with Microsoft Intune service. This is a one-time activity that you do to establish trust between Device Posture and Microsoft Intune.

Step 2: Configure policies to use Microsoft Intune information.

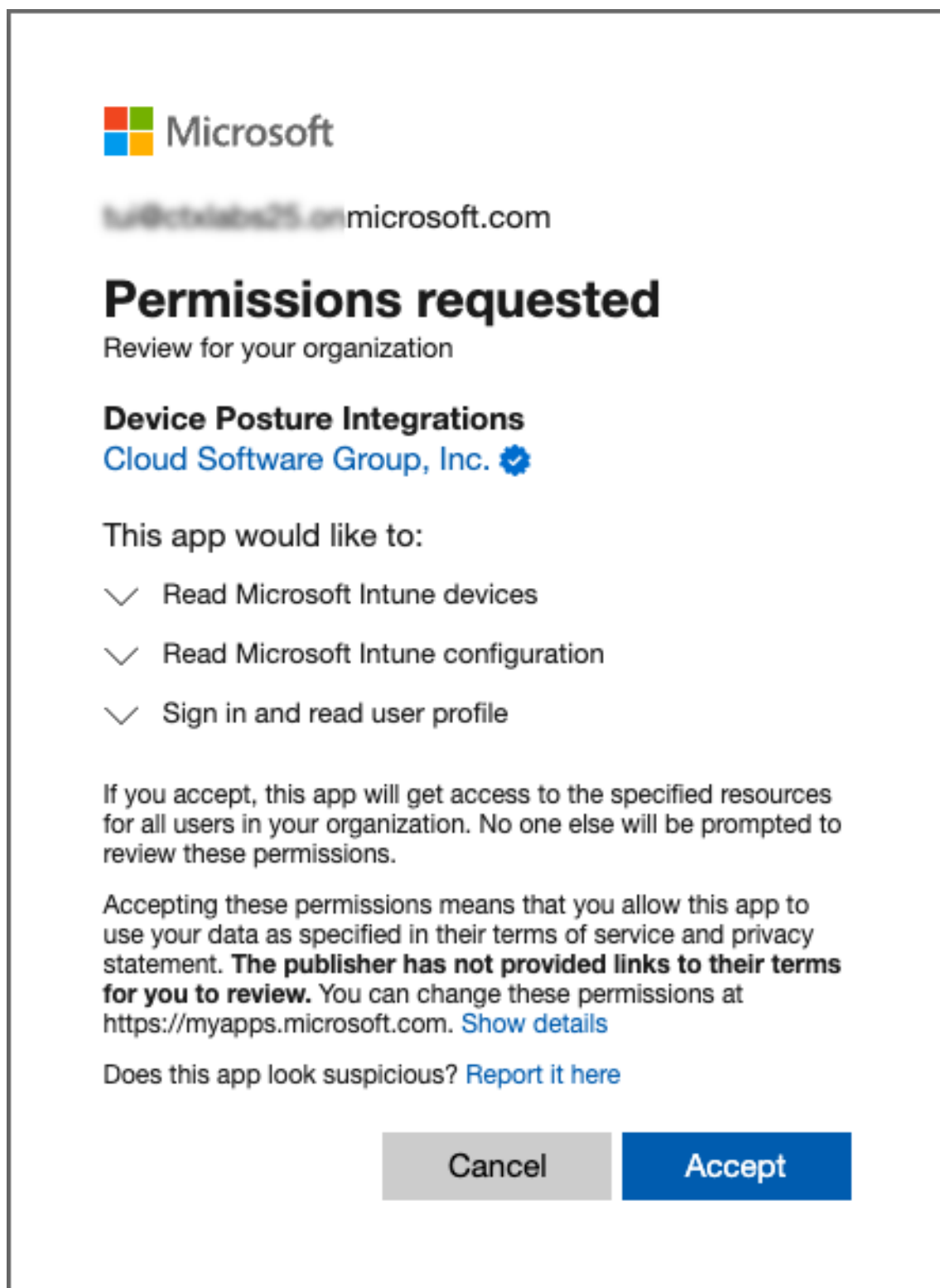
Step 1: Integrate device posture with Microsoft Intune

1. To access the **Integrations** tab, use one of the following methods:

- Access the URL <https://device-posture-config.cloud.com> on your browser, and then click the **Integrations** tab.
- Secure Private Access customers - On the Secure Private Access GUI, on the left side navigation pane, click **Device Posture**, and then click the **Integrations** tab.



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



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

Device Posture

API name	Claim value	Permission name	Type
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Read all managed devices	Application
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Read all service configuration for managed devices	Application

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

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

Step 2: Configure device posture policies

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

Create device policy

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

Platform

Select the operating system for this device posture scan. ?

Windows

Policy rules

Select a condition and apply access rules for your services and data. ?

Microsoft Intune

Matches all of

Compliant X Managed X

+ Add another rule

Policy result

If policy conditions and rules are met, the device scan will classify the user device as one of the following: ?

☒ Compliant

The device will be considered compliant and full access will be granted.

☐ Non-compliant

The device will be considered "non-compliant" and restricted access will be granted.

☐ Denied access

The device will be denied access to all resources.

Scan details

Name and set the priority order of this device scan. ?

Create

Cancel

2. Enter the name for the policy and set the priority.
3. Select the platform for which this policy is created.
4. In **Select Rule**, select **Microsoft Endpoint Manager**.
5. Select a condition, and then select the MEM tags to be matched.
 - **For Matches any of**, an OR condition is applied.
 - **For Matches all of**, an AND condition is applied.

Note:

You can use this rule with other rules that you configure for device posture.

6. In **Then the device is:** based on the conditions that you have configured, select one of the following.

- **Compliant (full access is granted)**
- **Non-compliant (Restricted access is granted)**
- **Denied login**

For more details about creating a policy, see [Configure device posture policy](#).

Device certificate check with Device Posture service

January 23, 2024

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

Points to note:

- Device Posture service supports only PEM issuer certificate type.
- For the device certificate check on Windows, the EPA client on the end device must be installed with administrative rights. For other checks, you do not require the local administrative rights. For details on the supported scans, see [Scans supported by device posture](#).
- To install the EPA client with administrative rights on Windows, run the following command in the location where the EPA client plug-in is downloaded.

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

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

```
1 Example: chain.pem
2
3 -----BEGIN CERTIFICATE-----
4 *****
5 -----END CERTIFICATE-----
6 -----BEGIN CERTIFICATE-----
7 *****
8 -----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**.

Import Issuer Certificate

Issuer certificate will be added to the Endpoint. View certificate details in certificate table once created.

Certificate Type *

PEM (Privacy Enhanced Mail)

Certificate File *

cgwsanitydc.pem

+ Choose Certificate

Import

Cancel

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

View imported certificates

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

Issuer Certificates

Issuer Certificates will be used to validate the device certificates as per the configured policies.

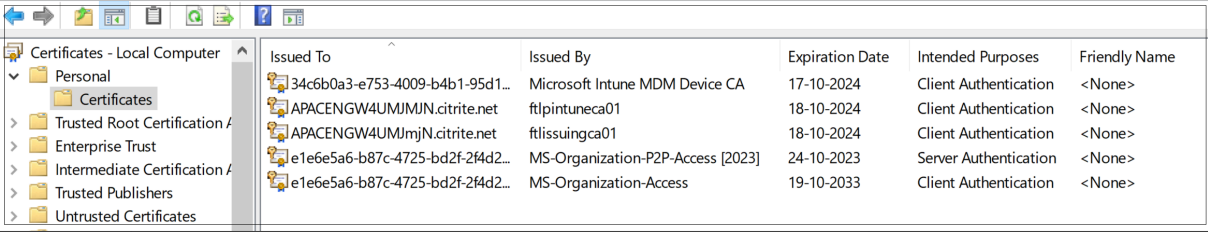
Import Issuer Certificate

Issuer	Certificates	Policies	Status	
cgwsanity-DC-CA	cgwsanitydc.pem	NA	Valid	
int-CA	combinedchain.pem	NA	Valid	

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.



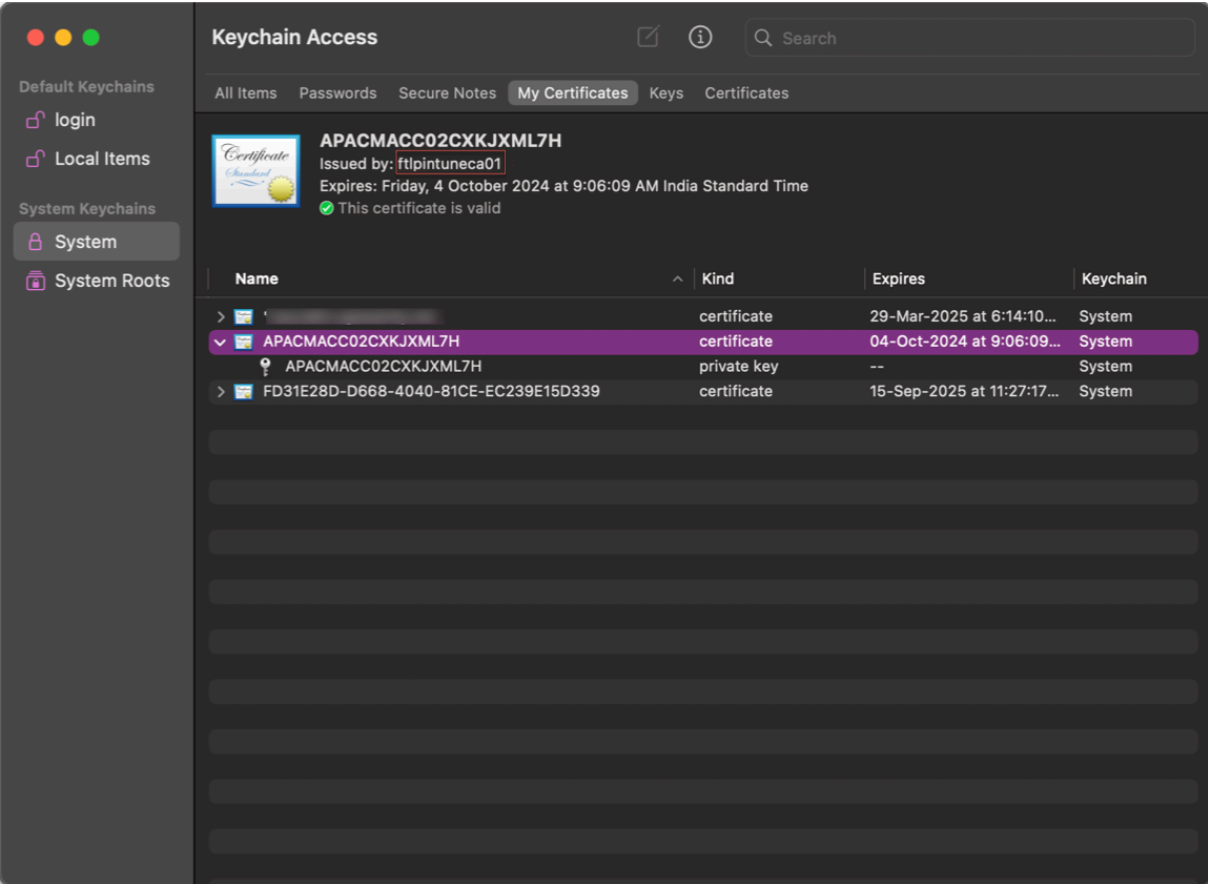
The screenshot shows the Windows Certificate Manager window. The left pane displays the hierarchy: Certificates - Local Computer > Personal > Certificates. The right pane shows a list of certificates with the following columns: Issued To, Issued By, Expiration Date, Intended Purposes, and Friendly Name.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
34c6b0a3-e753-4009-b4b1-95d1...	Microsoft Intune MDM Device CA	17-10-2024	Client Authentication	<None>
APACENGW4UMJMjN.citrite.net	ftlpintuneca01	18-10-2024	Client Authentication	<None>
APACENGW4UMJMjN.citrite.net	ftlissuingca01	18-10-2024	Client Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-P2P-Access [2023]	24-10-2023	Server Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-Access	19-10-2033	Client Authentication	<None>

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.



Enforce smart controls on DaaS using Device Posture

December 22, 2023

You can enforce smart controls while accessing the Citrix Desktop as a Service (DaaS) resources through the Citrix Device Posture service.

Note:

This is not an exhaustive configuration, but a sample on how to use Device Posture to configure Studio policies.

In this example, a policy is created to disable copy-paste functionality on Citrix DaaS resources using the Device Posture service tags (COMPLIANT and NON-COMPLIANT).

To disable copy-paste functionality for users coming from a NON-COMPLIANT device on Citrix DaaS, perform the following steps:

1. On the Citrix DaaS configuration page, Click the **Manage** tab.
2. Click the **Policies** tab.
3. Select **Create Policy**.
4. In **Select Settings**, select **Client Clipboard Redirection**.
5. In **Edit Setting**, select **Prohibited**, and then click **Save**.

Edit Setting
Client clipboard redirection

☐ Allowed
This setting will be allowed.

☒ Prohibited
This setting will be prohibited.

▼ **Description**
Allow or prevent the clipboard on the client device to be mapped to the clipboard on the server. By default, clipboard redirection is allowed.

To prevent cut-and-paste data transfer between a session and the local clipboard, select 'Prohibited'. Users can still cut and paste data between applications running in a session.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection using the Clipboard redirection bandwidth limit setting or the Bandwidth limit for clipboard redirection channel as percent of total session bandwidth setting.

▼ **Related settings**
Clipboard redirection bandwidth limit, Clipboard redirection bandwidth limit percent

Save **Cancel**

6. In the **Users and Machines** page, click **Filtered user and computers**, and then assign this policy to **Access Control**.

7. Go to **Filter for user settings only** and select **Access Control**.

Create Policy

Summary

Filters: 0 selected ☐ View selected only

Filter ↓	Value
<input type="checkbox"/> > Delivery Group	
<input type="checkbox"/> > Delivery Group type	
<input type="checkbox"/> > Organizational Unit (OU)	
<input type="checkbox"/> > Tag	
▼ Filters for user settings only	
<input type="checkbox"/> > Access control	
<input type="checkbox"/> > Citrix SD-WAN	
<input type="checkbox"/> > Client IP address	
<input type="checkbox"/> > Client name	
<input type="checkbox"/> > User or group	

Back Next Cancel

8. In the **Assign Policy** page, leave the default settings for **Mode** and **Connection Type**.

In **Gateway farm name**, enter **Workspace** and in **Access Condition**, enter **NON-COMPLIANT**.

Assign Policy

Access control

Apply policy based on the access control conditions through which a client connects.

Access control elements:

Mode	Connection type	Gateway farm name	Access condition		
Allow	With Citrix Gateway	Workspace	NON-COMPLIANT	+	<input checked="" type="checkbox"/> Enable

Save Cancel

9. Enter a name for the policy. Consider naming the policy according to who or what it affects, for example *Restricted Clipboard Access for non-compliant devices*. Optionally, add a description.
10. Click **Finish**.

Note:

The policy is disabled by default. Enabling the policy allows it to be applied immediately for the users logging on. Disabling prevents the policy from being applied. If you must prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

How to validate your policy configuration

Validate your policies to make sure that they are working as intended before widely implementing these policies. In the configuration example:

- For the users coming from a COMPLIANT end device, Citrix DaaS resources must be enumerated without the copy-paste restrictions.
- For the users coming from a NON-COMPLIANT end device, Citrix DaaS resources must be enumerated with the copy-paste restrictions.

Monitor and troubleshoot

May 30, 2024

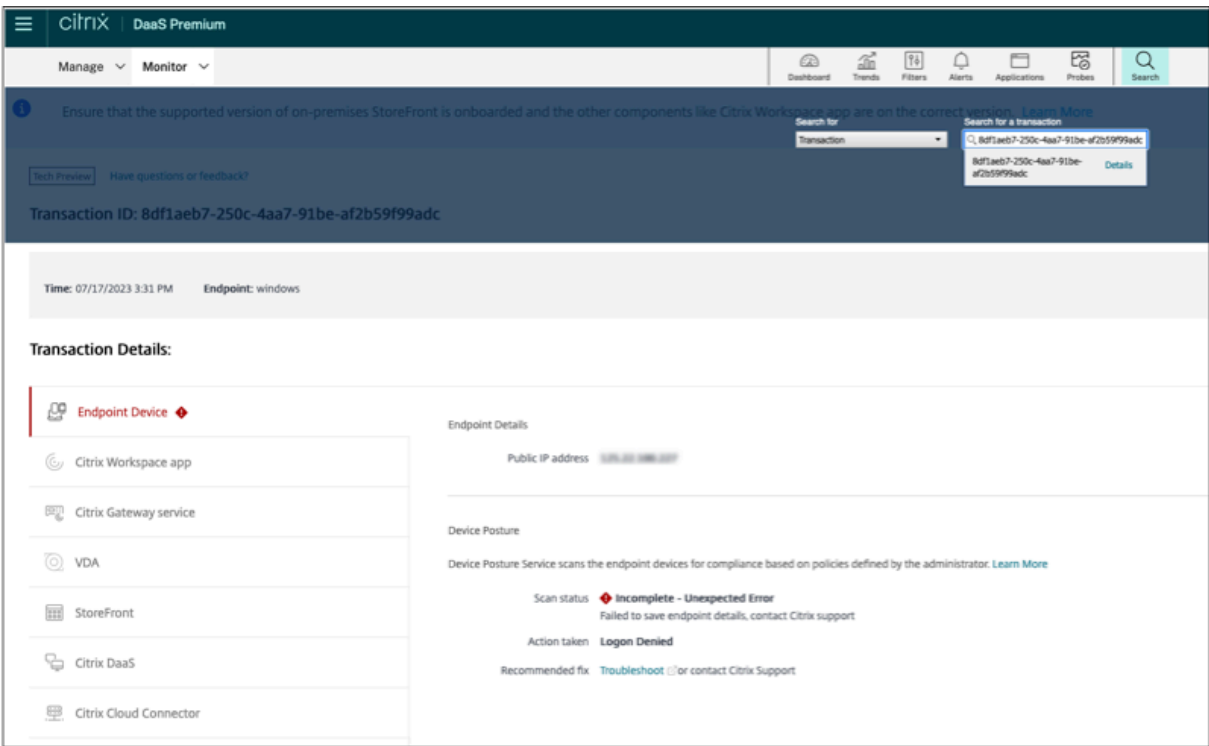
Device posture event logs can be viewed at two places:

- Citrix DaaS Monitor
- Citrix Secure Private Access dashboard

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**.



Device posture events on Secure Private Access dashboard

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

- 1. Sign into Citrix Cloud.
- 2. On the Secure Private Access tile, click **Manage** and then click **Dashboard**.
- 3. Click the **See more** link in the **Diagnostic Logs** chart to view the device posture event logs.

Diagnostic Logs (26198) Device Posture Logs (41)

Filters: Clear All

POLICY RESULT

- ☐ Compliant
- ☐ Non-Compliant
- ☐ Login Denied

Policy-Info = "Key-Word" Last 1 Week Search

Results are limited to the first 1000 records. Narrow your search criteria for more relevant results. Export to CSV format

TIME (UTC)	POLICY INFO	POLICY RESULT	STATUS	OPERATING SYSTEM	TRANSACTION ID	DESCRIPTION	INFO CODE
Tue, 11 Apr 2023 11:47:...	NoMatchingPolicy	Non-Compliant	Success	Windows	85562ba3-71c8-4839...		
Tue, 11 Apr 2023 11:45:...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:45:...	NoMatchingPolicy	Non-Compliant	Success	Windows	a418a959-e7cd-4a9d...		
Tue, 11 Apr 2023 11:44:...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:44:...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:43:...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:42:...	ms-MEM	Compliant	Success	Windows	cb57315f-48f7-45cb...		

- Admins can filter the logs based on the transaction ID in the Diagnostic logs chart. 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 for resolving the issue.

- 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/EPAPugin/EpaCloud.log
 - ~/Library/Application Support/Citrix/EPAPugin/epapugin.log

Device posture error logs

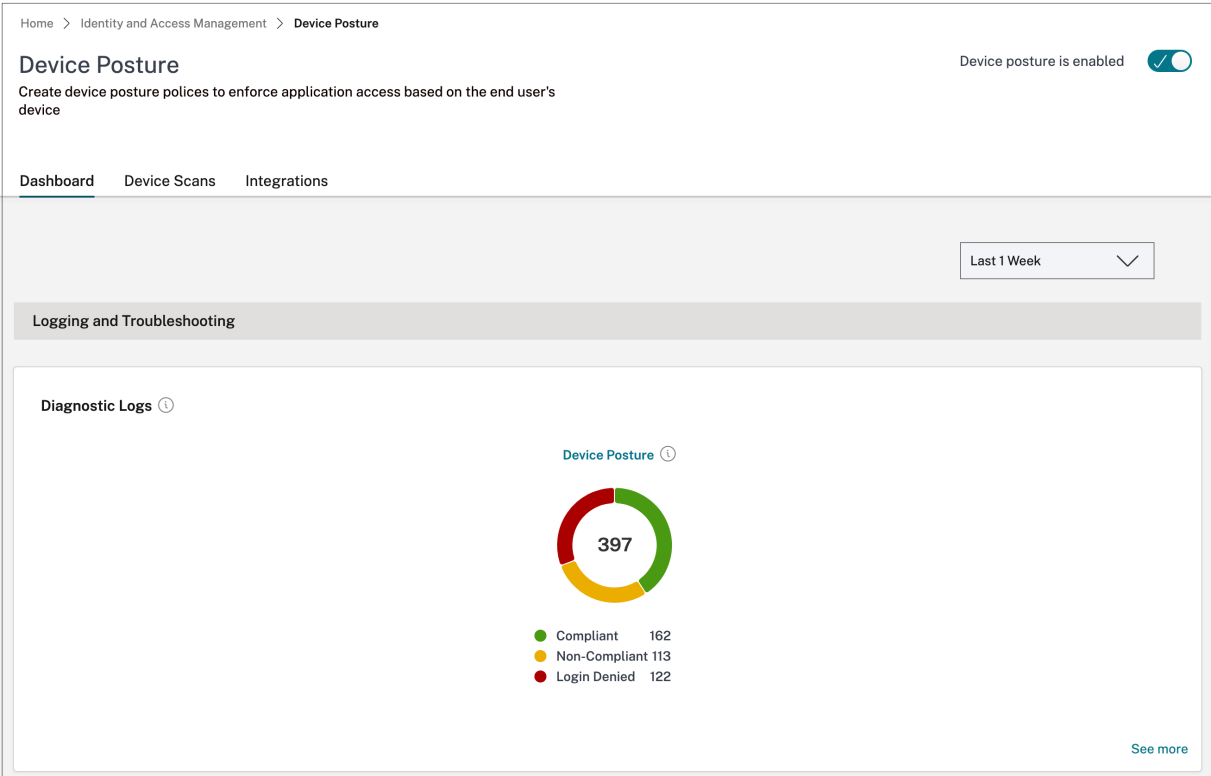
The following logs related to the Device Posture service can be viewed on the Citrix Monitor and Secure Private Access dashboard. For all these logs, it's recommended that you contact Citrix Support for resolution.

- 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 logs

May 12, 2024

You can use the dashboard in the Device Posture service portal for monitoring and troubleshooting purposes. To view the Device Posture service dashboard, click the **Dashboard** tab on Device Posture home page. The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service. You can 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**).



Note:

Device posture logs are also captured in the Secure Private Access service dashboard. To view the device posture logs, click the **Device Posture Logs** tab. You can refine your search based on the policy results (**Compliant**, **Non-compliant**, and **login Denied**). For more details, see [Diagnostic logs](#).

Manage Citrix Endpoint Analysis client for Device Posture service

February 28, 2024

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

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

Installation of the EPA client

During runtime, the Device Posture service prompts the end user to download and install the EPA client during run-time. For details, see [End-user flow](#).

Usually, an EPA client does not require local admin rights to download and install on an endpoint. However, to run device certificate check scans on an end device, the EPA client must be installed with administrator access. For details about installing an EPA client with administrator access, see [Install device certificate on the end device](#).

Upgrade of the EPA client for Windows

When a new version of the EPA client is released, the EPA clients for Windows are upgraded by default after the first installation. Auto-upgrade ensures that the end-user devices are always running on the latest version of the EPA client that is compatible with the Device Posture service. For the auto-upgrade, the EPA client must have been installed with administrator access.

Note:

Auto-upgrade is in preview. Sign up for the preview using <https://podio.com/webforms/29214695/2384946>.

Distribution of the EPA client

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

- **EPA client installer integrated with Citrix Workspace app:** The EPA client installer is integrated with Citrix Workspace app 2402 LTSR for Windows. This integration eliminates the need for the end users to install EPA client separately after installing Citrix Workspace app.

To install the EPA client as part of Citrix Workspace app, use the command line option `InstallEPAClient`. For example, `./CitrixworkspaceApp.exe InstallEPAClient`.

Note:

- EPA client installation as part of Citrix Workspace app is disabled, by default. It must be explicitly enabled by using the command line option `InstallEPAClient`.
- If an end device already has an EPA client installed and the end user installs Citrix Workspace app, the existing EPA client is upgraded.
- If an end user uninstalls Citrix Workspace app, then the integrated EPA client is also removed from the device, by default. However, if the EPA client was not installed as

part of the integrated Citrix Workspace app installation, then the existing EPA client is retained in the device.

- The EPA client installer integrated with Citrix Workspace app can also be used with NetScaler. For details, see [Manage EPA client when used with NetScaler and Device Posture](#).

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

Note:

- GACS is supported on Windows devices only for distributing the EPA client.
- To manage an EPA client through GACS, install Citrix Workspace Application (CWA) on the end devices.
- If CWA is installed with administrator privileges on an end user device, then GACS installs the EPA client with the same administrator privileges.
- If CWA is installed with user privileges on an end user device, then GACS installs the EPA client with the same user privileges.

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

Manage EPA client when used with NetScaler and Device Posture

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

- NetScaler based Adaptive Authentication with EPA
- NetScaler based on-prem gateway with EPA

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

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

For more information, see [Plug-in behaviors](#).

Considerations when EPA client is used with NetScaler and Device Posture

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

- If you have configured EPA with Adaptive Authentication or on-premises authentication or gateway virtual server, it is recommended that you disable version control of the EPA client on NetScaler. This is done to ensure that the GACS or Device Posture service does not push the latest version of the EPA client to the end devices.
- The EPA version control can be set to **Never** by using the CLI or the GUI. These configuration changes are supported on NetScaler 13.x and later versions.
 - CLI: Use the CLI commands for Adaptive Authentication and on-premises authentication virtual server.
 - GUI: Use the GUI for the on-premises gateway virtual server. For details, see [Control upgrade of Citrix Secure Access clients](#).

Sample CLI commands:

```
1 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;\""
2
3 add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS(\"
  pluginlist.xml\")" <rewrite_action_name>
4
5 bind authentication vserver <Authentication_Vserver_Name> -policy <
  rewrite_action_policy> -priority 10 -type RESPONSE
6 <!--NeedCopy-->
```

Data Governance

December 22, 2023

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

Data residency

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

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

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

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

Data collection

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

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

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

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

Data transmission

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

Data control

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

Data retention

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

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

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

Data export

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

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

Definitions

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



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).