# Device Posture

# Contents



# Device Posture

March 25, 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). 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 entitlement for Citrix Device Posture service is part of Citrix DaaS Premium, Citrix DaaS Premium Plus, and Citrix Secure Private Access Advanced licenses. Customers with other licenses can purchase a Device Posture Service entitlement as an add-on. For an add-on, customers must purchase a standalone Adaptive Authentication SKU, but don't necessarily have to deploy it to use the Device Posture service.
- Supported platforms:
  - Windows (10 and 11)
  - macOS 13 Ventura
  - macOS 12 Monterey
  - iOS
  - IGEL

> **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.
> - 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 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.
> - For IGEL OS support on the Device Posture service, the EPA client is built in as part of the IGEL OS. Contact the IGEL support team for installing the EPA client on the IGEL

> devices.

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

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

- Supported browsers: Chrome, Edge, and Firefox.
- Firewall configuration: To allow the Device Posture service to update the EPA clients on an end device, the firewall/proxy must be 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
  - *.citrixworkspacesapi.net

### Preview features

Device Posture service with IGEL. Sign up for the preview using https://podio.com/webforms/29062020/2362942.

### 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.

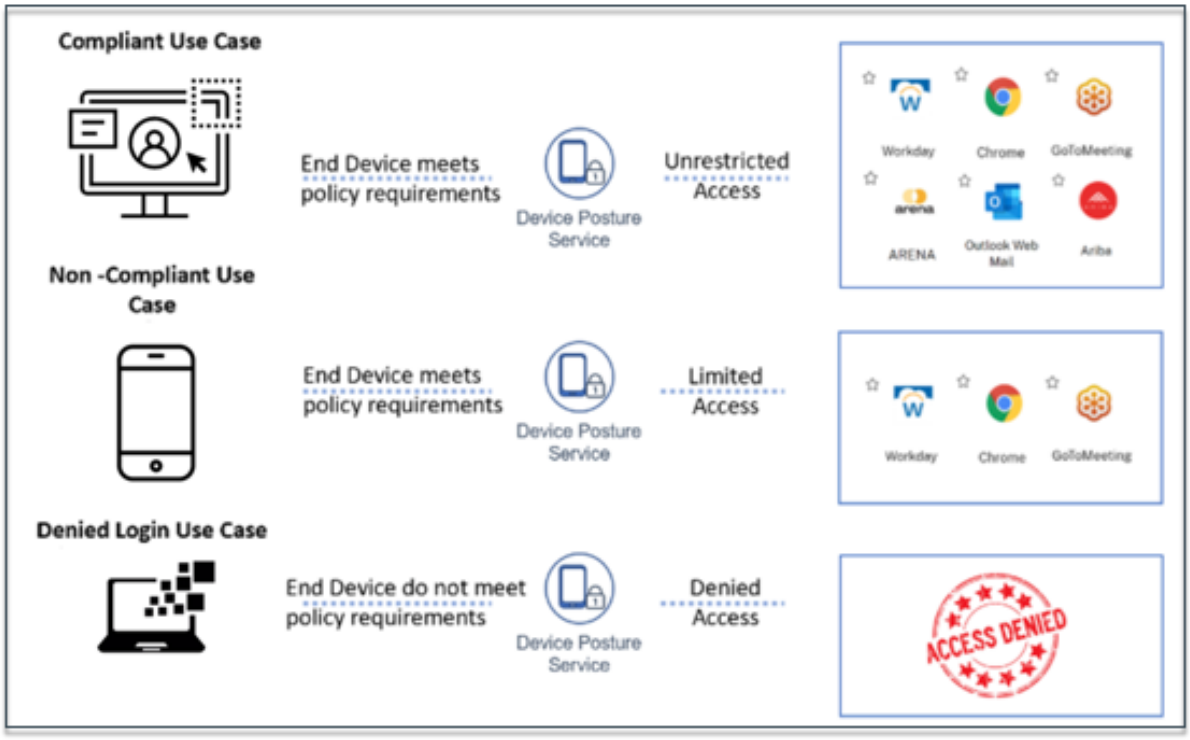
Following are the high-level conditions used to classify a device as compliant, non-compliant, and denied login.

- **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.
- **Denied login:** - A device that fails to meet the policy requirements is denied login.

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




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

## Scans supported by device posture

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

| Windows | macOS | iOS | IGEL |
|---|---|---|---|
| Citrix Workspace app version | Citrix Workspace app version | Citrix Workspace app version | - |
| Operating System version | Operating System version | Operating System version | - |
| File (exists, file name, and path) | File (exists, file name, and path) | - | File (exists, file name, and path) |
| Geolocation | Geolocation | - | - |
| Network location | Network location | - | - |
| MAC Address | MAC Address | - | - |
| Process (exists) | Process (exists) | - | - |
| Microsoft Endpoint Manager | Microsoft Endpoint Manager | - | - |
| CrowdStrike | CrowdStrike | - | - |
| Device Certificate | Device Certificate | - | - |
| Browser | Browser | - | - |
| Antivirus | Antivirus | - | - |
| Non-Numeric Registry (32 Bit) | - | - | - |
| Non-Numeric Registry (64 Bit) | - | - | - |
| Numeric Registry (32 Bit) | - | - | - |
| Numeric Registry (64 Bit) | - | - | - |
| Windows Update Installation Type | - | - | - |
| Windows Update Installation Last Update check | - | - | - |

**Note:**

- The browser and antivirus checks are in preview.
- For iOS support on Device Posture service, the EPA client is built in as part of the Citrix Work-

> space app for iOS. For details on the versions, see Citrix Workspace app for iOS.

### Third-party integration with device posture

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.

### Configure device posture

The 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**.

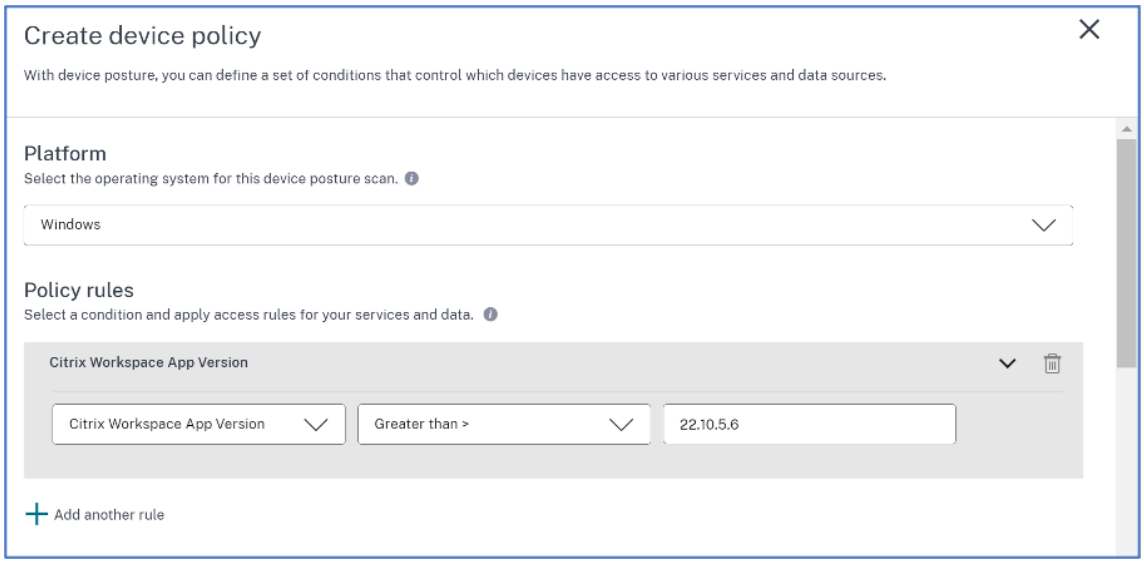
   > **Note:**
   >
   > - Secure Private Access service customers can directly click **Device Posture** on the left navigation in the admin user interface.
   > - For the first-time users, the Device Posture landing page prompts you to create a device posture policy. Device posture policy must individually 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:**
>
> - For 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, see Import device certificate while creating the policy for device certificate and Upload device certificate.
> - For the device certificate check, 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.

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




7. In **Policy result** based on the conditions that you've configured, select the type under which the device scan must classify the user device.

   - Compliant
   - Non-compliant
   - Denied access

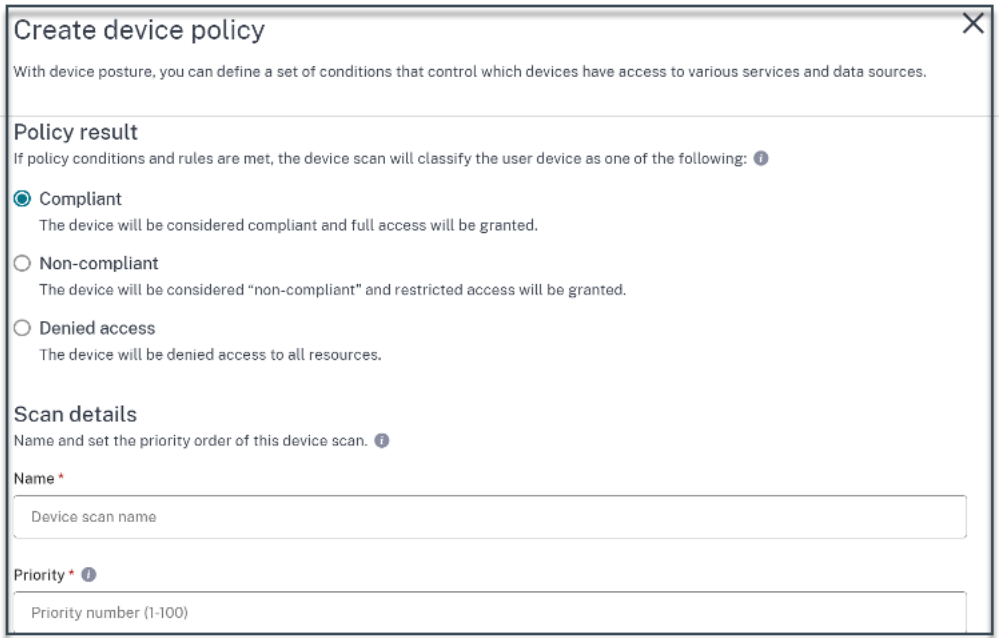
8. Enter a name for the policy.

9. In **Priority**, enter the order in which the policies must be evaluated.

   - You can enter a value between 1 through 100. It's recommended that you configure deny policies with higher priority, followed by non-compliant, and finally compliant.
   - The priority with the lower value has the highest preference.
   - Only the policies that are enabled are evaluated based on the priority.

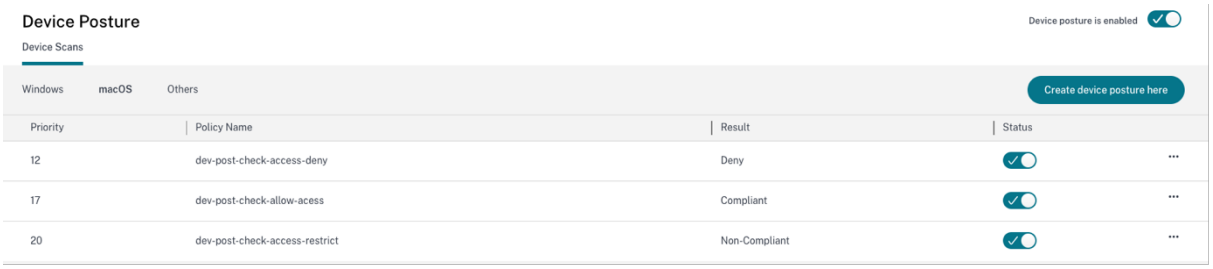
10. Click **Create**.




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

### 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 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

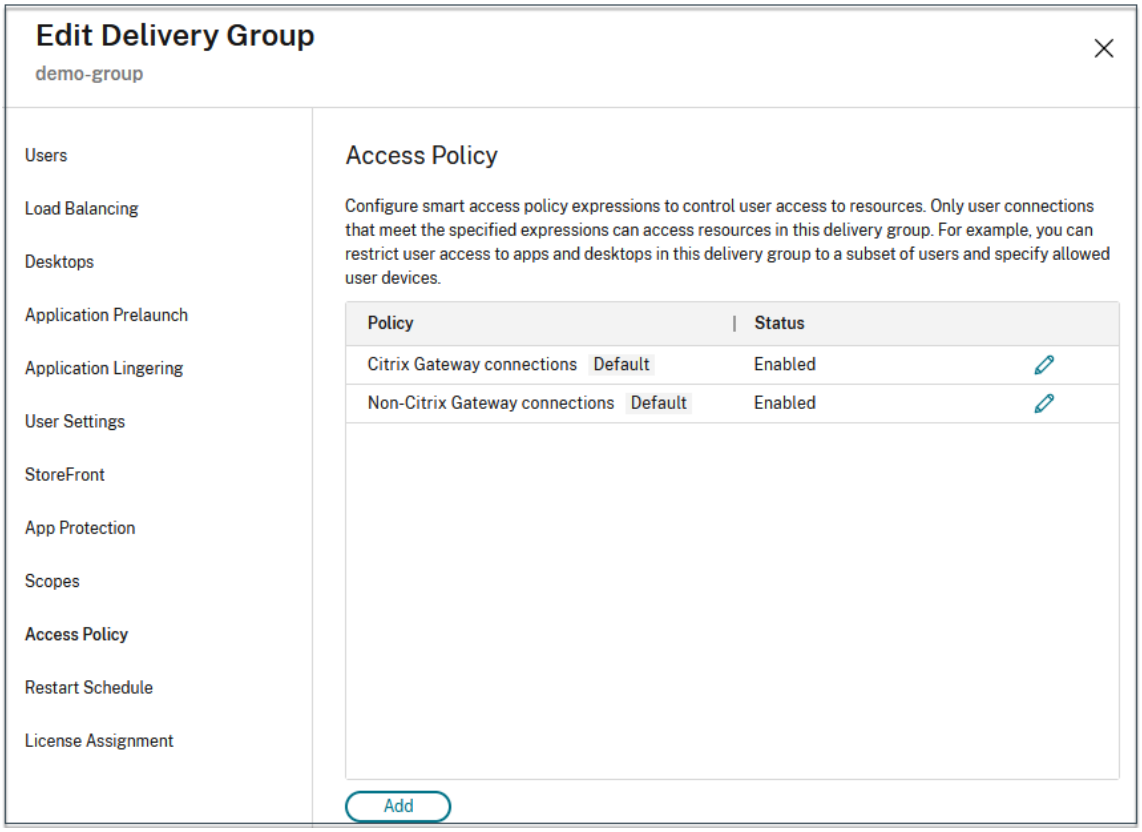
 

Access service and is used to provide contextual access based on device posture. Therefore, Citrix DaaS and Citrix Secure Private Access must be configured to enforce access control using device posture tags.

### Citrix DaaS configuration with Device Posture

Sign up for the preview.

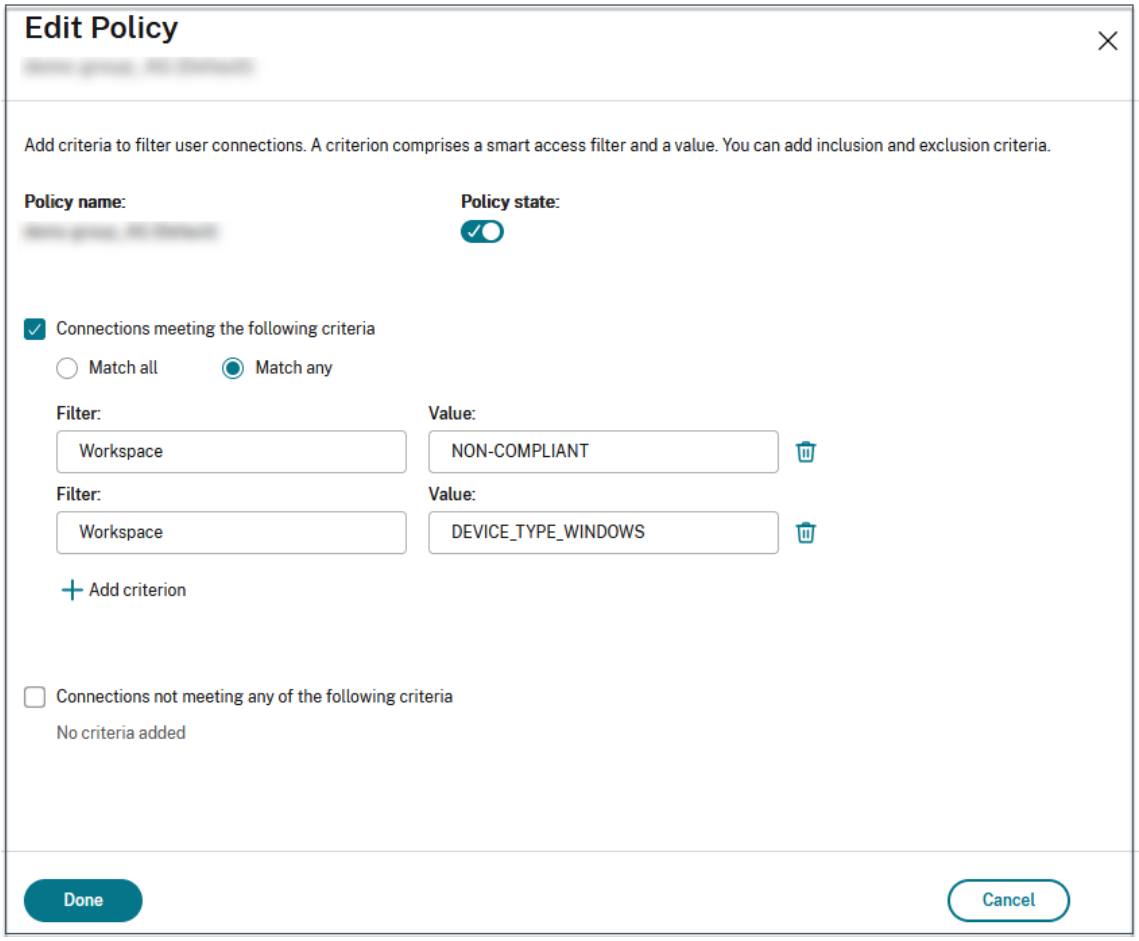
1. Sign into Citrix Cloud.
2. On the **DaaS** tile, click **Manage**.
3. Go to the **Delivery Group** section from the left-hand menu.
4. Select the delivery group for which you want to configure access control based on device posture and click **Edit**.
5. In the **Edit Delivery Group** page, click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




   a) On the Edit policy page, select **Connections meeting the following criteria.**
   b) Select **Match any**, and then click **Add criterion**.

c) Add criteria for all location tags you configured in Configure network locations: Type **Workspace** for **Filter** and **COMPLIANT** or **NON-COMPLIANT** for **Value**.




> **Note:**
>
> The syntax for the device classification tags must be entered in the same manner 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**

1. Sign into Citrix Cloud.

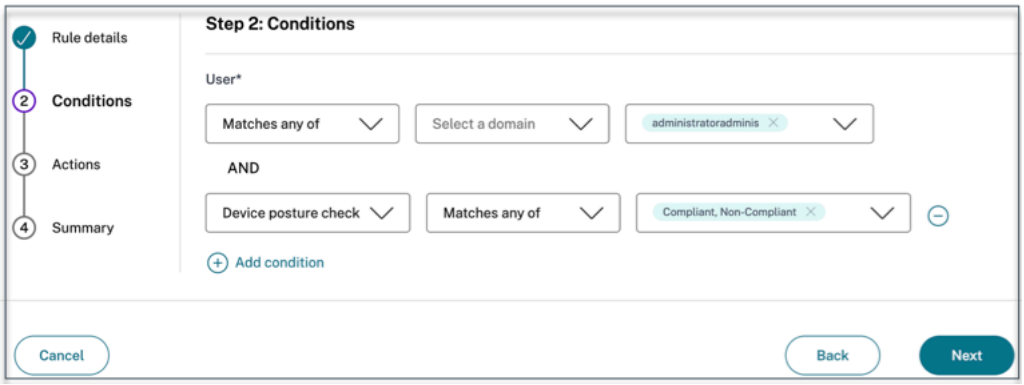
 

2. On the Secure Private Access tile, click **Manage**.
3. Click **Access Policies** on the left navigation and then click **Create policy**.
4. Enter the policy name and description of the policy.
5. In **Applications**, select the app or set of apps on which this policy must be enforced.
6. Click **Create 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
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.



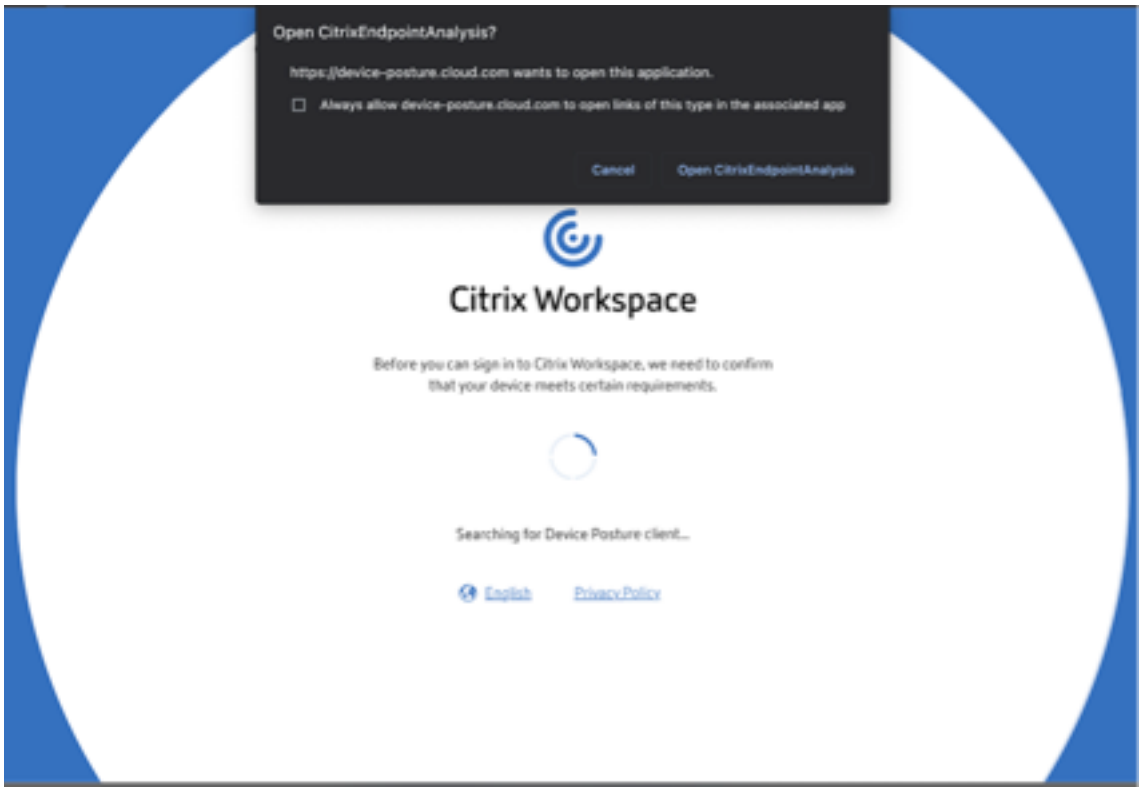
## End-user flow

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

### End-user flow via browser access

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

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




- When the end user clicks **Open Citrix End Point Analysis**, the device posture client runs and scans the endpoint parameters based on device posture policy requirements.
- If the latest device posture client isn't installed on the endpoint, the users are redirected to the page that displays the options **Check again** and **Download Client**. The user must click **Download Client**.
- If the latest device posture client is already installed on the endpoint, the user must click **Check again**.


**End-user flow via Citrix Workspace application**

- When an end-user logs on to the Citrix Workspace URL `https://your-workspace-url` through the Citrix Workspace application, the device posture client installed on the endpoint runs and scans the endpoint parameters based on device posture policy requirements.
- If the latest device posture client isn't installed on the endpoint, the users are redirected to the page that displays the options, **Check again** and **Download Client**. The user must click **Download Client**.
- If the latest device posture client is already installed on the endpoint, the user must click **Check again**.

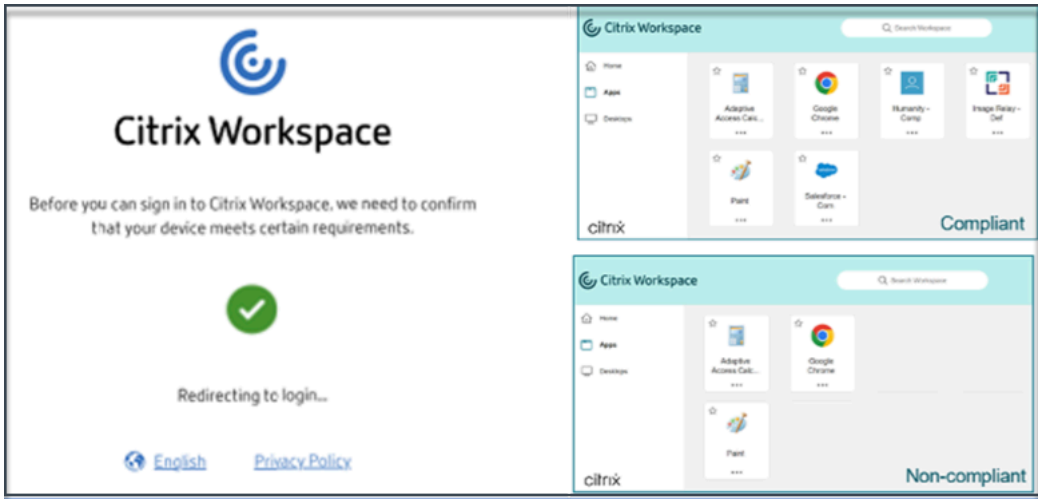
**End-user flow - Device posture results**

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

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

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




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


**Customized messages for access denied scenarios (Preview)** Admins have the option to customize the message that is displayed on the end device when an access is denied.

This feature is under preview. Sign up for the preview using https://podio.com/webforms/29219975/2385710.

Perform the following steps to add customized messages:

1. Navigate to the **Device Posture > Device Scans** page.
2. Click **Settings**.
3. Click **Edit** and in the **Message** box, enter the message that must be displayed in access denied scenarios. You can enter a maximum of 256 characters.

4. Click **Enable custom message on save** to enforce the option of displaying the custom message. If you do not select this checkbox, the custom message is created but not displayed on the devices in access denied scenarios.

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

5. Click **Save**.

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

## Monitor and troubleshoot Device Posture events

Device posture event logs can be viewed at two places:

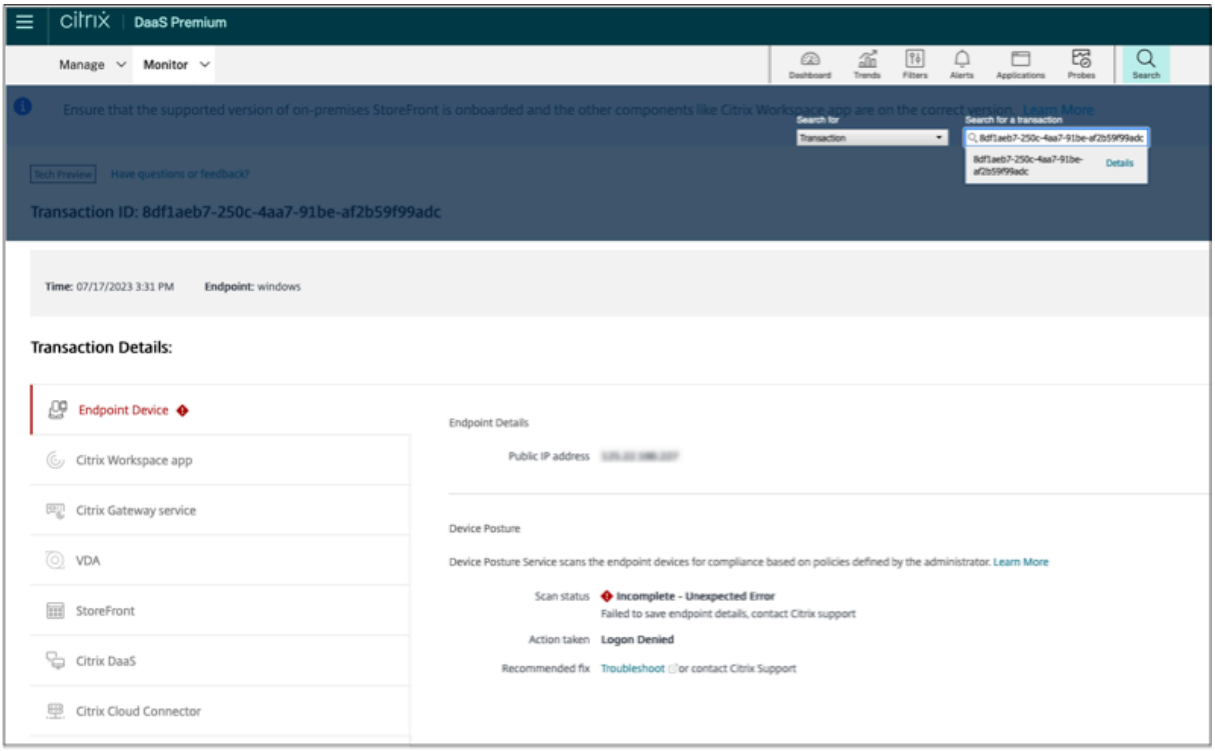
- Citrix DaaS Monitor
- Citrix Secure Private Access dashboard

### 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.
4. In the Monitor UI, search for the 32-digit transaction ID and click **Details**.

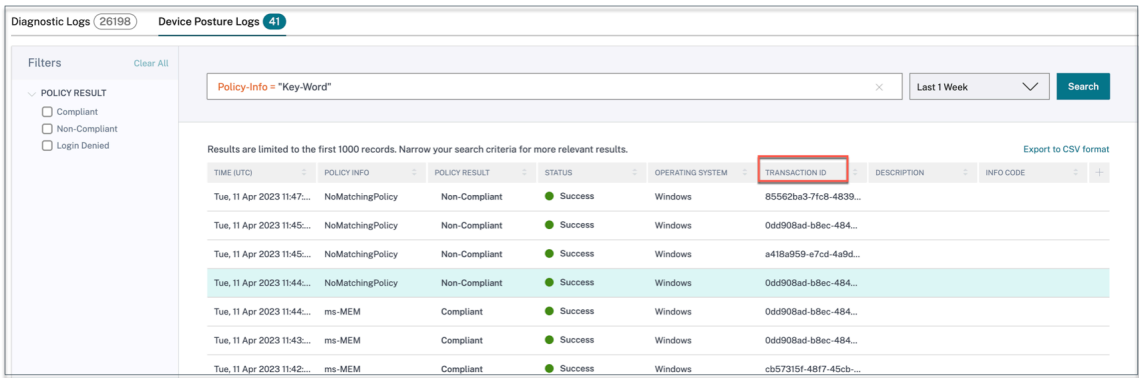
 




### Device posture events on Secure Private Access dashboard

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**.
3. Go to the Dashboard section from the left-hand menu.
4. Click the **See more** link in the **Diagnostic Logs** chart to view the device posture event logs.




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

## 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.

## 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.

## 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.

## What's new

March 25, 2024

### 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. For details, 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]

## 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.

**Step1:** Establish trust between Citrix Device Posture service and CrowdStrike ZTA service. This is a one-time activity.

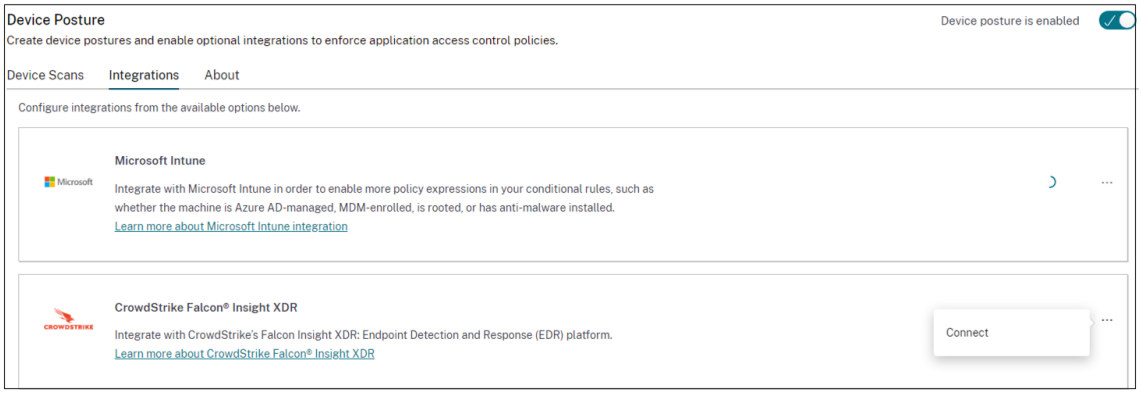
**Step 2:** Configure policies to use the CrowdStrike ZTA score as a rule to provide smart access to Citrix DaaS and Citrix Secure Private Access resources.

### 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**.

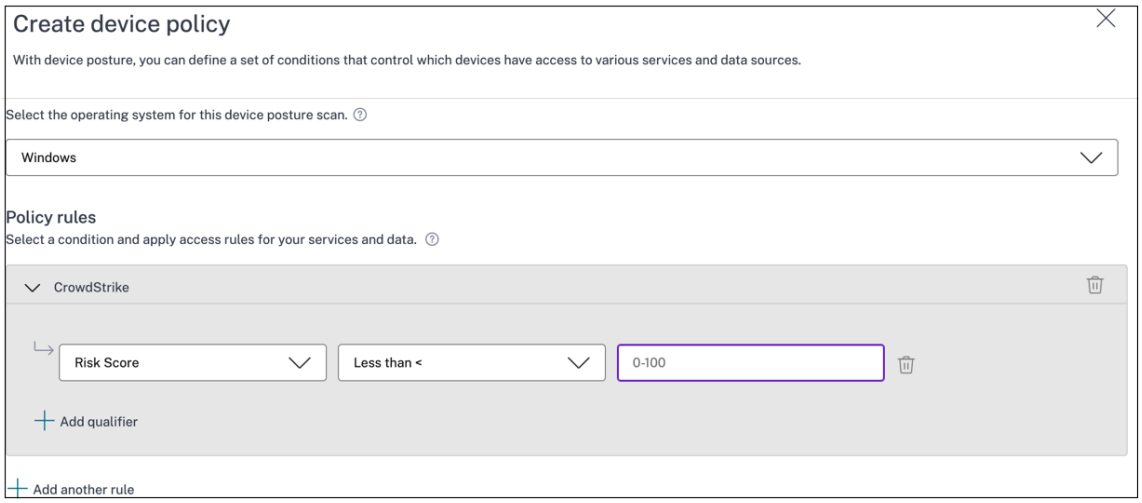
If the integration is not successful, the status appears as **Pending**. You must click the ellipsis button, and then click **Reconnect**.

### 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**.



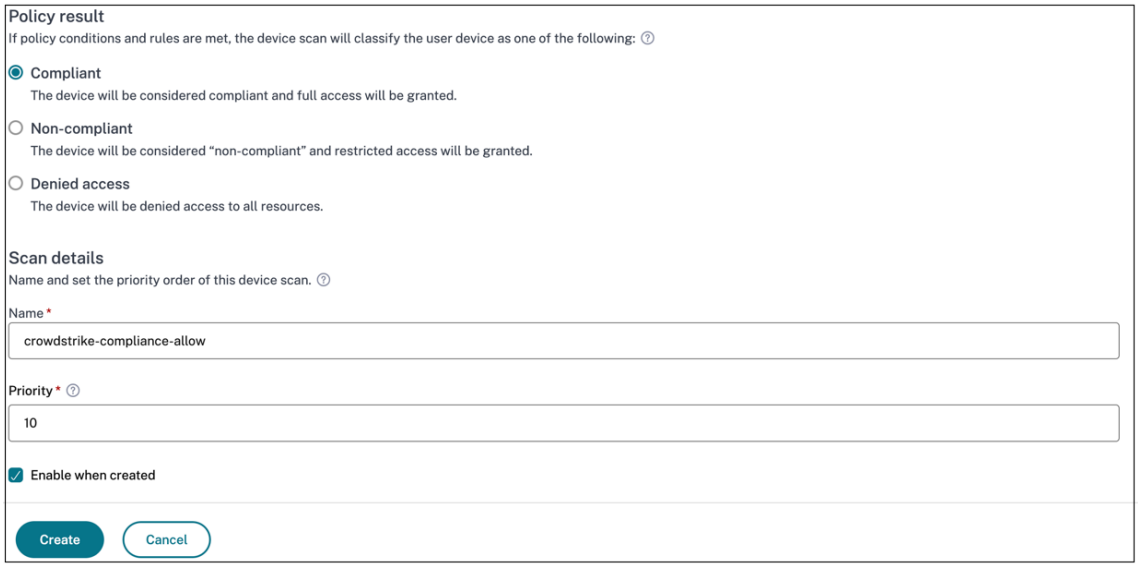

2. Select the platform for which this policy is created.
3. In **Policy Rule**, select **CrowdStrike**.
4. For the **Risk Score** qualifier, select the condition, and then enter the risk score.
5. Click **+** to add a qualifier that checks if the CrowdStrike Falcon sensor is running.

   > **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**




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

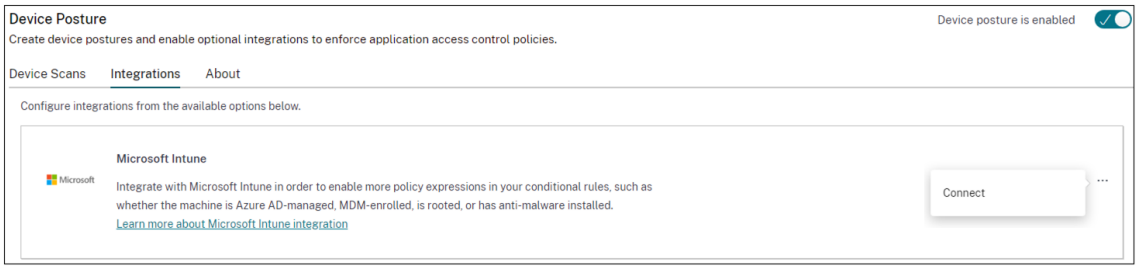
Intune integration configuration is a two-step process.

**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.

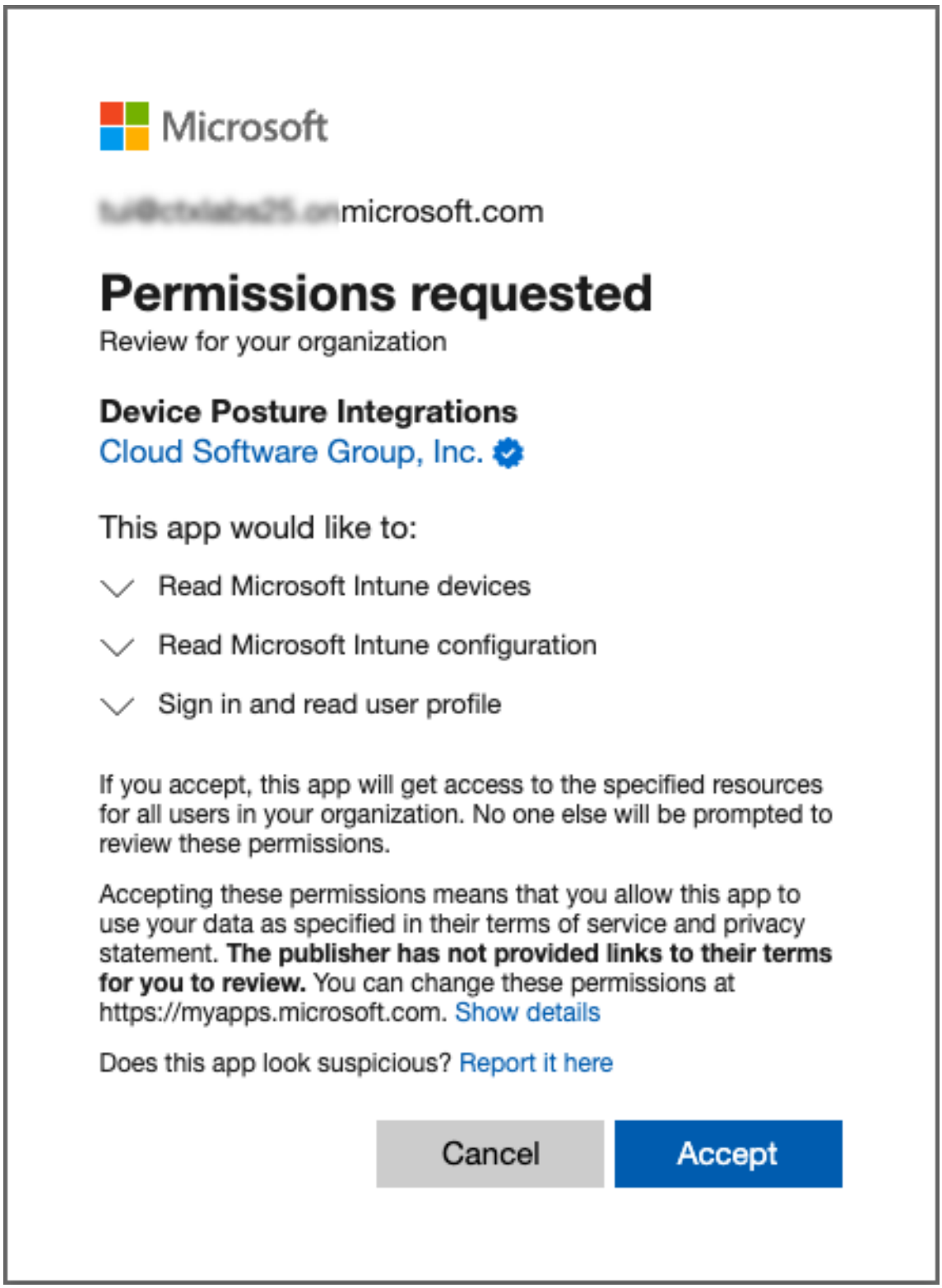
### Step 1: Integrate device posture with Microsoft Intune

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.

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

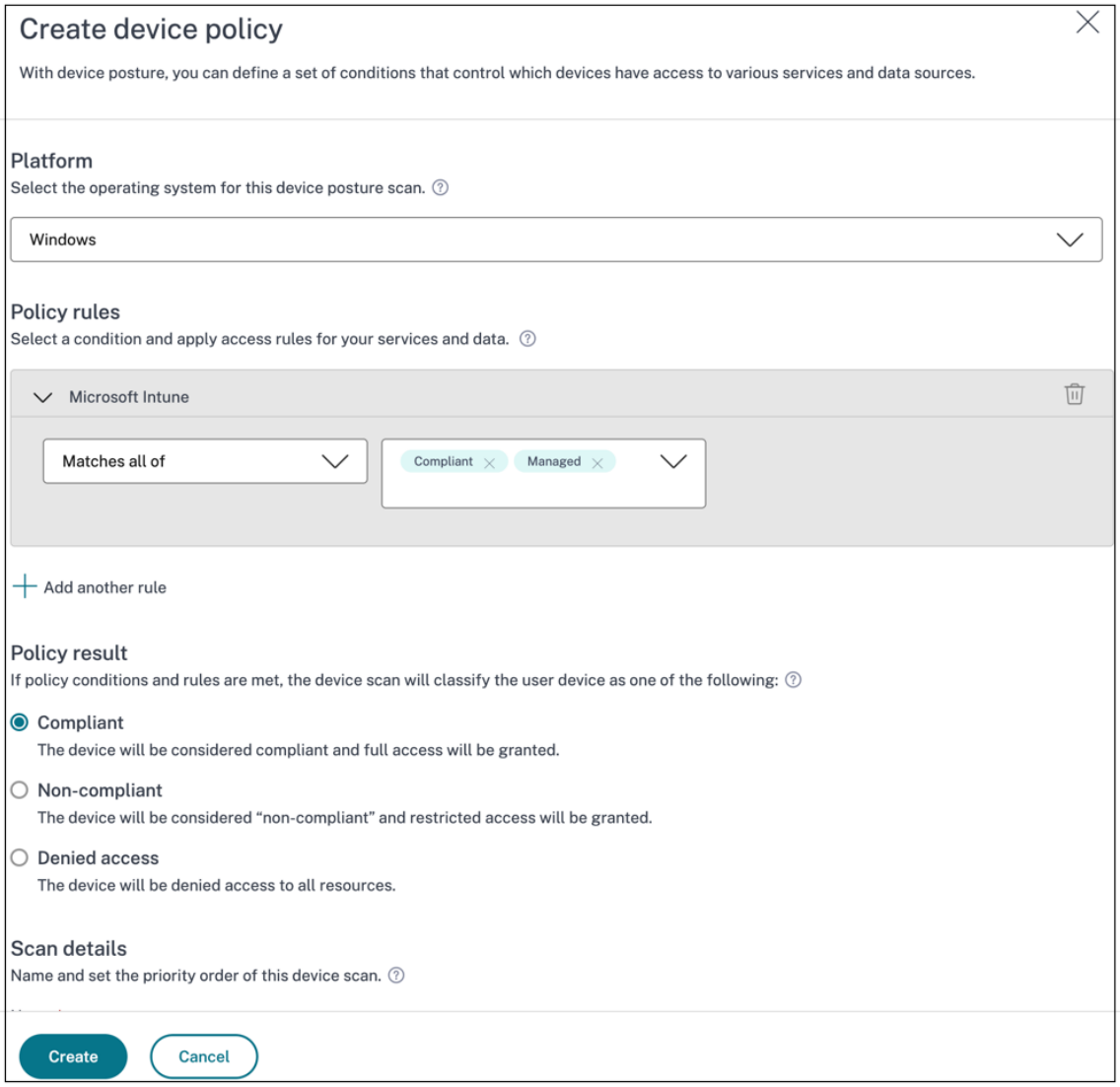
After the integration status changes from **Not Configured** to **Configured**, admins can create a device posture policy.

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

**Step 2: Configure device posture policies**

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




2. Enter the name for the policy and set the priority.
3. Select the platform for which this policy is created.
4. In **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.

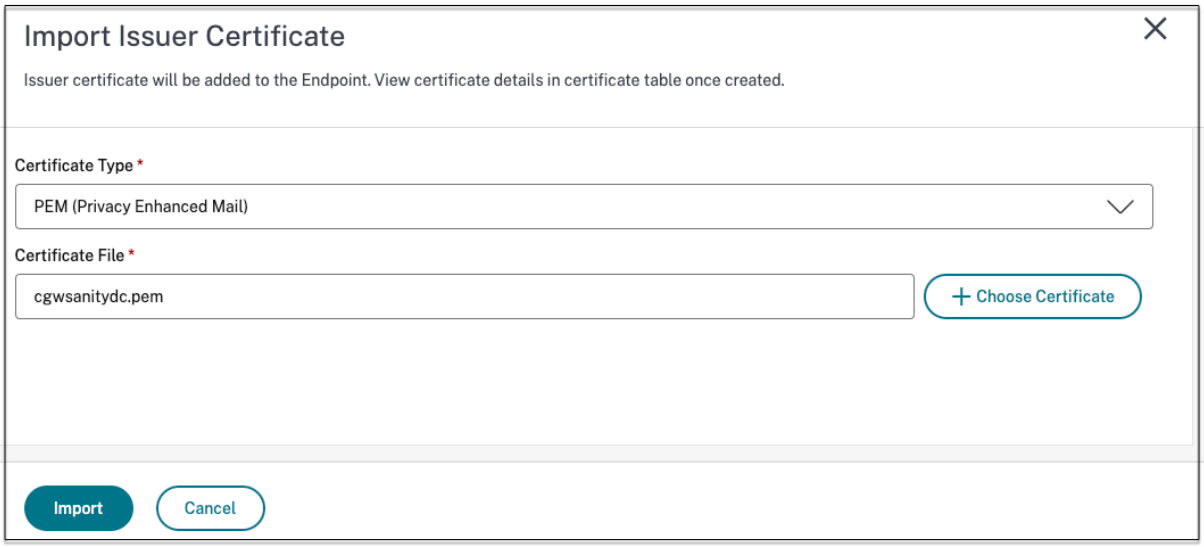
> **Points to note:**
>
> - Device Posture service supports only PEM issuer certificate type.
> - For the device certificate check on Windows, the EPA client on the end device must be installed with administrative rights. For other checks, you do not require the local administrative rights. For details 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.
>
> ```
> Example: chain.pem
>
> -----BEGIN CERTIFICATE-----
> ******************************
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
> ******************************
> -----END CERTIFICATE
> ```

### Upload device certificate

1. Click **Settings** on the Device Posture home page.

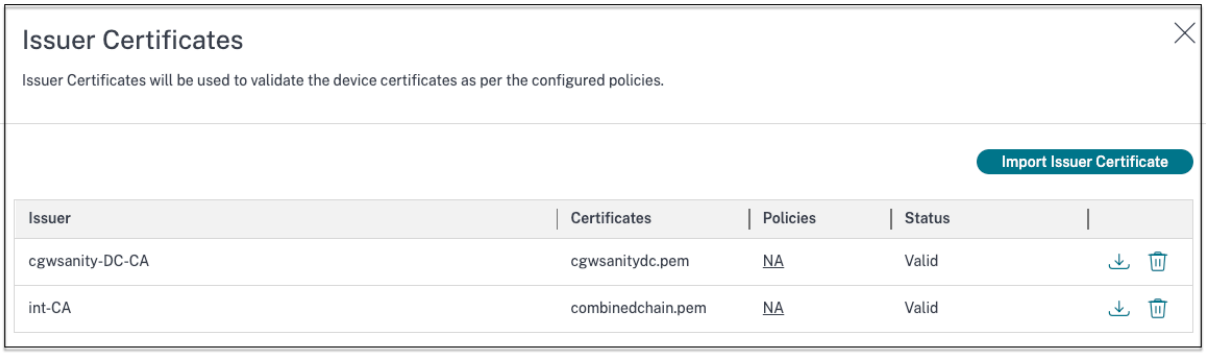
2. Click **Manage**, and then click **Import Issue Certificate**.
3. In **Certificate Type**, select the certificate type. Only the PEM type is supported.
4. In **Certificate File**, click **Choose Certificate** to select the issuer certificate.
5. Click **Open**, and then click **Import**.




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

## View imported certificates

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

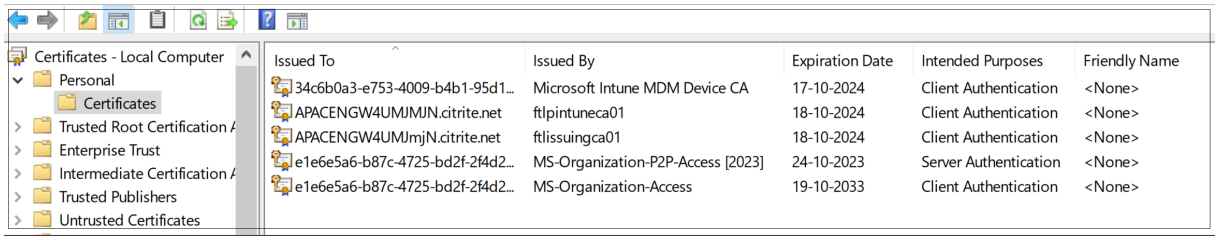



## Install the device certificate on the end device

**Windows:**

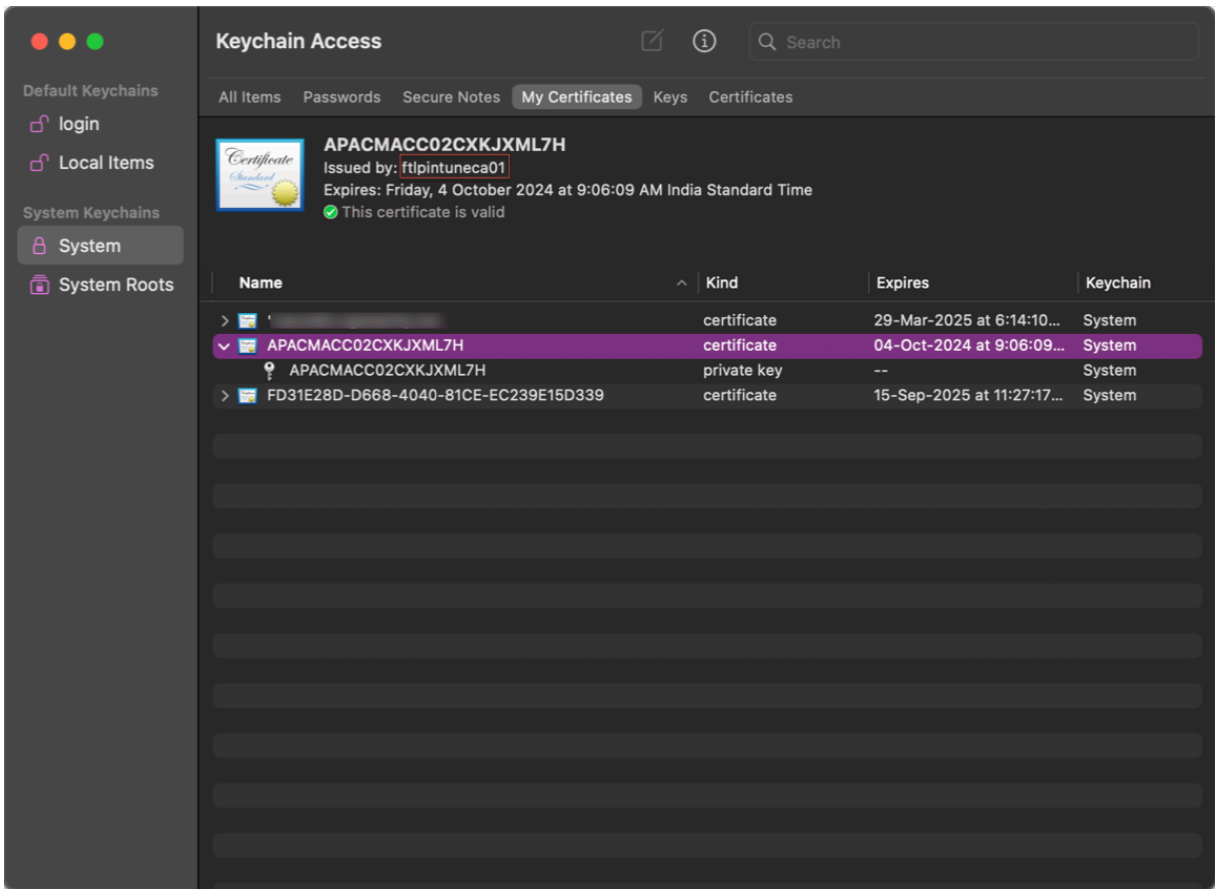
1. From the **Start** menu, open **Computer Certificate manager**.
2. Ensure that the certificate is installed in `Certificates - Local Computer\Personal\Certificates`.
   - The **Intended Purposes** must include **Client Authentication**.
   - The **Issued By** column must match the issuer name configured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



## Enforce smart controls on DaaS using Device Posture

December 22, 2023

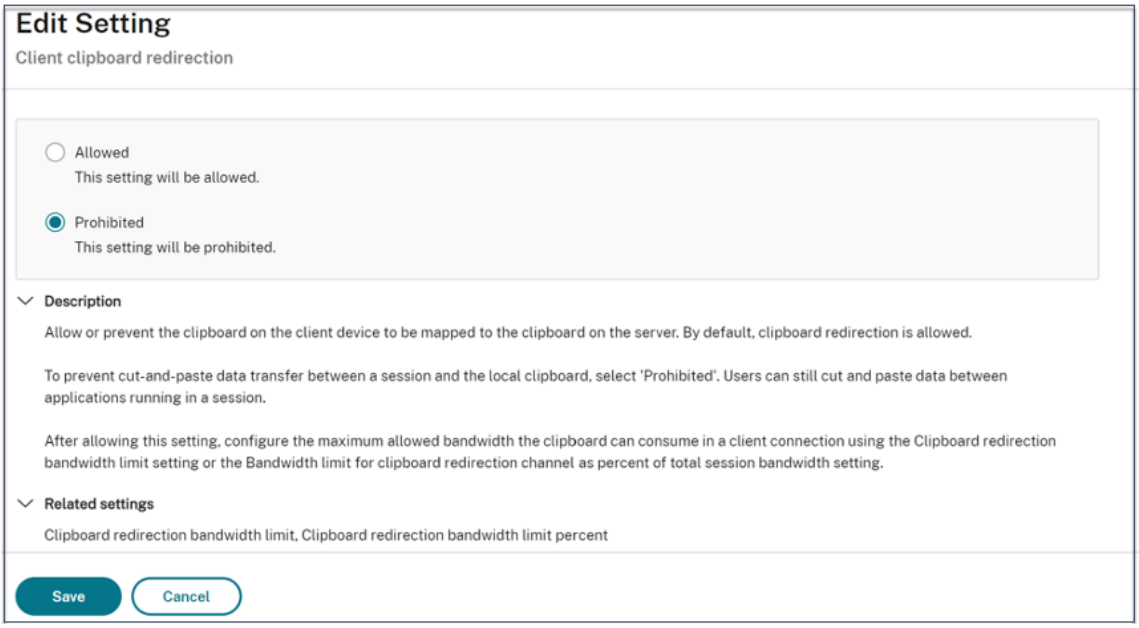
You can enforce smart controls while accessing the Citrix Desktop as a Service (DaaS) resources through the Citrix Device Posture service.

> **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:

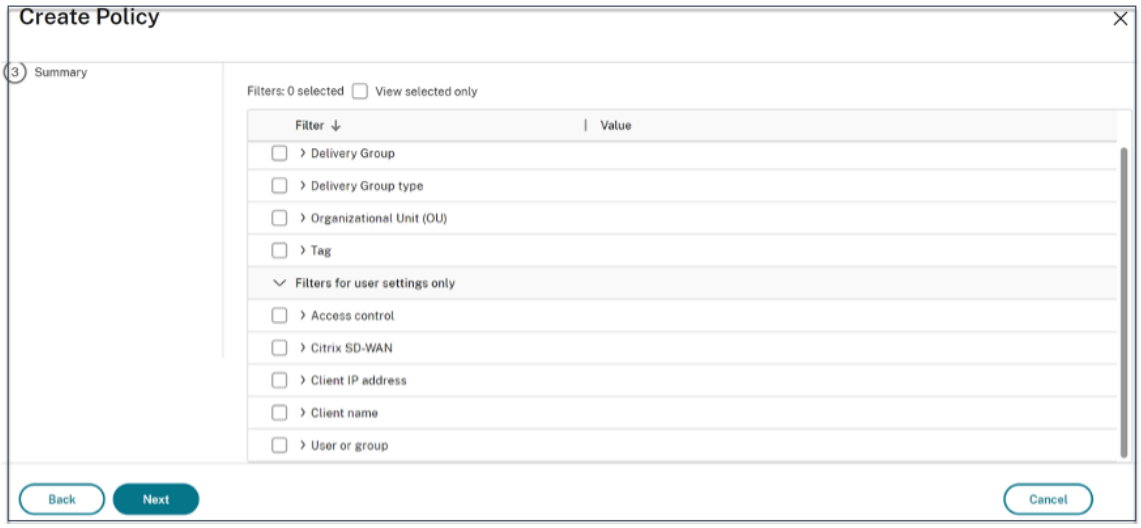
1. On the Citrix DaaS configuration page, Click the **Manage** tab.
2. Click the **Policies** tab.
3. Select **Create Policy**.
4. In **Select Settings**, select **Client Clipboard Redirection**.
5. In **Edit Setting**, select **Prohibited**, and then click **Save**.




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

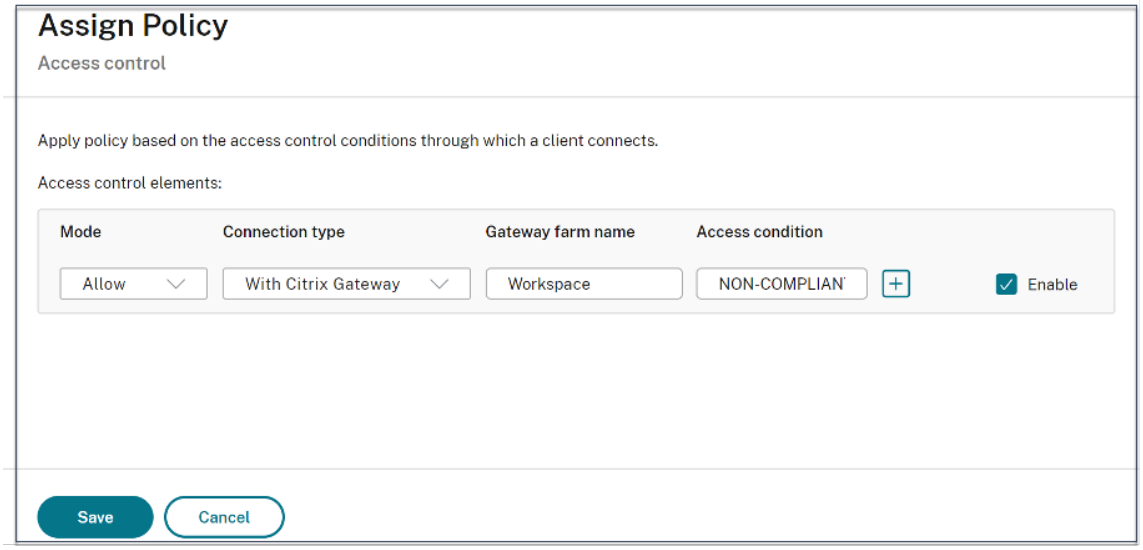
 

7. Go to **Filter for user settings only** and select **Access Control**.




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**.




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.

## Device posture logs

December 22, 2023

The Secure Private Access service dashboard captures the device posture logs in addition to the logs related to the SaaS/Web and TCP/UDP apps.

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:**

```
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
<!--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.