Citrix Workspace app

Contents

Citrix Workspace app

March 8, 2024

About Citrix Workspace app

Citrix Workspace app provides instant, secure, and seamless access to all the resources that your end users need to stay productive. Citrix Workspace app includes access to virtual desktops, virtual apps, web and SaaS apps, and features such as embedded browsing, and single sign-on (from anywhere and from any device).

Citrix Workspace app is a client application that can be deployed across devices on both cloud and on-premises environments. It builds on the capabilities of what was previously known as Citrix Receiver, and includes Citrix client technologies such as - HDX, the Citrix Gateway plug-ins, and Secure private access.

The client app is optimized to run on all client OS like Windows, macOS, Linux, iOS, and Android. It can also be accessed via a browser. For more details on the supported browsers, see Workspace Browser Compatibility.

Citrix Workspace app, powered by Citrix protocol and HDX (high-definition experience), delivers high-performance virtual app and desktop sessions. It is enhanced to deliver a secure login and internet browsing experience, easy management of your apps and desktops, advanced search capabilities, and more.

> **Note:**
>
> The app UI might vary based on the deployment of resources, that is, on cloud (leveraging workspace platform) or on-premises (leveraging StoreFront platform).

For information about the features available in Citrix Workspace app, see Citrix Workspace app feature matrix.

For information about the differences between LTSR and Current Releases, see Lifecycle Milestones for Citrix Workspace app.

Citrix Workspace app is available for the following operating systems:

- Citrix Workspace app for Android
- Citrix Workspace app for ChromeOS
- Citrix Workspace app for HTML5
- Citrix Workspace app for iOS

- Citrix Workspace app for Linux
- Citrix Workspace app for Mac
- Citrix Workspace app for Windows
- Citrix Workspace app for Windows (Store)

> **Important**
>
> **Data collected for Citrix Workspace app updates:**
>
> With respect to devices connected to the Internet, Citrix Workspace app might without additional notice, check for updates that are available for download and installation to the device and let the user know of their availability. Only non-personal identifiable information is transmitted when this happens, except to the extent that IP addresses may be considered personally identifiable in some jurisdictions.

Configure Citrix Workspace app using Global App Configuration service

Global App Configuration service provides a centralized interface to configure the Citrix Workspace app settings for end users. You can configure settings for both cloud and on-premises stores from a single interface. These settings are applicable to both managed and unmanaged devices (BYOD). For more information, see Global App Configuration service.

Language support

Citrix Workspace apps are adapted for use in languages other than English. This section lists the supported languages in the latest release of Citrix Workspace apps.

The following table lists the languages supported for Citrix Workspace app on various operating systems or platforms. A ☑ indicates that the app is available in that particular language.

Language	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
English	☑	☑	☑	☑	☑	☑	☑	☑
Danish	☑			☑				
Dutch	☑	☑	☑	☑	☑	☑	☑	☑
French	☑	☑	☑	☑	☑	☑	☑	☑
German	☑	☑	☑	☑	☑	☑	☑	☑
Italian	☑	☑	☑	☑	☑	☑	☑	☑

Language	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Japanese	☑	☑	☑	☑	☑	☑	☑	☑
Korean	☑	☑	☑	☑	☑		☑	☑
Portuguese (Brazil)	☑	☑	☑	☑	☑	☑	☑	☑
Russian		☑	☑		☑		☑	☑
Simplified Chinese	☑	☑	☑	☑	☑	☑	☑	☑
Spanish	☑	☑	☑	☑	☑	☑	☑	☑
Swedish	☑			☑				
Traditional Chinese		☑	☑				☑	☑

Feature flag

This article discusses feature flag management and the various Citrix Workspace apps that support feature flags.

Feature flag management

If an issue occurs with Citrix Workspace app in production, we can disable an affected feature dynamically in Citrix Workspace app even after the feature is shipped. To do so, we use feature flags and a third-party service called LaunchDarkly. You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements.

The following table calls out the various apps that support feature flags and the release versions in which feature flags were introduced in these apps.

App	Feature flag support	Version	Documentation
Citrix Workspace app for Android	Yes	10.7.5	Feature flag management for Citrix Workspace app for Android

App	Feature flag support	Version	Documentation
Citrix Workspace app for ChromeOS	Yes	1908	Feature flag management for Citrix Workspace app for ChromeOS
Citrix Workspace app for HTML5	Yes	1908	Feature flag management for Citrix Workspace app for HTML5
Citrix Workspace app for iOS	Yes	10.4.10	Feature flag management for Citrix Workspace app for iOS
Citrix Workspace app for Linux	Yes	2109	Feature flag management for Citrix Workspace app for Linux
Citrix Workspace app for Mac	Yes	2010	Feature flag management for Citrix Workspace app for Mac
Citrix Workspace app for Windows	Yes	2012	Feature flag management for Citrix Workspace app for Windows

Important update about Citrix Receiver

Beginning August 2018, Citrix Workspace app replaces Citrix Receiver. While you can still download older versions of Citrix Receiver, new features and enhancements are released for Citrix Workspace app.

Citrix Workspace app is a new client from Citrix that works similar to Citrix Receiver and is fully backward-compatible with your organization's Citrix infrastructure. Citrix Workspace app provides the full capabilities of Citrix Receiver, and new capabilities based on your organization's Citrix deployment.

Citrix Workspace app is built on Citrix Receiver technology, and is fully backward compatible with all Citrix solutions.

For more information, visit the Workspace app FAQ page.

Citrix Workspace web extensions

February 28, 2024

With the Citrix Workspace web extension you can launch your workspace apps everywhere without an `.ica` file, making your experience safer and more reliable. Opening your apps with the browser extension keeps all your apps and desktops in a single location and allows you to easily track your work and free your desktop of clutter. The Citrix Workspace web extension also provides the benefit of screen capture App Protection and seamless service continuity.

Install the Citrix Workspace web extensions

To install the Citrix Workspace web extension, follow these steps:

1. Navigate to your preferred browser's web store:
   - Chrome Web Store
   - Microsoft Edge Addons
   - Mac app store
2. Add and confirm installation of the Citrix Workspace web extension via your preferred browser app store.
3. Confirm the popup message that you want to add the web extension if necessary.
4. (Optional) Select the puzzle piece icon on the top right of the browser to pin the browser for easy access.
5. Select **Add Extension**.
6. Select the pushpin icon to pin the extension.

The Citrix Workspace web extension is now installed.

For additional information about the Citrix Workspace web extension, see the Citrix Workspace web extension blog.

Open SaaS apps within your Citrix Workspace instance

If the Citrix Workspace web extension isn't already enabled on your Workspace instance, follow these steps:

1. Select your account profile in the Workspace window.
2. Select **Advanced** from the profile menu.
3. Select **Use Web Browser** in the **Apps and Desktops Launch Preference** window.
4. Confirm **Open Citrix Workspace Launcher** in the popup window.

Your SaaS apps now open within your Citrix Workspace app window.

Citrix Workspace app feature matrix

Citrix Workspace app provides a gamut of features distributed across different platforms or operating systems. With this feature matrix, you can clearly understand the availability of the features across different platforms.

The Citrix Workspace web extension is accessible by any computer with a supported web browser and an Internet connection. To use all features and functions of the Citrix Workspace web extension, the following browser types are supported:

Browser name	Version
Google Chrome	Latest version
Microsoft Edge	Latest version
Apple Safari	Latest version

App Protection

February 28, 2024

App Protection is a feature for the Citrix Workspace app that provides enhanced security when using Citrix Virtual Apps and Desktops published resources. App Protection is supported for on-premises Citrix Virtual Apps and Desktops deployments, and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) with StoreFront and Workspace. It means that App Protection is supported on all cloud environments, on-premises environments, and hybrid environments. App Protection is also supported when you are connecting to StoreFront or Workspace via ADC Gateway.

Two policies provide anti-keylogging and anti-screen-capturing capabilities for a Citrix HDX session. The policies along with a minimum of Citrix Workspace app 2203.1 LTSR for Windows, Citrix Workspace app 2001 for Mac, or Citrix Workspace app 2108 for Linux can help protect data from keyloggers and screen scrapers.

When you enable anti-keylogging:

- A keylogger sees encrypted keystrokes.
- This feature is active only when a protected window is in focus.

Anti-screen-capturing when enabled:

- On Windows OS and macOS, when you capture a screen, only the content of the protected window is blank. This feature is active when a protected window isn't minimized. On the Linux OS, the entire capture is blank. This feature is active whether a protected window is minimized or not.
- When using the **Print Screen** button in Windows OS to take screenshots, the data is not copied to the clipboard. To take screenshots using the **Print Screen** button, minimize any protected apps.

You can configure the policies through PowerShell and through Web Studio. For more information, see Configure App Protection for virtual apps and desktops.

After buying this feature, make sure you enable the App Protection license.

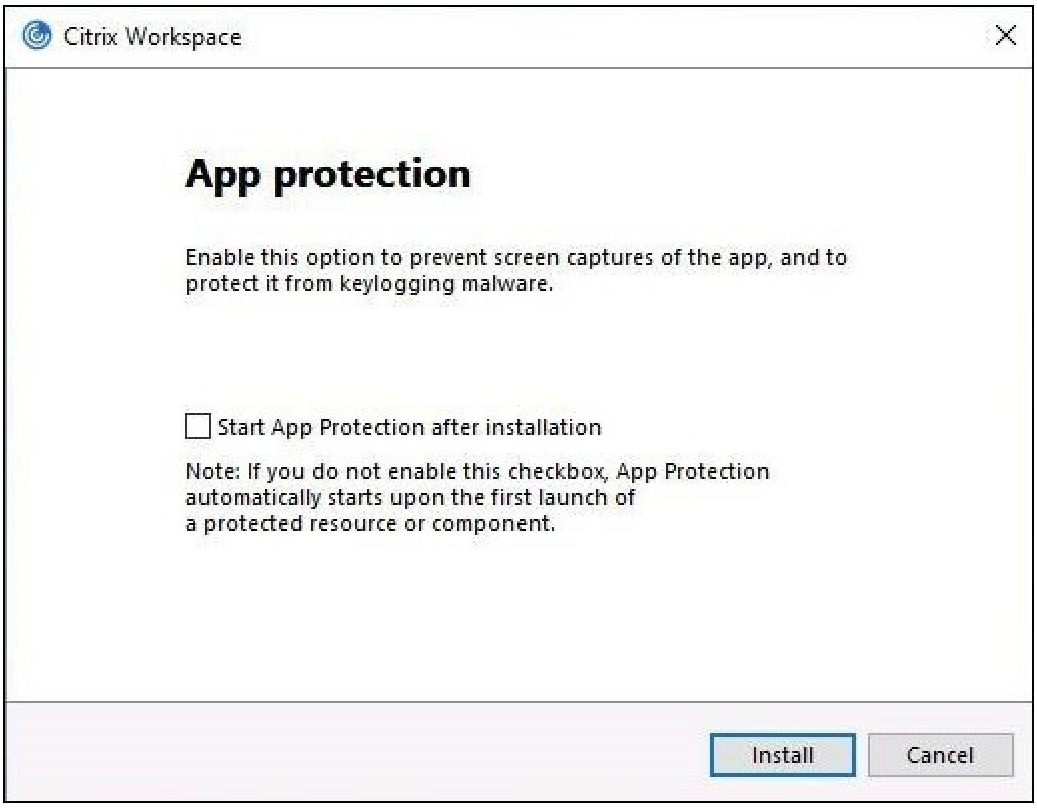
> **Disclaimer:**
>
> App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). Doing so means that App Protection policies can provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.
>
> Citrix App Protection policies work effectively with underlying operating system components, including ICA files. Citrix might not provide support if intentional tampering or modification of the underlying components is detected, to provide the integrity of policies applied.

Check if App Protection is installed

Citrix Workspace app for Windows

Starting with Citrix Workspace app version 2212, App Protection is installed by default. However, the component might be in an active or dormant state depending on whether the user selected the **Start App Protection after installation** checkbox.

- For Citrix Workspace app versions before 2311:



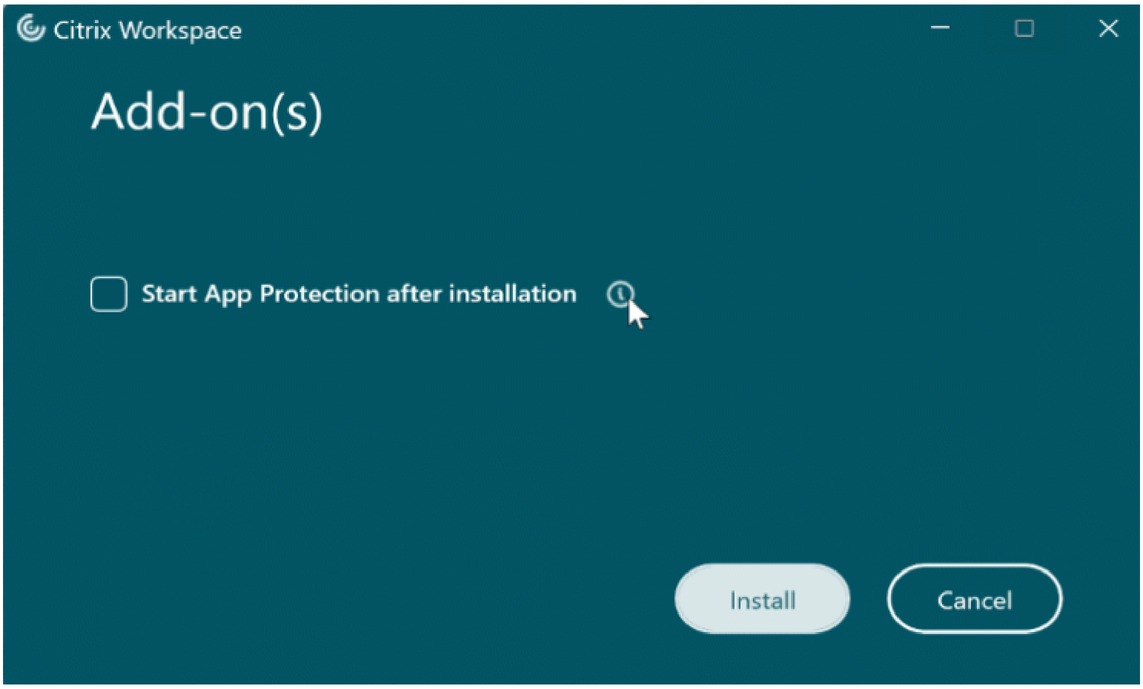
App protection

Enable this option to prevent screen captures of the app, and to protect it from keylogging malware.

□ Start App Protection after installation

Note: If you do not enable this checkbox, App Protection automatically starts upon the first launch of a protected resource or component.

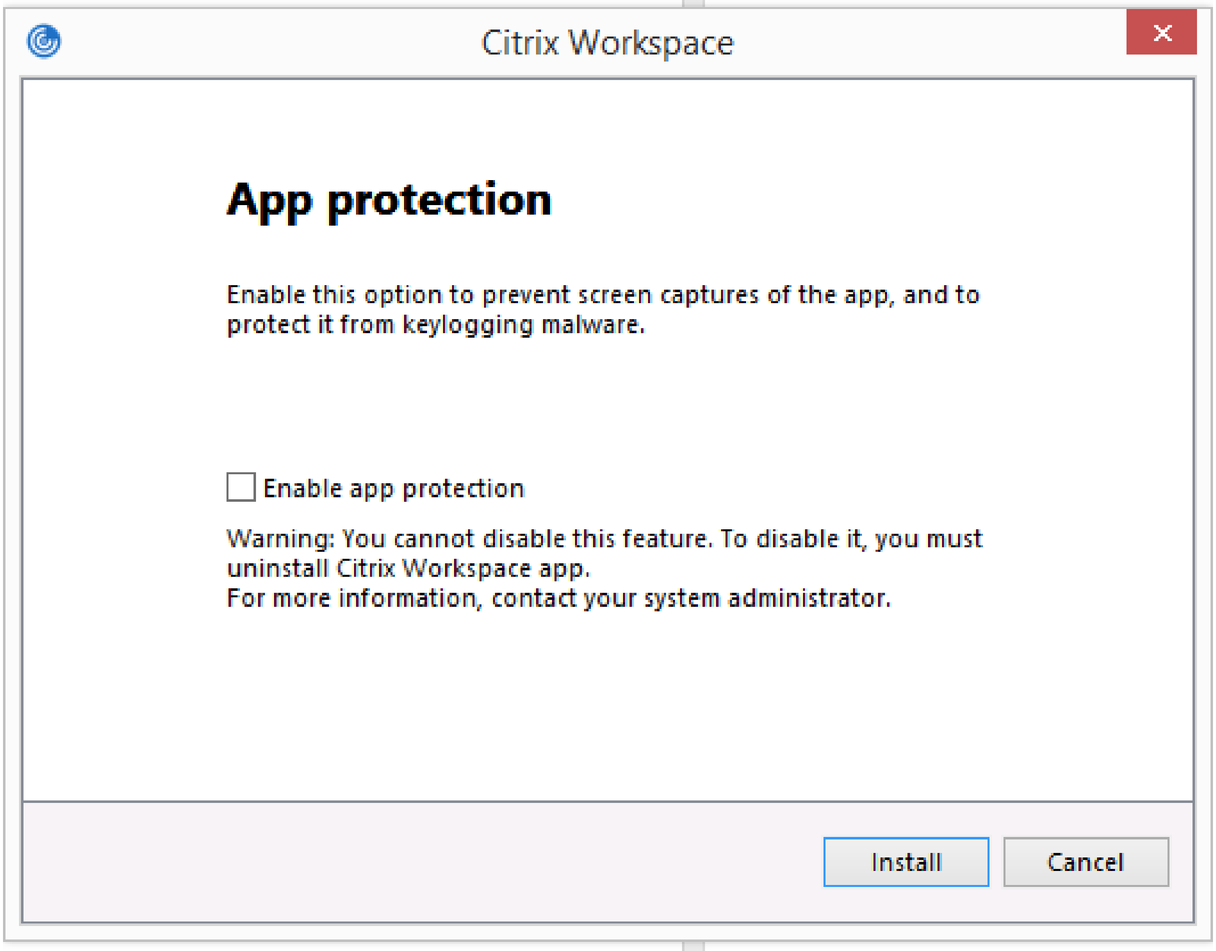
- From Citrix Workspace app version 2311 onwards:



Add-on(s)

□ Start App Protection after installation

For Citrix Workspace app versions before 2212, App Protection is installed and be in the active state only if you select the **Enable App Protection** checkbox while installing Citrix Workspace app.



Citrix Workspace

App protection

Enable this option to prevent screen captures of the app, and to protect it from keylogging malware.

□ Enable app protection

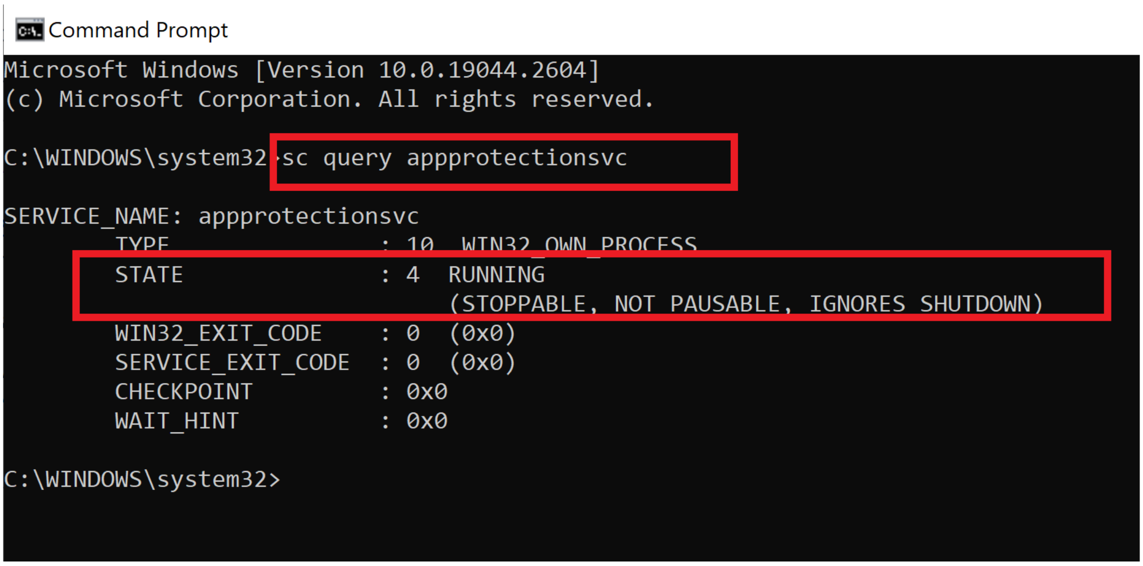
Warning: You cannot disable this feature. To disable it, you must uninstall Citrix Workspace app.
For more information, contact your system administrator.

App Protection can either be in the **STOPPED** state or **RUNNING** state.

To check the status of the service, do one of the following steps:

- For Citrix Workspace app version 2206 or later, run the following command:

```
sc query appprotectionsvc
<!--NeedCopy-->
```

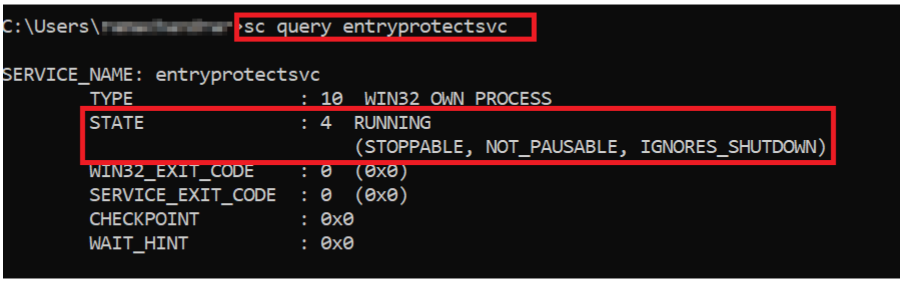


Command Prompt

```
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>sc query appprotectionsvc

SERVICE_NAME: appprotectionsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>
```

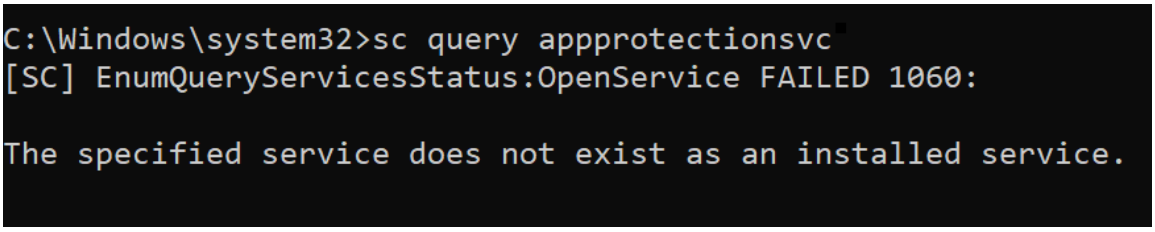
- For Citrix Workspace app versions before 2206, run the following command:

```
sc query entryprotectsvc
<!--NeedCopy-->
```



```
C:\Users\[redacted]>sc query entryprotectsvc

SERVICE_NAME: entryprotectsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

> **Note:**
>
> In Citrix Workspace app versions before 2212, if you didn't select the **Enable App Protection** checkbox while installing Citrix Workspace app and run the preceding command to check the status, then it displays the following error message:



```
C:\Windows\system32>sc query appprotectionsvc
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.
```

App Protection behavior on different environments

The behavior of App Protection depends on how you access the resources that are configured with App Protection policies. These resources include Virtual Apps and Desktops, internal web apps, and

SaaS apps. You can access these resources using a supported native Citrix Workspace app client or a web browser. App Protection performs varyingly on different environments:

- **Unsupported Citrix Receivers or Citrix Workspace apps** - The resources that are configured with App Protection policies are not available.
- **Supported Citrix Workspace app versions** - The resources that are configured with App Protection policies are available and launches properly.
- **Hybrid launch using Workspace store URL** - The resources that are configured with App Protection policies are always available. To successfully launch the resources on a web browser using the Workspace store URL, see App Protection for hybrid launch for Workspace.
- **Hybrid launch using StoreFront store URL** - The resources that are configured with App Protection policies are not available if the StoreFront customization is not deployed. To successfully launch the resources on a web browser using the StoreFront store URL, see App Protection for hybrid launch for StoreFront.

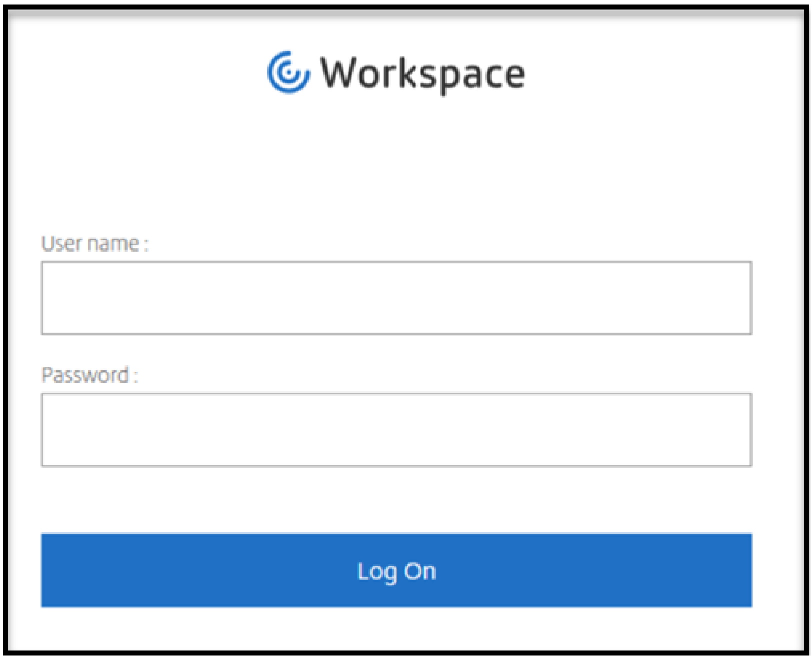
Protection is applied under the following conditions:

- **Anti-screen capture** –For Citrix Workspace app for Windows and Citrix Workspace app for Mac, it is enabled if any protected window is visible on the screen. To disable protection, minimize all protected windows. For Citrix Workspace app for Linux, it is enabled if any protected window is active. To disable protection, close all protected windows.
- **Anti-keylogging** –Enabled if a protected window is in focus. To disable protection, change focus to another window.

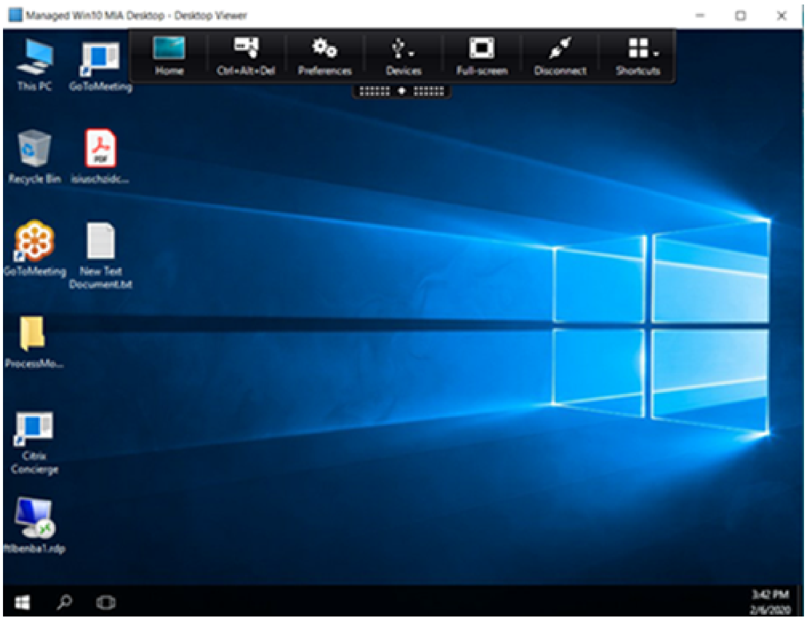
What does App Protection protect?

App Protection protects the following Citrix windows:

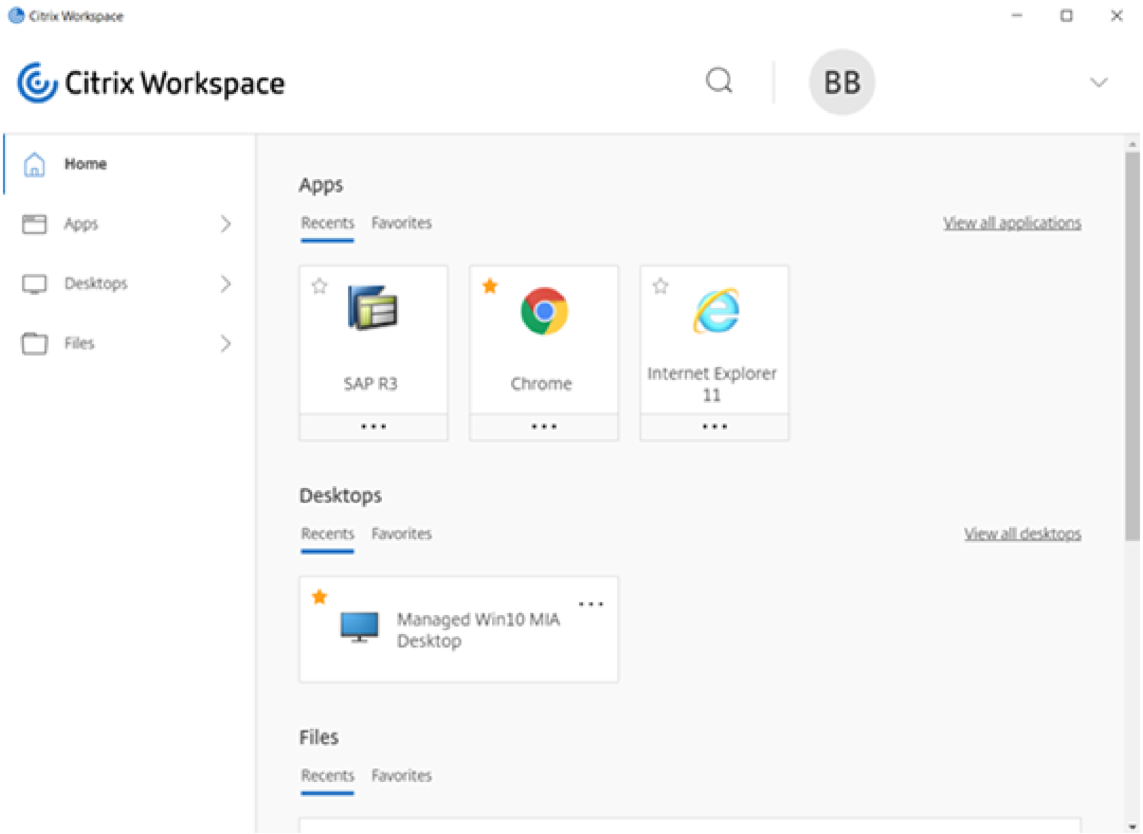
- Citrix sign in windows



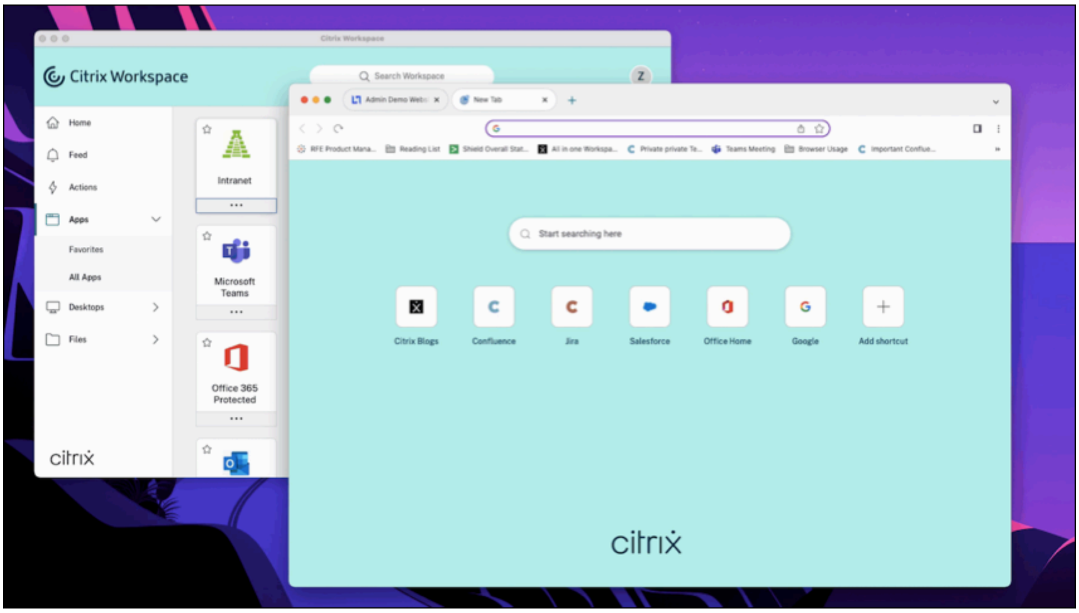
- Citrix Workspace app HDX session windows (For example, managed desktop)



- Self-Service (Store) windows



- Web and SaaS apps
  - Citrix Workspace app for Windows and Citrix Workspace app for Mac - Web and SaaS apps open in the Citrix Enterprise Browser. If the apps are configured to have the App Protection policies through the Citrix Secure Private Access, then App Protection is applied on a per tab basis.



  - Citrix Workspace app for Linux - Citrix Enterprise Browser is not supported.

What doesn't App Protection protect?

- The following items under the Citrix Workspace apps icon in the navigation bar:
  - Connections Center
  - All links under Advanced Preferences
  - Personalize
  - Check for Updates
  - Sign Out
- If you choose to protect a virtual desktop with anti-screen-capturing, users can still screen share from apps within the virtual desktop. However, for the apps outside of the virtual desktop, you can't take screenshots, or record the virtual desktop.

Limitations

The following limitations exist by design:

- App Protection enabled virtual apps and desktops are blocked from launching when accessed within RDP sessions.
- App Protection is not supported in double-hop and multiple-hop scenarios.
- App Protection is not supported if you're on an unsupported version of the Citrix Workspace app or Citrix Receiver. In that case, resources are hidden.
- When the App Protection features are applied to virtual apps and desktops, outgoing screen sharing might be affected if optimization is used.
- Citrix Workspace app with App Protection might not be compatible with some other security solutions or apps using similar underlying technology.
- App Protection is not supported when you launch resources from within the Citrix Secure Browser, or with Remote Browser Isolation.
- In Citrix Workspace app for Linux, you're unable to use snap applications when App Protection is installed.

Contextual App Protection

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture. For more information, see the following articles:

- Contextual App Protection for StoreFront

- Contextual App Protection for Workspace

App Protection for hybrid launch

Hybrid launch of Citrix Virtual Apps and Desktops is when you log in to Citrix Workspace app through the browser (Citrix Workspace for Web), and use the applications through the native Citrix Workspace app. The term hybrid is the result of users applying the combination Citrix Workspace app for Web and the native Citrix Workspace app to connect and use the resources. App Protection supports hybrid launch in Workspace and StoreFront. For more information, see the following articles:

- App Protection for hybrid launch for Workspace
- App Protection for hybrid launch for StoreFront

System requirements and compatibility

March 13, 2024

System requirements

As a prerequisite, make sure that you have installed the Citrix Workspace app using administrator rights.

Minimum versions of Citrix components

- Citrix Workspace app 2108 for Linux
- Citrix Workspace app 2203.1 LTSR for Windows
- Citrix Workspace app 2002 for Windows
- Citrix Workspace app 2305.1 for Windows (Store)
- Citrix Workspace app 2001 for Mac
- StoreFront 1912 LTSR
- Delivery Controller 1912
- Valid Citrix licenses. For more information, contact your Citrix Sales Representative or Citrix Partner.

> **Note:**
>
> If the users are on devices or Workspace app versions that don't support App Protection, then they can't access the protected resources. The protected resources include Virtual Apps and

> Desktops and Web and SaaS apps.

Licenses

The following section explains the different types of licenses available for App Protection based on the products, platforms, and use cases.

IT-managed VDI For all editions of IT-managed VDI, App Protection is available as an add-on. For more information, see IT-managed VDI.

Citrix DaaS for Hyperscalers

- Azure
- Google
- AWS

Citrix DaaS In the Feature Matrix for Citrix DaaS article, navigate to **DaaS cloud Services > Security and Monitoring > App Protection**.

Citrix Secure Private Access App Protection is available as a standalone attachment for Citrix Secure Private Access. For more information, navigate to **Citrix cloud services > Citrix Secure Private Access** in the Service descriptions for Citrix Services article.

Citrix Universal subscription App Protection is included with the following services:

- Citrix Universal Premium
- Citrix Universal Premium Plus

It is available as an add-on with the following editions:

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

For more information, see this article.

Operating system platforms

App Protection policies runtime is installed on the endpoint that you are connecting *from* and not on the VDA you are connecting *to*. So, only the operating system version of the endpoint is significant.

(App Protection can connect to VDAs hosted on any supported operating systems described in Citrix Virtual Apps and Desktops System requirements.)

The App Protection feature is supported on endpoints running the following operating systems:

- Windows 11
- Windows 10
- Windows 8.1
- macOS High Sierra (10.13) and higher
- 64-bit Ubuntu 22.04
- 64-bit RHEL 9
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

> **Note:**
>
> For App Protection, Citrix Workspace app for Linux requires a Gnome Display Manager along with the supported operating systems.

Compatibility matrix

Compatibility matrix for Citrix Cloud based products

App Protection features compatible with Citrix Cloud based products are as follows:

Feature	Citrix Cloud	Citrix Cloud Japan
Anti-keylogging and Anti-screen capture for virtual apps and desktops	Yes	Yes
Anti-keylogging and Anti-screen capture for web or SaaS apps	Yes	No
Anti-DLL for Windows	Yes	Yes through Group Policy Object (GPO)
Anti-DLL Allow Listing	Yes	Yes through GPO
Global App Configuration service (GACS)	Yes	No
Authentication or Self-Service plug-in screen protection for Linux	Yes	Yes through AuthManConfig.xml

Feature	Citrix Cloud	Citrix Cloud Japan
Authentication or Self-Service plug-in screen protection for Mac	Yes through GACS	Yes through GACS
Authentication or Self-Service plug-in screen protection for Windows	Yes	Yes through GPO
CAS App Protection ScreenShot events	Yes	No
Contextual App Protection	Yes	Yes based on the user
Policy Tampering Detection	Yes	Yes
App Protection Posture Check	Yes	Yes
Local App Allowlisting or Filter - Windows	Yes	Yes through GPO
Local App Protection - Windows	Yes	Yes through GPO

App Protection features

March 5, 2024

This article highlights the App Protection features supported by Citrix Workspace app for Windows, Citrix Workspace app for Linux, and Citrix Workspace app for Mac.

Anti-keylogging

With encryption, App Protection’s anti-keylogging capabilities scramble the text the user is typing for both physical and on-screen keyboards. The anti-keylogging feature encrypts the text before any keylogging tool can access it from the kernel or OS level. A keylogger installed on the client endpoint reading the data from the OS or driver captures the hashed text instead of the keystrokes that the user is typing. App Protection policies are active not only for published applications and desktops, but for Citrix Workspace authentication dialogs as well. Your Citrix Workspace is protected from the moment when your users open the first authentication dialog. App Protection scrambles keystrokes, returning indecipherable text to key loggers.

The admins can choose to enable anti-keylogging for the following types resources:

- Virtual Apps and Desktops
- Internal web and SaaS apps
- Authentication screens
- Self-Service plug-in (SSP) screens

Anti-screen capture

Anti-screen capture prevents an app from trying to take a screenshot or recording the screen within a virtual app or desktop session. The screen capture software can't detect content within the capture region. The area selected by the app grays out, or the app captures nothing instead of the screen section that it expects to copy. The anti-screen capture feature applies to
snip and sketch, Snipping Tool, and **Shift+Ctrl+Print Screen** on Windows.

Another use case for anti-screen capture is preventing sharing of sensitive data in a virtual meeting or web conferencing applications like GoToMeeting, Microsoft Teams, or Zoom. App Protection prevents unintended sharing by returning a blank screen in web conferences when apps are protected. This feature makes sure that the sensitive data isn't accidentally leaked from the organization. This feature can help with compliance in regulated industries, as the intention is not considered when disclosing a data breach.

The admins can choose to enable anti-screen capture for the following types resources:

- Virtual Apps and Desktops
- Internal web and SaaS apps
- Authentication screens
- Self-Service plug-in (SSP) screens

> **Note:**
>
> If you have launched two virtual desktops where one virtual desktop is enabled with the Anti-screen capture feature and the other virtual desktop isn't enabled with the Anti-screen capture feature, then the Anti-screen capture feature is applicable for both the virtual desktops. You can' t take the screenshot of either virtual desktops.
>
> In case if you have minimized the virtual desktop that is enabled with Anti-screen capture, the Anti-screen capture feature is still applicable for the virtual desktop without the Anti-screen capture feature.

Screen capture detection and notification

For Citrix Workspace app, you can view a notification when a possible attempt of screen capture is made on any protected resources. For information on the resources protected by App Protection, see What does App Protection protect?

The notification appears when there is an:

- attempt to take a screenshot or record video through a screen-capturing tool.
- attempt to take a screenshot through the Print Screen key.

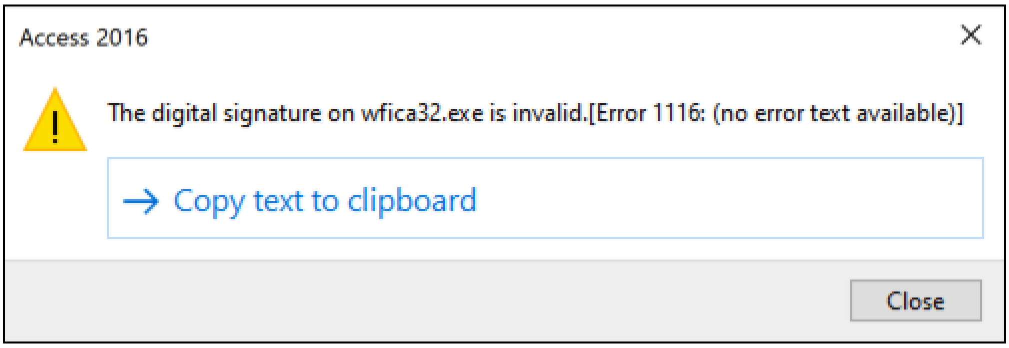
> **Note:**
>
> - The notification appears only once per running instance of the screen capture tool. The notification appears again if you relaunch the tool and try to capture the screen.
> - On Citrix Workspace app for Windows 2212 and later, sign-in windows and Self-Service (Store) windows are not protected by default.

Anti-DLL Injection

The Anti-DLL Injection security enhancement helps protect the Citrix Workspace app from certain unauthorized dynamic-link libraries (DLL) or untrusted modules. If such untrusted modules are injected, the Citrix Workspace app detects these interventions and stops the modules from loading. Also, if any untrusted or malicious DLL is detected before the session launch, App Protection blocks the session launch and displays an error message. Closing the error message exits the virtual app and desktop session.

This feature is applicable for all protected virtual apps and desktops and the Citrix Workspace app authentication window (on-premises deployment/StoreFront).

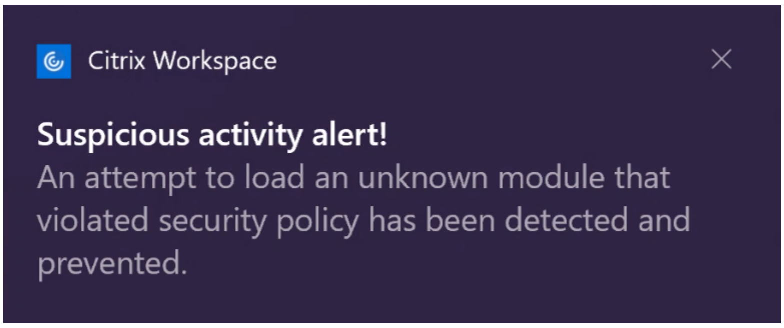
This enhancement exits the session immediately when certain untrusted or malicious DLLs exist on the protected component.



Access 2016

The digital signature on wfica32.exe is invalid.[Error 1116: (no error text available)]

The enhancement displays a notification when an untrusted or malicious DLL is blocked. Closing the message exits the virtual app and desktop session.



Citrix Workspace

Suspicious activity alert!
An attempt to load an unknown module that violated security policy has been detected and prevented.

Disclaimer: This capability works by filtering access to required functions of the underlying operating system (specific API calls required to load DLLs). Doing so means that it can provide protection even against certain custom and purpose-built hacker tools. However, as operating systems evolve, new ways of loading DLLs can emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

This feature support Citrix Workspace app for Windows version 2206 and later.

> **Note:**
>
> Previously, anti-screen capture and anti-keylogging capabilities were enforced by default for Citrix authentication and Citrix Workspace app screens. However, starting from 2212, these capabilities are disabled by default and need to be configured using the Group Policy Object. For information on the GPO configuration, see Enhancement to App Protection configuration.

Compatibility with HDX optimization for Microsoft Teams

Optimized Microsoft Teams supports screen sharing when Citrix Workspace app is enabled with App Protection in the Desktop Viewer mode only. When you click **Share content** in Microsoft Teams, the screen picker provides the following options:

- **Window** option to share any open app - This option is displayed only if the VDA version is 2109 or later.
- **Desktop** option to share the contents on your VDA desktop - This option is displayed only for the following versions of Citrix Workspace app:
  - Citrix Workspace app for Linux version 2311 or later
  - Citrix Workspace app for Mac version 2308 or later
  - Citrix Workspace app for Windows version 2309 or later

> **Note:**
>
> For Citrix Workspace app for Linux, the Desktop share option is disabled by default. To enable it, add the `UseGbufferScreenSharing` parameter in your *config.json* file as follows:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine
vim /var/.config/citrix/hdx_rtc_engine/config.json
{

      "UseGbufferScreenSharing":1
 }

<!--NeedCopy-->
```

Optimized Microsoft Teams enabled with App Protection also supports the Citrix virtual monitor layout which allows you to share each virtual monitor individually.

> **Limitation:**
>
> - Optimized Microsoft Teams enabled with App Protection doesn't support screen sharing on Published Desktops enabled with Local App Access (LAA).
> - Client-rendered content such as Browser content using BCR cannot be captured or shared. If you try to screen capture, it is displayed as a black screen.
>
> **Note:**
>
> For Citrix Workspace app for Linux and Citrix Workspace app for Mac, this feature is in Technical Preview.

Local App Protection (Preview)

App Protection offers enhanced security to defend customers against keyloggers, and accidental and malicious screen capture at endpoints. Currently App Protection capabilities are only offered for Workspace resources. With this feature, App Protection capabilities are extended to local apps on endpoints. Starting with Citrix Workspace app 2210 for Windows, App Protection can be applied to local apps on Windows devices.

Register for the Preview of this feature using the Podio form.

Policy Tampering Detection

Policy Tampering Detection feature prevents the user from accessing the virtual app or desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered. If policy tampering is detected, then the virtual app or desktop session is terminated.

> **Note:**
>
> The policy Tampering Detection feature will be enabled by default in a future version.

To configure Policy Tampering Detection, see Configure Policy tampering detection.

Posture Check

To detect and block launching virtual apps and desktops that are enabled with App Protection policies from Citrix Workspace app versions that do not support the Policy Tampering Detection feature, enable App Protection Posture Check.

> **Note:**
>
> If Posture Check is enabled and you are using the Citrix Workspace app version that does not support Posture Check, then the sessions enabled with App Protection policies are terminated.

To configure Posture Check, see Configure Posture Check.

> **Limitation:**
>
> Posture Check stops working intermittently when you are using Windows Workstation VDAs hosted on Microsoft Azure.

App Protection with DoubleHop scenario

App Protection features are not supported in a double hop scenario. Double hop means a Citrix Virtual Apps or Virtual Desktops session running within a Citrix Virtual Desktops session. You were allowed to launch virtual apps and desktops that are enabled with App Protection policies in a double hop scenario however the App Protection features were not applied.

Starting from the Citrix Workspace app for Windows 2309 version, a Windows Group Policy is introduced which allows you to block launching virtual apps and desktops enabled with App Protection policies in a double hop scenario. For more information about enabling the **Block DoubleHop Launch** setting, see Enable Block DoubleHop Launch setting.

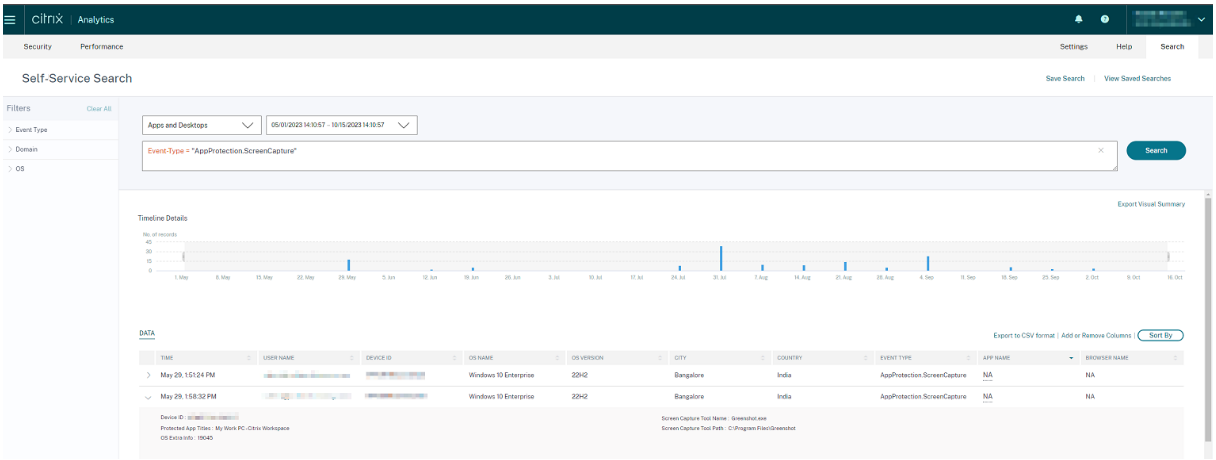
Citrix Analytics Service for App Protection

When you use Citrix Virtual Apps and Desktops, user events corresponding to their activities and actions are generated. Citrix Analytics for Security has a feature named **Self-service search** that records those user events and provides you the insights about them. **Self-service search** enables you to find, filter, and explore those user events so that you can understand what user event is done and act depending on the severity of the event. For more information about **Self-service search**, see Self-service search.

Self-service search for Apps and Desktops has an event type `AppProtection.ScreenCapture` that allows you to determine if any attempts are made to take screenshots of the virtual apps or desktops that are enabled with App Protection policies. For more information about how to search for a user event, see Specify search query to filter events.

This service provides the following information:

- Device ID
- Protected App Titles
- OS Extra Info
- Screen Capture Tool Name
- Screen Capture Tool Path



Event-Type = "AppProtection.ScreenCapture"

TIME	USER NAME	DEVICE ID	OS NAME	OS VERSION	CITY	COUNTRY	EVENT TYPE	APP NAME	BROWSER NAME
May 29, 1:51:24 PM	[redacted]	[redacted]	Windows 10 Enterprise	22H2	Bangalore	India	AppProtection.ScreenCapture	NA	NA
May 29, 1:58:32 PM	[redacted]	[redacted]	Windows 10 Enterprise	22H2	Bangalore	India	AppProtection.ScreenCapture	NA	NA

Device ID : [redacted]
Protected App Titles : My Work PC - Citrix Workspace
OS Extra Info : 19045

Screen Capture Tool Name : Greenshot.exe
Screen Capture Tool Path : C:\Program Files\Greenshot

Configure App Protection

February 28, 2024

App Protection provides enhanced security when you use the Citrix Workspace app. The feature restricts the ability of clients to be compromised with keylogging and screen-capturing malware. App Protection prevents exfiltration of confidential information, such as user credentials and sensitive information displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

This article explains how to configure App Protection on Citrix Workspace app on different platforms.

App Protection is available on Citrix Workspace app for the following platforms:

- Citrix Workspace app for Windows
- Citrix Workspace app for Linux
- Citrix Workspace app for Mac

> **Disclaimer**
>
> App Protection policies filter the access to required functions of the underlying operating system.

> Specific API calls are required to capture screen or keyboard presses. App Protection policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.

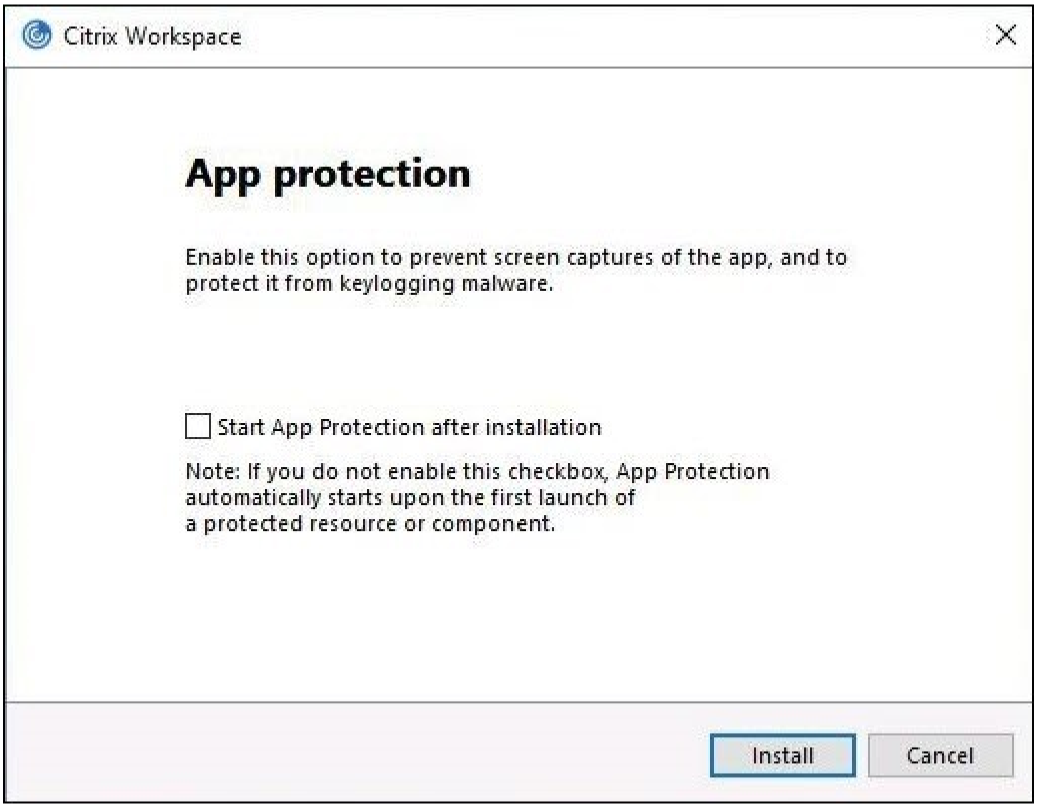
Citrix Workspace app for Windows

Prerequisites

- Enable the App Protection feature on the Controller. For more information, see App Protection.
- Citrix Virtual Apps and Desktops Version 1912 LTSR or later.
- StoreFront version 1912 LTSR or Workspace.
- Citrix Workspace app version 2203.1 LTSR or later.
- A valid App Protection license
- Starting from Citrix Workspace app version 2212, the App Protection component is installed by default during the Citrix Workspace app installation.

  The **Enable App Protection** checkbox that appears during the installation is replaced with **Start App Protection after installation**.

  - For Citrix Workspace app versions before 2311:



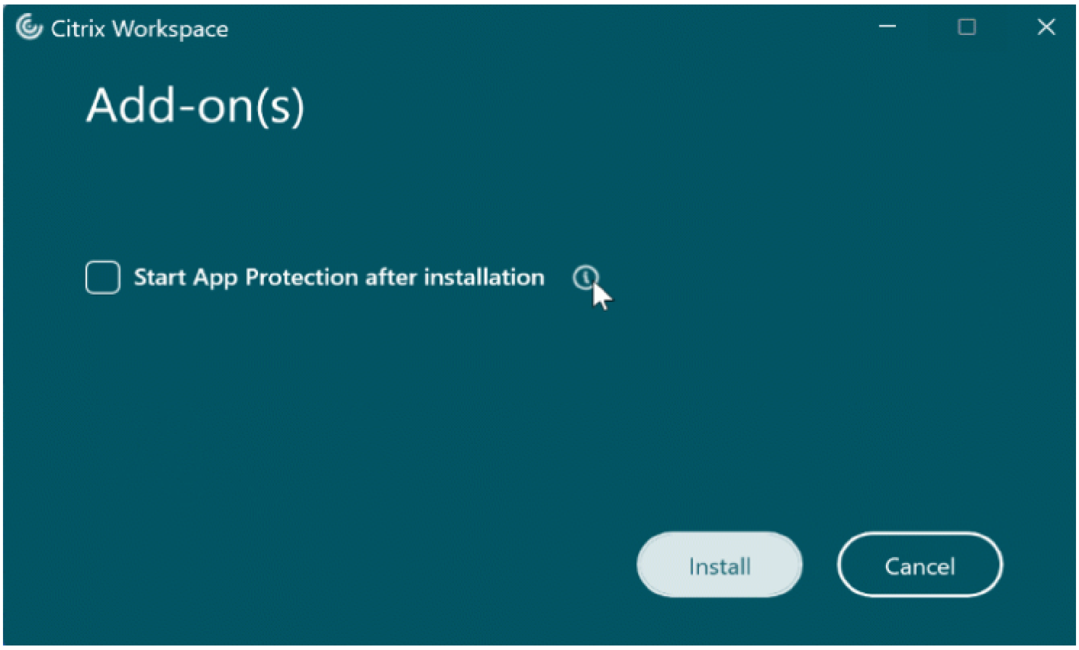
App protection

Enable this option to prevent screen captures of the app, and to protect it from keylogging malware.

□ Start App Protection after installation

Note: If you do not enable this checkbox, App Protection automatically starts upon the first launch of a protected resource or component.

- From Citrix Workspace app version 2311 onwards:



Add-on(s)

□ Start App Protection after installation

When you select this checkbox, App Protection starts immediately after the installation.

> **Note:**
>
> If you don't enable this checkbox, App Protection automatically starts upon the first start of a protected resource or component for customers who are entitled to App Protection.

Limitations

- This feature is supported only on desktop operating systems such as Windows 11, Windows 10, Windows 8.1.
- Starting with Version 2006.1, Citrix Workspace app isn't supported on Windows 7. So, App Protection doesn't work on Windows 7. For more information, see Deprecation.
- This feature isn't supported over Remote Desktop Protocol (RDP).

Command-line interface

You can start the App Protection component using the `/startappprotection` command line parameter. However, the previous `/includeappprotection` switch is deprecated.

The following table provides information on screens protected depending on deployment:

App Protection deployment	Screens protected	Screens not protected
Included in Citrix Workspace app	Self-service plug-in and Authentication manager / User credentials dialog	Connection Center, Devices, Citrix Workspace app error messages, Auto client reconnect, Add account
Configured on the Controller	ICA session screen (both apps and desktops)	Connection Center, Devices, Citrix Workspace app error messages, Auto client reconnect, Add account

When you're taking a screenshot, only the protected window is blacked out. You can take a screenshot of the area outside the protected window. However, if you're using the **PrtScr** key to capture a screenshot on a Windows 10 device, you must minimize the protected window.

Previously, anti-screen capture and anti-keylogging capabilities were enforced by default for Citrix authentication and Citrix Workspace app screens. However, starting from 2212, these capabilities are disabled by default and need to be configured using the Group Policy Object.

> **Note:**
>
> This GPO policy isn't applicable for ICA and SaaS sessions. The ICA and SaaS sessions continue to be controlled using the Delivery Controller and Citrix Secure Private Access.

App Protection enhancement:

From Citrix Workspace app for Windows 2305 and later, anti-keylogging is enabled on the authentication and self-service plug-in screens if one of the following criteria is met:

- You have enabled App Protection using one of the following:
  - Select the **Start App Protection** checkbox during installation.
  - Start the App Protection component using the **/startappprotection** command line parameter.
- If you haven't selected the **Start App Protection** checkbox or used the **/startappprotection** command line parameter during the installation, then the anti-keylogging protection is enabled after launching the first protected resource.

> **Note:**
>
> The Global App Configuration service and Group policy objects settings override the preceding behavior. For example, if you've disabled the GACS or GPO policy for these screens, then the anti-keylogging isn't enabled on the authentication and SSP screens.

Configure the following App Protection features for Citrix Workspace app for Linux:

- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using Global App Configuration service UI, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Global App Configuration service UI.
- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using Group Policy Object, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Group Policy Object.
- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using API, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using GACS API.
- To configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- To configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps.
- To configure the Anti-DLL Injection feature, see Configure Anti-DLL Injection feature.
- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.

- To configure App Protection Posture Check, see Configure App Protection Posture Check.
- To enable Block DoubleHop Launch setting, see Block DoubleHop Launch.

Citrix Workspace app for Linux

Starting with version 2108, the App Protection feature is now fully functional. This feature supports the Virtual Apps and Desktops, and is enabled by default. However, you must configure the App Protection feature in the `AuthManConfig.xml` file to enable it for the authentication manager and the self-service plug-in interfaces.

Prerequisite

App Protection works best with the following operating systems along with the Gnome Display Manager:

- 64-bit Ubuntu 22.04, Ubuntu 20.04, and Ubuntu 18.04
- 64-bit Debian 10 and Debian 9
- 64-bit CentOS 7
- 64-bit RHEL 7
- ARMHF 32-bit Raspberry Pi OS (Based on Debian 10 (buster))
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

> **Note:**
>
> If you're using Citrix Workspace app earlier than version 2204, the App Protection feature does not support the operating systems that use `glibc` 2.34 or later.
>
> If you install the Citrix Workspace app with App Protection feature enabled on the OS that uses `glibc` 2.34 or later, the OS boot might fail on restarting the system. To recover from the OS boot failure, do one of the following:
>
> - Reinstall the OS.
> - Go to Recovery mode of the OS and uninstall the Citrix Workspace app using the terminal.
> - Boot through the live OS and remove the `rm -rf /etc/ld.so.preload` file from the existing OS.

Installing the App Protection component

1. When you install the Citrix Workspace app using the tarball package, the following message appears: **Do you want to install the App Protection component? Warning: You can't disable this feature. To disable it, you must uninstall Citrix Workspace app. For more information, contact your system administrator. [default $INSTALLER_N]:**

2. Enter **Y** to install the App Protection component. App Protection isn't installed by default.
3. Restart your machine for the changes to reflect. App Protection works as expected only after you restart your machine.

Installing the App Protection component on RPM packages Starting with Version 2104, App Protection is supported on the RPM version of Citrix Workspace app.

To install App Protection, do the following:

1. Install Citrix Workspace app.
2. Install the App Protection `ctxappprotection<version>.rpm` package from the Citrix Workspace app installer.
3. Restart the system for the changes to reflect.

Installing the App Protection component on Debian packages Starting with Version 2101, App Protection is supported on the Debian version of Citrix Workspace app.

To install the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

Starting with Version 2106, Citrix Workspace app introduces an option to configure the anti-keylogging and anti-screen capturing functionalities separately for both the authentication manager and self-service plug-in interfaces.

Configure the following App Protection features for Citrix Workspace app for Linux:

- To configure Anti-keylogging and Anti-screen capture for Authentication screen, see Configure using AuthManConfig.xml for authentication manager.
- To configure Anti-keylogging and Anti-screen capture for the Self-Service Plug-in screen, see Configure using AuthManConfig.xml for the Self-Service Plug-in interface.
- To configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.
- To configure App Protection Posture Check, see Configure App Protection Posture Check.

Citrix Workspace app for Mac

Configure the following App Protection features for Citrix Workspace app for Mac:

- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using Global App Configuration service UI, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Global App Configuration service UI.
- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using API, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using GACS API.
- To configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- To configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps.
- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.
- To configure App Protection Posture Check, see Configure App Protection Posture Check.

Recommendation

App Protection policies are primarily focused on enhancing the security and protection of an endpoint. Review all other security recommendations and policies for your environment. You can use a **Security and Control** policy template for a recommended configuration in environments with low tolerance to risk. For more information, see Policy templates.

Configure Anti-keylogging and Anti-screen capture

February 28, 2024

You can configure Anti-keylogging and Anti-screen capture for the following:

- Authentication and self-service plug-in
- Virtual Apps and Desktops
- Web and SaaS apps

Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in

You can configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using the following methods:

Configuration method	Citrix Workspace app for Linux	Citrix Workspace app for Mac	Citrix Workspace app for Windows
Using Group Policy Object	No	No	Yes
Using Global App Configuration service	No	Yes	Yes
Using AuthManConfig.xml	Yes	No	No

Using Group Policy Object

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace**.
3. Depending on whether you're configuring App Protection for an authentication manager, or self-service plug-in, use one of the following steps:

   - **Authentication manager**

     To configure anti-keylogging and anti-screen-capturing for the authentication manager, select **User authentication** > **Manage App Protection** policy.

   - **Self-service plug-in interface**

     To configure anti-keylogging and anti-screen capturing for the self-service plug-in interface, select **Self Service** > **Manage App Protection** policy.

4. Select one or both the following options:

   - **Anti-key logging**: Prevents keyloggers from capturing keystrokes.
   - **Anti-screen capturing**: Prevents users from taking screenshots and sharing their screen.

5. Click **Apply** and **OK**.

Expected Behavior:

The expected behavior depends upon the method by which you access the StoreFront that has the protected resources.

Using Global App Configuration service UI

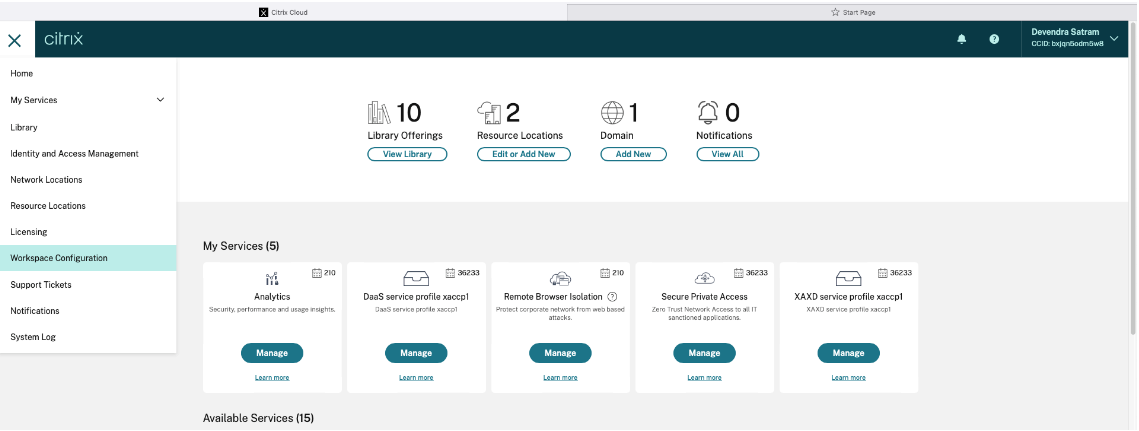
Starting with Citrix Workspace app for Windows 2302 or Citrix Workspace app for Windows 2301 versions, Citrix Workspace app allows you to configure App Protection for authentication screens and self-service plug-in using Global App Configuration service (GACS).

If you enable the anti-keylogging and the anti-screen capturing functionality using the GACS, they're applicable to both authentication and self-service plug-in screens.

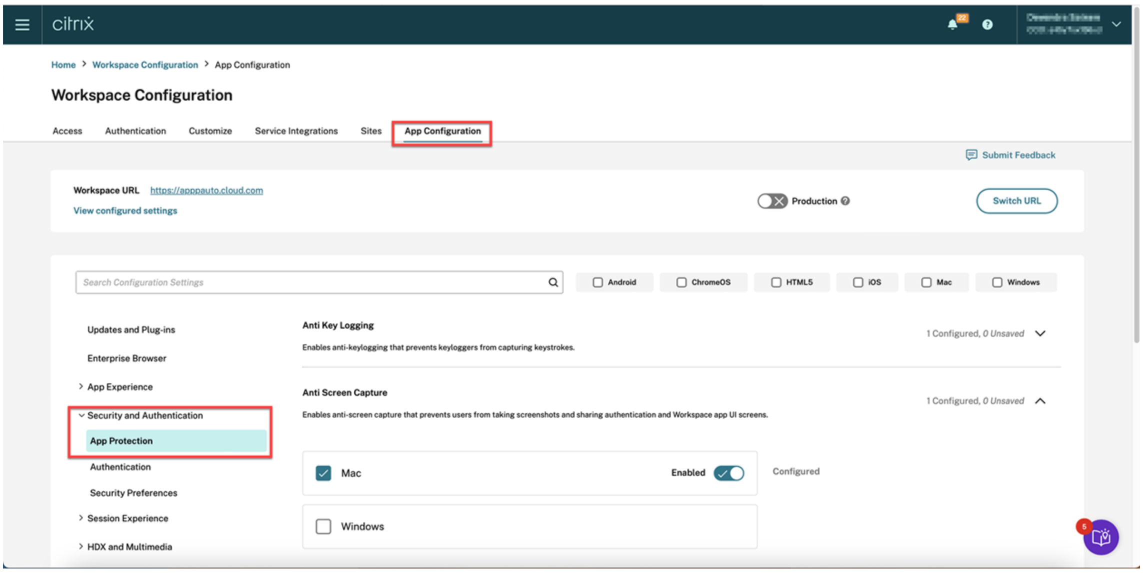
> **Note:**
>
> - Configuring anti-keylogging or anti-screen capture for authentication and self-service plug-in using GACS is applicable for Citrix Workspace app for Windows and Citrix Workspace app for Mac. It isn't applicable for Citrix Workspace app for Linux.
> - The GACS configurations don't apply for Virtual App and Desktops, and web and SaaS apps. These resources continue to be controlled using the Delivery Controller and Citrix Secure Private Access.
> - Starting with the Citrix Workspace app for Mac 2311 version, you can configure App Protection for the Authentication and Self-Service plug-in using the Global App Configuration service UI for both cloud stores and on-premises. However, if you're using Citrix Workspace app for Mac earlier than the 2311 version, then you can configure it only for cloud stores.

Administrators can configure App Protection using the Workspace Configuration UI:

1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.



2. Select **App Configuration** > **Security and Authentication** > **App Protection**.

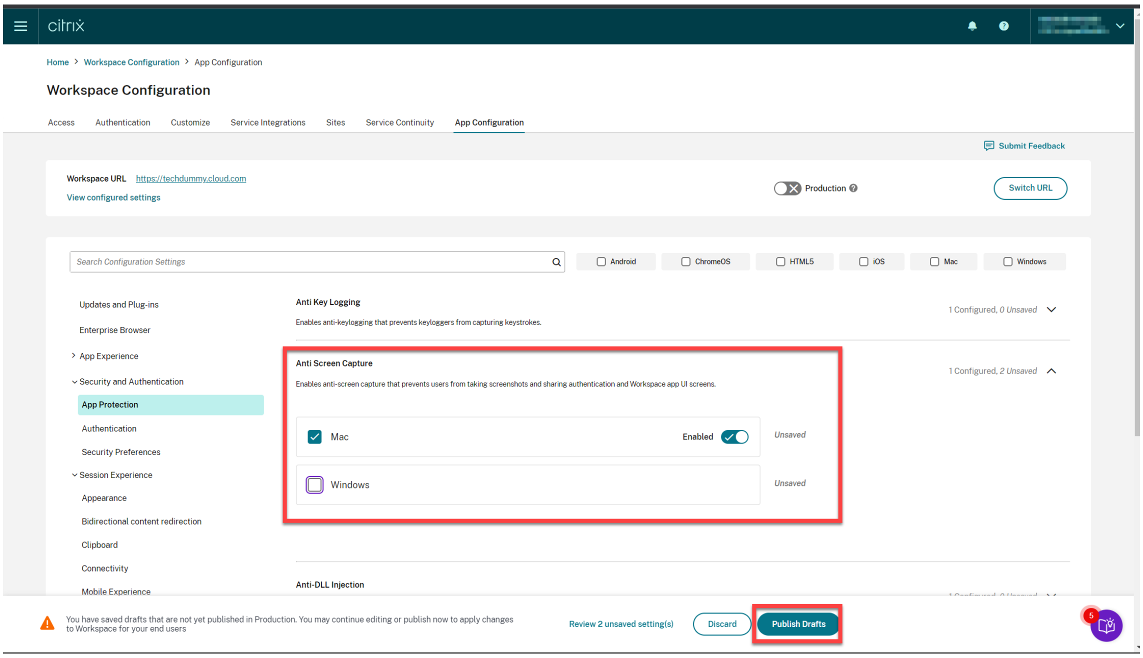


Enables anti-keylogging that prevents keyloggers from capturing keystrokes.

Enables anti-screen capture that prevents users from taking screenshots and sharing authentication and Workspace app UI screens.

3. Click **Anti Screen Capture** and then select the relevant Operating System (Windows or Mac).

4. Click the **Enabled** toggle button and then click **Publish Drafts**.



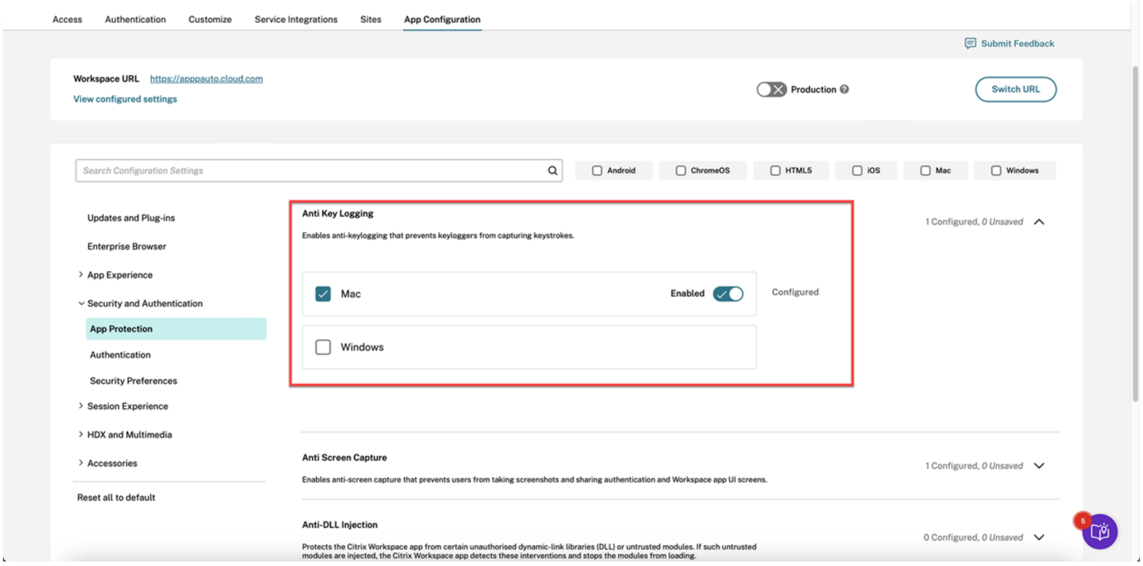
Enables anti-keylogging that prevents keyloggers from capturing keystrokes.

Enables anti-screen capture that prevents users from taking screenshots and sharing authentication and Workspace app UI screens.

You have saved drafts that are not yet published in Production. You may continue editing or publish now to apply changes to Workspace for your end users

5. Click **Anti Key Logging** and then select the relevant Operating System (Windows or Mac).

6. Click the **Enabled** toggle button and then click **Publish Drafts**.



Anti Key Logging

Enables anti-keylogging that prevents keyloggers from capturing keystrokes.

☑ Mac Enabled Configured

□ Windows

1 Configured, 0 Unsaved

Anti Screen Capture

Enables anti-screen capture that prevents users from taking screenshots and sharing authentication and Workspace app UI screens.

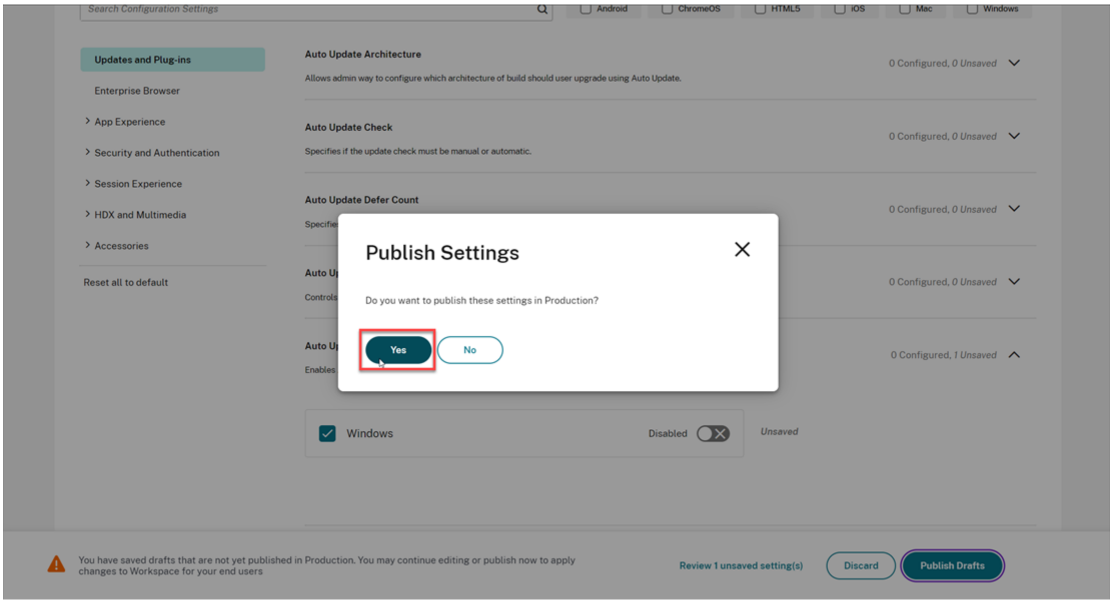
1 Configured, 0 Unsaved

Anti-DLL Injection

Protects the Citrix Workspace app from certain unauthorised dynamic-link libraries (DLL) or untrusted modules. If such untrusted modules are injected, the Citrix Workspace app detects these interventions and stops the modules from loading.

0 Configured, 0 Unsaved

7. In the **Publish Settings** dialog box, click **Yes**.



Auto Update Architecture

Allows admin way to configure which architecture of build should user upgrade using Auto Update.

0 Configured, 0 Unsaved

Auto Update Check

Specifies if the update check must be manual or automatic.

0 Configured, 0 Unsaved

Auto Update Defer Count

0 Configured, 0 Unsaved

Publish Settings

Do you want to publish these settings in Production?

0 Configured, 0 Unsaved

0 Configured, 1 Unsaved

☑ Windows Disabled Unsaved

You have saved drafts that are not yet published in Production. You may continue editing or publish now to apply changes to Workspace for your end users

Using Global App Configuration service API

The administrators can use the API to configure these App Protection features. The settings are as follows:

- **Setting to enable or disable anti-screen capturing:**

  "name": "enable anti screen capture for auth and ssp"
  "value": "true"or "false"

- **Setting to enable or disable anti-keylogging:**

> “name”: “enable anti key-logging for auth and ssp”
> “value”: “true”or “false”

Example: Following is a sample JSON file to enable anti-screen capture and anti-keylogging features for Citrix Workspace app in GACS:

```
{


          "category": "App Protection",

          "userOverride": true,

          "assignedTo": [

            "AllUsersNoAuthentication"

          ],

          "settings": [

            {


              "name": "enable anti screen capture for auth and ssp",

              "value": true

             }
 ,

            {


              "name": "enable anti key-logging for auth and ssp",

              "value": true

             }


          ] }
```

Using AuthManConfig.xml for an authentication manager

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i authmananti -A 1
    <key>AuthManAntiScreenCaptureEnabled</key>
    <value>true</value>
    <key>AuthManAntiKeyLoggingEnabled</key>
    <value>true </value>

<!--NeedCopy-->
```

Using AuthManConfig.xml for the Self-Service Plug-in interface

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i protection -A 4
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>

<!--NeedCopy-->
```

Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops

Two policies provide anti-keylogging and anti-screen capturing functionality in a session. You can configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops as follows:

> **Note:**
>
> From version 2103, Citrix DaaS supports App Protection with StoreFront and Workspace.

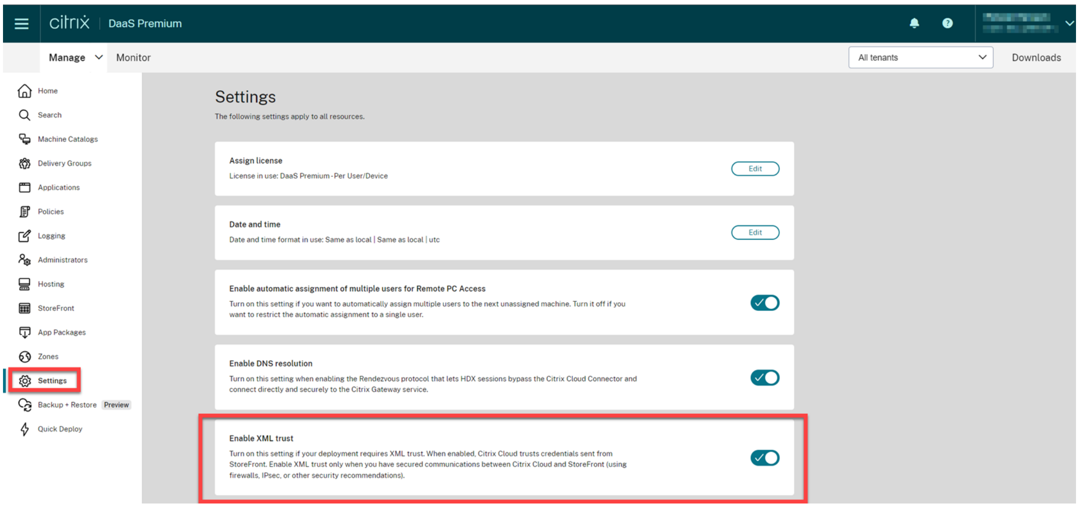
For information on App Protection configuration on Citrix Virtual Apps and Desktops and Citrix DaaS, see App Protection.

Using Web Studio

To configure Anti-keylogging and Anti-screen capture for Citrix Virtual Apps or Desktops through Web Studio, do the following steps:

1. App Protection requires XML trust. To enable XML trust, do the following steps:

    a) Sign in to your Citrix DaaS account and go to **Manage** > **Settings** > **Enable XML trust**.



Settings

The following settings apply to all resources.

Assign license

License in use: DaaS Premium - Per User/Device

Date and time

Date and time format in use: Same as local | Same as local | utc

Enable automatic assignment of multiple users for Remote PC Access

Turn on this setting if you want to automatically assign multiple users to the next unassigned machine. Turn it off if you want to restrict the automatic assignment to a single user.

Enable DNS resolution

Turn on this setting when enabling the Rendezvous protocol that lets HDX sessions bypass the Citrix Cloud Connector and connect directly and securely to the Citrix Gateway service.

Enable XML trust

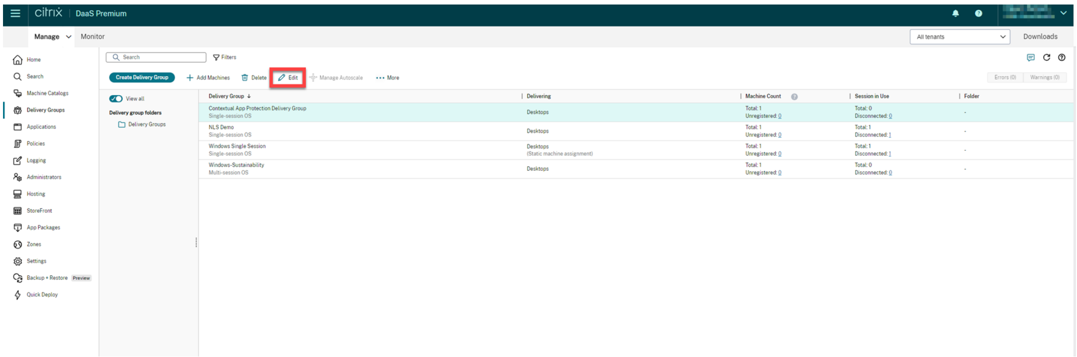
Turn on this setting if your deployment requires XML trust. When enabled, Citrix Cloud trusts credentials sent from StoreFront. Enable XML trust only when you have secured communications between Citrix Cloud and StoreFront (using firewalls, IPsec, or other security recommendations).

b) Turn on the **Enable XML trust** toggle.

2. To choose an App Protection method for a delivery group, do the following steps:

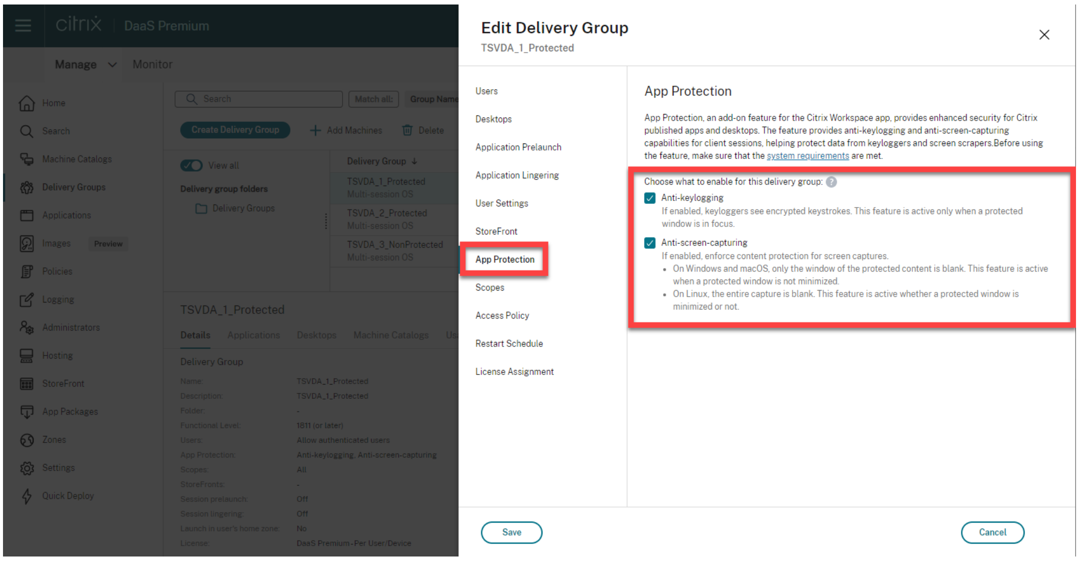
    a) In Citrix DaaS, go to **Manage** > **Delivery Groups**.

    b) Select a delivery group and then click **Edit** in the action bar.



Delivery Group	Delivering	Machine Count	Session in Use	Folder
Contextual App Protection Delivery Group Single-session OS	Desktops	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0	-
NLS Demo Single-session OS	Desktops	Total: 1 Unregistered: 0	Total: 1 Disconnected: 1	-
Windows Single Session Single-session OS	Desktops (Static machine assignment)	Total: 1 Unregistered: 0	Total: 1 Disconnected: 1	-
Windows-Sustainability Multi-session OS	Desktops	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0	-

    c) Click **App Protection** and then select **Anti-keylogging** and **Anti-screen capturing** checkboxes.



Edit Delivery Group
TSVDA_1_Protected

App Protection

App Protection, an add-on feature for the Citrix Workspace app, provides enhanced security for Citrix published apps and desktops. The feature provides anti-keylogging and anti-screen-capturing capabilities for client sessions, helping protect data from keyloggers and screen scrapers.Before using the feature, make sure that the system requirements are met.

Choose what to enable for this delivery group:

☑ Anti-keylogging
If enabled, keyloggers see encrypted keystrokes. This feature is active only when a protected window is in focus.

☑ Anti-screen-capturing
If enabled, enforce content protection for screen captures.
- On Windows and macOS, only the window of the protected content is blank. This feature is active when a protected window is not minimized.
- On Linux, the entire capture is blank. This feature is active whether a protected window is minimized or not.

d) Click **Save**.

Using PowerShell

> **Note:**
>
> In a Citrix DaaS environment, use the cmdlets in the Citrix Virtual Apps and Desktops Remote PowerShell SDK on any machine (apart from Citrix Cloud Connector machines) to issue the commands in this section.

Enable the following properties for the App Protection Delivery Group using the Citrix Virtual Apps and Desktops SDK on any installed Delivery Controller machine or on a machine with a stand-alone Studio installed that has the FMA PowerShell snap-ins installed.

- `AppProtectionKeyLoggingRequired`: `True`
- `AppProtectionScreenCaptureRequired`: `True`

You can enable each of these policies individually per Delivery Group. For example, you can configure keylogging protection only for DG1, and screen capture protection only for DG2. You can enable both policies for DG3.

Example:

To enable both policies for a Delivery Group naming **DG3**, run the following command on any Delivery Controller in the site:

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

To validate the settings, run this cmdlet:

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

Also, enable XML trust:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Make sure that you secure the network between the StoreFront and the Broker. For more information, see Knowledge Center articles CTX236929 and Securing the XenApp and XenDesktop XML Service.

Configure Anti-keylogging and Anti-screen capture for Web and SaaS apps

Web and SaaS apps open in the Citrix Enterprise Browser for Citrix Workspace app for Windows and Citrix Workspace app for Mac. If the apps are configured to have the App Protection policies via the Citrix Secure Private Access, then App Protection is applied on a per tab basis.

Configure App Protection for Web and SaaS apps using the following:

- To configure App Protection for Web and SaaS apps for Workspace, see Citrix Secure Private Access for Citrix Workspace.
- To configure App Protection for Web and SaaS apps for StoreFront, see Citrix Secure Private Access support for StoreFront.

Configure Anti-DLL Injection

February 28, 2024

By default, the Anti-DLL Injection feature is disabled. You can enable this feature using the following:

- Group Policy Object (GPO)
- Global App Configuration service (GACS)

Configure using Group Policy Object

The following policies are added to configure the Anti-DLL Injection feature:

- Anti-DLL Injection
- Anti-DLL Injection Module Allow List

Using the Anti-DLL Injection policy

Use this policy to enable or disable the Anti-DLL Injection feature. When this policy is not configured, the Anti-DLL Injection feature is disabled. The possible values are:

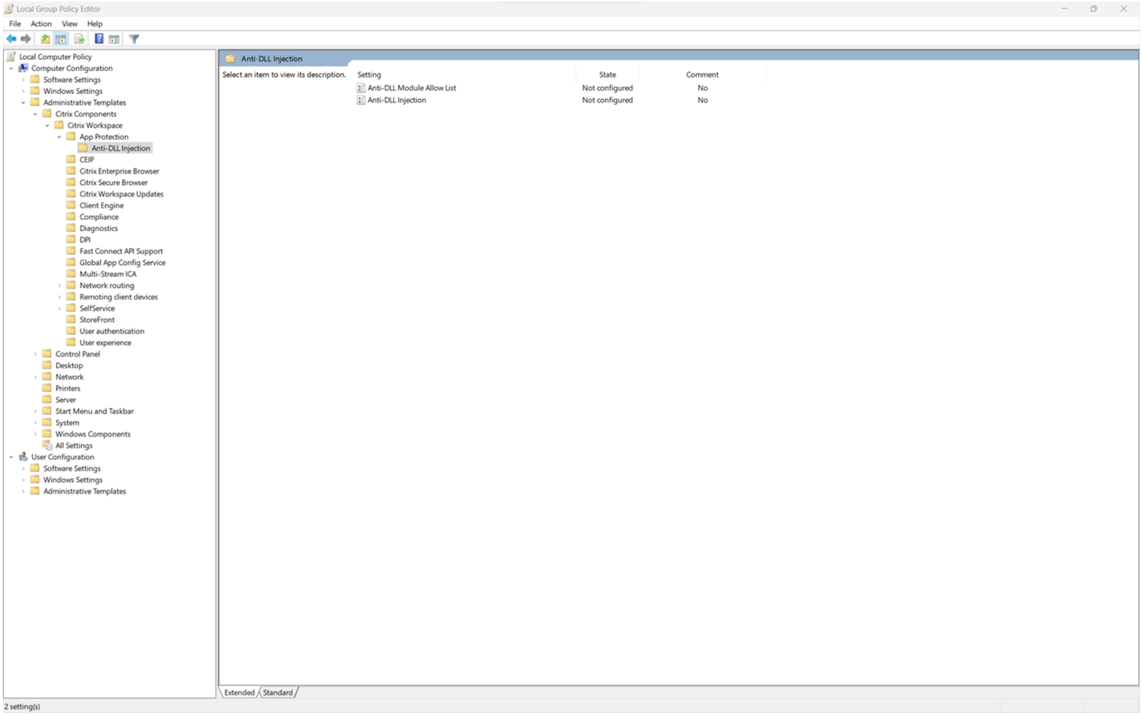
- **Enabled** –The Anti-DLL Injection feature is enabled for Citrix Authentication Manager, Citrix Workspace app UI, and Citrix Virtual Apps and Desktops. Administrators can select the required components to enable the Anti-DLL Injection feature.
- **Disabled** –The Anti-DLL Injection feature is disabled for Citrix Authentication Manager, Citrix Workspace app UI, and Citrix Virtual Apps and Desktops.

To enable the Anti-DLL Injection policy, do the following steps:

1. Open the Citrix Workspace app Group Policy Object administrative template by running the following command:

   ```
   gpedit.msc
   ```

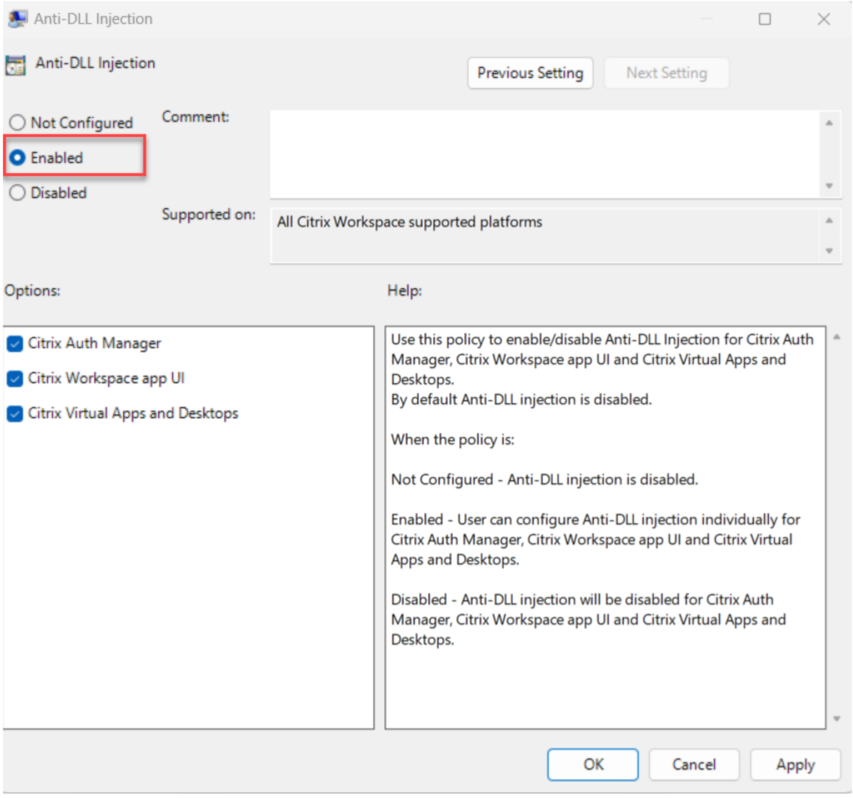
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Anti-DLL Injection**.

   Select an item to view its description.

Setting	State	Comment
Anti-DLL Module Allow List	Not configured	No
Anti-DLL Injection	Not configured	No

3. Click the **Anti-DLL Injection** policy and select **Enabled**. All the components are selected. However, you can modify the selection of the components from the Options section.



Anti-DLL Injection

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: All Citrix Workspace supported platforms

Options:

☑ Citrix Auth Manager
☑ Citrix Workspace app UI
☑ Citrix Virtual Apps and Desktops

Help:

Use this policy to enable/disable Anti-DLL Injection for Citrix Auth Manager, Citrix Workspace app UI and Citrix Virtual Apps and Desktops.
By default Anti-DLL injection is disabled.

When the policy is:

Not Configured - Anti-DLL injection is disabled.

Enabled - User can configure Anti-DLL injection individually for Citrix Auth Manager, Citrix Workspace app UI and Citrix Virtual Apps and Desktops.

Disabled - Anti-DLL injection will be disabled for Citrix Auth Manager, Citrix Workspace app UI and Citrix Virtual Apps and Desktops.

4. Click **OK**.

Using the Anti-DLL Injection Module Allow List policy

As an Administrator, you can use this policy to exclude any DLL from the Anti-DLL Injection feature. Citrix recommends you to use this policy only to handle any exceptional scenario. When this policy is not configured, no DLL is part of the allow list. All the DLLs are included for the anti-DLL protection. The possible values are:

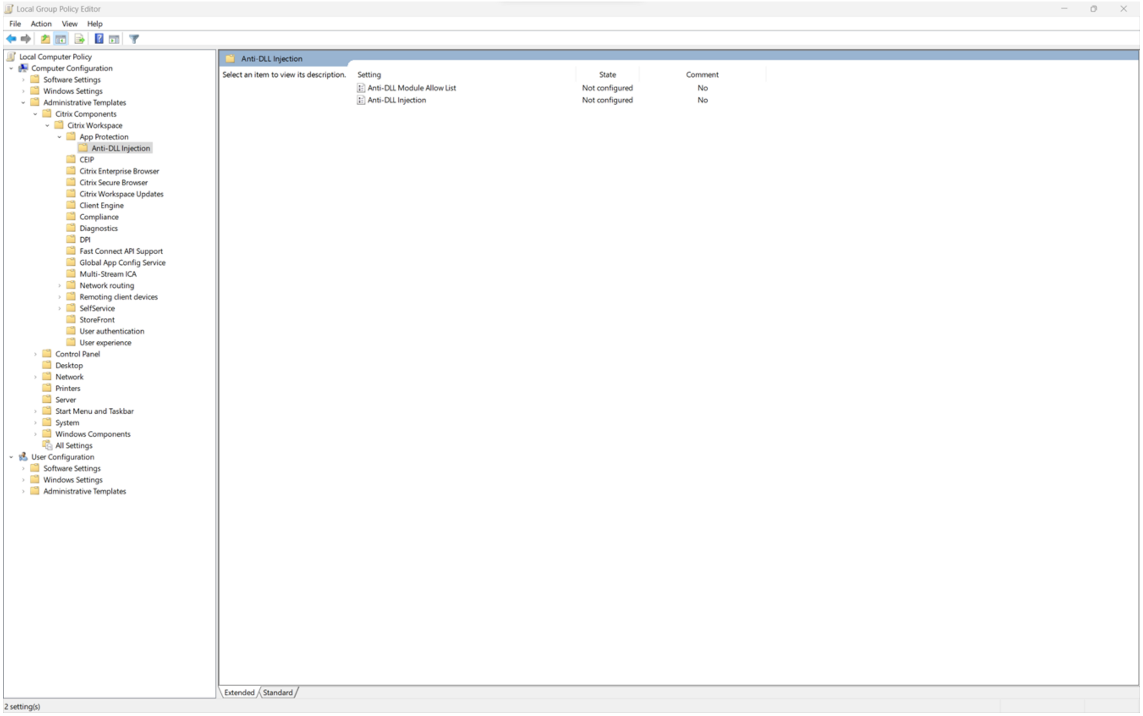
- **Enabled** - Excludes DLLs that are added in the allow list from the anti-DLL protection.
- **Disabled** - Clears the list of DLLs added to the allow list.

To enable the Anti-DLL Injection Module Allow List policy, do the following steps:

1. Open the Citrix Workspace app Group Policy Object administrative template by running the following command:

   ```
   gpedit.msc
   ```

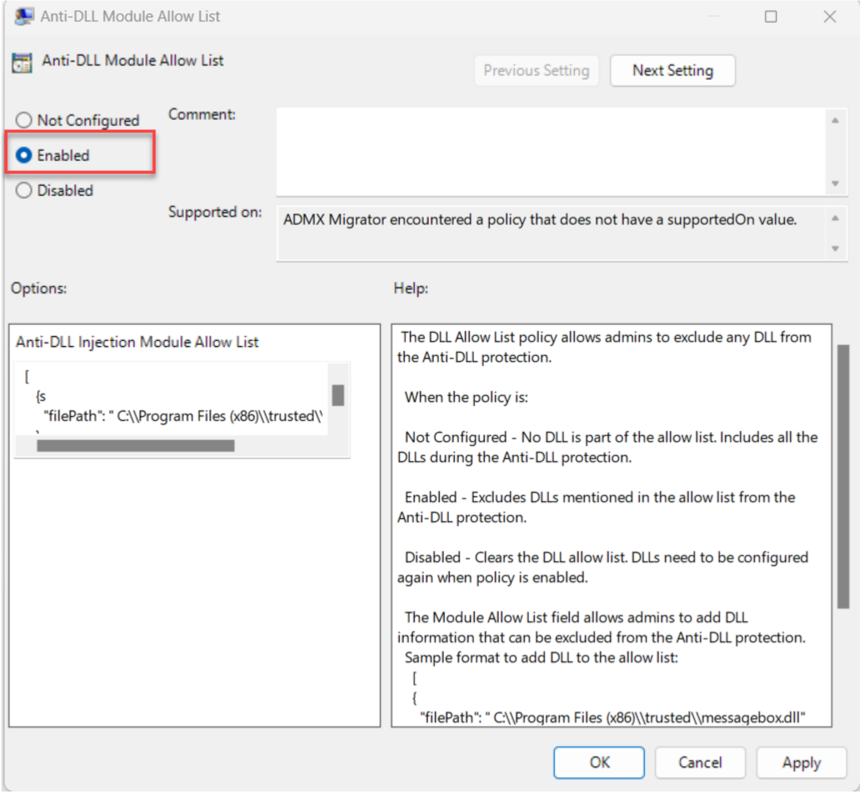
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Anti-DLL Module Allow List**.



Select an item to view its description.

Setting	State	Comment
Anti-DLL Module Allow List	Not configured	No
Anti-DLL Injection	Not configured	No

3. Click the **Anti-DLL Module Allow List** policy and select **Enabled**.



○ Not Configured
● Enabled
○ Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Anti-DLL Injection Module Allow List

```
[
  {s
    "filePath": " C:\\Program Files (x86)\\trusted\'
```

The DLL Allow List policy allows admins to exclude any DLL from the Anti-DLL protection.

When the policy is:

Not Configured - No DLL is part of the allow list. Includes all the DLLs during the Anti-DLL protection.

Enabled - Excludes DLLs mentioned in the allow list from the Anti-DLL protection.

Disabled - Clears the DLL allow list. DLLs need to be configured again when policy is enabled.

The Module Allow List field allows admins to add DLL information that can be excluded from the Anti-DLL protection.
Sample format to add DLL to the allow list:

```
[
{
"filePath": " C:\\Program Files (x86)\\trusted\\messagebox.dll"
```

4. Add the list of modules that you want to exclude from the anti-DLL protection in the **Anti-DLL Injection Module Allow List** field.

Sample format to add DLL to the allow list:

```
[
    {

        "filePath":"C:\\Program Files (x86)\\trusted\\messagebox.dll"
     }
 ,
    {

        "filePath":"%PROGRAMFILES%\\trusted\\logging.dll"
     }

]
<!--NeedCopy-->
```

5. Click **OK**.

Configure using the Global App Configuration service

The Administrators can use GACS to configure the Anti-DLL Injection feature. The settings are as follows:

- anti dll injection –Add the required modules that you want to enable the anti-DLL Injection feature
- anti dll module allow list –Add the required DLLs that you want to exclude from the anti-DLL protection

For more information, see Global App Configuration service.

The following is a sample JSON file for enabling **anti dll injection** and **anti dll module allow list** for Citrix Workspace app for Windows in GACS:

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "assignmentPriority": 0,
          "settings": [
            {

              "name": "anti dll injection",
              "value": [
                "Citrix Auth Manager",
                "Citrix Virtual Apps And Desktops",
                "Citrix Workspace app UI"
              ]
             }
 ,
            {

              "name": "anti dll module allow list",
              "value": [
                {

                  "filePath": "C:\\Program Files (x86)\\Citrix\\ICA Client\\wfica32.exe"
                 }
 ,
                {

                  "filePath": "C:\\Program Files (x86)\\Citrix\\ICA Client\\AuthManager\\AuthManSvr.exe"
                 }

              ]
             }

          ]
         }

      ]
     }
 ,
    "name": "name",
    "description": "desc",
    "useForAppConfig": true
   }

 }

<!--NeedCopy-->
```

Configure Policy Tampering Detection

February 28, 2024

Prerequisites

To configure Policy Tampering Detection feature, make sure that you have the following:

- For cloud deployments - Cloud Desktop Delivery Controller version 115 or later
- For on-premises deployments - Citrix Virtual Apps and Desktops version 2308 or later
- Windows Virtual Delivery Agent Installer version 2308 or later
- For Windows - Citrix Workspace app for Windows 2309 or later
- For Mac - Citrix Workspace app for Mac 2308 or later
- For Linux - Citrix Workspace app for Linux 2308 or later

To enable Policy Tampering Detection, the admin must start the **Citrix AppProtection Service** on the TS/WS VDAs which are hosting the virtual apps and desktops configured with App Protection.

Do one of the following steps to enable Policy Tampering Detection:

- Using the command prompt:

  1. On the leftmost of the taskbar, click the **Search** icon. Type **cmd** and then click **Run as administrator**. The **Command Prompt** screen appears.
  2. Run the following commands:

     ```
     sc config ctxappprotectionsvc start=auto
     sc start ctxappprotectionsvc

     <!--NeedCopy-->
     ```

- Using the user interface:

  1. On the leftmost of the taskbar, click the **Search** icon. Type **services.msc** and press **Enter**. The **Services** screen appears.
  2. Select **Citrix AppProtection Service** and then click **Start**.
  3. Right-click **Citrix AppProtection Service** and then select **Properties**.
  4. Select **General** > **Startup type** > **Automatic** and then click **OK** to make sure that the service starts automatically when the system starts.

Policy Tampering Detection feature is enabled successfully.

To detect and block prior versions of Citrix Workspace app that do not support Policy Tampering Detection, configure App Protection Posture Check. For more information about App Protection Posture Check, see App Protection Posture Check.

Configure App Protection Posture Check

February 28, 2024

To enable App Protection Posture Check, configure the new VDA Citrix Policy that is related to this feature.

Prerequisites

Make sure that you have the following:

- For cloud deployments - Cloud Desktop Delivery Controller version 115 or later
- For on-premises deployments - Citrix Virtual Apps and Desktops version 2308 or later
- Windows Virtual Delivery Agent Installer version 2308 or later
- For Windows - Citrix Workspace app for Windows 2309 or later
- For Mac - Citrix Workspace app for Mac 2308 or later
- For Linux - Citrix Workspace app for Linux 2308 or later

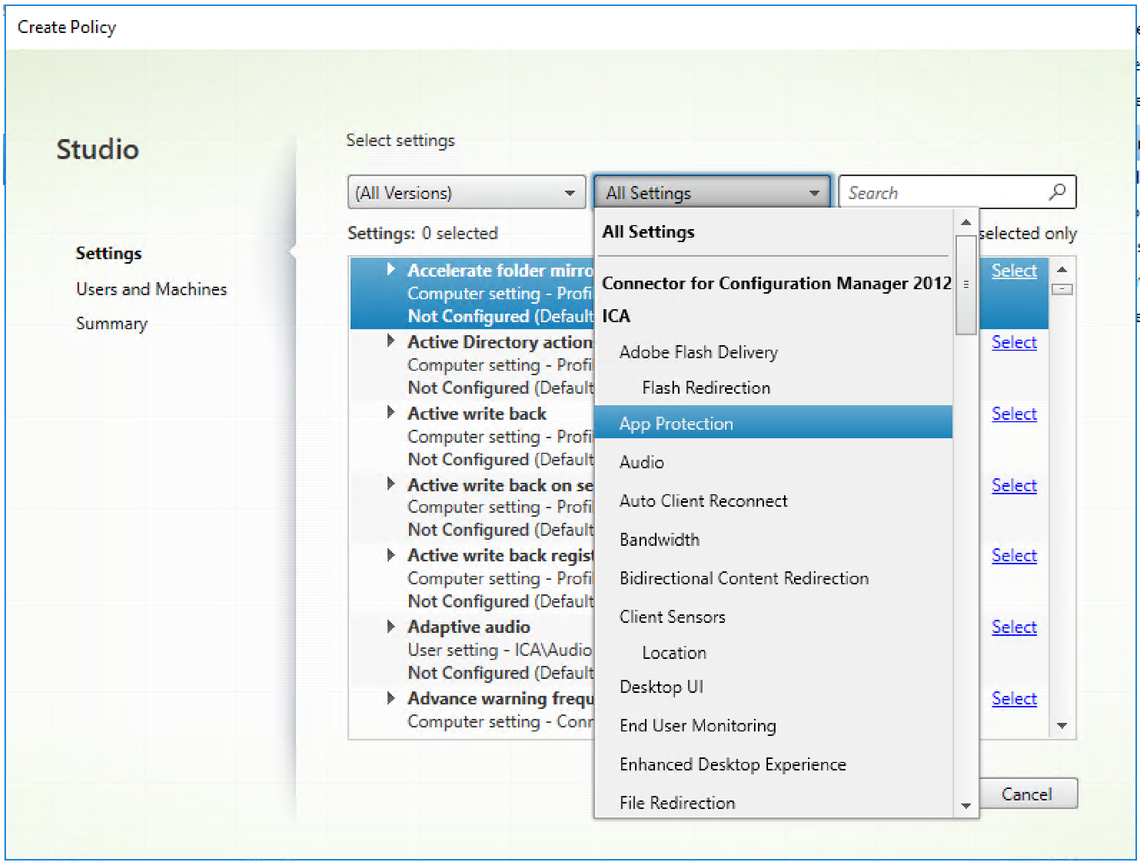
Configure the new VDA Citrix Policy for Posture Check as follows:

> **Note:**
>
> This new VDA Citrix Policy can be deployed using both Citrix Studio and Web Studio. The following procedure is deployed via Citrix Studio and you can use the same procedure for Web Studio also.

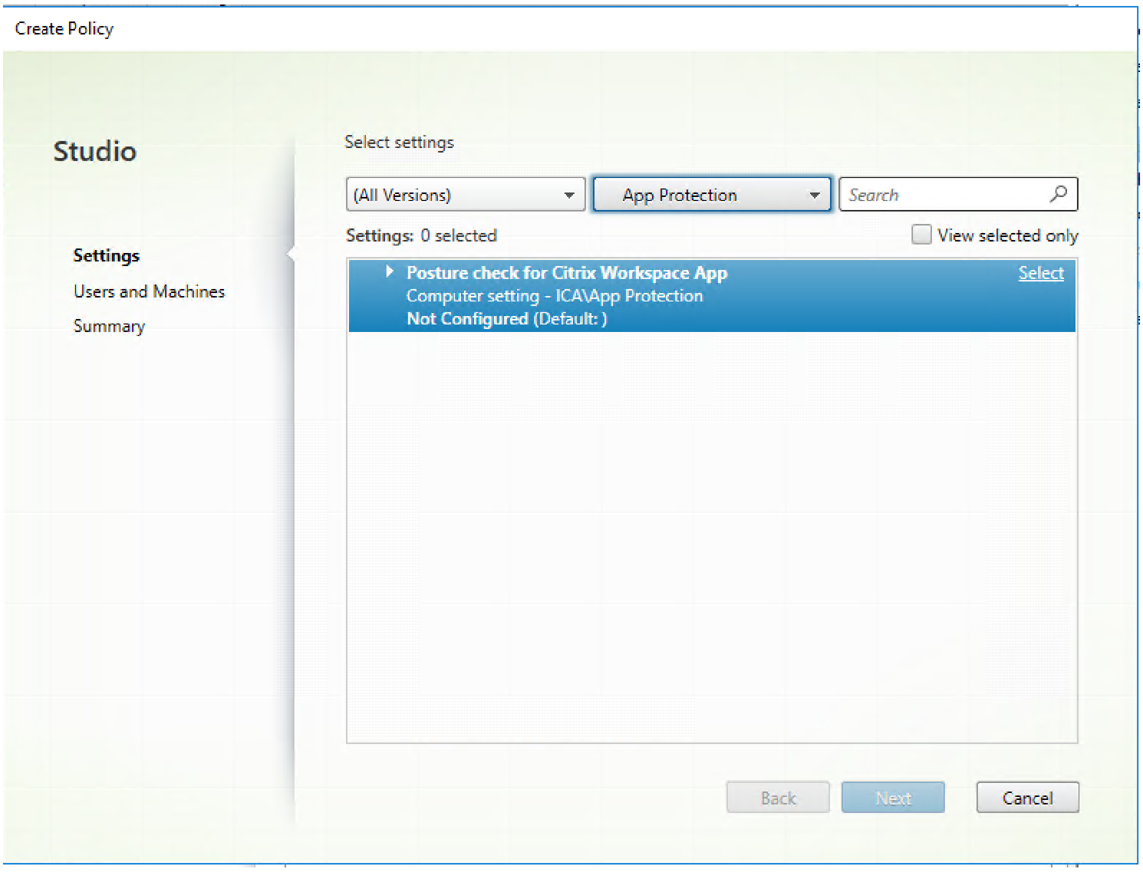
1. Open the Citrix Studio app on the Desktop Delivery Controller (DDC) for on-prem or Web Studio for Cloud deployments and then select **Policies**.

2. Under **Actions**, select **Policies** > **Create Policy**.

3. Click the **All Settings** drop-down menu and select **App Protection** under **ICA**.



4. Select **Posture check for Citrix Workspace app** and then click **Select**.



Settings: 0 selected

□ View selected only

Posture check for Citrix Workspace App
Computer setting - ICA\App Protection
Not Configured (Default:)

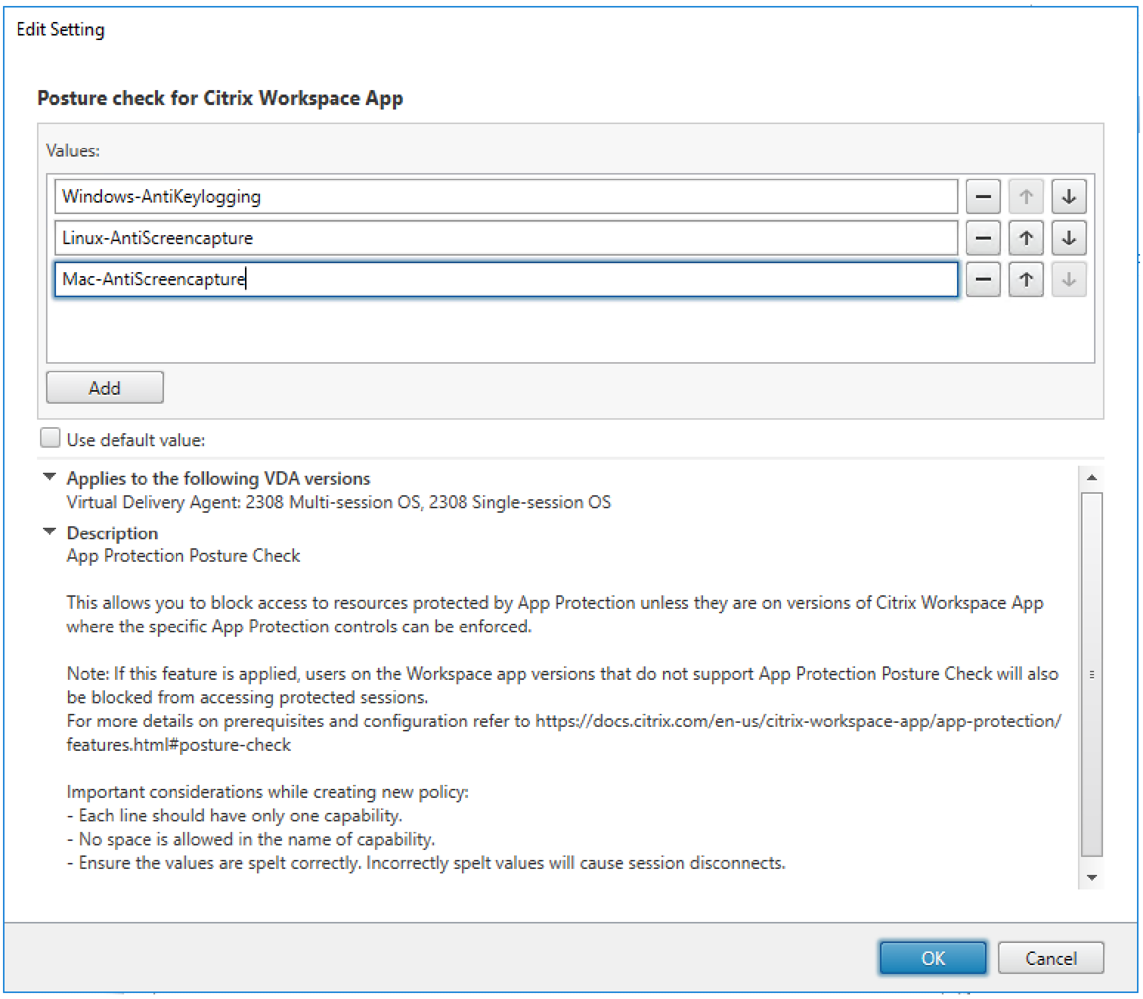
Select

The **Edit Setting** window appears.

5. Clear the **Use default value** checkbox.
6. Click **Add** and enter the relevant values from the following:

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

   For example, If you've added "Windows-AntiScreencapture"and "Windows-AntiKeylogging" , then the Citrix Workspace app for Windows that supports Posture Check and has these capabilities is allowed to connect to the VDA.



Posture check for Citrix Workspace App

Values:

Windows-AntiKeylogging

Linux-AntiScreencapture

Mac-AntiScreencapture

□ Use default value:

Applies to the following VDA versions

Virtual Delivery Agent: 2308 Multi-session OS, 2308 Single-session OS

Description

App Protection Posture Check

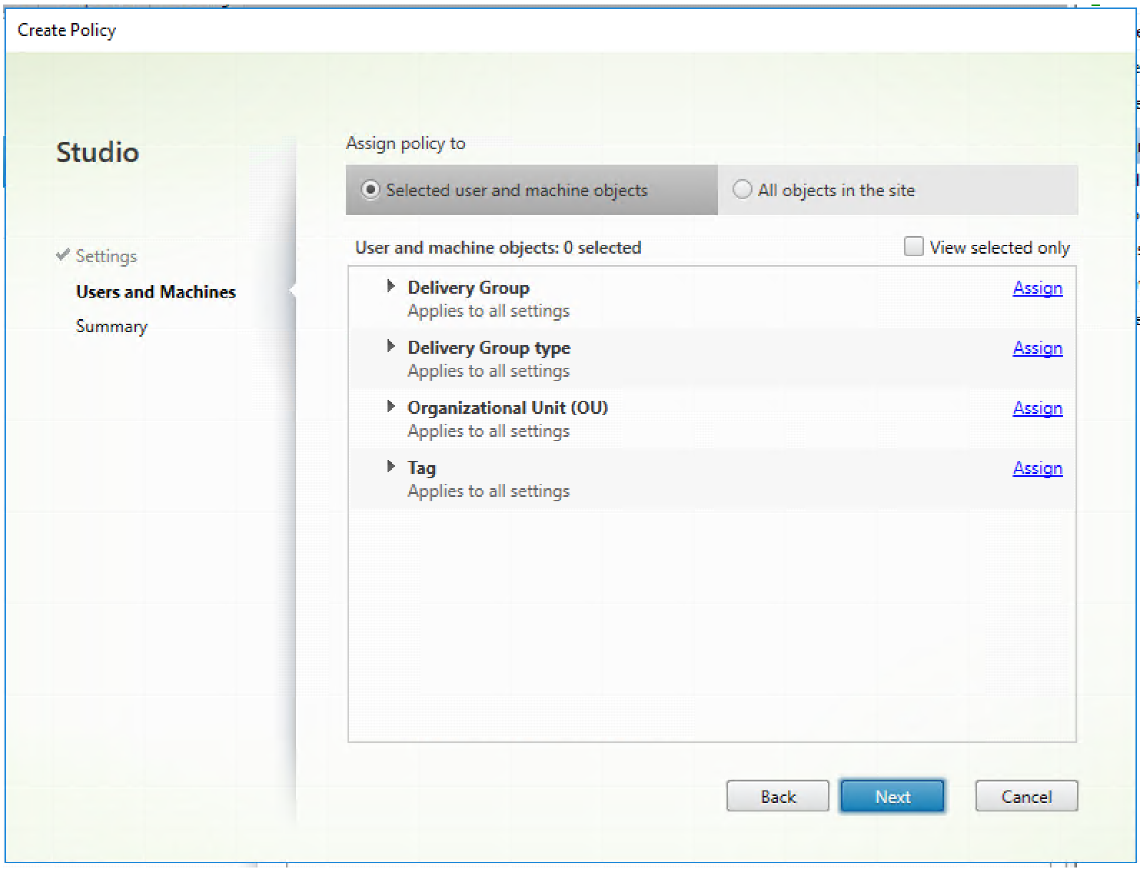
This allows you to block access to resources protected by App Protection unless they are on versions of Citrix Workspace App where the specific App Protection controls can be enforced.

Note: If this feature is applied, users on the Workspace app versions that do not support App Protection Posture Check will also be blocked from accessing protected sessions.
For more details on prerequisites and configuration refer to https://docs.citrix.com/en-us/citrix-workspace-app/app-protection/features.html#posture-check

Important considerations while creating new policy:
- Each line should have only one capability.
- No space is allowed in the name of capability.
- Ensure the values are spelt correctly. Incorrectly spelt values will cause session disconnects.

> **Note:**
>
> - Each entry must have only one capability.
> - No space is allowed in the name of capability.
> - Make sure that the values are spelt correctly. Incorrectly spelt values cause the session to terminate.
> - Values that don't have the prefix Windows-, Linux-, or Mac- are ignored.

7. After adding all the required values, click **OK**.
8. Click **Next**.
9. Select **Assign Policy to** > **Selected users and machine objects**.



Create Policy

Studio

✓ Settings

Users and Machines

Summary

Assign policy to

● Selected user and machine objects ○ All objects in the site

User and machine objects: 0 selected □ View selected only

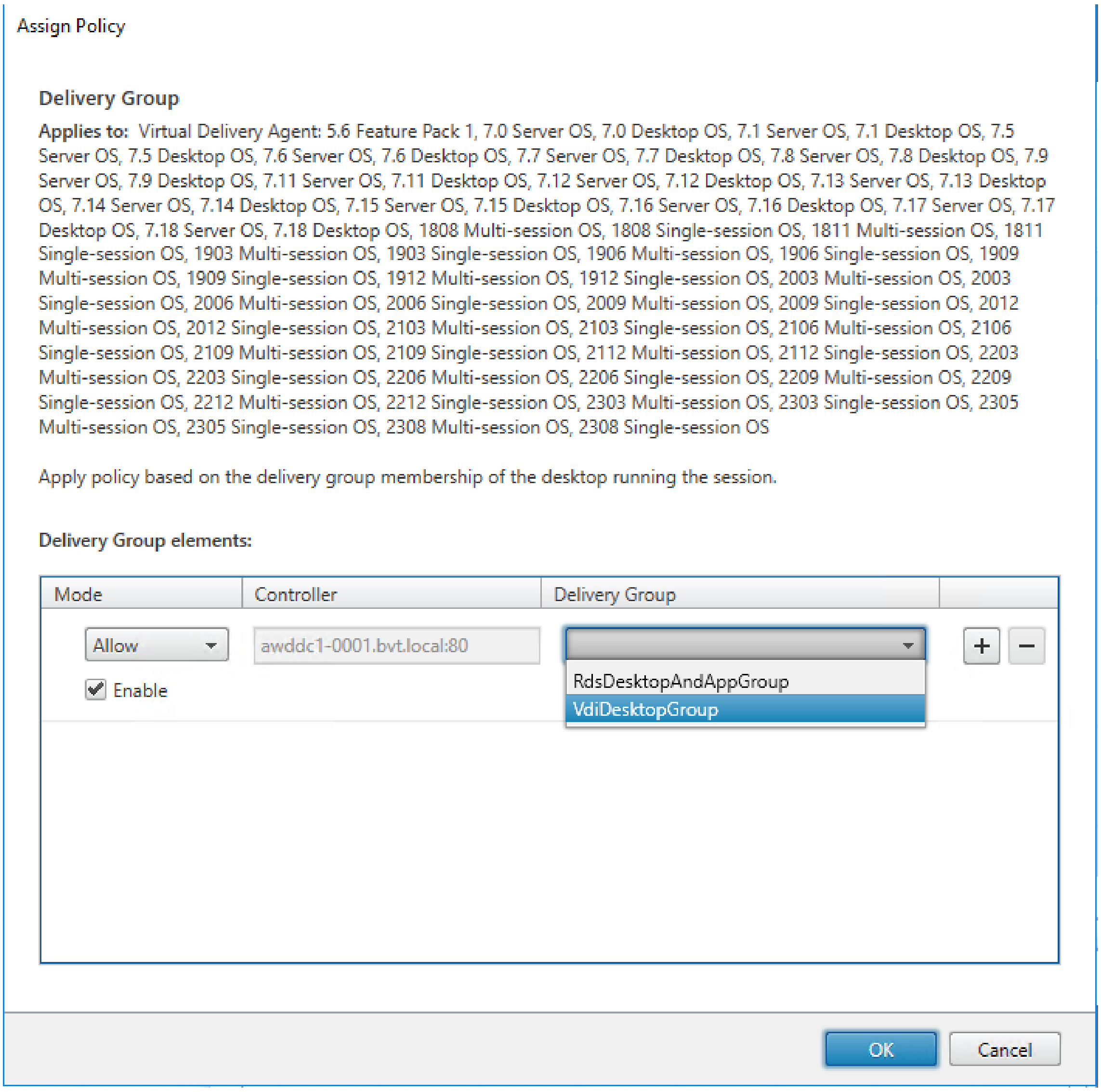
Delivery Group Assign
Applies to all settings

Delivery Group type Assign
Applies to all settings

Organizational Unit (OU) Assign
Applies to all settings

Tag Assign
Applies to all settings

10. Select the required delivery groups where this policy must be deployed and then click **OK**.



Assign Policy

Delivery Group

Applies to: Virtual Delivery Agent: 5.6 Feature Pack 1, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS, 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 1808 Multi-session OS, 1808 Single-session OS, 1811 Multi-session OS, 1811 Single-session OS, 1903 Multi-session OS, 1903 Single-session OS, 1906 Multi-session OS, 1906 Single-session OS, 1909 Multi-session OS, 1909 Single-session OS, 1912 Multi-session OS, 1912 Single-session OS, 2003 Multi-session OS, 2003 Single-session OS, 2006 Multi-session OS, 2006 Single-session OS, 2009 Multi-session OS, 2009 Single-session OS, 2012 Multi-session OS, 2012 Single-session OS, 2103 Multi-session OS, 2103 Single-session OS, 2106 Multi-session OS, 2106 Single-session OS, 2109 Multi-session OS, 2109 Single-session OS, 2112 Multi-session OS, 2112 Single-session OS, 2203 Multi-session OS, 2203 Single-session OS, 2206 Multi-session OS, 2206 Single-session OS, 2209 Multi-session OS, 2209 Single-session OS, 2212 Multi-session OS, 2212 Single-session OS, 2303 Multi-session OS, 2303 Single-session OS, 2305 Multi-session OS, 2305 Single-session OS, 2308 Multi-session OS, 2308 Single-session OS

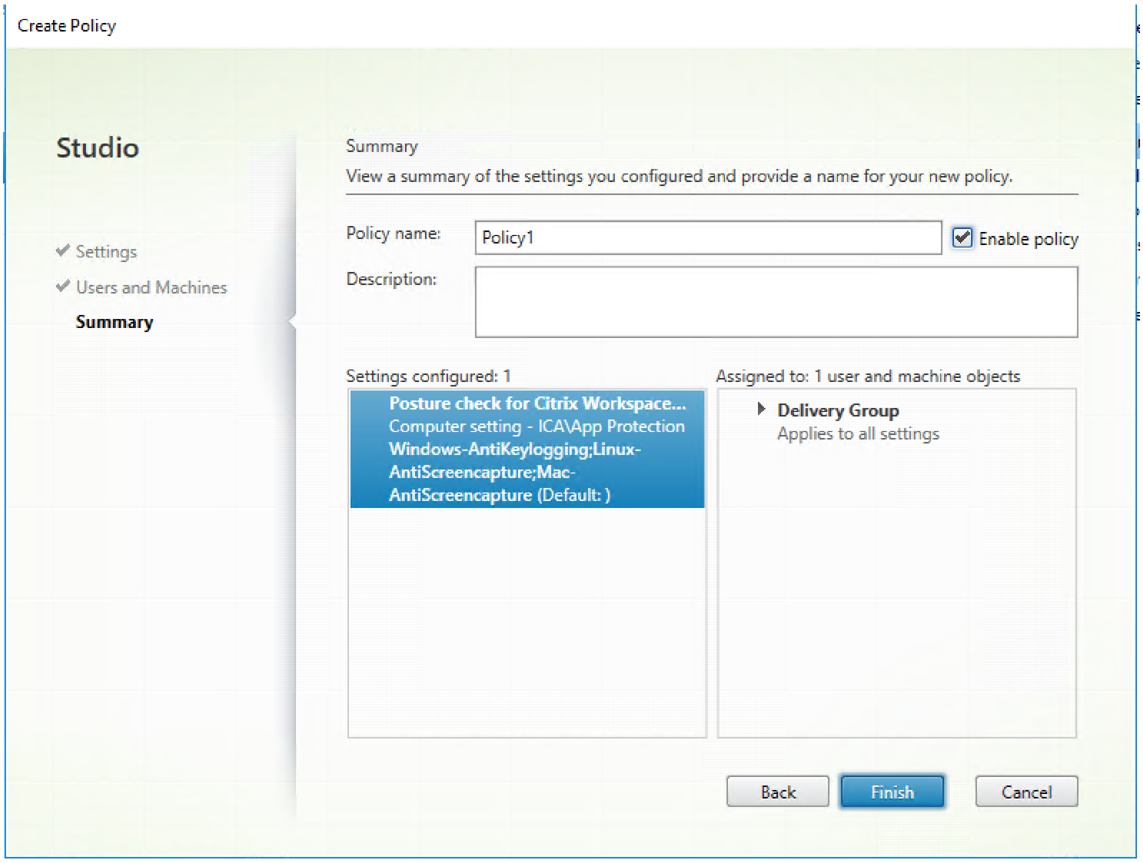
Apply policy based on the delivery group membership of the desktop running the session.

Delivery Group elements:

Mode	Controller	Delivery Group	
Allow ☑ Enable	awddc1-0001.bvt.local:80	RdsDesktopAndAppGroup VdiDesktopGroup	+ −

11. Click **Next**.

12. Enter the policy name in the **Policy name** field and then select the **Enable policy** checkbox.



Create Policy

Summary

View a summary of the settings you configured and provide a name for your new policy.

Policy name: Policy1 ☑ Enable policy

Description:

Settings configured: 1

Posture check for Citrix Workspace...
Computer setting - ICA\App Protection
Windows-AntiKeylogging;Linux-AntiScreencapture;Mac-AntiScreencapture (Default:)

Assigned to: 1 user and machine objects

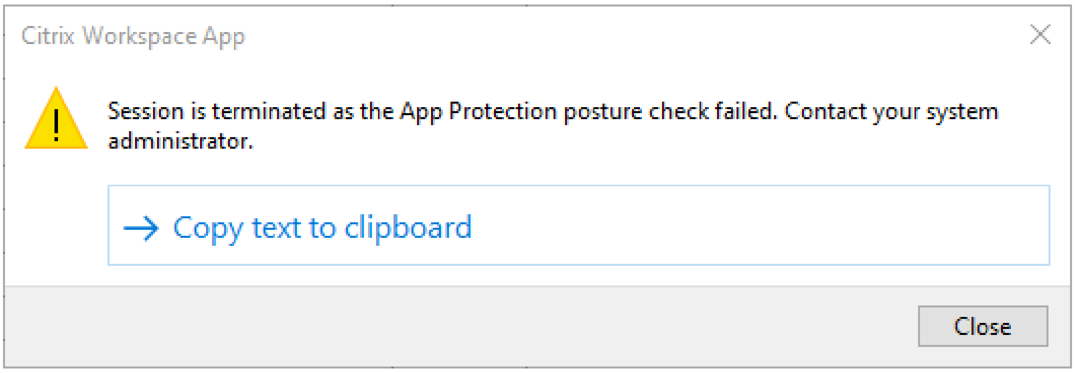
Delivery Group
Applies to all settings

13. Click **Finish**.

A policy for posture check is created.

Expected behavior if App Protection Posture Check fails

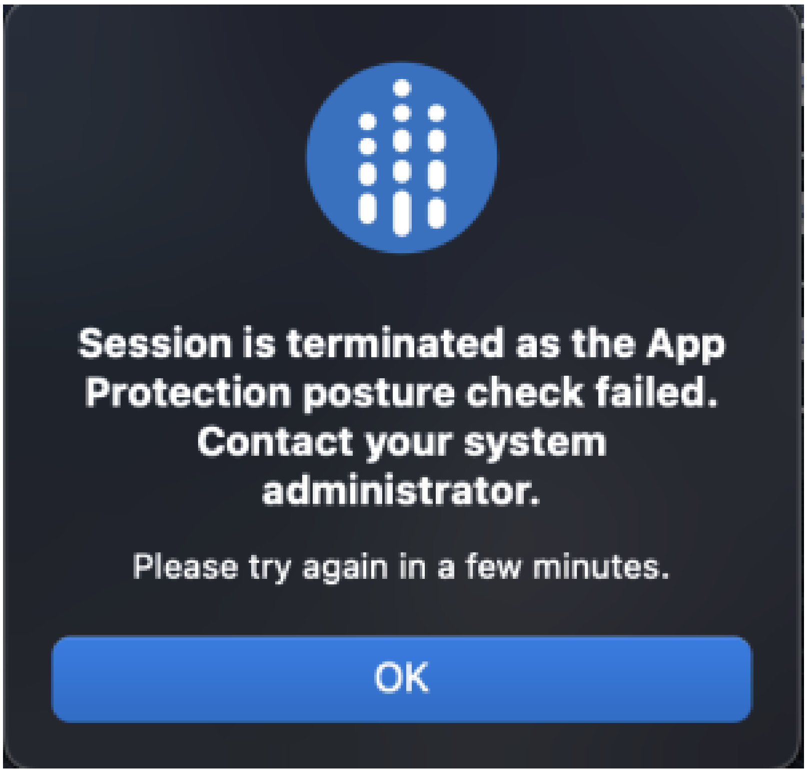
- If the Posture Check VDA Citrix Policy is enabled and you're using a Citrix Workspace app version that does not support the Posture Check feature, then the session is terminated without displaying any error message.
- If you're using a Citrix Workspace app version that supports the Posture Check feature, then the session is terminated displaying the following error messages respectively:
  - Windows:



Citrix Workspace App

Session is terminated as the App Protection posture check failed. Contact your system administrator.

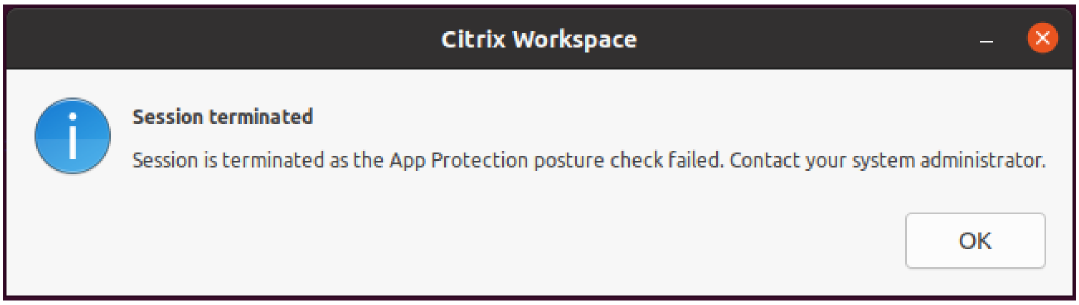
- Mac



Session is terminated as the App Protection posture check failed. Contact your system administrator.

Please try again in a few minutes.

- Linux



Citrix Workspace

Session terminated

Session is terminated as the App Protection posture check failed. Contact your system administrator.

Block DoubleHop Launch

February 28, 2024

To block double hop launch, make sure that you're running Citrix Workspace app for Windows 2309 or later on the first hop.

Deploy the following configurations to all VDAs on the first hop:

1. Update the latest GPO policies. For more information, see Update latest GPO policies.
2. Launch **Group Policy Editor** and then go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Block DoubleHop Launch**.
3. Select **Enabled** and then click **OK**.

   Block DoubleHop Launch setting is enabled and you're blocked if you try to do double hop launch.

> **Note:**
>
> Windows Server OS doesn't support App Protection. So, the Virtual Apps and Desktops that are enabled with App Protection aren't displayed if you're running a Windows server OS on the first hop.

Troubleshoot

February 28, 2024

This article explains how to troubleshoot App Protection on different platforms for Citrix Workspace app.

For troubleshooting scenarios, see the following:

- Generic troubleshooting scenarios
- Policy Tampering Detection
- App Protection Posture Check

Citrix Workspace app for Windows

1. Collect logs as described in log collection.

2. Press **Win + R** to open the Run box > type `cmd` > Select **Enter**.
3. Run the following commands:
   - If you are using a Citrix Workspace app for Windows version before 2311, then run the following commands:
     - `sc query appprotectionsvc`
     - `sc query entryprotectdrv`
     - `sc query epinject6`
     - `sc query epusbfilter`
   - If you are using Citrix Workspace app for Windows version 2311 or later, then run the following commands:
     - `sc query appprotectionsvc`
     - `sc query ctxapdriver`
     - `sc query ctxapinject`
     - `sc query ctxapusbfilter`

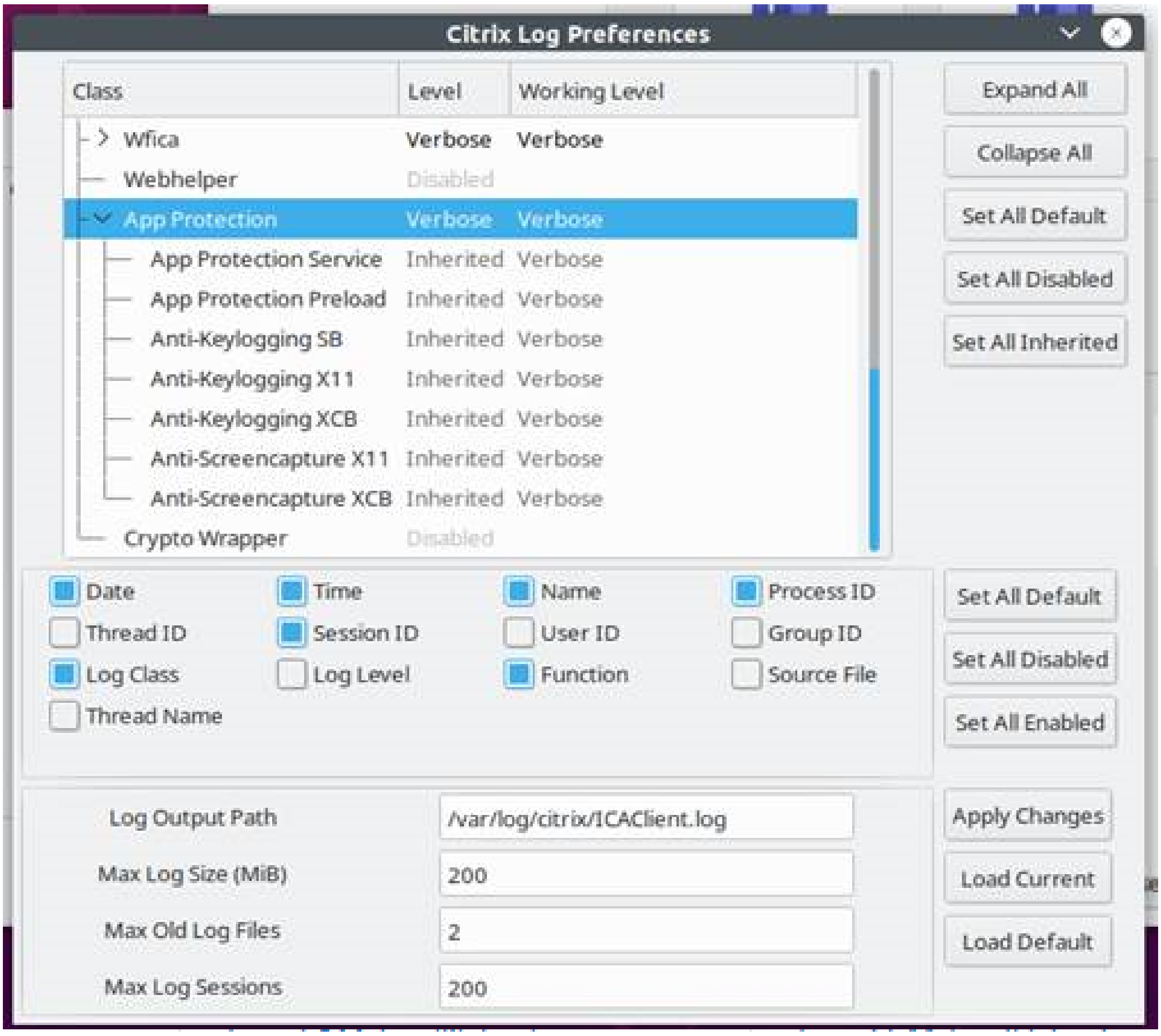
Provide the results along with the traces collected from the log collection tool.

Citrix Workspace app for Mac

Provide the logs by collecting them as described in log collection.

Citrix Workspace app for Linux

1. Run the set log executable found in the *util* folder of the installation. For example, `/opt/Citrix/ICAClient/util/setlog`.
2. Click **Set All Disabled** (This step is optional, and makes sure that only the required logs are collected).
3. Go to App Protection logging.
4. Set App Protection log level to Verbose by right-clicking and selecting Verbose (only warnings and errors are logged).
5. Expand the App Protection class and right-click its child element. Select **Group > Inherited**.
6. Enable logs for **wfica**. Right-click **wfica** and select **Verbose**. If App Protection is not installed or not detectable by **wfica**, then you get the log as **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
7. When you launch the session, the logs are recorded in the file that is mentioned in the *Log output Path* of the set log.



Class	Level	Working Level
Wfica	Verbose	Verbose
Webhelper	Disabled	
App Protection	Verbose	Verbose
App Protection Service	Inherited	Verbose
App Protection Preload	Inherited	Verbose
Anti-Keylogging SB	Inherited	Verbose
Anti-Keylogging X11	Inherited	Verbose
Anti-Keylogging XCB	Inherited	Verbose
Anti-Screencapture X11	Inherited	Verbose
Anti-Screencapture XCB	Inherited	Verbose
Crypto Wrapper	Disabled	

☑ Date ☑ Time ☑ Name ☑ Process ID
□ Thread ID ☑ Session ID □ User ID □ Group ID
☑ Log Class □ Log Level ☑ Function □ Source File
□ Thread Name

Log Output Path: /var/log/citrix/ICAClient.log
Max Log Size (MiB): 200
Max Old Log Files: 2
Max Log Sessions: 200

Generic troubleshooting

February 28, 2024

Resources enabled with App Protection policies aren't displayed on native apps

If the resources enabled with App Protection policies aren't displayed on the native apps, then do the following steps:

1. Update your Citrix Workspace app to any higher version if it's older than the following:

   - Citrix Workspace app 2108 for Linux

  - Citrix Workspace app 2203.1 LTSR for Windows
  - Citrix Workspace app 2002 for Windows
  - Citrix Workspace app 2305.1 for Windows (Store)
  - Citrix Workspace app 2001 for Mac

2. Make sure that you haven't installed the Citrix Workspace app in a Windows Multisession Operating System such as Windows 2K16 or Windows 2K22.

3. If the preceding conditions are met but still the resources aren't displayed, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Resources enabled with App Protection policies aren't displayed on the browser while using the on-premises store

If the resources enabled with App Protection policies aren't displayed on the browser while using the on-premises store, then do the following steps:

1. Make sure that your Delivery Controller version isn't before version 1912.

   > **Note:**
   >
   > App Protection isn't supported if you're using a Delivery Controller before version 1912.

2. If you're using StoreFront versions between 1912 and 2203, verify if you've enabled the StoreFront customization. For more information about enabling StoreFront customization, see Enable StoreFront customization.

3. If you're using StoreFront version 2308 or later, you don't need to enable the StoreFront customization. Verify if you've enabled App Protection for hybrid launch on StoreFront correctly using Hybrid launch through StoreFront version 2308 or later.

4. Verify if you've enabled the App Protection features for the delivery group correctly.

5. If the preceding conditions are met but the resources are still not displayed, collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Collect Logs for Citrix Workspace app and Collect Logs for StoreFront.

Unable to establish a secure environment when launching App Protection-enabled resources

For the Citrix Workspace app for Windows, the **Start App Protection after installation** checkbox must be enabled during the installation to make sure that the App Protection services are started and the secure environment is established. If you didn't enable the **Start App Protection after installation** checkbox during the installation, the App Protection service starts automatically when you launch a resource enabled with App Protection policies. Based on the system load, App Protection might take time to start. Sometimes, it might start or time out. So, selecting the **Start App Protection after installation** checkbox during installation is recommended. Usually, re-launch the resource enabled with App Protection and the secure connection must be established. However, if you are still not able to launch the resource enabled with App Protection, then do the following steps:

1. Open Command Prompt as Admin and run the following command and check if the App Protection service is running:

   ```
   sc query AppProtectionSvc
   <!--NeedCopy-->
   ```

2. If the App Protection service is not running, then start the service by running the following command:

   ```
   sc start AppProtectionSvc
   <!--NeedCopy-->
   ```

3. If you continue to get the error, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Unable to enable or disable App Protection

If you aren't able to enable or disable App Protection for a delivery group for On-premises or Cloud using either Web Studio or PowerShell, then do the following steps:

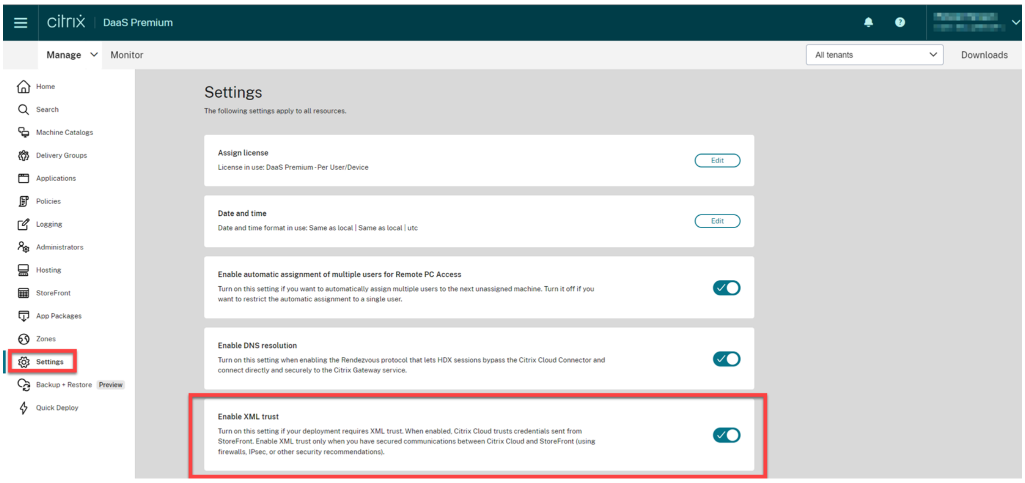
1. Check if you have the required license. If the required licenses aren't available, then you can't enable the App Protection.
2. If the necessary licenses aren't available, then fetch the required licenses and add the licenses.
3. After adding the licenses, restart the license server and try enabling App Protection again.
4. If valid licenses are available but still you aren't able to enable or disable the App Protection, then check if the `TrustRequestsSentToTheXmlServicePort` is enabled by running the following command:

   ```
   Get-BrokerSite | Select-Object TrustRequestsSentToTheXmlServicePort
   <!--NeedCopy-->
   ```

5. If the `TrustRequestsSentToTheXmlServicePort` isn't enabled, then enable the XML Trust using one of the following methods:

   - **Using Web Studio:**

a) Sign in to your Citrix DaaS account and go to **Manage** > **Settings** > **Enable XML trust**.



Settings

The following settings apply to all resources.

Assign license

License in use: DaaS Premium - Per User/Device

Date and time

Date and time format in use: Same as local | Same as local | utc

Enable automatic assignment of multiple users for Remote PC Access ✓

Turn on this setting if you want to automatically assign multiple users to the next unassigned machine. Turn it off if you want to restrict the automatic assignment to a single user.

Enable DNS resolution ✓

Turn on this setting when enabling the Rendezvous protocol that lets HDX sessions bypass the Citrix Cloud Connector and connect directly and securely to the Citrix Gateway service.

Enable XML trust ✓

Turn on this setting if your deployment requires XML trust. When enabled, Citrix Cloud trusts credentials sent from StoreFront. Enable XML trust only when you have secured communications between Citrix Cloud and StoreFront (using firewalls, IPsec, or other security recommendations).

b) Turn on the **Enable XML trust** toggle.

- **Using PowerShell:** Run the following command to enable XML trust:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
<!--NeedCopy-->
```

6. After enabling the `TrustRequestsSentToTheXmlServicePort`, enable App Protection again.
7. If the preceding conditions are met but you're still not able to enable or disable App Protection, then contact Citrix Technical Support.

App Protection policies are not applied properly

1. Make sure that the following conditions are met:

    - You're using a supported version of the Citrix Workspace app.
    - The Delivery Group has the proper features enabled.
    - The feature is installed on the endpoint.
    - The Citrix Workspace app was installed with the `/includeappprotection` switch enabled.

2. If the preceding conditions are met but still App Protection policies aren't applied properly, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Collect Logs for Citrix Workspace app

Screenshots not working on non-Citrix windows:

- Minimize or close the protected Citrix windows, including the Citrix Workspace app.

Troubleshoot Policy Tampering Detection

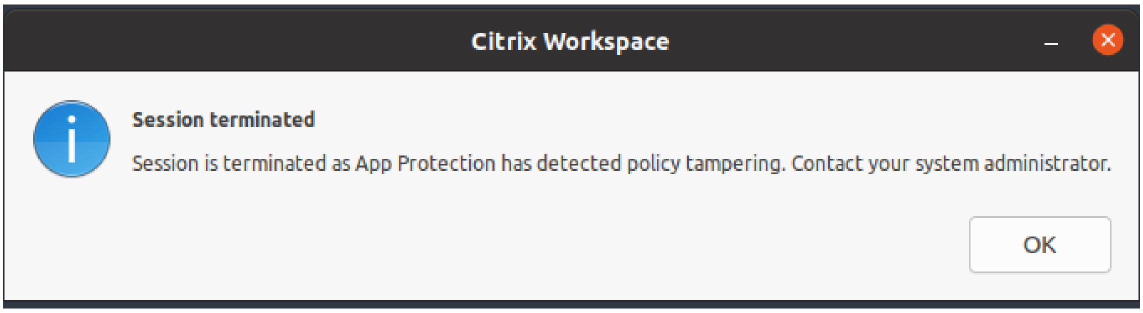
February 28, 2024

The following section describes some of the issues that you might face and how to troubleshoot them:

The ICA file is tampered and the session is still running

If the ICA file of a virtual app or desktop session that is enabled with the App Protection Policy Tampering Detection feature is tampered with, then the session must be terminated displaying one of the following error messages:

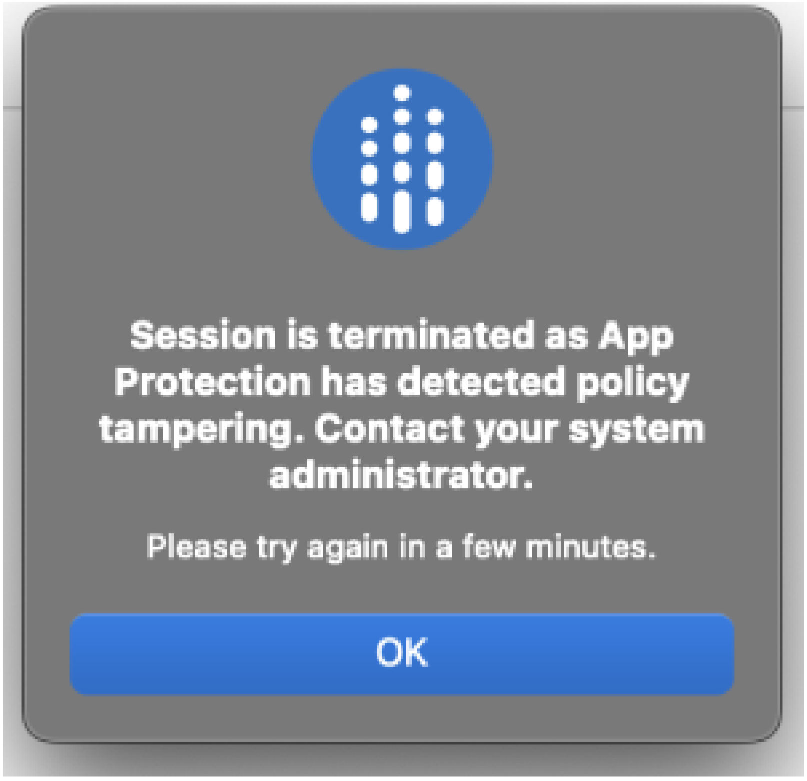
- Citrix Workspace app for Linux



Session terminated

Session is terminated as App Protection has detected policy tampering. Contact your system administrator.

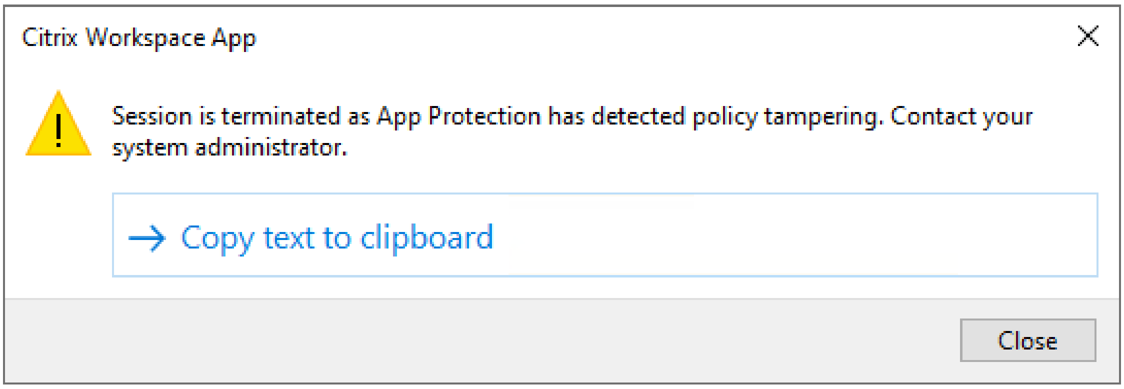
- Citrix Workspace app for Mac



Session is terminated as App Protection has detected policy tampering. Contact your system administrator.

Please try again in a few minutes.

- Citrix Workspace app for Windows



Citrix Workspace App

Session is terminated as App Protection has detected policy tampering. Contact your system administrator.

However, if the session is running even if the ICA file is tampered with and Policy Tampering Detection is enabled, then do the following steps:

1. In the Virtual Delivery Agent, do the following:

   a) Run the following command and check if the `ctxappprotectionsv` service is running:

   ```
   sc query ctxappprotectionsvc
   ```

   b) If the `ctxappprotectionsvc` service isn't running, then do the following steps to start the service:

i. Change the startup type of the `ctxappprotectionsvc` service to automatic by running the following command:

   ```
   sc config ctxappprotectionsvc start=auto
   ```

ii. Start the service by running the following command:

   ```
   sc start ctxappprotectionsvc
   ```

2. In the client, do the following:

   a) Check if the *vdappp.dll* file is in the installation location of the Citrix Workspace app. The default installation location of the Citrix Workspace app is as follows:

      - Windows - C:\Program Files (x86)\Citrix\ICA Client
      - Linux - /opt/Citrix/ICAClient
      - Mac - Not applicable

   b) For Citrix Workspace app for Windows, use *procexp.exe* and check if the *vdappp.dll* file is loaded in *wfica32.exe*.

   c) For Citrix Workspace app for Linux, check if the *vdappp.dll* file is loaded in *wfica.exe*.

3. If the session is still running, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Policy Tampering Detection stops working after rebooting Virtual Delivery Agent

If you reboot the Virtual Delivery Agent and the Policy Tampering Detection feature stops working, then it might be because the App Protection service isn't running after reboot. Do the following steps on the Virtual Delivery Agent:

1. Run the following command and check if the `ctxappprotectionsvc` service is running and set to **automatic**:

   ```
   sc query ctxappprotectionsvc
   ```

2. If the `ctxappprotectionsvc` service isn't running, then do the following steps to start the service:

   a) Change the startup type of the `ctxappprotectionsvc` service to **automatic** by running the following command:

      ```
      sc config ctxappprotectionsvc start=auto
      ```

   b) Start the service by running the following command:

      ```
      sc start ctxappprotectionsvc
      ```

3. If the Policy Tampering Detection feature is still not working, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Troubleshooting App Protection Posture Check

February 28, 2024

The following section describes some of the issues that you might face and how to troubleshoot them:

The session terminated without any error message

If your virtual app or desktop session terminates abruptly without displaying any error message, then do the following steps:

1. Check if your Citrix Workspace app version is earlier than one of the following versions:

    - Citrix Workspace app for Windows 2309
    - Citrix Workspace app for Mac 2308
    - Citrix Workspace app for Linux 2308

    > **Note:**
    >
    > If the Citrix Workspace app version is earlier than the versions listed in step 1 and the App Protection Posture Check feature is enabled, then the virtual app or desktop session terminates without displaying any error message. However, if the Citrix Workspace app version is greater than or equal to the versions listed in step 1 and the App Protection Posture Check feature is enabled, then the virtual apps or desktop session terminates displaying an error message.

2. Check whether the App Protection Posture Check feature is enabled.
3. If the Citrix Workspace app version is greater than or equal to the preceding versions and the Posture Check feature is also active, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

App Protection Posture Check is enabled but the session is not terminated for older versions

Generally, if the App Protection Posture Check feature is enabled and you are connecting through an older version of Citrix Workspace app, then the session must be terminated.

But if the session is not terminated, then do the following steps:

1. In the Virtual Delivery Agent, do the following:

   a) Run the following command and check if the `ctxappprotectionsvc` service is running:

   ```
   sc query ctxappprotectionsvc
   ```

   b) If the `ctxappprotectionsvc` service is not running, then do the following steps to start the service:

      i. Change the startup type of the `ctxappprotectionsvc service` to **automatic** by running the following command:

      ```
      sc config ctxappprotectionsvc start=auto
      ```

      ii. Start the service by running the following command:

      ```
      sc start ctxappprotectionsvc
      ```

2. Check if the Posture Check values that you have entered have one of the following prefixes:

   - For Citrix Workspace app for Windows, `windows-`
   - For Citrix Workspace app for Linux, `linux-`
   - For Citrix Workspace app for Mac, `mac-`

3. Check if the Posture Check values are correctly added as per the relevant platform as they are platform-specific.

4. Check the `reg` location (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) to verify if the Posture Check is synced with the Virtual Delivery Agent.

5. If all the preceding conditions are met and the session is still connected for the older versions of Citrix Workspace app, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

App Protection Posture Check is working on one platform but not working on another

Sometimes, the App Protection Posture Check feature might work on one platform and not on another. For example, the App Protection Posture Check feature is working on Citrix Workspace app for Windows but not on Citrix Workspace app for Linux.

In scenarios like these, do the following steps:

1. Check if the Posture Check values that you have entered have one of the following prefixes:

- For Citrix Workspace app for Windows, `windows-`
- For Citrix Workspace app for Linux, `linux-`
- For Citrix Workspace app for Mac, `mac-`

2. Check if the Posture Check values are correctly added as per the relevant platform as they are platform-specific.
3. Check the `reg` location (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) on the Virtual Delivery Agent to verify if the Posture Check is synced with the Virtual Delivery Agent. They must match with what was configured on Studio.
4. If all the preceding conditions are met and the session is still connected for the older versions of Citrix Workspace app, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

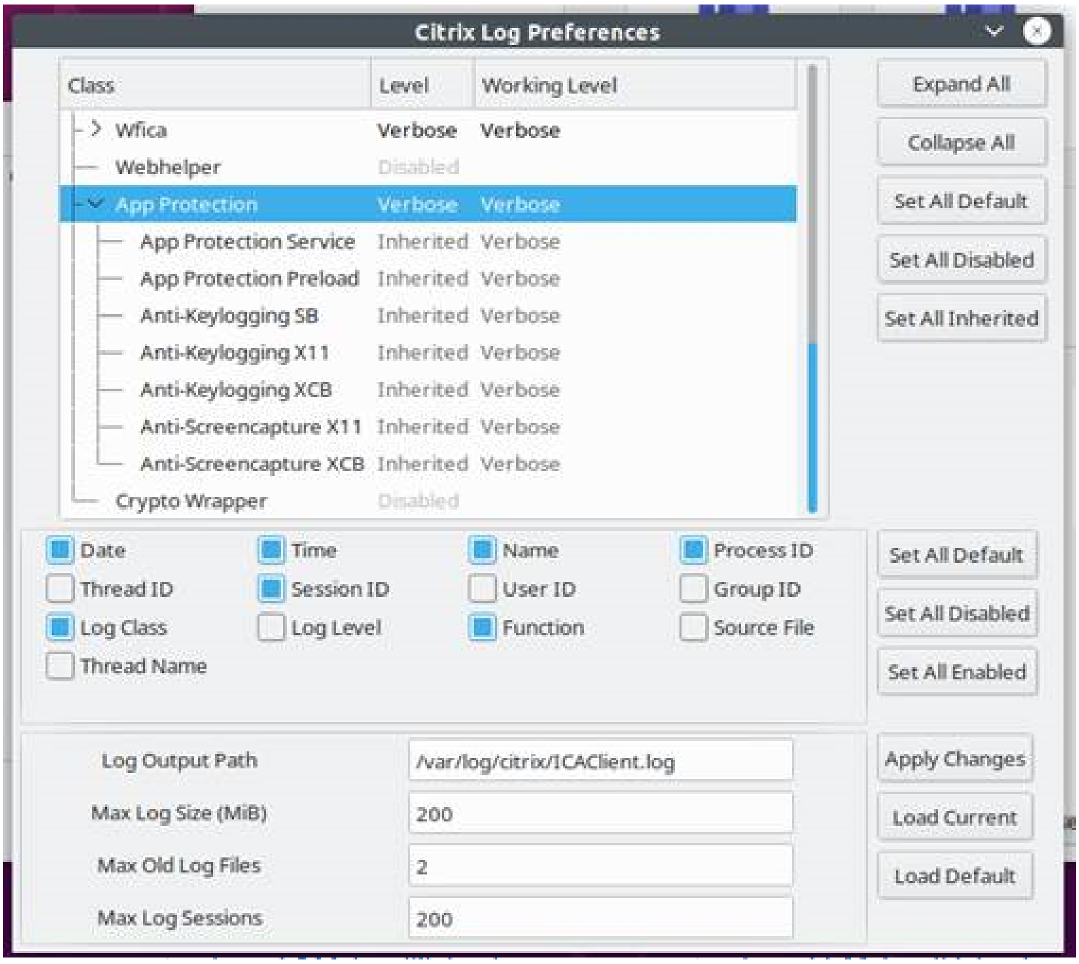
Log collection

February 28, 2024

- To collect logs for Citrix Workspace app for Windows, see Log collection for Windows.
- To collect logs for Citrix Workspace app for Mac, see Log collection for Mac.
- To collect logs for Citrix Workspace app for Linux, do the following steps:

  1. Run the set log executable found in the *util* directory of the installation. For example, */opt/Citrix/ICAClient/util/setlog*.
  2. (Optional) Click **Set All Disabled** and make sure that only the required logs are collected.
  3. Go to App Protection logging.
  4. Set the App Protection log level to Verbose by right-clicking and selecting **Verbose** (only warnings and errors are logged).
  5. Expand the App Protection class and right-click its child element. Select **Group** > **Inherited**.
  6. Use the linux logging utility (from *install dir*, launch *util/setlog*) and change the logging level for the virtual channel to Verbose.
  7. Enable logs for **wfica**. Right-click **wfica** and select **Verbose**. If App Protection isn't installed or not detectable by **wfica**, then you get the log as **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.

8. Click **wfica** and change the logging level for **winstation driver** to **Verbose**.
9. When you launch the session, the logs are recorded in the file that is mentioned in the log output Path of the set log.



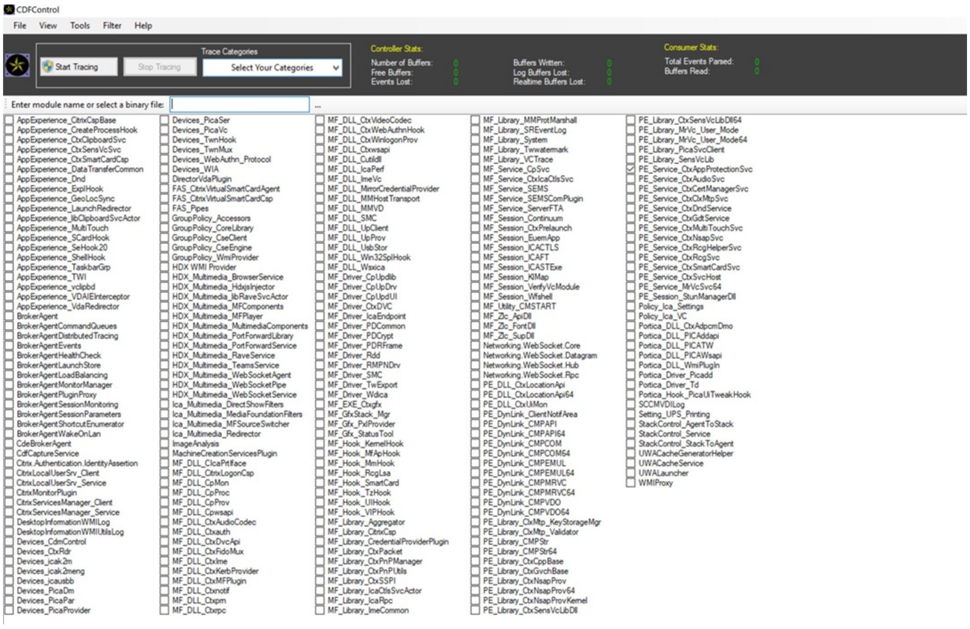
Citrix Log Preferences

Class	Level	Working Level
> Wfica	Verbose	Verbose
Webhelper	Disabled	
⌄ App Protection	Verbose	Verbose
App Protection Service	Inherited	Verbose
App Protection Preload	Inherited	Verbose
Anti-Keylogging SB	Inherited	Verbose
Anti-Keylogging X11	Inherited	Verbose
Anti-Keylogging XCB	Inherited	Verbose
Anti-Screencapture X11	Inherited	Verbose
Anti-Screencapture XCB	Inherited	Verbose
Crypto Wrapper	Disabled	

☑ Date	☑ Time	☑ Name	☑ Process ID
□ Thread ID	☑ Session ID	□ User ID	□ Group ID
☑ Log Class	□ Log Level	☑ Function	□ Source File
□ Thread Name			

Log Output Path	/var/log/citrix/ICAClient.log
Max Log Size (MiB)	200
Max Old Log Files	2
Max Log Sessions	200

- To collect logs for the Virtual Delivery Agent, do the following steps:
  1. To get traces from the App Protection service through CDF control, select all the modules.



Controller Stats:
Number of Buffers: 0
Free Buffers: 0
Events Lost: 0
Buffers Written: 0
Log Buffers Lost: 0
Realtime Buffers Lost: 0

Consumer Stats:
Total Events Parsed: 0
Buffers Read: 0

Enter module name or select a binary file:

□ AppExperience_CitrixCspBase
□ AppExperience_CreateProcessHook
□ AppExperience_CtxClipboardSvc
□ AppExperience_CtxSensVcSvc
□ AppExperience_CtxSmartCardCsp
□ AppExperience_DataTransferCommon
□ AppExperience_Dnd
□ AppExperience_ExplHook
□ AppExperience_GeoLocSync
□ AppExperience_LaunchRedirector
□ AppExperience_libClipboardSvcActor
□ AppExperience_MultiTouch
□ AppExperience_SCardHook
□ AppExperience_SeHook20
□ AppExperience_ShellHook
□ AppExperience_TaskbarGrp
□ AppExperience_TWI
□ AppExperience_vclipbd
□ AppExperience_VDAIEInterceptor
□ AppExperience_VdaRedirector
□ BrokerAgent
□ BrokerAgentCommandQueues
□ BrokerAgentDistributedTracing
□ BrokerAgentEvents
□ BrokerAgentHealthCheck
□ BrokerAgentLaunchStore
□ BrokerAgentLoadBalancing
□ BrokerAgentMonitorManager
□ BrokerAgentPluginProxy
□ BrokerAgentSessionMonitoring
□ BrokerAgentSessionParameters
□ BrokerAgentShortcutEnumerator
□ BrokerAgentWakeOnLan
□ CdeBrokerAgent
□ CdfCaptureService
□ Citrix.Authentication.IdentityAssertion
□ CitrixLocalUserSrv_Client
□ CitrixLocalUserSrv_Service
□ CitrixMonitorPlugin
□ CitrixServicesManager_Client
□ CitrixServicesManager_Service
□ DesktopInformationWMILog
□ DesktopInformationWMIUtilsLog
□ Devices_CdmControl
□ Devices_CtxRdr
□ Devices_icak2m
□ Devices_icak2meng
□ Devices_icausbb
□ Devices_PicaDm
□ Devices_PicaPar
□ Devices_PicaProvider
□ Devices_PicaSer
□ Devices_PicaVc
□ Devices_TwnHook
□ Devices_TwnMux
□ Devices_WebAuthn_Protocol
□ Devices_WIA
□ DirectorVdaPlugin
□ FAS_CitrixVirtualSmartCardAgent
□ FAS_CitrixVirtualSmartCardCsp
□ FAS_Pipes
□ GroupPolicy_Accessors
□ GroupPolicy_CoreLibrary
□ GroupPolicy_CseClient
□ GroupPolicy_CseEngine
□ GroupPolicy_WmiProvider
□ HDX WMI Provider
□ HDX_Multimedia_BrowserService
□ HDX_Multimedia_HdxjsInjector
□ HDX_Multimedia_libRaveSvcActor
□ HDX_Multimedia_MFComponents
□ HDX_Multimedia_MFPlayer
□ HDX_Multimedia_MultimediaComponents
□ HDX_Multimedia_PortForwardLibrary
□ HDX_Multimedia_PortForwardService
□ HDX_Multimedia_RaveService
□ HDX_Multimedia_TeamsService
□ HDX_Multimedia_WebSocketAgent
□ HDX_Multimedia_WebSocketPipe
□ HDX_Multimedia_WebSocketService
□ Ica_Multimedia_DirectShowFilters
□ Ica_Multimedia_MediaFoundationFilters
□ Ica_Multimedia_MFSourceSwitcher
□ Ica_Multimedia_Redirector
□ ImageAnalysis
□ MachineCreationServicesPlugin
□ MF_DLL_CIcaPrtIface
□ MF_DLL_CitrixLogonCsp
□ MF_DLL_CpMon
□ MF_DLL_CpProc
□ MF_DLL_CpProv
□ MF_DLL_Cpwsapi
□ MF_DLL_CtxAudioCodec
□ MF_DLL_Ctxauth
□ MF_DLL_CtxDvcApi
□ MF_DLL_CtxFidoMux
□ MF_DLL_CtxIme
□ MF_DLL_CtxKerbProvider
□ MF_DLL_CtxMFPlugin
□ MF_DLL_Ctxnotif
□ MF_DLL_Ctxpm
□ MF_DLL_Ctxrpc
□ MF_DLL_CtxVideoCodec
□ MF_DLL_CtxWebAuthnHook
□ MF_DLL_CtxWinlogonProv
□ MF_DLL_Ctxwsapi
□ MF_DLL_Cutildll
□ MF_DLL_IcaPerf
□ MF_DLL_ImeVc
□ MF_DLL_MirrorCredentialProvider
□ MF_DLL_MMHostTransport
□ MF_DLL_MMVD
□ MF_DLL_SMC
□ MF_DLL_UpClient
□ MF_DLL_UpProv
□ MF_DLL_UsbStor
□ MF_DLL_Win32SplHook
□ MF_DLL_Wsxica
□ MF_Driver_CpUpdlib
□ MF_Driver_CpUpDrv
□ MF_Driver_CpUpdUI
□ MF_Driver_CtxDVC
□ MF_Driver_IcaEndpoint
□ MF_Driver_PDCommon
□ MF_Driver_PDCrypt
□ MF_Driver_PDRFrame
□ MF_Driver_Rdd
□ MF_Driver_RMPNDrv
□ MF_Driver_SMC
□ MF_Driver_TwExport
□ MF_Driver_Wdica
□ MF_EXE_Ctxgfx
□ MF_GfxStack_Mgr
□ MF_Gfx_PxlProvider
□ MF_Gfx_StatusTool
□ MF_Hook_KernelHook
□ MF_Hook_MfApHook
□ MF_Hook_MmHook
□ MF_Hook_RcgLsa
□ MF_Hook_SmartCard
□ MF_Hook_TzHook
□ MF_Hook_UIHook
□ MF_Hook_VIPHook
□ MF_Library_Aggregator
□ MF_Library_CitrixCsp
□ MF_Library_CredentialProviderPlugin
□ MF_Library_CtxPacket
□ MF_Library_CtxPnPManager
□ MF_Library_CtxPnPUtils
□ MF_Library_CtxSSPI
□ MF_Library_IcaCtlsSvcActor
□ MF_Library_IcaRpc
□ MF_Library_ImeCommon
□ MF_Library_MMProtMarshall
□ MF_Library_SREventLog
□ MF_Library_System
□ MF_Library_Twwatermark
□ MF_Library_VCTrace
□ MF_Service_CpSvc
□ MF_Service_CtxIcaCtlsSvc
□ MF_Service_SEMS
□ MF_Service_SEMSComPlugin
□ MF_Service_ServerFTA
□ MF_Session_Continuum
□ MF_Session_CtxPrelaunch
□ MF_Session_EuemApp
□ MF_Session_ICACTLS
□ MF_Session_ICAFT
□ MF_Session_ICASTExe
□ MF_Session_KlMap
□ MF_Session_VerifyVcModule
□ MF_Session_Wfshell
□ MF_Utility_CMSTART
□ MF_Zlc_ApiDll
□ MF_Zlc_FontDll
□ MF_Zlc_SupDll
□ Networking.WebSocket.Core
□ Networking.WebSocket.Datagram
□ Networking.WebSocket.Hub
□ Networking.WebSocket.Rpc
□ PE_DLL_CtxLocationApi
□ PE_DLL_CtxLocationApi64
□ PE_DLL_CtxUiMon
□ PE_DynLink_ClientNotifArea
□ PE_DynLink_CMPAPI
□ PE_DynLink_CMPAPI64
□ PE_DynLink_CMPCOM
□ PE_DynLink_CMPCOM64
□ PE_DynLink_CMPEMUL
□ PE_DynLink_CMPEMUL64
□ PE_DynLink_CMPMRVC
□ PE_DynLink_CMPMRVC64
□ PE_DynLink_CMPVDO
□ PE_DynLink_CMPVDO64
□ PE_Library_ClxMtp_KeyStorageMgr
□ PE_Library_ClxMtp_Validator
□ PE_Library_CMPStr
□ PE_Library_CMPStr64
□ PE_Library_CtxCppBase
□ PE_Library_CtxGvchBase
□ PE_Library_CtxNsapProv
□ PE_Library_CtxNsapProv64
□ PE_Library_CtxNsapProvKernel
□ PE_Library_CtxSensVcLibDll
□ PE_Library_CtxSensVcLibDll64
□ PE_Library_MrVc_User_Mode
□ PE_Library_MrVc_User_Mode64
□ PE_Library_PicaSvcClient
□ PE_Library_SensVcLib
☑ PE_Service_CtxAppProtectionSvc
□ PE_Service_CtxAudioSvc
□ PE_Service_CtxCertManagerSvc
□ PE_Service_CtxClxMtpSvc
□ PE_Service_CtxDndService
□ PE_Service_CtxGdtService
□ PE_Service_CtxMultiTouchSvc
□ PE_Service_CtxNsapSvc
□ PE_Service_CtxRcgHelperSvc
□ PE_Service_CtxRcgSvc
□ PE_Service_CtxSmartCardSvc
□ PE_Service_CtxSvcHost
□ PE_Service_MrVcSvc64
□ PE_Session_StunManagerDll
□ Policy_Ica_Settings
□ Policy_Ica_VC
□ Portica_DLL_CtxAdpcmDmo
□ Portica_DLL_PICAddapi
□ Portica_DLL_PICATW
□ Portica_DLL_PICAWsapi
□ Portica_DLL_WmiPlugIn
□ Portica_Driver_Picadd
□ Portica_Driver_Td
□ Portica_Hook_PicaUiTweakHook
□ SCCMVDILog
□ Setting_UPS_Printing
□ StackControl_AgentToStack
□ StackControl_Service
□ StackControl_StackToAgent
□ UWACacheGeneratorHelper
□ UWACacheService
□ UWALauncher
□ WMIProxy

2. In certain cases, we might have to capture cdf traces from a different machine. To collect cdf traces, see CTX237216.

Contextual App Protection for Workspace

February 28, 2024

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture.

Implementing contextual App Protection

You can implement contextual App Protection using the connection filters defined in the Broker Access policy rule. The Broker Access policies define the rules controlling a user's access to delivery groups. The policy comprises a set of rules. Each rule relates to a single delivery group, and has a set of connection filters and access right controls.

Users gain access to a delivery group when their connection's details match the connection filters of one or more rules in the Broker Access policy. Users don't have access to any delivery group within a site by default. You can create more Broker Access policies based on requirements. Multiple rules can apply to the same delivery group. For more information, see New-BrokerAccessPolicyRule.

The following parameters in the Broker Access policy rule provide the flexibility to enable App Protection contextually if the user's connection matches the connection filters defined in the access policy rule:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Use the Smart Access policies referenced in the Broker Access policy rules to further refine the connection filters. Refer to the scenarios explained in this article to understand how to use the Smart Access policies to set up contextual App Protection.

Contextual App Protection scenarios

Following are some of the scenarios about how you can enable Contextual App Protection:

- Enable App Protection for External users coming through the Access gateway
- Enable App Protection for Untrusted Devices
- Enable App Protection based on Device Posture results
- Enable App Protection for specific user groups

Prerequisites

February 28, 2024

Make sure that you have the following:

- Network location service (NLS) for scenarios based on the user's network location
- Licensing requirements -
  - App Protection for DaaS
  - Adaptive Authentication entitlement for scenarios with Smart Access policies.

Scenario 1

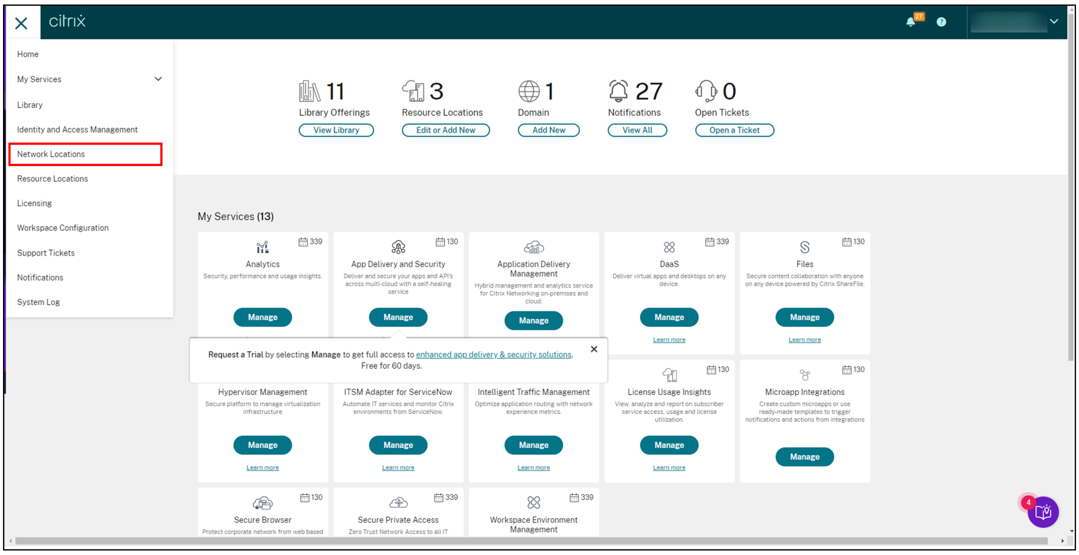
February 28, 2024

This scenario covers how to enable App Protection for external users coming through the Access Gateway.

1. Configure Adaptive Authentication.

2. Configure adaptive access based on your network location,

a) Sign in to Citrix Cloud and navigate to **Network Locations**.



Analytics — Security, performance and usage insights.

App Delivery and Security — Deliver and secure your apps and API's across multi-cloud with a self-healing service

Application Delivery Management — Hybrid management and analytics service for Citrix Networking on-premises and cloud.

DaaS — Deliver virtual apps and desktops on any device.

Files — Secure content collaboration with anyone on any device powered by Citrix ShareFile.

Request a Trial by selecting **Manage** to get full access to enhanced app delivery & security solutions. Free for 60 days.

Hypervisor Management — Secure platform to manage virtualization infrastructure

ITSM Adapter for ServiceNow — Automate IT services and monitor Citrix environments from ServiceNow.

Intelligent Traffic Management — Optimize application routing with network experience metrics.

License Usage Insights — View, analyze and report on subscriber service access, usage and license utilization.

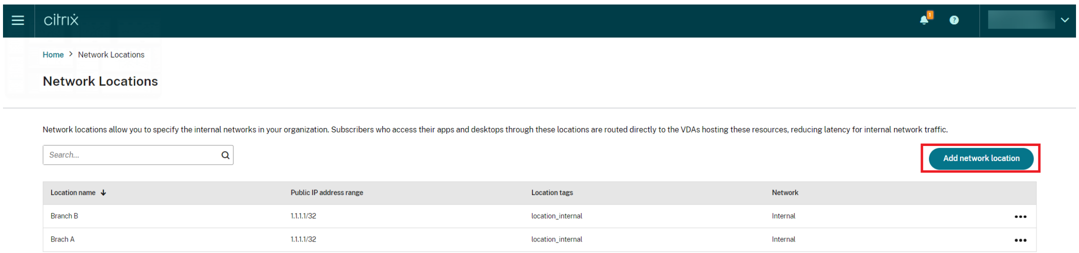
Microapp Integrations — Create custom microapps or use ready-made templates to trigger notifications and actions from integrations

Secure Browser — Protect corporate network from web based

Secure Private Access — Zero Trust Network Access to all IT

Workspace Environment Management

b) Click **Add Network location**.



Network locations allow you to specify the internal networks in your organization. Subscribers who access their apps and desktops through these locations are routed directly to the VDAs hosting these resources, reducing latency for internal network traffic.

Location name ↓	Public IP address range	Location tags	Network	
Branch B	1.1.1.1/32	location_internal	Internal	•••
Brach A	1.1.1.1/32	location_internal	Internal	•••

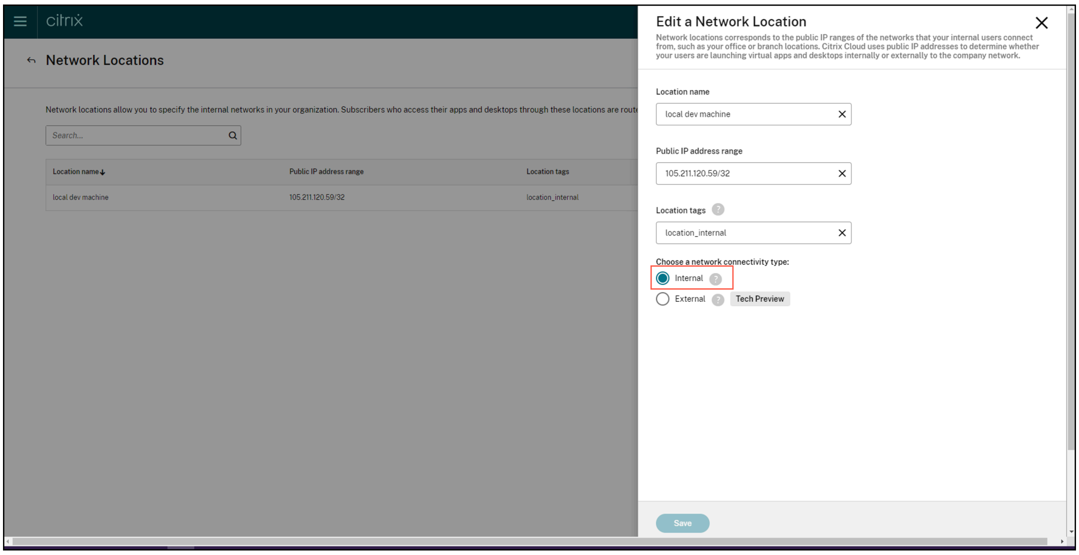
Add a Network Location screen appears.

c) In the **Location name** field, enter the relevant location name.

d) In the **Public IP address range** field, enter the network IP address or subnet that you want to consider as an internal network.

e) In the **Location tags** field, enter **location_internal**. For more information about the location tag, see Location tags.

f) Under **Choose a network connectivity type**, select *Internal*.



Network Locations

Network locations allow you to specify the internal networks in your organization. Subscribers who access their apps and desktops through these locations are route

Search...

Location name ↓	Public IP address range	Location tags
local dev machine	105.211.120.59/32	location_internal

Edit a Network Location

Network locations corresponds to the public IP ranges of the networks that your internal users connect from, such as your office or branch locations. Citrix Cloud uses public IP addresses to determine whether your users are launching virtual apps and desktops internally or externally to the company network.

Location name: local dev machine

Public IP address range: 105.211.120.59/32

Location tags: location_internal

Choose a network connectivity type:

● Internal

○ External Tech Preview

If you sign in to the Cloud store from a device whose IP address is configured as *Internal* under **Choose a network connectivity type** setting, then the connection is considered as an internal connection.

3. Configure Broker Access policy rules

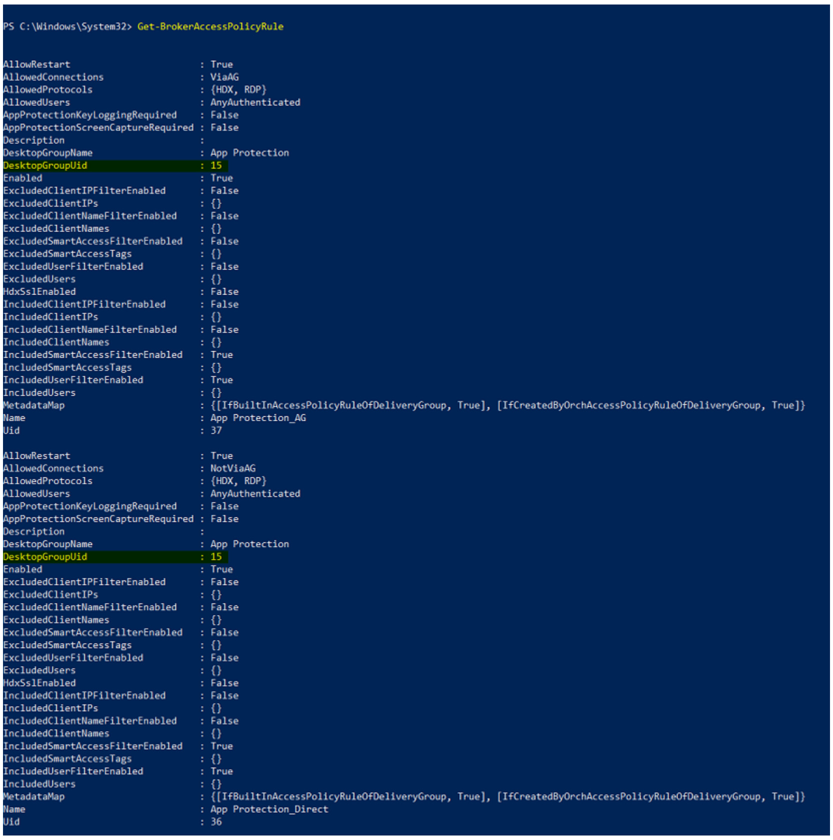
   For every delivery group, two broker access policies are created by default. One policy is for connections coming through the Access gateway, and the other policy is for direct connections. You can enable App Protection only for the connections coming through the Access gateway, which is the external connections. Use the following steps to configure the Broker Access policy rules:

   a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

   b) Run the command `Get-BrokerAccessPolicyRule`.

      A list of all the broker access policies for all the delivery groups that are present is displayed.

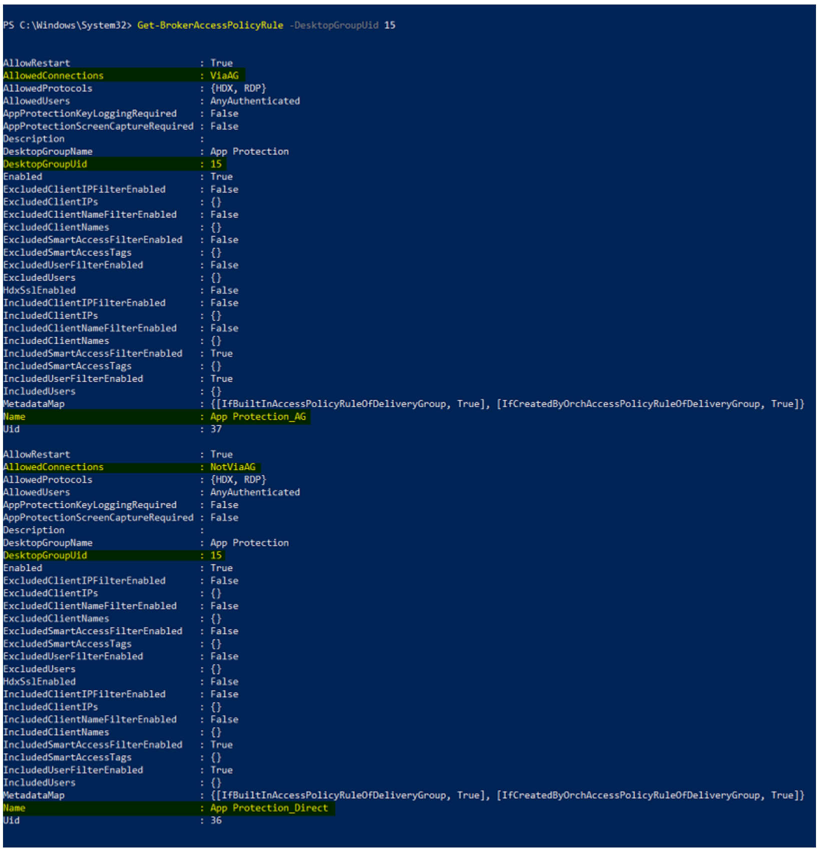
   c) Find the **DesktopGroupUid** for the delivery group that you want to change.



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                       : True
AllowedConnections                 : ViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_AG
Uid                                : 37

AllowRestart                       : True
AllowedConnections                 : NotViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_Direct
Uid                                : 36
```

d) Run the following command using the **DesktopGroupUid** to fetch policies applicable to the delivery group. There are at least two policies, one where *AllowedConnections* has *ViaAG* and another which has *NotViaAG*.

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule -DesktopGroupUid 15


AllowRestart                        : True
AllowedConnections                  : ViaAG
AllowedProtocols                    : {HDX, RDP}
AllowedUsers                        : AnyAuthenticated
AppProtectionKeyLoggingRequired     : False
AppProtectionScreenCaptureRequired  : False
Description                         :
DesktopGroupName                    : App Protection
DesktopGroupUid                     : 15
Enabled                             : True
ExcludedClientIPFilterEnabled       : False
ExcludedClientIPs                   : {}
ExcludedClientNameFilterEnabled     : False
ExcludedClientNames                 : {}
ExcludedSmartAccessFilterEnabled    : False
ExcludedSmartAccessTags             : {}
ExcludedUserFilterEnabled           : False
ExcludedUsers                       : {}
HdxSslEnabled                       : False
IncludedClientIPFilterEnabled       : False
IncludedClientIPs                   : {}
IncludedClientNameFilterEnabled     : False
IncludedClientNames                 : {}
IncludedSmartAccessFilterEnabled    : True
IncludedSmartAccessTags             : {}
IncludedUserFilterEnabled           : True
IncludedUsers                       : {}
MetadataMap                         : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                                : App Protection_AG
Uid                                 : 37

AllowRestart                        : True
AllowedConnections                  : NotViaAG
AllowedProtocols                    : {HDX, RDP}
AllowedUsers                        : AnyAuthenticated
AppProtectionKeyLoggingRequired     : False
AppProtectionScreenCaptureRequired  : False
Description                         :
DesktopGroupName                    : App Protection
DesktopGroupUid                     : 15
Enabled                             : True
ExcludedClientIPFilterEnabled       : False
ExcludedClientIPs                   : {}
ExcludedClientNameFilterEnabled     : False
ExcludedClientNames                 : {}
ExcludedSmartAccessFilterEnabled    : False
ExcludedSmartAccessTags             : {}
ExcludedUserFilterEnabled           : False
ExcludedUsers                       : {}
HdxSslEnabled                       : False
IncludedClientIPFilterEnabled       : False
IncludedClientIPs                   : {}
IncludedClientNameFilterEnabled     : False
IncludedClientNames                 : {}
IncludedSmartAccessFilterEnabled    : True
IncludedSmartAccessTags             : {}
IncludedUserFilterEnabled           : True
IncludedUsers                       : {}
MetadataMap                         : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                                : App Protection_Direct
Uid                                 : 36
```

In the screenshot, you see two policies:

- App Protection_AG - *AllowedConnections* with *ViaAG*, which is the policy for connections via the access gateway
- App Protection_Direct –*AllowedConnections* with *NotViaAG*, which is the policy for connections not via the access gateway

4. Enable App Protection policies only for external connections and disable for internal connections using the following commands:

   -
     ```
     Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt
      $true -IncludedSmartAccessTags Workspace:LOCATION_internal -
     AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ
      $false
     ```

   -
     ```
     New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc
      $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -
     AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi
      $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols
      HDX, RDP
     ```

   -
     ```
     Remove-BrokerAccessPolicyRule "App Protection_Direct”
     ```

5. Verification:

   Sign out of Citrix Workspace app and sign in again. Launch the protected resource from an external connection. You see that the App Protection policies are applied. Launch the same resource from an internal connection, a device from within the IP Address range configured in the first step. You see that the App Protection policies are disabled.

Scenario 2

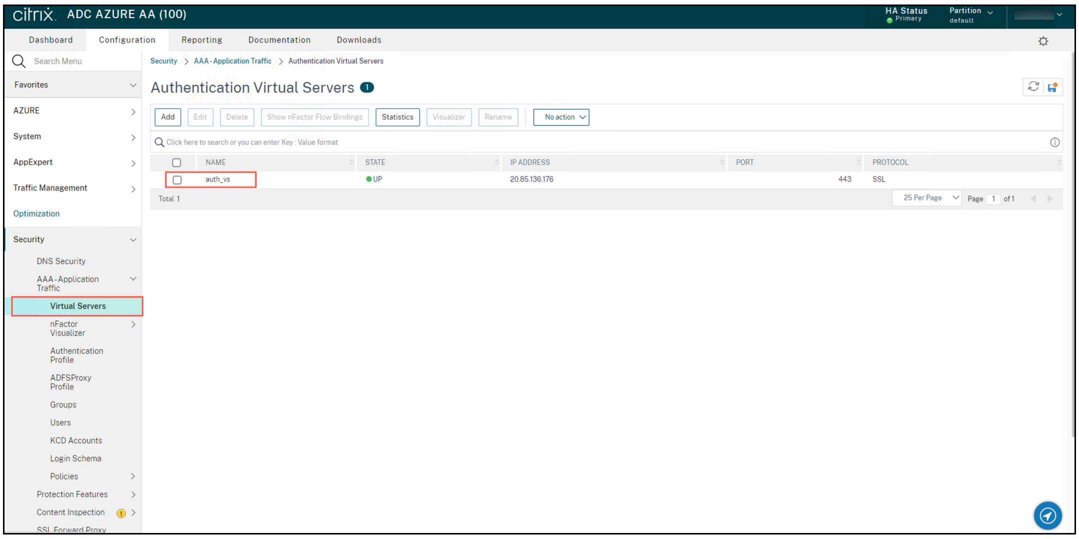
February 28, 2024

This scenario covers how to enable App Protection for untrusted devices.

There are many definitions for trusted and untrusted devices. For this scenario, let's consider a device trusted if the Endpoint analysis (EPA) scan is successful. All other devices are considered untrusted devices.

1. Configure Adaptive Authentication.
2. Create an Authentication policy with the EPA scan using the following steps:

   a) Sign in to Citrix ADC Administration UI. In the **Configuration** tab, navigate to **Security > AAA-Application Traffic > Virtual Servers**. Click the virtual server that you want to use, *auth_vs* in this case.

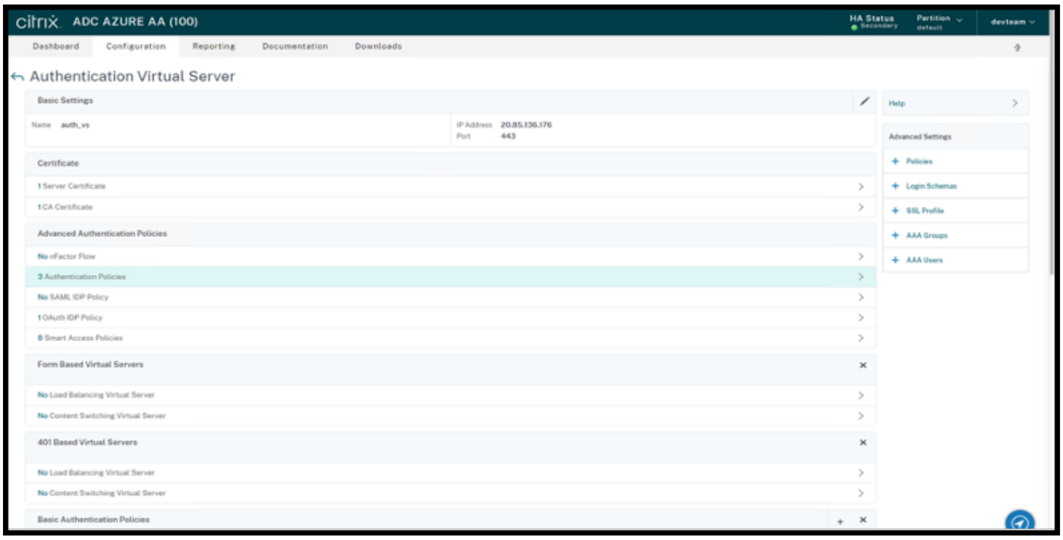


Authentication Virtual Servers 1

NAME	STATE	IP ADDRESS	PORT	PROTOCOL
auth_vs	● UP	20.85.136.176	443	SSL

Total 1

   b) Navigate to **Authentication Policies > Add Binding**.



Authentication Virtual Server

Basic Settings

Name auth_vs

IP Address 20.85.136.176

Port 443

Certificate

1 Server Certificate

1 CA Certificate

Advanced Authentication Policies

No nFactor Flow

3 Authentication Policies

No SAML IDP Policy

1 OAuth IDP Policy

8 Smart Access Policies

Form Based Virtual Servers

No Load Balancing Virtual Server

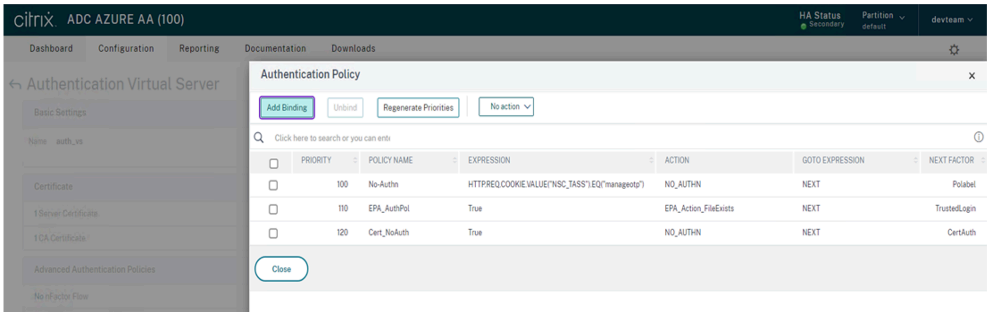
No Content Switching Virtual Server

401 Based Virtual Servers

No Load Balancing Virtual Server

No Content Switching Virtual Server

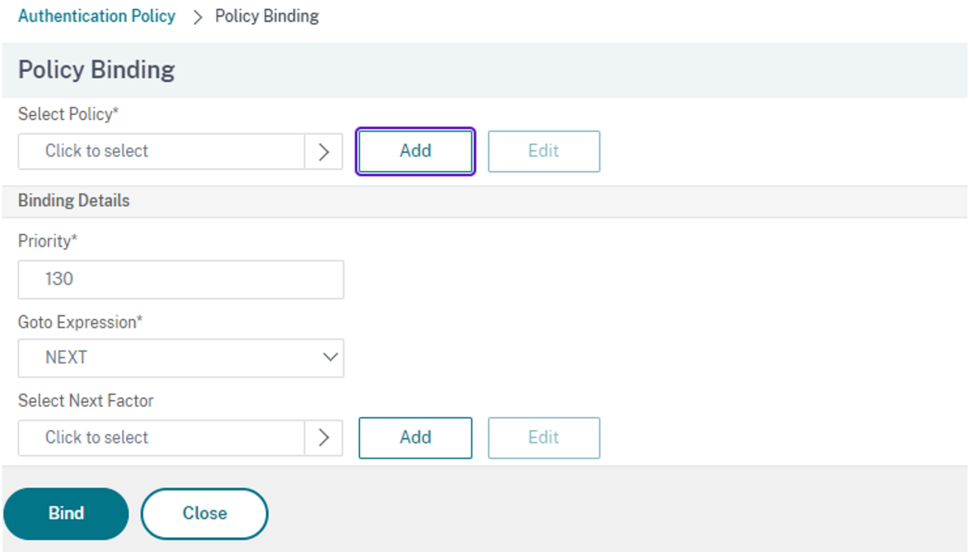
Basic Authentication Policies



Authentication Policy

	PRIORITY	POLICY NAME	EXPRESSION	ACTION	GOTO EXPRESSION	NEXT FACTOR
□	100	No-Authn	HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("manageotp")	NO_AUTHN	NEXT	Polabel
□	110	EPA_AuthPol	True	EPA_Action_FileExists	NEXT	TrustedLogin
□	120	Cert_NoAuth	True	NO_AUTHN	NEXT	CertAuth

c) Click **Add** to create a policy.



Policy Binding

Select Policy*

Click to select

Binding Details

Priority*

130

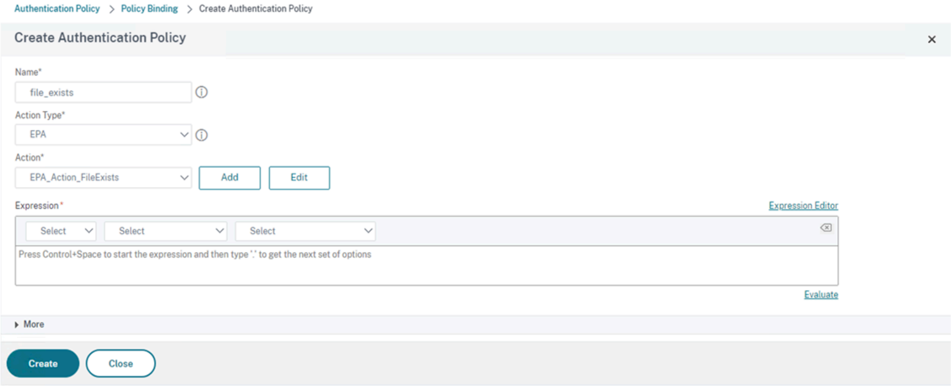
Goto Expression*

NEXT

Select Next Factor

Click to select

d) Create an authentication policy based on the EPA scan. Enter the name of the policy. Select **Action Type** as *EPA*. Click **Add** to create action.



Authentication Policy > Policy Binding > Create Authentication Policy

Create Authentication Policy

Name*: file_exists

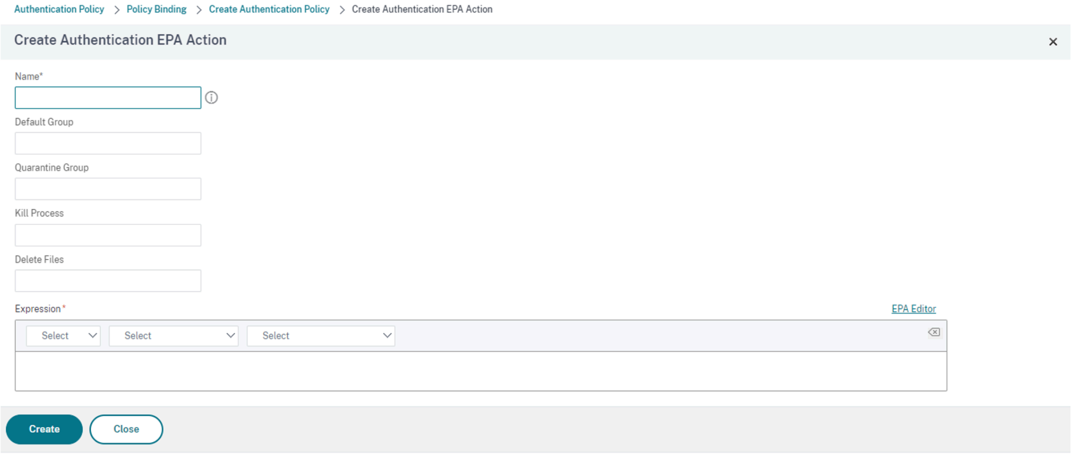
Action Type*: EPA

Action*: EPA_Action_FileExists

Expression*

Press Control+Space to start the expression and then type '.' to get the next set of options

Create Authentication EPA Action screen appears.



Authentication Policy > Policy Binding > Create Authentication Policy > Create Authentication EPA Action

Create Authentication EPA Action

Name*

Default Group

Quarantine Group

Kill Process

Delete Files

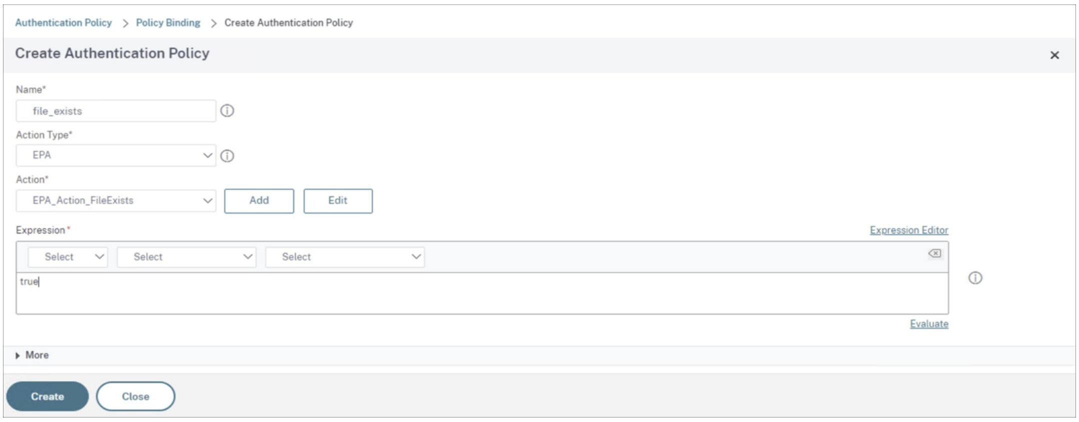
Expression*

e) On the **Create Authentication EPA Action** screen, enter the following details and click **Create** to create an action:

- **Name**: Name of the EPA action. In this case *EPA_Action_FileExists*.
- **Default Group**: Enter the default group name. If the EPA expression is *True*, users are added to the default group. The **Default Group** in this case is *FileExists*.
- **Quarantine Group**: Enter the quarantine group name. If the EPA expression is *False*, users are added to the quarantine group.
- **Expression**: Add the EPA expression that you want to scan. In this example, we consider the EPA scan to be successful if a particular file is present: `sys.client_expr("file_0_C:\\\\epa\\\\avinstalled.txt")`

You return to the **Create Authentication Policy** screen.

f) Enter **true** in the Expression editor, and click **Create**.



Authentication Policy > Policy Binding > Create Authentication Policy

Create Authentication Policy

Name*: file_exists

Action Type*: EPA

Action*: EPA_Action_FileExists

Expression*: true

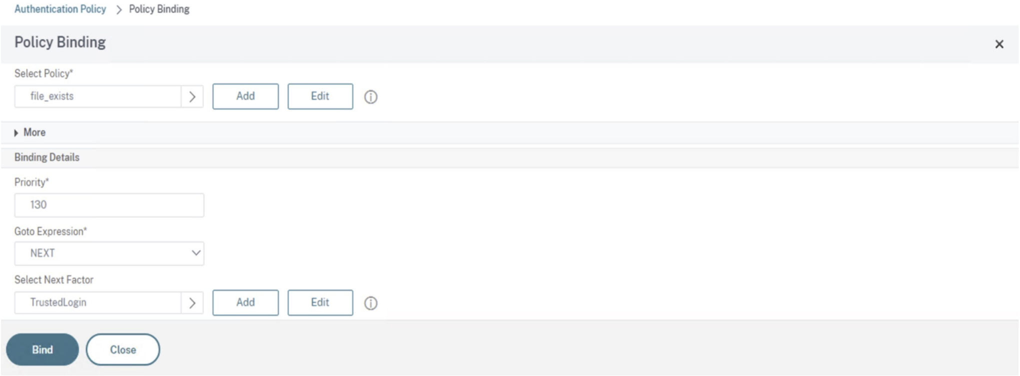
You return to the **Policy Binding** screen.

g) On the **Policy Binding** screen, do the following:

   i. Select the **Goto Expression** as **NEXT**.

   ii. In the **Select Next Factor** section, select the LDAP policy that you've configured for the authentication in the Application Delivery Controller (ADC).

   iii. Click **Bind**.



Authentication Policy > Policy Binding

Policy Binding

Select Policy*: file_exists

Binding Details

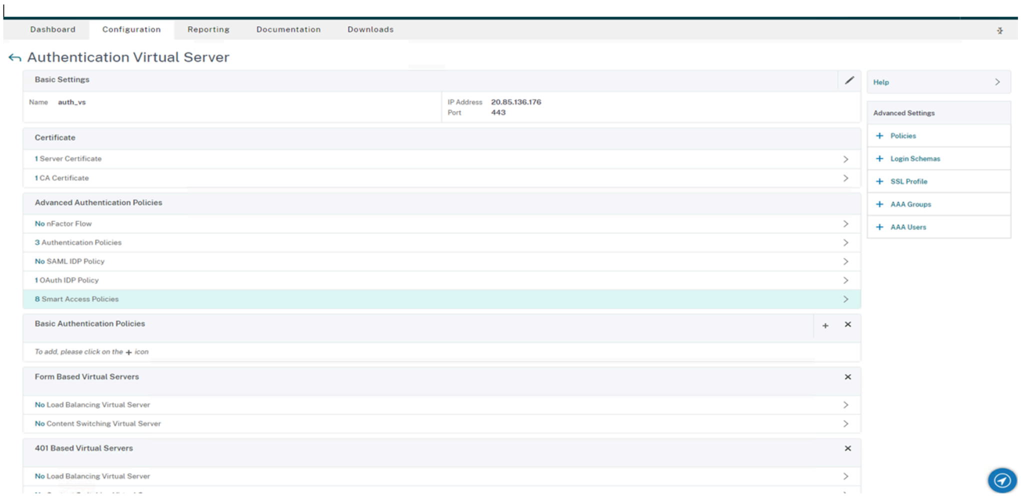
Priority*: 130

Goto Expression*: NEXT

Select Next Factor: TrustedLogin

3. Create a Smart Access Policy for trusted devices:

   a) Select **Smart Access Policies** on the **Authentication Virtual Server** page of the *auth_vs* server.



Authentication Virtual Server

Basic Settings

Name auth_vs

IP Address 20.85.136.176
Port 443

Certificate

1 Server Certificate

1 CA Certificate

Advanced Authentication Policies

No nFactor Flow

3 Authentication Policies

No SAML IDP Policy

1 OAuth IDP Policy

8 Smart Access Policies

Basic Authentication Policies

To add, please click on the + icon

Form Based Virtual Servers

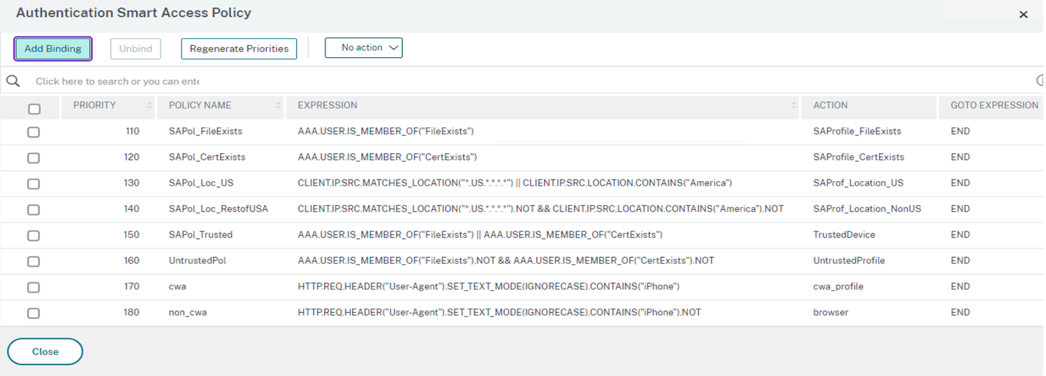
No Load Balancing Virtual Server

No Content Switching Virtual Server

401 Based Virtual Servers

No Load Balancing Virtual Server

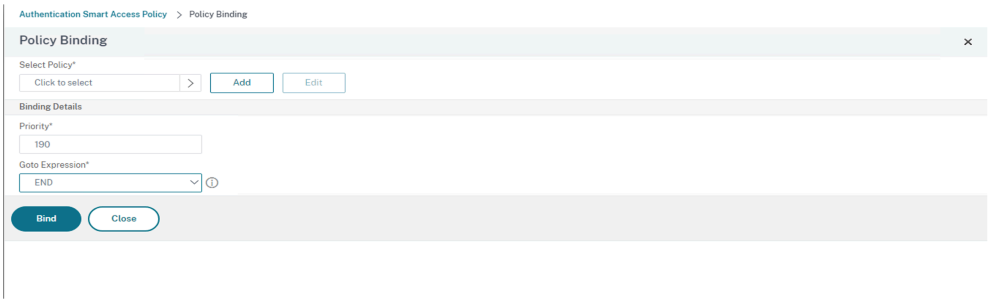
b) Click **Add Binding**.



Authentication Smart Access Policy

□	PRIORITY	POLICY NAME	EXPRESSION	ACTION	GOTO EXPRESSION
□	110	SAPol_FileExists	AAA.USER.IS_MEMBER_OF("FileExists")	SAProfile_FileExists	END
□	120	SAPol_CertExists	AAA.USER.IS_MEMBER_OF("CertExists")	SAProfile_CertExists	END
□	130	SAPol_Loc_US	CLIENT.IP.SRC.MATCHES_LOCATION("*.US.*.*.*.*") || CLIENT.IP.SRC.LOCATION.CONTAINS("America")	SAProf_Location_US	END
□	140	SAPol_Loc_RestofUSA	CLIENT.IP.SRC.MATCHES_LOCATION("*.US.*.*.*.*").NOT && CLIENT.IP.SRC.LOCATION.CONTAINS("America").NOT	SAProf_Location_NonUS	END
□	150	SAPol_Trusted	AAA.USER.IS_MEMBER_OF("FileExists") || AAA.USER.IS_MEMBER_OF("CertExists")	TrustedDevice	END
□	160	UntrustedPol	AAA.USER.IS_MEMBER_OF("FileExists").NOT && AAA.USER.IS_MEMBER_OF("CertExists").NOT	UntrustedProfile	END
□	170	cwa	HTTP.REQ.HEADER("User-Agent").SET_TEXT_MODE(IGNORECASE).CONTAINS("iPhone")	cwa_profile	END
□	180	non_cwa	HTTP.REQ.HEADER("User-Agent").SET_TEXT_MODE(IGNORECASE).CONTAINS("iPhone").NOT	browser	END

c) On the **Policy Binding** screen, click **Add** in the **Select Policy** section.



Policy Binding

Select Policy*

Binding Details

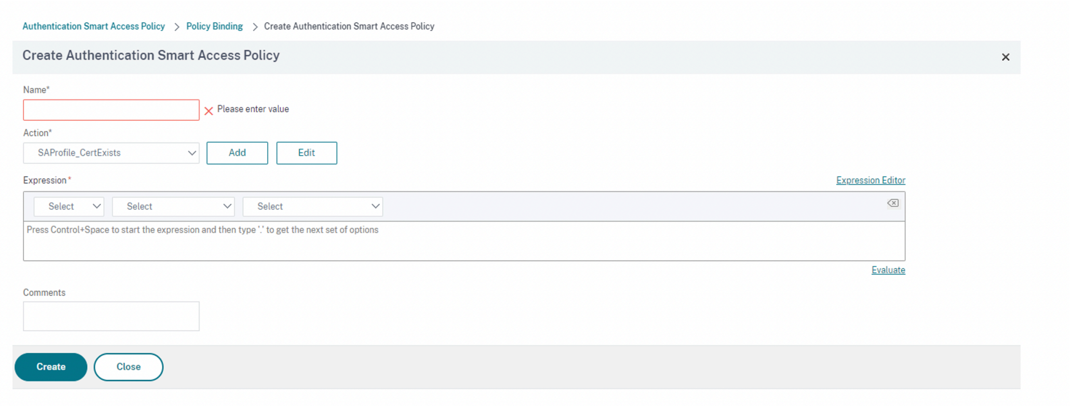
Priority*

190

Goto Expression*

END

The **Create Authentication Smart Access Policy** screen appears.


Authentication Smart Access Policy > Policy Binding > Create Authentication Smart Access Policy
Create Authentication Smart Access Policy
×
Name*
Action*
Add
Edit
Expression*
Expression Editor
Select
Select
Select
Evaluate
Comments
Create
Close

Please enter value

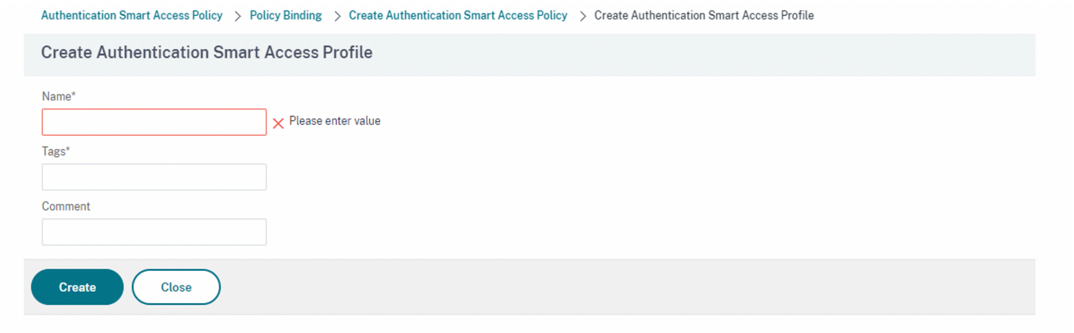
SAProfile_CertExists

Press Control+Space to start the expression and then type '.' to get the next set of options

d) On the **Create Authentication Smart Access Policy** screen, enter **Name** for the Smart Access Policy and click **Add** to create a Smart Access Profile.

The **Create Authentication Smart Access Profile** screen appears.

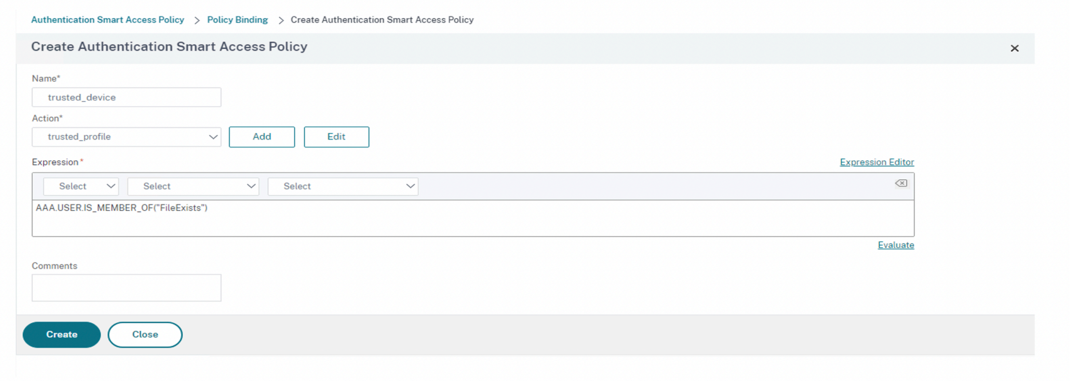
e) Add **Name** for the action. Enter *trusted* in **Tags**. The tag is later referenced in the Broker Access Policy rule for configuring. Click **Create**.


Authentication Smart Access Policy > Policy Binding > Create Authentication Smart Access Policy > Create Authentication Smart Access Profile
Create Authentication Smart Access Profile
Name*
Tags*
Comment
Create
Close

Please enter value

You return to the **Create Authentication Smart Access Policy** screen.

f) In the **Expression** section, enter the expression for which you want to push the tag. In this case, since the tag is pushed for trusted devices, enter `AAA.USER.IS_MEMBER_OF("FileExists")`. Click **Create**.


Authentication Smart Access Policy > Policy Binding > Create Authentication Smart Access Policy
Create Authentication Smart Access Policy
×
Name*
Action*
Add
Edit
Expression*
Expression Editor
Select
Select
Select
Evaluate
Comments
Create
Close

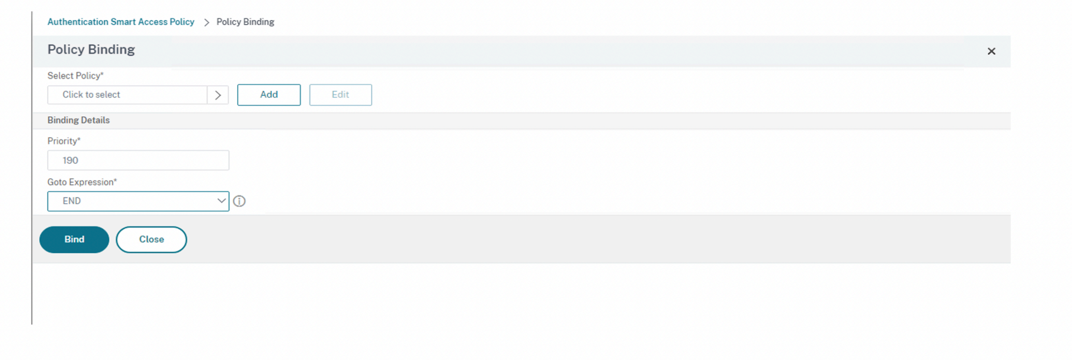
Name*: trusted_device

Action*: trusted_profile

Expression*: AAA.USER.IS_MEMBER_OF("FileExists")

You return to the **Policy Binding** screen.

g) Select the **Goto Expression** as *End* and Click **Bind**.



Authentication Smart Access Policy > Policy Binding

Policy Binding

Select Policy*: Click to select

Binding Details

Priority*: 190

Goto Expression*: END

4. Create a Smart Access Policy for untrusted devices:

    a) Follow the instructions of the previous step, except sub-steps **v** and **vi**.

    b) For the sub-step **v**, on the **Create Authentication Smart Access Profile** screen, add **Name** for the action. Enter *untrusted* in **Tags**. The tag is later referenced in the Broker Access Policy rule for configuring. Click **Create**.

    c) For the sub-step **vi**, in the **Expression** section of the **Create Authentication Smart Access Policy** screen, enter the expression for which you want to push the tag. In this case, since the tag is pushed for untrusted devices, enter `AAA.USER.IS_MEMBER_OF("FileExists").NOT`.

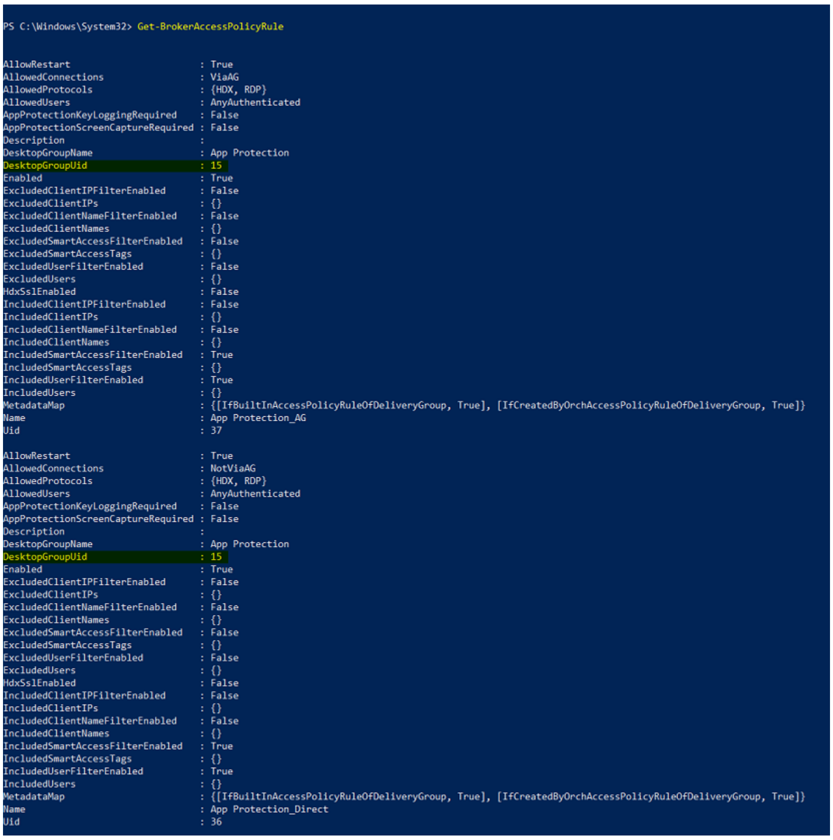
5. Configure the Broker Access policy rules:

    a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

    b) Run the command `Get-BrokerAccessPolicyRule`.

    A list of all the broker access policies for all the delivery groups which are present is displayed.

    c) Find the **DesktopGroupUid** for the delivery group that you want to change.



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                       : True
AllowedConnections                 : ViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_AG
Uid                                : 37

AllowRestart                       : True
AllowedConnections                 : NotViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_Direct
Uid                                : 36
```

d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To filter users using trusted devices, create another Broker Access policy using the command:

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) To disable App Protection for trusted devices and enable App Protection for untrusted devices, use the following command:

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false
```

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

6. Verification:

Sign out of Citrix Workspace app and sign in again. Launch the protected resource from a trusted device, one that meets the EPA scan condition. You see that the App Protection policies are not applied. Launch the same resource from an untrusted device. You see that the App Protection policies are applied.

Scenario 3

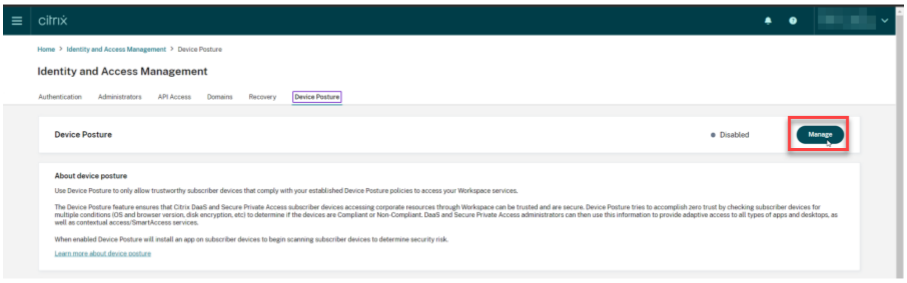
February 28, 2024

This scenario covers how to enable App Protection based on Device Posture results.

1. Configure Device Posture service:

    a) Sign in to Citrix Cloud.

    b) Navigate to **Identity and Access Management** > **Device Posture** and click **Manage**.

    About device posture

    Use Device Posture to only allow trustworthy subscriber devices that comply with your established Device Posture policies to access your Workspace services.

    The Device Posture feature ensures that Citrix DaaS and Secure Private Access subscriber devices accessing corporate resources through Workspace can be trusted and are secure. Device Posture tries to accomplish zero trust by checking subscriber devices for multiple conditions (OS and browser version, disk encryption, etc) to determine if the devices are Compliant or Non-Compliant. DaaS and Secure Private Access administrators can then use this information to provide adaptive access to all types of apps and desktops, as well as contextual access/SmartAccess services.

    When enabled Device Posture will install an app on subscriber devices to begin scanning subscriber devices to determine security risk.

    Learn more about device posture

    c) Click **Create device policy**.

    Create devicy policy page appears.

    d) Under **Policy rules**, click the **Select Rule** drop-down menu and select *Citrix Workspace app Version*.

    e) Click the **Select a rule** drop-down menu and select *Greater or equal to* >=.

    f) Enter the Citrix Workspace app version that you want to set as the condition. In this example, it is *23.7.0.19*.

    g) Under **Policy result**, select **Compliant**.

    h) In the **Name** field, enter a name for the policy.

    i) In the **Priority** field, enter the priority of the policy.

    j) Select the **Enable when created** checkbox to enable the policy since you created it.

    k) Click **Create**.

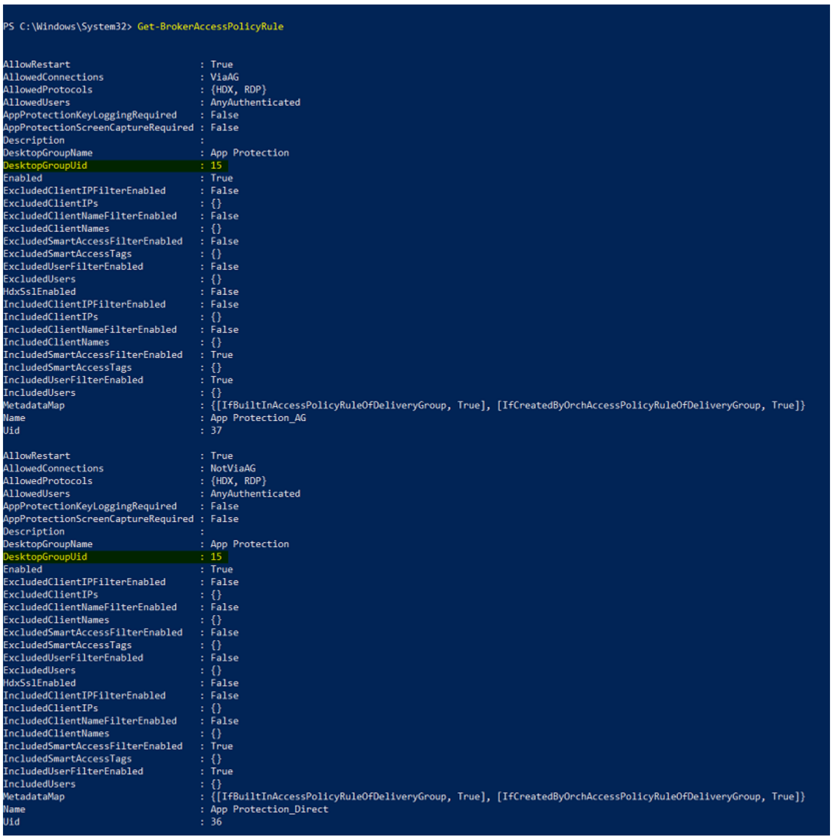
2. Configure the Broker Access policy rules:

a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

b) Run the command `Get-BrokerAccessPolicyRule`.

   A list of all the broker access policies for all the delivery groups which are present is displayed.

c) Find the **DesktopGroupUid** for the delivery group that you want to change.



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                       : True
AllowedConnections                 : ViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_AG
Uid                                : 37

AllowRestart                       : True
AllowedConnections                 : NotViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_Direct
Uid                                : 36
```

d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To apply App Protection to the compliant devices, run the following command:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) To apply App Protection to the non-compliant devices, run the following command:

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
```

```
$true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. Verification:

   Sign out of Citrix Workspace app. Sign in from a Citrix Workspace app version that is compliant with the device policy. You see that the App Protection policies are not applied. Again, sign out from the Citrix Workspace app and sign in from a Citrix Workspace app version that is not complaint with the device policy. You see that the App Protection policies are applied.

Scenario 4

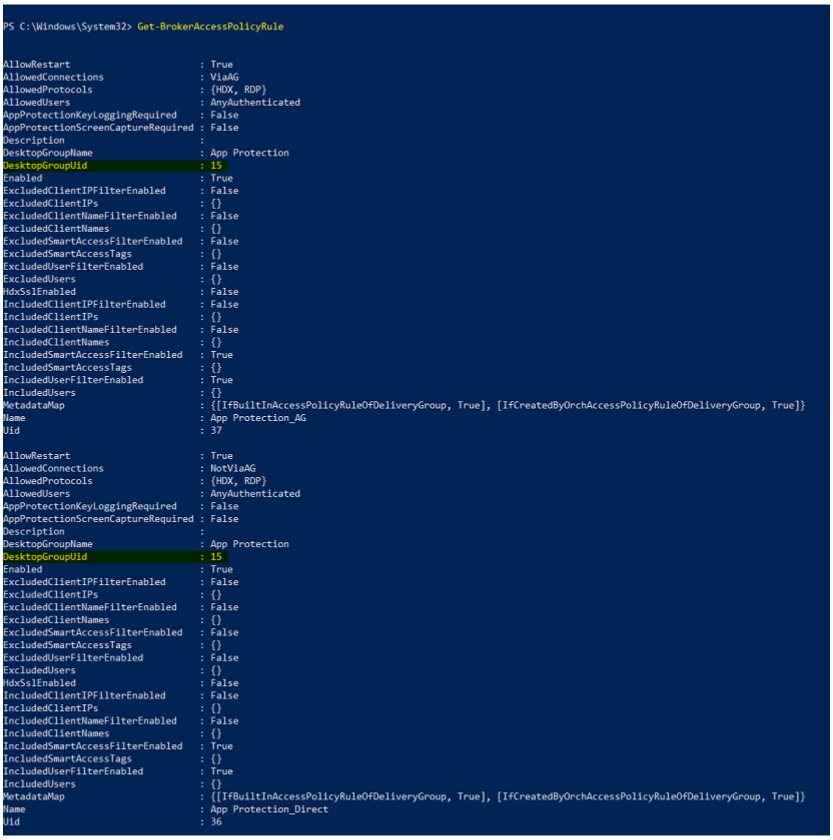
February 28, 2024

This scenario covers how to enable App Protection for specific user groups.

The following steps allow you to enable App Protection for users of a specific group:

1. Select the Active Directory user group for which you want to enable the App Protection policies for the users. In this example, the Active Directory user group is **ProductManagers**.
2. Configure the Broker Access policy rules:
   a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.
   b) Run the command `Get-BrokerAccessPolicyRule`.

      A list of all the broker access policies for all the delivery groups which are present is displayed.
   c) Find the **DesktopGroupUid** for the delivery group that you want to change.



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                       : True
AllowedConnections                 : ViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_AG
Uid                                : 37

AllowRestart                       : True
AllowedConnections                 : NotViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_Direct
Uid                                : 36
```

d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To enable App Protection policies for the users in the **ProductManagers** user group, run the following commands:

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) To disable App Protection policies for the users who are not a part of the the **ProductManagers** user group, run the following commands:

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. Verification:

Sign out of Citrix Workspace app, if already open. Sign in to Citrix Workspace app as a user in the **ProductManagers** Active Directory user group. Launch the protected resource and you see that App Protection is disabled. Sign out of Citrix Workspace app and Sign in again as a user who is not part of the **ProductManagers** Active Directory user group. Launch the protected resource and you see that App Protection is enabled.

Contextual App Protection for StoreFront

February 28, 2024

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture.

Implementing Contextual App Protection

You can implement contextual App Protection using the connection filters defined in the Broker Access policy rule. The Broker Access policies define the rules controlling a user's access to delivery groups. The policy comprises a set of rules. Each rule relates to a single delivery group, and has a set of connection filters and access right controls.

Users gain access to a delivery group when their connection's details match the connection filters of one or more rules in the Broker Access policy. Users don't have access to any desktop group within a site by default. You can create more Broker Access policies based on requirements. Multiple rules can apply to the same delivery group. For more information, see New-BrokerAccessPolicyRule.

The following parameters in the Broker Access policy rule provide the flexibility to enable App Protection contextually if the user's connection matches the connection filters defined in the access policy rule:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Use the Smart Access filters referenced in the Broker Access policies to refine the connection filters. For information on configuring Smart Access filters, see this CTX227055. Refer to the following scenarios to understand how to use the Smart Access policies to set up Contextual App Protection.

> **Note:**
>
> If App Protection is enabled on the Delivery Group, then Contextual App Protection cannot be applied by default. Disable App Protection on the Delivery Group by using the following command:
>
> ```
> Set-BrokerDesktopGroup -Name "Admin Desktop" -
>     AppProtectionKeyLoggingRequired $false -
>     AppProtectionScreenCaptureRequired $false
> ```

```
<!--NeedCopy-->
```

Prerequisites

To enable Contextual App Protection for StoreFront, make sure that you meet the requirements mentioned in the Prerequisites section.

Enable Contextual App Protection

1. Download the Contextual App Protection policies (feature table) for your Citrix Virtual Apps and Desktops version from the Citrix Downloads page.
2. Run the following PowerShell command in the delivery controller:

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. Run the following command to enable contextual App Protection in the delivery controller:

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   For example,

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
       AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```

Contextual App Protection scenarios

Following are some of the scenarios about how you can enable or disable Contextual App Protection:

- Disable App Protection for certain device types
- Disable App Protection for connections started from browser-based access and enable App Protection for connections from Citrix Workspace app
- Disable App Protection for users in a specific Active Directory group
- Enable App Protection for devices based on the EPA scan results
- Enable App Protection for specific user groups

Prerequisites

February 28, 2024

Make sure that you have the following:

- Citrix Virtual Apps and Desktops version 2109 or later
- Delivery Controller version 2109 or later
- StoreFront version 1912 LTSR or later
- VPN virtual server or gateway and authentication virtual server configurations
- Successful connection between NetScaler and StoreFront. For more information, see Integrate NetScaler Gateway with StoreFront
- XML table import is required up to Citrix Virtual Apps and Desktops version 2006
- Contextual App Protection feature table import is required up to Citrix Virtual Apps and Desktops version 2209
- Enable Smart Access on NetScaler Gateway, for scenarios that require Smart Access tags. For more information, see this support article.
- Licensing requirements -
  - App Protection On-premises license
  - Citrix Gateway Universal license for scenarios with Smart Access tags

Scenario 1

February 28, 2024

This scenario covers how to disable App Protection for certain device types.

The following are the steps to disable App Protection for iPhone users on a delivery group called `Win10Desktop`:

1. Create a Smart Access policy:

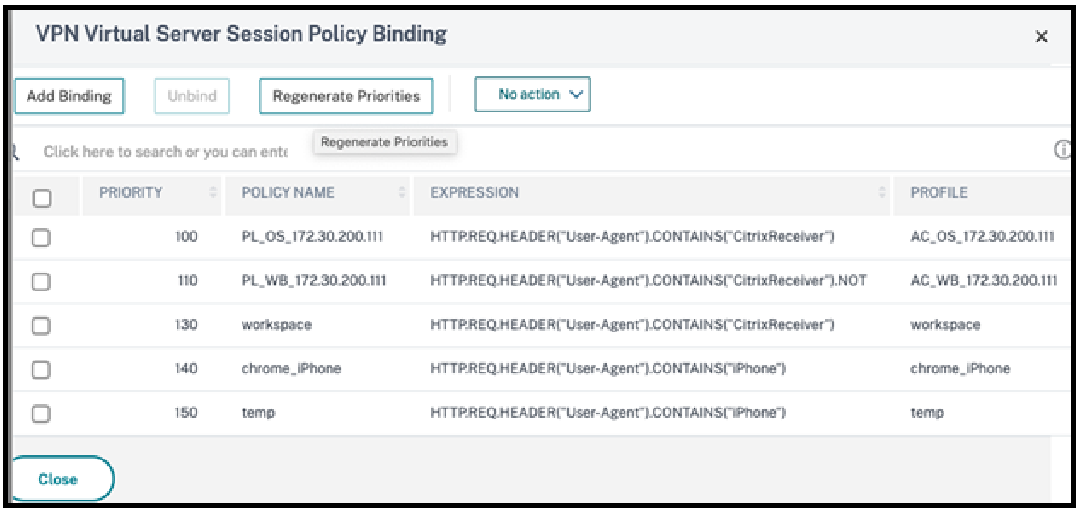
   a) Sign in to the Citrix ADC Administration UI.

   b) On the left navigation menu, go to **Citrix Gateway** > **Virtual Servers**.

      Note the VPN Virtual Server name, which is needed to configure the Broker Access Policy later on.

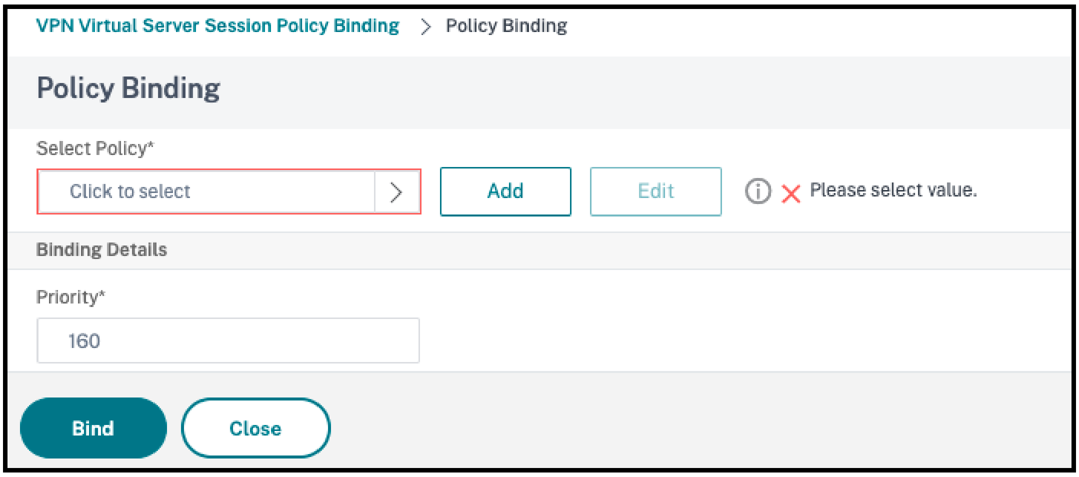
   c) Click **VPN Virtual Server**. Scroll to the bottom of the page and click **Session policies**. A list of session policies appears.

d) Click **Add Binding**.


VPN Virtual Server Session Policy Binding
×
Add Binding
Unbind
Regenerate Priorities
No action
Click here to search or you can ente
Regenerate Priorities
Close

□	PRIORITY	POLICY NAME	EXPRESSION	PROFILE
□	100	PL_OS_172.30.200.111	HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")	AC_OS_172.30.200.111
□	110	PL_WB_172.30.200.111	HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT	AC_WB_172.30.200.111
□	130	workspace	HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")	workspace
□	140	chrome_iPhone	HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")	chrome_iPhone
□	150	temp	HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")	temp

e) Click **Add to create a session policy**.



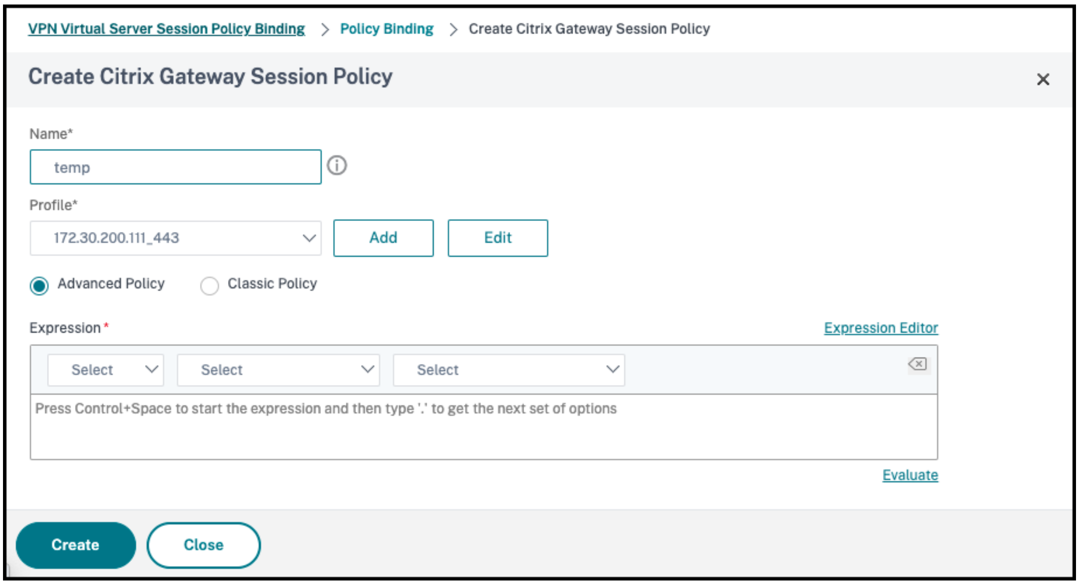
Select Policy*: Click to select

Please select value.

Binding Details

Priority*: 160

f) Enter a name for the session policy. In this scenario, it is *temp*.



VPN Virtual Server Session Policy Binding > Policy Binding > Create Citrix Gateway Session Policy

Create Citrix Gateway Session Policy

Name*: temp

Profile*: 172.30.200.111_443 — Add — Edit

● Advanced Policy ○ Classic Policy

Expression* — Expression Editor

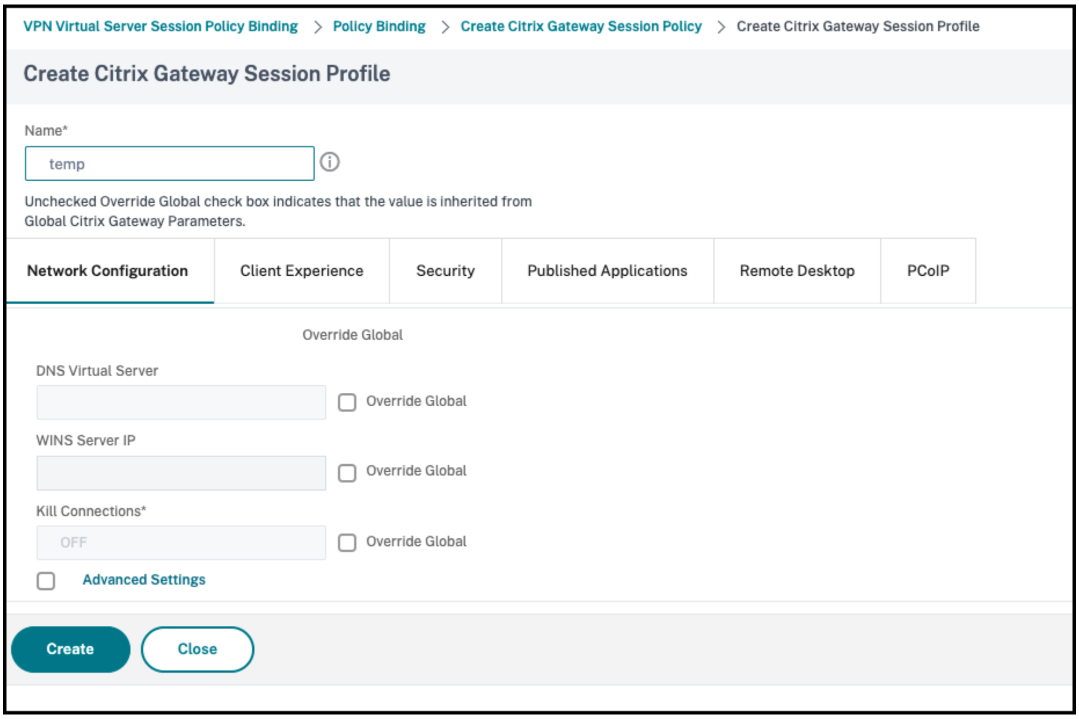
Select — Select — Select

Press Control+Space to start the expression and then type '.' to get the next set of options

Evaluate

Create — Close

g) Click **Add** next to Profile to specify a Profile name. Click **Create**.



VPN Virtual Server Session Policy Binding > Policy Binding > Create Citrix Gateway Session Policy > Create Citrix Gateway Session Profile

Create Citrix Gateway Session Profile

Name*: temp

Unchecked Override Global check box indicates that the value is inherited from Global Citrix Gateway Parameters.

Network Configuration | Client Experience | Security | Published Applications | Remote Desktop | PCoIP

Override Global

DNS Virtual Server — □ Override Global

WINS Server IP — □ Override Global

Kill Connections*: OFF — □ Override Global

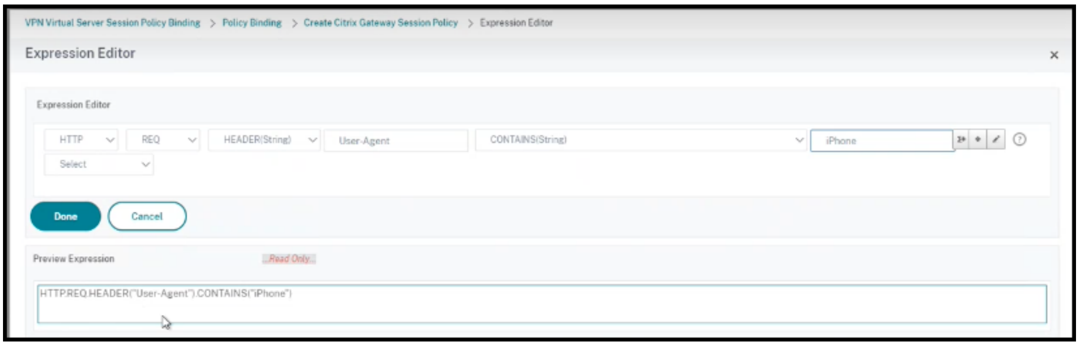
□ Advanced Settings

Create — Close

h) Click **Expression Editor** from the Session policy window.

i) Create the following expression to check for *iPhone* in the **User Agent** string:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
<!--NeedCopy-->
```


VPN Virtual Server Session Policy Binding > Policy Binding > Create Citrix Gateway Session Policy > Expression Editor
Expression Editor
×
Expression Editor
Select
Done
Cancel
Preview Expression
Read Only

HTTP | REQ | HEADER(String) | User-Agent | CONTAINS(String) | iPhone

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
```

j) Click **Bind** to create the session policy.

2. Create Broker access policy rules:

   To apply the policy for iPhone users accessing `Win10Desktop` through the access gateway, do the following steps:

   a) Run the following command in the Delivery controller (DDC):

   ```
   Get-BrokerAccessPolicyRule
   <!--NeedCopy-->
   ```

   which lists all the Broker Access policies defined in the DDC. In this scenario, the Broker Access policies for the delivery group `Win10Desktop` are `Win10Desktop_AG` and `Win10Desktop_Direct`. Note the desktop group UID of the delivery group for the next step.

   b) Create a broker access policy rule for `Win10Desktop` to filter iPhone users coming through the access gateway using the following command:

   ```
   New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
       DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
       ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
       AnyAuthenticated -AllowRestart $true -
       AppProtectionKeyLoggingRequired $false -
       AppProtectionScreenCaptureRequired $false -Enabled $true -
       IncludedSmartAccessFilterEnabled $true
   <!--NeedCopy-->
   ```

   Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the GetBrokerAccessPolicy Rule in step 1.

   c) To disable App Protection for `Win10Desktop` iPhone users coming through the access gateway, reference the Smart Access tag *temp* created in Step 1. Create Smart Access policy using the following command:

   ```
   Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
       IncludedSmartAccessTags Primary_HDX_Proxy:temp -
       AppProtectionScreenCaptureRequired $false -
       AppProtectionKeyLoggingRequired $false
   ```

```
<!--NeedCopy-->
```

Primary_HDX_Proxy is the VPN virtual server name from earlier in Step 1, Create Smart Access Policy.

d) To enable App Protection policies for the rest of the `Win10desktop` users, use the following command:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

3. **Verification**

   For iPhone: Sign out of the Citrix Workspace app, if already open on the iPhone. Sign in to Citrix Workspace app externally through the access gateway connection. You can see the required resources in StoreFront and App Protection has to be disabled.

   For devices other than the iPhone: Sign out of the Citrix Workspace app, if already open on the device. Sign in to Citrix Workspace app externally through an access gateway connection. You can see the required resources in the StoreFront and App Protection has to be disabled.

Scenario 2

February 28, 2024

This scenario covers how to disable App Protection for connections started from browser-based access and enable App Protection for connections started from Citrix Workspace app.

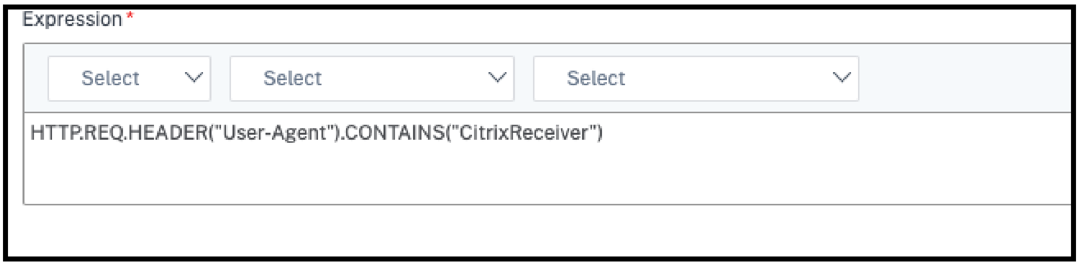
The following are the steps to disable App Protection for a delivery group called `Win10Desktop` when connections are started from a browser and enable App Protection for connections from Citrix Workspace app:

1. Create Smart Access policies:

   a) Create a Smart Access policy to filter the connections started from the Citrix Workspace app, as defined in the preceding scenario **Disable App Protection for certain device types**. Create the following expression, to check for **CitrixReceiver** in the **User Agent** string:

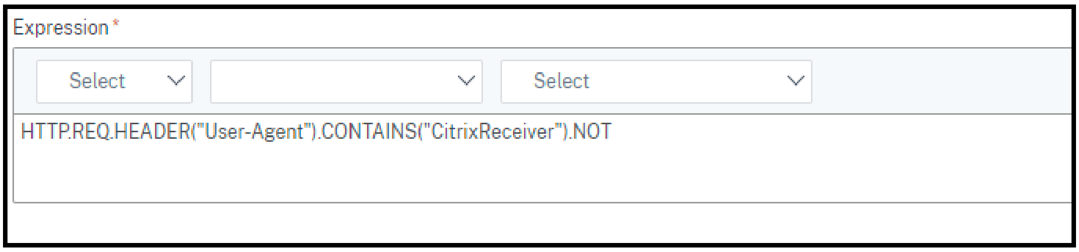
   ```
   HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
   <!--NeedCopy-->
   ```

In this scenario, the Smart Access policy is cwa.



HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")

b) Create another Smart Access policy to filter the connections that aren't started from the Citrix Workspace app, `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`. In this case, this Smart Access policy is *browser*.



HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT

2. Create Broker Access policy rules:

a) Run `GetBrokerAccessPolicyRule` to view the two broker access policies for `Win10Desktop`. For the delivery group `Win10Desktop`, the broker access policies are `Win10Desktop_AG` and `Win10Desktop_Direct`. Note the Desktop Group UID of `Win10Desktop`.

b) Create a Broker Access policy for `Win10Desktop` to filter connections started from the Citrix Workspace app by using the following command:

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the GetBrokerAccessPolicy Rule in step 1.

c) Use the following command to enable App Protection policies only for connections coming through CWA by referencing the Smart Access tag cwa:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
    IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

Primary_HDX_Proxy is the VPN virtual server name noted down earlier in Step 1, Create Smart Access Policy.

d) Use the following command to disable App Protection policies for the rest of the connections coming through the browser:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -IncludedSmartAccessTags Primary_HDX_Proxy:browser -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

3. **Verification**

   Sign out of Citrix Workspace app, if already open. Sign in to Citrix Workspace app again and launch the required resource from an external connection through an access gateway. You can see that the App Protection policies are enabled for the resource. Launch the same resource from the browser through an external connection and you can see that the App Protection policies are disabled.

Scenario 3

February 28, 2024

This scenario covers how to disable App Protection for users in a specific Active Directory group.

Following are the steps to disable App Protection for `Win10Desktop` users who are part of the Active Directory group **xd.local\sales**:

1. Run `Get-BrokerAccessPolicyRule` to view the two broker access policies for `Win10Desktop`. For a delivery group `Win10Desktop` there are two broker access policies, `Win10Desktop_AG` and `Win10Desktop_Direct`. Make a note of the Desktop Group UID of the `Win10Desktop`.

2. Create a Broker access policy rule for `Win10Desktop` to filter connections from users in the Active Directory group `xd.local\sales`.

   ```
   New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG -AllowedProtocols HDX, RDP -AllowedUsers Filtered -AllowRestart $true -Enabled $true
   <!--NeedCopy-->
   ```

   Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the Get-BrokerAccessPolicy Rule in step 1.

3. Use the following command to disable App Protection policies for the Windows 10 Desktop users, part of the AD group **xd.local\sales**:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
    AllowedUsers Filtered -IncludedUsers xd.local\sales -
    IncludedUserFilterEnabled $true -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

4. Use the following command to enable App Protection policies for the rest of the gateway connections except for the users from **xd.local\sales**:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

5. **Verification**

   Sign out of the Citrix Workspace app, if already open. Sign in to the Citrix Workspace app as a user in the **xd.local\sales** Active Directory group. Launch the protected resource and you see that App Protection is disabled.

   Sign out of the Citrix Workspace app and sign in again as a user who is not part of **xd.local\sales**. Launch the protected resource and you see that App Protection is enabled.

Scenario 4

February 28, 2024

This scenario covers how to enable App Protection for devices based on the EPA scan results.

Following are the steps to enable App Protection for the devices that pass the EPA scans:

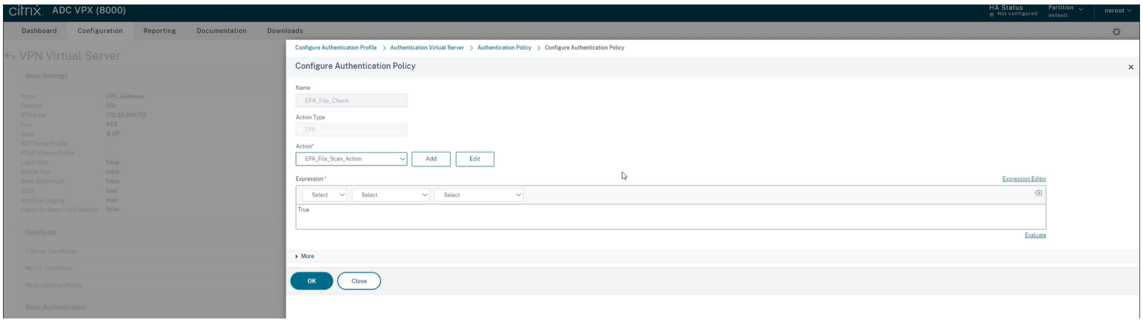
Prerequisites:

Make sure that you have the following:

- Authentication, authorization, and auditing user groups (for default and quarantined user groups) and associated policies
- LDAP server configurations and associated policies

1. Sign in to Citrix ADC and go to **Configuration** > **Citrix Gateway** > **Virtual Servers**.
2. Select the relevant Virtual Server and click **Edit**.

3. Edit the existing Authentication Profile.
4. Select the relevant Virtual Server and click **Edit**.
5. Click **Authentication Policies** > **Add Binding**.
6. Under **Select Policy**, click **Add**.
7. In the **Name** field, enter the name of the Authentication Policy.
8. In the **Action Type** drop-down list, select **EPA**.
9. In the **Expression** field, enter `True`.



Configure Authentication Policy

Name: EPA_File_Check

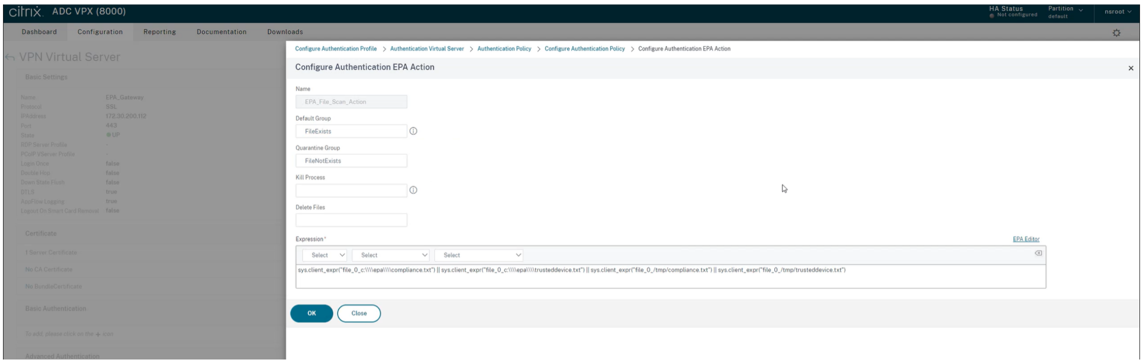
Action Type: EPA

Action*: EPA_File_Scan_Action

Expression*: True

10. Under **Action**, click **Add**.
11. In the **Name** field, enter the name of the EPA Action.
12. Enter the **Default Group** and **Quarantine Group** names. In this scenario, **Default Group** name is **FileExists** and **Quarantine Group** name is **FileNotExists**.
13. In the **Expression** field, enter the following value:

```
sys.client_expr("file_0_c:\\\\epa\\\\compliance.txt") || sys.client_expr("file_0_c:\\\\epa\\\\trusteddevice.txt") || sys.client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("file_0_/tmp/trusteddevice.txt")
<!--NeedCopy-->
```


citrix. ADC VPX (8000)
HA Status Not configured
Partition default
nsroot
Dashboard
Configuration
Reporting
Documentation
Downloads
VPN Virtual Server
Configure Authentication Profile > Authentication Virtual Server > Authentication Policy > Configure Authentication Policy > Configure Authentication EPA Action

Configure Authentication EPA Action

Name: EPA_File_Scan_Action

Default Group: FileExists

Quarantine Group: FileNotExists

Kill Process:

Delete Files:

Expression*: sys.client_expr("file_0_c:\\\\epa\\\\compliance.txt") || sys.client_expr("file_0_c:\\\\epa\\\\trusteddevice.txt") || sys.client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("file_0_/tmp/trusteddevice.txt")

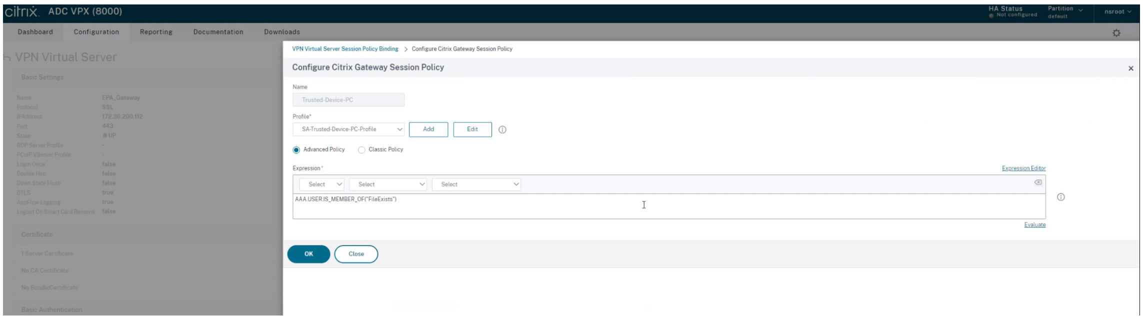
14. Click **Create** and then click **Bind**.
15. Click **Session Policies** > **Add Binding**.

16. Under **Select Policy**, click **Add**.

17. In the **Name** field, enter the name of the Session Policy.

18. In the **Expression** field, enter the following value:

```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```



Name EPA_Gateway
Protocol SSL
IPAddress 172.30.200.112
Port 443
State UP
RDP Server Profile -
PCoIP VServer Profile -
Login Once false
Double Hop false
Down State Flush false
DTLS true
AppFlow Logging true
Logout On Smart Card Removal false

1 Server Certificate
No CA Certificate
No BundleCertificate

Configure Citrix Gateway Session Policy

Name: Trusted-Device-PC

Profile*: SA-Trusted-Device-PC-Profile

● Advanced Policy ○ Classic Policy

Expression*: AAA.USER.IS_MEMBER_OF("FileExists")

19. Click **Create** and then click **Bind**.

20. On the leftmost side of the taskbar, click the **Search** icon.

21. Type **Powershell** and open **Windows Powershell**.

22. Use the following command to disable App Protection policies for devices that have passed the EPA scans by referencing the **Smart Access tag"EPA_GW:Trusted-Device-PC"**:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

where, *EPA_GW* is the VPN Virtual Server name.

23. Use the following command to enable App Protection policies for devices that have failed the EPA scans by referencing the **Smart Access tag"EPA_GW:Trusted-Device-PC"**:

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
    $true -ExcludedSmartAccessFilterEnabled $true -
    ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    IncludedSmartAccessFilterEnabled $true -
    AppProtectionScreenCaptureRequired $true
<!--NeedCopy-->
```

24. **Verification**

    Sign out of the Citrix Workspace app, if already open. Sign in to the Citrix Workspace app from a trusted device. Launch the protected resource and you see that App Protection is disabled.

Sign out of the Citrix Workspace app and Sign in again from an untrusted device. Launch the protected resource and you see that App Protection is enabled.

Scenario 5

December 27, 2023

This scenario covers how to enable App Protection for specific user groups.

To enable App Protection for users of a specific group, see Enable App Protection for specific user groups

App Protection support for hybrid launch through Workspace

February 28, 2024

Hybrid launches of Citrix Virtual Apps and Desktops are when you sign in to Citrix Workspace for Web by typing the store URL in the native browser, and launching the virtual apps and desktops through the native Citrix Workspace app and its HDX engine. The term hybrid is the result of using the combination of Citrix Workspace app for Web and the native Citrix Workspace app to connect and use the resources.

> **Note:**
>
> When no native Citrix Workspace app components are installed on the endpoint, it's a zero-install configuration where both the Citrix Workspace store and the HDX engine are within the browser. This scenario is known as the Citrix Workspace app for HTML5, which is hosted either on Citrix Workspace or Citrix StoreFront. This document does not address that scenario.

Prerequisites

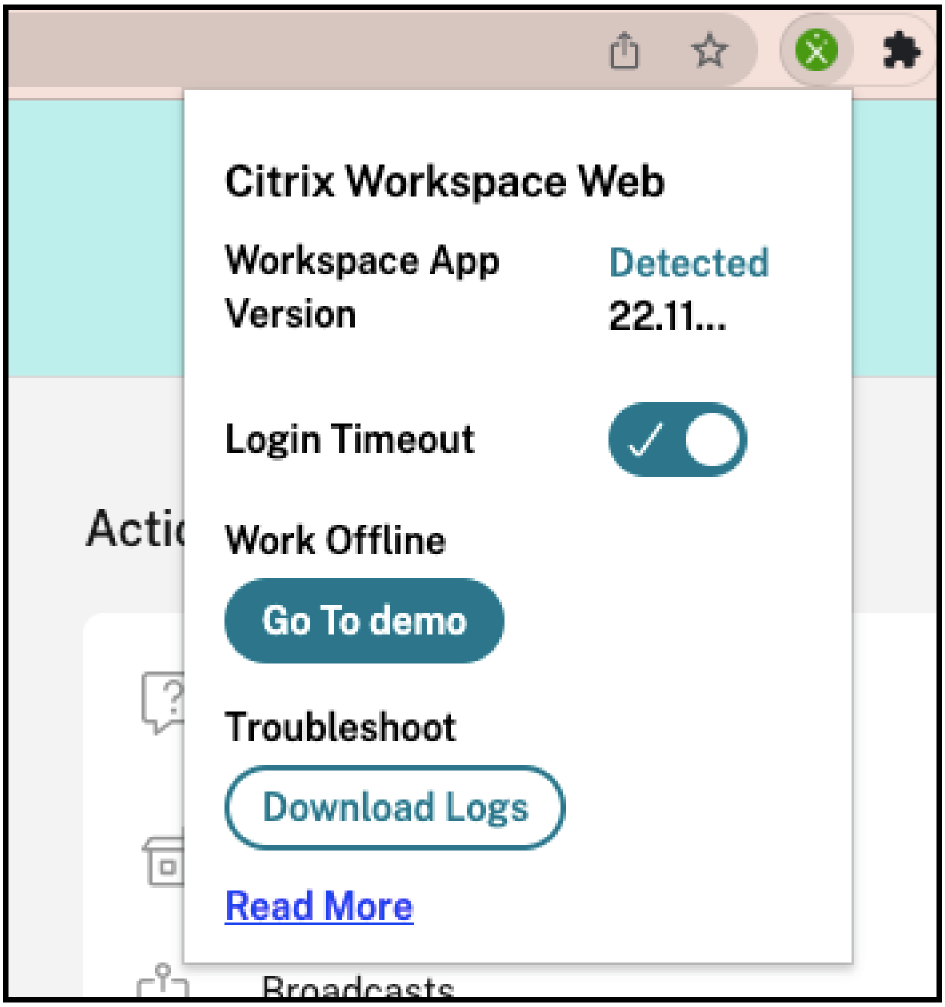
- Make sure that you're on a browser that supports the Citrix Workspace Web extension.
- Make sure that the DNS suffix of your Workspace URL is cloud.com. Currently, custom domains are not supported.
- Make sure that you're on one of the following versions of Citrix Workspace app:
  - Citrix Workspace app for Windows 2106 or later
  - Citrix Workspace app for macOS 2106 or later

Enable App Protection for hybrid launch

1. Install the Citrix Workspace Web extension for your browser before adding the store. Use one of the following links based on your browser:

   - Chrome
   - Edge Chromium

   Once you install the extension, you see it in the extensions section of your browser.



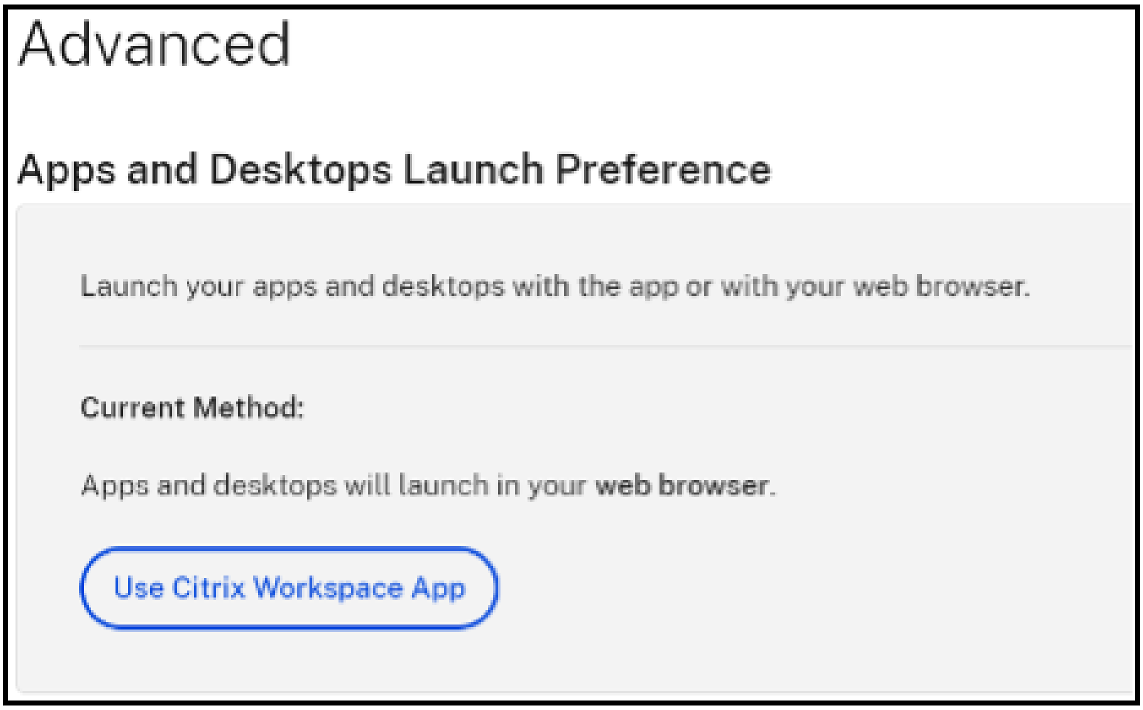
Citrix Workspace Web

Workspace App Version: Detected 22.11...

Login Timeout: ✓

2. Sign in to the store from your native browser.
3. Navigate to your **Profile > Account Settings > Advanced**.

   In the **Apps and Desktops Launch Preference** section, you can see the current method in which the apps and desktops currently launch in your web browser. Click **Use Citrix Workspace app**.



Advanced

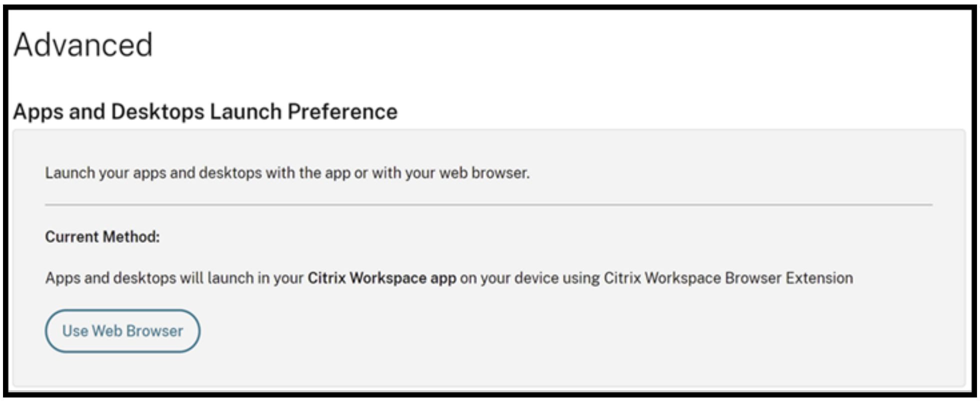
Apps and Desktops Launch Preference

Launch your apps and desktops with the app or with your web browser.

Current Method:

Apps and desktops will launch in your **web browser**.

If you're using the Citrix Workspace app to launch the resources, you see the following option. In such a case, no changes are required.



Advanced

Apps and Desktops Launch Preference

Launch your apps and desktops with the app or with your web browser.

Current Method:

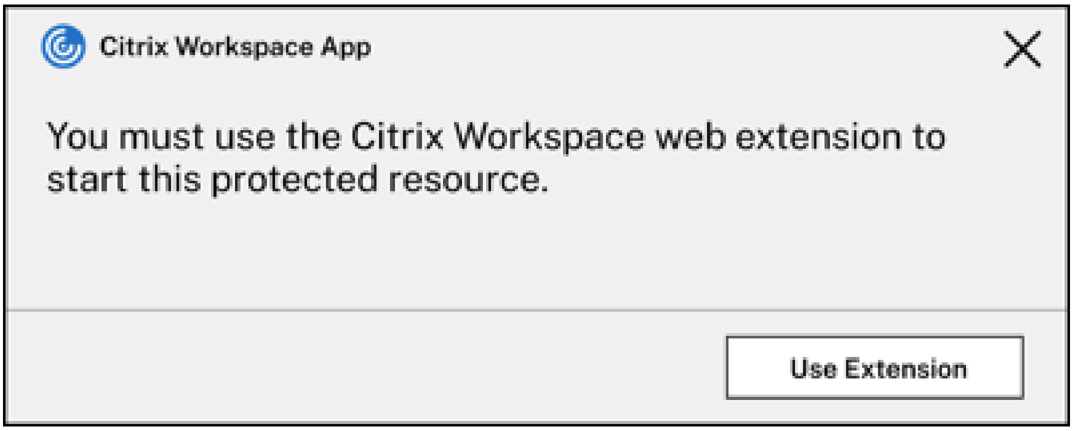
Apps and desktops will launch in your **Citrix Workspace app** on your device using Citrix Workspace Browser Extension

4. You can now launch your protected virtual app or desktop.

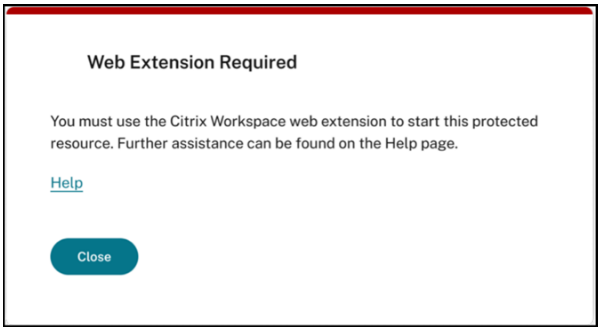
Common failure scenarios

Here are some scenarios to demonstrate failure in launches and how to fix them.

- You get one of the following errors when you disable or uninstall the Citrix Workspace Web extension before launching the protected application. To avoid it, install the extension before you log in to Citrix Workspace for Web.

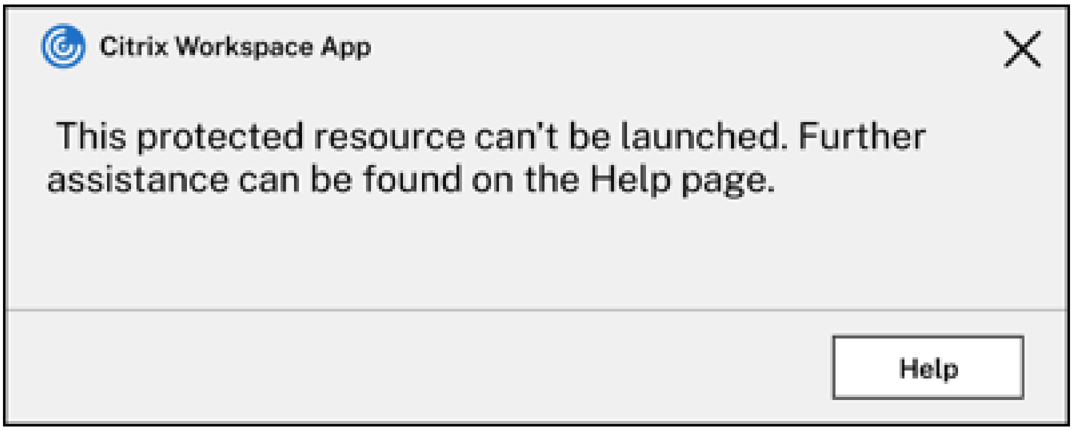


You must use the Citrix Workspace web extension to start this protected resource.

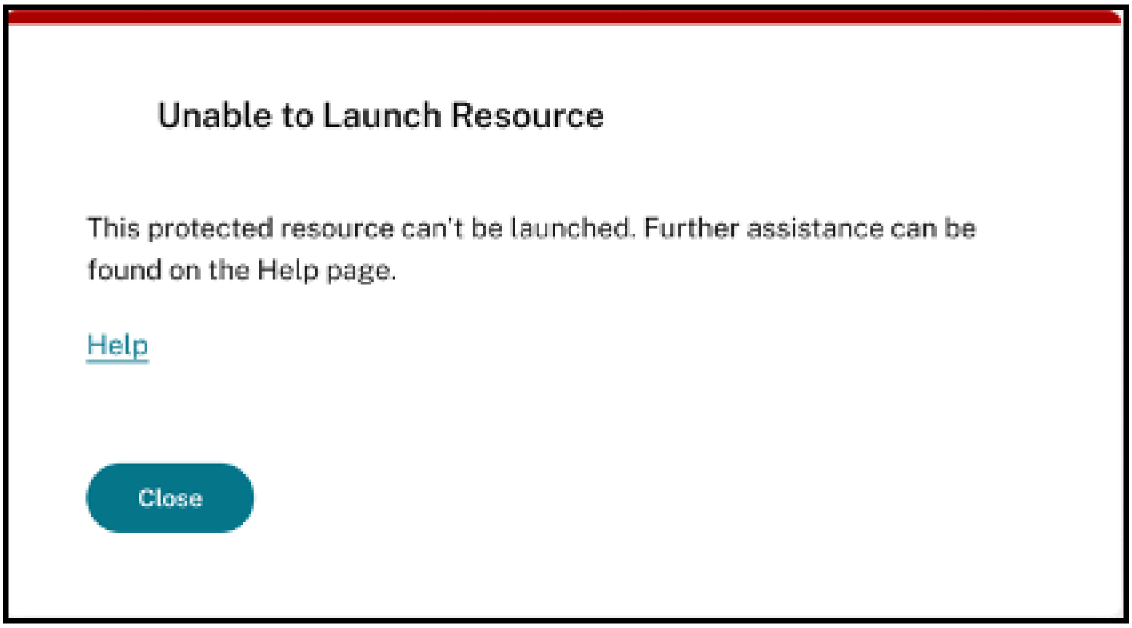

Web Extension Required

You must use the Citrix Workspace web extension to start this protected resource. Further assistance can be found on the Help page.

- You get one of the following errors when the launch preference is set as **Web Browser**. Change the launch preference to **Use Citrix Workspace app** to resolve this error. For more information, see this support article.



This protected resource can't be launched. Further assistance can be found on the Help page.



Unable to Launch Resource

This protected resource can't be launched. Further assistance can be found on the Help page.

App Protection support for hybrid launch through StoreFront

February 28, 2024

Hybrid launch of Citrix Virtual Apps and Desktops is when you sign in to StoreFront for Web by typing the store URL in the native browser and launch the virtual apps and desktops through the native Citrix Workspace app and its HDX engine. The term hybrid is the result of using the combination of StoreFront for Web and the native Citrix Workspace app to connect and use the resources.

> **Note:**
>
> When no native Citrix Workspace app components are installed on the endpoint, it's a zero-install configuration where both the Citrix Workspace store and the HDX engine are within the browser. This scenario is known as Citrix Workspace app for HTML5, which is hosted either on Citrix Workspace or Citrix StoreFront. This document does not address that scenario.

App Protection support for hybrid launch through StoreFront provides the ability for App Protection enabled resources to be displayed and launched from browsers.

> **Note:**
>
> If you select the options **Use light version** (which uses the HTML5 client) or **Already installed**, then the App Protection enabled sessions are blocked as Citrix Workspace app isn't detected successfully in the browser.

If you're using StoreFront 2308 or later, then you can access the apps and desktops that are enabled with App Protection policies using a web browser if StoreFront is configured appropriately and the browser successfully detects the native Citrix Workspace app. If you're using versions between StoreFront 1912 and 2203, then you must apply the customization as described in the How to deploy section.

> **Limitation:**
>
> StoreFront determines the Citrix Workspace app version when you sign in to the website for the first time. If you later install a different version of Citrix Workspace app, then StoreFront isn't aware of the change. So, it might incorrectly allow or disallow the launching of virtual apps and desktops enabled with App Protection policies. Citrix recommends configuring App Protection Posture Check which blocks launching virtual apps and desktops from previous versions of Citrix Workspace app that do not support App Protection. For more information about Posture Check, see App Protection Posture Check.

Hybrid launch through StoreFront version 2308 or later

StoreFront versions 2308 and later automatically supports hybrid launch of virtual apps and desktops enabled with App Protection policies. For more information about enabling App Protection for hybrid launch on StoreFront 2308 or later, see App Protection for hybrid launch via StoreFront.

Hybrid launch through StoreFront versions between 1912 and 2203

StoreFront versions between 1912 and 2203 supports the enabling of hybrid launch of virtual apps and desktops that are enabled with App Protection policies using a customization as follows:

Citrix recommends removing this customization when upgrading to StoreFront 2308 or later.

Prerequisites

For information about the required versions of Citrix components for App Protection, see System requirements.

How to deploy

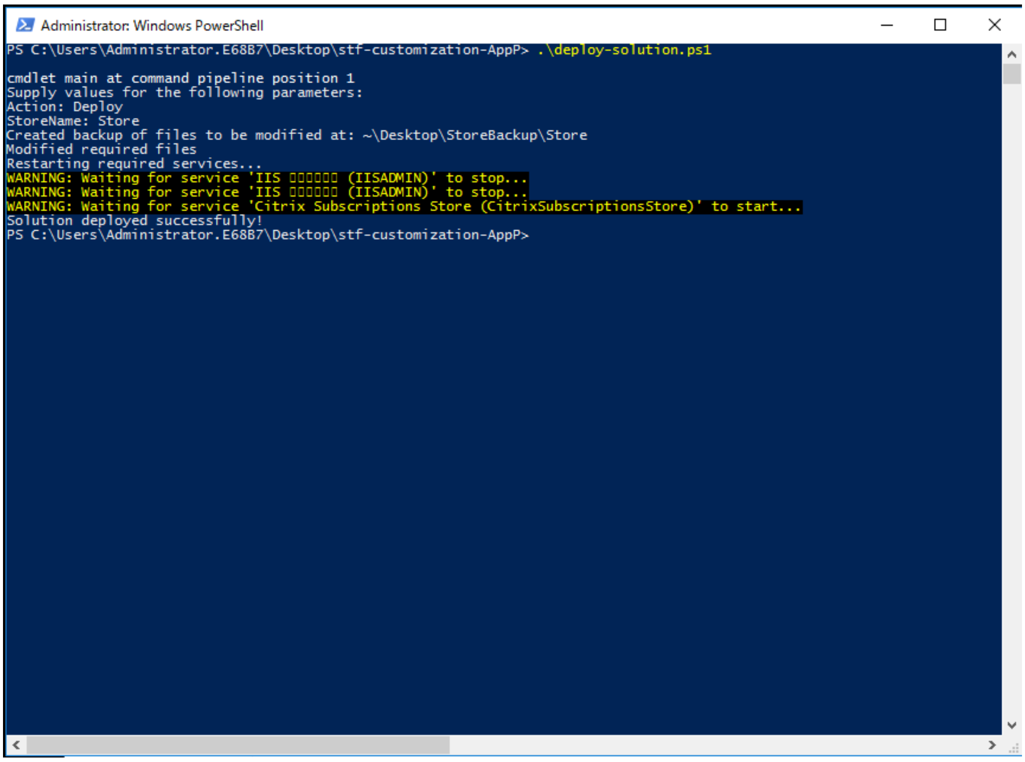
1. Download the Zip file named *stf-customization-AppP.zip*, which has all the required files that you must deploy to the StoreFront server machine. Download the file from Citrix Downloads. The file includes the following:

   - DLLs that you must copy to the store's bin folder

- JavaScript files and other files required for the solution to work
- *deploy-solution.ps1* PowerShell script, which the StoreFront admin uses to deploy the solution

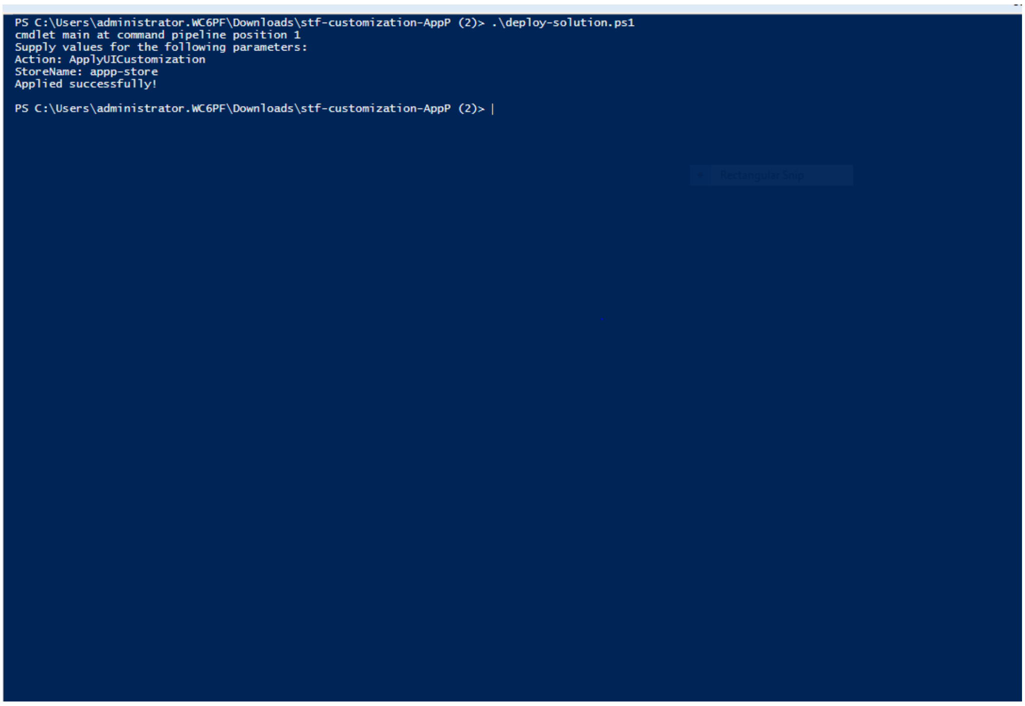
2. Unzip the *stf-customization-AppP.zip* file and open a new administrator PowerShell where the files are extracted. Run the `deploy-solution.ps1` command, which takes the following arguments:

   - `-Action`: The action that the script takes. The allowed values are as follows:
     - The `Deploy` action deploys the solution in a seamless manner. It creates a backup of files that this solution changes, copies the solution files, and restarts the services. The following screenshot describes the command to deploy the solution on the StoreFront server:



```
PS C:\Users\Administrator.E68B7\Desktop\stf-customization-AppP> .\deploy-solution.ps1

cmdlet main at command pipeline position 1
Supply values for the following parameters:
Action: Deploy
StoreName: Store
Created backup of files to be modified at: ~\Desktop\StoreBackup\Store
Modified required files
Restarting required services...
WARNING: Waiting for service 'IIS □□□□□□ (IISADMIN)' to stop...
WARNING: Waiting for service 'IIS □□□□□□ (IISADMIN)' to stop...
WARNING: Waiting for service 'Citrix Subscriptions Store (CitrixSubscriptionsStore)' to start...
Solution deployed successfully!
PS C:\Users\Administrator.E68B7\Desktop\stf-customization-AppP>
```

     - The `ApplyUICustomization` action applies a customization on the store UI so that you don't see the **Already installed** and **Use light version** options. This action enforces detection of the native Citrix Workspace app in the browser and makes sure that you bypass the blocked or unsupported scenarios.



```
PS C:\Users\administrator.WC6PF\Downloads\stf-customization-AppP (2)> .\deploy-solution.ps1
cmdlet main at command pipeline position 1
Supply values for the following parameters:
Action: ApplyUICustomization
StoreName: appp-store
Applied successfully!

PS C:\Users\administrator.WC6PF\Downloads\stf-customization-AppP (2)> |
```

  - The `RemoveUICustomization` action undoes the action of `ApplyUICustomization` and the **Already Installed** and **Use light version** options appear again.

- `-StoreName`: The name of the store for which the action must be taken. This parameter is mandatory and it must be passed along with the `Deploy` action.
- `-BackupDir`: Parameter that can be passed with the `Deploy` action to create a backup at the required directory. If not passed, the backup is created on the desktop. This parameter is an optional parameter.

> **Note:**
>
> If there are any existing customizations in *StoreCustomization_Input.dll* or *StoreCustomization_Launch.dll*, deploying this solution overrides them.

The App Protection enabled apps and desktops will only display after deploying the customizations. Without the deployment, the apps and desktops don't display.

How to revert StoreFront customization

Do the following steps to revert the preceding StoreFront customization:

1. Go to *\Desktop\StoreBackup<store name>* directory and copy the following files to the respective directories:

    - *StoreCustomization_Input.dll* and *StoreCustomization_Launch.dll* files to the *IISINETPub\Citrix<store name>\bin* directory

   - _web.config_ file to the _IISINETPub\Citrix\StoreWeb_ directory
   - _*.js_ and _style.css_ files to the _IISINETPub\Citrix\StoreWeb\Custom_ directory

     > **Note:**
     >
     > If there are customization files other than the preceding files in the \Desktop\StoreBackup<store name> directory, copy those files and directories to the relevant directories as needed.

2. Open PowerShell.
3. Stop the **IISADMIN** and **CitrixSubscriptionsStore** services by running the following commands:

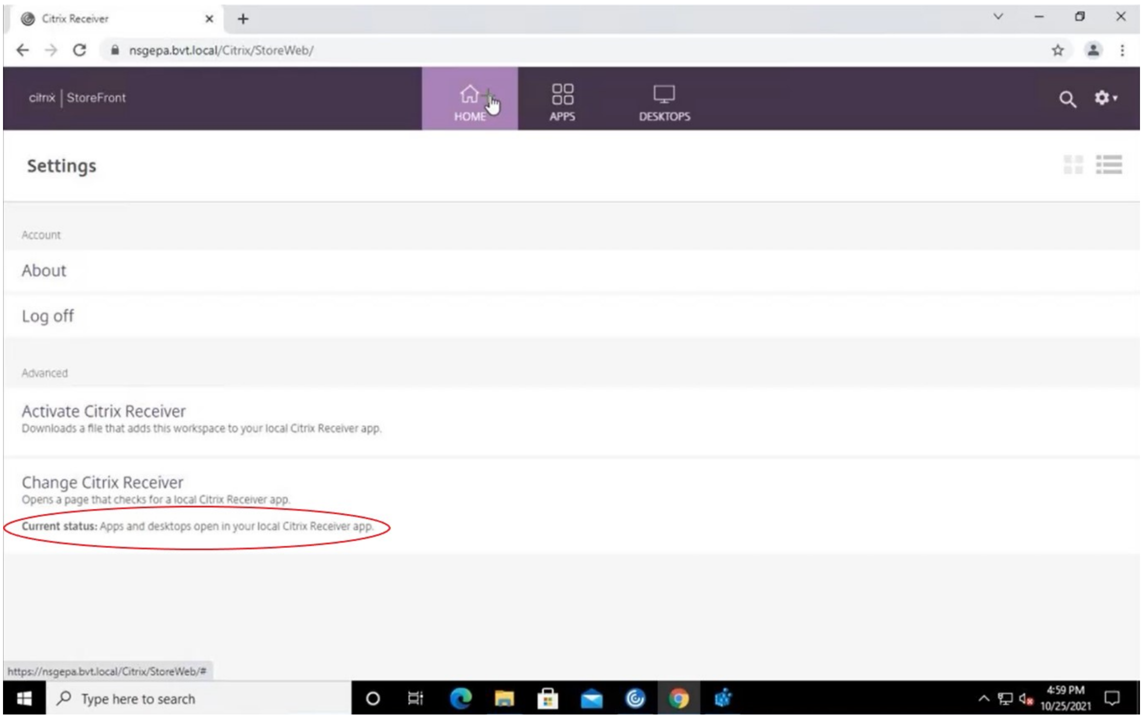
   ```
   sc stop IISADMIN
   sc stop CitrixSubscriptionsStore
   <!--NeedCopy-->
   ```

4. Start the **IISADMIN** and **CitrixSubscriptionsStore** services again by running the following commands:

   ```
   sc start IISADMIN
   sc start CitrixSubscriptionsStore
   <!--NeedCopy-->
   ```

End user experience of hybrid launch for protected resources

1. After the deployment of the solution by the admin on the StoreFront server, sign in to your store on the client side and then access StoreFront using the URL in a web browser.
2. To see if Citrix Workspace app is successfully detected in the browser, check the **Current status** in your **Account Settings**.



Settings

Account

About

Log off

Advanced

Activate Citrix Receiver
Downloads a file that adds this workspace to your local Citrix Receiver app.

Change Citrix Receiver
Opens a page that checks for a local Citrix Receiver app.

Current status: Apps and desktops open in your local Citrix Receiver app.

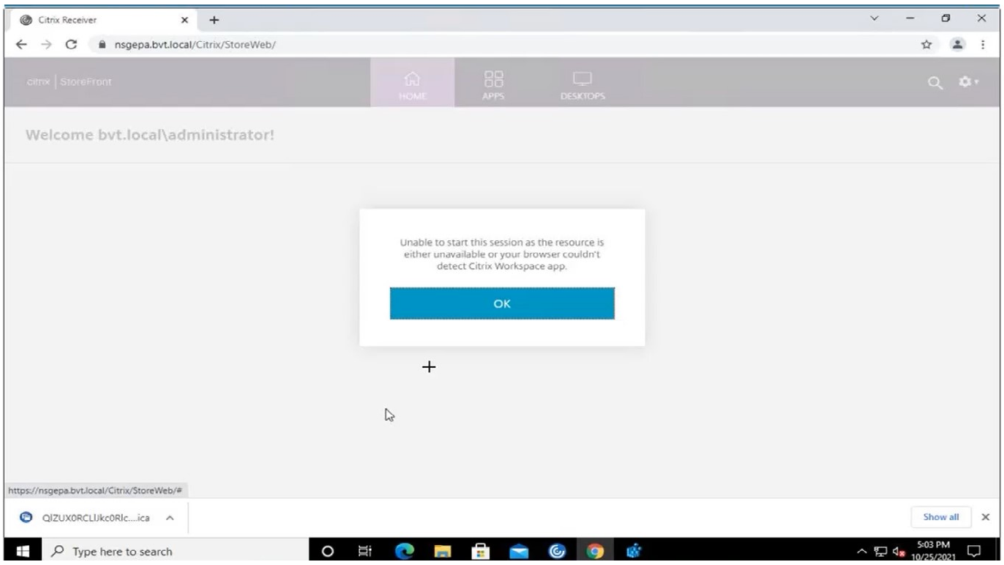
After Citrix Workspace app is detected, you can see and launch all the virtual apps and desktops that are enabled with App Protection.

Enable tracing on StoreFront

To enable tracing in StoreFront, see the StoreFront documentation. This trace can be used to verify whether the configured NetScaler Gateway session policy labels are passed down to the store properly.

Troubleshooting

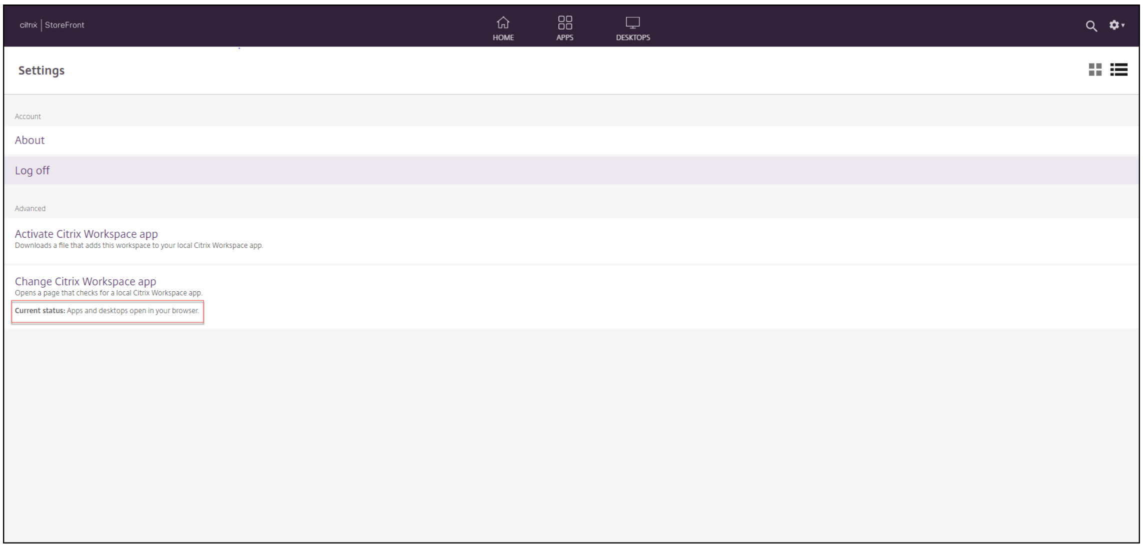
When you launch the App Protection enabled sessions, you might sometimes face the following error:



Unable to start this session as the resource is either unavailable or your browser couldn't detect Citrix Workspace app.

The possible reasons for this error are as follows:

- The apps and desktops are configured to open in a browser.

  Settings

  Account

  About

  Log off

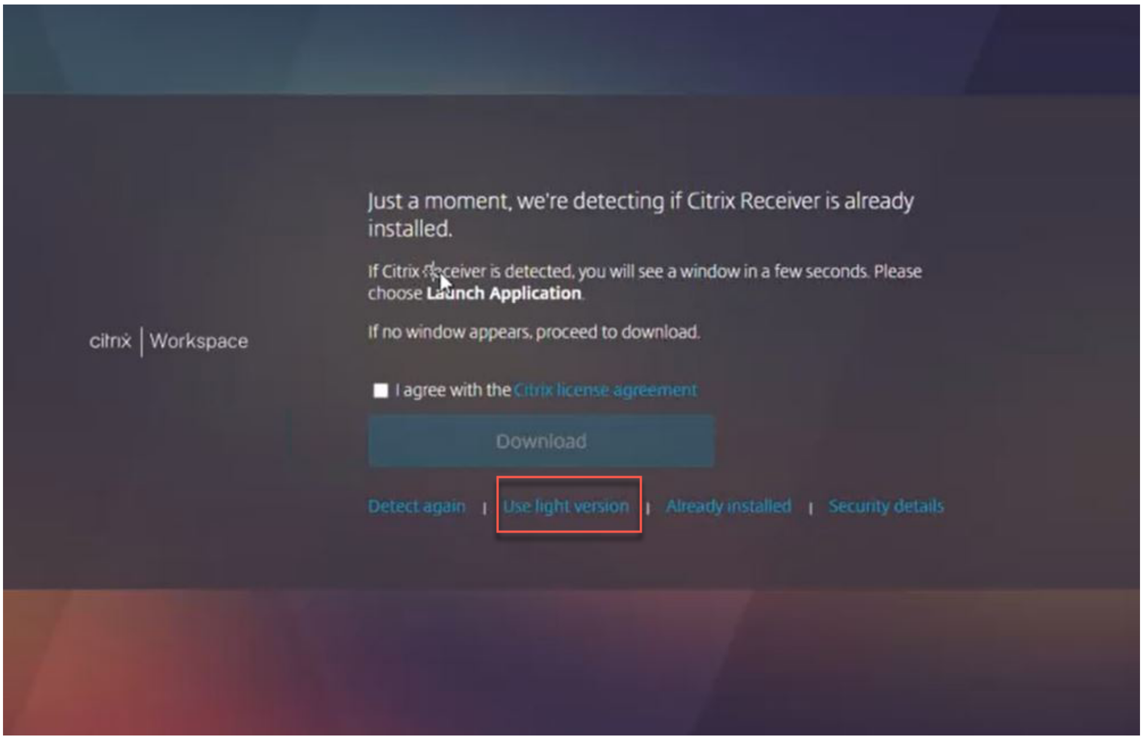
  Advanced

  Activate Citrix Workspace app
  Downloads a file that adds this workspace to your local Citrix Workspace app.

  Change Citrix Workspace app
  Opens a page that checks for a local Citrix Workspace app.

  Current status: Apps and desktops open in your browser.

  You face this scenario if you clicked **Use light version** during Citrix Workspace app detection as shown in the following screen:



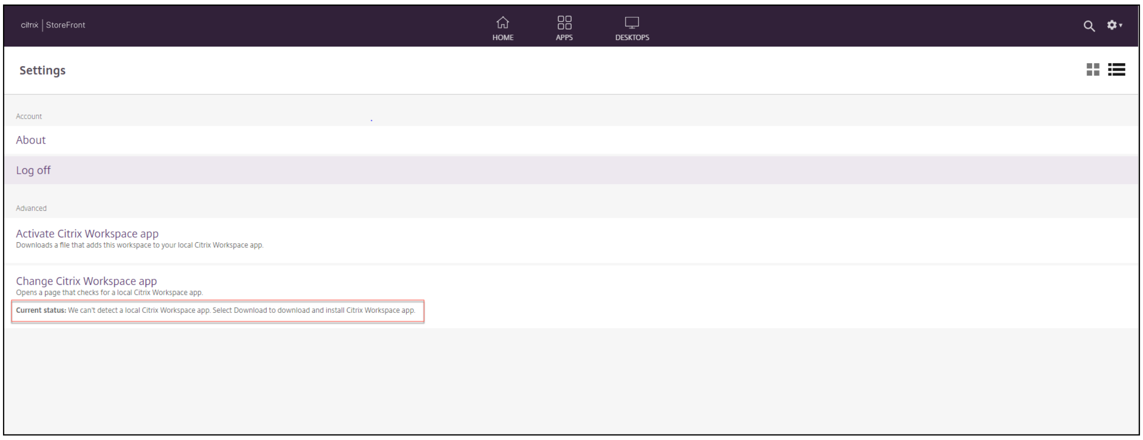
Just a moment, we're detecting if Citrix Receiver is already installed.

If Citrix Receiver is detected, you will see a window in a few seconds. Please choose **Launch Application**.

If no window appears, proceed to download.

citrix | Workspace
□ I agree with the Citrix license agreement
Download
Detect again | Use light version | Already installed | Security details

- The browser doesn’t detect Citrix Workspace app.

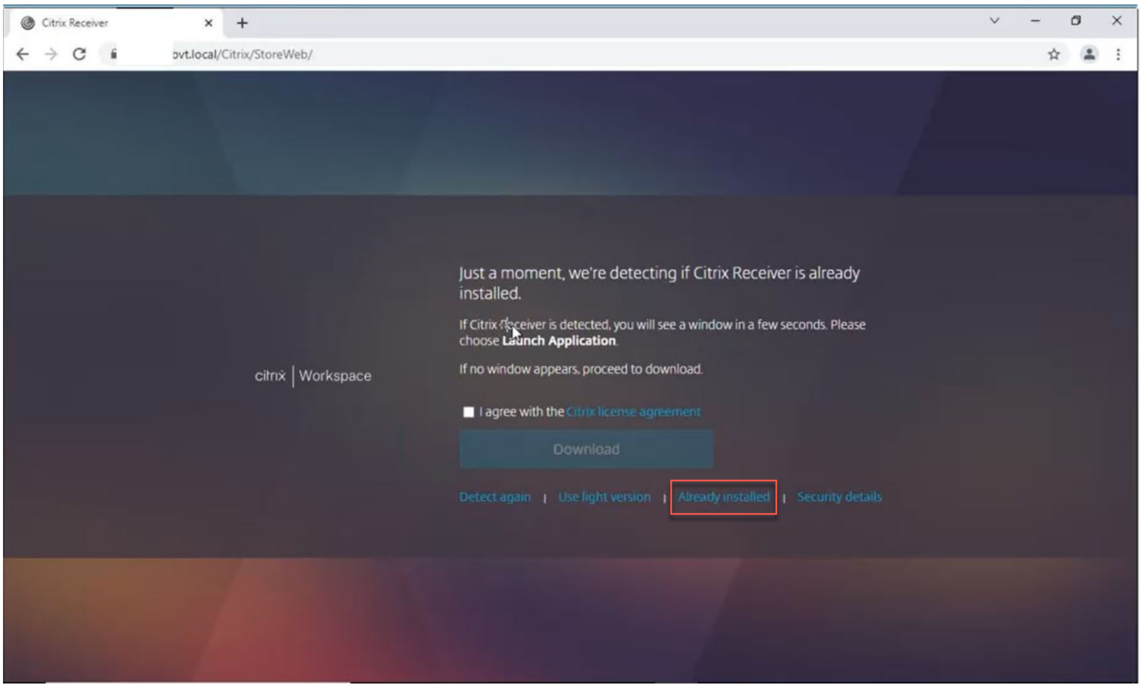


Activate Citrix Workspace app
Downloads a file that adds this workspace to your local Citrix Workspace app.

Change Citrix Workspace app
Opens a page that checks for a local Citrix Workspace app.

Current status: We can't detect a local Citrix Workspace app. Select Download to download and install Citrix Workspace app.

You face this scenario if you clicked **Already installed** during Citrix Workspace app detection as shown in the following screen:


Citrix Receiver
ovt.local/Citrix/StoreWeb/
citrix | Workspace

Just a moment, we're detecting if Citrix Receiver is already installed.

If Citrix Receiver is detected, you will see a window in a few seconds. Please choose **Launch Application**.

If no window appears, proceed to download.

□ I agree with the Citrix license agreement

Download
Detect again | Use light version | Already installed | Security details

Solution: To correct the preceding scenarios and launch the App Protection enabled sessions, click **Change Citrix Workspace app** in **Account Settings** and wait for Citrix Workspace app to be detected.

Optimization

Citrix Workspace app detection is mandatory to launch the App Protection enabled sessions. To avoid failures during hybrid launches for protected sessions, the StoreFront admins can use the `ApplyUICustomization` action of the `deploy-solution.ps1` command and hide the **Use light version** and **Already installed** options.

Citrix Workspace app release timelines

March 14, 2024

This release timeline illustrates the target release cadence and dates of Citrix Workspace app releases. Although exact dates might change, we want to help you plan ahead. We also want to make it easier for you to manage Citrix Workspace app deployments.

You can download new releases from the Citrix Workspace app Downloads page. Citrix Workspace app for Android, Citrix Workspace app for iOS, and Citrix Workspace app for Windows (Store) are also available for download from their respective app stores. If you have enabled Citrix Workspace Updates for Citrix Workspace app for Mac or Windows, you're notified to accept the download and install the update. Consider subscribing to our RSS feed to receive alerts when new releases become available.

For details about the features available in each Citrix Workspace app, see Citrix Workspace app feature matrix.

For lifecycle information, see Lifecycle Milestones for Citrix Workspace app.

Target release cadence

The following Citrix Workspace app platforms follow a quarterly release cadence:

- Linux
- Mac
- Windows

The following Citrix Workspace app platforms follow a six-week interval release cadence:

- ChromeOS
- HTML5

The following Citrix Workspace app platforms follow a biweekly release cadence:

- Android
- iOS

> **Note:**
>
> Citrix Workspace app for Windows and Citrix Workspace app for Mac, going forward will be having major and minor releases in a quarter. Minor releases will be denoted as '.10'and these releases will include minor enhancements around quality and performance improvements. The minor '.10'release isn't expected to have any major features.

Target release dates for desktop apps

Citrix Workspace app	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024	Jul 2024	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024
Windows		☑	-	☑	☒	-	☑	☒	-	☑	-
Windows LTSR	☒	☑	-	-	☒	-	-	☒	-	-	☒

Citrix Workspace app	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024	Jul 2024	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024
Mac	-	☑	-	☑	☒	-	☑	☒	-	☑	-
ChromeOS and HTML5	☑	-	☑	☑	☑	-	☑	☑	☑	-	☑
Linux	-	☑	-	☑	-	-	☑	-	-	☑	-

Note: The ☒ symbol denotes minor releases. The ☒ symbol denotes cumilative updates (CUs).

Target release dates for mobile and tablet apps

Citrix Workspace app for Android and Citrix Workspace app for iOS follow a biweekly release cadence.

> **Disclaimer:**
>
> The development, release, and timing described for our products remains at our sole discretion and is subject to change without notice or consultation. The data provided is for informational purposes only and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions or incorporated into any contract.

Citrix Workspace app feature matrix

March 7, 2024

Citrix Workspace app provides a gamut of features distributed across different platforms or operating systems. With this feature matrix, you can clearly understand the availability of the features across different platforms. In each section, along with the feature matrix, you can find the feature definition table that describes every feature in brief.

Citrix Workspace

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Citrix Virtual Apps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Virtual Desktops	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Secure Private Access	Yes	Yes	No	Yes	Yes	Yes	No	No
Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Yes	No	No	Yes	No	No	No	No
Web/SaaS apps with SSO	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Mobile Apps	No	No	No	No	Yes	Yes	No	No
App Personalization service	Yes	No	No	Yes	Yes	Yes	No	No

Feature	Definition
Citrix Virtual Apps	Access Citrix Virtual Apps through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.
Citrix Virtual Desktops	Access Citrix Virtual Desktops through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.
Citrix Secure Private Access	With the Citrix Secure Private Access IT admins can govern access to approved SaaS apps. Also, with a simplified single sign-on experience admins can protect the organization's network and end-user devices from malware and data leaks by filtering access to specific websites and website categories.
Citrix Enterprise Browser	Browser delivered with the Citrix Workspace app to access SaaS and Web Apps securely.
Web/SaaS apps with SSO	Access SaaS/Web Apps configured using Secure Workspace Access with SSO.
Citrix Mobile apps	Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.
Citrix Mobile App Upgrades	Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.
App Personalization service	Allows to have a personalized corporate experience. You can have a custom app name and a co-branded icon for your Citrix Workspace app across the app workflow.

Workspace Management

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Auto configure using DNS for email discovery	Yes	Yes	No	Yes	Yes	Yes	No	No
Centralized Management settings	Yes	Yes	Yes	No	No	No	No	Yes
Global App Config service (Workspace)	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Global App Config service (StoreFront)	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
App Store updates	No	No	No	No	Yes	Yes	No	No
Citrix Auto updates	Yes	Yes	No	Yes	No	No	No	No

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Client App Management	Yes	No	No	No	Not applicable	Not applicable	Not applicable	Not applicable

Feature	Definition
Auto configure using DNS for email discovery	Enable Citrix Workspace app to be configured via auto-discovered settings.
Centralized Management settings	App setting from a centralized service, for example, Google Chrome management or GPOs.
Global App Config service (Workspace)	The Global App Configuration service for Citrix Workspace allows a Citrix administrator to deliver Workspace service URLs and Citrix Workspace app settings through a centrally managed service.
Global App Config service (StoreFront)	The Global App Configuration service for Citrix StoreFront allows a Citrix administrator to deliver Citrix Workspace app settings through a centrally managed service.
App Store updates	Updates from vendor application store
Citrix Auto updates	Updates for Windows and Mac through Citrix Auto-upgrade functionality
Client App Management	Enables Citrix Workspace app to become a single client app that is required on the end point to install and manage agents such as Secure Access Agent and End Point Analysis (EPA) plug-in. With this feature, administrators can easily deploy and manage required agents from a single management console.

User interface

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Desktop Viewer/-Toolbar	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-tasking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Follow Me Sessions (Workspace Control)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Definition
Desktop Viewer/Toolbar	Enables in session control of session functions like sending Ctrl+Alt+Del via a toolbar.
Multi-tasking	Enables multiple apps and desktops to be used at the same time.
Follow Me Sessions (Workspace Control)	Allows users to move between devices and automatically connect to all of their sessions.

HDX Host Core

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Adaptive transport	Yes	Yes	Yes	Yes	Yes	Yes	No	No
HDX adaptive throughput	Yes	Yes	No	No	No	No	No	No
SDWAN support	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Session reliability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Auto-client Reconnect	Yes	Yes	Yes	Yes	No	Yes	No	No
Session sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-port ICA	Yes	Yes	Yes	No	No	No	No	No

Feature	Definition
Adaptive transport	Enables EDT transport for HDX for improved throughput independent of network conditions.
SDWAN support	Enables SDWAN acceleration for QoS, TCP, compression, and de-duplication.
Session reliability	Keeps sessions active and on the user's screen when network connectivity is interrupted.
Auto-client Reconnect	Prompts and reconnects the session on connection interruption.

Feature	Definition
Session Sharing	Enables the published app to run over the same connection as other published applications when already running on the same server.
Multi-port ICA	Allows support for multiple TCP ports for HDX traffic to improve the Quality of Service.

HDX IO / Devices / Printing

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Local printing	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Generic USB redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Client drive mapping / File transfer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TWAIN 2.0	Yes	No	No	No	No	No	No	No

Feature	Definition
Local printing	Enables users to print documents via shared or local printers.

Feature	Definition
Generic USB redirection	Enables use of USB devices inside the session. For example, keyboard, mouse, external webcam and so on.
Client drive mapping / File Transfer	Enables use of client drives inbuilt or attached for data storage.
TWAIN	Allows mapping client TWAIN devices, such as digital cameras or scanners.

HDX integration

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Local App Access	Yes	Yes	No	No	No	No	No	No
Multi-touch	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Mobility pack	Yes	Yes	No	No	Yes	Yes	Yes	Yes
HDX Insight	Yes	Yes	Yes	Yes	No	No	Yes	Yes
HDX Insight with NSAP VC	Yes	Yes	Yes	Yes	Yes *(3)*	Yes *(3)*	No	No
EUEM experience matrix	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Bi-directional content redirection	Yes	Yes	No	No	No	No	No	No
URL redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Browser content redirection	Yes	No	Yes	No	No	No	No	Yes
File open in Citrix Workspace app	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Location Based Services (Location available via API-description)	Yes	Yes	No	No	Yes	Yes	No	No

Feature	Definition
Local App Access	Access the local application on a client device inside the session.

Feature	Definition
Multi-touch	Enables 10 finger multi-touch control of Windows/Linux desktops and apps.
Mobility pack	Enables native device experience features (for example, auto popup keyboard and local device UI controls) and tablet-optimized desktops.
HDX insight	Provides visibility into the session startup/end times using ICA network performance metrics.
HDX insight with NSAP VC	Provide visibility into the session startup/ end time using the NetScaler App Experience or NSAP Virtual channel to get HDX insights.
EUEM experience matrix	Provides Citrix admins visibility into the logon duration metrics via the Citrix Virtual Desktop that was formerly known as XenDesktop 7 Director.
Bi-directional Content redirection	Enables client to host and host to client URL redirection.
URL redirection	Allows running of applications locally on the client.
Browser content redirection	Enables an entire webpage (a browser's viewport) to be redirected to the endpoint for local rendering, offloading the server.
File open in Citrix Workspace app	Allows opening a local file in Citrix Workspace app using a hosted application (Client to Server Content Redirection).
Location Based Services (Location available via API-description)	Enables location information to be used by applications delivered by Citrix Virtual Desktop earlier known as XenDesktop.

HDX multimedia

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Audio playback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bi-directional Audio (VoIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Webcam redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Video playback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Teams optimization	Yes	Yes	Yes (x64 only)	Yes	No	No	Yes	Yes
Skype for Business Optimization Pack	Yes	Yes	Yes	Yes	No	No	No	No

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Cisco Jabber unified communications optimization	Yes	Yes	Yes	No	No	No	No	No
Windows Multimedia redirection	Yes	Yes	Yes	No	No	No	No	No
UDP audio	Yes	Yes	Yes	No	No	No	No	No

Feature	Definition
Audio Playback	Enables server rendered audio playback.
Bi-directional audio (VoIP)	Enables use of hosted softphone / voice chat collaboration applications.
Webcam redirection	Enables use of video chat collaboration applications using a local webcam.
Video playback	Enable viewing of recorded videos.
Microsoft Teams optimization	Offloads Microsoft Teams media processing from the Citrix server to the user device.
Skype for Business optimization	Offloads Skype for Business media processing from the Citrix server to the user device. For Citrix Workspace app for Android, we support only on Chrome devices.

Feature	Definition
Cisco Jabber unified communications optimization	Offloads Jabber media processing from the Citrix server to the user device.
Windows Multimedia redirection	Enables Windows Multimedia to be rendered on the user device, offloading the server.
UDP audio	Support for audio input and output over UDP.

Security

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
TLS 1.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.0/1.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DTLS 1.0	Yes	Yes	Yes	Yes	Yes	Yes	No	No
DTLS 1.2	Yes	Yes	Yes	Yes	No	No	No	No
SHA2 Cert	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Smart Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote Access via Citrix Gateway	Yes *(1)*	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Workspace for Web Access	Yes	Yes	Yes	Yes	Via ICA file	Yes	Yes	Yes
IPV6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
App Protection	Yes	Yes	Yes	Yes	No	No	No	No

Feature	Definition
TLS 1.2	Successor to SSL, strong communication channel security.
TLS 1.0/1.1	Successor to SSL, strong communication channel security.
DTLS 1.0	DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.
DTLS 1.2	DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.
SHA2 Cert	Ability to use SHA2 certificates.
Smart access	Controls access to available apps by using Gateway policies and filters.
Remote access via Gateway	Provides users with secure access to enterprise apps, virtual desktops, and data anywhere without a VPN client.
Workspace for Web access	Access to hosted applications or virtual desktops using a browser.
IPV6	Enables use on IPV6 networks.

HDX graphics

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
H.264-enhanced Super-Codec	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Client hardware acceleration	Yes	Yes	Yes	Yes	No	Yes	No	No
3DPro graphics	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
External monitor support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Desktop composition redirection	Yes	Yes	No	No	No	No	No	No
True Multi-monitor	Yes	Yes	Yes	Yes	No	No	Yes	Yes

Feature	Definition
H.264-enhanced SuperCodec	Enables streamlined delivery of applications using XenApp/Desktop 7.X H264-enhanced Supercodec.
Client hardware acceleration	Enables hardware acceleration for HDX features like graphics, webcam. The use of hardware capability varies with different Citrix Workspace apps.
3DPro Graphics	Enables use of 3D professional graphics applications hosted in the data center.
External monitor support	Enables use of an external monitor.

Feature	Definition
Desktop composition redirection	Enables graphics command that is remote to the client for rendering to make sure server scalability. Deprecated in Receiver for Mac 12.9 version.
True Multi-monitor	XenApp or XenDesktop creates the same number of monitors as supported by the client.

Authentication

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Federated authentication (SAML/Azure AD)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ADC full VPN	Yes	Yes	Yes	Yes	No	No	No	No
RSA soft token	No	No	No	No	Yes	Yes	No	No
Challenge response SMS (Radius)	Yes	Yes	No	Yes	No	No	No	No

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
User Cert Auth via Gateway (via native Workspace app)	No	No	No	No	Yes	Yes	Yes	Yes
User Cert Auth via Gateway (via browser)	Yes *(4)*	Yes *(4)*	No	Yes	No	No	Yes	Yes
Smart card (CAC, PIV, and so on)	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Proximity/Contactless card	Yes	Yes	Yes	No	No	No	No	Yes
Credential insertion (for example, Fast Connect, Storebrowse)	Yes	Yes	Yes	No	No	No	No	Yes

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Pass through authentication	Yes	Yes	No	No	No	No	No	No
Save credentials *On-prem and only StoreFront	Yes	Yes	No	Yes	No	No	No	No
ADC nFactor authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ADC Native OTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Biometric authentication (Touch ID, Face ID)	No	No	No	No	Yes	No	No	No
Single sign-On to Citrix Mobile apps	No	No	No	No	Yes	Yes	No	No
Anonymous store access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Definition
Federated Authentication (SAML/Azure AD)	Enables the FAS server for the user authentication that delegates the Microsoft ADFS server (or other SAML-aware IdP) either by Azure AD or SAML.
ADC (NetScaler) Full VPN	Builds full VPN tunnel for Gateway.
RSA Soft Token	Enables simplified authentication when using RSA Soft Tokens.
Challenge Response SMS (Radius)	Enables a use of challenge response authentication for example the use of SMS pass codes.
User Cert Auth via Gateway (via browser only)	Enables use of users certificates as one factor for authentication with Gateway, which is for browser-based authentication on Windows and Linux.
Smart Card (CAC, PIV, and so on)	Enables use of a standard PC/SC compatible cryptographic smart card for authentication and signing.
Proximity/Contactless Card	Enables users to use Citrix apps or desktops by authenticating with proximity or contactless smart card.
Credential insertion (for example, Fast Connect, Storebrowse)	Enables users to use Citrix apps or desktops by authenticating with a proximity or contactless smart card. Storebrowse is a command-line utility tool available with Citrix Workspace app for Windows. You can use Storebrowse to customize Citrix Workspace app by scripting the Storebrowse utility.
Pass through authentication	Passes user credentials to a web interface site and then to the Citrix Virtual Apps and Desktops servers. This process prevents users to explicitly authenticate at any point during the Citrix app launch process.
Save credentials *On-prem and only StoreFront	Enables save credentials for on-prem and only using Citrix StoreFront.

Feature	Definition
Gateway native OTP	Gateway supports one-time passwords (OTPs) without having to use a third-party server, by keeping the entire configuration on the NetScaler appliance.
NetScaler nFactor authentication	nFactor authentication enables dynamic authentication flows based on the user profile. Sometimes, these flows can be simple flows to be intuitive to the user. The minimum version of NetScaler required is 12.1.49.x.
Biometric authentication (Touch ID, Face ID)	Enables Biometric authentications such as Touch ID and Face ID.
Single sign-on to Citrix Mobile apps	Enables single sign-on to Citrix Mobile apps.
Anonymous store access	Support access for unauthenticated (anonymous) users.

Input experience

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Keyboard layout sync - client to VDA (Windows VDA)	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Keyboard layout sync - client to VDA (Linux VDA)	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Keyboard layout sync - VDA to client (Windows VDA)	No	No	No	No	No	No	No	No
Keyboard layout sync - VDA to client (Linux VDA)	No	No	No	No	No	No	No	No
Unicode keyboard layout mapping	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Keyboard input mode - unicode	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Windows 2311.1 and Windows Store 2309.1	Windows 2203.1 LTSR	Linux 2402	Mac 2311	iOS 24.2.0	Android 24.3.0	HTML5 2312	ChromeOS 2402
Keyboard input mode - scancode	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Server IME	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Generic client IME (CTXIME) for CJK IMEs	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Command line interface	Yes	Yes	No	No	No	No	No	No
Keyboard sync setting UI and configurations	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Input mode setting UI and configurations	No	No	Yes	Yes	Yes	No	No	No

Language bar setting UI and configurations	Yes	Yes	No	Yes	No	No	No	No

Feature	Definition
Keyboard layout sync - client to VDA (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Windows VDA.
Keyboard layout sync - client to VDA (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Linux VDA.
Keyboard layout sync - VDA to client (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Windows VDA. The keyboard layout on the Windows VDA gets automatically set on the client device.
Keyboard layout sync - VDA to client (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Linux VDA. The keyboard layout on the Linux VDA gets automatically set on the client device.
Unicode keyboard layout mapping	Supports Unicode keyboard layout mapping for Windows VDA with non-Windows Citrix Workspace app.
Keyboard input mode - unicode	Unicode input mode sends the key from the client-side keyboard to VDA and VDA generates the same character in the VDA. Applies client-side keyboard layout.

Feature	Definition
Keyboard input mode - scancode	Scancode input mode sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
Server IME	Provides service (or VDA) side Input Method Editor (IME) usability and experience.
Generic client IME (CTXIME) for CJK IMEs	Provides enhanced Client IME usability and improved seamless experience for East Asian languages (Chinese, Japanese, Korean).
Command line interface	Users can enable or disable client IME using the command-line interfaces.
Keyboard sync setting UI and configurations	Users can choose different keyboard layout synchronization options using the GUI.
Input mode setting UI and configurations	Users can choose different keyboard input mode options using the GUI.
Language bar setting UI and configurations	Users can choose to show or hide the remote language bar in a VDA app session using the GUI. The language bar displays the preferred input language in a session.
Keyboard layout sync GPO administrative template	Administrators can override the keyboard layout synchronization configurations by deploying the corresponding policies from the Citrix Workspace app Group Policy Object administrative template.

Table indicators

Indicator	Description
1	StoreFront only
2	HDX 3D Pro reverts to JPEG for these Citrix Workspace apps. 3 Mbps is recommended compared to 1.5 Mbps with H.264 Deep Compression.

Indicator	Description
3	For NSAP VC, the Workspace app for iOS/Android supports, but for ADC/ADM, the support is still pending.
4	User Cert Auth via Gateway (via browser only) method of authentication doesn't support Citrix Workspace app client detection. You can open a virtual app or desktop using Citrix Workspace app only if the ICA file is downloaded.

> **Note:**
>
> The development, release, and timing of any features or functionality described for our products remains at our sole discretion. The information provided here is for informational purposes only and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions or incorporated into any contract. The development, release, and timing of any features or functionality described for our products remains at our sole discretion and are subject to change without notice or consultation.