Citrix Workspace app
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace app</td>
<td>3</td>
</tr>
<tr>
<td>Citrix Workspace web extensions</td>
<td>6</td>
</tr>
<tr>
<td>App Protection</td>
<td>8</td>
</tr>
<tr>
<td>System requirements and compatibility</td>
<td>17</td>
</tr>
<tr>
<td>App Protection features</td>
<td>20</td>
</tr>
<tr>
<td>Configure App Protection</td>
<td>26</td>
</tr>
<tr>
<td>Configure Anti-keylogging and Anti-screen capture</td>
<td>33</td>
</tr>
<tr>
<td>Configure Anti-DLL Injection</td>
<td>42</td>
</tr>
<tr>
<td>Configure Policy Tampering Detection</td>
<td>48</td>
</tr>
<tr>
<td>Configure App Protection Posture Check</td>
<td>49</td>
</tr>
<tr>
<td>Block DoubleHop Launch</td>
<td>57</td>
</tr>
<tr>
<td>Troubleshoot</td>
<td>57</td>
</tr>
<tr>
<td>Contextual App Protection for Workspace</td>
<td>67</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>68</td>
</tr>
<tr>
<td>Scenario 1</td>
<td>68</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>73</td>
</tr>
<tr>
<td>Scenario 3</td>
<td>81</td>
</tr>
<tr>
<td>Scenario 4</td>
<td>83</td>
</tr>
<tr>
<td>Contextual App Protection for StoreFront</td>
<td>85</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>87</td>
</tr>
<tr>
<td>Scenario 1</td>
<td>87</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>91</td>
</tr>
<tr>
<td>Scenario 3</td>
<td>93</td>
</tr>
</tbody>
</table>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
Citrix Workspace app

Scenario 4 94
Scenario 5 97
App Protection support for hybrid launch through Workspace 97
App Protection support for hybrid launch through StoreFront 101
Citrix Workspace app release timelines 109
Citrix Workspace app feature matrix 111
Citrix Workspace app

January 23, 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

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

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.

<table>
<thead>
<tr>
<th>Language</th>
<th>Android</th>
<th>ChromeOS HTML5</th>
<th>iOS</th>
<th>Linux</th>
<th>macOS</th>
<th>Windows</th>
<th>Windows Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Danish</td>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dutch</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>French</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>German</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Italian</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Japanese</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Korean</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Portuguese(Brazil)</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Russian</td>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>App</th>
<th>Feature flag support</th>
<th>Version</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace app for Android</td>
<td>Yes</td>
<td>10.7.5</td>
<td>Feature flag management for Citrix Workspace app for Android</td>
</tr>
<tr>
<td>Citrix Workspace app for ChromeOS</td>
<td>Yes</td>
<td>1908</td>
<td>Feature flag management for Citrix Workspace app for ChromeOS</td>
</tr>
<tr>
<td>Citrix Workspace app for HTML5</td>
<td>Yes</td>
<td>1908</td>
<td>Feature flag management for Citrix Workspace app for HTML5</td>
</tr>
<tr>
<td>App</td>
<td>Feature flag support</td>
<td>Version</td>
<td>Documentation</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------</td>
<td>---------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Citrix Workspace app for iOS</td>
<td>Yes</td>
<td>10.4.10</td>
<td>Feature flag management for Citrix Workspace app for iOS</td>
</tr>
<tr>
<td>Citrix Workspace app for Linux</td>
<td>Yes</td>
<td>2109</td>
<td>Feature flag management for Citrix Workspace app for Linux</td>
</tr>
<tr>
<td>Citrix Workspace app for Mac</td>
<td>Yes</td>
<td>2010</td>
<td>Feature flag management for Citrix Workspace app for Mac</td>
</tr>
<tr>
<td>Citrix Workspace app for Windows</td>
<td>Yes</td>
<td>2012</td>
<td>Feature flag management for Citrix Workspace app for Windows</td>
</tr>
</tbody>
</table>

**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**

December 27, 2023

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
Citrix Workspace app

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 required.

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 is not 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.

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

Citrix Workspace app feature matrix

Citrix Workspace app provides 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:

<table>
<thead>
<tr>
<th>Browser name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest version</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Latest version</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>Latest version</td>
</tr>
</tbody>
</table>

App Protection

December 27, 2023

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 is not 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 purchasing this feature, ensure 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 can emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

Citrix App Protection policies work effectively with underlying operating system components, including ICA files. Citrix would not be able to 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 prior to 2311:
From Citrix Workspace app version 2311 onwards:

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

```sql
sc query appprotectionsvc
<!--NeedCopy-->```
Citrix Workspace app

For Citrix Workspace app versions prior to 2206, run the following command:

```
1. sc query appprotectionsvc
```

Note:

In Citrix Workspace app versions prior to 2212, if you hadn’t selected 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:

```
[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
Citrix Workspace app

SaaS apps. You can access these resources using a supported native Citrix Workspace app client or a web browser. App Protection performs variedly 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

- 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

- 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 won’t be able to 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 may be impacted 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

December 27, 2023

System requirements

As a prerequisite, ensure 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 won’t be able to access the protected resources. The protected resources include Virtual
Citrix Workspace app

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. Therefore, 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 18.04 and Ubuntu 20.04
- 64-bit Debian 9 and Debian 10
- 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:**

For App Protection, Citrix Workspace app for Linux requires 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:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix Cloud</th>
<th>Citrix Cloud Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-keylogging and Anti-screen capture for virtual apps and desktops</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-keylogging and Anti-screen capture for web or SaaS apps</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Anti-DLL for Windows</td>
<td>Yes</td>
<td>Yes through Group Policy Object (GPO)</td>
</tr>
<tr>
<td>Anti-DLL Allow Listing</td>
<td>Yes</td>
<td>Yes through GPO</td>
</tr>
<tr>
<td>Global App Configuration service (GACS)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Authentication or Self-Service plug-in screens protection for Linux</td>
<td>Yes</td>
<td>Yes through AuthManConfig.xml</td>
</tr>
</tbody>
</table>
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/OS level. A keylogger installed on the client endpoint, reading the data from the OS/driver, would capture hashed text instead of the keystrokes 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:
Anti-screen capture

Anti-screen capture prevents an app from attempting to take a screenshot of or a recording of the screen within a virtual app or desktop session. The screen capture software won’t be able to detect content within the capture region. The area selected by the app is grayed 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 ensures that sensitive data is not accidentally leaked from the organization. This 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 is not 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 attempt screen capture.
- 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.

The enhancement displays a notification when an untrusted or malicious DLL is blocked. Closing the message exits the virtual app and desktop session.
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, Desktop share option is disabled by default. To enable it, add UseGbufferScreenSharing parameter in your config.json file as follows:
Optimized Microsoft Teams enabled with App Protection also supports 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 will be terminated.

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

To configure Policy Tampering Detection, see Configure Policy tampering detection.
Citrix Workspace app

**Posture Check**

To detect and block launching virtual apps and desktops enabled with App Protection policies from Citrix Workspace app versions that do not support 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 will be 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 enabled with App Protection policies in a double hop scenario however the App Protection features were not applied.

Starting from Citrix Workspace app for Windows 2309 release, 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 performed and take actions 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 named **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

Configure App Protection

December 29, 2023

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:
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:

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

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.
Citrix Workspace app

- 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]:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
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:

```
1 export DEBIAN_FRONTEND="noninteractive"
2 sudo debconf-set-selections <<< "icaclient app_protection/install_app_protection select yes"
3 sudo debconf-show icaclient
4 * app_protection/install_app_protection: yes
5
6 sudo apt install -f ./icaclient_<version>_amd64.deb
7 <!--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**

December 29, 2023

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:

<table>
<thead>
<tr>
<th>Configuration method</th>
<th>Citrix workspace app for Linux</th>
<th>Citrix workspace app for Mac</th>
<th>Citrix workspace app for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Group Policy Object</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Using Global App Configuration service</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Using AuthManConfig.xml</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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 releases, 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 Citrix Workspace app for Mac 2311 release, you can configure App Protection for Authentication and Self-Service plug-in using 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 release, 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**.

   ![Workspace Configuration](image)

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

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

**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:**
Citrix Workspace app

“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 authentication manager

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

```
/opt/Citrix/ICAClient/configAuthManConfig.xml | grep -i authmananti -A 1
<key>AuthManAntiScreenCaptureEnabled</key>
<value>true</value>
```
Citrix Workspace app

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

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

```bash
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i protection -A 4
<selfservice>
  <antiscreencaptureenabled>true</antiscreencaptureenabled>
  <antikeyloggingenabled>true</antikeyloggingenabled>
</selfservice>
```

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

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

In addition, enable XML trust:

Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true

Ensure 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

December 27, 2023

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 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**.

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.
4. Click OK.

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

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.
Citrix Workspace app

Sample format to add DLL to the allow list:

```
1 [ 
2   { 
3     "filePath":"C:\Program Files (x86)\trusted\messagebox.dll"
4   }, 
5     { 
6       "filePath": "%PROGRAMFILES%\trusted\logging.dll"
7     }
8 ] 
9 <!--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.

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:

```
1 { 
2   "serviceURL": { 
3     "url": "https://tuleshtest.cloudburrito.com:443" 
4   }, 
5   "settings": { 
6     "appSettings": { 
7       "windows": [ 
8         { 
9           "category": "App Protection", 
10           "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",
"useFor AppConfig": true
}
Configure Policy Tampering Detection

December 27, 2023

Prerequisites

To configure Policy Tampering Detection feature, ensure 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 App Protection Service on the TS/WSVDAs which are hosting the virtual apps and desktops configured with App Protection.

Perform 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:

     
     ```
     1 sc config ctxappprotectionsvc start=auto
     2 sc start ctxappprotectionsvc
     3 <!--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 App Protection Service and then click Start.
  3. Right-click Citrix App Protection Service and then select Properties.
  4. Select General > Startup type > Automatic and then click OK to ensure 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

December 27, 2023

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

### Prerequisites

Ensure 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 via Citrix Studio and you can use the same procedure for Web Studio also.

1. Open the Citrix Studio app on 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.
The **Edit Setting** window appears.

5. Clear the **Use default value** checkbox.

6. Click **Add** and enter the relevant values from the following:

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

For example, if you’ve added “Windows-AntiScreeencapture” and “Windows-AntiKeylogging”, then the Citrix Workspace app for Windows that supports Posture Check and has these capabilities are allowed to connect to the VDA.
Note:

- Each entry must have only one capability.
- No space is allowed in the name of capability.
- Ensure 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- will be ignored.

7. After adding all the required values, click **OK**.

8. Click **Next**.

9. Select **Assign Policy to > Selected users and machine objects**.
10. Select the required delivery groups where this policy must be deployed and then click **OK**.
11. Click **Next**.

12. Enter the policy name in the **Policy name** field and then select the **Enable policy** checkbox.
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 Posture Check feature, then the session is terminated without displaying any error message.
- If you’re using Citrix Workspace app version that supports Posture Check feature, then the session is terminated displaying the following error messages respectively:
  - Windows:
Session is terminated as the App Protection posture check failed. Contact your system administrator.

- Mac

- Linux
**Block DoubleHop Launch**

December 27, 2023

To block double hop launch, ensure that you’re running Citrix Workspace app for Windows 2309 or later on the first hop and 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:**

If you’re running Windows server OS on the first hop, then the virtual apps and desktops enabled with App Protection aren’t displayed since App Protection isn’t supported on Windows Server OS.

**Troubleshoot**

December 29, 2023

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

**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 Citrix Workspace app for Windows version earlier to 2311, then run the following commands:
     - `sc query appprotectionsvc`
If you are using Citrix Workspace app for Windows version 2311 or later, then run the following commands:

- `sc q entryprotectdrv`
- `sc q epinject6`
- `sc q epusbfilter`

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 is an optional step, and ensures that only 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 mentioned in the Log output Path of the set log.
Generic troubleshooting

Applications are not enumerating or not starting:
Ensure the following:

• You’re using a supported version of the Citrix Workspace app.
• The Delivery Group has the proper features enabled.

App Protection policies are not applying properly:
Ensure the following:

• 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.

**Screenshots not working on non-Citrix windows:**

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

**Troubleshoot Policy Tampering Detection**

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 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

![Image of Citrix Workspace app terminated message](image)

- Citrix Workspace app for Mac
Citrix Workspace app for Windows

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 `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. In the client, do the following:

   a) Check if the `vdapp.p.dll` file is located 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 `vdapp.p.dll` file is loaded in `wfica32.exe`.

   c) For Citrix Workspace app for Linux, check if the `vdapp.p.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 could be because the App Protection service is not 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 is not 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

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 apps 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 apps 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:

1. In the Virtual Delivery Agent, do the following:
Citrix Workspace app

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

```bash
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:

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

ii. Start the service by running the following command:

```bash
sc start ctxappprotectionsvc
```

2. Check if the Posture Check values that you have entered has 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, 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 has 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**

- 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/ICA/Client/util/setlog.
  2. (Optional) Click Set All Disabled and ensure that only 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 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 is not 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 mentioned in the log output Path of the set log.
• To collect logs for the Virtual Delivery Agent, do the following steps:

1. To get traces from App Protection service through CDF control, select all the modules.
2. In certain cases, we might need to capture cdf traces from a different machine. To collect cdf traces, see CTX237216.

**Contextual App Protection for Workspace**

December 27, 2023

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 contains 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:
Citrix Workspace app

- **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**

December 27, 2023

Ensure that you have the following:

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

**Scenario 1**

December 27, 2023

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

2. Configure adaptive access based on your network location,
a) Sign in to Citrix Cloud and navigate to Network Locations.

b) Click Add Network location.

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


   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.
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
```
In the screenshot, you see two policies:

- **App Protection_AG - AllowedConnections** with *ViaAG*, which represents the policy for connections via the access gateway
- **App Protection_Direct - AllowedConnections** with *NotViaAG*, which represents the policy for connections 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"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequired $false


- 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

December 27, 2023

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

There are multiple 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.


2. Create Authentication policy with 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.

   ![Configuration Tab](image)

   b) Navigate to Authentication Policies > Add Binding.
c) Click **Add** to create a policy.

   ![Authentication Policy](image)

   ![Authentication Policy](image)

   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.
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**.
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**.

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.
b) Click **Add Binding**.

![Add Binding screen](image1)

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

![Policy Binding screen](image2)

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

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**.

You return to the **Policy Binding** screen.
g) Select the **Goto Expression** as *End* and Click **Bind**.

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 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.
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:

```
```

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 -IncludedSmartAccessTags 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 App Protection policies are applied.

**Scenario 3**

December 27, 2023

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.
   c) Click Create device policy.
      Create devicy policy page appears.
   d) Under Policy rules, click on the Select Rule dropdown menu and select Citrix Workspace app Version.
   e) Click Select a rule dropdown 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 Enable when created check box to enable the policy since you created it.
   k) Click Create.

2. Configure the Broker Access policy rules:
a) Install Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.


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.

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 -IncludedSmartAccessWorkspace:COMPLIANT
```

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

```
Citrix Workspace app

```powershell
$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 compliant with the device policy. You see that the App Protection policies are applied.

**Scenario 4**

December 27, 2023

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


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

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

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

```powershell
New-BrokerAccessPolicyRule "Example Rule Name_1" -DesktopGroupUid 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilterEnabled $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:

```powershell
```

3. Verification:

Sign out of Citrix Workspace app, if already open. Sign in to Citrix Workspace app as a user in 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 Product Managers Active Directory user group. Launch the protected resource and you’ll see that App Protection is enabled.

**Contextual App Protection for StoreFront**

December 27, 2023

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 contains 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 additional 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 scenarios below 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
```
Prerequisites

To enable Contextual App Protection for StoreFront, ensure 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:

   ```powershell
   1 asnp Citrix*
   2 Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   3 <--NeedCopy-->
   ```

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

   ```powershell
   1 Import-ConfigFeatureTable <path to the downloaded feature table>
   2 <--NeedCopy-->
   ```

   For example,

   ```powershell
   1 Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.AppProtContextualAccess.xml
   2 <--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

Ensure 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 required till Citrix Virtual Apps and Desktops version 2006 release
- Contextual App Protection feature table import required till Citrix Virtual Apps and Desktops version 2209 release
- 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

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

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 toCitrix Gateway > Virtual Servers.
      Note the VPN Virtual Server name, which is needed to configure the Broker Access Policy later on.
   c) ClickVPN Virtual Server. Scroll to the bottom of the page and clickSession policies. A list of session policies appears.
d) Click **Add Binding**.

![VPN Virtual Server Session Policy Binding]

```
PRIORITY  POLICY NAME  EXPRESSION                        PROFILE
      100  PL_05,172.30.200.111  HTTPREQ.HEADER("User-Agent") CONTAINS("CitrixReceiver")  AC_05,172.30.200.111
      130  workspace            HTTPREQ.HEADER("User-Agent") CONTAINS("CitrixReceiver") workspace
      140  chrome_iPhone        HTTPREQ.HEADER("User-Agent") CONTAINS("iPhone") chrome_iPhone
      150  temp                 HTTPREQ.HEADER("User-Agent") CONTAINS("iPhone") temp
```

**Close**

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

![VPN Virtual Server Session Policy Binding]

```
Policy Binding
Select Policy:

Search:
Click to select
Add Edit

Please select value.

Priority
160
```

**Bind Close**

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

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

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

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

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
2 ``
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):

```
2. <!--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:

```
2. <!--NeedCopy-->  
```

**Uid_of_desktopGroup** is the DesktopGroupUID of the delivery group got by running the GetBrokerAccessPolicyRule 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:

```
1. Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -IncludedSmartAccessTags Primary_HDX_Proxy:temp -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequired $false  
2. <!--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:

```
1. Set-BrokerAccessPolicyRule Win10Desktop_AG -
   AppProtectionScreenCaptureRequired $true -
   AppProtectionKeyLoggingRequired $true
2. <!--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 access gateway connection. You can see the required resources in the StoreFront and App Protection has to be disabled.

### Scenario 2

December 27, 2023

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.

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:

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

In this scenario, the Smart Access policy is cwa.
b) Create another Smart Access policy to filter the connections that aren’t started from the Citrix Workspace app, \texttt{HTTP.REQ.HEADER(“User-Agent”).CONTAINS(“CitrixReceiver”).NOT}. In this case, this Smart Access policy is \textit{browser}.

2. Create Broker Access policy rules:

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

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

```powershell
2 <!--NeedCopy--> 
```

\texttt{Uid_of_desktopGroup} is the DesktopGroupUID of the delivery group got by running the \texttt{GetBrokerAccessPolicyRule} 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 \texttt{cwa}:

```powershell
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -IncludedSmartAccessTags Primary_HDX_Proxy:cwa -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequired $true
2 <!--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:

```powershell
1 Set-BrokerAccessPolicyRule Win10Desktop_AG -
   IncludedSmartAccessTags Primary_HDX_Proxy:browser -
   AppProtectionScreenCaptureRequired $false -
   AppProtectionKeyLoggingRequired $false
2 <!--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 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

December 27, 2023

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*:

```powershell
1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
   DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG -
   AllowedProtocols HDX, RDP -AllowedUsers Filtered -
   AllowRestart $true -Enabled $true
2 <!--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:

```powershell
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -AllowedUsers Filtered -IncludedUsers xd.local\sales -IncludedUserFilterEnabled $true -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequired $false
```

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:

```powershell
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers Anyauthenticated -ExcludedUserFilterEnabled $true -ExcludedUsers xd.local\sales -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequired $true
```

5. Verification

Sign out of the Citrix Workspace app, if already open. Sign in to the Citrix Workspace app as a user in 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**

December 27, 2023

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:**

Ensure 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**.

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:

```
1 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:

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

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":

   ```
   1 Set-BrokerAccessPolicyRule "Contextual App Protection Delivery Group_AG" -IncludedSmartAccessFilterEnabled $true - IncludedSmartAccessTags EPA_GW:Trusted-Device-PC - AppProtectionScreenCaptureRequired $false
   2 <!--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":

   ```
   2 <!--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**

December 27, 2023

Hybrid launches of Citrix Virtual Apps and Desktops is when you sign in to Citrix Workspace for Web, by typing in 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 reside within the browser. This 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**

- Ensure that you’re on a browser that supports the Citrix Workspace Web extension.
- Ensure that the DNS suffix of your Workspace URL is cloud.com. Currently, custom domains are not supported.
- Ensure 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
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’ll see it in the extensions section of your browser.

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.
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.

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 get one of the following errors when the launch preference is **Web Browser**. Change the launch preference to **Use Citrix Workspace app** to resolve this. For more information, see this support article.
App Protection support for hybrid launch through StoreFront

December 27, 2023

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 Citrix Workspace store and the HDX engine reside within the browser. This 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.
Citrix Workspace app

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 native Citrix Workspace app is successfully detected by the browser. 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 Citrix Workspace app version when you sign in to the website for the first time. If you subsequently install a different version of Citrix Workspace app, then StoreFront won’t be 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 enabling of hybrid launch of virtual apps and desktops 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
Citrix Workspace app

- 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:

  ![Deploy command screenshot](image)

  - 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 ensures that you bypass the blocked or unsupported scenarios.
Citrix Workspace app

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

  - **StoreName**: 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 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 `IISINET-Pub\Citrix<store name>\bin` directory
Citrix Workspace app

- `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:

   1. `sc stop IISADMIN`
   2. `sc stop CitrixSubscriptionsStore`
   3. <!--NeedCopy-->

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

   1. `sc start IISADMIN`
   2. `sc start CitrixSubscriptionsStore`
   3. <!--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**.
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:
The possible reasons for this error are as follows:

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

You face this scenario if you clicked **Use light version** during Citrix Workspace app detection as shown in the following screen:
• **The browser doesn’t detect Citrix Workspace app.**

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

December 27, 2023

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 two-week release cadence:

- Android
- ChromeOS
- HTML5
- iOS

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

- Linux
- Mac
- Windows

**Target release dates**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>iOS</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>ChromeOS</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>HTML5</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Linux</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Mac</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Windows</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>
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

February 1, 2024

Citrix Workspace app provides 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix virtual apps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix virtual desktops</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Citrix Secure Private Access | Yes       | Yes                 | No         | Yes      | Yes        | Yes            | Yes        | No           | No
### Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Enterprise Browser (formerly Citrix Workspace Browser)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Web/SaaS apps with SSO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Mobile Apps App Personalization service</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix virtual apps</td>
<td>Access Citrix virtual apps through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.</td>
</tr>
<tr>
<td>Citrix virtual desktops</td>
<td>Access Citrix virtual desktops through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Secure Private Access</td>
<td>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.</td>
</tr>
<tr>
<td>Citrix Enterprise Browser</td>
<td>Browser delivered with the Citrix Workspace app to access SaaS and Web Apps securely.</td>
</tr>
<tr>
<td>Web/SaaS apps with SSO</td>
<td>Access SaaS/Web Apps configured using Secure Workspace Access with SSO.</td>
</tr>
<tr>
<td>Citrix Mobile apps</td>
<td>Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.</td>
</tr>
<tr>
<td>Citrix Mobile App Upgrades</td>
<td>Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.</td>
</tr>
<tr>
<td>App Personalization service</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Workspace Management

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto configure using DNS for email discovery</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Centralized Management settings</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Global App Config service (Workspace)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Global App Config service (Store-Front)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>App Store updates</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Citrix Auto updates</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
<th>Client App Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto configure using DNS for email discovery</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>Centralized Management settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global App Config service (Workspace)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global App Config service (StoreFront)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Store updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix Auto updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client App Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

__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 endpoint 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Viewer/Toolbar</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-tasking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Follow Me Sessions (Workspace Control)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Feature Definition

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

HDX Host Core
## Feature Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive transport</td>
<td>Enables EDT transport for HDX for improved throughput independent of network conditions.</td>
</tr>
<tr>
<td>SDWAN support</td>
<td>Enables SDWAN acceleration for QoS, TCP, compression, and de-duplication.</td>
</tr>
<tr>
<td>Session reliability</td>
<td>Keeps sessions active and on the user’s screen when network connectivity is interrupted.</td>
</tr>
<tr>
<td>Auto-client Reconnect</td>
<td>Prompts and reconnects the session on connection interruption.</td>
</tr>
</tbody>
</table>
Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Sharing</td>
<td>Enables the published app to run over the same connection as other published applications when already running on the same server.</td>
</tr>
<tr>
<td>Multi-port ICA</td>
<td>Allows support for multiple TCP ports for HDX traffic to improve the quality of service.</td>
</tr>
</tbody>
</table>

**HDX IO / Devices / Printing**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local printing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Generic USB redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client drive mapping/File transfer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TWAIN 2.0</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local printing</td>
<td>Enables users to print documents via shared or local printers.</td>
</tr>
</tbody>
</table>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
## Citrix Workspace app

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

### HDX integration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311</th>
<th>Windows 2309.1</th>
<th>Windows 2203.1</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local App Access</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Multi-touch Mobility pack</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HDX Insight with NSAP VC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (3)</td>
<td>Yes (3)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EUEM experience matrix</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bi-directional content redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>URL redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Browser content redirection</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>File open in Citrix Workspace app</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Location Based Services (Location available via API description)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Feature Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local App Access</td>
<td>Access the local application on a client device inside the session.</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

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

### HDX multimedia

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio playback</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bi-directional Audio (VoIP)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Webcam redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video playback</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Teams optimization</td>
<td>Yes (x64 only)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Skype for Business</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Jabber unified communications optimization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows Multimedia redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UDP audio</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Jabber unified communications optimization</td>
<td>Offloads Jabber media processing from the Citrix server to the user device.</td>
</tr>
<tr>
<td>Windows Multimedia redirection</td>
<td>Enables Windows Multimedia to be rendered on the user device, offloading the server.</td>
</tr>
<tr>
<td>UDP audio</td>
<td>Support for audio input and output over UDP.</td>
</tr>
</tbody>
</table>

### Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TLS 1.0/1.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DTLS 1.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DTLS 1.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SHA2 Cert</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Access via Citrix Gateway</td>
<td>Yes (1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Via ICA file</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Workspace for Web Access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPV6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>App Protection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Feature Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.2</td>
<td>Successor to SSL, strong communication channel security.</td>
</tr>
<tr>
<td>TLS 1.0/1.1</td>
<td>Successor to SSL, strong communication channel security.</td>
</tr>
<tr>
<td>DTLS 1.0</td>
<td>DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.</td>
</tr>
<tr>
<td>DTLS 1.2</td>
<td>DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.</td>
</tr>
<tr>
<td>SHA2 Cert</td>
<td>Ability to use SHA2 certificates.</td>
</tr>
<tr>
<td>Smart access</td>
<td>Controls access to available apps by using Gateway policies and filters.</td>
</tr>
<tr>
<td>Remote access via Gateway</td>
<td>Provides users with secure access to enterprise apps, virtual desktops, and data anywhere without a VPN client.</td>
</tr>
<tr>
<td>Workspace for Web access</td>
<td>Access to hosted applications or virtual desktops using a browser.</td>
</tr>
<tr>
<td>IPV6</td>
<td>Enables use on IPV6 networks.</td>
</tr>
</tbody>
</table>

### HDX graphics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.264-enhanced Super-Codec</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client hardware acceleration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3DPro graphics</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External monitor support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Desktop composition redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>True Multi-monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Feature Definition

- **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.
## Citrix Workspace app

### Feature Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop composition redirection</td>
<td>Enables graphics command that is remote to client for rendering to ensure server scalability. Deprecated in Receiver for Mac 12.9 release.</td>
</tr>
<tr>
<td>True Multi-monitor</td>
<td>XenApp or XenDesktop creates the same number of monitors as supported by the client.</td>
</tr>
</tbody>
</table>

### Authentication

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311</th>
<th>Windows 2203.1</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated authentication (SAM-L/Azure AD)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ADC full VPN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RSA soft token</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Challenge response SMS (Radius)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Cert Auth via Gateway (via native Workspace app)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Cert Auth via Gateway (via browser)</td>
<td>Yes (4)</td>
<td>Yes (4)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart card (CAC, PIV, etc.)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Proximity/Contactless Credential</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Pass through authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save credentials <em>On-prem and only Store-Front</em></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ADC nFactor authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ADC Native OTP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Biometric authentication (Touch ID, Face ID)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Single sign-On to Citrix Mobile apps</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Anonymous store access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Authentication (SAML/Azure AD)</td>
<td>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.</td>
</tr>
<tr>
<td>ADC (NetScaler) Full VPN</td>
<td>Builds full VPN tunnel for Gateway.</td>
</tr>
<tr>
<td>RSA Soft Token</td>
<td>Enables simplified authentication when using RSA Soft Tokens.</td>
</tr>
<tr>
<td>Challenge Response SMS (Radius)</td>
<td>Enables a use of challenge response authentication for example the use of SMS pass codes.</td>
</tr>
<tr>
<td>User Cert Auth via Gateway (via browser only)</td>
<td>Enables use of users certificates as one factor for authentication with Gateway, which is for browser-based authentication on Windows and Linux.</td>
</tr>
<tr>
<td>Smart Card (CAC, PIV, etc.)</td>
<td>Enables use of standard PC/SC compatible cryptographic smart card for authentication and signing.</td>
</tr>
<tr>
<td>Proximity/Contactless Card</td>
<td>Enables users to use Citrix apps or desktops by authenticating with proximity or contactless smart card.</td>
</tr>
<tr>
<td>Credential insertion (for example, Fast Connect, Storebrowse)</td>
<td>Enables users to use Citrix apps or desktops by authenticating with 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.</td>
</tr>
<tr>
<td>Pass through authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Save credentials *On-prem and only StoreFront</td>
<td>Enables save credentials for on-prem and only using Citrix storefront.</td>
</tr>
</tbody>
</table>
Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway native OTP</td>
<td>Gateway supports one-time passwords (OTPs) without having to use a third-party server, by keeping the entire configuration on the NetScaler appliance.</td>
</tr>
<tr>
<td>NetScaler nFactor authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Biometric authentication (Touch ID, Face ID)</td>
<td>Enables Biometric authentications such as Touch ID and Face ID.</td>
</tr>
<tr>
<td>Single sign-on to Citrix Mobile apps</td>
<td>Enables single sign-on to Citrix Mobile apps.</td>
</tr>
<tr>
<td>Anonymous store access</td>
<td>Support access for unauthenticated (anonymous) users.</td>
</tr>
</tbody>
</table>

### Input experience

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard layout sync - client to VDA (Windows VDA)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## Citrix Workspace app

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard layout sync - client to VDA (Linux VDA)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Keyboard layout sync - VDA to client (Windows VDA)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Keyboard layout sync - VDA to client (Linux VDA)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Unicode keyboard layout mapping</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Keyboard input mode - unicode</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows 2311 and Windows Store 2309.1</th>
<th>Windows 2203.1 LTSR</th>
<th>Linux 2311</th>
<th>Mac 2311</th>
<th>iOS 24.1.0</th>
<th>Android 24.1.0</th>
<th>HTML5 2312</th>
<th>ChromeOS 2312</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard input mode - scan-code</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server IME</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Generic client IME (CTXIME) for CJK IMEs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Command line interface</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Keyboard sync setting UI and configurations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Input mode setting UI and configur-ations</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## Feature Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard layout sync - client to VDA (Windows VDA)</td>
<td>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.</td>
</tr>
<tr>
<td>Keyboard layout sync - client to VDA (Linux VDA)</td>
<td>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.</td>
</tr>
<tr>
<td>Keyboard layout sync - VDA to client (Windows VDA)</td>
<td>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.</td>
</tr>
<tr>
<td>Keyboard layout sync - VDA to client (Linux VDA)</td>
<td>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.</td>
</tr>
<tr>
<td>Unicode keyboard layout mapping</td>
<td>Supports Unicode keyboard layout mapping for Windows VDA with non-Windows Citrix Workspace app.</td>
</tr>
<tr>
<td>Keyboard input mode - unicode</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>StoreFront only</td>
</tr>
<tr>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td>Indicator</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>For NSAP VC, the Workspace app for iOS/Android supports, but for ADC/ADM, the support is still pending.</td>
</tr>
<tr>
<td>4</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.