Citrix Workspace app for Mac

Contents

About this release

September 5, 2022

> **Note:**
>
> Starting with macOS Catalina, there are additional security requirements for root CA certificates and intermediate certificates that administrators must configure. For more information, see Apple Support article HT210176.

Native support for Apple silicon (M1 chip) [Technical Preview]

Citrix Workspace app for macOS now natively supports Macs with Apple silicon (M1 chip) by way of a universal architecture. With the universal architecture, the Citrix Workspace app runs natively on both Apple silicon and Intel-based Mac computers without Rosetta emulation. The technical preview build runs natively on Macs with Apple silicon and it must be installed and tested on Macs using M1 chips.

> **Note:**
>
> Citrix continues to support Intel-based Macs that use the Rosetta 2 dynamic binary translator. However, Citrix will soon deprecate the Citrix Workspace app for Mac that uses Rosetta emulation. Keep a look out for an announcement in the Deprecation section.

You can download the universal architecture build from the **Citrix Workspace App for macOS (Apple silicon) - Universal Architecture** section at Downloads. If you're using Citrix Workspace app on a Mac running Apple silicon (M1 chip), you must upgrade the HDX RealTime Optimization Pack (RTOP). This ensures that the audio-video conferencing and Voice over Internet Protocol enterprise telephony through Microsoft Skype for Business is optimized. You can install the HDX RealTime Media Engine 2.9.500 for Mac from the Citrix website at Downloads.

If your organization uses any third-party plug-ins or virtual channels, you must ensure that these plug-ins are compatible with Macs running Apple silicon. If the plug-ins are developed in-house then you must rebuild these plug-ins before installing the universal architecture build.

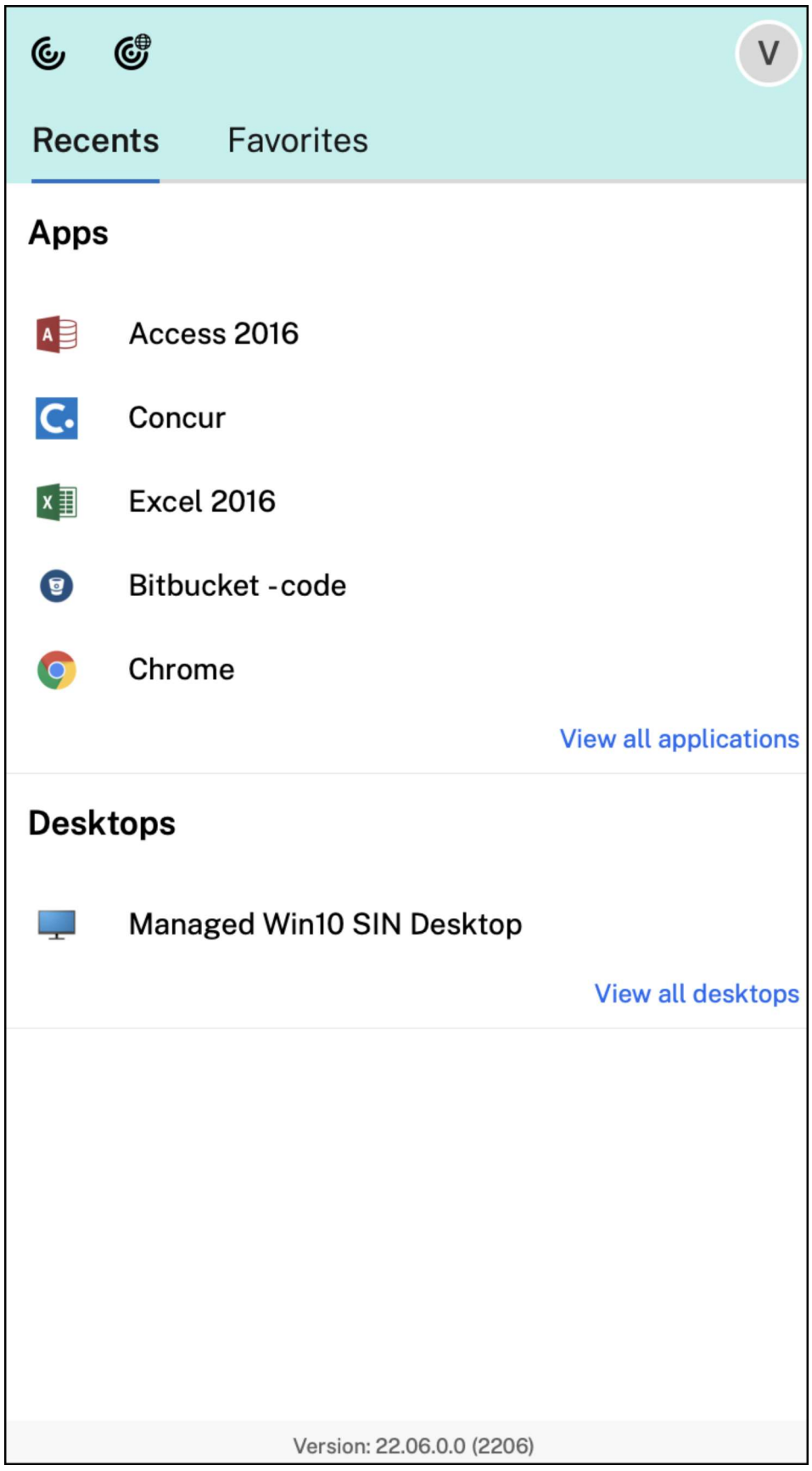
For more information such as uninstalling the universal architecture build or using the Custom Virtual Channel SDK (VCSDK), see the Native support Apple silicon [Technical preview] section.

What's new in 2208.1

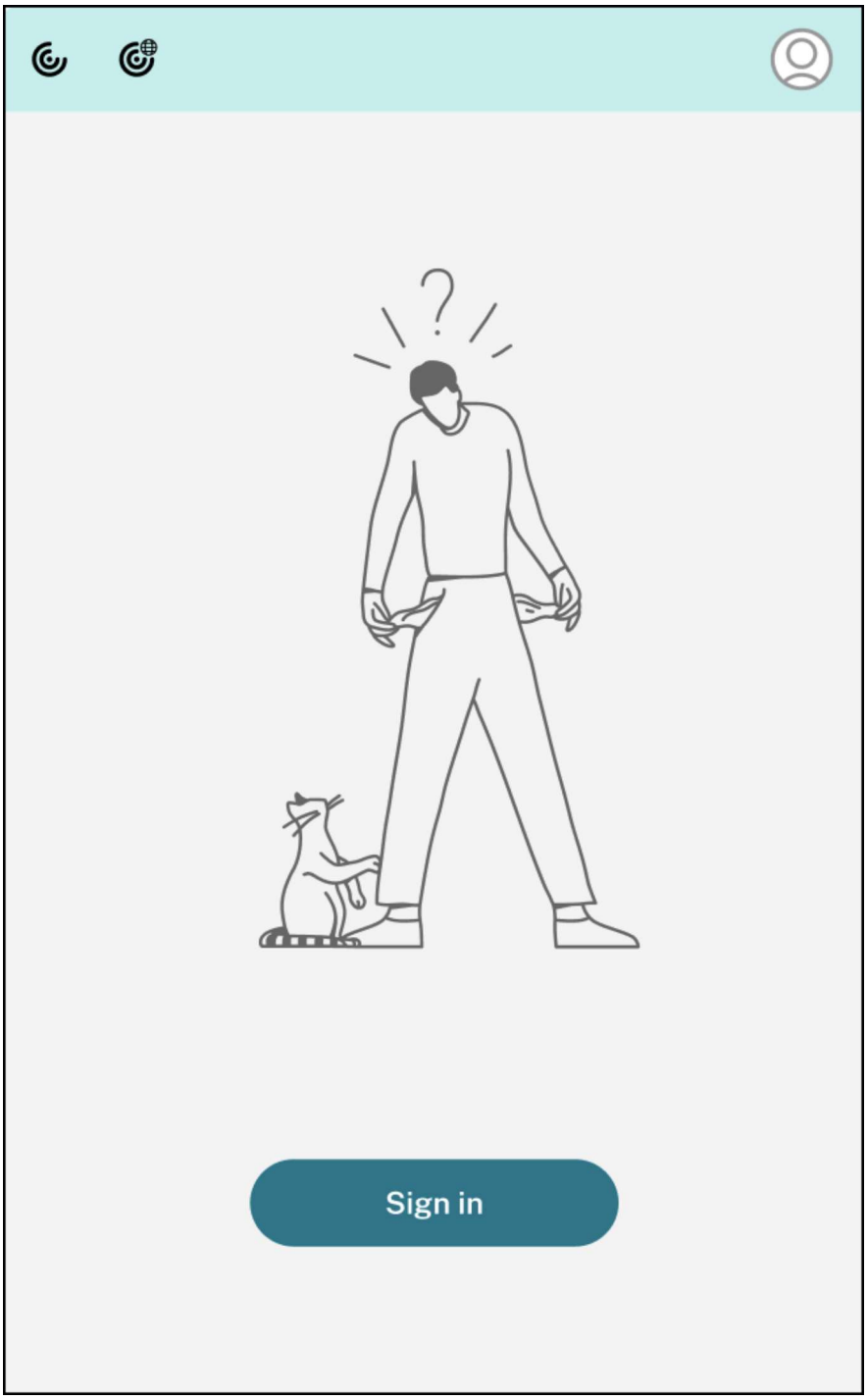
View apps, desktops, and Citrix Workspace Browser from menu bar through a quick access menu

You can now view your most recently used or favorite apps and desktops or open a Citrix Workspace Browser window by clicking the Citrix Workspace icon in the menu bar. This feature provides easy access to some of your resources without having to open the Citrix Workspace app.

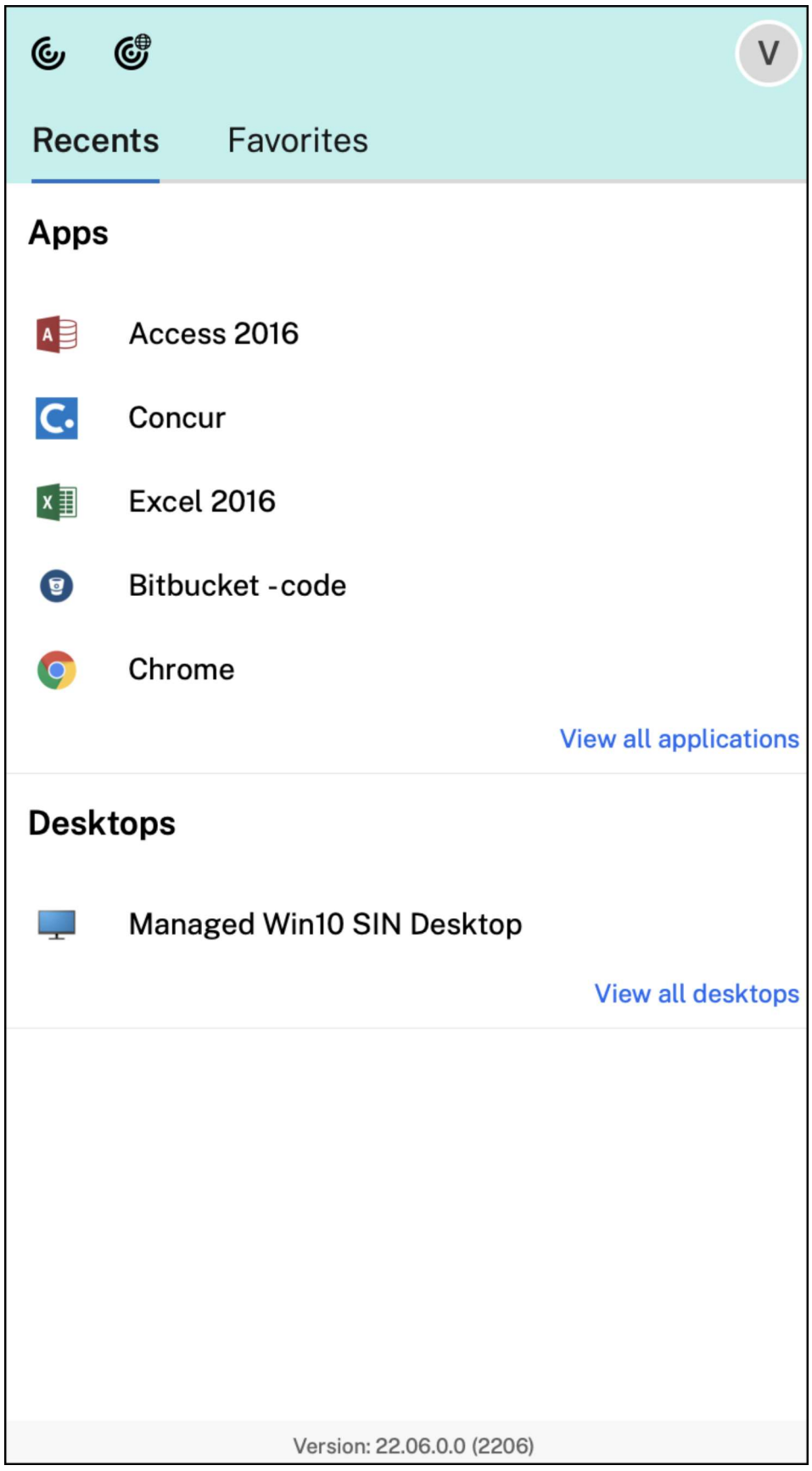
> **Note:**
>
> This feature is not available on on-premises setups.



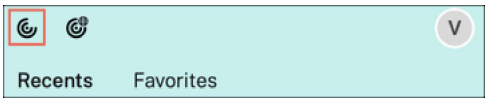
If you've not configured any accounts, a sign-in prompt appears.



A maximum of 5 of your recently used or favorite apps or desktops appear in the options under the **Recent** and **Favorites** tabs respectively. To view the other apps in the Citrix Workspace app, click **View all applications**. To view the other desktops in the Citrix Workspace app, click **View all desktops**.

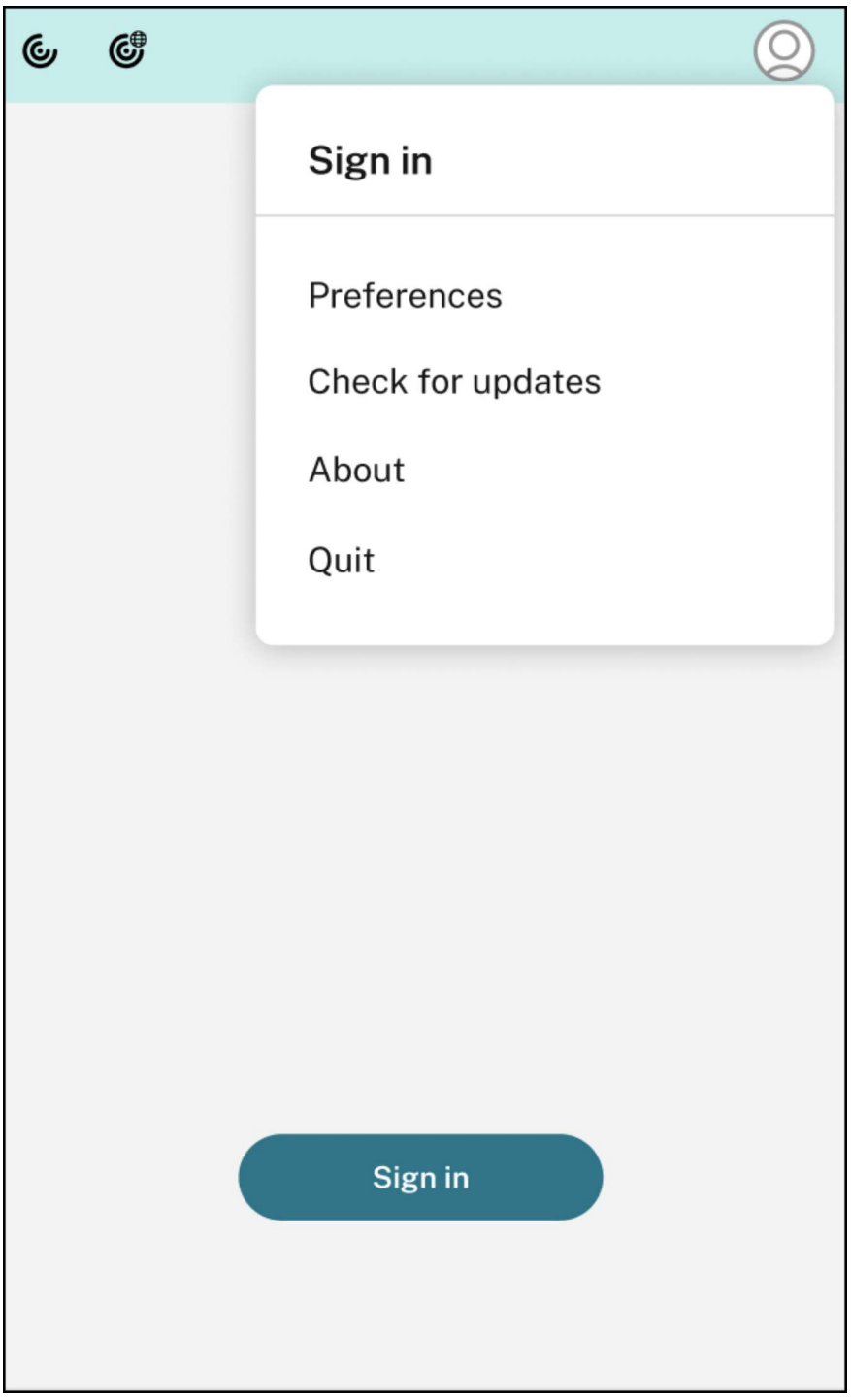


You can open the Citrix Workspace UI by clicking the Citrix Workspace app icon.



You can open the Citrix Workspace Browser, without opening a web or SaaS app by clicking the Citrix Workspace Browser icon.

> **Note:**
>
> The Citrix Workspace Browser is not available if the configured store doesn't have any web or SaaS apps. Further, it is available only if your admin has configured Citrix Secure Private Access.



You can view the following options when you click the **Account** icon in the top-right corner:

- Preferences
- Check for updates
- About
- Quit

Support for authentication using FIDO2 [Technical Preview]

With this release, users can authenticate virtual apps or desktops by using FIDO2 security keys. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. For more information about FIDO2 see FIDO2 Authentication.

This feature currently supports roaming authenticators (USB only) with PIN code and touch capabilities. You can configure FIDO2 Security Keys based authentication. For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.

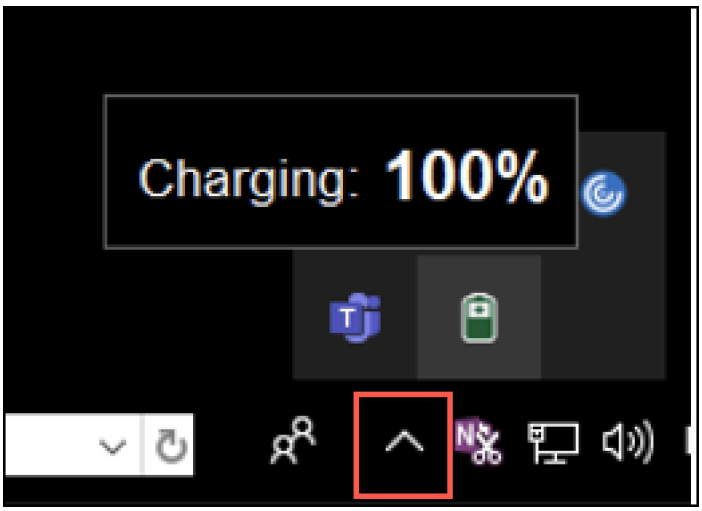
When you access an app or a website that supports FIDO2, a prompt appears, requesting access to the security key. If you've previously registered your security key with a PIN (a minimum of 4 and a maximum of 64 characters), then you must enter the PIN while signing in.

If you've registered your security key previously without a PIN, simply touch the security key to sign in.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds not be deployed in production environments.

Battery status indicator

The battery status of the device now appears in the notification area of a Citrix Desktop session. To view the battery status within the desktop session, click the **Show hidden icons** arrow in the taskbar.



> **Note:**
>
> The battery status indicator does not appear for server VDAs.

Citrix Workspace Browser

This release includes Citrix Workspace Browser version 103.1.1.14, based on Chromium version 103. For more information about the Citrix Workspace Browser, see the Citrix Workspace Browser documentation.

Citrix Workspace Browser Profiles

Profiles help you keep personal information such as history, bookmarks, passwords, and other settings separate for each of your Citrix Workspace accounts. Based your Workspace store, a profile is created, allowing you to have a unique and personalized browsing experience.

> **Note:**
>
> After you upgrade to version 103.1.1.14 and sign in to the device for the first time, only your previously saved passwords are removed. When you sign in to the device using a different store for the first time, all your previously saved data is lost.

Open all web and SaaS apps through the Citrix Workspace Browser [Technical Preview]

From this release, all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Workspace Browser. You can register for this technical preview by using this Podio form.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Fixed issues in 2208.1

- When the Citrix Workspace login prompt appears, clicking the Cancel button doesn't close the popup and it appears repeatedly. [CVADHELP-19919]
- If you're using Direct Workload Connection in Citrix Cloud to connect to VDAs directly, a black screen appears and you're disconnected from the VDA. This issue occurs when Network Location Service (NLS) is enabled. [HDX-40588]

- When you use a multi-touch gesture to swipe between full-screen apps, the Citrix Workspace desktop session window turns black for a moment. This issue occurs on Macs with a notch display. [HDX-42314]

Known issues in 2208.1

- No new issues have been observed in this release.

Earlier releases

This section lists features in previous releases along with their fixed and known issues. Releases reach End of Life (EOL) 18 months after the release date. For details about lifecycle dates for the supported versions, see Lifecycle Milestones for Citrix Workspace app and Citrix Receiver.

2206.1

Uninstall app by dragging the Citrix Workspace app icon to the bin

You can now simply drag or move the Citrix Workspace app icon into the bin to completely uninstall the app.

Previously, dragging the Workspace app icon into the bin would remove the app but leave behind certain system files on your Mac. With this release, the Citrix Workspace app and all its associated files are removed from your device when you drag the icon to the bin.

To uninstall the Citrix Workspace app by dragging it to the bin, do the following:

1. Close the Citrix Workspace app, if it's running.
2. Drag the Citrix Workspace app to the bin.
   Alternatively, you can right click on the Citrix Workspace app and select **Options** > **Move to Bin**.
3. Provide your system credentials when prompted.
4. Close all running apps (Citrix Workspace) and click **Continue** to confirm.
   The Citrix Workspace app and all its system files are deleted from your device.

Support for service continuity in the Safari browser

The Citrix Workspace service continuity feature is now supported for the Safari browser. Users must install Citrix Workspace app for Mac and the Citrix Workspace web extension. Service continuity removes (or minimizes) the dependency on the availability of the components involved in the connection process. It allows you to connect to your virtual apps and desktops regardless of the cloud services' health status. For more information, about the service continuity feature, see the section Service continuity.

Improved audio echo cancellation support [Technical Preview]

Citrix Workspace app now supports echo cancellation in adaptive audio and legacy audio codecs. This feature is designed for real time audio use cases, and it improves the user experience.
Citrix recommends using adaptive audio.

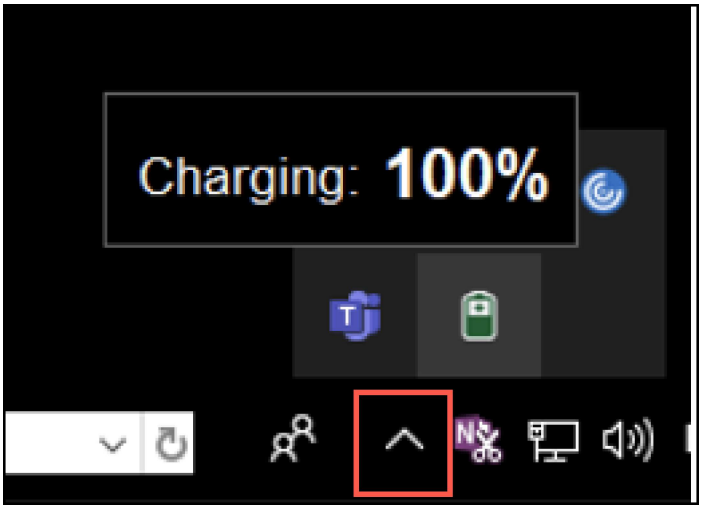
> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds not be deployed in production environments.

Enhancements to Optimized Microsoft Teams

In optimized Microsoft Teams, you can now use the video function when more than one virtual desktop or app session is in use.

Battery status indicator [Technical Preview]

The battery status of the device now appears in the notification area of a Citrix Desktop session.



> **Note:**
>
> The battery status indicator does not appear for server VDAs.
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance. It is advised that Beta

> builds not be deployed in production environments.

Citrix Workspace Browser

This release includes Citrix Workspace Browser version 101.1.1.14, based on Chromium version 101. For more information about the Citrix Workspace Browser, see the Citrix Workspace Browser documentation.

Fixed issues in 2206.1

- The mouse pointer is misaligned on Macs with a notch display. [CVADHELP-19337]
- You're not signed out of the Workspace app when the inactivity timeout value lapses. This issue occurs intermittently. [CVADHELP-19812]
- You might get an error when you try to uninstall Citrix Workspace app. [CVADHELP-19121]
- In optimized Microsoft Teams, the video function might not work if you start another virtual desktop or app session. [HDX-40451]
- While sharing the screen or an app during the Microsoft Teams call, your peer might see visual artifacts. This issue occurs due to unstable frame rates, such as incorrect video playback (frozen or transient black frames). This release includes improved frame rates or sampling rates that help to reduce visual artifacts. [HDX-38032]

2204

Global App Configuration Service settings for `allowedWebStoreURLs`

Admins can now use Global App Config Service to configure settings of Custom Web Stores. Admins can configure the Custom Web Stores by using the `allowedWebStoreURLs` property. For more information about the Global App Configuration Service, see Getting Started.

Support to open Citrix Workspace app in maximized mode

Admins can configure the `maximise workspace window` property in the Global App Configuration Service to enable the Citrix Workspace app to open in the maximized mode by default. For more information about the Global App Configuration Service, see Getting Started.

Support for high DPI monitors [Technical preview]

Citrix Workspace app for Mac is now compatible with high DPI monitors with resolution greater than 4K. On desktop sessions, apps, text, images, and other graphical elements appear in a size that can be viewed comfortably on these high-resolution monitors.

To enable this feature, run the following command in macOS terminal:

```
defaults write com.citrix.receiver.nomas EnableHighDPI -bool YES
```

Admins can edit the **Display memory limit** policy, which specifies the maximum video buffer size in kilobytes for a desktop session, to suit the display resolution. The default value for the Display memory Limit policy is 65536 KB and is sufficient for up to 2x4K monitors (2x32400KB). Admins must edit this value by navigating to **Citrix Studio** > **Policies** > **Display memory limit** and use a value of 393216 KB to use this feature.

For more information about the Display memory limit policy, see Display memory limit.

> **Note:**
>
> This feature works with a maximum of two connected monitors.
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Enhancement to Permanent Client Access License (CAL) for Remote Desktop Sessions

With this release, if you are running CAL in your environment to access remote desktops, when the client ID is greater than 15 characters, you can launch the remote desktop session with a permanent license.

To enable this feature, admins must configure the **`default.`**`ica` file by doing the following:

1. In the StoreFront server, navigate to *C:\inetpub\wwwroot\Citrix<StoreName>\App_Data* and open the **`default.`**`ica` file with any editor.
2. Add the following line in the **[WFClient]** section:

```
isRDSLicensingEnabled=On
```

Restore default keyboard settings

If you had previously modified the keyboard preferences in the Citrix Workspace app, you can now restore default keyboard settings. To restore the keyboard settings to its default values, open the Citrix Workspace app, navigate to **Preferences** > **Keyboard** and click **Restore Defaults**. Click **Yes** to confirm.

App Protection compatibility with HDX optimization for Microsoft Teams

With this release, full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group. When you click **Share content** in Microsoft Teams, the screen picker removes the **Desktop** option. You can only select the Window option to share any open app, if the VDA is 2109 or higher. If you are connected to VDA older than 2019, no content is selectable.

Citrix Workspace Browser

This release includes Citrix Workspace Browser version 99.1.1.8, based on Chromium version 99. For more information about the Citrix Workspace Browser, see the Citrix Workspace Browser documentation.

Make Citrix Workspace Browser your default browser

You can now make Citrix Workspace Browser your default browser. Once you have made the Citrix Workspace Browser your default browser, all links and Web and SaaS apps open in the Citrix Workspace Browser by default.
To make Citrix Workspace Browser your default browser on macOS, do the following:

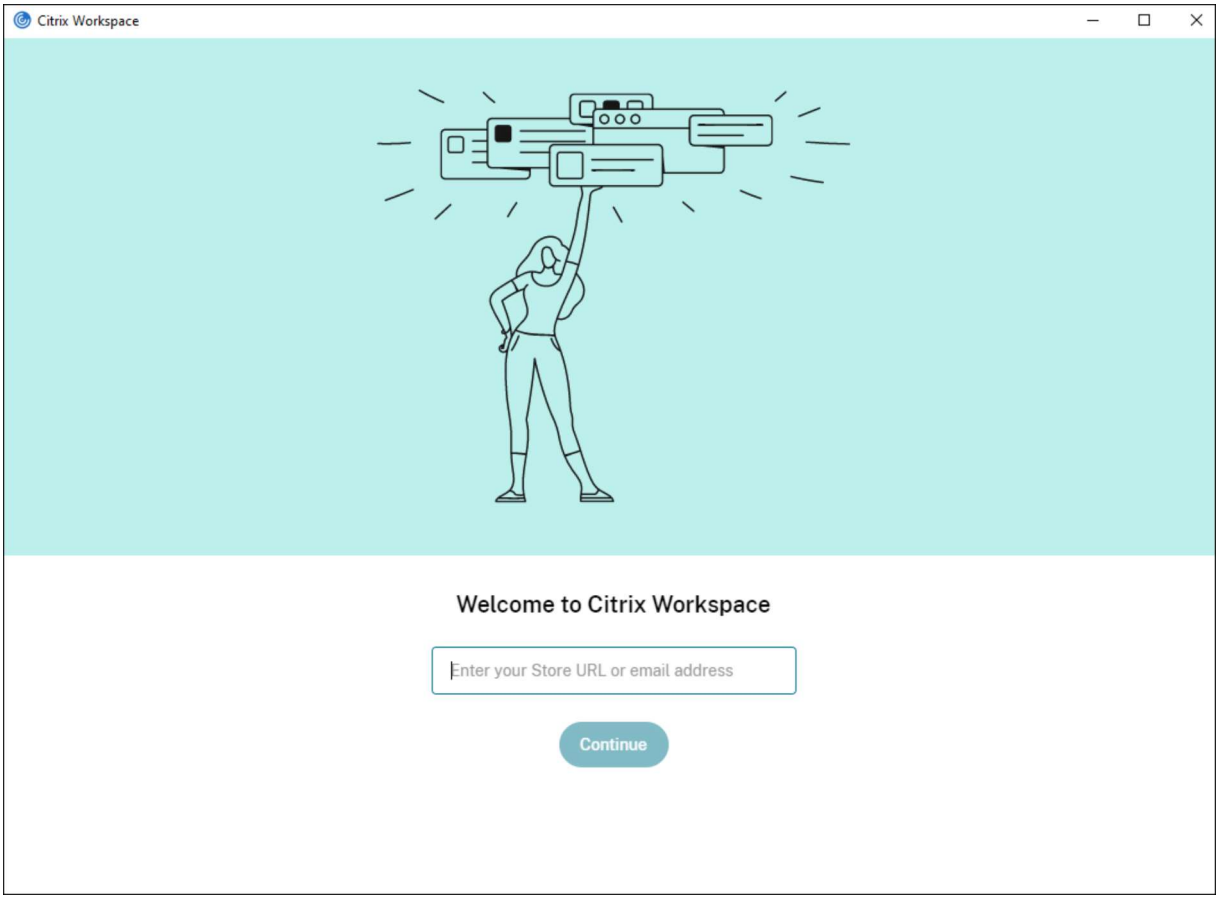
1. Open the Citrix Workspace Browser and click the ellipsis icon and open the **Settings** menu.
2. Click the **Default Browser** option on the left pane.
3. In the Default browser page, click **Make default**. When prompted, click **Use Citrix Workspace Browser** to confirm your choice and apply the changes.

Fixed issues

- The mouse pointer is misaligned on Macs with a notch display. [CVADHELP-19337]
- You're not signed out of the Workspace app when the inactivity timeout value lapses. This issue occurs intermittently. [CVADHELP-19812]
- You might get an error when you try to uninstall Citrix Workspace app. [CVADHELP-19121]
- In optimized Microsoft Teams, the video function might not work if you start another virtual desktop or app session. [HDX-40451]
- While sharing the screen or an app during the Microsoft Teams call, your peer might see visual artifacts. This issue occurs due to unstable frame rates, such as incorrect video playback (frozen or transient black frames). This release includes improved frame rates or sampling rates that help to reduce visual artifacts. [HDX-38032]

2203.1

This release includes a simplified and intuitive onboarding experience for first time users.



Inactivity timeout for Citrix Workspace app

The inactivity timeout feature logs you out of the Citrix Workspace app based on a value that the admin sets. Admins can specify the amount of idle time that is allowed before a user is automatically signed out of the Citrix Workspace app. You're automatically signed out when no activity from the mouse, keyboard, or touch occurs for the specified interval of time, within the Citrix Workspace app window. The inactivity timeout does not affect the already running Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sessions or the Citrix StoreFront stores.

For more information see Inactivity Timeout for Citrix Workspace app.

PDF Universal Printing

You can now use the PDF universal printing feature when printing from a Mac. You no longer need to install the HP Color LaserJet 2800 Series PS driver when auto-creating client printers on a Mac by using the Citrix Universal Printer Driver (UPD).

For more information about using this feature, see Printing.

Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps [Technical Preview]

This feature simplifies the configuration of SSO for internal web apps and SaaS apps while using third party identity providers (IdPs). The enhanced SSO experience reduces the entire process to a few commands. It eliminates the mandatory prerequisite to configure Citrix Secure Private Access in the IdP chain to set up SSO. It also improves the user experience, provided the same IdP is used for authentication to both the Citrix Workspace app and the particular web or SaaS app being launched.

You can register for this technical preview by using this Podio form.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Support for Transport Layer Security (TLS) protocol version 1.3 on Linux VDAs [Technical preview]

If you're running TLS version 1.3, you can now connect to virtual apps and desktops hosted on the Linux operating system.

> **Note:**
>
> You can't connect to Windows virtual apps and desktops if you're running TLS version 1.3.

Technical previews are available for customers to test in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds not be deployed in production environments.

Share apps using the 'Share content' feature in Microsoft Teams

You can now share individual applications, windows, or full screen using the screen sharing feature in Microsoft Teams. Citrix Virtual Delivery Agent 2109 is a prerequisite for this feature.
To show a specific application, click **Share content** in your meeting controls and select the application of interest. After a red border appears around the app you select, peers on the call can see your app.

If you minimize the app, Microsoft Teams displays the last image from the shared app. Maximize the window to resume sharing.

Multi-window chat and meetings for Microsoft Teams

Users can now use multiple windows for chat and meetings in Microsoft Teams (1.5.00.5967 or higher) when optimized by HDX in Citrix Virtual Apps and Desktops and Citrix DaaS. Users can pop out their conversations or meetings in a variety of ways. For details on the pop-out window feature, see Teams Pop-Out Windows for Chats and Meetings on the Microsoft Office 365 site.

If you're running an older version of Citrix Workspace App or VDA, be aware that Microsoft will deprecate the single-window code in the future. However, you will have a minimum of nine months to upgrade to a version of the VDA/CWA that supports multiple windows (2203 or later).

> **Note:**
>
> This feature is available only after the roll-out of a future update from Microsoft Teams. Got more details, see Microsoft 365 roadmap.

Give or take control in Microsoft Teams

You can use the **Give control** button to give control access of your shared screen to other users participating in the meeting. The other participant can make selections and modify the shared screen through keyboard, mouse, and clipboard input. You both now have control of the shared screen and you can take back the control anytime.

To take control during screen sharing sessions, any participant can request control access through the **Request control** button. The person sharing the screen can then approve or deny the request. When you have the control, you can control the keyboard and mouse input on the screen shared and release control to stop sharing control.

> **Note:**
>
> This feature is available only after the roll-out of a future update from Microsoft Teams.

StoreFront to Workspace migration

As your organization transitions from on-premises StoreFront to Workspace, users are required to manually add the new Workspace URL to the Citrix Workspace app. This feature enables admins to seamlessly migrate users from a StoreFront store to a Workspace store with minimal user interaction.

For more information about this feature, see StoreFront to Workspace URL Migration.

Global App Config Service

The new 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. For more information, see Global App Configuration Service documentation.

Extend multiple monitors in full-screen mode

You can now enter full-screen mode on two or more monitors simultaneously. To use this feature, perform the following steps:

1. Open the Citrix Viewer.
2. To use full-screen mode on the other connected monitors, drag the window from your primary monitor to span into the connected monitors. From the menu bar, select **View** > **Enter Full Screen**. The window goes into full screen mode on those monitors.

   > **Note:**
   >
   > If you have previously selected the **Use All Displays In Full Screen** option, ensure to unselect it as this selection extends full screen on all connected monitors.

Citrix recommends using a maximum of 3 monitors, including the primary monitor.

Citrix Workspace Browser

This release includes Citrix Workspace Browser version 98.1.2.17, based on Chromium version 98. For features or bugs fixes in the Citrix Workspace Browser, see What's new in the Citrix Workspace browser documentation.

Fixed issues

- During active sessions, the Citrix Workspace app watermark becomes transparent, displaying content from windows in the background. This issue occurs only in seamless mode. [CVADHELP-19153]
- When launching a session from a VDA (2112 or higher) through a Citrix ADC, you might experience a session interruption, with session reliability starting but not reconnecting. [CVADHELP-19687]
- The Large File Receive pop-up dialog from the Mimecast plug-in doesn't appear in Outlook. [HDX-37137]
- When the value for Path MTU Discovery (PMTUD) is not 1500 (default), users can't fall back to TCP on an Azure cloud environment. [HDX-37215]

- You might experience high CPU utilization on endpoint when webcam is turned on in an optimized Microsoft Teams video call. [HDX-37168]
- In Citrix Workspace app, you might experience intermittent failures when answering or making a Microsoft Teams call. The following error message appears:
  "Call could not be established." [HDX-38819]
- Citrix Workspace app sessions might not launch if the Citrix AppFlow is configured in Citrix ADC. [HDX-39496]
- When auto-update is disabled and you navigate to **Preferences** > **Advanced**, the Citrix Workspace app crashes. [RFMAC-10978]

2201

StoreFront to Workspace migration [Technical preview]

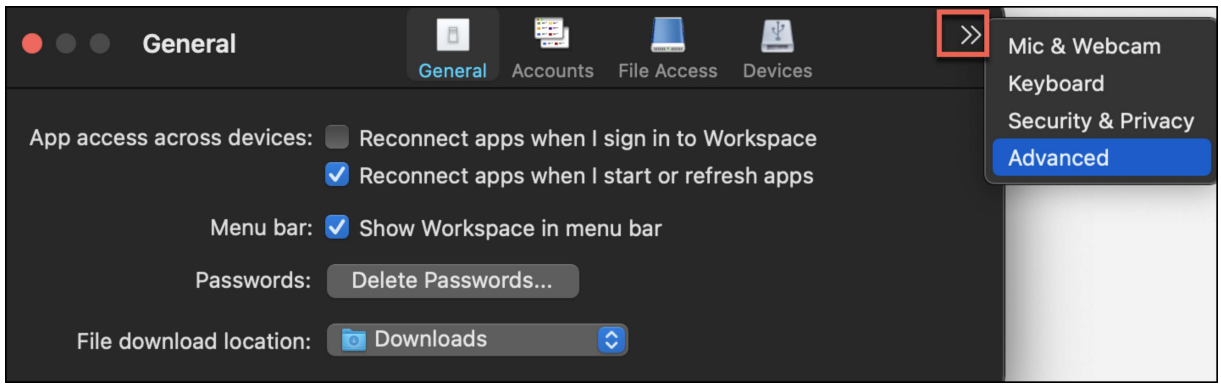
As your organization transitions from on-premises StoreFront to Workspace, users are required to manually add the new Workspace URL to the Citrix Workspace app. This feature enables admins to seamlessly migrate users from a StoreFront store to a Workspace store with minimal user interaction.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

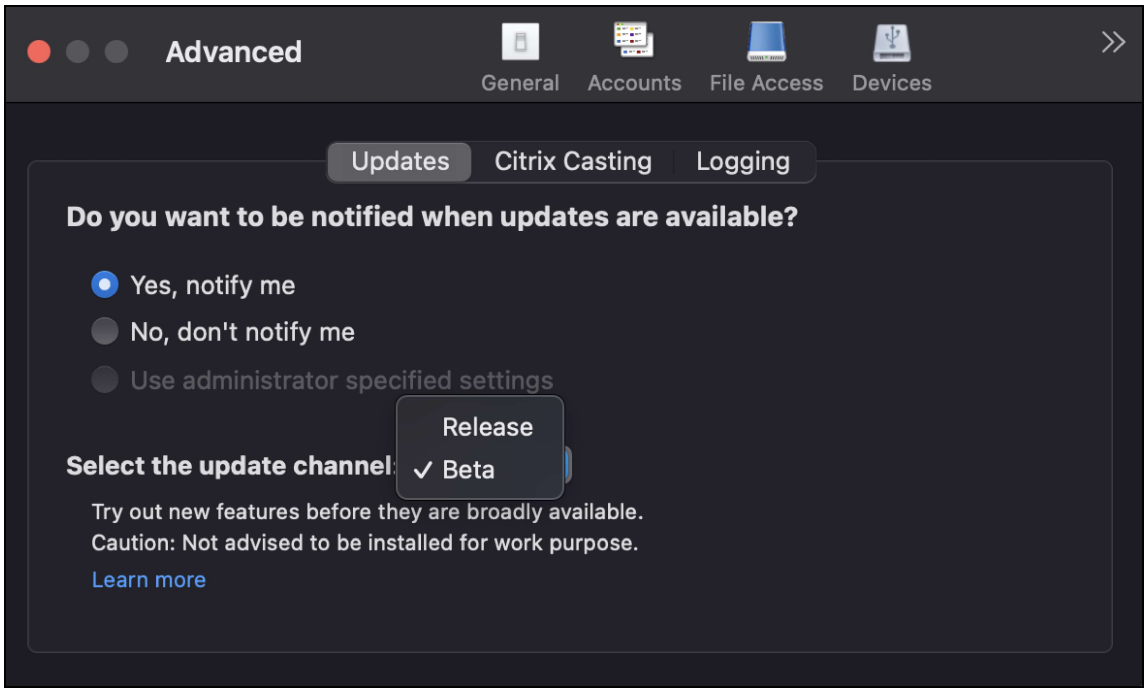
Citrix Workspace app Beta program

Starting with this release, you can automatically update existing installations of Citrix Workspace app to the most recent beta builds and test them. Beta builds are early access versions released before the general availability of a fully supported stable release update. You receive an update notification when the Citrix Workspace app is configured for automatic updates.

To access the beta builds, open the Citrix Workspace app, right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**. To update to beta builds, select the **Beta channel** from the drop-down list.



- **Beta** - Early access release to easily test and report issues before general availability.
- **Release** - Fully supported stable release update.



For more information about using this feature, see Update.

Extend multiple monitors in full-screen mode [Technical preview]

You can now enter full-screen mode on two or more monitors simultaneously. To use this feature, perform the following steps:

1. Open the Citrix Viewer.
2. To use full-screen mode on the other connected monitors, drag the window from your primary monitor to span into the connected monitors. From the menu bar, select **View** > **Enter Full Screen**. The window goes into full screen mode on those monitors.

> **Note:**
>
> If you have previously selected the **Use All Displays In Full Screen** option, ensure to unselect it as this selection extends full screen on all connected monitors.

Citrix recommends using a maximum of 3 monitors, including the primary monitor.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Fixed issues

- While selecting the candidate text from the Input Method Editor composition window using the left or right arrows in the keyboard, the input cursor doesn't move accordingly. This issue occurs when you launch a desktop with the **Use local keyboard layout, rather than the remote server keyboard layout** check box is selected in the **Preferences** > **Keyboard** window of Citrix Workspace app. This issue is observed only in the Chinese and Japanese language. [HDX-34956]
- The mouse pointer disappears intermittently in Workspace apps sessions and you are not able to click anything. [HDX-36820]
- The desktop session closes unexpectedly when you drag a cell in a PivotTable in an Excel sheet. [HDX-37178]
- Sometimes, you experience issues with graphics in your desktop session after you upgrade to version 2112 and when lossless and full screen H.264 codec policies are applied. [HDX-37272]
- After you upgrade from Citrix Workspace app 2010 to version 2112, you can't connect to desktops or apps. [RFMAC-10811]

2112

What's new

Support for custom web stores

You can now access your organization's custom web store from the Citrix Workspace app for Mac. Previously, you accessed all customized stores through the browser only.

Citrix Workspace app for Mac loads the custom web stores with a browser-like experience and extends App Protection capabilities to custom web stores. Making the custom portal accessible from the native

Citrix Workspace App provides comprehensive capabilities and user experience for this feature. For more details about Global App Configuration Service, see Getting Started.

For more information about configuring a custom web store, see Custom web store.

Request control in Microsoft Teams

With this release, you can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other modifications to the shared screen.

To take control when a screen is being shared, click **Request control** at the top of the Microsoft Teams screen. The meeting participant who's sharing the screen can either allow or deny your request. When you're done, click **Release control**.

Limitation:

The **Request Control** option is not available during peer-to-peer calls between an optimized user and a user on the native Microsoft Teams desktop client that is running on the endpoint. As a workaround, users can join a meeting to get the **Request Control** option.

Dynamic e911

With this release, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it allows you to do the following:

- Configure and route emergency calls.
- Notify security personnel.

Notification is provided based on the current location of the Citrix Workspace app running on the endpoint, instead of the Microsoft Teams client that runs on the VDA. Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112.1 for Windows, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law. For more information about this feature, see Support for dynamic e911 in the section **Microsoft Phone System**.

PDF Universal Printing (Technical preview)

The PDF universal printing feature is available with the Citrix Virtual Apps and Desktops 2112 release. This feature is disabled by default. To use this feature, you must sign up by using this web form. The feature is enabled for you once we receive your information. You also receive instructions about using the feature and the printing policies that must be enabled.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Service continuity

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services. Citrix Workspace Web extensions make service continuity available to users who access their apps and desktops through a browser.

Together, the Citrix Workspace app and the Workspace Web extension use Workspace connection leases to give browser users access to their apps and desktops during outages. For more information, see Service continuity

Citrix Workspace Browser

This release of the Workspace Browser is based on Chromium version 95. For features or bugs fixes in the Citrix Workspace browser, see What's new in the Citrix Workspace browser documentation.

Fixed issues

- The "Cannot connect to server error" appears when the transport protocol switches from Enlightened Data Transport (EDT) to TCP. [CVADHELP-18310]
- If a Progressive Web App (PWA) that is protected is opened on macOS, the **App Protection** policies aren't enforced. [RFMAC-10128]

2111

What's new

- With this release, users cannot manually roll back Citrix Workspace app for Mac to a version that is lower than the version installed on their systems. For example, if a Mac device has Citrix Workspace app Version 2109 installed on it, then you cannot manually roll back the app to version 2108 or lower.
- Launch the remote desktop session with a permanent license, if you're running Client Access Licenses (CAL) to access remote desktops. You can launch the remote desktop session when the client ID is greater than 15 characters.

- To load Citrix Virtual Channel SDK on a Mac running Citrix Workspace app 2111, you must recompile your custom virtual channels. For details, see Update Custom Virtual Channels on Citrix Workspace app for Mac.

Support for custom web stores [Technical preview]

With this release, you can access your organization's custom web store from the Citrix Workspace app for macOS. Admins must add the custom web store to the list of allowed URLs in the Global App Configuration Service to use this feature. After adding the URLs, you can provide the custom web store URL in the Add Account option in Citrix Workspace app. The custom web store opens in the native Citrix Workspace app for macOS.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Citrix Workspace Browser - For new features or bugs fixes in Citrix Workspace browser, see What's new in the Citrix Workspace browser documentation.

Fixed issues

- On devices running macOS, Advanced Audio Coding (AAC) is not supported. [CTXBR-1844]
- If you have configured the Citrix Workspace app using the `.cr` file and signed in with your credentials, there's a delay before the home page appears. [RFMAC-9990]
- Open a protected SaaS app, open a new tab, and separate the new tab into a new window by dragging it out of the tab bar. Now arrange two windows next to each other and open a new tab in the second window and take a screenshot. You are able to capture the screenshot for the protected SaaS app as well in. [RFMAC-10060]
- Switching from one store to another might sign you out from the first store. [RFMAC-10137]
- When you enter incorrect credentials while signing into the Citrix Workspace app, the "Incorrect credentials" error message doesn't appear and an authentication prompt appears again. Sometimes, **Domain\User** appears in the authentication prompt instead of **User name**. [RFMAC-10210]
- Calls fail when an optimized Microsoft Teams P2P call is made from Citrix Workspace app for Mac 2109 to Citrix Workspace app for Windows 2109. [HDX-35223]

2109.1

What's new

macOS Monterey Support

Citrix Workspace app for Mac is supported on macOS Monterey (12.0.1).

Fixed issues

- If you have opened a protected app, an unprotected SaaS app, and a protected desktop session, the browser exits unexpectedly. This issue occurs when you switch from the protected desktop session window to the unprotected SaaS app. [CTXBR-2087]
- If your admin has installed external extensions in Google Chrome, the Citrix Workspace Browser crashes when you open it. [CTXBR-2135]

2109

What's new

> **Note:**
>
> If Service continuity is enabled, and you upgrade to version 2109, the connection lease files are refreshed. All the existing leases are deleted and new leases are fetched as part of functionality enhancements.

Citrix Workspace app for Mac on macOS Monterey Beta

Citrix Workspace app 2109 for Mac has been tested on macOS Monterey Beta 7. Use this setup in a test environment and provide your feedback.

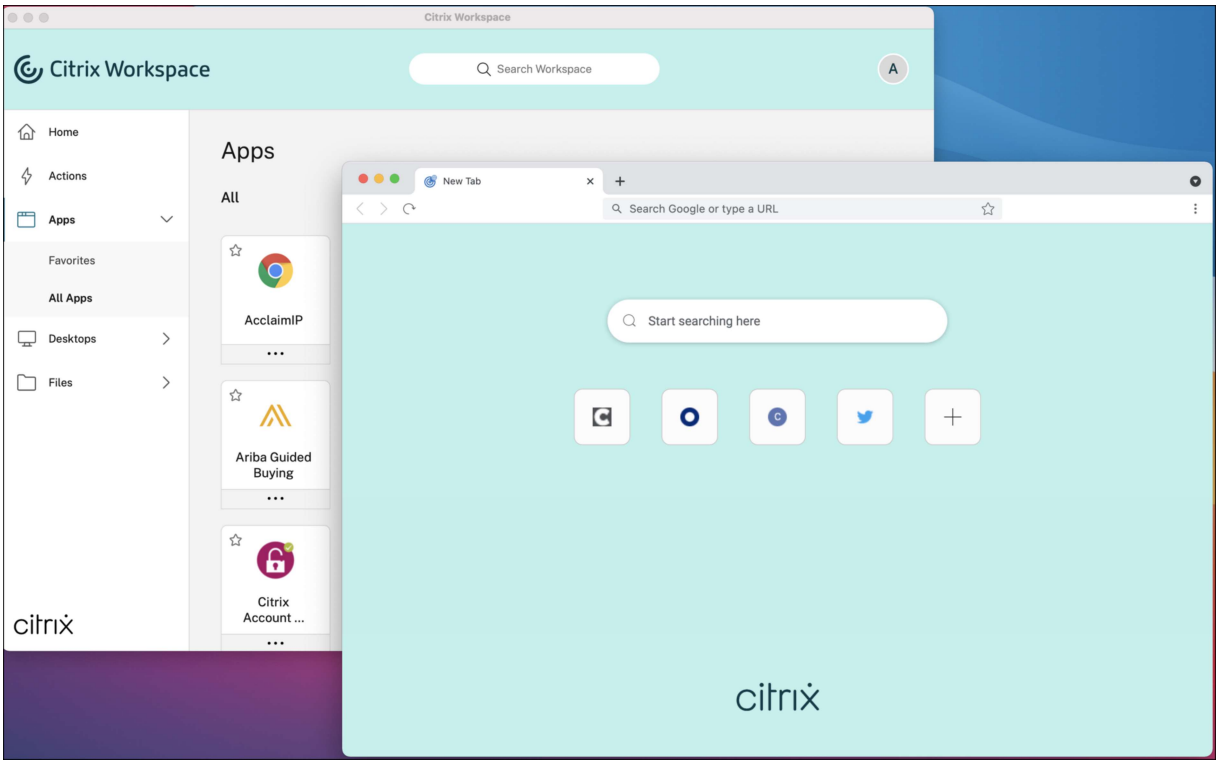
> **Caution:**
>
> Do not use Citrix Workspace app for Mac on macOS Monterey Beta versions in production environments.

Email-based auto-discovery of store

You can now provide your email address in Citrix Workspace app for Mac to automatically discover the store associated with the email address. If there are multiple stores associated with a domain, by default the first store returned by the Global App Configuration Service is added as the store of choice. Users can always switch to another store if necessary.

Citrix Workspace Browser

Citrix Workspace Browser is a native browser running on the client machine. It enables users to open web or SaaS apps from the Citrix Workspace app in a secure manner. The browser ensures a consistent user interface while accessing various web or SaaS apps while improving your productivity and giving you a great performance in rendering those apps.



With a continued focus on enriching the user-experience, the new Workspace browser brings you an enhanced and a more native browser-like experience, complete with the following features:

- VPN-less access to internal webpages
- Microphone and webcam support
- Tabbed browsing experience
- Multi-window views
- Editable omnibox
- Bookmarks
- Shortcuts on the new tab page
- Customizable settings
- Analytics

Admins can enable Secure Private Access or App protection policies including anti key-logging, anti-screen capture, download, printing, clipboard restrictions, and watermarking in varying combinations on a per-URL basis.

For more information, see Citrix Workspace Browser documentation.

End Point Analysis (EPA) enhancement

Starting with this release, Citrix Workspace app for macOS supports End Point Analysis (EPA). Advanced Endpoint Analysis (EPA) scans the device for endpoint security requirements configured on the Citrix Gateway. When the scan completes successfully, a user is granted access.

> **Note:**
>
> This feature works only if you have configured nFactor authentication in your environment.

For more information about the EPA scan, see Advanced Endpoint Analysis scans.

Adaptive audio

With Adaptive audio, you don't need to configure the audio quality policies on the VDA. Adaptive audio optimizes settings for your environment and replaces legacy audio compression formats to provide an excellent user experience. For more information, see Adaptive Audio.

Support for H.264 Advanced Video Coding (MPEG-4 AVC) with Microsoft Teams

This release includes support for hardware accelerated H.264 video encoding/decoding, which reduces the load on CPU usage and improves your video conferencing experience. The multimedia engine of Citrix HDX optimized Microsoft Teams (HdxRtcEngine.exe) now uses Apple's Video Toolbox framework for encoding and decoding. This framework compresses and decompresses video faster and in real time. Also, the offloading of encoding and decoding to the GPU is optimized. Hardware accelerated video decoding and encoding is enabled by default if a device supports it. This enhancement reduces the load on the CPU during multimedia usage when Microsoft Teams is optimized with HDX.

Fixed issues

- After you sign in to the Citrix Workspace app for Mac, you are prompted for authentication after a few hours. [RFMAC-10032]
- When you add a store in the Citrix Workspace app, change the authentication domain in the server console, leave the app idle for a few minutes, and then open any app or desktop session, the Citrix workspace app may crash. [RFMAC-10133]
- When a virtual app or desktop is already running and you start another virtual app or desktop, Citrix Viewer appears but the virtual app does not open. This issue occurs on devices running macOS 11.6. [RFMAC-10134]

2108.1

What's new

This release addresses several issues that help to improve overall performance and stability.

Fixed issues

When a virtual app or desktop is already running and you start another virtual app or desktop, Citrix Viewer appears but the virtual app does not open. This issue occurs on devices running macOS 11.6. [RFMAC-10134]

2108

What's new

Citrix Workspace app for Mac now supports Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT). It increases the reliability and compatibility of the EDT protocol and provides an improved user experience.

> **Note:**
>
> EDT MTU discovery is supported on macOS Big Sur and later.

Fixed issues

- There is a lag in video during conference calls in Microsoft Teams. [HDX-32603]
- On Mac clients running macOS Big Sur, an HTTP 404 or HTTP/1.1 internal server error might occur. The issue occurs when attempting to reconnect to sessions. [RFMAC-9448]

2107

What's new

This release addresses several issues that help to improve overall performance and stability.

Fixed issues

This release also addresses several issues that help to improve overall performance and stability.

2106

What's new

Support for customized URLs through 301 redirects

You can add URLs that redirect to Citrix Workspace from StoreFront or Citrix Gateway through HTTP 301 redirects.

If you're migrating from StoreFront to Citrix Workspace, you can redirect the StoreFront URL to a Citrix Workspace URL through an HTTP 301 redirect. As a result, when adding an old StoreFront URL, you're automatically redirected to Citrix Workspace.

Example of a redirect:

The StoreFront URL: `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` can be redirected to a Citrix Workspace URL: `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`.

> **Note:**
>
> - Citrix Workspace app for Mac does not support Dual Tone Multi Frequency (DTMF) with Microsoft Teams due to pending changes from Microsoft.
> - From this release onward, the Citrix Viewer's version number and the Citrix Workspace app's version number might not match. This change does not affect your experience.

Service continuity

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services.

For more information, see Service continuity section in the Citrix Workspace documentation.

Microsoft Teams enhancements

When the **Desktop Viewer** is in full screen mode, the user can select one from all the screens covered by the **Desktop Viewer** to share. In the window mode, the user can share the **Desktop Viewer** window. In the seamless mode, the user can select one screen from the screens connected to the endpoint device.
When the Desktop Viewer changes the window mode (maximized, restore, or minimize), the screen sharing stops.

When the user wants to share the screen, previews for all available screens appear in the screen sharing panel, making it intuitive to select the right one by from the previews.

Fixed issues

This release also addresses several issues that help to improve overall performance and stability.

2104

What's new

Citrix Workspace app for Mac supports manual user sign-on to network shares unless your organization enables single sign-on. To access shared network locations, open Citrix Workspace app, navigate to **Files** > **Network Shares** and provide your credentials. For more information about setting up network shares, see Create and manage storage zone connectors.

Fixed issues

This release also addresses several issues that help to improve overall performance and stability.

2102

What's new

This release addresses several issues that help to improve overall performance and stability.

Fixed issues

This release also addresses several issues that help to improve overall performance and stability.

2101

What's new

Apple silicon (M1 chip) support

Citrix Workspace app for Mac now supports Apple silicon devices (M1 chip) using Rosetta 2 on macOS Big Sur (11.0 and later). As a result, all third party virtual channels must use Rosetta 2. Otherwise, these virtual channels might not work in Citrix Workspace app for Mac on macOS Big Sur (11.0 and later). For more information about Rosetta, see the Apple support article.

Microsoft Teams optimization support for seamless app sessions

Citrix Workspace app for Mac now supports Microsoft Teams optimization for seamless app sessions. As a result, you can launch Microsoft Teams as an application from within the Citrix Workspace app. For more information, see the following:

- Optimization for Microsoft Teams
- Microsoft Teams redirection

Support for Dual Tone Multi Frequency (DTMF) with Microsoft Teams

Citrix Workspace app for Mac now supports Dual Tone Multi Frequency (DTMF) signaling interaction with telephony systems (for example, PSTN) and conference calls in Microsoft Teams. This feature is enabled by default.

Fixed issues

- Attempts to open a Microsoft Teams meeting using OWA (Outlook Web App) might fail, causing all related windows to exit unexpectedly. [CTXBR-1175]
- When you start a video call, Microsoft Teams might become unresponsive, displaying a `Citrix HDX not connected` error. [RFMAC-6727]
- On macOS Big Sur (11.0.1), attempts to connect USB devices might fail, causing the session to exit unexpectedly. [RFMAC-7079]
- In a published desktop, files saved to your local Mac device might display a file created date of 30 Nov 1979 instead of the current date. [CVADHELP-16309]
- Sometimes, the logon screen in published apps might not display properly, resulting in a reduced window size and red background color. [CVADHELP-16027]
- Audio calls might disconnect on your side when you disconnect and connect audio devices. [RFMAC-7371]
- Attempts to copy text from within Office 365 apps might succeed even when the clipboard restriction policy is enabled. [CTXBR-1166]
- Attempts to launch Microsoft Teams might fail due to issues with the HDX RealTime Connector engine and the following error message appears.

  ```
  Sorry, we couldn't connect you
  ```

  [CVADHELP-16432]

2012

What's new

Apple silicon (M1 chip) support preview

Citrix Workspace app for Mac now supports Apple silicon devices (M1 chip) on a preview basis.

Screen sharing optimization with Microsoft Teams

Citrix Workspace app for Mac now supports screen sharing optimization with Microsoft Teams. For more information, see the following:

- Optimization for Microsoft Teams
- Microsoft Teams redirection

Performance improvements

This release addresses several issues that help to improve overall performance and stability.

Fixed issues

- When using Citrix Workspace app for Mac 2008 or later, attempts to launch multiple instances of a published application might fail. [CVADHELP-16019]
- Attempts to launch Generic USB redirection might fail when you use a USB docking station. [RFMAC-6687]
- Attempts to open a window using CTRL+O in published desktops might result in two open windows. [CVADHELP-15747]
- When using Citrix Workspace app for Mac on macOS Big Sur Beta, audio calls might disconnect. The issue occurs when you disconnect audio devices and connect different audio devices during an audio call. [RFMAC-6112]
- HDX RealTime Connector engine might exit unexpectedly when you turn the camera on and off in Microsoft Teams. [RFMAC-6293]
- Attempts to launch Citrix Files from within Citrix Workspace app for Mac might fail due to issues with single sign-on. [RFMAC-4477]

Known issues

Known issue in 2204

- When traffic is tunneled through NGS, Citrix Workspace app might fail to upload or download files that are greater than 64 MB. [CTXBR-3354]

Known issues in 2203.1

- You can't click the **Create** button in the Jira app unless the browser window is maximized. [CTXBR-1976]
- Web socket connections aren't tunneled through Citrix Secure Private Access. [CTXBR-2439]

- After upgrading the Citrix Workspace app to version 2203, a question mark icon appears on the Citrix Workspace Browser icon. This issue occurs if the Workspace browser was pinned to the dock before the upgrade. [CTXBR-2864]
- When you click the **Reset settings** option on the **Advanced** settings section of the Citrix Workspace Browser, the log settings do not reset to default. As a workaround, click the **Reset to default log settings** option available on the **Logs** page. [CTXBR-2929]
- After you upgrade from Citrix Workspace Browser version 2201 to version 2203, previously saved passwords are lost and you're unable to save new passwords. [CTXBR-3063]
- Full screen mode is not available on Macs with a notch. [CVADHELP-19337]
- When you launch a desktop or app session using the browser, the session window launches in the background, behind the browser window. [RFMAC-11362]

Known issues in 2201

- The client name appears with random characters in the Citrix Broker Service and the Citrix Director if you are using the Citrix Workspace app in the offline (intranet) mode. [RFMAC-10842]

Known issues in 2112

- In Citrix Workspace app, you might experience intermittent failures when answering or making a Microsoft Teams call. The following error message appears:
  "Call could not be established." [HDX-38819]

Known issues in 2111

No new issues have been observed in this release.

Known issues in 2109.1

No new issues have been observed in this release.

Known issues in 2109

- If you have configured the Citrix Workspace app using the `.cr` file, and signed in with your credentials, the home page appears after a delay. [RFMAC-9990]
- If a Progressive Web App (PWA) that is protected is opened on macOS, the *App Protection* policies aren't enforced. [RFMAC-10128]

- After you add stores in the Citrix Workspace app and change the **Current Reauthentication Period** in **Reauthentication Period for Workspace App** and switch from on-premises to the cloud store after a few minutes, you are signed out of the cloud store and an authentication prompt appears. Once you sign in to the Citrix Workspace app, the spinner appears indefinitely and you are unable to sign in. [RFMAC-10140]

Known issues in 2108.1

No new issues have been observed in this release.

Known issues in 2108

When you start a subscribed SaaS app after changing the authentication domain in the server console, the session does not start and the following error message appears:

“AuthDomain has changed. Please sign in again after some time” [RFMAC-9616]

Known issues in 2107

When you change the authentication domain in the server console and sign in with your credentials, the following error message appears:

“Cannot connect to the server”

You can access the store once you click **OK**. [RFMAC-9494]

Known issues in 2106

A black window appears when you share your screen. [HDX-30083]

Known issues in 2104

No new issues have been observed in this release.

Known issues in 2102

No new issues have been observed in this release.

Known issues in 2101

- Attempts to access files under Network Shares from within Citrix Workspace app for Mac might fail even when the option is enabled. [RFMAC-7272]

- On macOS Big Sur, attempts to launch the web SAML single sign-on app on Citrix Workspace app for Mac might fail, displaying the following error message.

  ```
  Page could not load. Please try again later or contact your administrator
   for assistance. Incident ID:-202
  ```

  [RFMAC-7282]

Known issues in 2012

- When you start a video call, Microsoft Teams might become unresponsive, displaying a `Citrix HDX not connected` error. As a workaround, restart Microsoft Teams or the VDA. [RFMAC-6727]
- Video calls on Microsoft Skype for Business are not supported on macOS Big Sur (11.0.1).
- On macOS Big Sur (11.0.1), attempts to connect USB devices might fail, causing the session to exit unexpectedly. As a workaround, reconnect the USB device. [RFMAC-7079]

Third-party notices

Citrix Workspace app might include third-party software licensed under the terms defined in the following document:

Citrix Workspace app for Mac Third-Party Notices

Native support for Apple silicon [Technical preview]

August 9, 2022

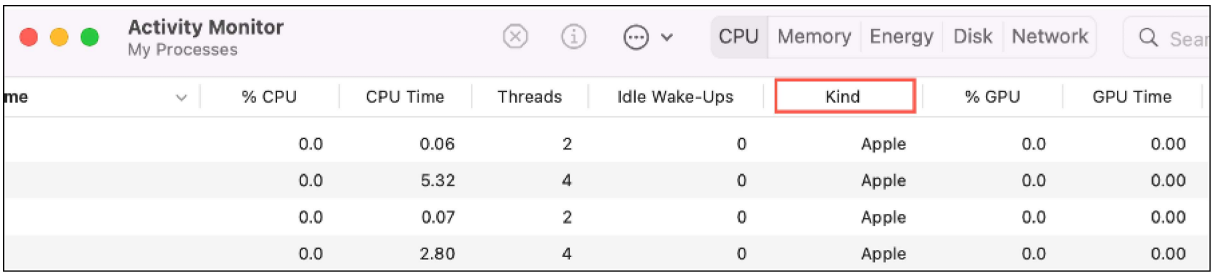
Native support for Apple silicon (M1 chip) - Universal architecture

Citrix Workspace app for macOS now natively supports Macs with Apple silicon (M1 chip). By default, the technical preview build runs natively on Macs with Apple silicon and it must be installed and tested on Macs using M1 chips. You can download the universal architecture build from the **Citrix Workspace App for macOS (Apple silicon) - Universal Architecture** section at Downloads.

> **Note:**
>
> Citrix continues to support Intel-based Macs that use the Rosetta 2 dynamic binary translator. However, Citrix will soon deprecate the Citrix Workspace app for Mac that uses Rosetta emulation. Keep a look out for an announcement in the Deprecation section.

If you are using Citrix Workspace app on a Mac running Apple silicon (M1 chip), you must upgrade the HDX RealTime Optimization Pack (RTOP) by installing the HDX RealTime Media Engine 2.9.500 for Mac from the Citrix website at Downloads.

To determine if the Citrix Workspace app is running natively on Apple silicon, open **Activity monitor** on your Mac. The column titled **Kind** in the **CPU** tab indicates whether the Workspace app is running on Apple Silicon or Intel processor.



Uninstall the universal architecture build and install the Citrix Workspace app for an Intel-based Mac

You can switch to the Citrix Workspace app for an Intel-based Mac by uninstalling the universal architecture build. To uninstall the Citrix Workspace app, see the Uninstall section.

Once you've uninstalled the app, download the latest version of the Citrix Workspace app for an Intel-based Mac from Citrix Downloads and follow the steps listed in the section Manual install.

Citrix Virtual Channel SDK

The Citrix Virtual Channel software development kit (VCSDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) is used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- The Windows Monitoring API, which enhances the visual experience and support for third-party applications integrated with ICA.
- Working source code for virtual channel sample programs to demonstrate programming techniques.

The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

Load Custom Virtual Channels on Macs with Apple silicon (M1 chip)

As an end-user, you can load the Custom Virtual Channel SDK (VCSDK) successfully on a Mac with the M1 chipset. With universal architecture, you must load the VCSDK on Macs with Apple silicon by recompiling your Custom Virtual Channels using the latest VCSDK on M1 chipset device. You can download the universal architecture build from the **Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture** section at Downloads.

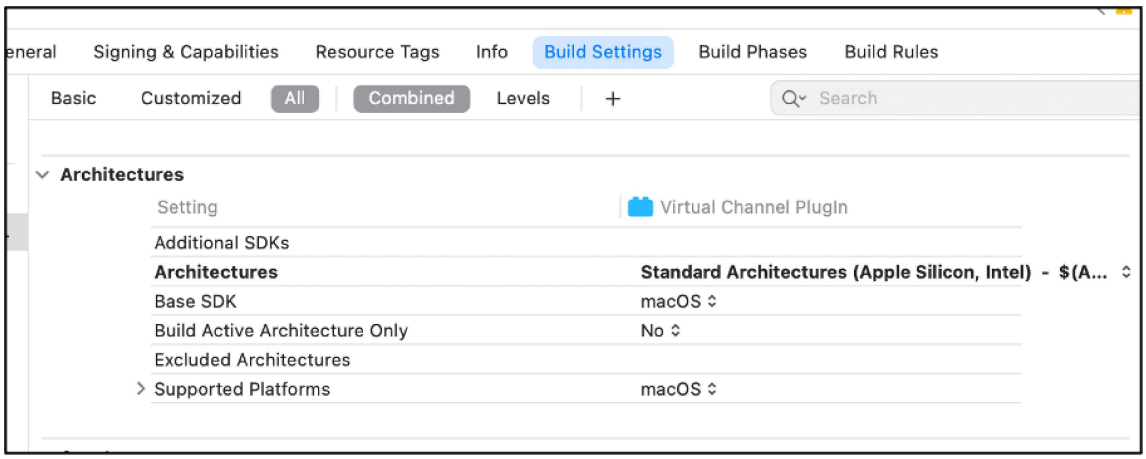
To load the VCSDK, do the following:

1. Download Virtual Channel SDK 2204 for macOS from Downloads.
2. Open your Custom Virtual Channel project in Xcode.
3. Change your code.
4. Compile your Custom Virtual Channel to generate the virtual channel bundle.

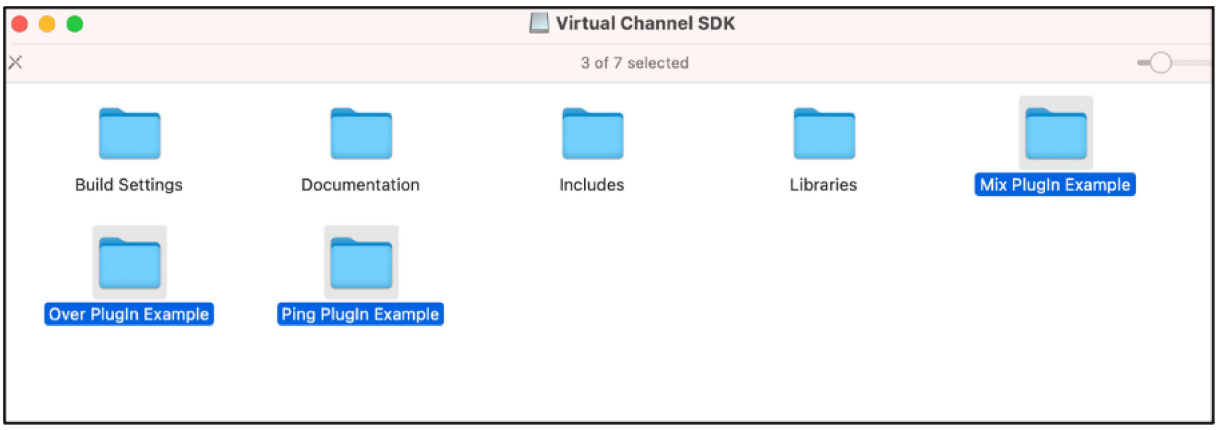
Test your Virtual Channel Software Development Kit (VCSDK)

If you're using the Citrix Virtual Channel Software Development Kit (VCSDK), you must make some changes so your customized virtual channels run correctly. To test your VCSDKs, do the following:

1. Ensure that all the linked libraries of your customized virtual channels are compiled for Universal Binary.
2. Change the Project file to support Universal Binary:
    - Open **Project** > **Build Settings**.
    - Set **Architectures** to **Standard Architectures**.



Examples for the VCSDK can be found inside *VCSDK.dmg*. These examples support Apple's Universal macOS Binary that runs natively on both Apple silicon and Intel-based Mac computers, because it contains executable code for both architectures. You can use these examples as a reference.



> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It's advised that Beta builds aren't deployed in production environments.

System requirements and compatibility

August 24, 2022

Supported operating systems

Citrix Workspace app for Mac supports the following operating systems:

- macOS Monterey (up to 12.5.1)
- macOS Big Sur 11
- macOS Catalina 10.15

Compatible Citrix products

Citrix Workspace app is compatible with all the currently supported versions of Citrix Virtual Apps and Desktop, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), and Citrix Gateway as listed in the Citrix Product Lifecycle Matrix.

Compatible browsers

Citrix Workspace app for Mac is compatible with the following browsers:

- Google Chrome
- Microsoft Edge
- Safari

Hardware requirements

- 1 GB of free disk space
- A working network or Internet connection to connect to servers

Connections, Certificates, and Authentication

Connections

Citrix Workspace app for Mac supports the following connections to Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service):

- HTTPS
- ICA-over-TLS

Citrix Workspace app for Mac supports the following configurations:

For LAN connections	For secure remote or local connections
StoreFront using StoreFront services or Citrix Receiver for website;	Citrix Gateway 12.x-13.x, including VPX

Certificates

Private (Self-signed) certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the user device. Then, you can successfully access Citrix resources using Citrix Workspace app for Mac.

> **Note:**
>
> When the remote gateway's certificate can't be verified upon connection, an untrusted certificate warning appears, as the root certificate isn't included in the local keystore. When a user continues to add a store, the store addition fails. However, on the web browser, the user might be able to authenticate to the store but connections to sessions fail.

Importing root certificates for devices

Obtain the certificate issuer's root certificate and email it to an account configured on your device. When clicking the attachment, you are asked to import the root certificate.

Wildcard certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app for Mac supports wildcard certificates.

Intermediate certificates with Citrix Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be mapped to the Citrix Gateway server certificate. For information on this task, see Citrix Gateway documentation. For more information about installing, linking, and updating certificates, see How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway.

Server Certificate Validation Policy

Citrix Workspace app for Mac has a stricter validation policy for server certificates.

> **Important**
>
> Before installing this version of Citrix Workspace app for Mac, confirm that the server or gateway certificates are correctly configured as described here. Connections can fail if:
>
> - the server or gateway configuration includes a wrong root certificate
> - the server or gateway configuration does not include all intermediate certificates
> - the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
> - the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Workspace app for Mac uses **all** the certificates supplied by the server (or gateway). Citrix Workspace app for Mac then checks whether the certificates are trusted. If the all the certificates are not trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app for Mac's connection to fail.

Suppose that a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Workspace app for Mac.

Then, Citrix Workspace app for Mac checks that all these certificates are valid. Citrix Workspace app for Mac also checks that it already trusts the "Root Certificate". If Citrix Workspace app for Mac does not trust the "Root Certificate", the connection fails.

> **Important**
>
> Some certificate authorities have more than one root certificate. If you require this stricter validation, ensure that your configuration uses the appropriate root certificate. For example, there are currently two certificates ("DigiCert"/"GTE CyberTrust Global Root," and "DigiCert Baltimore Root"/"Baltimore CyberTrust Root") that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available ("DigiCert Baltimore Root"/"Baltimore CyberTrust Root"). If you configure "GTE CyberTrust Global Root" at the gateway, Citrix Workspace app for Mac connections on those user devices fail. Consult the certificate authority's documentation to determine which root certificate must be used. Root certificates eventually expire, as do all certificates.
>
> **Note**
>
> Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

Now suppose that a gateway is configured with these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Then, Citrix Workspace app for Mac uses these two certificates. It then searches for a root certificate on the user device. If it finds a trusted certificate that validates correctly, such as "Example Root Certificate", the connection succeeds. Otherwise, the connection fails. This configuration supplies the intermediate certificate that Citrix Workspace app for Mac needs, but also allows Citrix Workspace app for Mac to choose any valid, trusted, root certificate.

Now suppose that a gateway is configured with these certificates:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Wrong Root Certificate"

A web browser might ignore the wrong root certificate. However, Citrix Workspace app for Mac does not ignore the wrong root certificate, and the connection fails.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- "Example Server Certificate"
- "Example Intermediate Certificate 1"

- “Example Intermediate Certificate 2”

> **Important**
>
> Some certificate authorities use a cross-signed intermediate certificate, intended for situations when there is more than one root certificate. An earlier root certificate is still in use at the same time as a later root certificate. In this case, there are at least two intermediate certificates. For example, the earlier root certificate “Class 3 Public Primary Certification Authority” has the corresponding cross-signed intermediate certificate “Verisign Class 3 Public Primary Certification Authority - G5.” However, a corresponding later root certificate “Verisign Class 3 Public Primary Certification Authority - G5” is also available, which replaces “Class 3 Public Primary Certification Authority.” The later root certificate does not use a cross-signed intermediate certificate.
>
> **Note**
>
> The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By). This distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such “Example Intermediate Certificate 2”).

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- “Example Server Certificate”
- “Example Intermediate Certificate”

Avoid configuring the gateway to use the cross-signed intermediate certificate, as it selects the earlier root certificate:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Example Cross-signed Intermediate Certificate” [not recommended]

It is not recommended to configure the gateway with only the server certificate:

- “Example Server Certificate”

In this case, if Citrix Workspace app for Mac cannot locate all the intermediate certificates, the connection fails.

Authentication

For connections to StoreFront, Citrix Workspace app for Mac supports the following authentication methods:

Authentication method	Workspace for Web using browsers	StoreFront Services site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes		
Domain	Yes	Yes	Yes*	Yes*
Domain pass-through				
Security token			Yes*	Yes*
Two-factor authentica-tion (domain with security token)			Yes*	Yes*
SMS			Yes*	Yes*
Smart card	Yes	Yes	Yes*	Yes
User certificate			Yes	Yes (Citrix Gateway Plug-in)

*Available only for deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

Install, Uninstall, and Upgrade

July 18, 2022

Citrix Workspace app for Mac contains a single installation package and supports remote access through Citrix Gateway, and Secure Web Gateway.

You can install Citrix Workspace app for Mac in any of the following ways:

- From the Citrix website
- Automatically from Workspace for Web

- Using an Electronic Software Distribution (ESD) tool.

By default, the Citrix Workspace app is installed in the **Applications** directory. The installation paths are as follows:

- Full install - `"/Applications/Citrix\ Workspace.app/"`
- Citrix Workspace app for Mac executable - `"/Applications/Citrix\ Workspace.app/Contents/MacOS/Citrix\ Workspace"`

Manual install

By a user from Citrix.com

As a first-time user, you can download Citrix Workspace app for Mac from Citrix.com or your own download site. You can then set up an account by entering an email address instead of a server URL. Citrix Workspace app for Mac determines the Citrix Gateway or StoreFront server associated with the email address. Then it prompts the user to log on and continue the installation. This feature is referred to as email-based account discovery.

> **Note:**
>
> A first-time user is a user who does not have Citrix Workspace app for Mac installed on their user device.

Email-based account discovery for a first-time user does not apply if you have downloaded from a location other than Citrix.com (such as a Citrix Receiver for website).

If your site requires the configuration of Citrix Workspace app for Mac, use an alternate deployment method.

Using an Electronic Software Distribution (ESD) tool

A first-time Citrix Workspace app for Mac user must enter a server URL to set up an account.

From Citrix Downloads page

You can install Citrix Workspace app for Mac from a network share, or directly on to the user device. You can install the app by downloading the file from the Citrix website at Downloads.

To install Citrix Workspace app for Mac:

1. Download the .dmg file for the version of Citrix Workspace app for Mac that you want to install from the Citrix website.
2. Open the downloaded file.
3. On the Introduction page, click **Continue**.

4. On the **License** page, click **Continue**.
5. Click **Agree** to accept the terms of the License Agreement.
6. On the **Installation Type** page, click **Install**.
7. On the **Add Account** page, select **Add Account** and then click **Continue**.
8. Enter the user name and password of an administrator on the local device.

Uninstall

You can now simply drag or move the Citrix Workspace app icon into the bin to completely uninstall the Citrix Workspace app for Mac. To uninstall the Citrix Workspace app, do the following:

1. Close the Citrix Workspace app, if it's running.
2. Drag the Citrix Workspace app to the bin.
   Alternatively, you can right-click on the Citrix Workspace app and select **Options** > **Move to Bin**.
3. Provide your system credentials when prompted.
4. Close all running apps (Citrix Workspace) and click **Continue** to confirm.
   The Citrix Workspace app and all its system files are deleted from your device.

You can also uninstall Citrix Workspace app for Mac manually by opening the .dmg file. Select **Uninstall Citrix Workspace App** and follow the on-screen instructions. The .dmg file is the file that is downloaded from Citrix when installing Citrix Workspace app for Mac for the first time. If the file is no longer on your computer, download the file again from Citrix Downloads to uninstall the application.

Upgrade

Citrix Workspace app for Mac sends you notifications when there is an update available for an existing version or an upgrade to a newer version. For more information about automatic updates, see Automatic update.

You can upgrade Citrix Workspace app for Mac from any of the previous versions of Citrix Workspace app for Mac. For more information about updating the app manually, see Manual update.

When you upgrade to a newer version of Citrix Workspace app for Mac, the previous version is uninstalled automatically. You don't need to restart your machine.

Update

February 15, 2022

Manual update

To manually update the Citrix Workspace app for Mac, download and install the latest version of the app from the Citrix Downloads page.

Automatic update

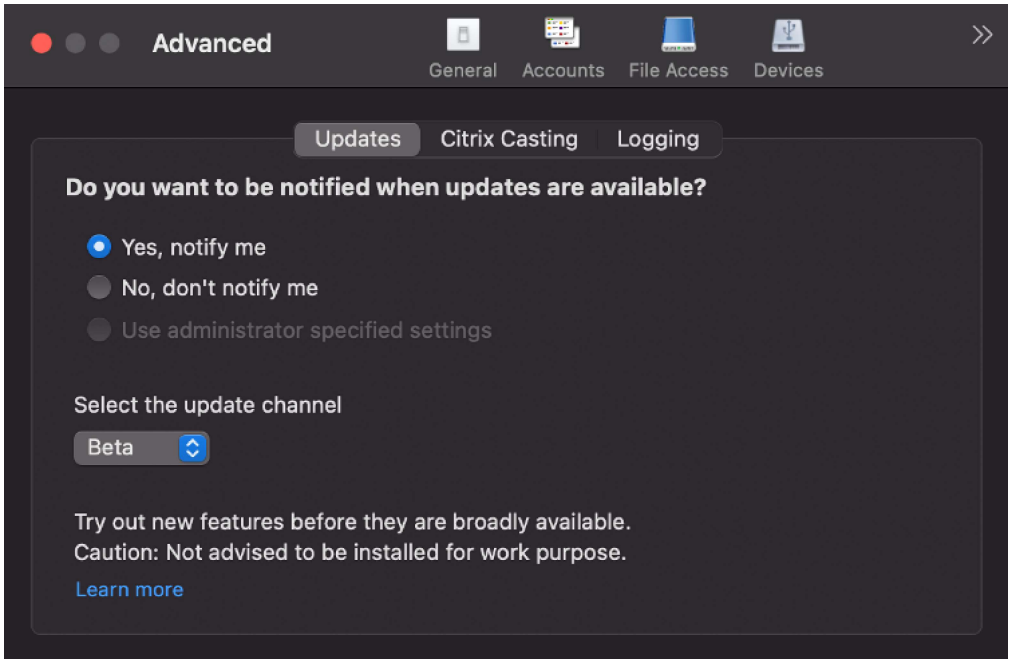
When a new version of the Citrix Workspace app releases, Citrix pushes the update on the system that has the Citrix Workspace app installed. You are notified of the available update.

> **Note:**
>
> - If you've configured an SSL intercepting outbound proxy, add an exception to the Workspace auto-update signature service `https://citrixupdates.cloud.com/` and the download location `https://downloadplugins.citrix.com/` to receive updates from Citrix.
> - Your system must have an internet connection to receive updates.
> - Workspace for web users cannot download the StoreFront policy automatically.
> - Citrix HDX RTME for macOS is included in Citrix Workspace Updates. You are notified of the available HDX RTME update on the Citrix Workspace app.
> - Starting with Version 2111, Citrix Workspace updates log paths are modified. The Workspace updates logs are present at `/Library/Logs/Citrix Workspace Updater`. For information about collecting logs, see Log collection section.

Installing Citrix Workspace app Beta program

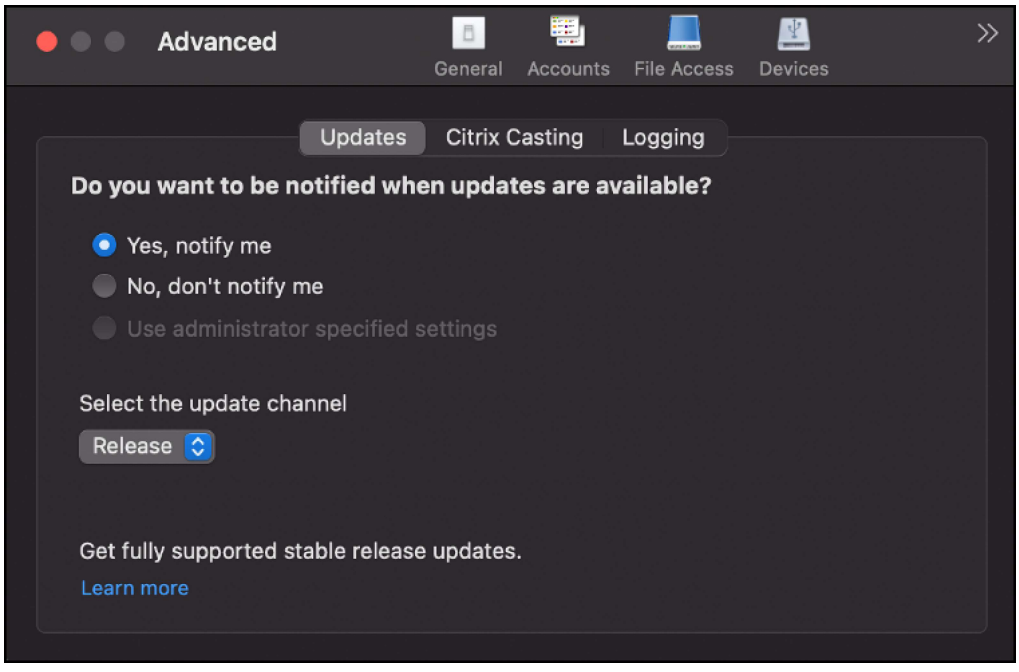
You receive an update notification when the Citrix Workspace app is configured for automatic updates. To install the Beta build on your system, perform the following steps:

1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Beta** from the drop-down list, when the Beta build is available.



To switch from a Beta build to a Release build, perform the following steps:

1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Release** from the **Select the update channel** drop-down list.



> **Note:**
>
> Beta builds are available for customers to test in their non-production or limited production en-

> vironments, and to share feedback. Citrix does not accept support cases for beta builds but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that you do not deploy Beta builds in production environments.

Advanced configuration for automatic updates (Citrix Workspace Updates)

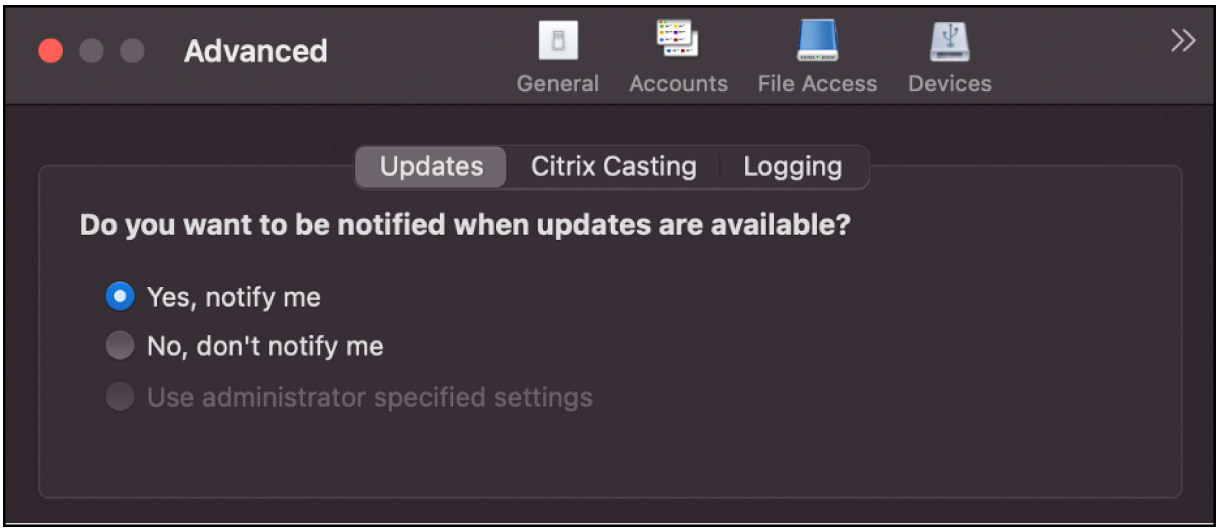
You can configure Citrix Workspace updates using the following methods:

1. GUI
2. StoreFront

Configure Citrix Workspace updates using the GUI

Individual users can override the Citrix Workspace updates setting using the **Advanced** preferences dialog, which is a per-user configuration and the settings apply only to the current user. To configure the update using the GUI, perform the following steps:

1. Select the Citrix Workspace app helper icon on your Mac.
2. From the drop-down list, select **Preferences** > **Advanced**.
3. Select the update notification preference and close the window.



Configure Citrix Workspace updates using StoreFront

1. Use a text editor to open the `web.config` file, which is typically in the `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Locate the user account element in the file (Store is the account name of your deployment).

   For example: `<account id=... name="Store">`

Before the </account> tag, navigate to the properties of that user account:

```
<properties>
       <clear/>
 </properties>
 <!--NeedCopy-->
```

3. Add the auto-update tag after <*clear* /> tag.

```
<account>

    <clear />

    <account id=”d1197d2c-ac82-4f13-9346-2ee14d4b0202” name=”
       F84Store”

      description=”” published=”true” updaterType=”Citrix”
         remoteAccessType=”None”>

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef=”1__Citrix_F84Store”>

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>

            <properties>

              <property name=”Auto-Update-Check” value=”auto” />
```



```
32
33                <property name="Auto-Update-DeferUpdate-Count" value
                     ="1" />
34
35                <property name="Auto-Update-Rollout-Priority" value=
                     "fast" />
36
37                    </properties>
38
39           </metadata>
40
41         </annotatedServiceRecord>
42
43       </annotatedServices>
44
45       <metadata>
46
47         <plugins>
48
49           <clear />
50
51         </plugins>
52
53         <trustSettings>
54
55           <clear />
56
57         </trustSettings>
58
59         <properties>
60
61           <clear />
62
63         </properties>
64
65       </metadata>
66
67     </account>
68
69 <!--NeedCopy-->
```

The meaning of the properties and their possible values are detailed as follows:

- **Auto-update-Check:** Indicates that Citrix Workspace app detects an update automatically when available.

- **Auto-update-Rollout-Priority:** Indicates the delivery period in which you can receive the update.
- **Auto-update-DeferUpdate-Count:** Indicates the number of times that you can defer the notifications for the release updates.

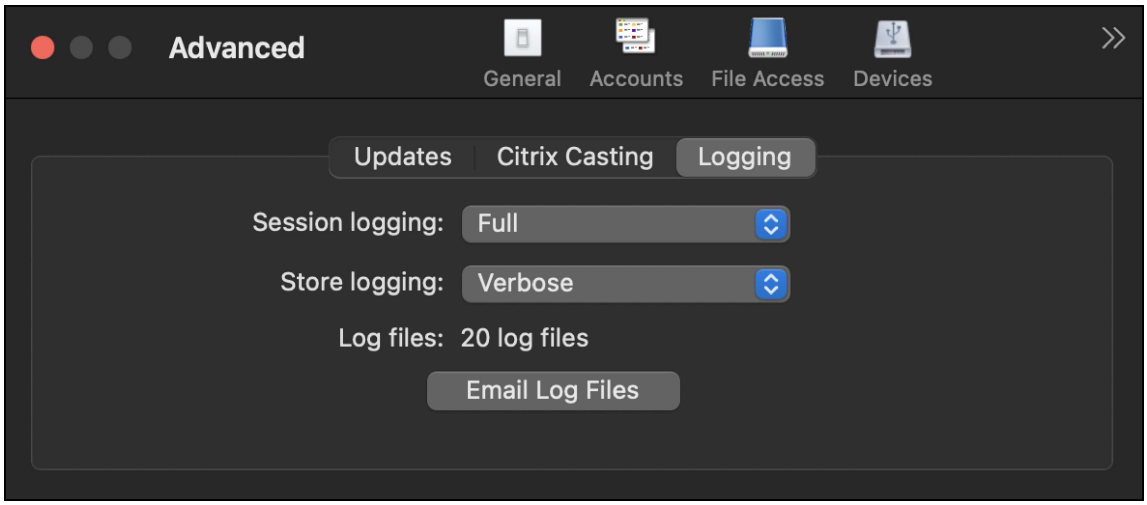
Log collection

Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, provide support.

You can collect logs using the GUI.

Collecting logs:

1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Logging**.



4. Select one of the following session log levels:
   - **Disabled (Default)**: Minimum logs are collected for basic troubleshooting.
   - **Connection Diagnostics**: Identifies errors while connecting. All logging is enabled up until the point when the session is deemed successful.
   - **Full**: Captures everything including the connection diagnostics. Once enabled, the Citrix Workspace app will store up to 10 session logs after which they are deleted starting with the oldest to maintain 10 logs.

> **Note:**
>
> Selecting the **Full** logging option can impact performance and must be used only while troubleshooting an issue because of the amount of data. Do not enable full logging during

> normal use. Enabling this level of logging triggers a warning dialog that must be acknowledged for you to continue.

5. Select one of the following store log levels:
   - **Disabled (Default)**: Minimum logs are collected for basic troubleshooting.
   - **Normal**: Only store communication logs are collected.
   - **Verbose**: Detailed authentication and store communication logs are collected.
6. Click **Email Log Files** to collect and share logs as a .zip file.

Configure

June 29, 2022

After the Citrix Workspace app for Mac software is installed, the following configuration steps allow users to access their hosted applications and desktops.

Users might connect from the Internet or from remote locations. For those users, configure the authentication through Citrix Gateway.

Administrator tasks and considerations

This article discusses the tasks and considerations that are relevant for administrators of Citrix Workspace app for Mac.

> **Important:**
>
> If you are running macOS 10.15, ensure that your system is compliant with Apple's requirements for trusted certificates in macOS 10.15. Perform this check before you upgrade to Citrix Workspace app for Mac version 2106.

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.

You can enable traffic and communication to LaunchDarkly in the following ways:

Enable traffic to the following URLs

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com

List IP addresses in an allow list

If you must list IP addresses in an allow list, for a list of all current IP address ranges, see LaunchDarkly public IP list. You can use this list to ensure that your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Statuspage page.

LaunchDarkly system requirements

Ensure that the apps can communicate with the following services if you have split tunneling on Citrix ADC set to **OFF** for the following services:

- LaunchDarkly service.
- APNs listener service

Sentry

Sentry is used to collect app logs to analyze issues and crashes to improve product quality. Citrix does not collect or store any other personal user information or use Sentry for feature analytics data. For more information about Sentry, go to [https://sentry.io/welcome/].

Content Collaboration Service integration

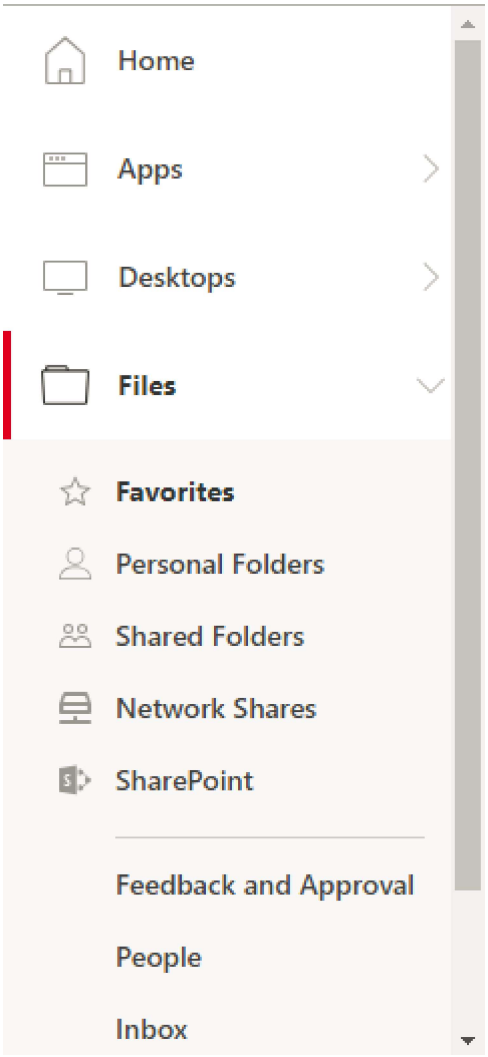
Citrix Content Collaboration enables you to easily and securely exchange documents, send large documents by email, securely handle document transfers to third parties, and access a collaboration space.

Citrix Content Collaboration provides many ways to work, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

You can access Citrix Content Collaboration functionality from the Citrix Workspace app using the **Files** tab displayed within Citrix Workspace app. You can view the **Files** tab only if Content Collaboration Service is enabled in the Workspace configuration in the Citrix Cloud console.

> **Note:**
>
> Windows Server 2012 and Windows Server 2016 don't support Citrix Content Collaboration integration due to a security option set in the operating system.

The following image displays the example contents of the **Files** tab of the new Citrix Workspace app:



Limitations

- Resetting Citrix Workspace app does not cause Citrix Content Collaboration to log off.
- Switching stores in Citrix Workspace app does not cause Citrix Content Collaboration to log off.

USB redirection

HDX USB device redirection enables redirection of USB devices to and from a user device. A user can connect a flash drive to a local computer and access it remotely from a virtual desktop or a desktop

hosted application.

During a session, users can plug and play devices, including Picture Transfer Protocol (PTP) devices. For example:

- Digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players
- Point-of-sale (POS) devices, and other devices such as 3D Space Mice, Scanners, Signature Pads and so on.

> **Note:**
>
> Double-hop USB is not supported for desktop hosted application sessions.

USB redirection is available for the following:

- Windows
- Linux
- Mac

By default, USB redirection is allowed for certain classes of USB devices, and denied for others. To restrict the types of USB devices made available to a virtual desktop, update the list of USB devices supported for redirection. More information is provided later in this section.

> **Tip**
>
> Where security separation between the user device and server is needed, ensure that you inform users about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide superior performance and bandwidth efficiency over a WAN. Optimized virtual channels are usually the best option, especially in high latency environments.

> **Note:**
>
> For USB redirection purposes, Citrix Workspace app for Mac handles a SMART board the same as a mouse.

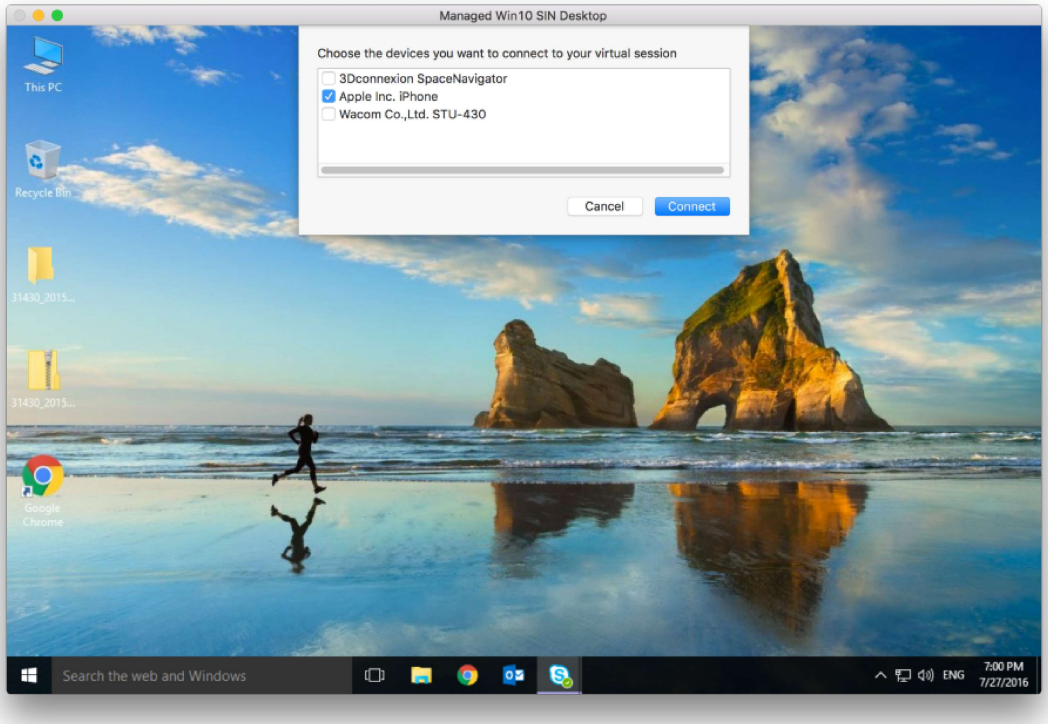
The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports. For example, a CDM virtual channel is used to view files on a camera or to provide audio to a headset. The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, might not work as expected with the optimized virtual channel. Use the Generic USB virtual channel as an alternative.

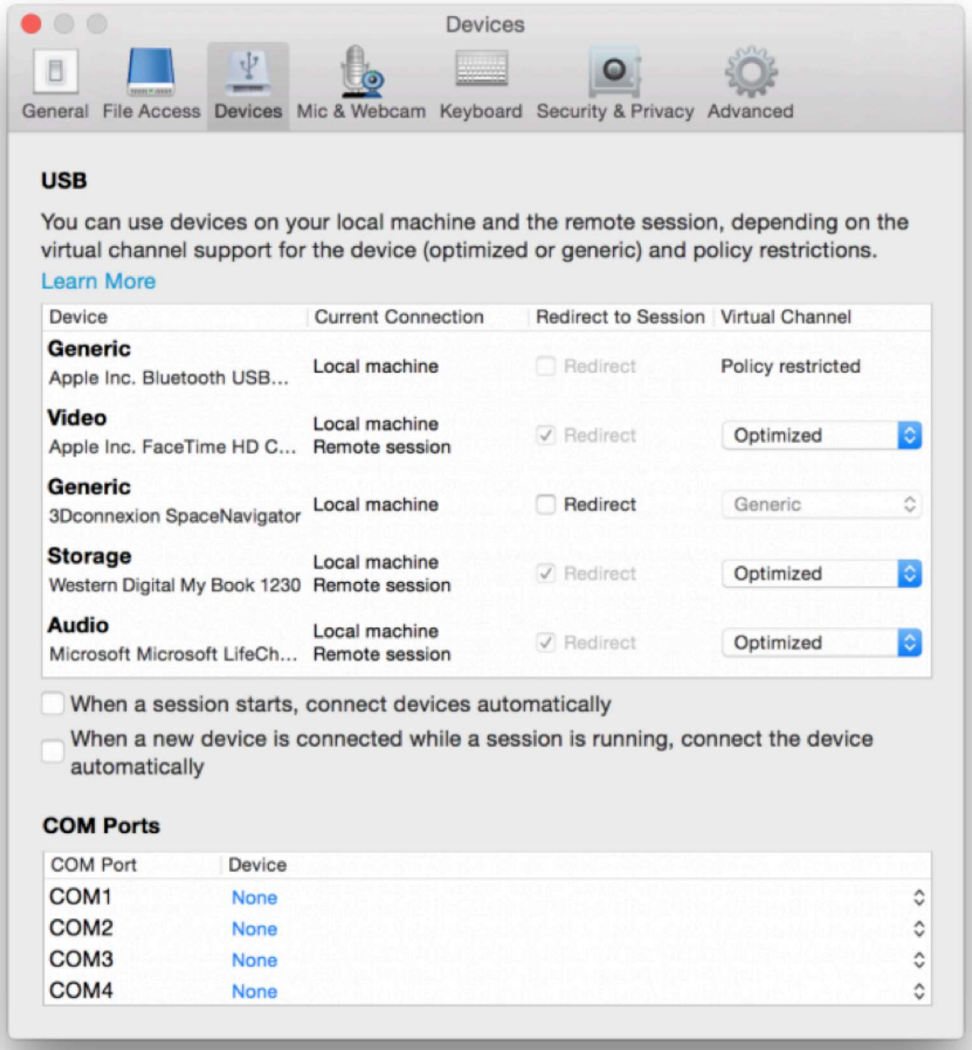
Certain devices are not redirected by default, and are only available to the local session. For example, it would not be appropriate to redirect a NIC that is directly attached via internal USB.

To use USB redirection:

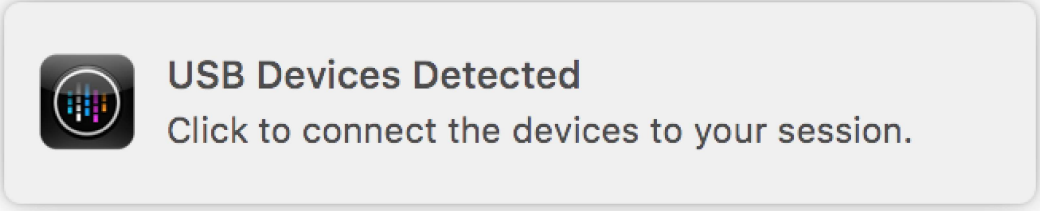
1. Connect the USB device to the device where Citrix Workspace app for Mac is installed.
2. You are prompted to select the available USB devices on your local system.



3. Select the device you want to connect and click **Connect**. If the connection fails, an error message appears.
4. In the **Preferences** window **Devices** tab, the connected USB device is listed in the USB panel:



5. Select the type of virtual channel (Generic or Optimized) for the USB device.
6. A message is displayed. Click to connect the USB device to your session:



Use and remove USB devices

Users can connect a USB device before or after starting a virtual session. When using Citrix Workspace app for Mac, the following apply:

- Devices connected after a session starts immediately appear in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, sometimes you can resolve the problem by waiting to connect the device until after the virtual session has started.
- To avoid data loss, use the **Windows Safe** removal menu before removing the USB device.

Supported USB devices

With Apple announcing the deprecation of Kernel Extensions (KEXT), Citrix Workspace app for Mac migrated to the new user mode USB framework `IOUSBHost` provided by Apple. This article lists the supported USB devices.

USB devices that are compatible with USB redirection

The following USB devices work seamlessly with USB redirection:

- 3DConnexion SpaceMouse
- Mass Storage Devices
- Kingston DataTraveler USB Flash Drive
- Seagate external HDD
- Kingston/Transcend Flash drive 32 GB/64 GB
- NIST PIV smartcard /reader
- YubiKey

USB devices that fail with USB redirection

The following device is not compatible with USB redirection:

- Transcend SSD external Hard disk

Unverified USB Devices

There are plenty of devices, unverified by Citrix, for successful USB redirection with Citrix Workspace app for Mac. Here are some of these devices:

- Other Hard Disks
- Special Keys on the keyboard and headsets that use custom HID protocol

Support for Mass Storage devices

We have seen that not all types of Mass Storage devices can be redirected successfully. For the devices which fail to redirect, there is an optimized virtual channel called Client Drive mapping. Using the Client Drive mapping, access to the mass storage devices can be controlled through the policies on the delivery controller.

Support for Isochronous devices

Generic USB redirection doesn't support Isochronous class of USB devices in Citrix Workspace app for Mac. Isochronous mode of data transfer in a USB specification indicates devices that stream the timestamped data at a constant rate. For example: WebCams, USB Headphones, and so on

Support for Composite devices

A USB composite device is a single gadget that can perform more than one function. For example: multi-function printers, iPhone, and so on. Currently, Citrix Workspace app for Mac does not support redirection of composite devices to the Citrix Virtual Apps and Desktops and Citrix DaaS session.

Alternatives for unsupported USB devices

There are optimized virtual channels that can handle devices that are not supported with generic USB redirection. These virtual channels are optimized for speed when compared to generic USB redirection. Some examples are as follows:

- **Webcam redirection:** Optimized for raw webcam traffic. Microsoft Teams Optimization Pack has its own method of webcam redirection. Hence, it does not fall under the Webcam redirection virtual channel.
- **Audio redirection:** Optimized to transfer Audio streams.
- **Client Drive Mapping:** Optimized for redirecting mass storage devices to the Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session. For example: Flash Drives, Hard Disks, DVD ROM/RW, and so on.

Enlightened Data Transport (EDT)

By default, EDT is enabled in Citrix Workspace app for Mac.

Citrix Workspace app for Mac reads the **EDT** settings as set in the default.ica file and applies it accordingly.

To disable EDT, run the following command in a terminal:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```


Session reliability and auto client reconnect

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application that they are using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes until connectivity resumes on the other side of the tunnel. Session reliability reconnects users without reauthentication prompts.

> **Important**
>
> - Citrix Workspace app for Mac users cannot override the server setting.
> - With Session reliability enabled, the default port used for session communication switches from 1494 to 2598.

You can use session reliability with Transport Layer Security (TLS).

> **Note**
>
> TLS encrypts only the data sent between the user device and Citrix Gateway.

Using session reliability policies

The **session reliability connections** policy setting allows or prevents session reliability.

The **session reliability timeout** policy setting has a default of 180 seconds, or three minutes. Though you can extend the time the session reliability keeps a session open, this feature is convenient to the user. Therefore, it does not prompt the user for reauthentication.

> **Tip**
>
> Extending session reliability timeouts might cause a user to get distracted and walk away from the device, leaving the session accessible to unauthorized users.

By default, incoming session reliability connections use port 2598, unless you change the port number in the session reliability port number policy setting.

You can configure the **Auto client reconnect authentication policy** setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes, or disconnects, the user session after the amount of time you specify in the **Session reliability timeout policy** setting. After that, the auto client reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

> **Note**
>
> Session reliability is enabled by default at the server. To disable this feature, configure the policy

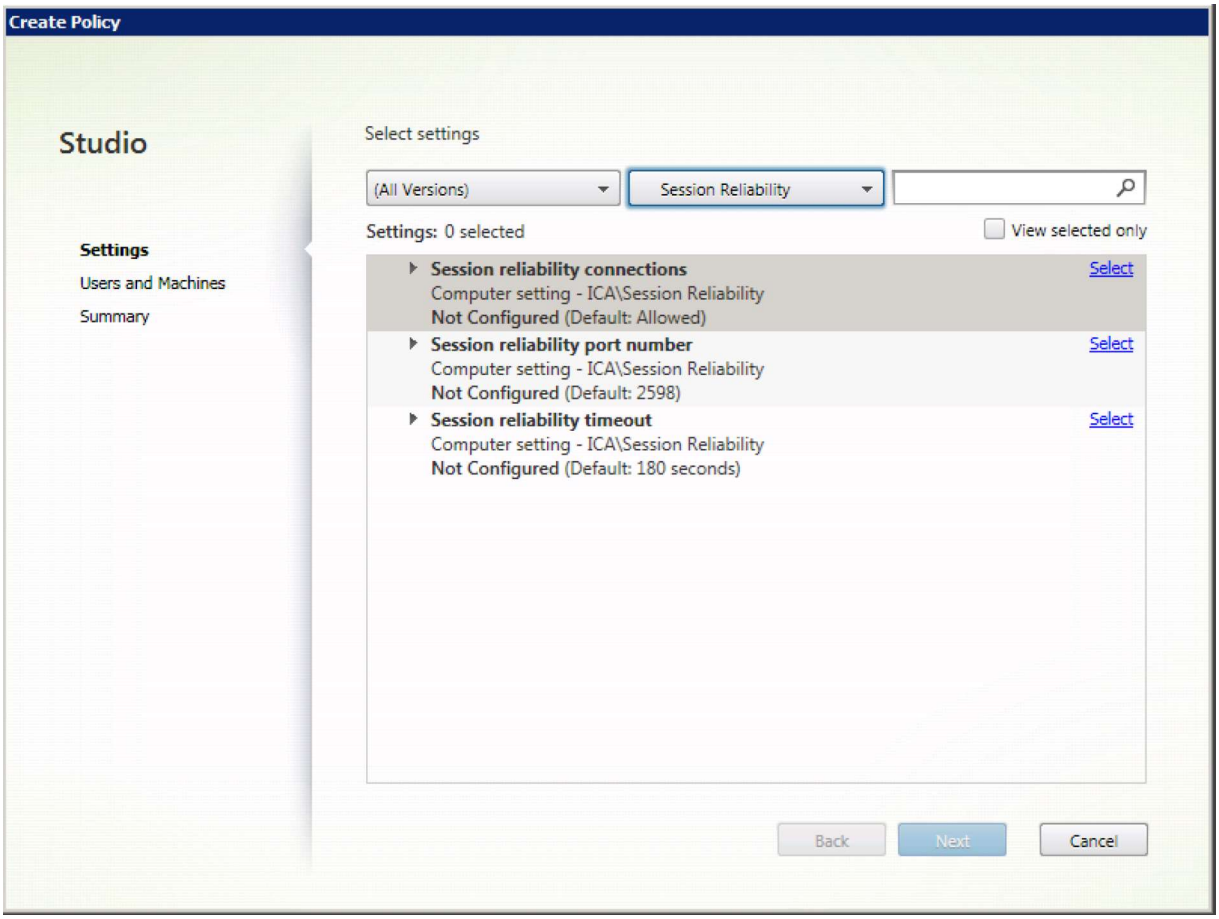
> managed by the server.

Configuring session reliability from Citrix Studio

By default, session reliability is enabled.

To disable session reliability:

1. Launch Citrix Studio.
2. Open the **Session Reliability connections** policy.
3. Set the policy to **Prohibited**.



Configuring session reliability timeout

By default, the session reliability timeout is set to 180 seconds.

> **Note:**
>
> Session reliability timeout policy can be configured only with XenApp and XenDesktop 7.11 and later.

To modify session reliability timeout:

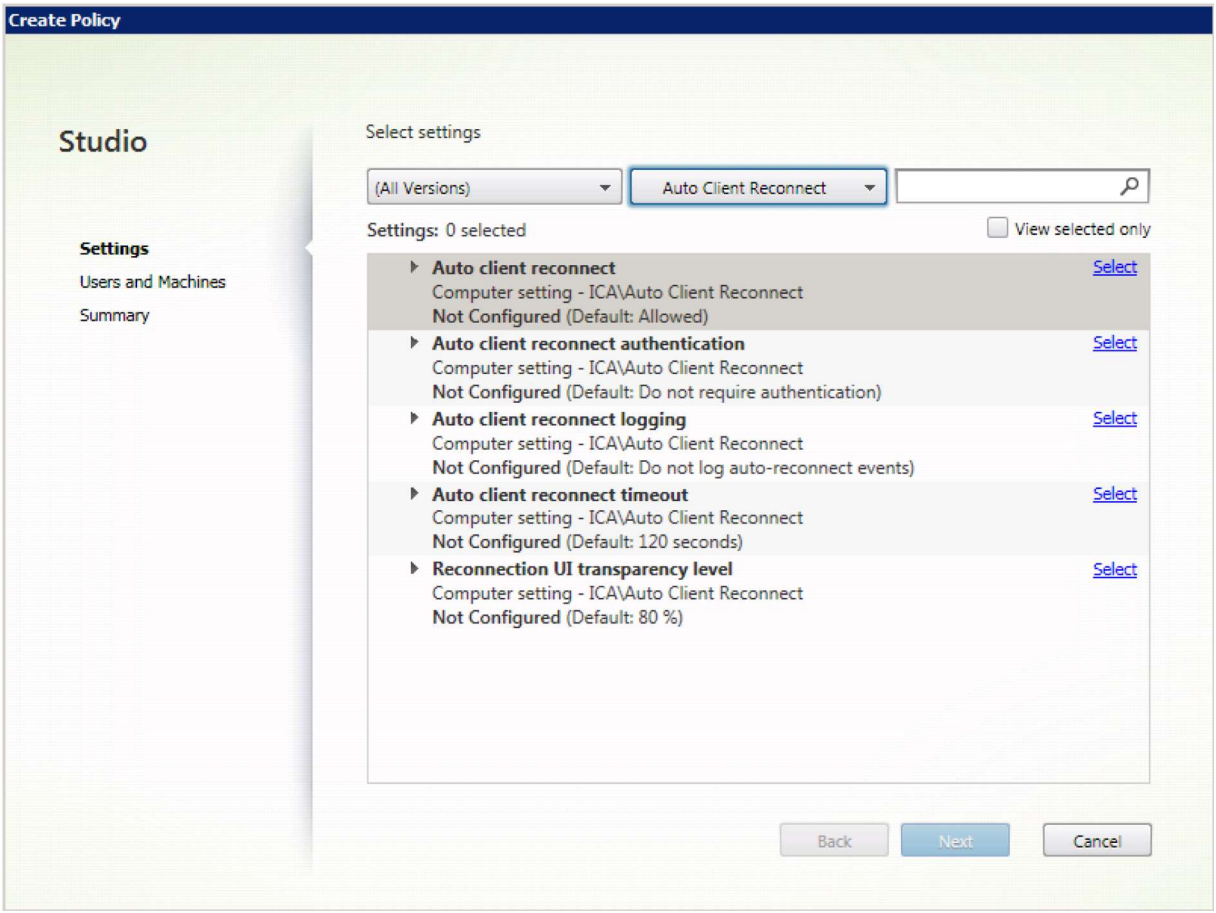
1. Launch Citrix Studio.
2. Open the **Session reliability timeout** policy.
3. Edit the timeout value.
4. Click **OK**.

Configuring auto client reconnection using Citrix Studio

By default, auto client reconnection is enabled.

To disable auto client reconnection:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect policy**.
3. Set the policy to **Prohibited**.



Configuring Auto client reconnection timeout

By default, the Auto client reconnection timeout is set to 120 seconds.

> **Note:**
>
> Auto client reconnect timeout policy can be configured only with XenApp and XenDesktop 7.11 and later.

To modify auto client, reconnect timeout:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect** policy.
3. Edit the timeout value.
4. Click **OK**.

> **Limitations:**
>
> On a Terminal Server VDA, Citrix Workspace app for Mac uses 120 seconds as timeout value irrespective of the user settings.

Configuring the Reconnect user interface Transparency

The Session User Interface is displayed during a session reliability and auto client reconnect attempts. The Transparency level of the user interface can be modified using Studio policy.

By default, Reconnect UI Transparency is set to 80%.

To modify Reconnect user interface Transparency level:

1. Launch Citrix Studio.
2. Open the **Reconnect UI Transparency level** policy.
3. Edit the value.
4. Click **OK**.

Auto client reconnect and session reliability interaction

There are mobility challenges associated with switching between various access points, network disruptions, and display timeouts related to latency. These create challenging environments when trying to maintain link integrity for active Citrix Workspace app for Mac sessions. Citrix enhanced session reliability and auto reconnection technologies resolve this issue.

This feature, allows users to reconnect to sessions automatically after recovery from network disruptions. These features, enabled by policies in Citrix Studio, can be used to improve the user experience.

> **Note:**
>
> Auto client reconnection and session reliability timeout values can be modified using the **default.ica** file in StoreFront.

Auto client reconnection

Auto client reconnection can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled. For information about modifying this policy, see the auto client reconnection section earlier in this article.

Use the default.ica file in StoreFront to modify the connection timeout for AutoClienreconnect. By default, this timeout is set to 120 seconds (or two minutes).

Setting	Example	Default
TransportReconnectRetryMaxT	TransportReconnectRetryMaxT	120

Session reliability

Session reliability can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled.

Use the **default.ica** file in StoreFront to modify the connection timeout for session reliability. By default, this timeout is set to 180 seconds (or three minutes).

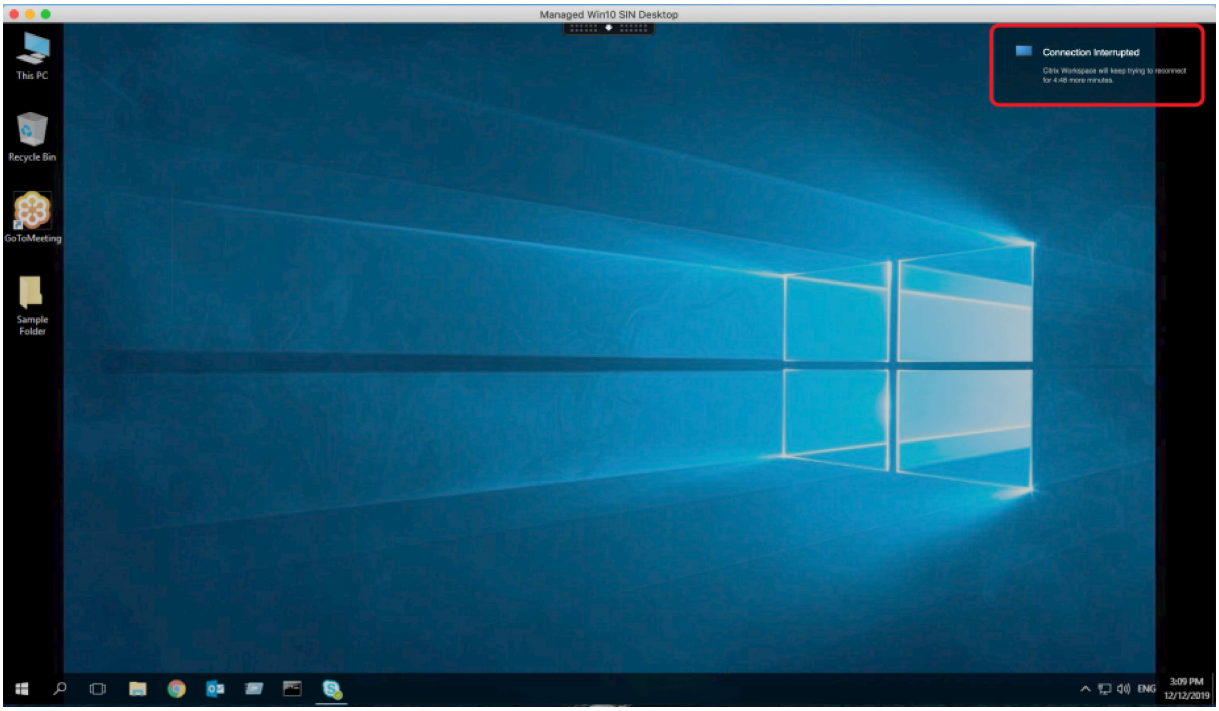
Setting	Example	Default
SessionReliabilityTTL	SessionReliabilityTTL=120	180

How auto client reconnection and session reliability work

When auto client reconnection and session reliability are enabled for a Citrix Workspace app for Mac, consider the following:

- A session window is grayed out when a reconnection is in progress. A countdown timer displays the amount of time remaining before the session is reconnected. Once a session is timed out, it is disconnected.

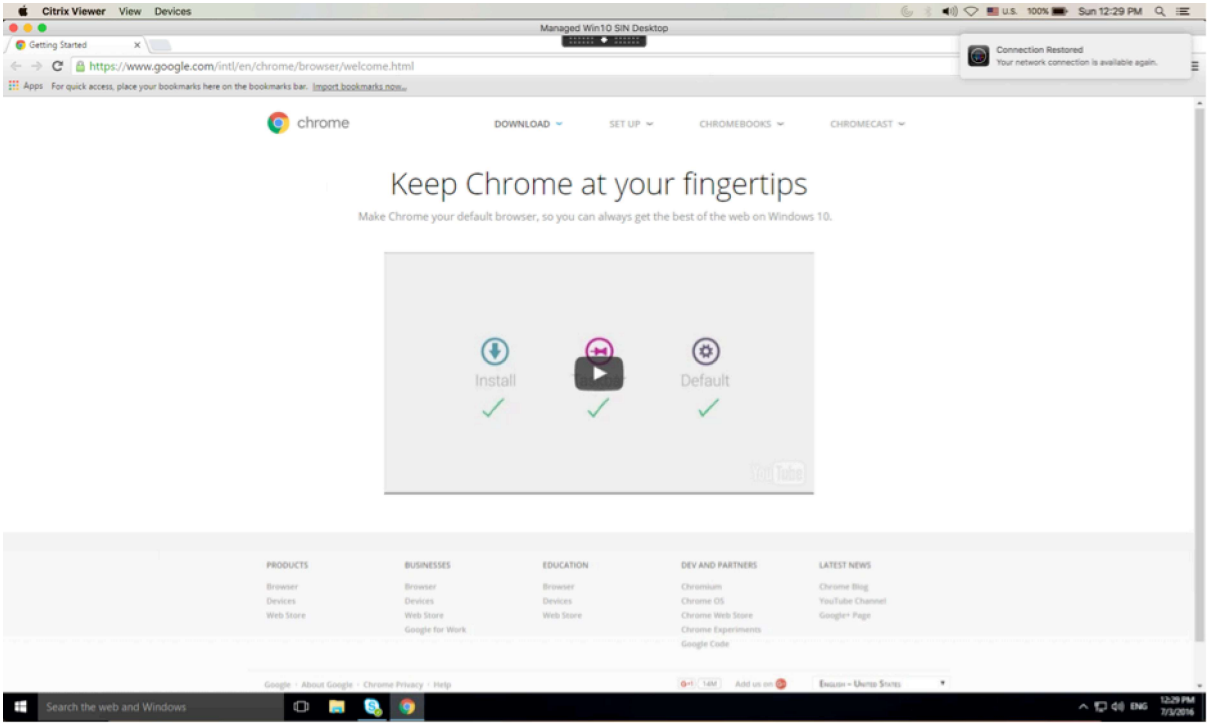
By default, the reconnect countdown notification starts at 5 minutes. This timer value represents the combined default values for each of the timers (auto client reconnection and session reliability), 2 and 3 minutes respectively. The following image illustrates the countdown notification which appears in the upper right portion of the session interface:



Tip

You can alter the grayscale brightness used for an inactive session using a command prompt. For example, defaults write com.citrix.receiver.nomas NetDisruptBrightness 80. By default, this value is set to 80. The maximum value cannot exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

- Users are notified when a session successfully reconnects (or when a session is disconnected). This notification appears in the upper right portion of the session interface:



- A session window which is under auto client reconnect and session reliability control provides an informational message indicating the state of the session connection. Click **Cancel Reconnection** to move back to an active session.

Customer Experience Improvement Program (CEIP)

Data Collected	Description	What we Use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app for Mac and automatically sends the data to Citrix and Google Analytics.	This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app.

Additional Information

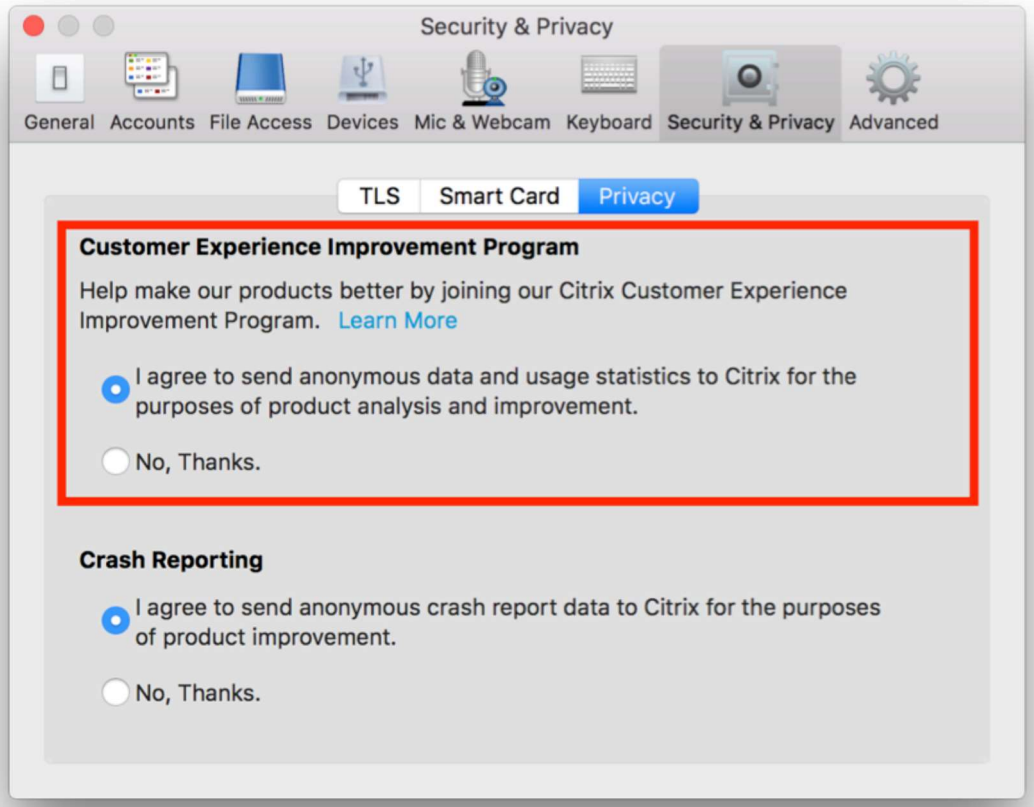
Citrix handles your data in accordance with the terms of your contract with Citrix. Your data is protected, according to Citrix Services Security Exhibit available at the Citrix Trust Center.

Citrix uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. Review

how Google handles data collected for Google Analytics.

To disable sending CEIP data to Citrix and Google Analytics, perform the following steps:

1. In the **Preferences** window, select **Security and Privacy**.
2. Select the **Privacy** tab.
3. Select **No, Thanks** to disable CEIP or to forego participation.
4. Click **OK**.



Alternatively, you can disable CEIP by running the terminal command:

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```

> **Note:**
>
> No data is collected for the users in European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK).

The specific data elements collected by Google Analytics are:

Operating System Version	Workspace app version	Generic USB Redirection Usage	Store configuration
Citrix Workspace Browser Usage	Citrix Virtual Apps and Desktop Session Launch Status	Auto-update preference	Auto-update Status
Session launch method	Uninstall information	Inactivity Timeout Feature Usage	Email Discovery Feature Usage
Custom Web Store Feature Usage	Reconnection preferences	Global App Config Service Usage	Restore Keyboard Usage
Delete Password Feature Usage	Auto-update channel	Connection Lease Details	

Application delivery

When delivering applications with Citrix Virtual Apps and Desktops and Citrix DaaS, consider the following options to enhance the experience for your users when they access their applications:

Web access mode

Without any configuration, Citrix Workspace app for Mac provides web access mode: browser-based access to applications and desktops. Users simply open a browser to a Workspace for Web and select and use the applications that they want. In web access mode, no app shortcuts are placed in the App Folder on your user's device.

Self-service mode

Add a StoreFront account to Citrix Workspace app for Mac or configure Citrix Workspace app for Mac to point to a StoreFront site. Then, you can configure self-service mode, which enables your users to subscribe to applications through Citrix Workspace app for Mac. This enhanced user experience is similar to that of a mobile app store. In self-service mode you can configure mandatory, auto-provisioned, and featured app keyword settings as needed. When one of your users selects an application, a shortcut to that application is placed in the App Folder on the user device.

When they access a StoreFront 3.0 site, your users see the Citrix Workspace app for Mac preview.

When publishing applications on your Citrix Virtual Apps farms, you can enhance the experience for users accessing those applications through StoreFront stores. Ensure that you include meaningful de-

scriptions for the published apps. The descriptions are visible to your users through Citrix Workspace app for Mac.

Configure self-service mode

As mentioned previously, you can add a StoreFront account to Citrix Workspace app for Mac or configure Citrix Workspace app for Mac to point to a StoreFront site. Thus, you can configure the self-service mode, which allows users to subscribe to applications from the Citrix Workspace app for Mac user interface. This enhanced user experience is similar to that of a mobile app store.

In self-service mode, you can configure mandatory, auto-provisioned, and featured app keyword settings as needed.

- Automatically subscribe all users of a store to an app by appending the string `**KEYWORDS:Auto**` to the description, while publishing the app in Citrix Virtual Apps. When users log in to the store, the app is automatically provisioned without the need for manual subscription to the app.
- Advertise applications to users or make commonly used applications easier to find by listing them in the Citrix Workspace app for Mac Featured list. To list apps in the Mac Featured list, append the string `**KEYWORDS:Featured**` to the app description.

For more information, see the StoreFront documentation.

Citrix Workspace Updates

Configuring using the GUI

An individual user can override the **Citrix Workspace Updates** setting using the **Preferences** dialog. This process is a per-user configuration and the settings apply only to the current user.

1. Go to the **Preferences** dialog in Citrix Workspace app for Mac.
2. In the **Advanced** pane, click **Updates**. The Citrix Workspace Updates dialog appears.
3. Select one of the following options:
    - Yes, notify me
    - No, don't notify me
    - Use administrator specified settings
4. Close the dialog box to save the changes.

Configuring Citrix Workspace Updates using StoreFront

Administrators can configure Citrix Workspace Updates using StoreFront. Citrix Workspace app for Mac only uses this configuration for users who have selected "Use administrator specified settings."

To manually configure it, follow these steps.

1. Use a text editor to open the web.config file. The default location is `C:\inetpub\wwwroot\Citrix\Roaming\web.config`
2. Locate the user account element in the file (Store is the account name of your deployment)

   For example: <account id=… name="Store">

   Before the *</account>* tag, navigate to the properties of that user account:

   <properties>

   <clear />
   </properties>
3. Add the auto-update tag after *<clear />* tag.

auto-update-Check

The auto-update check determines that Citrix Workspace app for Mac can detect if updates are available.

Valid values:

- Auto – Is used to get notifications when updates are available.
- Manual – Is used to not get any notification when updates are available. Users must check manually for updates by selecting **Check for Updates**.
- Disabled – Is used to disable Citrix Workspace Updates.

auto-update-DeferUpdate-Count

Determines the number of times the user is notified to upgrade before forcibly updating to the latest version of Citrix Workspace app for Mac. By default, this value is 7.

Valid values:

- -1 – The user gets reminded later when an update is available.
- 0 – Force-updates the user to the latest version of Citrix Workspace app for Mac when the update is available.
- Positive integer – The user is reminded these many times before being forced to update. Citrix recommends not to set this value higher than 7.

auto-update-Rollout-Priority

Determines how quickly a device sees that an update is available.

Valid values:

- Auto – The Citrix Workspace Updates system decides when available updates roll out to users.
- Fast – Available updates roll out to users on high priority as determined by Citrix Workspace app for Mac.
- Medium – Available updates roll out to users on medium priority as determined by Citrix Workspace app for Mac.
- Slow – Available updates roll out to users on low priority as determined by Citrix Workspace app for Mac.

Keyboard layout synchronization

Keyboard layout synchronization enables users to switch among preferred keyboard layouts on the client device when using a Windows or Linux VDA. This feature is disabled by default.

To enable keyboard layout synchronization, go to **Preferences > Keyboard** and select "Use local keyboard layout, rather than the remote server keyboard layout."

> **Note:**
>
> 1. Using the local keyboard layout option activates the client IME (Input Method Editor). Users working in Japanese, Chinese, or Korean can use the server IME. They must disable the local keyboard layout option by clearing the option in **Preferences > Keyboard**. The session will revert to the keyboard layout provided by the remote server when they connect to the next session.
> 2. The feature works in the session only when the toggle in the client is turned on and the corresponding feature enabled on the VDA. A menu item,"**Use Client Keyboard Layout,**" in **Devices** > **Keyboard** > **International** is added to show the enabled state.

Limitations

- Using the keyboard layouts listed in "**Supported Keyboard Layouts in Mac**" works while using this feature. When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality cannot be confirmed.
- Remote apps that run with elevated privileges can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.
- When a user is working within an RDP session, it's not possible to change the keyboard layout using the `Alt + Shift` shortcuts when RDP is deployed as an app. As a workaround, users can use the language bar in the RDP session to switch the keyboard layout.

Keyboard layout support for Windows VDA

Supported keyboard layouts on Mac

Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

Keyboard layout support for Linux VDA

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

By default, the keyboard layout synchronization feature is turned on. To control this feature alone, open the **Config** file in the ~/**Library**/**Application Support**/**Citrix Receiver**/ folder, locate the "**EnableIMEEnhancement**" setting and turn the feature on or off by setting the value to "true" or "false," respectively.

> **Note:**
>
> The setting change takes effect after restarting the session.

Language bar

You can choose to show or hide the remote language bar in an application session using the GUI. The language bar displays the preferred input language in a session. In earlier releases, you might change this setting using only the registry keys on the VDA. Starting with Citrix Workspace for Mac version 1808, you can change the settings using the **Preferences** dialog. The language bar appears in a session by default.

> **Note:**
>
> This feature is available in sessions running on VDA 7.17 and later.

Configure showing or hiding the remote language bar

1. Open Preferences.
2. Click Keyboard.
3. Click or unclick Show the remote language bar for the published applications.

> **Note:**
>
> The setting changes take effect immediately. You can change the settings in an active session. The remote language bar does not appear in a session if there is only one input language.

Citrix Casting

Citrix Casting is used to cast your Mac screen to nearby Citrix Ready workspace hub devices. Citrix Workspace app for Mac supports Citrix Casting to mirror your Mac screen to workspace hub connected monitors.

For more information, see the Citrix Ready workspace hub documentation.

Prerequisites

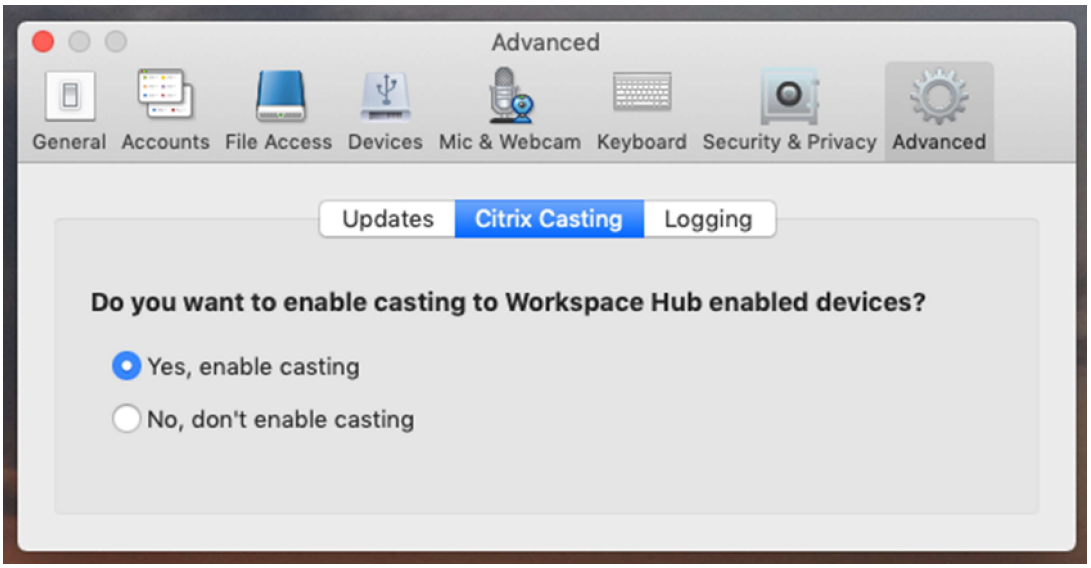
- Latest supported version of Citrix Workspace app.
- Bluetooth enabled on the device for hub discovery.

- Both Citrix Ready workspace hub and Citrix Workspace app must be on the same network.
- Ensure Port 55555 isn't blocked between the device running Citrix Workspace app and the Citrix Ready workspace hub.
- Port 55556 is the default port for SSL connections between mobile devices and the Citrix Ready workspace hub. You can configure a different SSL port on the Raspberry Pi's settings page. If the SSL port is blocked, users cannot establish SSL connections to the workspace hub.
- For Citrix Casting, ensure port 1494 isn't blocked.

Enable Citrix Casting

Citrix Casting is disabled by default. To enable Citrix Casting using Citrix Workspace app for Mac:

1. Go to **Preferences**.
2. Select **Advanced** in the panel and then choose **Citrix Casting**.
3. Select **Yes, enable casting**.



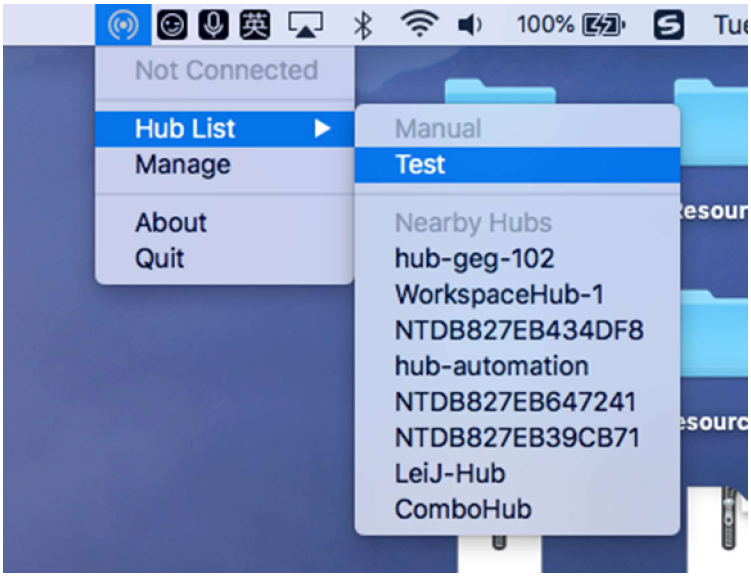
A notification appears when Citrix Casting is launched and a Citrix Casting icon appears in the menu bar.

> **Note:**
>
> After enabling, Citrix Casting launches with Citrix Workspace app for Mac automatically every time until you disable it by selecting **No, don't enable casting** in **Preferences > Advanced > Citrix Casting**.

Discover workspace hub devices automatically

To connect to workspace hubs automatically:

1. On your Mac, sign in to Citrix Workspace app and ensure that Bluetooth is turned on. Bluetooth is used to discover nearby workspace hubs.
2. Select the **Citrix Casting** icon in the menu bar. All Citrix Casting functions are operated through this menu.
3. The **Hub List** submenu shows all nearby workspace hubs on the same network. Hubs are listed in descending order by their proximity to your Mac and display their workspace hub configured names. All automatically discovered hubs display under **Nearby Hubs**.
4. Choose the hub you want to connect to by selecting its name.



To cancel selection of a workspace hub during connection, select **Cancel**. You can also use **Cancel** if the network connection is poor and connecting is taking longer than usual.

> **Note:**
>
> Occasionally, your chosen hub might not appear in the menu. Check the **Hub List** menu again after a few moments or add your hub manually. Citrix Casting receives the workspace hub's broadcasting periodically.

Discover workspace hub devices manually

If you cannot find the Citrix Ready workspace hub device in the **Hub List** menu, add the workspace hub's IP address to access it manually. To add a workspace hub:

1. On your Mac, sign in to Citrix Workspace app and ensure that Bluetooth is turned on. Bluetooth is used to discover nearby workspace hubs.
2. Select the **Citrix Casting** icon in the menu bar.
3. Select **Manage** in the menu. The **Manage hubs** window appears.
4. Click **Add new** to enter the IP address of your hub.

5. After successfully adding the device, the **Hub name** column displays the hub's friendly name. Use this name to identify the hub in the **Manual** section of the **Hub List** submenu.

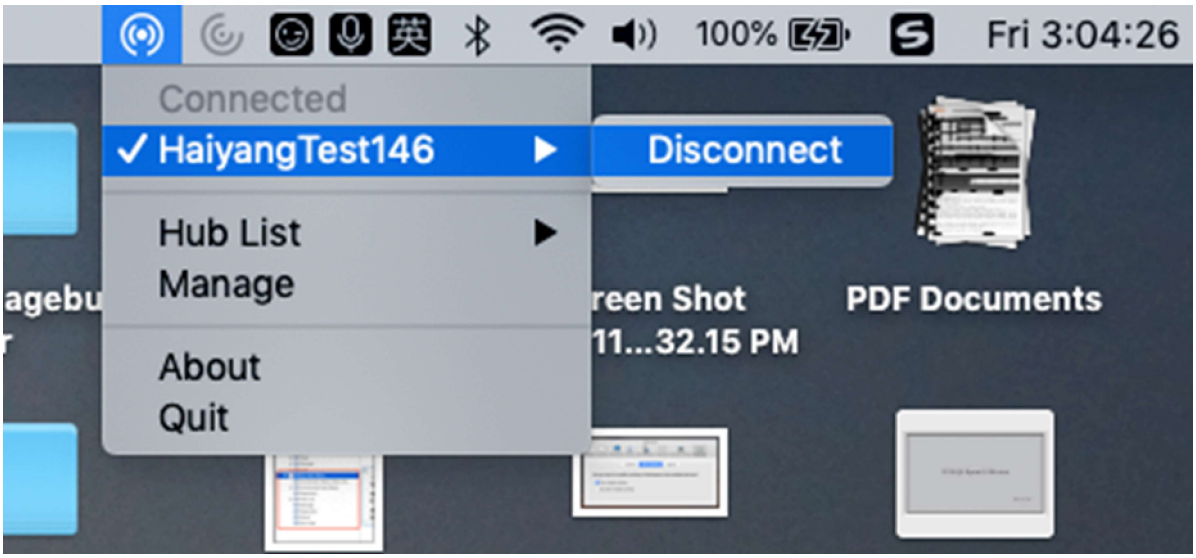
> **Note:**
>
> Currently, only **Mirror** mode is supported. **Mirror** is the only available choice in the **Display Mode** column.

Disconnect the workspace hub device

You can disconnect your current session and exit the Citrix Ready workspace hub automatically or manually.

- To disconnect the screen casting session automatically, close your laptop.
- To disconnect the screen casting session manually:

1. Select the **Citrix Casting** icon.
2. In the list of hubs, select the name of your workspace hub. The **Disconnect** option appears to the right.
3. Select **Disconnect** to exit the hub.



Known issues

- There are small latency issues when viewing the mirrored screen. In poor network conditions, latency might be even longer.
- When SSL is enabled in a Citrix Ready workspace hub and the hub's certificate is not trusted, an alert window appears. To solve the issue, add the certificate to your trusted certificate list with the Keychain tool.

Client-side microphone input

Citrix Workspace app for Mac supports multiple client-side microphone inputs. Locally installed microphones can be used for:

- Live events, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Digital dictation support is available with Citrix Workspace app for Mac.

You can use microphones attached to your device by choosing one of the following options from the **Mic & Webcam** settings in **Citrix Workspace app for Mac** > **Preferences**:

- Use my microphone and webcam
- Don't use my microphone and webcam
- Ask me each time

If you select **Ask me each time**, a dialog box appears each time you connect asking whether you want to use your microphone in that session.

Windows special keys

Citrix Workspace app for Mac provides several options and easier ways to substitute special keys such as function keys in Windows applications with Mac keys. Use the **Keyboard** tab to configure the options you want to use, as follows:

- "Send Control character using" lets you choose whether to send Command-character keystroke combinations as Ctrl+character key combinations in a session. Select "Command or Control" from the pop-up menu to send familiar Command-character or Ctrl-character keystroke combinations on the Mac as Ctrl+character key combinations to the PC. If you select Control, you must use Ctrl-character keystroke combinations.
- "Send Alt character using" lets you choose how to replicate the Alt key within a session. If you select Command-Option, you can send Command-Option and keystroke combinations as Alt+ key combinations within a session. Alternatively, if you select Command, you can use the Command key as the Alt key.
- "Send Windows logo key using Command (right)". Lets you send the Windows logo key to your remote desktops and applications when you press the Command key on the right side of the keyboard. If this option is disabled, the right Command key has the same behavior as the left Command key according to the above two settings in the preferences panel. However, you can still send the Windows logo key using the Keyboard menu; choose **Keyboard > Send Windows Shortcut >** Start.
- "Send special keys unchanged" lets you disable the conversion of special keys. For example, the combination Option-1 (on the numeric keypad) is equivalent to the special key F1. You can

change this behavior and set this special key to represent 1 (the number one on the keypad) in the session. To do this, select the “Send special keys unchanged” check box. By default, this check box is not selected so Option-1 is sent to the session as F1.

You send the function and other special keys to a session using the **Keyboard** menu.

If your keyboard includes a numeric keypad, you can also use the following keystrokes:

PC key or action	Mac options
INSERT	0 (the number zero) on the numeric keypad. Num Lock must be off; you can turn this on and off using the **Clear** key; Option-Help
DELETE	Decimal point on the numeric keypad. Num Lock must be off; you can turn this on and off using the **Clear** key; Clear
F1 to F9	Option-1 to -9 (the numbers one to nine) on the numeric keypad
F10	Option-0 (the number zero) on the numeric keypad
F11	Option-Minus Sign on the numeric keypad
F12	Option-Plus Sign on the numeric keypad

Windows shortcuts and key combinations

Remote sessions recognize most Mac keyboard combinations for text input, such as Option-G to input the copyright symbol ©. Some keystrokes you make during a session, however, do not appear on the remote application or desktop. The Mac operating system interprets them. This can result in keys triggering Mac responses instead.

You might also want to use certain Windows keys, such as Insert, that many Mac keyboards do not have. Similarly, some Windows 8 keyboard shortcuts display charms and app commands, and snap and switch apps. Mac keyboards do not mimic these shortcuts. However, these can be sent to the remote desktop or application using the **Keyboard** menu.

Keyboards and the ways keys are configured can differ widely between machines. Citrix Workspace app for Mac therefore offers several choices to ensure that keystrokes can be forwarded correctly to hosted applications and desktops. These keystrokes are listed in the table. The default behavior is described. If you adjust the defaults (using the Citrix Workspace app or other preferences), different keystroke combinations might be forwarded and other behavior might be observed on the Remote PC Access.

> **Important**
>
> Certain key combinations listed in the table are not available when using newer Mac keyboards. In most of these cases, keyboard input can be sent to the session using the Keyboard menu.

Conventions used in the table:

- Letter keys are capitalized and do not imply that the Shift key must be pressed simultaneously.
- Hyphens between keystrokes indicate that keys must be pressed together (for example, Control-C).
- Character keys create text input and include all letters, numbers, and punctuation marks. Special keys do not create input by themselves but act as modifiers or Controllers. Special keys include Control, Alt, Shift, Command, Option, arrow keys, and function keys.
- Menu instructions relate to the menus in the session.
- Depending on the configuration of the user device, some key combinations might not work as expected, and alternative combinations are listed.
- Fn refers to the Fn (Function) key on a Mac keyboard. Function key refers to F1 to F12 on either a PC or Mac keyboard.

Windows key or key combination	Mac equivalents
Alt+character key	Command–Option–character key (for example, to send Alt-C, use Command-Option-C)
Alt+special key	Option–special key (for example, Option-Tab); Command–Option–special key (for example, Command-Option-Tab)
Ctrl+character key	Command–character key (for example, Command-C); Control–character key (for example, Control-C)
Ctrl+special key	Control–special key (for example, Control-F4); Command–special key (for example, Command-F4)
Ctrl/Alt/Shift/Windows logo + function key	****Choose Keyboard > Send Function**** key > Control/Alt/Shift/Command-Function key
Ctrl+Alt	Control-Option-Command
Ctrl+Alt+Delete	Control-Option-Fn-Command-Delete; Choose Keyboard > Send Ctrl-Alt-Del
Delete	Delete; Choose Keyboard > Send Key > Delete; Fn-Backspace (Fn-Delete on some US keyboards)

Windows key or key combination	Mac equivalents
End	End; Fn-Right Arrow
Esc	Escape; Choose Keyboard > Send Key > Escape
F1 to F12	F1 to F12; Choose Keyboard > Send Function Key > F1 to F12
Home	Home; Fn-Left Arrow
Insert	Choose Keyboard > Send Key > Insert
Num Lock	Clear
Page Down	Page Down; Fn-Down Arrow
Page Up	Page Up; Fn-Up Arrow
Spacebar	Choose Keyboard > Send Key > Space
Tab	Choose Keyboard > Send Key > Tab
Windows logo	Right Command key (a keyboard preference, enabled by default); Choose Keyboard > Send Windows Shortcut > Start
Key combination to display charms	Choose Keyboard > Send Windows Shortcut > Charms
Key combination to display app commands	Choose Keyboard > Send Windows Shortcut > App Commands
Key combination to snap apps	Choose Keyboard > Send Windows Shortcut > Snap
Key combination to switch apps	Choose Keyboard > Send Windows Shortcut > Switch Apps

Use Input Method Editors (IME) and international keyboard layouts

Citrix Workspace app for Mac allows you to use an Input Method Editor (IME) on either the user device or on the server.

When client-side IME is enabled, users can compose text at the insertion point rather than in a separate window.

Citrix Workspace app for Mac also allows users to specify the keyboard layout they want to use.

To enable client-side IME

1. From the Citrix Viewer menu bar, choose **Keyboard > International > Use Client IME**.
2. Ensure that the server-side IME is set to direct input or alphanumeric mode.
3. Use the Mac IME to compose text.

To indicate explicitly the starting point when composing text

- From the Citrix Viewer menu bar, choose **Keyboard > International > Use Composing Mark**.

To use server-side IME

- Ensure that the client-side IME is set to alphanumeric mode.

Mapped server-side IME input mode keys

Citrix Workspace app for Mac provides keyboard mappings for server-side Windows IME input mode keys that are not available on Mac keyboards. On Mac keyboards, the **Option** key is mapped to the following server-side IME input mode keys, depending on the server-side locale:

Server-side system locale	Server-side IME input mode key
Japanese	Kanji key (Alt + Hankaku/Zenkaku in Japanese keyboard)
Korean	Right-Alt key (Hangul/English toggle on Korean keyboard)

To use international keyboard layouts

- Ensure both client-side and server-side keyboard layouts are set to the same locale as the default server-side input language.

Multiple monitors

Users can set Citrix Workspace app for Mac to work in full-screen mode across multiple monitors.

1. Open the Citrix Viewer.
2. From the menu bar, click **View** and select one of the following options, based on your requirement:
   - **Enter Full Screen** - Full screen on the primary monitor only.
   - **Use All Displays In Full Screen** - Full screen on all connected monitors.

3. Drag the Citrix Virtual Desktops screen between the monitors.

The screen is now extended to all monitors.

Limitations

- Full-screen mode is only supported on one monitor or all monitors, which are configurable through a menu item.
- Citrix recommends using a maximum of 2 monitors. Using more than 2 monitors might degrade session performance or cause usability issues.
- Full screen mode is not available on Macs with a notch.

Desktop toolbar

Users can now access the **Desktop** Toolbar in both windowed and full-screen mode. Previously, the toolbar was only visible in full-screen mode. Other toolbar changes include:

- The **Home** button has been removed from the toolbar. This function can be run by using the following commands:
  - Cmd-Tab to switch to the previous active application.
  - Ctrl-Left Arrow to switch to the previous Space.
  - Using the built-in trackpad or Magic Mouse gestures to switch to a different Space.
  - Moving the cursor to the edge of screen while in full-screen mode displays a Dock where you can choose which applications to make active.
- The **Windowed** button has been removed from the toolbar. Follow one of these methods to switch from full-screen mode to windowed mode:
  - On OS X 10.10, click the green window button on the drop-down menu bar.
  - On OS X 10.9, click the blue menu button on the drop-down menu bar.
  - On all versions of OS X, select **Exit Full Screen** from the **View** menu of the drop-down menu bar.
- Support to drag between windows in full screen with multiple monitors.

Workspace Control

Workspace Control lets desktops and applications follow users as they move between devices. For example, clinicians in hospitals to move from workstation to workstation without having to restart their desktops and applications on each device.

Policies and client drive mappings change appropriately when you move to a new user device. Policies and mappings are applied according to the user device where you are currently logged on to the session. For example, a healthcare worker can sign out from a device in the emergency room and sign-

in to a workstation in the X-ray laboratory. The policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session in the X-ray laboratory.

To configure workspace Control settings

1. Click the down arrow icon in the Citrix Workspace app for Mac window and choose **Preferences**.
2. Click **General** tab.
3. Choose one of the following:
    - Reconnect apps when I start Citrix Workspace app. Allows users to reconnect to disconnected apps when they start Citrix Workspace app.
    - Reconnect apps when I start or refresh apps. Allows users to reconnect to disconnected apps either when they start apps or when they select Refresh Apps from the Citrix Workspace app for Mac menu.

Mapping client drives

Client drive mapping allows you to access local drives on the user device such as CD-ROM drives, DVDs, and USB memory sticks, during sessions. When a server configuration allows client drive mapping, users can access locally stored files and work on them during sessions. Users can also save them either on a local drive or on a drive on the server.

Citrix Workspace app for Mac monitors the directories in which hardware devices such as CD-ROMs, DVDs, and USB memory sticks are typically mounted on the user device and automatically maps any new ones that appear during a session to the next available drive letter on the server.

You can configure the level of read and write access for mapped drives using Citrix Workspace app for Mac preferences.

To configure read and write access for mapped drives

1. On the Citrix Workspace app for Mac home page, click the down arrow icon, and then click **Preferences**.
2. Click **File Access**.
3. Select the level of read and write access for mapped drives from the following options:
    - Read and Write
    - Read only
    - No access
    - Ask me each time
4. Log off from any open sessions and reconnect to apply the changes.

Custom web store

You can access your organization's custom web store from the Citrix Workspace app for Mac. To use this feature, the admin must add the custom web store to the list of allowed URLs in the `allowedWebStoreURLs` property in the Global App Configuration Service.

For more information about configuring web store URLs for end-users, see Global App Configuration Service.

To add a custom web store URL, perform the following steps:

1. Open the Citrix Workspace app and navigate to **Accounts**.
2. In the **Accounts** window, click the **+** icon and type the URL.

To delete a custom web store URL, perform the following steps:

1. Open the Citrix Workspace app and navigate to **Accounts**.
2. In the **Accounts** window, select the account you want to delete and click the **-** icon.

Inactivity Timeout for Citrix Workspace app

The inactivity timeout feature logs you out of the Citrix Workspace app based on a value that the admin sets. Admins can specify the amount of idle time that is allowed before a user is automatically signed out of the Citrix Workspace app. You're automatically signed out when no activity from the mouse, keyboard, or touch occurs for the specified interval of time, within the Citrix Workspace app window. The inactivity timeout does not affect the already running Citrix Virtual Apps and Desktops and Citrix DaaS sessions or the Citrix StoreFront stores.

The inactivity timeout value can be set starting from 1 minute to 1440 minutes. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module. Click here to download the PowerShell modules for Citrix Workspace Configuration.

The end-user experience is as follows:

- A notification appears three minutes before you're signed out, with an option to stay signed in, or sign out. The notification appears if you've enabled Citrix Workspace app notifications in the system preferences of your Mac.
- The notification appears only if the configured inactivity timeout value is greater than 5 minutes. For example, if the configured value is 6 minutes, a notification appears when 3 minutes of inactivity is detected. If the configured inactivity timeout value is less than or equal to 5 minutes, the user is signed out without a notification.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click Sign out to end the session for the current store.

StoreFront to Workspace migration

StoreFront to Workspace URL migration enables you to seamlessly migrate your end users from a StoreFront store to Workspace store with minimal user interaction.

Consider, all your end users have a StoreFront store `storefront.com` added to their Workspace app. As an administrator, you can configure a StoreFront URL to Workspace URL Mapping {'storefront.com':'xyz.cloud.com'} in the Global App Configuration Service. The Global App Config Service pushes the setting to all Citrix Workspace app instances, on both managed and unmanaged devices, that have the StoreFront URL `storefront.com` added.

Once the setting is detected, Citrix Workspace app adds the mapped Workspace URL `xyz.cloud.com` as another store. When the end user launches the Citrix Workspace app, the Citrix Workspace store opens. The previously added StoreFront store `storefront.com` remains added to the Citrix Workspace app. Users can always switch back to the StoreFront store `storefront.com` using the **Switch Accounts** option in the Citrix Workspace app. Admins can control the removal of the StoreFront store `storefront.com` from the Citrix Workspace app at the users' end points. The removal can be done through the global app config service.

To enable the feature, do the following steps:

1. Configure StoreFront to Workspace mapping using the Global App Config Service. For more information on Global App config service, see Global App Configuration Service.
2. Edit the payload in the app config service:

```
{
  "serviceURL": Unknown macro: \{
  "url" }

,
"settings":{

"name":"Productivity Apps", [New Store Name]
"description":"Provides access StoreFront to Workspace Migration",
"useForAppConfig":true,
"appSettings":
{
  "macos":[ Unknown macro: \{
  "category" }

]
 }

 }
```



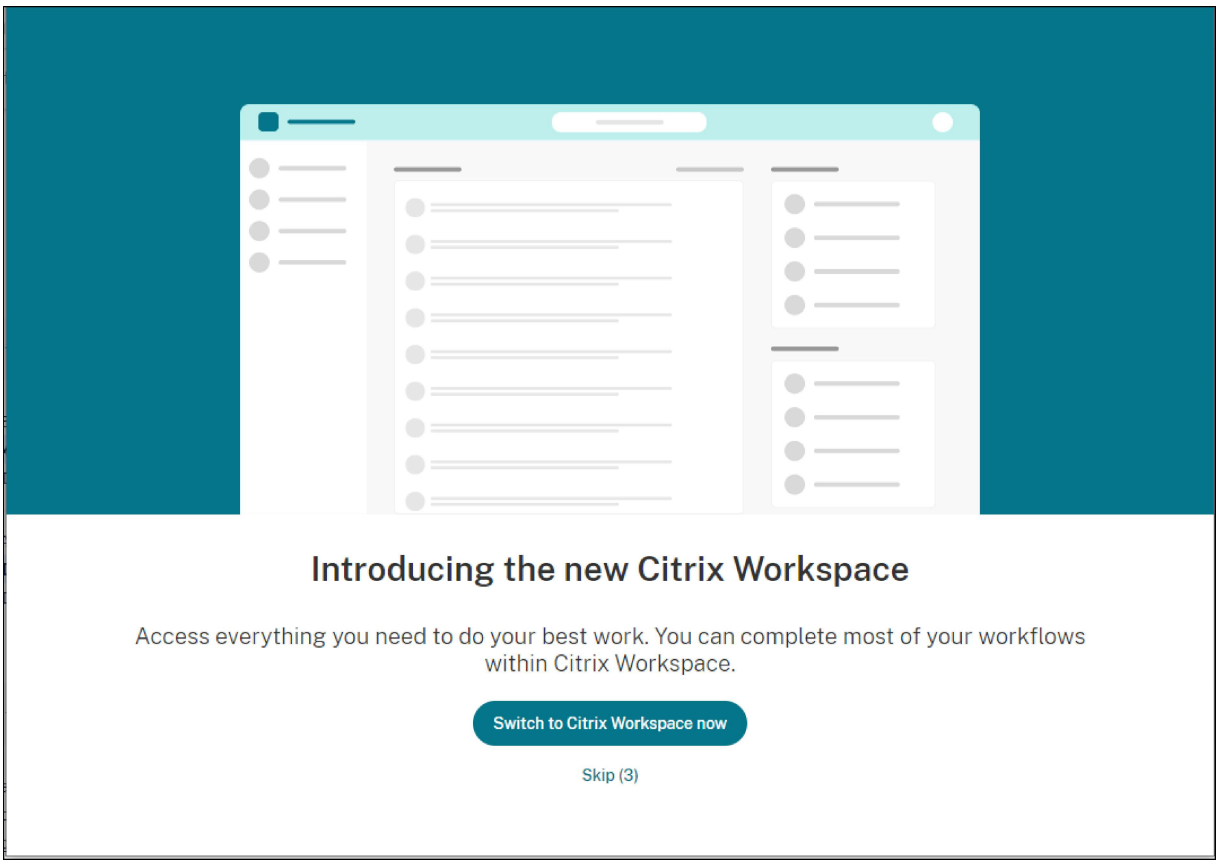
```
20
21   }
22
23 <!--NeedCopy-->
```

> **Note:**
>
> If you're configuring the payload for the first time, use `POST`.
> If you're editing the existing payload configuration, use `PUT` and check that you have the payload that consists of all the supported settings.

3. Specify the StoreFront URL `storefront.com` as the value for **URL** in the **serviceURL** section.
4. Configure the Workspace URL `xyz.cloud.com` inside the section **migrationUrl**.
5. Use **storeFrontValidUntil** to set the timeline for the removal of the StoreFront store from the Citrix Workspace app. This field is optional. You can set the following value based on your requirement:
   - Valid date in the format (YYYY-MM-DD)

     > **Note:**
     >
     > If you have provided a past date, then the StoreFront store is removed immediately upon URL migration. If you have provided a future date, then the StoreFront store is removed on the set date.

Once the app config service settings are pushed, the following screen appears:



When the user clicks **Switch to Citrix Workspace now**, the Workspace URL is added to Citrix Workspace app and the authentication prompt appears. Users have a limited option to delay the transition up to three times.

Microsoft Teams

Encoder performance estimator

The `HdxRtcEngine.exe` is the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection. The `HdxRtcEngine.exe` can estimate the best encoding resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 480p, 720p, and 1080p.

The performance estimation process uses macroblock code to determine the best resolution that can be achieved with the particular endpoint. The Codec negotiation includes the highest possible resolution. The Codec negotiation can be between the peers, or between the peer and the conference server.

There are four performance categories for endpoints that have its own **maximum** available resolution:

Endpoint performance	Maximum resolution	Registry key value
Fast	1080p (1920x1080 16:9 @ 30 fps)	3
Medium	720p (1280x720 16:9 @ 30 fps)	2
Slow	360p (640x360 16:9 @ 30 fps or 640x480 4:3 @ 30 fps)	1
Very slow	240p (320x180 16:9 @ 30 fps or 320x240 4:3 @ 30 fps)	0

To set the video encoding resolution value, to, for example 360p, run the following command from the terminal:

```
defaults write com.citrix.HdxRtcEngine OverridePerformance -int 1
```

For more information about Microsoft Teams optimization, see Optimization for Microsoft Teams.

Printing

You can now use PDF universal printing when printing from a MAC. You no longer need to install the HP Color LaserJet 2800 Series PS driver when auto-creating printers with Universal Print Driver if you chose to use PDF Universal Printing.

PostScript Printing

By default, the auto-redirected client printers are created with the Citrix UPD with PostScript support. For more details, see the support article CTX296662.

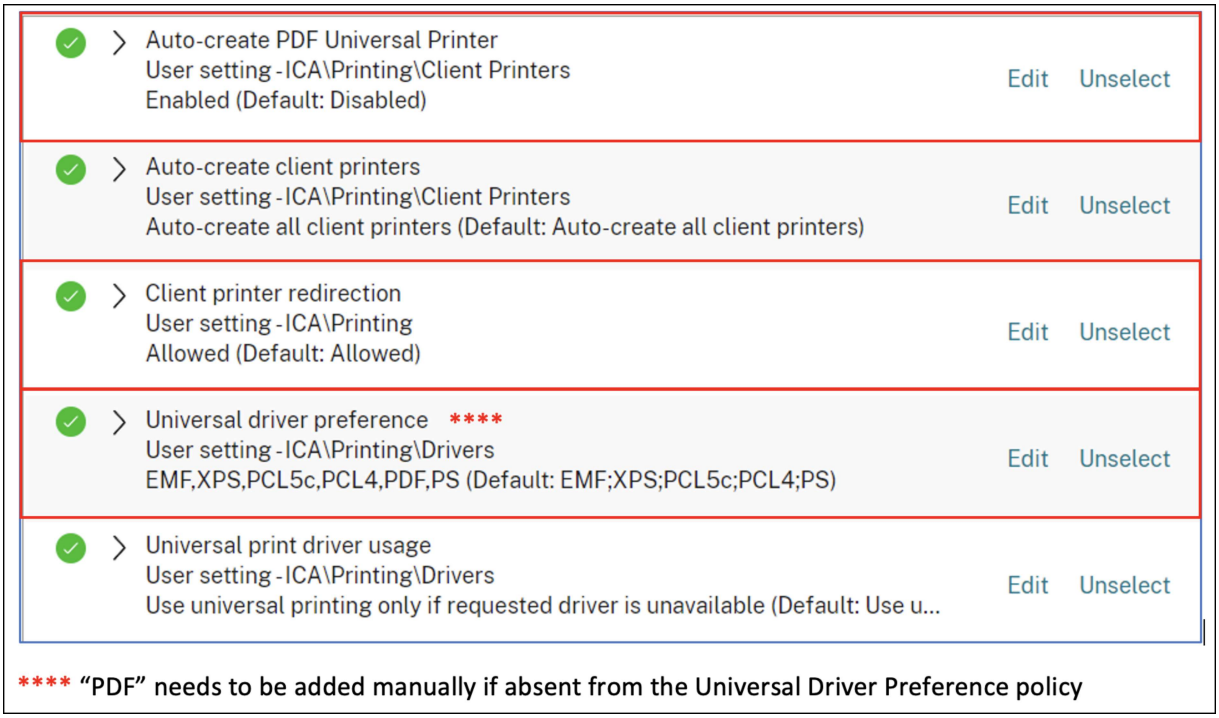
Ensure that the Client printer redirection, the Universal Print Driver Usage, and the Universal print driver priority policies are set to default. Also ensure that you've installed the HP Color LaserJet 2800 Series PS driver on the VDA.
For more information about installing the driver, see the support article CTX140208.

PDF Universal Printing

Prerequisites:

- Citrix Workspace app for Mac version 2112 or later - Enables consumption of PDF print streams for Citrix Workspace app for Mac.
- Citrix Virtual Apps and Desktops version 2112 or later - Enables PDF universal printing for auto-created client printers.

- Enable the Client printer redirection policy in the Citrix Studio or web console.



You can print via PDF once you configure either or both of the following options:

1. Provide a single PDF Universal Printer created in each session.
2. Use the UPD for regular auto-created printers.

Provide a single PDF Universal Printer created in each session

To enable creation of the **PDF Universal Printer** in sessions from a Mac client or any other PDF enabled client endpoint, go to Citrix Studio or the web console and enable the **Auto-Create PDF universal printer** policy.
Once the policy is enabled, the PDF universal printer is created in the session. The printer is called **Citrix PDF Printer**.

Using this printer in a session generates a PDF output that's delivered to the client and handed to the default PDF handling application on the endpoint. For the macOS client, this is typically the built-in **Preview** application, but it could be any registered PDF handling application such as Adobe Acrobat Reader.

Use the UPD for regular auto-created printers

To enable PDF universal printing for all redirected client printers in a session from a Mac client, visit Citrix Studio or a web console and configure the Universal print driver priority policy to place the PDF metafile format in before PS within the priority list.

After you make this change, auto-created printers that use a universal driver with a PDF-capable Mac client uses the Citrix PDF Universal Driver instead of the HP Color LaserJet 2800 Series PS driver on the host.
When using one of the auto-created printers in a session, PDF is used as the intermediate format of the print job; but the print output flows directly to the selected client-attached printer.

Authenticate

June 29, 2022

Smart card

Citrix Workspace app for Mac supports smart card authentication in the following configurations:

- Smart card authentication to Workspace for Web or StoreFront 3.12 and later.
- Citrix Virtual Apps and Desktops 7 2203 and later.
- XenApp and XenDesktop 7.15 and later.
- Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office that allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.
- Citrix Workspace app for Mac supports using multiple certificates with a single smart card or with multiple smart cards. When your user inserts a smart card into a card reader, the certificates are available to all applications running on the device, including Citrix Workspace app for Mac.
- For double-hop sessions, a further connection is established between Citrix Workspace app for Mac and your user's virtual desktop.

About smart card authentication to Citrix Gateway

There are multiple usable certificates when you use a smart card to authenticate a connection. Citrix Workspace app for Mac prompts you to select a certificate. After you select a certificate, Citrix Workspace app for Mac prompts you to enter the smart card password. Once authenticated, the session launches.

If there is only one suitable certificate on the smart card, Citrix Workspace app for Mac uses that certificate and does not prompt you to select it. However, you must still enter the password associated with the smart card to authenticate the connection and to start the session.

Specifying a PKCS#11 module for smart card authentication

> **Note:**
>
> Installing the PKCS#11 module is not mandatory. This section only applies to ICA sessions. It does not apply to Citrix Workspace access to Citrix Gateway or StoreFront where a smart card is required.

To specify the PKCS#11 module for smart card authentication:

1. In Citrix Workspace app for Mac, select **Preferences**.
2. Click **Security & Privacy**.
3. In the **Security & Privacy** section, click **Smart Card**.
4. In the **PKCS#11** field, select the appropriate module. Click **Other** to browse to the location of the PKCS#11 module if the desired one is not listed.
5. After selecting the appropriate module, click **Add**.

Supported readers, middleware, and smart card profiles

Citrix Workspace app for Mac supports most macOS-compatible smart card readers and cryptographic middleware. Citrix has validated the operation with the following.

Supported readers:

- Common USB connect smart card readers

Supported middleware:

- Clarify
- ActivIdentity client version
- Charismathics client version

Supported smart cards:

- PIV cards
- Common Access Card (CAC)
- Gemalto .NET cards

Follow the instructions provided by your vendor's macOS-compatible smart card reader and cryptographic middleware for configuring user devices.

Restrictions

- Certificates must be stored on a smart card, not on the user device.
- Citrix Workspace app for Mac does not save the user certificate choice.
- Citrix Workspace app for Mac does not store or save the user's smart card PIN. OS handles the PIN acquisitions, which might have its own caching mechanism.

- Citrix Workspace app for Mac does not reconnect sessions when a smart card is inserted.
- To use VPN tunnels with smart card authentication, you must install the Citrix Gateway Plug-in and log on through a webpage. Use your smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway Plug-in is not available for smart card users.

Conditional Access with Azure Active Directory

This authentication method is currently not supported on Citrix Workspace app for Mac.

Secure communications

August 23, 2022

To secure the communication between your Site and Citrix Workspace app for Mac, you can integrate your connections with a range of security technologies, including Citrix Gateway. For information about configuring Citrix Gateway with Citrix StoreFront, see the StoreFront documentation.

> **Note:**
>
> Citrix recommends using Citrix Gateway to secure communications between StoreFront servers and users' devices.

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace and servers. Citrix Workspace app for Mac supports SOCKS and secure proxy protocols.
- Citrix Secure Web Gateway. You can use Citrix Secure Web Gateway to provide a single, secure, encrypted point of access through the internet to servers on internal corporate networks.
- SSL Relay solutions with Transport Layer Security (TLS) protocols
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you use a firewall that maps the server's internal IP address to an external internet address such as network address translation (NAT), configure the external address.

> **Note:**
>
> Starting with macOS Catalina, Apple has enforced extra requirements for root CA certificates and intermediate certificates which administrators must configure. For more information, see Apple Support article HT210176.

Citrix Gateway

To enable remote users to connect to your XenMobile deployment through Citrix Gateway, you can configure Citrix Gateway to support StoreFront. The method for enabling access depends on the edition of XenMobile in your deployment.

If you deploy XenMobile in your network, allow connections from internal or remote users to StoreFront through Citrix Gateway, by integrating Citrix Gateway with StoreFront. This deployment allows users to connect to StoreFront to access published applications from XenApp and virtual desktops from XenDesktop. Users connect through Citrix Workspace app for Mac.

Connecting with the Citrix Secure Web Gateway

If the Citrix Secure Web Gateway Proxy is installed on a server in the secure network, you can use the Citrix Secure Web Gateway Proxy in Relay mode. For more information about Relay mode, see the XenApp and Citrix Secure Web Gateway documentation.

If you are using Relay mode, the Citrix Secure Web Gateway server functions as a proxy and you must configure Citrix Workspace app for Mac to use:

- The fully qualified domain name (FQDN) of the Citrix Secure Web Gateway server.
- The port number of the Citrix Secure Web Gateway server. Citrix Secure Web Gateway Version 2.0 does not support Relay mode.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example, my_computer.example.com is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (example), and a top-level domain (`com`). The combination of intermediate and top-level domain (`example.com`) is referred to as the domain name.

Connecting through a proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app for Mac and servers. Citrix Workspace app for Mac supports both SOCKS and secure proxy protocols.

When the Citrix Workspace app for Mac communicates with the Web server, it uses the proxy server settings configured for the default web browser on the user device. Configure the proxy server settings for the default Web browser on the user device accordingly.

Connecting through a firewall

Network firewalls can allow or block packets based on the destination address and port. Citrix Workspace app for Mac must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 for a secure Web server) for user device to Web server communication. For Citrix Workspace to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

TLS

Transport Layer Security (TLS) is the latest, standardized version of the TLS protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

Citrix Workspace app for Mac supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

> **Note**
>
> Citrix Workspace app for Mac uses platform (OS X) crypto for connections between Citrix Workspace app for Mac and StoreFront.

The following cipher suites are deprecated for enhanced security:

- Cipher suites with prefix “TLS_RSA_*”
- Cipher suites RC4 and 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Citrix Workspace app for Mac supports only the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

For DTLS 1.0 users, Citrix Workspace app for Mac 1910 and later supports only the following cipher suite:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Upgrade your Citrix Gateway version to 12.1 or later if you want to use DTLS 1.0. Otherwise, it falls back to TLS based on the DDC policy.

The following matrices provide details of internal and external network connections:

		Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

		External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

Note:

- Use Citrix Gateway 12.1 or later for EDT to work properly. Older versions do not support ECDHE cipher suites in DTLS mode.
- Citrix Gateway doesn't support DTLS 1.2. So, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` and `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` aren't supported. Citrix Gateway must be configured to use `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` to work properly

> in DTLS 1.0.

Configuring and enabling Citrix Workspace app for TLS

There are two main steps involved in setting up TLS:

1. Set up SSL Relay on your Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server and obtain and install the necessary server certificate.
2. Install the equivalent root certificate on the user device.

Installing root certificates on user devices

To use TLS to secure communications between TLS-enabled Citrix Workspace app for Mac and the server farm, you need a root certificate on the user device. This root certificate verifies the signature of the Certificate Authority on the server certificate.

macOS X comes with about 100 commercial root certificates already installed. However, if you want to use another certificate, you can obtain one from the Certificate Authority and install it on each user device.

Install the root certificate on each device, depending on your organization's policies and procedures, instead of prompting users to install it. The easiest and safest way is to add root certificates to the macOS X keychain.

To add a root certificate to the keychain

1. Double-click the file containing the certificate. This action automatically starts the Keychain Access application.
2. In the Add Certificates dialog box, choose one of the following from the Keychain pop-up menu:
   - login (The certificate applies only to the current user.)
   - System (The certificate applies to all users of a device.)
3. Click OK.
4. Type your password in the Authenticate dialog box and then click OK.

The root certificate is installed and used by TLS-enabled clients and by any other application using TLS.

About TLS policies

This section provides information for configuring security policies for ICA sessions over TLS. You can configure certain TLS settings used for ICA connections in Citrix Workspace app for Mac. These settings are not exposed in the user interface. Changing them requires running a command on the device running Citrix Workspace app for Mac.

> **Note**
>
> TLS policies are managed in other ways - by devices controlled by an OS X server or another mobile device management solution.

TLS policies include the following settings:

SecurityComplianceMode. Sets the security compliance mode for the policy. If you don't configure SecurityComplianceMode, FIPS is used as the default value. Applicable values for this setting include:

- **None**. No compliance mode is enforced
- **FIPS**. FIPS cryptographic modules are used
- **SP800-52**. NIST SP800-52r1 compliance is enforced

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. Specifies the TLS protocol versions that are accepted during protocol negotiation. This information is represented as an array and any combination of the possible values is supported. When this setting is not configured, the values TLS10, TLS11, and TLS12 are used as the default values. Applicable values for this setting include:

- **TLS10**. Specifies that the TLS 1.0 protocol is allowed.
- **TLS11**. Specifies that the TLS 1.1 protocol is allowed.
- **TLS12**. Specifies that the TLS 1.2 protocol is allowed.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. Improves the cryptographic authentication of the Citrix server and improves the overall security of the SSL/TLS connections between a client and a server. This setting governs the handling of a trusted root certificate authority (CA) while opening a remote session through SSL when using the client for OS X.

When you enable this setting, the client checks whether the server's certificate is revoked. There are several levels of certificate revocation list checking. For example, the client can be configured to check only its local certificate list, or to check the local and network certificate lists. In addition, certificate checking can be configured to allow users to log on only if all Certificate Revocation lists are verified.

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows admins to revoke security certificates (invalidated before their expiry date) if there is cryptographic compromise of certificate private keys, or unexpected changes in the DNS name.

Applicable values for this setting include:

- **NoCheck**. No Certificate Revocation List check is performed.
- **CheckWithNoNetworkAccess**. Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate

Revocation List isn't critical for verification of the server certificate presented by the target SSL Relay or Citrix Secure Web Gateway server.

- **FullAccessCheck**. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay or Citrix Secure Web Gateway server.
- **FullAccessCheckAndCRLRequired**. Certificate Revocation List check is performed, excluding the root Certificate Authority. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.
- **FullAccessCheckAndCRLRequiredAll**. Certificate Revocation List check is performed, including the root certificate authority. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

> **Note**
>
> If you don't set SSLCertificateRevocationCheckPolicy, FullAccessCheck is used as the default value.
>
> ```
> defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy
>  FullAccessCheckAndCRLRequired
> ```

Configuring TLS policies

To configure TLS settings on an unmanaged computer, run the **defaults** command in Terminal.app.

defaults is a command line application that you can use to add, edit, and delete app settings in an OS X preferences list file.

To change settings:

1. Open **Applications > Utilities \ > Terminal**.
2. In Terminal, run the command:

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

Where:

<name>: The name of the setting as described earlier.

<type>: A switch identifying the type of the setting, either -string or -array. If the setting type is a string, this setting can be omitted.

<value>: The value for the setting. If the value is an array and multiple values need to be specified, separate the values with a space.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```


Reverting to the default configuration

To reset a setting back to its default:

1. Open **Applications > Utilities \ > Terminal**.
2. In Terminal, run the command:

```
defaults delete com.citrix.receiver.nomas <name>
```

Where:

<name>: The name of the setting as described earlier.

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Security settings

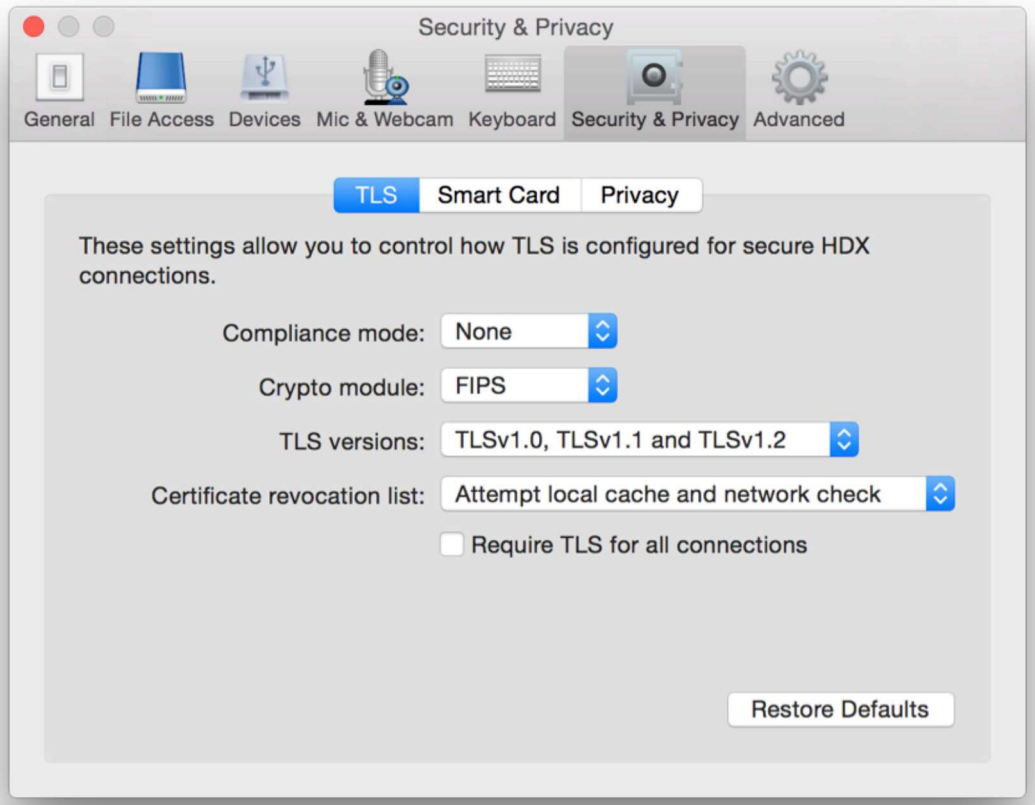
Security improvements and enhancements were introduced with Citrix Receiver for Mac version 12.3, including the following:

- improved security configuration user interface. In previous releases, the command line was the preferred method to make security-related changes. Configuration settings related to session security are now simple and accessible from the UI. This improvement improves the user experience while creating a seamless method for the adoption of security-related preferences.
- view TLS connections. You can verify connections that use a specific TLS version, encryption algorithms, mode, key size, and SecureICA status. In addition, you can view the server certificate for TLS connections.

The improved **Security and Privacy** screen includes the following new options in the **TLS** tab:

- set the compliance mode
- configure the crypto module
- select the appropriate TLS version
- select the certificate revocation list
- enable settings for all TLS connections

The following image illustrates the **Security and Privacy** settings accessible from the UI:



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States