



Citrix Workspace app for iOS

Contents

About this release	3
Prerequisites for installing	25
Install, Upgrade	32
Get started	32
Configure	40
Authenticate	78
Secure	85
Troubleshoot	90

About this release

January 27, 2023

What's new in 22.12.0

Siri shortcuts using App Intent API

Previously, Siri integration required manual intervention where the user had to configure Siri and Siri shortcuts using the option in the **Settings** menu. However, with the integration of new App Intent API, Citrix Workspace users can now invoke apps or desktops without any additional setup.

Users can start virtual apps or desktops by issuing simple voice commands to Siri, for example:

1. "Hey, Siri. Launch application in Workspace".
2. Say the name of the app or desktop that you want to open when prompted by Siri.

Note:

You can also invoke the shortcuts from the Shortcuts app or Spotlight search on your device.

Multitasking capabilities using Stage Manager

Citrix Workspace app for iOS now enables you to take advantage of Apple's Stage Manager feature on iPad devices.

You can now open Citrix Workspace app in Window mode and run multiple application windows on iPad simultaneously when Stage Manager is enabled. This also allows you to resize the window and thereby change the session resolution.

Note:

Extending display to an external monitor from within Citrix Workspace app is supported only when the app is in full screen.

Support for Apple's native non-mirror mode [Technical Preview]

You can now extend the display using Apple's non-mirror mode available with iPad OS 16.2. You can multi-task by running the Citrix Workspace app, virtual apps, and virtual desktops on the external monitor and leaving the iPad screen free to run other native apps.

Note:

Support for Apple's non-mirror mode extend display is available on selected iPad models only. For more information, see [Apple documentation](#).

If you don't want to use this technical preview feature, you can always use Citrix Workspace app in full-screen mode.

Known issues:

- Citrix Workspace app UI appears abnormally on the external monitor when the session disconnects.
- If the session is running in full screen mode on the external monitor, the device pointer locks at a random place when you move the session to the iPad screen. You will not be able to use the mouse connected to the session. As a workaround, resize the session to window mode on the iPad screen and move the device pointer into session. This allows you to use the mouse in both window and full screen mode.

These issues occur when the Stage Manager and Non-Mirror Mode are On.

Changes to iOS version

Starting from Citrix Workspace app for iOS version 2212, iOS version 13 and earlier versions are no longer supported.

Fixed issues in 22.12.0

Citrix Workspace app for iOS session disconnects immediately when you open an application. This issue occurs when HDX Insight is enabled on the Citrix ADC 13.1. [CVADHELP-21374]

Known issues in 22.12.0

When you rotate the iPad device, the display of the virtual app and desktop session might be unusual. This issue occurs when the device is connected to an external monitor, Citrix Workspace app is in Extend mode, and the resolution is Auto-fit Medium. [HDX-47280]

Note:

For a complete list of issues in the earlier releases, see [Known issues](#).

Earlier releases

This section provides information on the new features and fixed issues in the previous releases that we support as per the [Lifecycle Milestones for Citrix Workspace app](#).

22.11.0

What's new

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

Fixed issues

- Trackpad click might not work during the virtual desktop session. This issue occurs when multi-touch is disabled. [CVADHELP-21211]
- The Citrix Workspace app screen moves when you tap return at the bottom of the screen. This issue occurs when **iOS Settings > General > Predictive** option is enabled. [CVADHELP-20540]

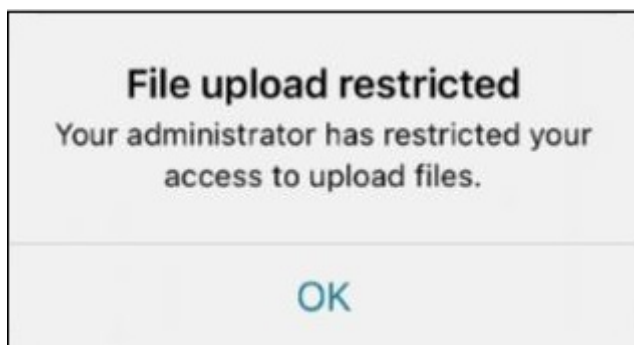
22.9.5

What's new

File upload restriction for web or SaaS apps

Administrators can now restrict the file upload for individual web or SaaS apps when Restrict uploads policy is enabled in the Citrix Secure Private Access.

When you launch web or SaaS apps that have file upload restrictions, the following error message appears:



For information on enabling the policy, see [Create an adaptive access policy](#) in the Citrix Secure Private Access document.

Fixed issues

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

22.9.0

What's new

Inactivity timeout for Citrix Workspace app sessions

Admins can specify the amount of idle time that is allowed. After the time-out value, an authentication prompt appears.

The inactivity timeout value can be set starting from 1 minute to 24 hours. By default, the inactivity timeout isn't configured. Admins can configure the `inactivityTimeoutInMinutesMobile` property by using a PowerShell module. Click [here](#) to download the PowerShell modules for Citrix Workspace app configuration.

When you have reached the specified time-out value, the end-user experience is as follows depending on the authentication type configured:

- After the inactivity timeout, you will receive a prompt to provide biometric authentication to access the Citrix Workspace app again.
- If you can cancel the biometric authentication prompt, the following message appears:

Citrix Workspace app is locked.

You must authenticate to continue to use Workspace app.

If the passcode is not configured on the iOS, you have to sign in with credentials after the inactivity timeout.

Note:

This feature is applicable for customers on Workspace (Cloud) only.

iOS version support

Citrix Workspace app for iOS now supports iOS 16.

Provision to disable LaunchDarkly service

Starting with this release, LaunchDarkly service can be disabled on both on-premises and cloud stores.

Fixed issues

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

22.8.0

What's new

iOS version support

Citrix Workspace app 22.8.0 for iOS supports only iOS 13 and later.

Reporting an issue

This release includes changes to the user interface for reporting an issue.

- **Contact the Support Team** option and dialog is replaced with **Report Issue**.
- **Log Options** is replaced with **Advanced**.

The new **Report Issue** dialog allows you to:

- Provide a description of the issue.
- Attach and preview the required images.
- Share the files via different applications installed on your device.

Report Issue option is also available while adding the Store URL. Tap the ellipsis (...) button on the upper-right corner of the Citrix Workspace app Sign in screen and tap **Report Issue** or **Settings > Report Issue**.

Advanced settings now allow you to modify:

- **Location:** log file location.
- **Log level:** Change log level to Low, Medium, or Verbose. The default log level is Low.
- **Clear logs:** To delete all the information from the log file. Selecting this option enables you to reproduce the issue and collect fresh log details.

Fixed issues

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

22.7.5

What's new

Enhancement to smart card based authentication

Citrix Workspace app for iOS now supports Thursby and Feitian readers for smart card based authentication. For information on the supported readers, see [Smart cards](#).

Fixed issues

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

22.7.0

What's new

Store list management

This feature enhances end user experience by clearing the published apps and desktops, and the user details from the store list when you sign out. The store list management feature is helpful when multiple users share a device and the user's privacy is important. This feature is applicable for both on-premises and cloud stores.

With this feature, the usability of the following workflows is improved:

- Sign out from the account
- Delete an account
- Edit an account

Fixed issues

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

22.6.5

What's new

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

Fixed issues

- When you upgrade your device to iOS 15, entries such as **Control + F**, **Command + Tab**, and **Command + Enter**, through the external keyboard might not work as expected. You might also see the up arrow key functioning as the down arrow. [CVADHELP-19084]
- During the Citrix Workspace app session, the on-screen keyboard keeps popping when your device is connected to an external keyboard and the iOS **Settings > General > Predictive** option is enabled. The issue occurs when you upgrade your device to iOS 15 or higher. [CVADHELP-20145]

22.6.1

What's new

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

Fixed issues

Launching resources like apps and desktops might fail and prompt with the following certificate error:

“Client Certificate Missing”

The issue occurs when you have selected a certificate while signing in to Citrix Workspace app.

[CVADHELP-20422]

22.6.0

What's new

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

Fixed issues

- When you create an account using the manual setup process, selecting an edition is difficult under the **Citrix Gateway** option. The issue is that the options change in the sequence arbitrarily. [CVADHELP-20188]

22.5.0

What's new

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

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#) in StoreFront documentation.

Fixed issues

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

22.4.6

What's new

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

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#) in StoreFront documentation.

Fixed issues

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

22.4.5

What's new

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.

Store list management [Feature preview](#)

This feature enhances end user experience by clearing the published apps and desktops, and the user details from the store list when you sign out. The store list management feature is helpful when multiple users share a device and the user's privacy is important. This feature is applicable for both on-premises and cloud stores.

With this feature, the usability of the following workflows is improved:

- Sign out from the account
- Delete an account
- Edit an account

Fixed issues

- When you launch a session for the first time, trying to launch apps inside the session is successful. However, the subsequent launches fail. The issue occurs when you use the **Optional Certificate** for multifactor authentication with Azure. [CVADHELP-19391]

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#) in StoreFront documentation.

22.4.1

What's new

Extended multi-monitor support with Generic Mouse for iPad

You can extend the desktop session onto an external monitor when you connect your iPad with a Generic Mouse. This feature supports iPadOS version 14.0 and later.

For more information, see [Extended multi-monitor support with Generic Mouse for iPad](#) in the Configure section.

Note:

The external display resolution depends on:

- adapters
- iPad
- other hardware used

Feature limitations

- To ensure that the Citrix Workspace app receives primary mouse clicks, disable AssistiveTouch in iOS **Settings > Accessibility > Touch > AssistiveTouch**.
- Tracking Speed and Natural Scrolling options from iOS settings doesn't affect the generic mouse inside the session. However, scrolling speed can be controlled from the iOS **Settings**. You can access Tracking speed and Natural scrolling options from the **Mouse Settings** screen inside the session toolbar.
- When an iPad is used in the split mode and the monitor is connected, the generic mouse works only in the mirror mode inside a desktop session.
- If the native cursor is over the multi-tasking menu before the app obtains the pointer lock, that is, before the session launch, the mouse events aren't received. As a workaround, pull down the Notification Center and move the native pointer to a different location and dismiss the Notification Center.
- Audio redirection fails when you connect an iPad to an external monitor. The audio plays through the iPad speakers. [HDX-39159]

Known issues in the feature

- While the session is active, the desktop image that appears on an iPad or an external monitor gets disturbed when you change the:
 - Display arrangement
 - Resolution
 - Orientation or
 - Display modes

As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].

- On rare occasions, you can observe a few seconds lag in the audio when the video is played on the external monitor. [HDX-39159]
- On rare occasions, the VDA display is truncated on an iPad and on the external monitor. As a workaround, disconnect, and reconnect the monitor. If the issue persists, disconnect and relaunch the session. [HDX-37100]
- When you maximize the video to full-screen on the external monitor, you might observe video quality issues. [HDX-39159]
- On rare occasions, inside a desktop session, attempt to move the apps from an iPad to the external monitor fails. As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-36981]
- On rare occasions, when you connect an iPad to an external monitor using third-party adapters, the Display Modes aren't visible under the Display Options. [HDX-39713]
- Sometimes, a line is observed under the mouse pointer inside the VDA session. [RFIOS-9569]

Siri integration

You can interact with Siri to launch resources like apps and desktops without launching Citrix Workspace app each time.

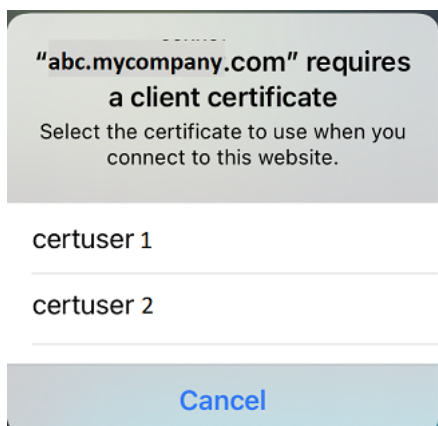
For more information, see [Siri integration](#) in the Configure section.

Safari view controller

End users can now handle certificate-based authentication where, the certificates are saved onto the device keychain. While signing in, Citrix Workspace app detects the list of certificates on your device, and you can choose a certificate for authentication.

Important:

After you choose the certificate, the selection persists for the next Citrix Workspace app launch. To choose another certificate, you can select **Reset Safari** option from the iOS device settings or reinstall Citrix Workspace app.



Note:

This feature supports on-premises deployments.

For more information, see [Safari View Controller](#) in the Configure section.

Fixed issues

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

22.3.5

What's new

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 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 produc-

tion 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.

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#) in StoreFront documentation.

Fixed issues

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

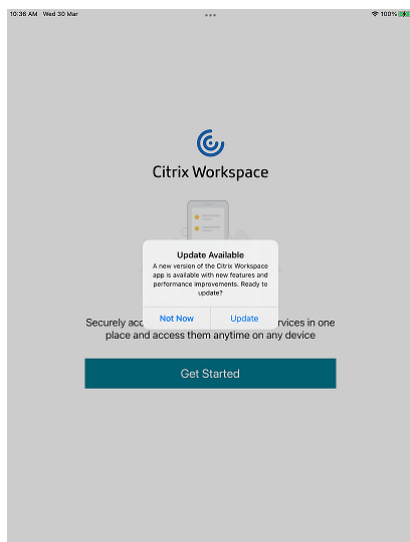
22.3.0

What's new

Use the latest version

This feature helps you to use the latest version of Citrix Workspace app. When you launch the Citrix Workspace app, the in-app prompt asks you to update to the latest version.

When you tap **Update**, the Apple store page appears. Download the latest version of the app.

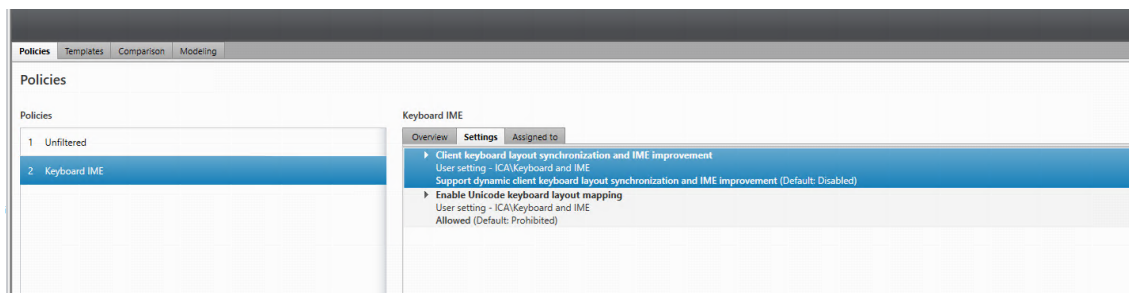


Generic Client IME for East Asian languages

Generic Client Input Method Editor (IME) feature enhances input and display experience with Chinese, Japanese, and Korean (CJK) language characters on iOS devices. You are recommended to use the client IME instead of the VDA-side IME for a better user experience.

Prerequisites

- Enable the Client keyboard layout synchronization and IME improvement and Enable Unicode keyboard layout mapping on your Windows VDA through the group policy.



For more information see, Knowledge Center article [CTX312404](#).

You can also enable the options using the following registries on your Windows VDA:

- 1 - HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0
- 2 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value = DWORD 1
- 3 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value = DWORD 1

- Enable **Settings > Keyboard Options > Keyboard Layout Sync** option from Citrix Workspace app.

IME user interface

Generally, IME provides UI components such as candidate window and composition window. The composition window contains the composition characters and composition UI elements, for example, underline and background color. The candidate window displays the candidate list.



The composition window enables you to distinguish between the confirmed characters and the composing characters. The composition window and the candidate window move with the input cursor.

As a result, the feature provides:

- An enhanced input of characters at the cursor location in the composition window.
- An enhanced display in the composition and the candidate window.

Currently, you can use this feature on the sessions hosted on Windows VDAs and supports both soft keyboards and external physical keyboards.

Feature limitations

- This feature synchronizes client-side keyboard layout and IME to the VDA-side. However, this feature doesn't support synchronization from the VDA-side to the client-side.
- We recommend you use Apple's native keyboards and IMEs. The third-party IMEs like Gboard for iOS, Sogou Chinese IME, and Baidu IME aren't supported.

Fixed issues in 22.3.0

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

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#) in StoreFront documentation.

22.2.5

What's new

Enhanced search functionality

When you search for a keyword, you can view the search results that are a part of:

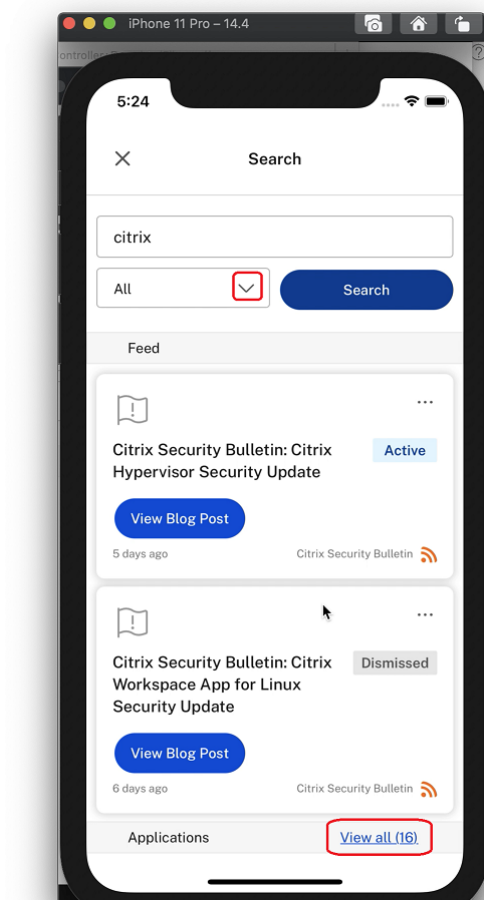
- notification feeds
- files
- folders
- desktops
- specific content stored in connected applications

Use the drop-down menu to select a specific category and to see just those results. In each section of search, you have two options:

- View all (Number of matches): Use this option to expand the search results.
- View less: Use this option to collapse the expanded search results.

Note:

This feature is the request-only preview. To get it enabled in your environment, fill out the Podio form <https://podio.com/webforms/27156424/2086506>.



Service Continuity **Feature preview**

Note:

This feature is in public technical preview.

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.

Fixed issues

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

22.2.0

What's new

Feeds widget on iOS home screen

You can configure and view the Citrix Workspace app notification feeds using a widget. You can add it on the iOS home screen. This feature enhances your experience and lets you view the recent feeds.

For more information, see [Feeds widget](#).

Spotlight search enhancement

The app icon matches the corresponding app search. Previously, the Citrix Workspace app icon was displayed for all the searches.

For more information, see [Spotlight search enhancement](#).

Accessing recent apps by 3D-Touch gesture

You can access a list of recently launched apps for quick access when you use the 3D-Touch (long-press) gesture on the **Citrix Workspace app** icon.

Migration from on-premises to cloud account

Administrators can seamlessly migrate the end users from an on-premises StoreFront store URL to a Workspace URL. Administrators can do the migration with minimum end user interaction using the [Global App Configuration Service](#).

For more information, see [Migration from on-premises to cloud account](#).

Extended multi-monitor support with Generic Mouse for iPad **Feature preview**

You can extend the desktop session onto an external monitor when you connect your iPad with a Generic Mouse. This feature supports iPadOS version 14.0 and later.

For more information, see [Extended multi-monitor support with Generic Mouse for iPad](#).

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#).

Fixed issues in 22.2.0

- On rare occasions, when you access Secure Hub to open a virtual application, the Citrix Workspace app crashes. [RFIOS-9886]
- When you launch the session in presentation mode, if you visit the **Display options** and navigate back to the session, you can occasionally observe a duplicate mouse pointer. Also, you can observe the issue (occasionally) when you dismiss an alert. [RFIOS-9711]
- After you sign in to the on-premises store and launch a desktop for the first time, the generic mouse becomes unresponsive.

You can apply either of the workarounds:

- Switch to another app or go to the home screen and return to the workspace app
- Disconnect and relaunch the session [RFIOS-9654]

21.12.0

What's new

Reposition the in-session toolbar

With this release, you can reposition the in-session toolbar. You can choose to position it either on the top or on the right of the screen. When you drag the toolbar notch away from the toolbar edge, the rectangle drag indicator and the drop target appear. Drop the drag indicator over the drop target to reposition the toolbar.

Previously, the in-session toolbar was fixed either on the top or on the right.

Notes:

- The feature is applicable for iPad users only.
- The feature functions with touch or mouse.
- The feature functions with an iPad or on an external display.
- The last toolbar position persists for the next session or the application launch.

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#).
- We now support iOS 15.
- For information on the deprecation of iOS version 11.x and 12.x, see the [deprecation](#) table.

Fixed issues

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

21.11.0

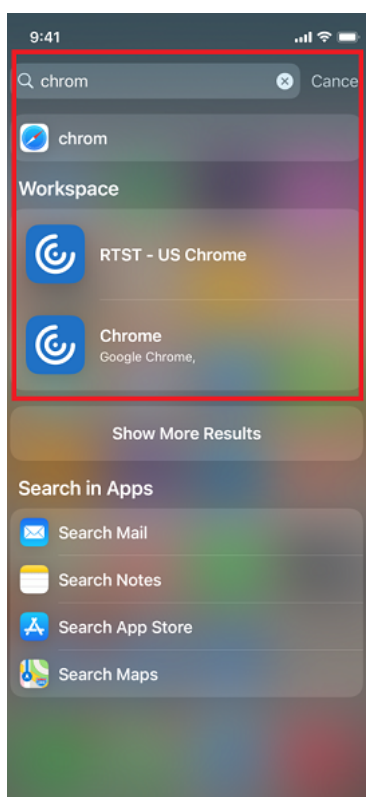
What's new

Access of apps and desktops through Spotlight search

In this release, we've introduced the Spotlight search feature. You can use Spotlight search to find your desktops and your Web, SaaS (Software-as-a-Service), and desktop apps. You can then access these apps and desktops directly from Spotlight search without launching Citrix Workspace app.

Note:

- The Spotlight search feature doesn't support mobile apps.



Service Continuity **Feature preview**

Note:

This feature is in public technical preview.

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.

Recommendations and notes

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see [HTTPS](#).
- We now support iOS 15.

Fixed issues

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

Known issues

Known issues in 22.2.0

- While the session is active, the desktop image that appears on an iPad or an external monitor gets disturbed when you change the:
 - display arrangement
 - resolution
 - orientation or
 - display modes

As a workaround, disconnect and relaunch the session. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].

- On rare occasions, moving apps from a few iPads to an external monitor and conversely isn't as expected. The issue occurs when you use a generic mouse. [RFIOS-9655]

Known issues in 21.10.5

- When using Microsoft Excel Online, you might not be able to type Japanese characters. The issue occurs when you move from one cell to another. As a workaround, double tap on the cell for the keyboard to appear. [CVADHELP-16494]
- When you type Japanese characters in the title text box of Microsoft PowerPoint Online, the cursor goes back to the beginning of the text. The issue occurs after pressing the Enter key in the title box. [CVADHELP-16417]
- After selecting an external display resolution, only portions of the session might appear or the resolution is too small. Also, an icon you click doesn't get selected, with the Citrix X1 Mouse, within an HDX session.

Also, after selecting a non-default external display resolution, the mouse might not work. [RFIOS-9231], [RFIOS-9229], [RFIOS-9227], [RFIOS-9210]

Known issues in 21.9.5

You might have to tap twice on any app to launch apps for the first time in the **Apps** section. When you move out of the **Apps** section and then back to it, you might have to tap twice again to launch any app. The issue occurs only in Apple iPads and in Portrait mode only. [RFIOS-8954]

Known issues in 21.9.0

You might have to tap twice on any app to launch apps for the first time in the **Apps** section. When you move out of the **Apps** section and then back to it, you might have to tap twice again to launch any app. The issue occurs only in Apple iPads and in Portrait mode only. [RFIOS-8954]

Known issues in 21.6.5

- There is a slight lag in audio when both microphone and camera are turned on in a video conference call. [RFIOS-8053]
- The iPhone volume is low in Microsoft Teams calls in HDX sessions. [RFIOS-8507]
- The audio or the microphone stops working intermittently. As a workaround, restart the HDX session for it to work again. [RFIOS-8502]

Known issues in 21.4.5

The following sites crash when opened in Workspace from Feeds/Actions or from Web/SaaS apps:

- 1 - <<https://www.lowes.com>>
- 2 - <<https://www.washingtonpost.com>>

The crash occurs only for customers on Cloud stores. [RFIOS-7888]

Known issues in 21.4.0

Citrix Workspace app for iOS crashes intermittently when you open **Settings** and click **Device Storage**. As a work-around, reinstall Citrix Workspace app. [RFIOS-8015]

Known issues in 21.1.5

Attempts to access your device storage in an HDX session might fail if your store is added as a web interface. [RFIOS-7349]

Known issues in 20.9.0

- In a cloud setup, apps recently launched from Citrix Workspace for iOS might not load on the Today widget in iPhones and iPads. [RFIOS-5528]
- Attempts to open a downloaded ICA file from the Safari web browser might fail intermittently. This issue occurs on Citrix Workspace app for iOS running on iOS 14 devices. Try the following two workarounds:
 - Wait for sometime before opening the downloaded file (even if the download complete icon appears)
 - Go to **Settings > Safari Downloads**. Select **On My iPad** to save the downloaded files. [RFIOS-6599]

Known issues in 20.2.0

- When you sign out of a cloud account using **Settings > Store > Sign Out**, the sign-out process might not work as expected. The issue occurs intermittently on iPhones. As a workaround, relaunch Citrix Workspace app. [RFIOS-5197]
- When you edit and save the **Store** settings and then abandon the edits by canceling authentication, the Workspace account might get removed from the app. The issue occurs in a cloud setup. [RFIOS-5433]
- In a cloud setup, when you edit and save the account settings, Citrix Workspace app might intermittently become unresponsive. As a workaround, relaunch Citrix Workspace app. [RFIOS-5379]

Known issues in 20.1.5

- In a cloud setup, when you open the Citrix Workspace app, the app badge count isn't cleared. [RFIOS-5194]
- When you sign out of a cloud account using **Settings > Store > Sign Out**, the sign-out process might not work as expected. The issue occurs intermittently on iPhones. As a workaround, relaunch Citrix Workspace app. [RFIOS-5197]

Known issues in 20.1.0

- In a cloud setup, you might observe an incorrect badge count. [RFIOS-5194]
- In iOS 13.3 devices, you might observe an incorrect badge count. [RFIOS-5204]
- The “Try the Demo” option is unavailable. [RFIOS-4902]

Limitations

- We recommend that you use **Control + C** and **Control + V** keys on the soft keyboard of your device to copy and paste. **Command + C** and **Command + V** keys on an external keyboard might not work. [HDX-32431]
- Attempts to launch an app by tapping the ICA file in the download manager fail when using the Safari web browser.
To ensure successful app launches from Safari, make sure the latest version of Citrix Workspace app or Citrix Receiver for iOS (but not both) is present on the device. [RFIOS-5502]
- After migrating to Citrix Workspace from StoreFront, the screen flickers momentarily while tapping the **Next** button on the Pendo guide.
- While starting web and SaaS apps from within the Citrix Workspace app, if the app uses Google IdP and requires the user to sign in then the authentication will fail with the error message “Access Denied”. [RFIOS-11904]

Feature preview

Feature previews are available for customers to use 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.

Prerequisites for installing

January 11, 2023

System requirements and compatibility

Device requirements

- Citrix Workspace app for iOS version 22.9.0 or later supports iOS 16 and iPadOS 16.
- Citrix Workspace app for iOS version 21.9.1 or later supports iOS 15 and iPadOS 15.
- Citrix Workspace app for iOS version 20.9.0 or later supports iOS 14 and iPadOS 14.
- This software update has been validated on the following devices:
 - iPhone 7x models, iPhone 8x models, and only iPhone X model.
 - All iPad models (including iPad Pro) except for iPad 1 and iPad 2, which aren’t supported.
- External display support
 - iPhone - as supported by iOS.
 - iPad - as supported by iOS (does not use the whole screen).

Server requirements

Verify if you've installed all the latest hotfixes for your servers.

- For connections to virtual desktops and apps, Citrix Workspace app supports Citrix StoreFront and Web Interface.

StoreFront:

- StoreFront 3.6 or later (recommended). Citrix Workspace app has been validated with the latest version of StoreFront; previous supported versions include StoreFront 2.6 or later.

Provides direct access to StoreFront stores. Citrix Workspace app also supports prior versions of StoreFront.

Note:

With XenApp and XenDesktop 7.8, Citrix introduced support for the Framehawk virtual channel and 3D Pro. This functionality was extended to Citrix Workspace app.

- StoreFront configured with a Workspace for website.

Provides access to StoreFront stores from a Safari web browser. Users must manually open the ICA file using the browser. For the limitations of this deployment, see the [StoreFront](#) documentation.

Web Interface:

- Web Interface 5.4 with Web Interface sites
- Web Interface 5.4 with XenApp and XenDesktop sites
- Web Interface on Citrix Gateway (browser-based access only using Safari)

Enable the rewrite policies provided by Citrix Gateway.

- **Citrix Virtual Apps and Desktops, XenApp, and XenDesktop** (any of the following products):
 - Citrix Virtual Apps and Desktops 7 1808 or later
 - Citrix XenDesktop 7.x or later
 - Citrix XenApp 7.5 or later

Connections, certificates, and authentication

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

	Workspace for Web using browsers	StoreFront Services site (native)	StoreFront XenApp and XenDesktop Site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor authentication (domain with security token)				Yes*	Yes*
SMS				Yes*	No
Smart card		Yes		Yes*	Yes*
User certificate				Yes (Citrix Gateway plug-in)	Yes (Citrix Gateway plug-in)

*Available only for:

- Workspace for websites.
- Deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

For connections to the Web Interface 5.4, Citrix Workspace app supports the following authentication methods:

Note:

Web Interface uses the term Explicit to represent domain and security token authentication.

	Web Interface (browsers)	Web Interface XenApp and XenDesktop Site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface XenApp and XenDesktop Site
Anonymous	Yes			
Domain	Yes	Yes	Yes*	
Domain pass-through	Yes			
Security token			Yes*	
Two-factor authentication (domain with security token)			Yes*	
SMS			Yes*	
Smart card				
User certificate			Yes (Require Citrix Gateway plug-in)	

Certificates

Private (self-signed) certificates

You can successfully access Citrix resources using Citrix Workspace app:

- when a private certificate is installed on the remote gateway.
- when the root certificate for the organization's certificate authority is installed on the device.

Note:

When the remote gateway's certificate cannot be verified upon connection (because the root certificate isn't included in the local keystore), an untrusted certificate warning appears. If a user chooses to continue through the warning, a list of applications is displayed; however, applications fail to start.

Manually installed certificate

In iOS 10.3 and later, a certificate included in a profile that you install manually isn't automatically trusted for SSL. To trust manually installed certificate profiles in iOS:

1. Make sure you've installed the certificate profile on the device.
2. Go to **Settings > General > About > Certificate Trust Settings**.

Each root that has been installed through a profile appears under **Enable Full Trust For Root Certificates**.

3. You can toggle trust on or off for each root.

Import root certificates on iPad and iPhone devices

Obtain the root certificate of the certificate issuer and email it to an email account configured on your device. When clicking the attachment, you're 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 supports wildcard certificates.

Intermediate certificates and Citrix Gateway

When your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway (or Access Gateway) server certificate. Also, for Access Gateway installations, see [Install, link, and update certificates](#) that matches your requirement in Citrix ADC documentation.

RSA SecurID authentication is supported for Secure Gateway configurations (through the Web Interface only) and all supported Access Gateway configurations.

Citrix Workspace app supports all authentication methods supported by Access Gateway.

Joint Server Certificate Validation Policy

Releases of Citrix Workspace app have a stricter validation policy for server certificates.

Important

Before installing Citrix Workspace app, confirm that the certificates at the server or gateway are correctly configured as described here. Connections might 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 now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous releases, Citrix Workspace app then also checks that the certificates are trusted. If the certificates aren't not all 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 connections 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:

- Example Server Certificate
- Example Intermediate Certificate
- Example Root Certificate

Then, Citrix Workspace app checks if all these certificates are valid. Citrix Workspace app also validates if **Example Root Certificate** certificate is already trusted.

Notes:

- If Citrix Workspace app does not trust **Example Root Certificate**, the connection fails.
- Some certificate authorities have more than one root certificate. If you require a stricter validation, make sure that your configuration uses the appropriate root certificate.

For example, there're currently two certificates:

- DigiCert or GTE CyberTrust Global Root
- DigiCert Baltimore Root or Baltimore CyberTrust Root

These certificates 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** or **Baltimore CyberTrust Root**).

If you configure **GTE CyberTrust Global Root** at the gateway, Citrix Workspace app connections on those user devices fails. Consult the certificate authority's documentation to determine which root certificate has to be used. Also note that root certificates eventually expire, as do all certificates.

Then, Citrix Workspace app uses these two certificates. The app searches for a root certificate on the user device. If the app finds one that validates correctly, and is also trusted (such as **Example Root Certificate**), the connection succeeds. Otherwise, the connection fails.

This configuration supplies the intermediate certificate that Citrix Workspace app needs, but also allows Citrix Workspace app 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 doesn't 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. Such certificates are intended for situations where there're more than one root certificate, and an earlier root certificate is still in use at the same time as a later root certificate. In such cases, at least two intermediate certificates exist.

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). The Issuer name 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 Citrix Workspace app selects the earlier root certificate:

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

It isn't recommended to configure the gateway with only the server certificate:

- Example Server Certificate

In such cases, if Citrix Workspace app can't locate all the intermediate certificates, the connection fails.

Install, Upgrade

January 11, 2023

Upgrade

To upgrade to the latest Citrix Workspace app, do any of the following steps:

- Download the Citrix Workspace app from the [Citrix Download](#) page and install the app to upgrade from Citrix Receiver to Citrix Workspace app.
- Upgrade your Citrix Workspace app using the app store.

For information about the features available in Citrix Workspace app for iOS, see [Citrix Workspace app feature matrix](#).

Get started

January 11, 2023

Setup

Citrix Workspace app for iOS supports the configuration of Web Interface for your Citrix Virtual Apps deployment. There're two types of Web Interface sites:

- XenApp and XenDesktop Sites
- Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) Sites.

Web Interface sites enable client devices to connect to the server farm. Authentication between Citrix Workspace app for iOS and a Web Interface site can be handled using various solutions, including Citrix Secure Web Gateway.

Also, you can configure StoreFront to provide authentication and resource delivery services for Citrix Workspace app. The configuration enables you to create centralized enterprise stores to deliver desktops, applications, and other resources to users.

For more information about configuring connections, including videos, blogs, and a support forum, see <http://community.citrix.com>.

Before your users access applications hosted in your Citrix Virtual Apps and Desktops and Citrix DaaS deployment, configure the following components in your deployment as described here.

- When publishing applications on your farms or sites, consider the following options to enhance the experience for users accessing those applications through StoreFront stores.
 - Verify to include meaningful descriptions for published applications because these descriptions are visible to users in Citrix Workspace app.
 - You can emphasize published applications for your mobile device users. You can list the applications under the Featured list. To populate this list on Citrix Workspace app, edit the properties of applications that are published on your servers. You can now append the KEYWORDS: Featured string to the value of the **Application description** field.
 - To enable the screen-to-fit mode, which adjusts the application to the screen size of mobile devices, edit the properties of applications that are published on your servers and append the KEYWORDS: mobile string to the value of the Application description field. This keyword also activates the auto-scroll feature for the application.
 - To automatically subscribe all users of a store to an application, append the KEYWORDS: Auto string to the description when you publish the application in Citrix Virtual Apps. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
- If the Web Interface of your Citrix Virtual Apps and Desktops and Citrix DaaS deployment does not have a site, create one. The name of the site and how you create it depends on the version of Web Interface you've installed.

Manual setup

In general, when Citrix Workspace app connects to Citrix Gateway, Citrix Workspace app tries to locate a XenApp and XenDesktop Site or Citrix Virtual Apps website after authenticating. If no site is detected, Citrix Workspace app for iOS displays an error. To avoid this situation, you can configure an account manually so Citrix Workspace app for iOS can connect to Citrix Gateway.

1. Tap the **Accounts** icon > **Accounts Screen** > **Plus Sign (+)**. The New Account screen appears.
2. In the lower left corner of the screen, tap the icon to the left of **Options** and tap **Manual setup**. Other fields appear on the screen.
3. In the **Address** field, type the secure URL of the site or Citrix Gateway (for example, agee.mycompany.com).
4. Select one of the following connection options. The other fields on the screen change, depending on your selection.

- **Web Interface** - Select for Citrix Workspace app to display a Citrix Virtual Apps website similar to a Web browser. This UI is also known as Web View.
 - **XenApp Services** - Select for Citrix Workspace app for iOS to locate a specific XenApp and XenDesktop Site for which authentication through Citrix Gateway isn't configured. In the additional options that appear on this screen, provide site logon credentials.
 - <StoreFront FQDN>: If there're many stores, a list is presented and the user can choose the store to add.
 - <StoreFront FQDN>/citrix/<Store Name>: This option adds the StoreFront store <Store Name>.
 - <StoreFront FQDN>/citrix/PnAgent/config.xml: This option adds the default legacy PNAgent store.
 - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: This option adds the legacy PNAgent store associated with <Store Name>.
 - Citrix Gateway - Select for Citrix Workspace app for iOS to connect to a XenApp and XenDesktop Site through a specific Citrix Gateway. In the additional options on this screen, select the server edition and its logon credentials, including whether it requires a security token for authentication.
5. For certificate security, use the setting in the Ignore certificate warnings field to determine whether you want to connect to the server even if it has an invalid, self-signed, or expired certificate. The default setting is OFF.
- Important: If you do enable this option, make sure you're connecting to the correct server. Citrix strongly recommends that all servers have a valid certificate to protect user devices from online security attacks. A secure server uses an SSL certificate issued from a certificate authority. Citrix does not support self-signed certificates and does not recommend by-passing the certificate security.
6. Tap Save.
7. Type your user name and password (or token, if you selected two-factor authentication), and then tap Log On. The Citrix Workspace app for iOS screen appears, in which you can access your desktops and add and open your apps.

StoreFront

Important:

- When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition versions from 9.3, and Citrix Gateway versions through 13.
- Citrix Workspace app for iOS supports only XenApp and XenDesktop Sites on Web Interface.
- Citrix Workspace app for iOS supports launching sessions from Workspace for Web, as long as the web browser works with Workspace for Web. If launches do not occur, configure your account through Citrix Workspace app for iOS directly. Users must manually open the ICA

file using the browser Open in Workspace function. For the limitations of this deployment, see the [StoreFront](#) documentation.

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Workspace app for iOS. Create stores that count and sum up desktops and applications from the following:

- Citrix Virtual Apps and Desktops and Citrix DaaS sites
 - Citrix Virtual Apps farms
1. Install and configure StoreFront. For details, see the [StoreFront](#) product documentation. For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for iOS.
 2. Configure stores for StoreFront as you would for other Citrix Virtual Apps and Desktops and Citrix DaaS applications. No special configuration is needed for mobile devices. For details, see User Access Options in the StoreFront section of Product Documentation. For mobile devices, use either of these methods:
 - Provisioning files. You can provide users with provisioning files (.cr) that has connection details for their stores. After installation, users open the file on the device to configure Citrix Workspace app for iOS automatically. By default, Workspace for websites offer users a provisioning file for the single store for which the site is configured. Alternatively, you can use the Citrix StoreFront management console to generate provisioning files for single or many stores that you can manually distribute to your users.
 - Manual configuration. You can directly inform users of the Citrix Gateway or store URLs to access their desktops and applications. For connections through Citrix Gateway, users also must know the product edition and required authentication method. After installation, users type these details into Citrix Workspace app, which tries to verify the connection and, if successful, prompts users to sign in.
 - Automatic configuration. Tap **Add Account** on the Welcome screen and type the URL of the StoreFront server in the address field. The configuration of the account happens automatically while the account is added.

To configure Citrix Gateway

If you have users who connect from outside the internal network, configure authentication through Citrix Gateway. For example, users who connect using the Internet from a remote location.

- When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition versions from 9.3, and Citrix Gateway versions through 13.

Web Interface

To configure the Web Interface site, users with iPhone and iPad devices can launch applications through your Web Interface site and the built-in Safari browser on the mobile device. Configure the Web Interface site the same as you would for other Citrix Virtual Apps applications. If no XenApp and XenDesktop Site is configured for the mobile device, Citrix Workspace app for iOS automatically uses your Web Interface site. No special configuration is needed for mobile devices.

The built-in Safari browser supports Web Interface 5.x.

To launch applications on the iOS device

On the mobile device, users can log on to the Web Interface site using their normal logon and password.

Automatic provision for mobile devices

In StoreFront, use the **Export Multi-Store Provisioning File** and **Export Provisioning File** tasks to generate files containing connection details for stores, including any Citrix Gateway deployments and beacons configured for the stores. Make these files available to users to enable them to configure Citrix Workspace app for iOS automatically with details of the stores. Users can also obtain Citrix Workspace app for iOS provisioning files from Workspace for websites.

Important:

In many server deployments, use only one server at a time to modify the configuration of the server group. Verify if the Citrix StoreFront management console isn't running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile. Select the Stores node in the left pane of the Citrix StoreFront management console.
2. To generate a provisioning file containing details for multiple stores, in the Actions pane, click Export Multi-Store Provisioning File and select the stores to include in the file.
3. Click Export and Save the provisioning file with a `.cr` extension to a suitable location on your network.

User access information

You must provide users with the Citrix Workspace app for iOS account information they need to access their hosted their applications, desktops, and data. You can provide this information by:

- Configuring email-based account discovery

- Providing users with a provisioning file
- Providing users with account information to enter manually

Configure email-based account discovery

You can configure Citrix Workspace app for iOS to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Workspace app for iOS installation and configuration. Citrix Workspace app determines the Access Gateway or StoreFront server, or Endpoint Management virtual appliance that are associated with the email address that are based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications, desktops, and data.

Note:

Email-based account discovery isn't supported if Citrix Workspace app for iOS is connecting to a Web Interface deployment.

Add DNS Service Location (SRV) record to enable email-based discovery

During initial configuration, Citrix Workspace app can contact Active Directory Domain Name System (DNS) servers to obtain details of the stores available for users. This means that users do not need to know the access details for their stores when they install and configure Citrix Workspace app for iOS. Instead, users enter their email addresses and Citrix Workspace app contacts the DNS server. You can gather the domain details from the email address.

To enable Citrix Workspace app to locate available stores that are based on the users' email addresses:

- configure Service Location (SRV) locator resource records for Access Gateway.
- configure the StoreFront or AppController connections on your DNS server.

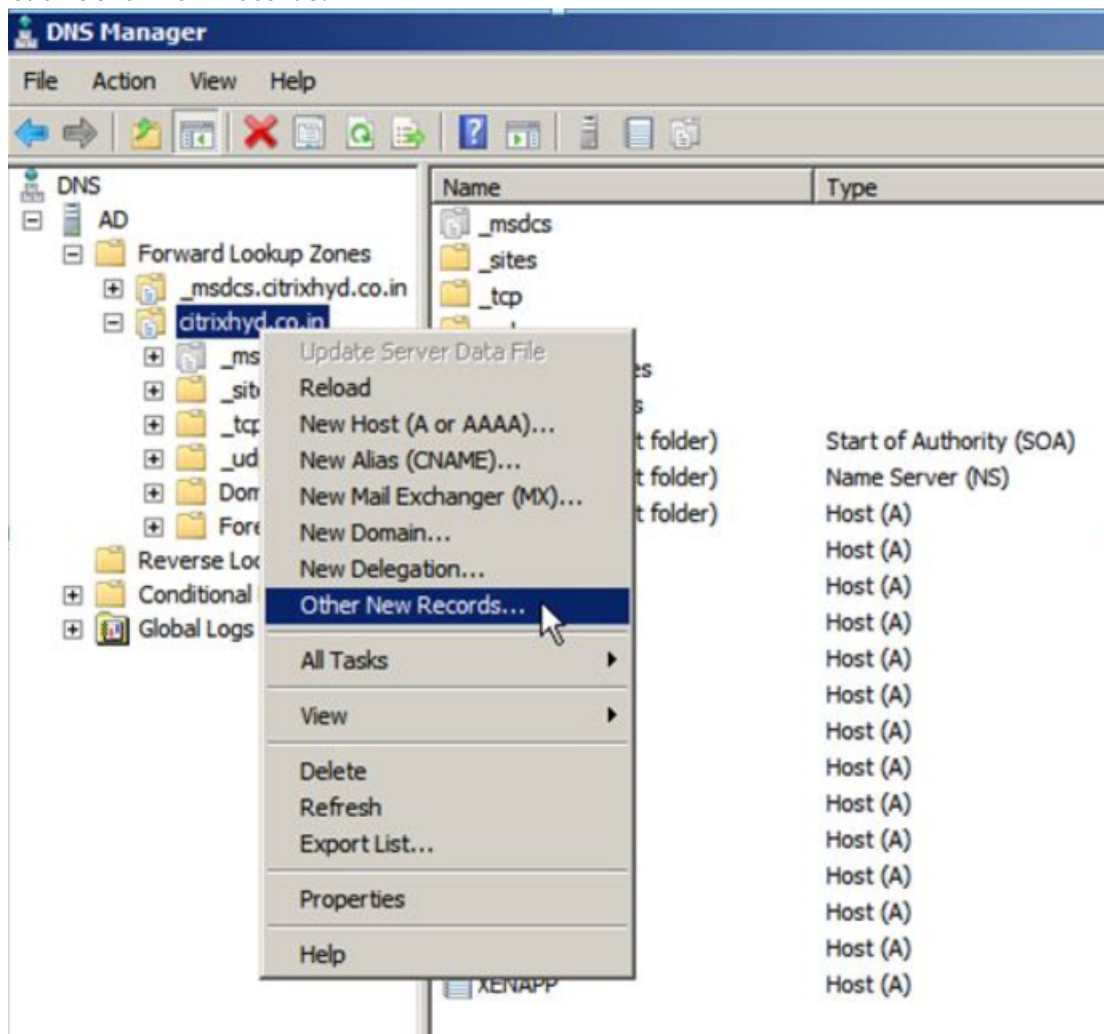
You must install a valid server certificate on the Access Gateway appliance and the StoreFront or App-Controller server to enable email-based account discovery. The full chain to the root certificate must also be valid. For the best user experience, install either a certificate with:

- a Subject
- a Subject Alternative Name entry of *discoverReceiver.domain*.
- a wildcard certificate for the domain containing your users' email accounts.

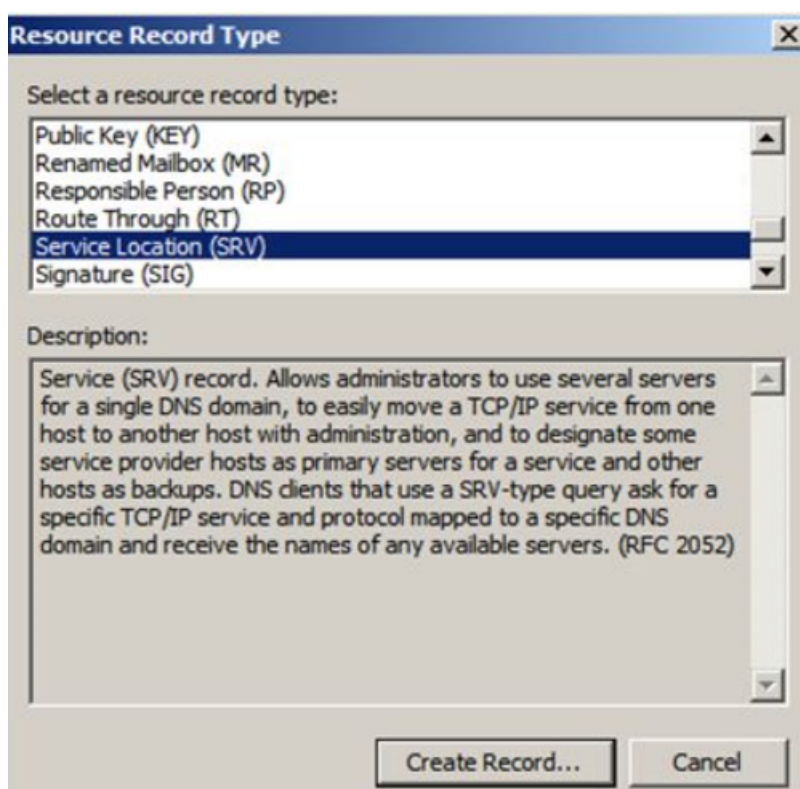
To allow users to configure Citrix Workspace app for iOS by using an email address, add an SRV record to your DNS zone as follows:

1. Log into your DNS server.
2. In DNS, right-click your Forward Lookup Zone.

3. Click **Other New Records**.



4. The **Resource Record Type** dialog box appears.
5. Under **Select a resource record type**, select **Service Location (SRV)**.
6. Select **Create Record**.



7. The Properties dialog box appears.
8. Select the **Service Location** tab.
9. Under **Service**, enter the host value `_citrixreceiver`.
10. Under **Protocol**, enter the value `_tcp`.
11. Under **Host offering this service**, specify the fully qualified domain name (FQDN) and port for your Access Gateway appliance (to support both local and remote users) or the StoreFront or AppController server (to support users on the local network only).
12. Click OK.

Note:

Your StoreFront FQDN must be unique and different from the Access Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Access Gateway virtual server isn't supported. Citrix Workspace app requires a unique StoreFront FQDN address that is only resolvable from user devices that are connected to the internal network. If not, Citrix Workspace app users can't use email-based account discovery.

Provide users with a provisioning file

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Citrix Workspace app for iOS automatically. After installing Citrix Workspace app for iOS, users simply open the `.cr` file on the

device to configure Citrix Workspace app for iOS. If you configure Workspace for websites, users can also obtain Citrix Workspace app for iOS provisioning files from those sites.

For more information, see the [StoreFront](#) documentation.

Provide users with account information to enter manually

If providing users with account details to enter manually, ensure you distribute the following information to enable them to connect to their hosted and desktops successfully:

- The StoreFront URL or XenApp and XenDesktop Site hosting resources; for example: `servername.company.com`.
- For access using Citrix Gateway, provide the Citrix Gateway address and required authentication method.

When a user enters the details for a new account, Citrix Workspace app tries to verify the connection. If successful, Citrix Workspace app for iOS prompts the user to log on to the account.

Configure

January 27, 2023

Administrator tasks and considerations

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

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

- `app.launchdarkly.com`

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- [Firehose.launchdarkly.com](https://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 Status](#) page.

LaunchDarkly system requirements

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

- LaunchDarkly service.
- APNs listener service

Provision to disable LaunchDarkly service:

You can disable LaunchDarkly service on both on-premises and cloud stores.

On the cloud setup, administrators can disable the LaunchDarkly service by setting the enableLaunchDarkly attribute to False in the Global App Configuration Service.

```
1 {
2
3     "assignedTo": [
4         "AllUsersNoAuthentication"
5     ],
6     "category": "Third Party Services",
7     "settings": [
8         {
9
10            "name": "Enable Launch Darkly",
11            "value": "true"
12        }
13    ],
14     "userOverride": false
15 }
16 }
17
```

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

For more information, see [Global App Configuration Service](#) documentation.

On the on-premises deployment, do the following:

1. Use a text editor to open the web.config file, which is typically at `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:

```
1 <properties>
2 <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. Add the `enableLaunchDarkly` tag and value as false.

```
<property name="enableLaunchDarkly" value="false"/>
```

Note:

Most of the features are behind a feature flag controlled by LaunchDarkly. In the environments where it is disabled, you have to wait for a minimum of 90 days to avail the feature.

Inactivity timeout for Citrix Workspace app sessions

Admins can specify the amount of idle time that is allowed. After the time-out value, an authentication prompt appears.

The inactivity timeout value can be set starting from 1 minute to 24 hours. By default, the inactivity timeout isn't configured. Admins can configure the `inactivityTimeoutInMinutesMobile` property by using a PowerShell module. Click [here](#) to download the PowerShell modules for Citrix Workspace app configuration.

When you have reached the specified time-out value, the end-user experience is as follows depending on the authentication type configured:

- After the inactivity timeout, you will receive a prompt to provide biometric authentication to access the Citrix Workspace app again.
- If you can cancel the biometric authentication prompt, the following message appears:

Citrix Workspace app is locked.

You must authenticate to continue to use the Workspace app.

If the passcode is not configured on the iOS, you have to sign in with credentials after the inactivity timeout.

Note:

This feature is applicable for customers on Workspace (Cloud) only.

Save passwords

Using the Citrix Web Interface Management console, you can configure the authentication method to allow users to save their passwords. When you configure the user account, the encrypted password is saved until the first time the user connects. Consider the following:

- If you enable password saving, Citrix Workspace app for iOS stores the password on the device for future logons and does not prompt for passwords when users connect to applications.

Note:

The password is stored only if users enter a password when creating an account. If no password is entered for the account, no password is saved, regardless of the server setting.

- If you disable password saving (default setting), Citrix Workspace app for iOS prompts users to enter passwords every time they connect.

Note:

For StoreFront direct connections, password saving isn't available.

To override password saving

If you configure the server to save passwords, users who prefer to require passwords at logon can override password saving:

- When creating the account, leave the password field blank.
- When editing an account, delete the password and save the account.

Use the Save Password feature

Citrix Workspace app has a feature that streamlines the connection process by allowing you to save your password, which eliminates the extra step of having to authenticate a session every time you open Citrix Workspace app.

Note:

The save password functionality currently supports the PNA protocol. It does not support StoreFront *native* mode. However, this functionality works when StoreFront enables PNA *legacy*

mode.

Configure StoreFront

To configure StoreFront to enable the save password functionality:

1. If you are configuring an existing Store, go to step 3.
2. To configure a new StoreFront deployment, follow the best practices described in [Install, set up, upgrade, and uninstall](#).
3. Open the Citrix StoreFront management console. Ensure the base URL uses HTTPS and is the same as the common name specified when generating your SSL certificate.
4. Select the Store that you want to configure.
5. Click **Configure XenApp Service Support**.
6. Enable **XenApp Service support**, select the **Default store** (optional), and Click **OK**.
7. Navigate to the template configuration file at c:\inetpub\wwwroot\Citrix\\Views\PnaConfig\.
8. Make a backup of Config.aspx.
9. Open the original Config.aspx file.
10. Edit the line <EnableSavePassword>**false**</EnableSavePassword> to change the **false** value to **true**.
11. Save the edited Config.aspx file.
12. On the StoreFront server, run PowerShell with administrative rights.
13. In the PowerShell console:
 - a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`
 - b. Type "Set-ExecutionPolicy RemoteSigned"
 - c. Type ".\ImportModules.ps1"
 - d. Type "Set-DSServiceMonitorFeature -ServiceUrl" <https://localhost:443/StorefrontMonitor>
14. If you have a StoreFront group, run the same commands on all the members in the group.

Configure Citrix Gateway to save passwords

Note:

This configuration uses Citrix Gateway load balance servers.

To configure Citrix Gateway to support the save password functionality:

1. Log in to the Citrix Gateway management console.
2. Follow the Citrix best practices to create a certificate for your load balance virtual servers.
3. On the configuration tab, navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.
4. Enter the server name and IP address of the StoreFront server.
5. Click **Create**. If you have a StoreFront group, repeat step 5 for all the servers in the group.
6. On the configuration tab, navigate to **Traffic Management > Load Balancing > Monitor** and click **Add**.
7. Enter a name for the monitor. Select **STOREFRONT** as the Type. At the bottom of the page, select **Secure** (required since the StoreFront server is using HTTPS).
8. Click the **Special Parameters** Tab. Enter the StoreFront name configured earlier, and select the **Check Backed Services** and click **Create**.
9. On the **Configuration** tab navigate to **Traffic Management > Load Balancing > Service Groups** and click **Add**.
10. Enter a name for your Service Group and set the protocol to **SSL** and click **Ok**.
11. On the right-hand of the screen under Advanced Settings, select **Settings**.
12. Enable Client IP and enter the following for the Header value: **X-Forwarded-For** and click **OK**.
13. On the right-hand of the screen under Advanced Settings, select **Monitors**. Click the arrow to add new monitors.
14. Click the **Add** button and then select the **Select Monitor** drop-down menu. A list of monitors (configured on Citrix Gateway) appears.
15. Click the radio button beside the monitors that you created earlier and click **Select**, then click **Bind**.
16. On the right-hand of the screen (under Advanced Settings), select **Members**. Click the arrow to add new service group members.
17. Click the **Add** button and then select the **Select Member** drop-down menu.
18. Select the **Server Based** radio button. A list of server members (configured on Citrix Gateway) appears. Click the radio button beside the StoreFront servers than you created earlier.
19. Enter 443 for the port number and specify a unique number for the Hash ID, then click **Create**, then click **Done**. If everything has been configured properly, the **Effective State** should show a green light, indicating that monitoring is functioning properly.
20. Navigate to Traffic Management -> Load Balancing -> Virtual Servers and click **Add**. Enter a name for the server and select **SSL** as the protocol.

21. Enter the IP address for the StoreFront load-balanced server and click **OK**.
22. Select the **Load Balancing Virtual Server Service Group** binding, click the arrow, and add the Service Group created previously. Click **OK** twice.
23. Assign the SSL certificate created for the Load Balance virtual server. Select **No Server Certificate**.
24. Select the Load Balance server certificate from the list and click **Bind**.
25. Add the domain certificate to the Load Balance Server. Click **No CA certificate**.
26. Select the domain certificate and click **Bind**.
27. On the right side of the screen, select **Persistence**.
28. Change the Persistence to **SOURCEIP** and set the time-out to **20**. Click **Save**, then click **Done**.
29. On your domain DNS server, add the load balance server (if not already created).
30. Launch Citrix Workspace app for iOS on your iOS device and enter the full XenApp URL.

Content Collaboration Service integration

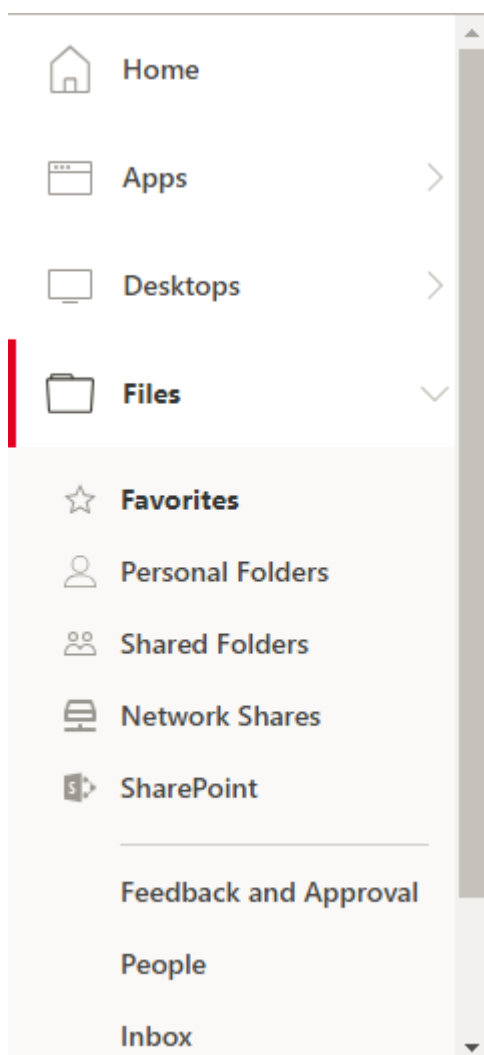
Citrix Content Collaboration enables you to easily and securely exchange documents, send large documents by email, securely handle document transfers to third parties, and access a collaboration space. Citrix Content Collaboration provides many ways to work, including a web-based interface, mobile clients, 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:

Citrix Content Collaboration integration in Citrix Workspace app isn't supported on Windows Server 2012 and Windows Server 2016 due to a security option set in the operating system.

The following image displays 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.

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 the Workspace app for iOS and automatically sends the data to Google Firebase.	This data helps Citrix improve the quality, reliability, and performance of the Workspace app.

Additional Information

Citrix handles your data in accordance with the terms of your contract with Citrix, and protects it as specified in the [Citrix Services Security Exhibit](#) available on the [Citrix Trust Center](#).

Citrix uses Google Firebase to collect certain data from Citrix Workspace app as part of CEIP. Review how Google [handles data collected for Google Firebase](#).

To stop sending CEIP data to Citrix and Google Firebase:

1. Open Citrix Workspace app for iOS.
2. Tap **Home** > **Settings**.
3. Navigate to the **General** section.
4. Disable the **Send Usage Statistics** option.

Note:

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

The specific CEIP data elements collected by Google Firebase are:

Session information and session launch method	Citrix stores and store configuration	Auth type and authentication configuration	ICA connections
HDX session launch	Store app session	WebView action open	WebView action copy
WebView action share	Workspace app review	Connection status, connection error, connection center usage	External display
Socket status	Session duration	HDX over UDP	Session launch time

Device information	Device model info	Send usage statistics	App language, Workspace app language
Keyboard language	Citrix store type	Citrix store combination	Store protocol type
Store count	HDX UDP status	RSA token installations	

Citrix Ready workspace hub

The Citrix Ready workspace hub combines digital and physical environments to deliver apps and data within a secure smart space. The complete system connects devices (or things), like mobile apps and sensors, to create an intelligent and responsive environment.

Citrix Ready workspace hub is built on the Raspberry Pi 3 platform. The device running Citrix Workspace app connects to the Citrix Ready workspace hub and casts the apps or desktops on a larger display.

For more information about the Citrix Ready workspace hub, see [Citrix Ready workspace hub](#) documentation.

Citrix Ready workspace hub supports a Secure Sockets Layer (SSL) connection between mobile devices and the hub for security purposes. Set a Fully Qualified Domain Name (FQDN) either manually or automatically to uniquely identify each device. For more information, see [Security connection](#) in the Citrix Ready workspace hub documentation.

Citrix Ready workspace hub is enabled on Citrix Workspace app when all the following system requirements are met:

- Citrix Workspace app 1810.1 for iOS or later
- Bluetooth enabled
- Mobile device and workspace hub using the same Wi-Fi network

Configure

To turn on Citrix Ready workspace hub features, go to **Settings** and tap **Citrix Casting** to enable the feature on your device. For more information, see the help documentation for the [iOS](#) devices.

Citrix Workspace app integrates a new procedure to add or to remove a workspace hub from the trusted list on iOS devices. For more information, see [Security Connection](#).

Known limitation

- On VDA 7.18 and earlier, casting to a workspace hub requires the desktop or other resource you are using to have the .h264 full-screen policy enabled and the legacy graphics policy to be disabled.

Session sharing

When users log off from a Citrix Workspace app account, if there're still connections to applications or desktops, users have the option to disconnect or log off:

- **Disconnect:** Logs off from the account but leaves the Windows application or desktop running on the server. The user can then start another device, launch Citrix Workspace app for iOS, and reconnect to the last state before the user disconnects from the iOS device. This option allows users to reconnect from one device to another device and resume working in running applications.
- **Log off:** Logs off from the account, closes the Windows application, and logs off from the Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server. This option allows users to disconnect from the server and log off from the account. When they launch Citrix Workspace app for iOS again, it opens in the default state.

Workspace with intelligence

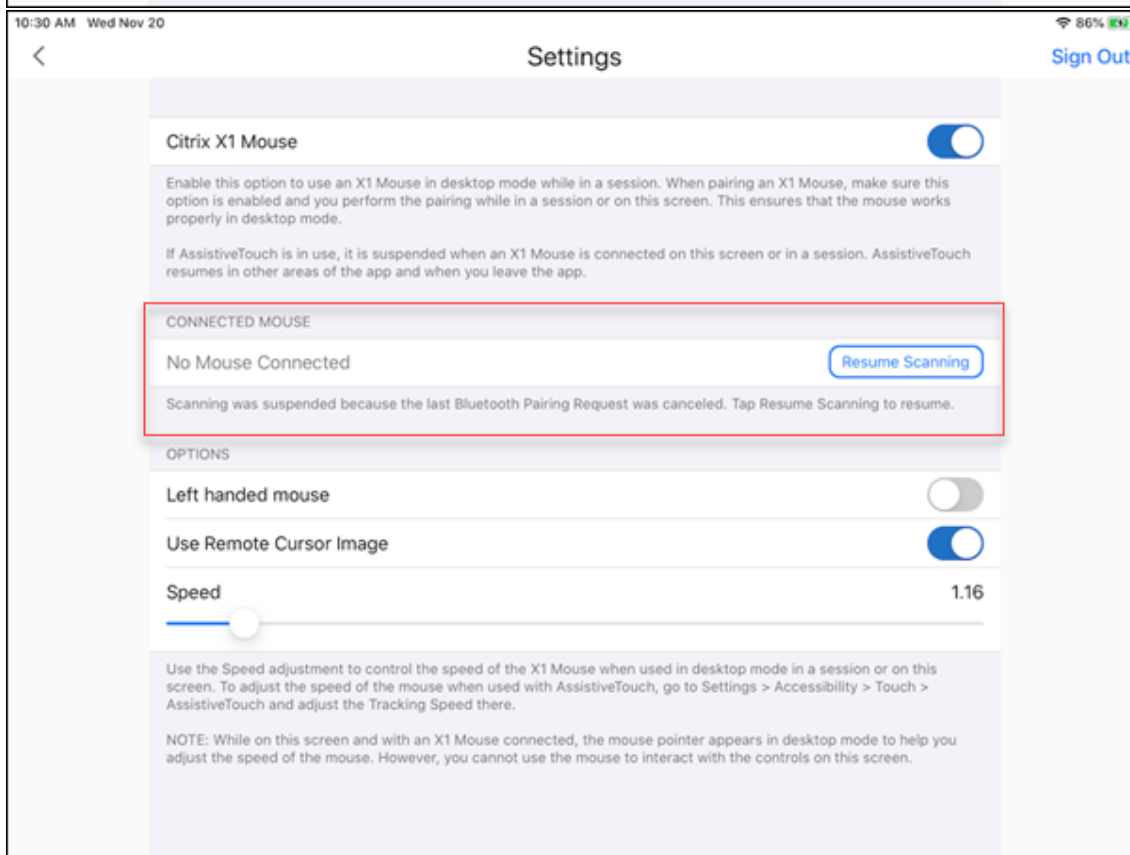
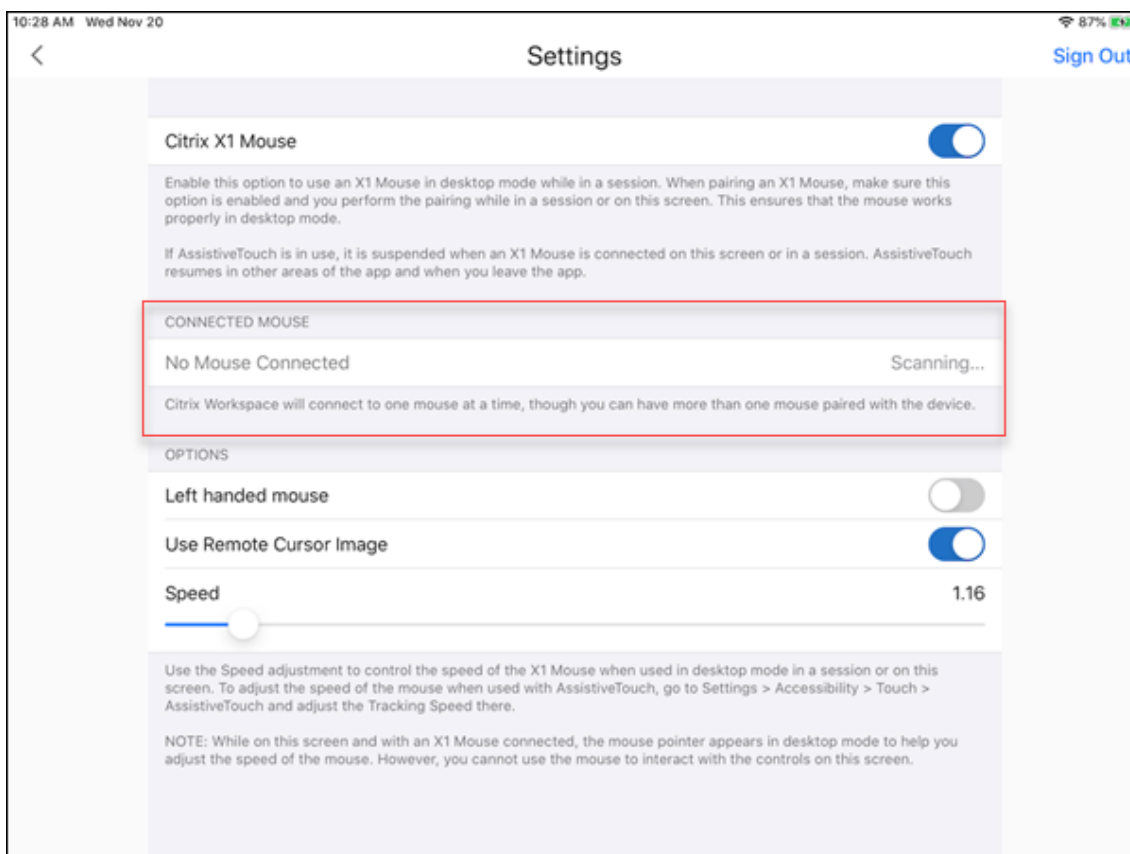
Starting with the 1911 release, the app is optimized to take advantage of the upcoming intelligent features when they're released. For more information, see [Workspace Intelligence Features - Microapps](#).

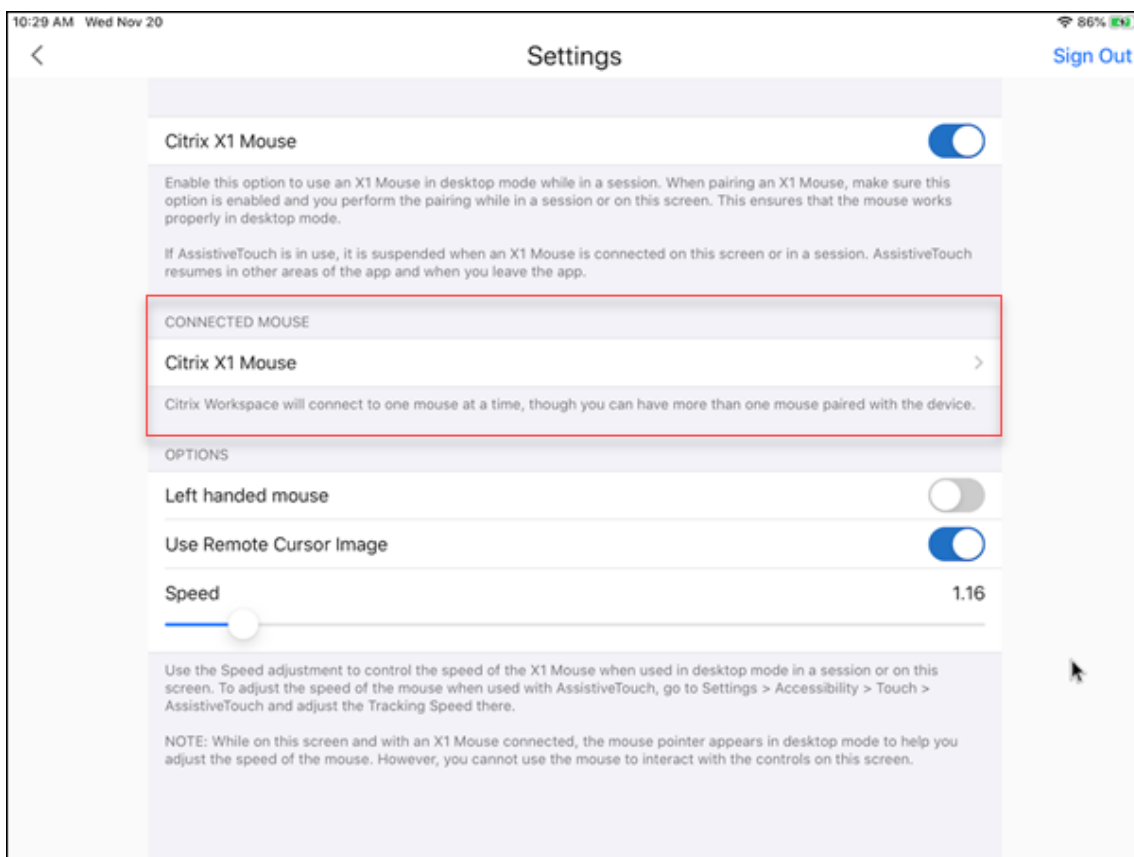
Citrix X1 Mouse

Citrix X1 Mouse pairing and connection status

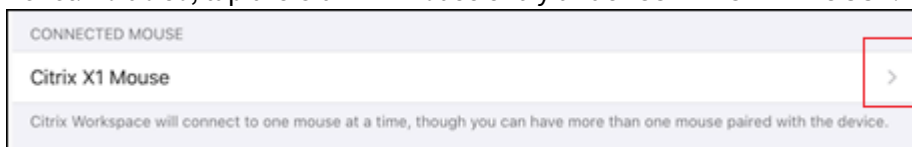
This feature lets you have more control over the Citrix X1 Mouse pairing process. On the **Settings** screen, you can:

- Pair the Citrix X1 Mouse. You can also pair an X1 Mouse when you are in a session.
- View the connection status.

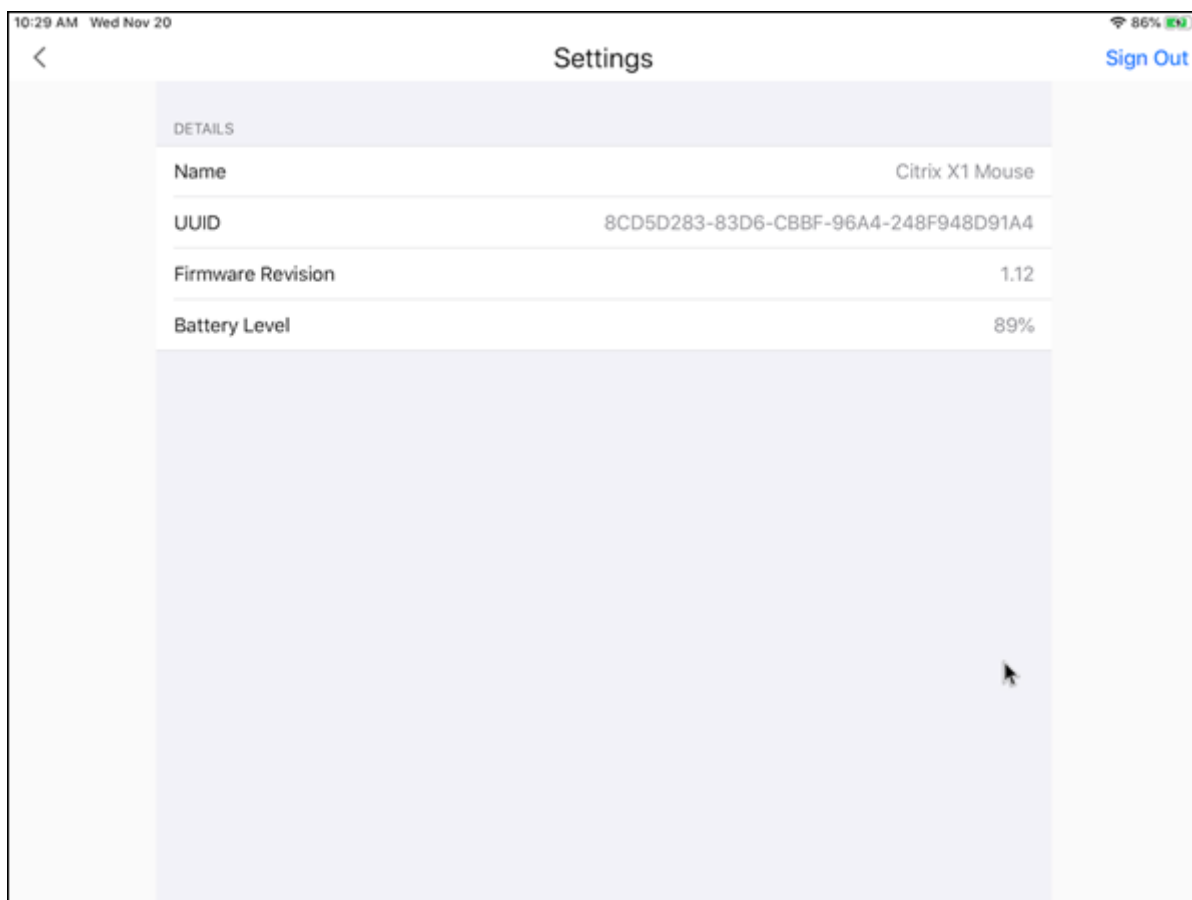




- View the Citrix X1 Mouse properties such as **Name**, **UUID**, **Firmware Revision**, and **Battery Level**. To do so, tap the Citrix X1 Mouse entry under **CONNECTED MOUSE**.



Connected mouse properties:



AssistiveTouch

With the AssistiveTouch feature enabled on iOS 13 or later, you can see the AssistiveTouch cursor if you switch between desktop mouse mode and AssistiveTouch mode.

Note:

In desktop mouse mode, the pointer cursor appears. In AssistiveTouch mode, the round cursor appears.

The AssistiveTouch cursor appears when you:

- Leave a session
- Go to the iOS App Switcher screen
- Go to the iOS home screen or another app

Desktop mode resumes when you navigate back to Citrix Workspace app and when you are in a session.

External monitor and toolbar support

You can use the Citrix X1 Mouse to operate the toolbar on an external monitor. You can move the toolbar notch horizontally, while the toolbar is closed. When you connect your iOS device to the external monitor, Citrix Workspace app automatically detects the screen resolution of the external monitor. You can use the **Display** button on the toolbar to select a particular screen resolution. You can access the **Display** option without having to add an account or sign in first.

Generic Mouse

Generic mouse and trackpad support

You can use a generic mouse or trackpad to right-click, scroll, and hover in HDX sessions. The actions are similar to the Citrix X1 Mouse. The style of the local mouse cursor changes to match that of the remote cursor.

Notes:

- This feature is available on iPadOS 13.4 and later.
- This feature isn't supported on iPhones.

Limitation

If you have an external monitor connected while in a session, the generic mouse cursor remains on the native device due to an iOS limitation.

Generic mouse support on external monitors

You can use a generic mouse on external monitors connected to an iPad. Generic mouse is supported on devices running iOS 13.4 or later.

Important:

To use a generic mouse with external monitors, ensure that **Presentation** mode is turned off in your Citrix Workspace app by navigating to **Settings > Display options**.

The toolbar on the external monitor is hidden when you use a generic mouse. Also, the mouse pointer is mirrored on the external monitor and appears on both your iPad screen and on the external monitor simultaneously.

Session roaming on iPad

Starting with the 1906 release, session roaming is available on iPhone and iPad touch devices when using a cloud store. For more information, see the help documentation for [iOS devices](#).

Keyboard layout synchronization

Keyboard layout synchronization enables users to switch preferred keyboard layouts on the client device. This feature is disabled by default.

To enable keyboard layout synchronization, go to **Settings > Keyboard Options** and enable the **Keyboard Layout Sync** option.

Note:

Using the local keyboard layout option activates the client IME (Input Method Editor). If you are working in Japanese, Chinese, or Korean language and prefer to use the server IME, disable the local keyboard layout option by clearing the option in **Preferences > Keyboard**.

Special key support

Support for the following single keys on an external keyboard of iOS 13.4 and later:

- PageUp
- PageDown
- Home
- End
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Special key combinations support

This release adds support for the following key combinations on iOS external keyboards:

- Windows + R
- Windows + D
- Windows + E
- Windows + L

- Windows + M
- Windows + S
- Windows + CTRL+ S
- Windows + T
- Windows + U
- Windows + Number
- Windows + UP
- Windows + Down
- Windows + Left
- Windows + Right
- Windows + X
- Windows + K
- CTRL + ESC

Host to client redirection

Content redirection allows you to control whether users access information by using applications published on servers or applications running locally on user devices.

Host to client redirection is one type of content redirection. It is supported only on Server OS VDAs (not Desktop OS VDAs).

When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs. If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA. When host to client redirection is disabled, users open the URLs with web browsers or multimedia players on the server VDA.

When host to client redirection is enabled, users cannot disable it.

Host to client redirection was previously known as server to client redirection.

For more information, see [General content redirection](#).

Support for Purebred derived credentials

Starting with the 1810 release, Citrix Workspace app for iOS introduces support for Purebred derived credentials. When connecting to a Store that allows derived credentials, users can log on to Citrix Workspace app for iOS using a virtual smart card. This feature is supported only on on-premises deployments.

Note:

Citrix Virtual Apps and Desktops 7 1808 or later is required to use this feature.

For information on configuring derived credentials, see [Derived credentials](#).

Webpage

External sharing of webpages

You can share the webpages you open from Citrix Workspace app with others. You can:

- copy a link from within a webview
- directly open a webpage in Safari
- send links directly to people or apps

To do share, tap the ... icon on the top right of the webview or long tap any link within the webview and tap the option you need.

Webview

Enhanced webview with native controls for SaaS apps

You can have an enhanced webview with native controls for SaaS apps. This enhancement allows you to:

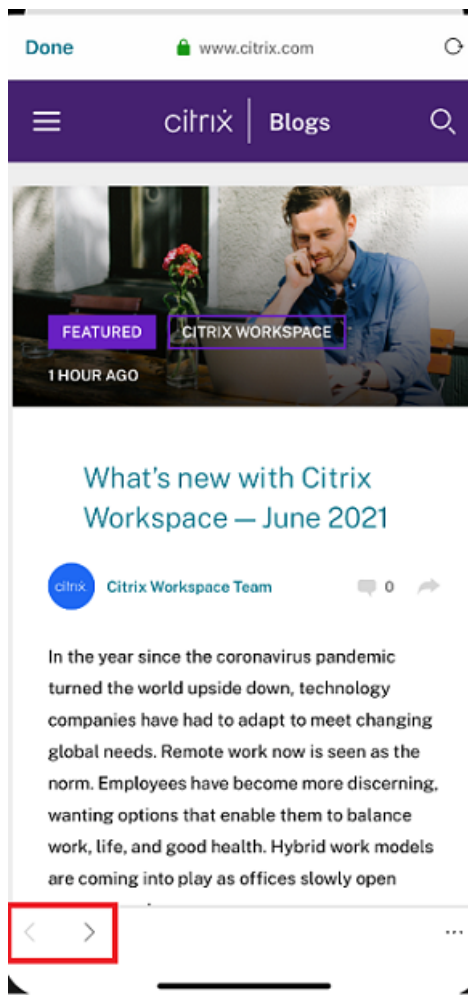
- View the URL of your apps.
- View the security information of your apps.
- Share your apps.

Also, you can now swipe your apps left and right to move forward and backward, respectively.

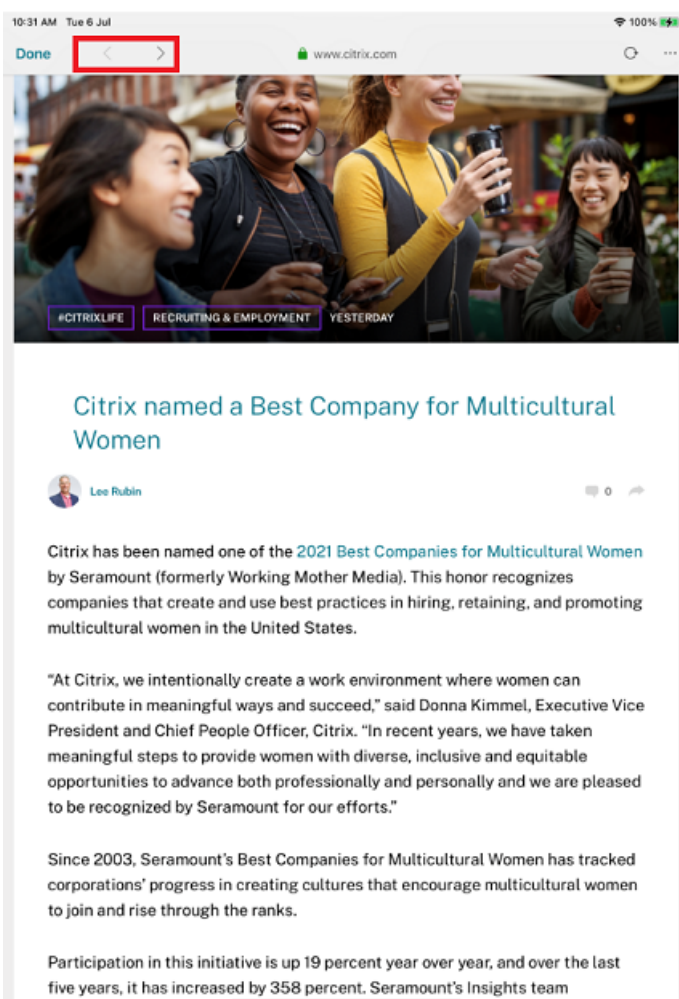
Usability enhancement

The usability enhancement lets you navigate back and forth within web and Software-as-a-Service (SaaS) apps, in addition to the microapp view.

The navigation buttons appear at the bottom left of your Workspace web and SaaS app sessions of your iPhone.



The navigation buttons appear at the top left of your Workspace web and SaaS app sessions of your iPad.



Client Drive Mapping (CDM)

You can select a specific device storage access for every configured store. Device storage access has the following options.

- No access
- Read-only access
- Read and write access
- Ask me every time

If you select **Ask me every time**, a prompt appears, asking you to select the type of device storage access at every launch. By default the **No access** option is selected.

Note:

This feature applies only on direct ICA launches and Citrix Gateway configured stores. Stores without end-to-end SSL setup aren't supported.

The **Device Storage** settings are available under a new section in the settings called **Store Settings**. To view **Device Storage**, navigate to **Settings > Store Settings**.

Microphone and camera access

You can now access your microphone and camera for audio-video conferencing through a VDA session. Citrix Workspace app requires your permission to access microphone or camera which can be provided by navigating to **Settings** on your device and enabling camera or microphone.

Also, per-store microphone and camera access as a part of the client-selective trust security feature has been included to allow Citrix Workspace app to trust access from a VDA session.

Citrix Workspace app requires the user's permission to access the microphone or camera.

You can configure the access levels by navigating to **Settings > Store Settings**. In the **Store Settings** menu, click a store to enable the required microphone or camera access. The selected setting for microphone or camera access is applied on a per-store basis.

Cloud stores

You can access the web, SaaS apps, and websites hosted by your organization, regardless of your access location. This feature is available only for customers on cloud stores.

Citrix Workspace mobile app web viewer

The web viewer is an in-app browsing solution running within the Citrix Workspace app. It enables users to open web or SaaS apps from the Citrix Workspace app in a secure manner. The web viewer 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 web viewer brings you an enhanced and a more native browser-like experience, complete with the following features:

- VPN-less access to internal webpages
- SSO for web and SaaS with Adaptive access policies
- File downloading with preview
- Seamless navigation between pages and sites
- Ability to share URLs
- Find in page
- Same view when accessing links through the activity feed

Administrators can enable Secure Private Access (SPA) including download, clipboard, navigation restrictions, file upload, and watermarking in varying combinations on a per-URL basis.

User experience

EDT stack parameters enabled by default

The **Read EDT stack parameter** option is removed from **Advanced > Adaptive Transport Settings** and is enabled in the background by default. This update provides a better user experience by ensuring that you don't have to enable this feature when you install Citrix Workspace app for iOS.

End user experience monitoring enhancement

We now support the EUEM (End user experience monitoring) client startup metrics. EUEM helps in collecting highly granular session experience monitoring data in real time. It sends the data to the Director dashboard, so that the administrator can monitor the user experience. The data is collected through the Session experience monitoring service (SEMS) present on the VDA. Client startup metrics data available for monitoring on the dashboard includes:

- ICA file download duration.
- Session creation client duration. Session creation client duration represents the time taken to create a session, from the moment an ICA file is launched to the time when the connection is established.
- Session lookup client duration. Session lookup client duration represents the time taken to query every session for hosting the requested published application. The check is performed on the client to determine whether an existing session can handle the application launch request.
- Citrix real-time recording of the ICA round trip time, also known as ICA RTT. ICA RTT is the time that elapses from when the user presses a key until the response is displayed at the endpoint.

Battery status indicator

The battery status of the device now appears in the notification area within the virtual desktop session. This feature is supported only on VDA versions 7.18 and later.

Note:

In sessions running on Microsoft Windows 10 VDAs, the battery status indicator might take about 1 to 2 minutes to appear.

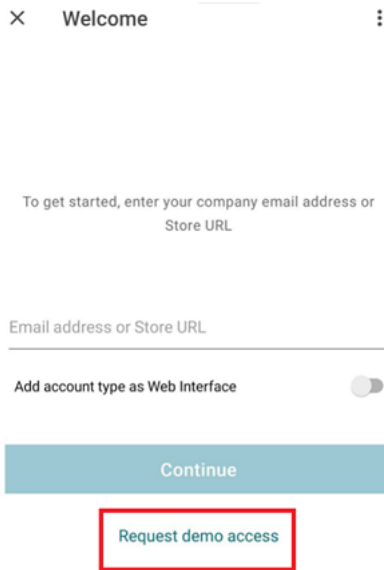
Free demo access

Trying out the Citrix Workspace experience on mobile devices just got easier. Potential users and anyone interested now have free demo access of the Citrix Workspace app for iOS.

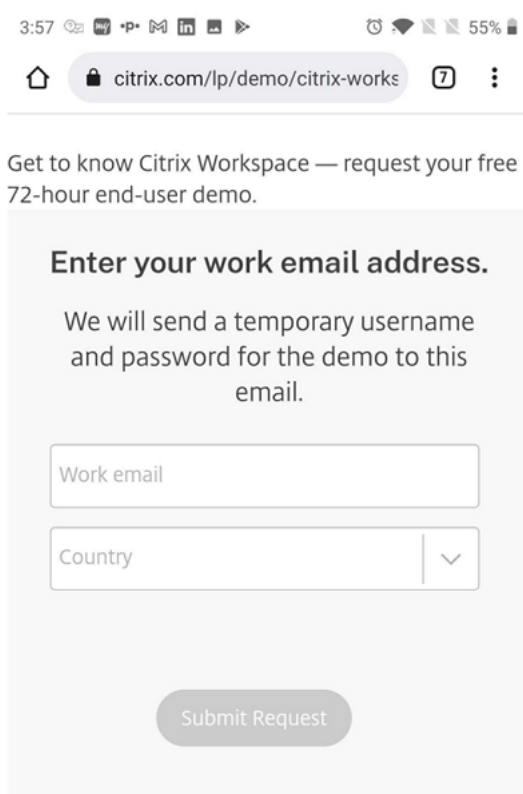
You can get to know about Citrix Workspace app by requesting a free 72-hour trial.

To request free demo access:

1. Tap **Request demo access** on the **Citrix Workspace app Sign in** screen.



-
2. The Citrix request demo access webpage appears.
 3. Enter your required details like name, company, address, phone number, city, work email address, and then tap **Submit Request**.



3:57 [notification icons] [signal strength] [Wi-Fi] [55% battery]

citrix.com/lp/demo/citrix-works

Get to know Citrix Workspace — request your free 72-hour end-user demo.

Enter your work email address.

We will send a temporary username and password for the demo to this email.

Work email

Country ▼

Submit Request

4. You receive a temporary user name and password on your work email address. Enter the temporary user name and password on the **Sign in** screen.
You now have free demo access to Citrix Workspace app for 72 hours.

Long press functionality to access resource

You can now long press the Citrix Workspace app icon and access your most recently launched resource. You can now quit the Citrix Workspace app and access your most recently launched resource.

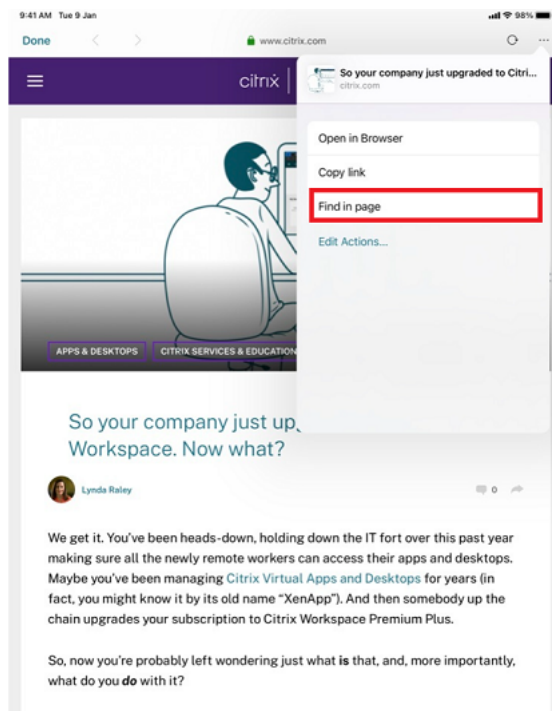
Find in page enhancement

The Find in page enhancement lets you search for words or phrases. This usability enhancement is applicable within your Web, Software-as-a-Service (SaaS) apps, and from the microapp view.

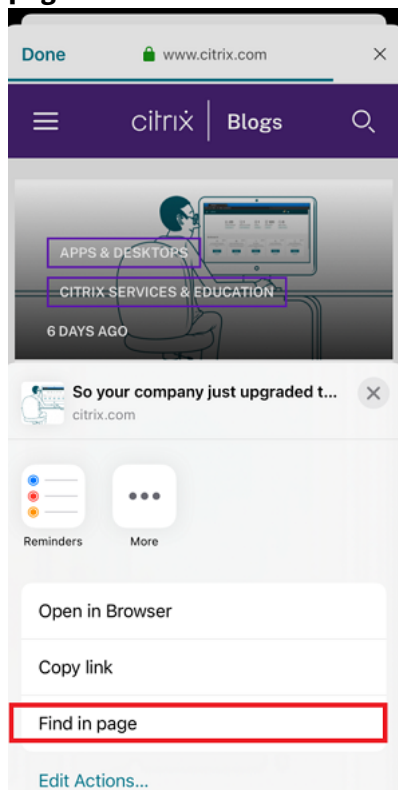
To search:

1. On your iPad, tap the ellipsis (...) button on the upper-right corner and then select **Find in page**.

Citrix Workspace app for iOS

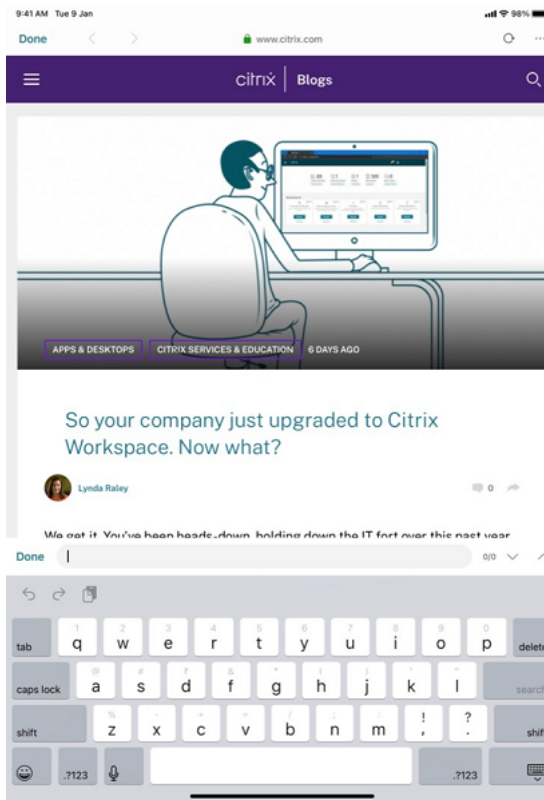


On your iPhone, tap the ellipsis (...) button on the lower-right corner and then select **Find in page**.

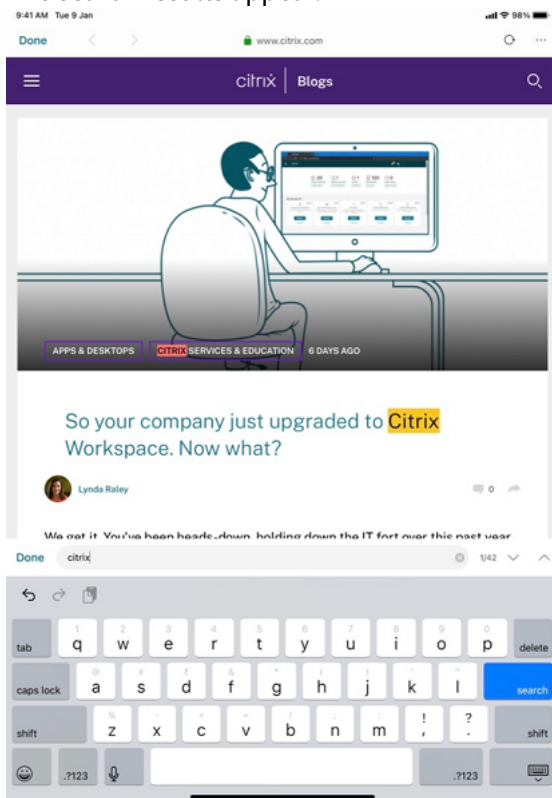


The on-screen keyboard appears.

Citrix Workspace app for iOS



2. Type the text that you want to search for in the text box (for example, type the word “Citrix”). The search results appear.

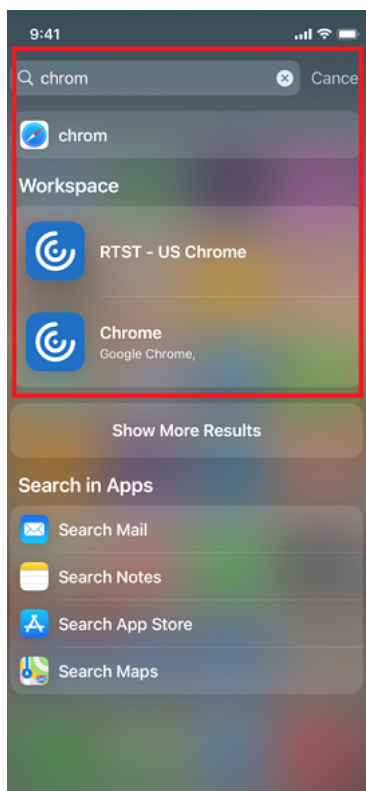


Access of apps and desktops through Spotlight search

You can use Spotlight search to find your desktops and your Web, SaaS (Software-as-a-Service), and desktop apps. You can then access these apps and desktops directly from Spotlight search without launching Citrix Workspace app.

Note:

The Spotlight search feature doesn't support mobile apps.



Reposition the in-session toolbar

You can reposition the in-session toolbar either on the top or on the right of the screen. When you drag the toolbar notch away from the toolbar edge, the rectangle drag indicator and the drop target appear. Drop the drag indicator over the drop target to reposition the toolbar.

Notes:

- The feature is applicable for iPad users only.
- The feature functions with touch or mouse.
- The feature functions with an iPad or on an external display.
- The last toolbar position persists for the next session or the application launch.

Feeds widget

You can configure and view the Citrix Workspace app notification feeds using a widget. You can add it on the iOS home screen. This feature enhances your experience and lets you view the recent feeds.

Tapping the feed opens the detailed view on the Citrix Workspace app. This feature supports iOS version 14.0 and later.

Note:

This feature supports cloud accounts. However, if there's no cloud account configured, the widget displays an appropriate message to add a Workspace store.

To configure the notification feed widget:

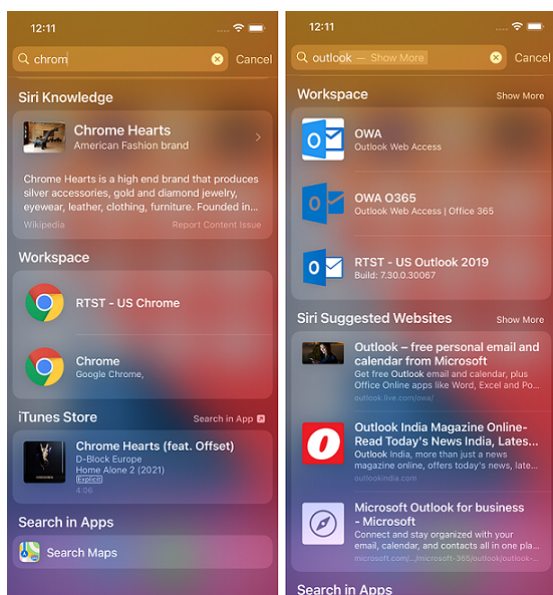
1. Touch and hold anywhere on the home screen. The apps begin to jiggle.
2. Tap the **+** button at the top of the screen. The **Search Widget** screen appears.
3. Enter the word **Workspace** in the search box and tap the **Citrix Workspace app**. The **Activity Feed** screen appears.
4. Click **Add Widget**. The widget appears on the home screen.
5. Click **Done**. You can now interact with the **Feeds** widget.

Note:

To remove the widget, tap and hold the widget to open the **quick actions** menu. Tap **Remove Widget**, then tap **Remove**.

Spotlight search enhancement

The app icon matches the corresponding app search. Previously, the Citrix Workspace app icon was displayed for all the searches.



Accessing recent apps by 3D-Touch gesture

You can access a list of recently launched apps for quick access when you use the 3D-Touch (long-press) gesture on the **Citrix Workspace app** icon.

Migration from on-premises to cloud account

Administrators can seamlessly migrate the end users from an on-premises StoreFront store URL to a Workspace URL. Administrators can do the migration with minimum end user interaction using the [Global App Configuration Service](#).

To configure:

1. Navigate to the [Global App Configuration Store Settings API](#) URL and enter the cloud store URL. For example, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigate to **API Exploration > SettingsController > postDiscoveryApiUsingPOST** > click **POST**.
3. Click **INVOKE API**.
4. Enter and upload the payload details. Enter the StoreFront store expiry date in the epoch timestamp in milliseconds format.

For example,

```
1  "migrationUrl": [  
2  {  
3  
4  
5  "url": "<cloud store url>"  
6  "storeFrontValidUntil": "<epoch timestamp in milliseconds>",  
7  }  
8  
9  ] ,  
10 <!--NeedCopy-->
```

5. Click **EXECUTE** to push the service.

End user Experience

As an end user, if you're using the Citrix Workspace app for the first time, after successful authentication, the **Introducing the new Citrix Workspace** migration screen appears (if eligible). After you tap the **Try new Citrix Workspace now** option, migration begins. Upon successful migration, you can access the Workspace store (cloud store).

Note:

You can skip the migration for three attempts. Later, the migration is forced without an option to skip.



After you migrate to the Workspace (cloud) store, you can view both the StoreFront and the Workspace store under **Settings**. When you switch from a cloud store to the on-premises StoreFront store, a feedback screen appears to gather your response.

Note:

The StoreFront store has an expiry date. Post the expiry date, the store gets deleted.

Extended multi-monitor support with Generic Mouse for iPad

Note:

This feature is in [preview](#) for version 22.3.5 and earlier.

You can extend the desktop session onto an external monitor when you connect your iPad with a Generic Mouse. This feature supports iPadOS version 14.0 and later.

Note:

- This feature can be partially available in earlier versions. To use the complete feature, upgrade to version 22.1.0.
- Disable AssistiveTouch in iOS **Settings** > **Accessibility** > **Touch** > **AssistiveTouch** for the Citrix Workspace app to receive primary mouse clicks.

Configure Extend mode

To enable the **Extend** mode:

1. Connect the external monitor to the iPad using the HDMI cable and the required adapters.

Note:

The setup works best with an Apple's USB-C to Digital AV Multiport Adapter or Lightning Digital AV Adapter.

2. Navigate to the application **Settings > Display options** and toggle **ON** the **External display**. Different display modes appear. Mirror and Presentation modes also use Generic Mouse, if the iPadOS version is 14.0 and later.

3. Select the **Extend** option.

You can select one of the following display modes:

- **Mirror:** Allows you to mirror the display on the external monitor connected to the iPad.
- **Presentation:** Allows you to change your external monitor to trackpad.
- **Extend:** Allows you to display different views or screens on each display.

Note:

- Set the **Extend** mode before you launch and extend the desktop session.
- The **Extend** mode isn't supported on the iPhone until announced.

Configure display arrangement

To configure the display arrangement:

1. Select the **Extend** mode, the **Display arrangement** option appears.
2. Reposition the **External display** tile left, top, right, or bottom to the iPad display.

Note:

You can adjust the display arrangement when you're in a session using the in-session toolbar > **Display** setting icon.

Note:

The external display resolution depends on:

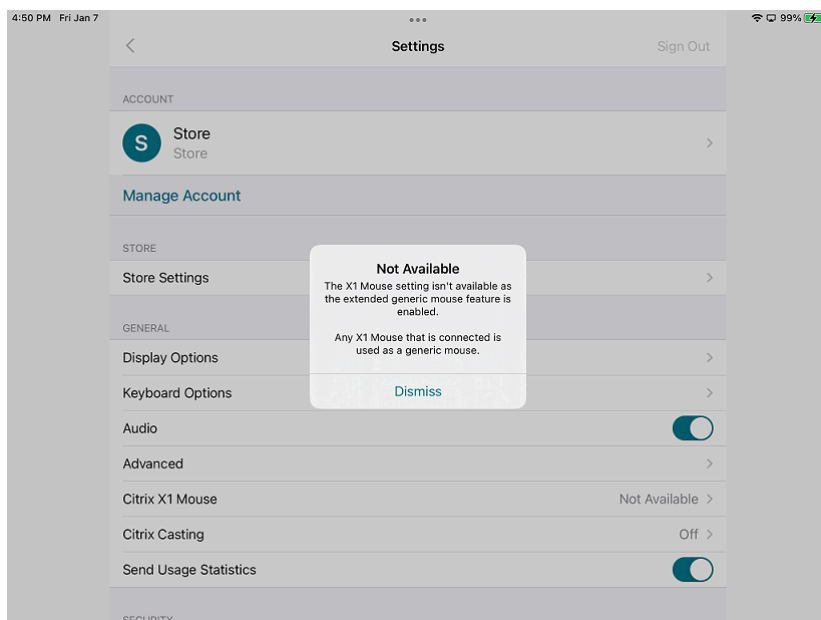
- adapters
- iPad
- other hardware used

Generic Mouse mode versus Citrix X1 Mouse mode

The Generic Mouse mode automatically takes precedence over the Citrix X1 Mouse mode. If you have an X1 Mouse connected, it's used as a Generic Mouse instead. So, the X1 Mouse settings page isn't accessible when the Generic Mouse feature flag is enabled.

Note:

For iPadOS version 14.0 and later, any X1 Mouse that is connected to the iPad behaves as a Bluetooth mouse.

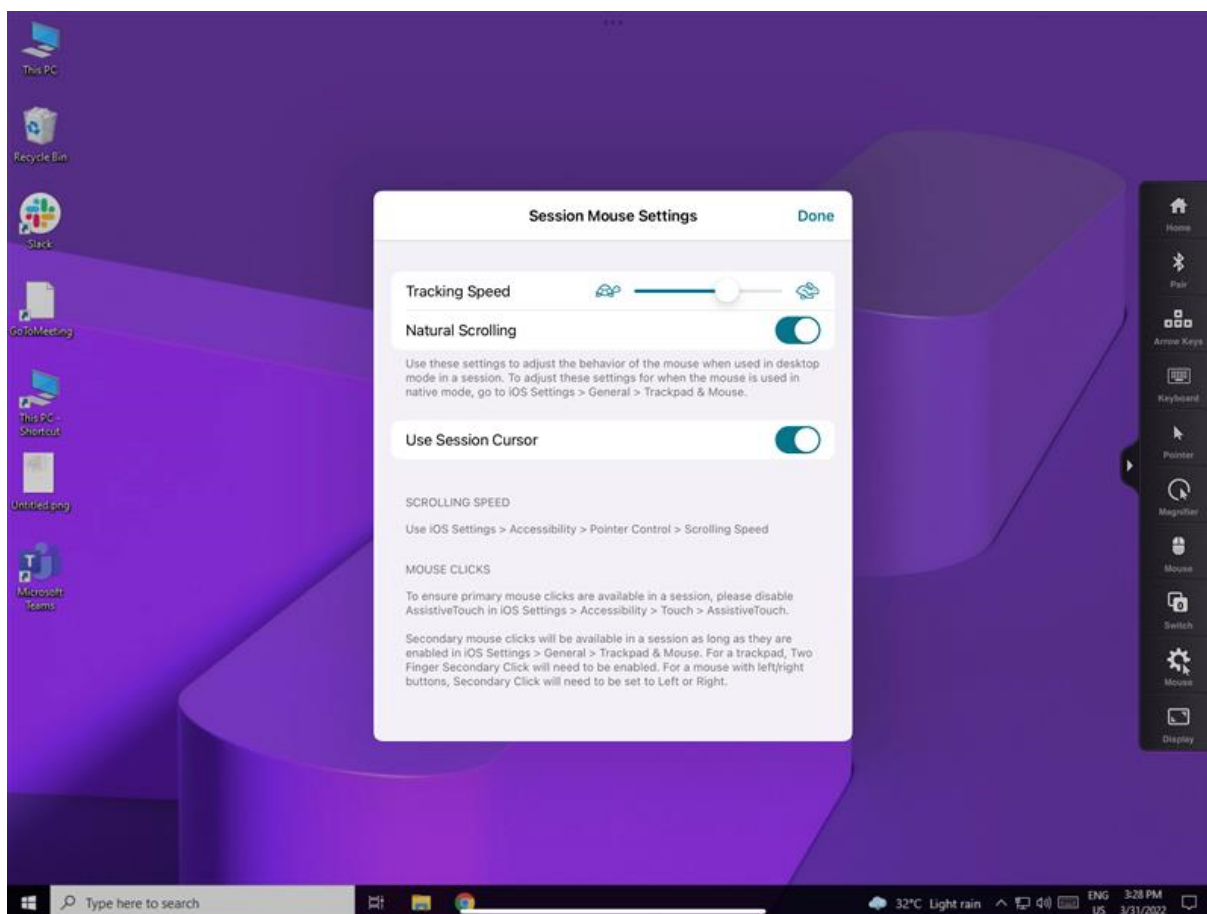


Generic Mouse icon

The **Mouse** settings icon is added on the in-session toolbar next to the **Display** settings icon. Use the **Mouse** settings to adjust the tracking speed of the Generic Mouse when you are in a session. You can also toggle using the remote cursor image.

Note:

You can adjust the tracking speed of the native mouse from the iOS settings.



Feature limitations

- To ensure that the Citrix Workspace app receives primary mouse clicks, disable AssistiveTouch in iOS **Settings > Accessibility > Touch > AssistiveTouch**.
- Tracking Speed and Natural Scrolling options from iOS settings doesn't affect the generic mouse inside the session. However, scrolling speed can be controlled from the iOS **Settings**. You can access Tracking speed and Natural scrolling options from the **Mouse Settings** screen inside the session toolbar.
- When an iPad is used in the split mode and the monitor is connected, the generic mouse works only in the mirror mode inside a desktop session.
- If the native cursor is over the multi-tasking menu before the app obtains the pointer lock, that is, before the session launch, the mouse events aren't received. As a workaround, pull down the Notification Center and move the native pointer to a different location and dismiss the Notification Center.
- Audio redirection fails when you connect an iPad to an external monitor. The audio plays through the iPad speakers. [HDX-39159]

Known issues in the feature

- While the session is active, the desktop image that appears on an iPad or an external monitor gets disturbed when you change the:
 - Display arrangement
 - Resolution
 - Orientation or
 - Display modes

As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].

- On rare occasions, you can observe a few seconds lag in the audio when the video is played on the external monitor. [HDX-39159]
- On rare occasions, the VDA display is truncated on an iPad and on the external monitor. As a workaround, disconnect, and reconnect the monitor. If the issue persists, disconnect and relaunch the session. [HDX-37100]
- When you maximize the video to full-screen on the external monitor, you might observe video quality issues. [HDX-39159]
- On rare occasions, inside a desktop session, an attempt to move the apps from an iPad to the external monitor fails. As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-36981]
- On rare occasions, when you connect an iPad to an external monitor using third-party adapters, the Display Modes aren't visible under the Display Options. [HDX-39713]
- Sometimes, a line is observed under the mouse pointer inside the VDA session. [RFIOS-9569]

Siri integration

You can interact with Siri to launch resources like apps and desktops without launching Citrix Workspace app each time.

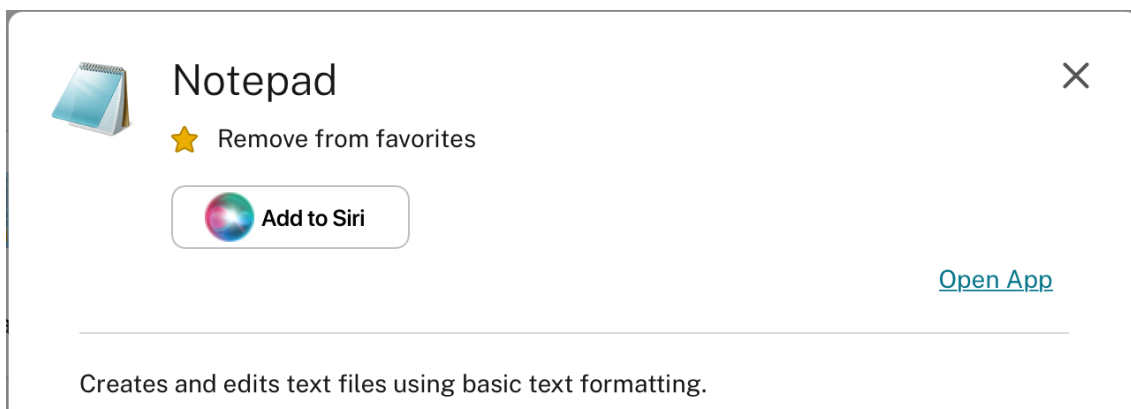
For more information, see [Siri integration](#) in the Configure section.

To configure

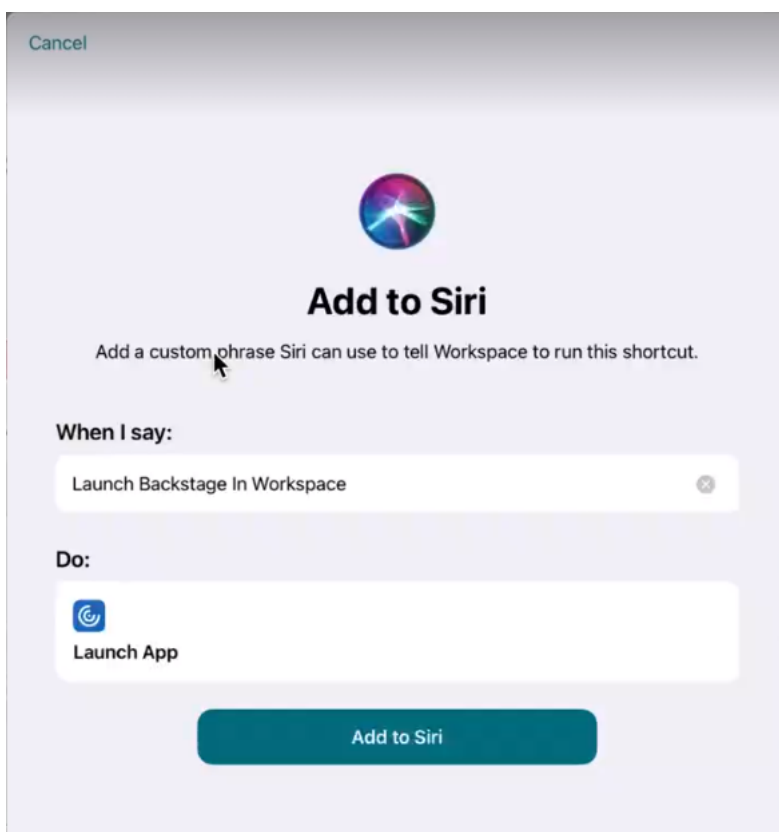
1. Launch Citrix Workspace app and tap **Apps** or **Desktops**. Select the resource that you want to add to the Siri shortcut.
2. Tap ellipsis (...). A dialog box appears.

Note:

If you are an iPhone or an iPad Desktop user, tap **ellipsis (...)** > **App Details** screen > **View Details**. A dialog box appears. Continue with step 3.



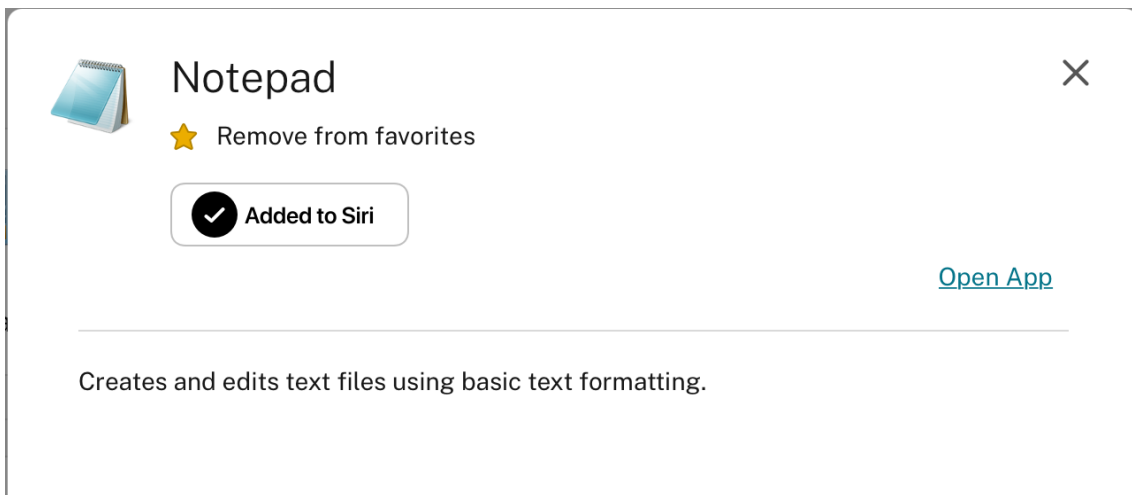
3. Tap **Add to Siri**. The **Add to Siri** dialog box appears.



4. (Optional) Edit the custom phrase for invoking Siri. Tap **Add to Siri**. The resource is now added to the Siri shortcut. Close the dialog box.

Note:

A few devices support recording the custom phrase for invoking Siri.



Application Settings

Launch Citrix Workspace app and tap on your profile icon > **Application Settings** > **Siri Configuration**. To enable the feature, tap **Add to Siri**.

You can now use your voice to launch the resource.

To edit or delete the shortcut

1. Select the resource.
2. Tap ellipsis (...). A dialog box appears.
3. Tap **Added to Siri**. The **Edit Shortcut** dialog box appears.

You can modify the custom phrase for invoking Siri and tap **Save Shortcut** or tap **Delete Shortcut** to remove the existing shortcut.

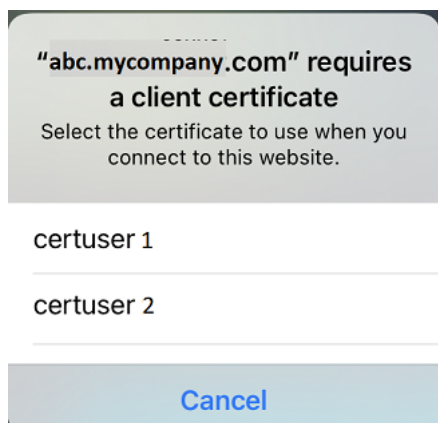
Safari view controller

End users can now handle certificate-based authentication where, the certificates are saved onto the device keychain. While signing in, Citrix Workspace app detects the list of certificates on your device, and you can choose a certificate for authentication.

Important:

After you choose the certificate, the selection persists for the next Citrix Workspace app launch. To choose another certificate, you can "Reset Safari" from iOS device settings or reinstall Citrix

Workspace app.



Note:

This feature supports on-premises deployments.

To configure:

1. Navigate to the [Global App Configuration Store Settings API](#) URL and enter the cloud store URL. For example, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigate to **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > click **POST**.
3. Click **INVOKE API**.
4. Enter and upload the payload details. Select one of the following values:
 - “Embedded”: you can use WKWebView. This option is set by default.
 - “system”: you can use the Safari view controller.

For example,

```
1 "category": "Authentication",
2 "userOverride": false,
3 "settings": [
4 {
5   "name": "Web Browser to use for Authentication", "value": "*
   Embedded*/*System*" }
6 ,
7 <!--NeedCopy-->
```

On iOS or iPad devices, administrators can switch the browser being used for the authentication process from embedded browser to system browser, when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment. For more information, see [Configure Rewrite policy for authentication process](#).

5. Click **EXECUTE** to push the service.

Configure Rewrite policy for authentication process

On iOS or iPad devices, administrators can switch the browser being used for the authentication process from embedded browser to system browser, when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment. To achieve this, configure the NetScaler Rewrite policy by using the Netscaler command line:

1. `enable ns feature REWRITE`
2. `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
3. `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ ("/cgi/authenticate")"insert_auth_browser_type_hdr_act`
4. `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_pol -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Moving to the system browser provides support for additional capabilities such as:

- Better experience with certificate based authentication.
- Ability to use existing user certificate from the devices keystore during authentication process.
- Support for few third-party authenticators like SITHS eID.

Embedded browser is used as the default browser for authentication if the administrator has not configured the above Rewrite policy.

This table lists the browsers that are used for authentication based on the configuration on the NetScaler Gateway and Global App Config Service:

NetScaler Gateway	Global App Configuration Service	Browser used for authentication
System	System	System
System	Embedded	System
Embedded	System	System
Embedded	Embedded	Embedded
No Configuration	System	System
No Configuration	Embedded	Embedded

Authenticate

January 11, 2023

Client certificate authentication

Important:

- When using StoreFront, Citrix Workspace app supports:
 - Citrix Access Gateway Enterprise Edition Version 9.3
 - NetScaler Gateway Version 10.x through Version 11.0
 - Citrix Gateway Version 11.1 and later
- Citrix Workspace app for iOS supports client certificate authentication.
- Only Access Gateway Enterprise Edition 9.x and 10.x (and later releases) support client certificate authentication.
- Double-source authentication types must be CERT and LDAP.
- Citrix Workspace app also supports optional client certificate authentication.
- Only P12 formatted certificates are supported.

Users signing in to a Citrix Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. Client certificate authentication can also be used with another authentication type, LDAP, to provide double-source authentication.

Administrators can authenticate end users based on the client-side certificate attributes as follows:

- the client authentication is enabled on the virtual server.
- the virtual server requests for a client certificate.
- to bind a root certificate to the virtual server on Citrix Gateway.

When users sign in to the Citrix Gateway virtual server, after authentication, users can extract the user name and domain information from the **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** field in the certificate. It is in the format “username@domain.”

When the user extracts the user name and domain successfully, and provides the other required information, such as password, the authentication is successful. If the user does not provide a valid certificate and credentials, or if the username/domain extraction fails, authentication fails.

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

To configure the XenApp farm

Create a XenApp farm for mobile devices in the Citrix Virtual Apps console or Web Interface console. The console depends on the version of Citrix Virtual Apps that you've installed.

Citrix Workspace app uses a XenApp farm to get information about the applications a user has rights to. The same information is shared to the apps that are running on the device. This method is similar to the way you use the Web Interface for traditional SSL-based Citrix Virtual Apps connections where, you can configure Citrix Gateway.

Configure the XenApp farm for Citrix Workspace app for mobile devices to support connections from Citrix Gateway as follows:

1. In the XenApp farm, select **Manage secure client access** > **Edit secure client access** settings.
2. Change the Access Method to Gateway Direct.
3. Enter the FQDN of the Citrix Gateway appliance.
4. Enter the Secure Ticket Authority (STA) information.

To configure the Citrix Gateway appliance

For client certificate authentication, configure Citrix Gateway with two-factor authentication using the Cert and LDAP authentication policies. To configure the Citrix Gateway appliance:

1. Create a session policy on Citrix Gateway to allow incoming Citrix Virtual Apps connections from Citrix Workspace app. Specify the location of your newly created XenApp farm.
 - Create a session policy to identify that the connection is from Citrix Workspace app. As you create the session policy, configure the following expression and choose Match All Expressions as the operator for the expression:

```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
```

- In the associated profile configuration for the session policy, on the **Security** tab, set **Default Authorization** to **Allow**.

On the **Published Applications** tab, if the setting isn't a global setting (you selected the Override Global check box), verify if the **ICA Proxy** field is set to **ON**.

In the Web Interface **Address** field, enter the URL including the config.xml for the XenApp farm that the device users use, for example:

- /XenAppServerName/Citrix/PNAgent/config.xml
- or
- /XenAppServerName/CustomPath/config.xml.

- Bind the session policy to a virtual server.
- Create authentication policies for Cert and LDAP.

- Bind the authentication policies to the virtual server.
- Configure the virtual server to request client certificates in the TLS handshake. To do so, navigate to the **Certificate > open SSL Parameters > Client Authentication > set Client Certificate to Mandatory**.

Important:

If the server certificate that is used on the Citrix Gateway is a part of a certificate chain, for example, an intermediate certificate, install the certificates on the Citrix Gateway. For information about installing certificates, see the Citrix Gateway documentation.

To configure the mobile device

If client certificate authentication is enabled on Citrix Gateway, users are authenticated based on certain attributes of the client certificate. After authentication, you can extract the user name and domain from the certificate. You can apply specific policies for each user.

1. From Citrix Workspace app, open the **Account**, and in the Server field, type the matching FQDN of your Citrix Gateway server. For example, GatewayClientCertificateServer.organization.com. Citrix Workspace app automatically detects that the client certificate is required.
2. Users can either install a new certificate or choose one from the already installed certificate list. For iOS client certificate authentication, download and install the certificate from Citrix Workspace app only.
3. After you select a valid certificate, the user name and domain fields on the sign-in screen is pre-populated using the user name from the certificate. An end user can type other details, including the password.
4. If client certificate authentication is set to optional, users can skip the certificate selection by pressing Back on the certificates page. In this case, Citrix Workspace app proceeds with the connection and provides the user with the logon screen.
5. After users complete the initial sign-in, they can start applications without providing the certificate again. Citrix Workspace app stores the certificate for the account and uses it automatically for future logon requests.

Smart cards

Citrix Workspace app supports SITHS smart cards for in-session connections only.

If you're using FIPS Citrix Gateway devices, configure your systems to deny SSL renegotiations. For details, see Knowledge Center article [CTX123680](#).

The following products and configurations are supported:

- Supported readers:

- Precise Biometrics Tactivo for iPad Mini Firmware version 3.8.0
- Precise Biometrics Tactivo for iPad (fourth generation) and Tactivo for iPad (third generation) and iPad 2 Firmware version 3.8.0
- BaiMobile® 301MP and 301MP-L Smart Card Readers
- Thursby PKard USB reader
- Feitian iR301 USB reader
- Supported VDA Smart Card Middleware
 - Activelidentity
- Supported smartcards:
 - PIV cards
 - Common Access Card (CAC)
- Supported configurations:
 - Smart card authentication to Citrix Gateway with StoreFront 2.x and XenDesktop 7.x or later or XenApp 6.5 or later

To configure Citrix Workspace app to access apps

1. If you want to configure Citrix Workspace app automatically to access apps when you create an account, in the Address field, type the matching URL of your store. For example:
 - storefront.organization.com
 - netscalervserver.organization.com
2. Select the **Use Smartcard** option when you're using a smart card to authenticate.

Note:

Logons to the store are valid for about one hour. After that time, users must log on again to refresh or launch other applications.

RSA SecurID authentication

Citrix Workspace app supports RSA SecurID authentication for Secure Web Gateway configurations. The configurations are through the Web Interface and for all Citrix Gateway configurations.

URL scheme required for the software token on Citrix Workspace app for iOS: The RSA SecurID software token used by Citrix Workspace app registers the URL scheme com.citrix.securid only.

If end users have installed both the Citrix Workspace app and the RSA SecurID app on their iOS device, users must select the URL scheme **com.citrix.securid** to import the RSA SecurID Software Authenticator (software token) to Citrix Workspace app on their devices.

To import an RSA SecurID soft token

To use an RSA Soft Token with the Citrix Workspace app, as an administrator, ensure that the end users follow:

- the policy for PIN length
- the type of PIN (numeric only and alphanumeric)
- the limits on PIN reuse

After the end user is successfully authenticated to the RSA server, the end user needs to set up the PIN only once. After the PIN verification, they're also authenticated with the StoreFront server. After all the verification, the Workspace app displays available, published applications and desktops.

To use an RSA soft token

1. Import the RSA soft token provided to you by your organization.
2. From the email with your SecurID file attached, select **Open in Workspace** as the import destination. After the soft token is imported, Citrix Workspace app opens automatically.
3. If your organization provided a password to complete the import, enter the password provided to you by your organization and click **OK**. After clicking **OK**, you'll see a message that the token was successfully imported.
4. Close the import message, and in Citrix Workspace app, tap **Add Account**.
5. Enter the URL for the Store provided by your organization and click **Next**.
6. On the Log On screen, enter your credentials: user name, password, and domain. For the Pin field, enter **0000**, unless your organization has provided you with a different default PIN. The PIN 0000 is an RSA default, but your organization might have changed it to follow with their security policies.
7. At the top left, click **Log On**. A message appears to create a PIN.
8. Enter a PIN that is 4 to 8 digits long and click **OK**. A message appears to verify your new PIN.
9. Enter your PIN again and click **OK**. You can now access your apps and desktops.

Next Token Code

Citrix Workspace app supports the next token code feature when you configure Citrix Gateway with RSA SecurID authentication. If you enter three incorrect passwords, an error message appears on the Citrix Gateway plug-in. To sign in, wait for the next token. The RSA server can be configured to disable a user's account if a user logs on too many times with an incorrect password.

Derived credentials

Support for Purebred derived credentials within Citrix Workspace app is available. When connecting to a Store that allows derived credentials, users can log on to Citrix Workspace app using a virtual smart card. This feature is supported only on on-premises deployments.

Note:

Citrix Virtual Apps and Desktops 7 1808 or later is required to use this feature.

To enable derived credentials in Citrix Workspace app:

1. Go to **Settings > Advanced > Derived Credentials**.
2. Tap **Use Derived Credentials**.

To create a virtual smart card to use with derived credentials:

1. In **Settings > Advanced > Derived Credentials**, tap **Add New Virtual Smart Card**.
2. Edit the name of the virtual smart card.
3. Enter an 8-digit numeric-only PIN and confirm.
4. Tap **Next**.
5. Under Authentication Certificate, tap **Import Certificate...**
6. The document picker displays. Tap **Browse**.
7. Under Locations, select **Purebred Key Chain**.
8. Select the suitable authentication certificate from the list.
9. Tap **Import Key**.
10. Repeat steps 5–9 for the Digital Signature Certificate and the Encryption Certificate, if wished.
11. Tap **Save**.

You can import three or less certificates for your virtual smart card. The authentication certificate is required for the virtual smart card to work properly. The encryption certificate and digital signature certificate can be added for use in a VDA session.

Note:

When connecting to an HDX session, the created virtual smart card is redirected into the session.

Known limitations

- Users can only have one active card at a time.
- Once a virtual smart card is created, it cannot be edited. Delete and create card.
- A PIN can be invalid up to 10 times. After the tenth try, the virtual smart card gets deleted.
- When you select derived credentials, the virtual smart card overrides a physical smart card.

nFactor authentication

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide many proofs of identify to gain access. Multifactor authentication makes authentication steps and the associated credential collection forms configurable by the administrator.

Native Citrix Workspace app can support this protocol by building on the Forms logon support already implemented for StoreFront. The web logon page for Citrix Gateway and Traffic Manager virtual servers also consumes this protocol.

For more information, see [SAML authentication](#), and [Multi-Factor \(nFactor\) authentication](#).

Limitations:

- With nFactor support enabled, you can't use biometric authentication such as Touch ID and Face ID.
- Certificate-based authentication isn't supported.

nFactor Advanced authentication policy support

We now support certificate-based authentication on Citrix Workspace app when configured through nFactor Advanced authentication policies on Citrix Gateway. nFactor authentication helps configure flexible and agile multi-factor schemas.

User-agent string:

By default, the user-agent string used during the nFactor authentication now includes the Citrix Workspace app identifier.

Current user-agent string, for example, `Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0`

is replaced with

New user-agent string, for example, `Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0/CitrixReceiver/22.1.0 iOS/15.2 CitrixReceiver-iPhone X1Class CWACapable 302RedirectionCapable CFNetwork Darwin`

This change is applicable for on-premises deployments only.

Note:

The version or device model information might vary based on the environment.

Secure

January 11, 2023

To secure the communication between your server farm and Citrix Workspace app, integrate your connections to the server farm with a range of security technologies, including Citrix Gateway.

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 app and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.

- Secure Web Gateway.

You can use Secure Web Gateway with Web Interface to provide single, secure, and encrypted point of access through the Internet to servers on internal corporate networks.

You can use Secure Web Gateway with Web Interface to provide single, secure, and encrypted data. The servers on internal corporate networks, can access the secured data through the Internet.

- 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 are using Citrix Workspace app through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

Citrix Gateway

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

If you deploy Citrix Endpoint Management 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.

Secure Web Gateway

This topic applies only to deployments using the Web Interface.

You can use the Secure Web Gateway in either Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app and the server. If you are using the Secure Web Gateway in **Normal** mode, Citrix Workspace app doesn't require any configuration. Verify that end users are connecting through the Web Interface.

Citrix Workspace app uses settings that are configured remotely on the Web Interface server to connect to servers running the Secure Web Gateway.

If the Secure Web Gateway Proxy is installed on a server in the secure network, you can use the Secure Web Gateway Proxy in Relay mode. If you are using Relay mode, the Secure Web Gateway server functions as a proxy and you must configure Citrix Workspace app to use:

- The fully qualified domain name (FQDN) of the Secure Web Gateway server.
- The port number of the Secure Web Gateway server.

Note:

Secure Web Gateway Version 2.0 doesn't 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.

Proxy server

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

Citrix Workspace app uses proxy server settings to communicate with the Citrix Virtual Apps and Desktops server. The proxy server settings are remotely configured on the Web Interface server.

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

Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, Citrix Workspace app must be able to communicate through the firewall with both the web server and Citrix server. The firewall must permit HTTP traffic for user device to Web server communication. Usually, the HTTP traffic is over the standard HTTP port 80 or 443 if a secure Web server is in use. For Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server isn't configured with an alternate address, you can configure Web Interface to provide an alternate address to Citrix Workspace app for iOS. Citrix Workspace app for iOS then connects to the server using the external address and port number.

TLS

Citrix Workspace app supports TLS 1.0, 1.1 and 1.2 with the following cipher suites for TLS connections to XenApp and XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Note:

Citrix Workspace app running on iOS 9 and later or version 21.2.0 does not support the following TLS cipher suites:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

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 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 uses iOS platform crypto for connections between Citrix Workspace app and StoreFront.

Configure and enable TLS

There're two main steps involved in setting up TLS:

1. Set up SSL Relay on your Citrix Virtual Apps and Desktops server and your Web Interface server and obtain and install the necessary server certificate.
2. Install the equivalent root certificate on the user device.

Install root certificates on user devices

To secure communications between TLS-enabled Citrix Workspace app and Citrix Virtual Apps and Desktops, you need a root certificate on the user device. The certificate can verify the signature of the Certificate Authority on the server certificate.

iOS comes with about 100s of commercial root certificates that are preinstalled. If you want to use a different certificate, you can receive one from the Certificate Authority and install it on each user device.

Depending on your organization's policies and procedures, you can install the root certificate on each user device instead of directing users to install it. The easiest and safest way is to add root certificates to the iOS keychain.

To add a root certificate to the keychain

1. Send yourself an email with the certificate file.
2. Open the certificate file on the device. This action automatically starts the Keychain Access application.
3. Follow the prompts to add the certificate.
4. Starting with iOS 10, verify that the certificate is trusted by going to iOS **Settings > About > Certificate Trust Setting**.

Under Certificate Trust Settings, see the section "ENABLE FULL TRUST FOR ROOT CERTIFICATES." Make sure that your certificate has been selected for full trust.

The root certificate is installed. The TLS-enabled clients and other application can use the root certificate using TLS.

XenApp and XenDesktop Site

To configure the XenApp and XenDesktop Site:

Important:

- Citrix Workspace app uses XenApp and XenDesktop Sites, which supports Citrix Secure Gateway 3.x.
- Citrix Workspace app uses Citrix Virtual Apps websites, which supports Citrix Secure Gateway 3.x.
- XenApp and XenDesktop Sites supports only single-factor authentication.
- Citrix Virtual Apps websites supports both single-factor and dual factor authentication.
- All the built-in browsers support Web Interface 5.4.

Before beginning this configuration, install and configure Citrix Gateway to operate with Web Interface. You can adapt these instructions to fit your specific environment.

If you're using a Citrix Secure Gateway connection, do not configure Citrix Gateway settings on Citrix Workspace app.

Citrix Workspace app uses a XenApp and XenDesktop Site to get information about the applications an end user has rights to. In the process, the information is presented to Citrix Workspace app running on your device. Similarly, you can use the Web Interface for traditional SSL-based Citrix Virtual Apps connections. For the same SSL-based connection, you can configure Citrix Gateway. XenApp and XenDesktop Sites running on the Web Interface 5.x have this configuration ability built in.

Configure the XenApp and XenDesktop Site to support connections from a Citrix Secure Gateway connection:

1. In the XenApp and XenDesktop Site, select **Manage secure client access > Edit secure client access** settings.
2. Change the Access Method to **Gateway Direct**.
3. Enter the FQDN of the Secure Web Gateway.
4. Enter the Secure Ticket Authority (STA) information.

Note:

For the Citrix Secure Gateway, Citrix recommends using the Citrix default path (//XenAppServerName/Citrix/PNAgent). The default path enables the end users to specify the FQDN of the Secure Web Gateway they're connecting to. Don't use the full path to the config.xml file that is on the XenApp and XenDesktop Site. For example, //XenAppServerName/CustomPath/config.xml).

To configure the Citrix Secure Gateway

1. Use the Citrix Secure Gateway configuration wizard to configure the gateway.

The Citrix Secure Gateway supports the server in the secure network that hosts the XenApp Service site.

After selecting the **Indirect** option, enter the FQDN path of your Secure Web Gateway Server and continue the wizard steps.

2. Test a connection from a user device to verify that the Secure Web Gateway is configured correctly for networking and certificate allocation.

To configure the mobile device

1. When adding a Citrix Secure Gateway account, enter the matching FQDN of your Citrix Secure Gateway server in the **Address** field:

- If you created the XenApp and XenDesktop Site using the default path (/Citrix/PNAgent), enter the Secure Web Gateway FQDN: FQDNofSecureGateway.companyName.com
- If you customized the path of the XenApp and XenDesktop Site, enter the full path of the config.xml file, such as: FQDNofSecureGateway.companyName.com/CustomPath/config.xml

2. If you're manually configuring the account, then clear the Citrix Gateway option **New Account** dialog.

Troubleshoot

January 11, 2023

Disconnected sessions

Users can disconnect (but not log off) from a Citrix Workspace app for iOS session in the following ways:

- While viewing a published app or desktop in session:
 - tap the arrow at the top of the screen to view the in-session drop-down menu.
 - tap the **Home** button to return to the launch pad.
 - notice the white shadow under the icon of one of the published apps that are still in an active session; tap the icon.
 - tap disconnect.
- Close Citrix Workspace app for iOS:
 - double-tap the device's **Home** button.

- locate Citrix Workspace app for iOS in the iOS app switcher view.
- tap disconnect in the dialog that appears.
- Pressing the home button on their mobile device.
- Tapping Home or Switch in the app's drop-down menu.

The session stays in a disconnected state. Although the user can reconnect later, you can verify that disconnected sessions are shown inactive after a specific interval.

To display the app in inactive mode, configure a session timeout for the ICA-TCP connection in Remote Desktop Session Host Configuration (formerly known as "Terminal Services Configuration").

For more information about configuring Remote Desktop Services (formerly known as "Terminal Services"), refer to the Microsoft Windows Server product documentation.

Expired passwords

Citrix Workspace app for iOS supports the ability for users to change their expired passwords. Prompts appear for users to enter the required information.

Jailbroken devices

Your users can compromise the security of your deployment by connecting with jailbroken iOS devices. Jailbroken devices are those devices whose owners have modified them, usually with the effect of bypassing certain security protections.

When Citrix Workspace app for iOS detects a jailbroken iOS device, Citrix Workspace app for iOS displays an alert to the user.

To further help to secure your environment, you can configure StoreFront or Web Interface to help to prevent detected jailbroken devices from running apps.

Requirements

- Citrix Receiver for iOS 6.1 or later
- StoreFront 3.0 or Web Interface 5.4 or later
- Access to StoreFront or Web Interface through an administrator account

To help to prevent detected jailbroken devices from running apps

1. Log on to your StoreFront or Web Interface server as a user who has administrator privileges.
2. Find the file default.ica, which is in one of the following locations:
 - C:\inetpub\wwwroot\Citrix\storename\conf (Microsoft Internet Information Services)

- C:\inetpub\wwwroot\Citrix\storename\App_Data (Microsoft Internet Information Services)
 - ./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF (Apache Tomcat)
3. Under the section **[Application]**, add the following: **AllowJailBrokenDevices=OFF**
 4. Save the file and restart your StoreFront or Web Interface server.

After you restart the StoreFront server, users who see the alert about jailbroken devices can't launch apps from your StoreFront or Web Interface server.

To allow detected jailbroken devices to run apps

If you do not set AllowJailBrokenDevices, the default is to display the alert to users of jailbroken devices but still allow them to launch applications.

If you want to specifically allow your users to run applications on jailbroken devices:

1. Log on to your StoreFront or Web Interface server as a user who has administrator privileges.
2. Find the file default.ica, which is in one of the following locations:
 - C:\inetpub\wwwroot\Citrix\storename\conf (Microsoft Internet Information Services)
 - C:\inetpub\wwwroot\Citrix\storename\App_Data (Microsoft Internet Information Services)
 - ./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF (Apache Tomcat)
3. Under the section **[Application]** add the following: **AllowJailBrokenDevices=ON**
4. Save the file and restart your StoreFront or Web Interface server.

When you set AllowJailBrokenDevices to ON, your users see the alert about using a jailbroken device, but they can run applications through StoreFront or Web Interface.

Loss of HDX audio quality

From Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), HDX audio to Citrix Workspace app for iOS might lose quality when using audio and video simultaneously.

The issue occurs when the Citrix Virtual Apps and Desktops and Citrix DaaS HDX policies can't handle the amount of audio data with the video data.

For suggestions about how to create policies to improve audio quality, see Knowledge Center article [CTX123543](#).

Numeric keys and special characters

If numeric keys or Chinese IME characters do not work properly, disable the Unicode Keyboard option. To do so, go to **Settings > Keyboard Options >** and set **Use Unicode Keyboard** to Off.

Slow connections

Follow the workaround if you experience any of the following issues:

- slow connections to the XenApp and XenDesktop Site
- missing application icons
- recurring **Protocol Driver Error** messages

Workaround:

Disable **Citrix PV Ethernet Adapter** properties for the network interface on the:

- Citrix Virtual Apps server
- Citrix Secure Web Gateway
- Web Interface server

The **Citrix PV Ethernet Adapter** properties include (all enabled by default):

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

No server restart is needed. This workaround applies to the Windows Server 2003 and 2008 32-bit. This issue does not affect the Windows Server 2008 R2.

**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

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).