



Citrix Workspace app for iOS

Contents

Citrix Workspace app for iOS	2
About this release	3
Features in Technical Preview	6
Citrix Workspace app for iOS - Preview	26
System requirements and compatibility	26
Install and upgrade	33
Get started	33
Configure Citrix Workspace app	41
Configure Workspace app using Unified Endpoint Management solutions	53
Peripheral devices	56
User Experience	80
Webview for Web and SaaS apps	93
Password management	95
Authenticate	98
Secure	123
Troubleshoot	129
Citrix Workspace app for iOS	140

Citrix Workspace app for iOS

June 4, 2024

Citrix Workspace app for iOS is client software available for download from the App Store. It enables you to access and run virtual desktops and hosted applications delivered by Citrix Virtual Apps and Desktops.

iOS is the operating system for Apple mobile devices such as iPads and iPhones. Citrix Workspace app for iOS runs on devices using the iOS operating system, such as iPhone X, iPad mini, and iPad Pro.

For detailed information about the features, fixed issues, and known issues, see the [About this Release](#) page.

For information about deprecated items, see the [Deprecation](#) page.

Language support

Citrix Workspace app for iOS is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for iOS, see [Language support](#).

Reference articles

- [Tech Brief: Citrix Workspace](#)
- [Global App Configuration service](#)
- [Workspace user interface \(UI\)](#)
- [Microsoft Teams optimization in Citrix Virtual Apps and Desktops environments](#)
- [Citrix Workspace app release timelines](#)
- [Developer Documentation](#)

What's new in related products

- [Citrix Workspace](#)
- [Citrix DaaS](#)
- [StoreFront](#)
- [Secure Private Access](#)
- [Citrix Workspace app for Mac](#)

Legacy documentation

For product releases that have reached End of Life (EOL), see [Legacy documentation](#).

About this release

June 28, 2024

Learn about new features, enhancements, fixed issues, and known issues.

Note:

Looking for Technical Previews? We have curated a list so that you can find them in one place. Explore our [Features in Technical Preview](#) page and share your feedback using the attached Podio form links.

What's new in 24.6.0

This release addresses areas that improve overall performance and stability.

Fixed issues in 24.6.0

- You might notice that the trackpad on the magic keyboard is not functioning properly in the virtual session on an iPad pro M4 device. For more information, see [Citrix Knowledge Center article - CTX677048](#). [HDX-66083]
- When you capture an image using the device camera from the virtual app session, you might notice that the captured image appears upside down. [CVADHELP-25448]
- When using Skype in a virtual session, you might notice that the screen freezes when you close Citrix Workspace app and reconnect to the session. [CVADHELP-25480]

Earlier releases

This section provides information on new features and fixed issues in the earlier releases that we support. For more information on the lifecycle of these releases, see [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

24.5.0

What's new

Support for authentication using FIDO2 when connecting to a cloud store Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to

enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Touch ID, and Face ID only). This feature is enabled by default. For more information, see [Support for authentication using FIDO2 when connecting to a cloud store](#).

Note:

Fido2 authentication is supported with the Chrome custom tabs by default. If you are interested in using FIDO2 authentication with WebView, register your interest using this [Podio form](#).

Support for document scanner Starting with the 2405 version, Citrix Workspace app for iOS supports the document scanner feature. With this feature, you can now scan and save multiple documents, all within the desktop session. This feature is enabled by default. For more information, see [Support for document scanner](#).

Technical Preview

- Support for single sign-on for Microsoft Entra ID joined VMs
- Support for enforcing biometric authentication to access Citrix Workspace app

For a complete list of Technical Preview features, see the [Features in Technical Preview](#) page.

Fixed issues

- You might notice that when using the barcode scanner in the virtual session, the text can't be scanned correctly. [HDX-63675]

24.4.0

What's new

This release addresses areas that improve overall performance and stability.

Deprecation announcement of the TLS 1.0 and TLS 1.1 protocols Citrix is planning to deprecate the support for TLS 1.0 and TLS 1.1 protocols in the future releases. The alternative protocol is TLS 1.2 or TLS 1.3. For more information, see [Deprecation](#).

Fixed issues

- When you open the device camera from the virtual app session, the Citrix Workspace app for iOS might close unexpectedly. [CVADHELP-24825]

24.3.5

What's new

Support for the twocanoes smart card utility reader Starting with the 24.3.5 version, Citrix Workspace app for iOS supports the twocanoes smartcard utility readers. For more information about the supported smart card readers and configuration details, see [Smart Cards](#).

Note:

The twocanoes smart card utility USB-C reader is supported for both Citrix Workspace app login and virtual session login. However, the twocanoes smart card utility Bluetooth reader is supported only for Citrix Workspace app login and not for virtual session login.

Support for configuring device name through UEM Starting with the 24.3.5 version, Citrix Workspace app for iOS enables administrators to assign and identify device names based on user groups through Unified Endpoint Management (UEM). For more information, see [Support for configuring device name through UEM](#).

Technical Preview

- Support for configuring Citrix Workspace app settings through UEM

For more information on this Technical Preview, see [Features in Technical Preview](#).

Fixed issues

This version addresses areas that improve overall performance and stability.

Known issues

Known issues in 24.5.0

You might notice that the trackpad on the magic keyboard is not functioning properly in the virtual session on an iPad pro M4 device. As a workaround, you can use an external mouse (either wired USB type-C connector or Bluetooth) to navigate the screen in the virtual session. [HDX-66083]

Known issues in 24.1.0

After upgrading Citrix Workspace app for iOS to version 24.1.0, the keyboard input using the virtual keyboard in the session might fail for applications based on Oracle Java Web Start software. [CVADHELP-24645]

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 a 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]

Deprecation

For information about deprecated items, see the [Deprecation](#) page.

Features in Technical Preview















June 28, 2024





Features in Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for features in technical preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

List of features in Technical Preview

The following table lists the features in technical preview. These features are request-only preview features. To enable and provide feedback for any of these features, fill out the respective forms.

Citrix Workspace app for iOS

Title	Available from version	Enablement form (Click the icon)	Feedback form (Click the icon)
Support for enforcing biometric authentication to access Citrix Workspace app	2405		
Support for single sign-on for Microsoft Entra ID-joined VMs	2405		
Support for configuring Citrix Workspace app settings through UEM	24.3.5		
Support for adaptive audio	24.3.0		
Support for Accessibility and VoiceOver	24.2.0		
External Webcam support	23.12.0		
Add multiple stores using Unified Endpoint Management (UEM)	23.9.0		
Delete multiple stores using Unified Endpoint Management (UEM)	23.9.0		
Enhanced web store experience	23.8.0		
Rapid Scan	23.3.5		

Title	Available from version	Enablement form (Click the icon)	Feedback form (Click the icon)
Support for Apple's native non-mirror mode	23.3.0		
Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps	23.3.0		

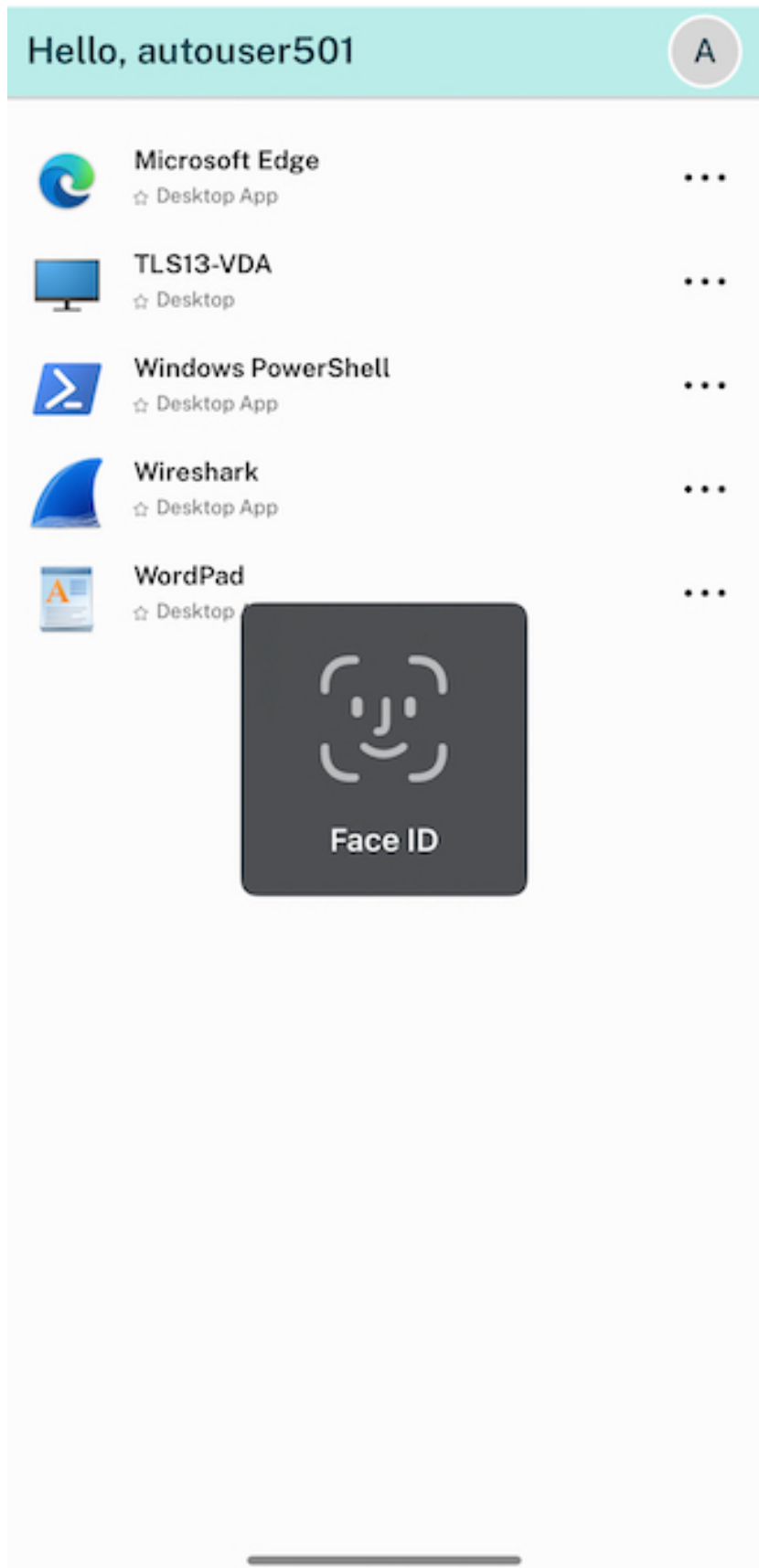
Support for enforcing biometric authentication to access Citrix Workspace app

Technical Preview from 2405
version

[Enablement form](#)

[Feedback form](#)

Starting with the version 24.5.0, administrators can now enforce a device's biometric authentication to access Citrix Workspace app for their users. With this feature, when you open Citrix Workspace app after dismissing it or bring it to the forefront after minimizing it, a prompt for Face ID or Touch ID verification appears to unlock and sign in. If the device does not support biometric authentication, the password or passcode authentication method is used to access the app. If the passcode is not enabled on the device, the account is signed out, requiring the user to sign in again to access the Citrix Workspace application.



Administrators can configure this feature using the unified endpoint management solution with the following key value pairs:

- **key:** `verify_biometric_on_app_foreground_transition`
- **value type:** Boolean
- **value:** true or false
 - If set to **true**, biometric authentication is required for end users to access Citrix Workspace app.
 - If set to **false**, biometric authentication is not enforced to access Citrix Workspace app. Users have the option to disable biometric authentication.

Support for single sign-on for Microsoft Entra ID joined VMs

Technical Preview from 2405
version

[Enablement form](#)

[Feedback form](#)

Starting with the 24.5.0 version, Citrix Workspace app for iOS supports users signing in to Azure AD-joined VM devices using single sign-on authentication. You need to provide Microsoft credentials when signing in to an Azure AD-joined VM device for the first time. For subsequent sign-ins, credentials are not required until the token expires.

Note:

- If the user does not use **WKwebview** for authentication, the credentials must be entered for the first time.
- This feature is applicable only for cloud stores.

Support for configuring Citrix Workspace app settings through UEM

Technical Preview from 24.3.5
version

[Enablement form](#)

[Feedback form](#)

Previously, you could only configure the store URL in the Citrix Workspace app using the Unified Endpoint Management (UEM).

Starting with the 24.3.5 version, you can also configure the Citrix Workspace app settings on the managed devices using any UEM solution that is deployed in your infrastructure.

Note:

As an administrator, if you have an option of configuring the Citrix Workspace app settings using UEM and Global App Configuration service (GACS), UEM always takes a higher preference over GACS.

The following is a sample json file to configure the Citrix Workspace app settings:

```
1  <dict>
2    <key>stores</key>
3    <array>
4      <dict>
5        <key>url</key>
6        <string>https://teststore.cloud.com</string>
7        <key>storeType</key>
8        <integer>1</integer>
9        <key>displayName</key>
10       <string>Cloud Store 1</string>
11       <key>appSettings</key>
12       <array>
13         <dict>
14           <key>category</key>
15           <string>audio</string>
16           <key>userOverride</key>
17           <false/>
18           <key>settings</key>
19           <array>
20             <dict>
21               <key>name</key>
22               <string>settings_audio_stream</string>
23               <key>value</key>
24               <true/>
25             </dict>
26           </array>
27         </dict>
28       <dict>
29         <key>category</key>
30         <string>authentication</string>
31         <key>userOverride</key>
32         <false/>
33         <key>settings</key>
34         <array>
35           <dict>
36             <key>name</key>
37             <string>settings_auth_web_browser</string>
38             <key>value</key>
39             <string>embedded</string>
40           </dict>
41         </array>
42       </dict>
43     </array>
44   </dict>
45 </dict>
```

```
46     <key>url</key>
47     <string>https://teststore.cloud.com</string>
48     <key>storeType</key>
49     <integer>1</integer>
50     <key>displayName</key>
51     <string>StoreFront1</string>
52     <key>appSettings</key>
53     <array>
54         <dict>
55             <key>category</key>
56             <string>audio</string>
57             <key>userOverride</key>
58             <false/>
59             <key>settings</key>
60             <array>
61                 <dict>
62                     <key>name</key>
63                     <string>settings_audio_stream</string>
64                     <key>value</key>
65                     <false/>
66                 </dict>
67             </array>
68         </dict>
69         <dict>
70             <key>category</key>
71             <string>authentication</string>
72             <key>userOverride</key>
73             <false/>
74             <key>settings</key>
75             <array>
76                 <dict>
77                     <key>name</key>
78                     <string>settings_auth_web_browser</string>
79                     <key>value</key>
80                     <string>system</string>
81                 </dict>
82             </array>
83         </dict>
84     </array>
85 </dict>
86 </array>
87 <key>storesToDelete</key>
88 <array>
89     <string>test.cldblr.com</string>
90     <string>test.cloud.com</string>
91 </array>
92 <key>restrict_user_store_modification</key>
93 <false/>
94 </dict>
95 <!--NeedCopy-->
```

Note:

The `userOverride` flag allows the user to modify the Citrix Workspace app settings. If the `userOverride` flag is set to true, the user can change the settings. If the `userOverride` flag is set to false for any settings, then the user can't modify it in the Citrix Workspace app settings.

Key value pair table

The following table provides the key value pair information:

Note:

You must add settings that are specific to a category in one block under that category.

Category	Setting	Description	Key	Value	Value Type	Default value
audio	Audio	Provides access to users to turn the audio on or off from the virtual app or desktop.	settings_audio_use	true/false	Boolean	TRUE
keyboard	Use Unicode Keyboard	Allows users to use a standard Unicode keyboard.	settings_use_unicode_keyboard	true/false	Boolean	TRUE
keyboard	Automatic keyboard	Enables or disables the automatic display of the keyboard in a session.	settings_automatic_keyboard	true/false	Boolean	TRUE

Category	Setting	Description	Key	Value	Value Type	Default value
keyboard	Keyboard Layout Sync	Allows users to switch to a preferred keyboard layout on the device.	settings_keyboard_layout_sync	true/false	Boolean	FALSE
keyboard	Use Custom Keyboards	Allows users to use third-party keyboards that are downloaded in the virtual session.	settings_allow_third_party_keyboards	true/false	Boolean	FALSE
display	Session Resolution	Allows users to select the screen resolution.	settings_resolution	0-9	Integer	5 (iPad) 3 (iPhone)
display	Presentation Mode	Allows you to use your iOS device as a trackpad to control your session while using an external display.	settings_presentation_mode	true/false	Boolean	FALSE
display	External Display	Connects an external display to the device.	settings_external_display	true/false	Boolean	TRUE

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Strict Certificate Validation	Enforces stricter control on server certificate validation.	settings_strictCertificateValidation	true/false	Boolean	FALSE
advanced	TLS Versions	Allows users to change their TLS settings for troubleshooting purposes.	settings_tlsVersion	0-3	Integer	0
advanced	Use Native Combo Box	Enables the use of the iOS native selection feature.	settings_nativeComboBox	true/false	Boolean	TRUE
advanced	Touch Enable (iPAD only)	Enables touch for all apps and desktops, including those that do not have the touch option enabled natively.	settings_multitouch	true/false	Boolean	true (iPad) false (iPhone)
advanced	Fullscreen View	Allows you to view your apps and desktops in full screen.	settings_mobile_fullscreen	true/false	Boolean	true (iPad) false (iPhone)

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Reconnect upon Login	Allows a session to automatically reconnect when a new account is added or during sign in.	settings_reconnect_login	true/false	Boolean	FALSE
advanced	Reconnect upon Refresh	Automatically reconnects to a session launched from another device upon refresh of the apps or desktops on the second device.	settings_reconnect_refresh	true/false	Boolean	FALSE
advanced	Enable HTTP Proxy	Allows you to use the HTTP proxy for a session.	settings_use_local_proxy	true/false	Boolean	TRUE
advanced	Use derived credentials	Allows to use derived credentials.	setting_useDerivedCredentials	true/false	Boolean	FALSE

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Smart Card in session	Allows the use of a smart card device within a session. This setting doesn't allow users to authenticate to the session.	settings_usesSmartCardInSession	true/false	Boolean	FALSE
advanced	Allow EDT	Enables adaptive transport support.	settings_allowEDT	true/false	Boolean	TRUE
advanced	Auto Tablet Mode	Enables to launch the virtual session in tablet mode, when there is no external keyboard or mouse detected.	settings_enableTabletModeSwitch	true/false	Boolean	TRUE
advanced	Keep Display On	Keep the screen on.	settings_stay_away	true/false	Boolean	FALSE
advanced	Use iPad storage	Allows you to access local drives on your device.	settings_clientdrive	true/false	Boolean	false

Citrix Workspace app for iOS

Category	Setting	Description	Key	Value	Value Type	Default value
X1 Mouse	Allow X1 Mouse	Allows you to switch access to your Citrix X1 Mouse.	settings_allow_x1_mouse	true/false	Boolean	FALSE
X1 Mouse	Citrix X1 Mouse speed	Allows users to control the speed of the mouse cursor within the virtual session.	settings_x1_mouse_speed	1-2	Integer	200 (iPadPro) 100 (All other devices)
X1 Mouse	Use remote cursor image for Citrix X1 Mouse	Makes the cursor match the app or desktop within a session. For example, if the cursor is over a text box, it changes to match the text box.	settings_x1_mouse_remote_cursor	true/false	Boolean	TRUE
authentication	Web Browser for Authentication	Allows you to identify usage of SafariView-Controller instead of WKWeb on the device.	settings_auth_system_embedding	system/embedded	String	Embedded

Category	Setting	Description	Key	Value	Value Type	Default value
thirdPartyServices	LaunchDarkly	Enables the Launch-Darkly flag on the Citrix Workspace app features.	enableLaunchDarkly	false	Boolean	true (non-EU regions)

Support for adaptive audio

Technical Preview from 24.3.0 version

[Enablement form](#)

[Feedback form](#)

Starting with the 24.3.0, Citrix Workspace app for iOS supports HDX adaptive audio. This feature improves user experience by providing improved audio quality and low latency.

For more information, see the [Audio policy setting](#) article in the Citrix Virtual Apps and Desktops documentation.

Support for Accessibility and VoiceOver

Technical Preview from 24.2.0 version

[Enablement form](#)

[Feedback form](#)

Starting with the 24.2.0 version, Citrix Workspace app for iOS supports the Accessibility and VoiceOver feature. This feature helps end users who have difficulty seeing the screen. The narrator reads the screen elements aloud when using the Citrix Workspace and the virtual sessions UI.

To enable the VoiceOver feature, navigate to iOS **Settings > Accessibility > VoiceOver** and turn it on.

You must use the accessibility standard gestures provided by iOS to interact with the Citrix workspace app. For example, you can swipe left and right on the screen to navigate between the menus as the voiceover for each item plays. For more information, see [Get started with accessibility features on iPhone](#) and [Get started with accessibility features on iPad](#) in the Apple support documentation.

External Webcam support

Technical Preview from 23.12.0
version

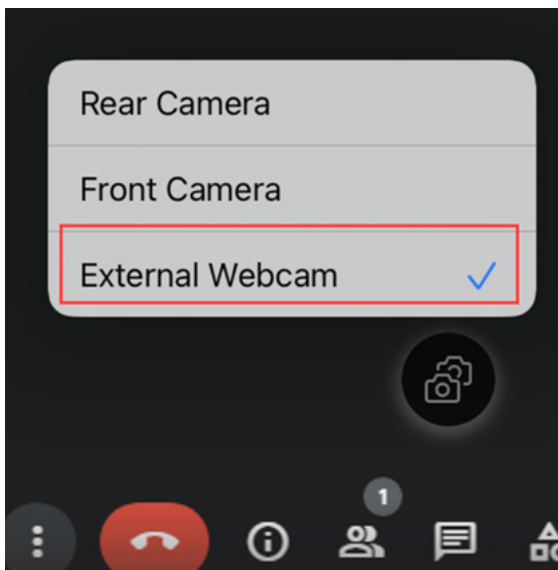
[Enablement form](#)

[Feedback form](#)

Citrix Workspace app for iOS now supports externally connected webcams within your DaaS sessions. Connect a webcam via USB and use it for video conferencing by clicking the Camera icon, then selecting the **External Webcam** option. It enhances the session experience by using the resources available to end users.

Note:

- The External Webcam is only supported on iPads running iOS 17 or later with a USB-C connector.
- The External Webcam option appears only after an external camera is detected.
- The client app settings have no effect on the camera within an HDX session. You must use the camera floating button that is enabled by Citrix to switch the camera position.



The next time you use a video conferencing app, the system remembers your preference and uses the camera preference accordingly. For example, if you concluded the last video call with **External Webcam** preference, next time the External Webcam is selected by default.

You can change your camera preference by tapping the camera icon on your screen. You can also change the camera preference during your calls.

This feature is available for customers on both cloud and on-premises stores.

Add multiple stores using Unified Endpoint Management (UEM)

Technical Preview from 23.12.0 [Enablement form](#)
version

[Feedback form](#)

Admins can use Unified Endpoint Management solutions to configure and add multiple stores for managed iOS devices. The details for each store can be added to an XML file. This XML file can then be uploaded while configuring the app configuration policy.

Note:

The XML file must be in a key-value format.

Configuration key	Value type	Description
url	String	The store URL. For example, example.cloud.com
storeType (optional)	Integer	If set to 1 , users can view the native or the default store loading. If set to 2 , users can view the store inside a web interface.
displayName (optional)	String	The name of the store.
restrict_user_store_modification (optional)	Boolean	If set to true , users can't modify that is, add, delete, or edit the store. If set to false , users can modify that is, add, delete, or edit the store.

Important

- If the **restrict_user_store_modification** flag is set to **true**, all the existing stores are deleted before adding a new UEM configured store.
- If storeType is not provided, the default interface is treated as native.

Sample XML Configuration to add stores

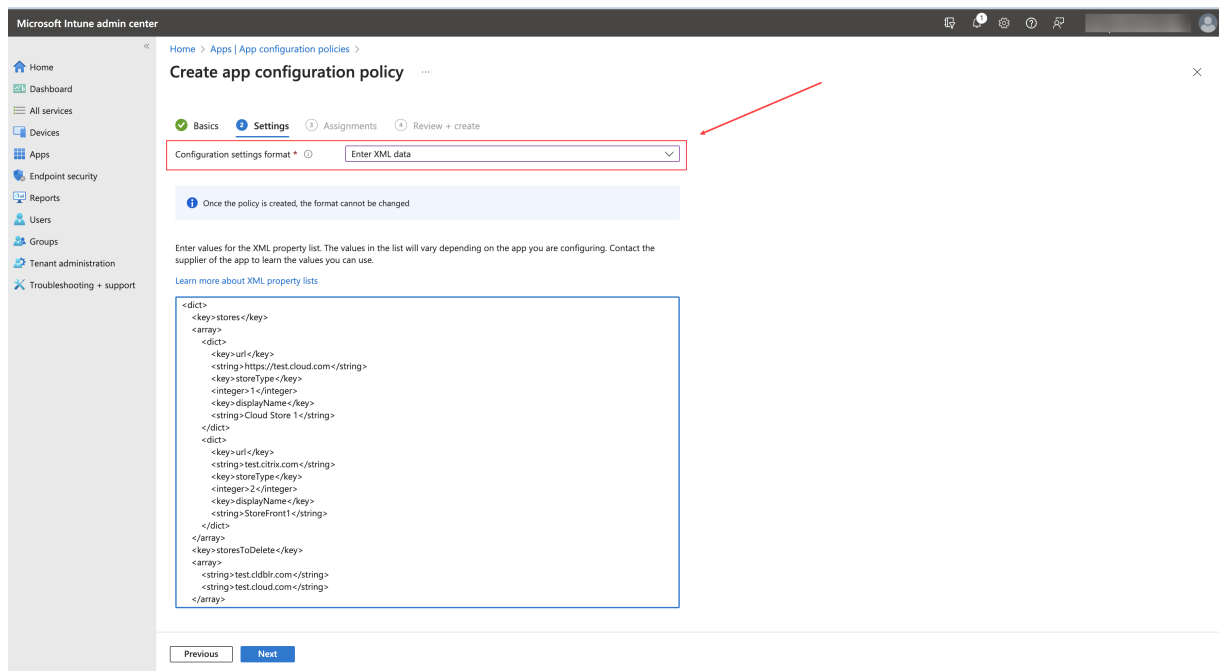
Refer to this sample XML file for more information.

```

1      <dict>
2          <key>stores</key>
3          <array>
4              <dict>
5                  <key>url</key>
6                  <string>test.cloud.com</string>
7                  <key>storeType</key>
8                  <integer>1</integer>
9                  <key>displayName</key>
10                 <string>Cloud Store </string>
11             </dict>
12             <dict>
13                 <key>url</key>
14                 <string>test.citrix.com</string>
15                 <key>storeType</key>
16                 <integer>2</integer>
17                 <key>displayName</key>
18                 <string>StoreFront</string>
19             </dict>
20         </array>
21         <key>restrict_user_store_modification</key>
22         <true/>
23     </dict>
24
25 <!--NeedCopy-->

```

Once the XML file is ready with the store configuration, admins can upload the file to the **Create app configuration policy** page. For example, in Microsoft Intune, admins need to select **Enter xml data** option from the **Configuration settings format** dropdown.



Delete multiple stores using Unified Endpoint Management (UEM)

Technical Preview from 23.12.0 [Enablement form](#)
version

[Feedback form](#)

Admins need to add a list of stores to be deleted to an XML file with the key name **storesToDelete** to delete one or more stores,.

Sample XML configuration to delete stores

Refer to this sample XML file for more information.

```
1     <dict>
2         <key>storesToDelete</key>
3     <array>
4         <string>test.cldblr.com</string>
5         <string>test.onprem.com</string>
6     </array>
7 </dict>
8
9 <!--NeedCopy-->
```

The following is a sample XML configuration file containing configuration for addition and deletion of stores.

```
1     <dict>
2         <key>stores</key>
3         <array>
4             <dict>
5                 <key>url</key>
6                 <string>test.cloud.com</string>
7                 <key>storeType</key>
8                 <integer>1</integer>
9                 <key>displayName</key>
10                <string>Cloud Store </string>
11            </dict>
12            <dict>
13                <key>url</key>
14                <string>test.citrix.com</string>
15                <key>storeType</key>
16                <integer>2</integer>
17                <key>displayName</key>
18                <string>StoreFront</string>
19            </dict>
20        </array>
21        <key>storesToDelete</key>
22        <array>
23            <string>test.cldblr.com</string>
```



```
24         <string>test.onprem.com</string>
25     </array>
26     <key>restrict_user_store_modification</key>
27     <true/>
28 </dict>
29
30 <!--NeedCopy-->
```

Enhanced web store experience

Technical Preview from 23.8.0
version

[Enablement form](#)

[Feedback form](#)

End users can now stay signed-in to a web interface store until they sign out or the session times out. End users can also access the settings option without signing out of the current store. Click the ellipses icon to access the following options:

- **Settings:** Use this option to add and manage your stores.
- **Sign Out:** Use this option to sign out of your current web interface store.

Rapid Scan

Technical Preview from 23.3.5
version

[Enablement form](#)

[Feedback form](#)

If you are signed into Citrix Workspace app on multiple devices, you can use the Rapid Scan feature to scan multiple documents with an iOS device. Then, transfer those scanned documents to a ios device.

For instructions on how to use the Rapid Scan feature to scan documents, follow these steps:

1. On your Mac device, right-click on the Citrix Workspace app icon in your desktop session and click **Rapid Scan**. A QR code is displayed.
2. On your iOS device, click **Settings > Rapid scan**.
3. Scan the QR code displayed on your Mac device to establish the connection between your Mac and iOS devices.
4. Scan any document and send it to your Mac device.
5. In your desktop session on your Mac device, you can locate the documents you scanned in the Finder.

Prerequisites

- Client drive mapping (CDM) must be enabled for the store.
- You must be signed into the same account in the Citrix Workspace app on both your iOS device and Mac device.
- You must be connected to the same Wi-Fi.
- The minimum version required of Citrix Workspace app for Mac is 2304.
- Rapid Scan requires read and write access on your device. To enable access, follow these steps:
 1. From your profile, click **Application Settings > Store Settings**.
 2. Click your current store.
 3. Click **Device Storage** and select **Read and write access**.

Support for Apple's native non-mirror mode

Technical Preview from 22.12.0 [Enablement form](#) [Feedback form](#)
version

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 the [Apple documentation](#).

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

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

Technical Preview from 22.3.5 [Enablement form](#) [Feedback form](#)
version

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.

Technical Preview to General Availability (GA)

Service or feature	General availability version
Support for document scanner	24.5.0
Support for FIDO2-based authentication	23.9.0

Citrix Workspace app for iOS - Preview

June 25, 2024

Citrix Workspace app for iOS 24.7.0 - Preview is coming soon. Look forward to the new features and resolved issues in the upcoming release.

The generally available version of Citrix Workspace app for iOS is 24.6.0. For more information on the current release, see [About this release](#).

System requirements and compatibility

June 26, 2024

Citrix Workspace app for iOS needs to be updated to the latest version that is available in the Apple Store to avail customer support.

Supported operating systems

Citrix Workspace app for Mac supports the following operating systems:

- iOS 17 and iPadOS 17.
- iOS 16 and iPadOS 16.
- iOS 15 and iPadOS 15.

At any point in time, Citrix supports only the latest and the previous two macOS operating systems (N, N-1, and N-2) only.

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:

Citrix Workspace app for iOS

	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.

Note:

The Citrix Gateway End-Point Analysis Plug-in (EPA) is supported on Citrix Workspace. On the native Citrix Workspace app, it's supported only when using nFactor authentication. For more information, see [Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication](#) in the Citrix ADC documentation.

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, an untrusted certificate warning appears. This issue is because the root certificate isn't included in the local key-store. 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 match 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 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** 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 and upgrade

November 7, 2023

You can download or upgrade to the latest version of Citrix Workspace app the Apple Store.

- First-time users can download Citrix Workspace app from the [Apple Store](#) and install it on their device.
- Existing users can upgrade to the latest version of Citrix Workspace app from the [Apple Store](#).

For information on configuring Citrix Workspace app, refer to the [Configure](#) section.

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

Get started

February 28, 2024

Setup

Citrix Workspace app for iOS supports the configuration of Web Interface for your Citrix Virtual Apps deployment. There are 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.
 - The screen-to-fit mode adjusts the application to the screen size of mobile devices. To enable this mode, 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 the Citrix Gateway isn't configured. In the additional options that appear on this screen, provide site logon credentials.
 - <StoreFront FQDN>: If there are 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 do 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 must also 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 do 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 is 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.

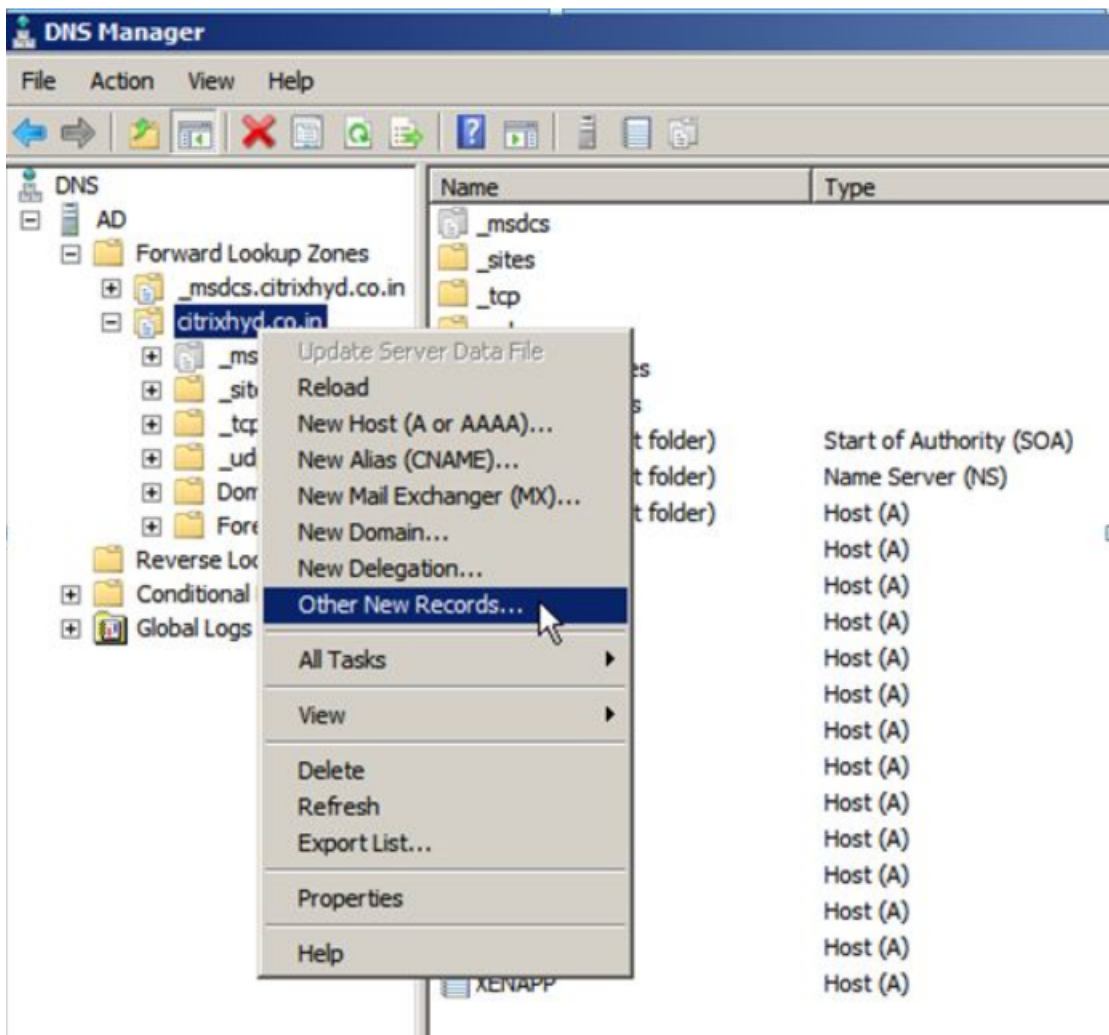
You must install a valid server certificate on the Access Gateway appliance and the StoreFront or AppController server to enable email-based account discovery. The full chain to the root certificate must also be valid. For the best user experience, install either a certificate with:

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

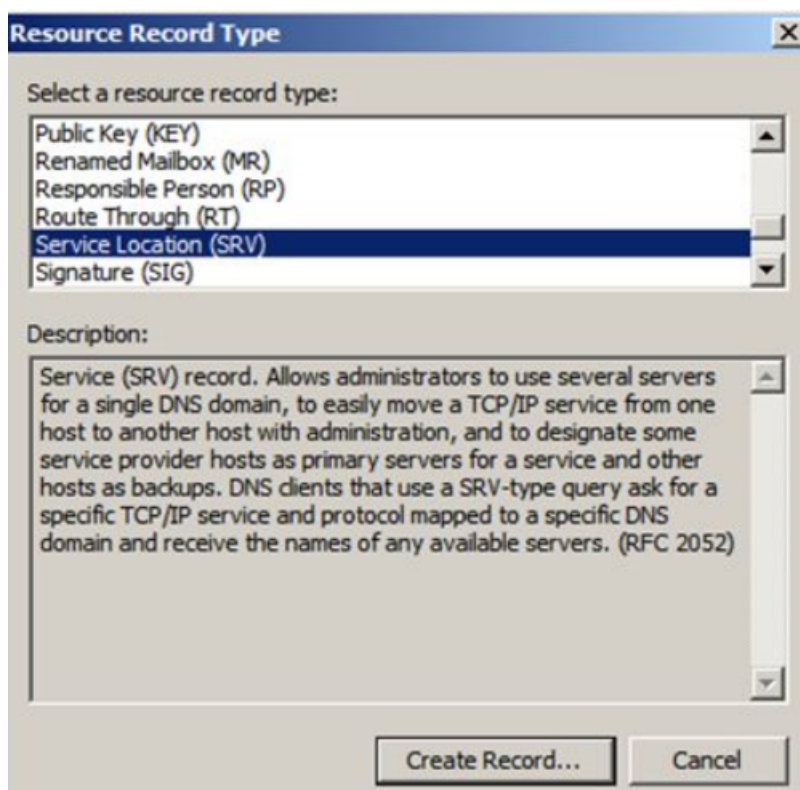
To allow users to configure Citrix Workspace app for iOS by using an email address, add an SRV record to your DNS zone as follows:

1. Log in to 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 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 the 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 Citrix Workspace app

June 28, 2024

This article lists tasks that help you configure Citrix Workspace app for iOS.

Feature flag management

If an issue occurs with Citrix Workspace app in production, the affected feature can be disabled dynamically in Citrix Workspace app. It is possible to do so even after the feature is shipped. 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 [LaunchDarkly Status](#).

LaunchDarkly system requirements

You must verify 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, you can disable the LaunchDarkly service by setting the `enableLaunchDarkly` attribute to `False`. You can achieve this from the Global App Configuration service UI.

```
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 the [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 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.
4. 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.

Inactivity timeout for Citrix Workspace app

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

- After the inactivity timeout, you'll 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.

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. The data is protected as specified in the [Citrix Services Security Exhibit](#). For more information, see 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 the European Union (EU), European Economic Area (EEA), Switzerland, the 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	

Known limitations

- On VDA 7.18 and earlier, casting to a workspace hub requires the desktop or other resource you're using to have the h.264 full-screen policy enabled and the legacy graphics policy to be disabled.

Session sharing

If users log off from a Citrix Workspace app account, they can still disconnect or log off from remote sessions.

- **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 and closes the Windows application. It also logs off from the Citrix Virtual Apps and Desktops, and Citrix DaaS 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.

Cloud stores

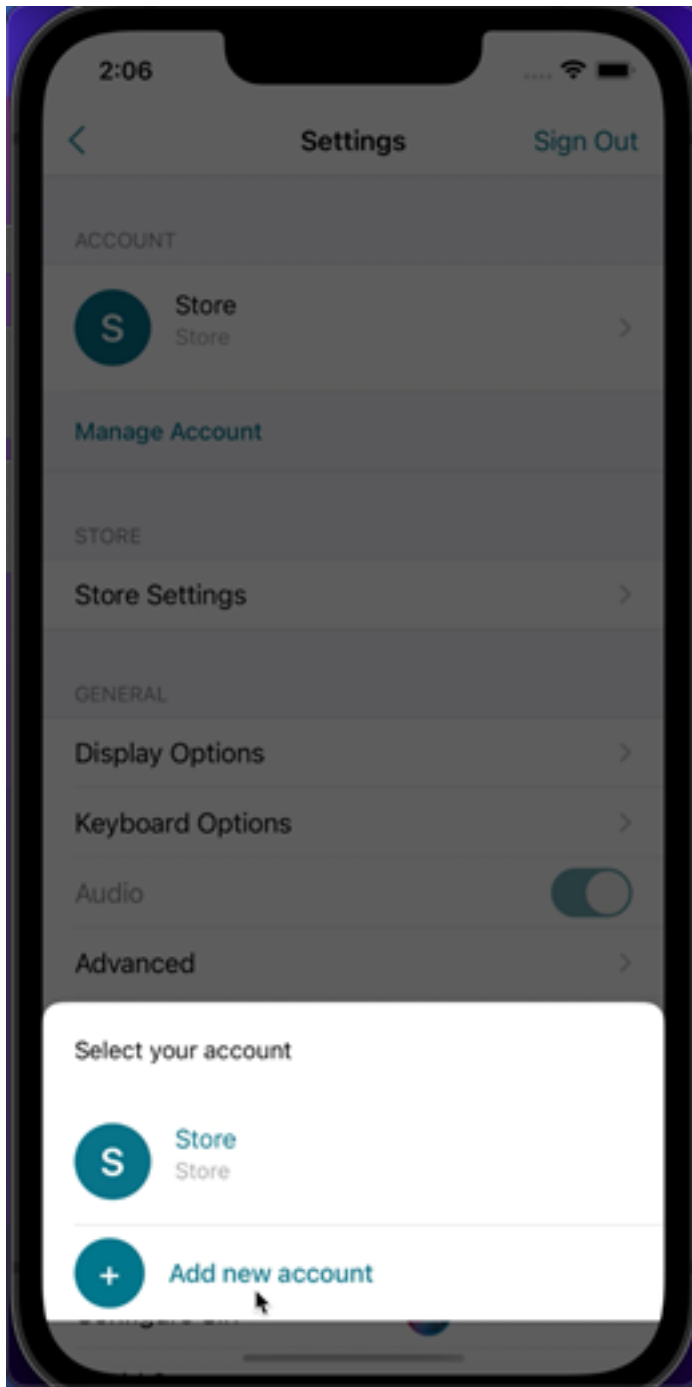
You can access the web, SaaS apps, and websites hosted by your organization regardless of your access location. This feature is available only for customers on cloud stores.

Support for multiple cloud stores

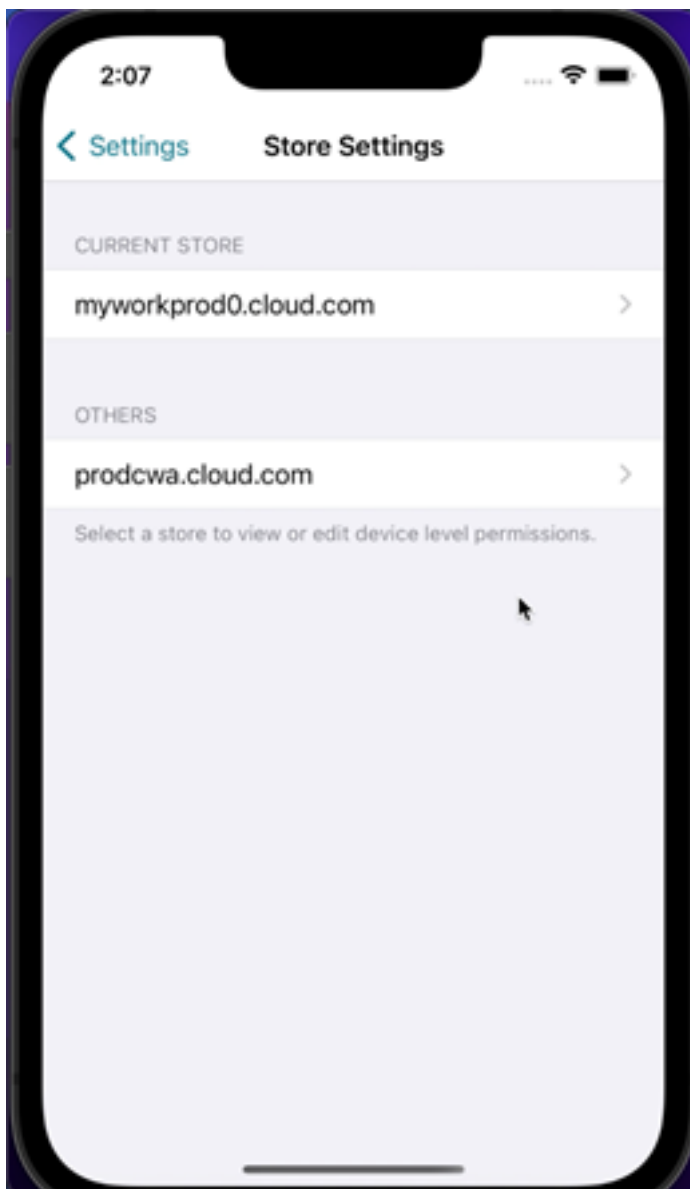
Starting with the 24.1.0 release, you can add multiple cloud store accounts to the Citrix Workspace app for iOS and iPadOS. Now, it's easy for end users to add and switch between multiple stores. This feature improves the user experience when accessing multiple stores.

To add another account, do the following steps:

1. Navigate to **Settings > Manage Account**. A dialog appears at the bottom of the screen with a list of your accounts.
2. Tap **Add new account**.



3. Type the URL or email address provided by your IT administrator. To optionally use a smart card to log on, tap **Use smart card**.
4. Tap **Continue**. The **Sign in** dialog appears with fields for your user name, password, domain, and passcode.
5. Type the information. For more information about the fields, contact your IT administrator.
6. Tap **Sign in**. Your new account is now set up.



Auto-populate store URL

Starting with the 23.2.0 version, when you're accessing the rebranded Citrix Workspace app for iOS, you can choose to auto-populate the store URL. This capability reduces manual intervention and provides quick access to the app. For more information about app personalization, see [App Personalization](#).

Support for deleting multiple stores at once

Starting with the 24.2.0 version, Citrix Workspace app for iOS supports the selection of multiple stores and deleting them. This feature improves the user experience while working with multiple stores. This feature is enabled by default.

To delete multiple stores at once from the **Stores** screen, do the following steps:

1. On the **Stores** screen, tap **Select**.
2. Select stores to delete. To delete all the stores, tap **Select All**.
3. Tap **Delete**.

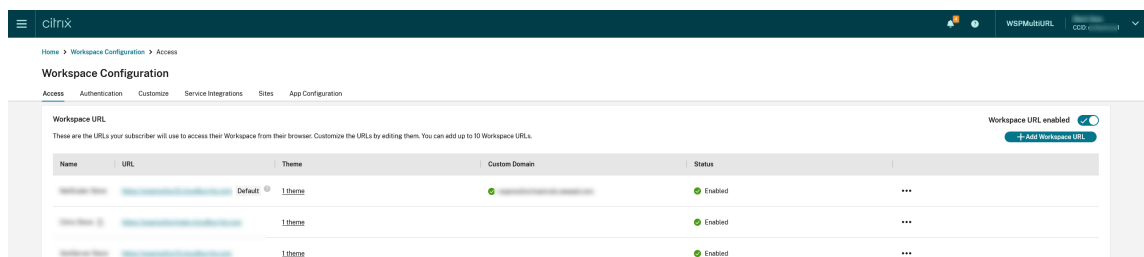
Support for administrator to restrict the user from changing the store name

Previously, users were able to change the store name by using the **Edit Account** option.

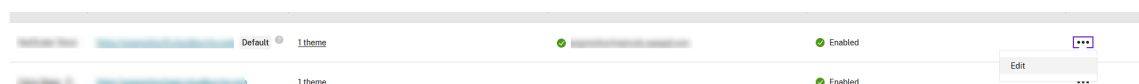
Starting with 24.2.0, Citrix Workspace app for iOS provides administrators an option to disable the user from changing the store name. With this feature, administrators can easily identify and maintain consistency in the store names.

To allow the end-users to change the store name, do the following steps:

1. Sign in to [Citrix Cloud](#) with your credentials.
2. Navigate to **Workspace Configuration > Access**. Under **Workspace URL**, you can find a list of existing store URLs.



3. Click the ellipsis menu for the store that you want to allow end-users to change the store name.
4. Select **Edit**.



5. On the **Edit Workspace URL** dialog box, select **Allow end-users to change this store name in Workspace (not allowed by default)**.

Store name

Allow end-users to change this store name in Workspace (not allowed by default).

6. Click **Save**.

Auto-populate store name

Starting with the 24.2.0 version, Citrix Workspace app for iOS supports store name updates by the administrator and automatically pushes the updated store names to the user. This feature improves the user experience by eliminating the need for manual intervention when updating the store name.

Note:

This feature can take effect only if the administrator has disabled the user from changing the store name.

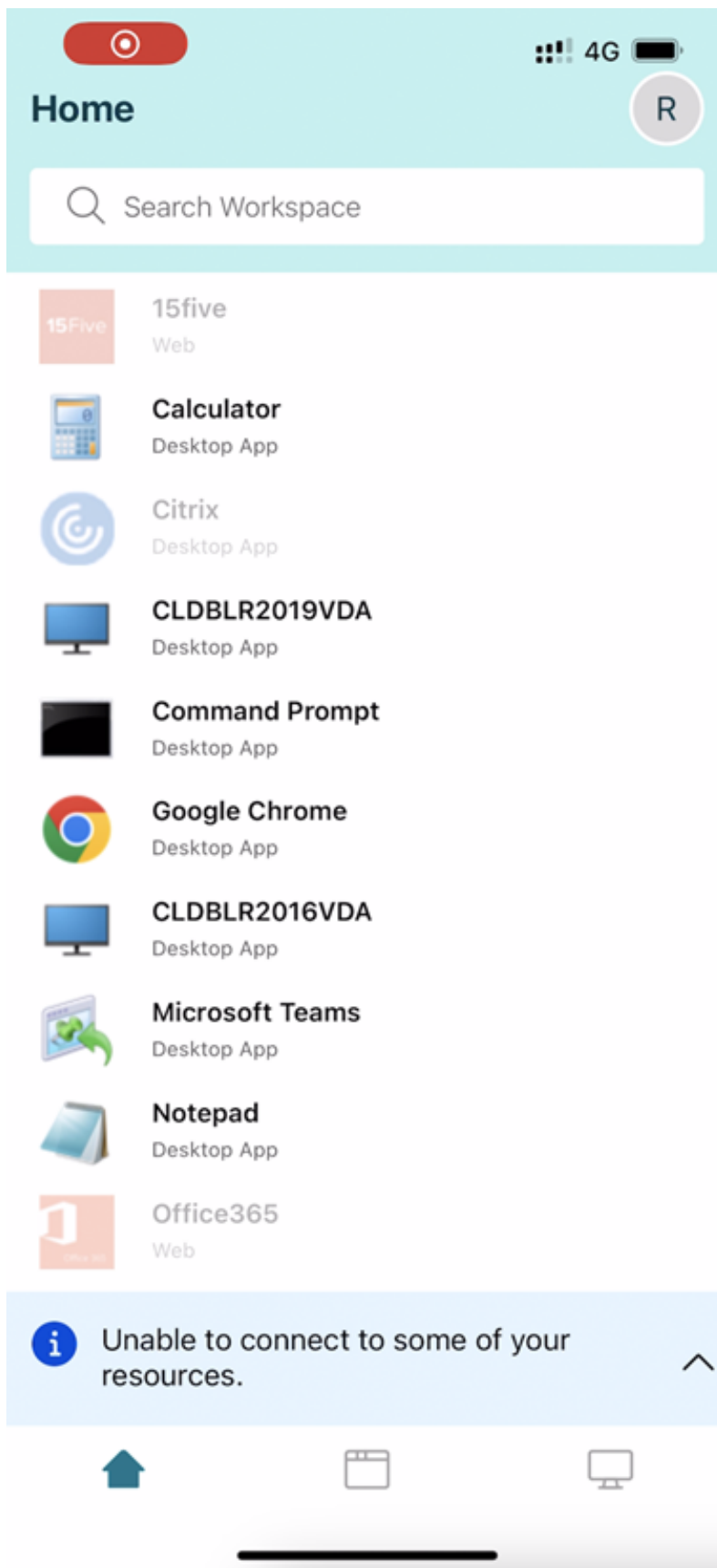
End user experience monitoring enhancement

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. It is calculated from the moment that an ICA file is launched till 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.

Enhanced the user interface for Service continuity offline mode

Starting with the 24.1.0 release, the Citrix Workspace app for iOS's user interface has been improved to be more informative, modern, and provide a user-friendly experience during Citrix Workspace outages. The fuzzy search feature is also included for offline mode. With this feature, you can find the results for apps or desktops with closely matching text and misspelled search terms. For more information about the Service continuity, see [Service continuity](#).



Global App Configuration service channel support

Starting with the 23.4.5 release, administrators can now use the Global App Configuration service to define settings and test them before rolling out the configuration to all end users. This process ensures that features and functionalities are well-tested before production.

Note:

- Citrix Workspace app for iOS supports the **Default** and **Test channel** configurations. By default, all users are on the **Default** channel.

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

For more information on how to configure, see [Global App Configuration service channel support](#).

Access Global App Configuration service enabled web stores

Starting with the 23.7.5 version, admins can now configure a web store (web interface) for email-based store discovery. Based on the email address entered by the end users while adding a store (on the Welcome screen), the Global App Configuration service helps identify the custom web (web interface) URL defined by the admin. The end user is then directed automatically to the web store configured by the admin. To know more about configuring web store URLs for end-users, see [Allowed custom web portal](#).

Configure Workspace app using Unified Endpoint Management solutions

June 28, 2024

Starting with the 23.3.0 version, Citrix Workspace app for iOS supports admin configuration of the Workspace app using AppConfig-based key-value pairs using Unified Endpoint Management (UEM) solutions.

How to configure

To configure your Workspace Store URL using Unified Endpoint Management solutions, follow these steps:

Note:

For demonstrative purposes, Microsoft Intune is used as the UEM solution in this example. The steps below and UI shown differs depending on your UEM provider.

1. Sign in to your Unified Endpoint Management (UEM) provider.
2. Add the Citrix Workspace app that you want to manage by your UEM provider. You can upload the app by using your UEM provider's portal to enable management by your UEM provider. Alternatively, you can link to the app in the App Store.
3. Create an app configuration policy for your app.
4. Add a key and value pair to the XML property list and fill in the following values:
 - **key:** `url`
 - **value type:** `String`
 - **value:** your store URL (for example, `prodcwa.cloud.com`)

Settings [Edit](#)

Configuration key	Value type	Configuration value
<code>url</code>	<code>String</code>	<code>prodcwa.cloud.com</code>

Limitations

- If a cloud store is already set up, and the administrator configures a new cloud store, your existing cloud store is deleted. It also deletes any associated data or settings of the existing cloud store. You receive a notification in Citrix Workspace. You must then sign in again so that the new cloud store is added to Citrix Workspace.
 - The above statement only applies to existing cloud stores. If an on-prem store is already configured and the admin configures a new cloud or on-prem store, then the new store is added and no deletion occurs.
- To apply new configurations, you must force-quit and restart the Citrix Workspace app.

Enhancements to Unified Endpoint Management solutions

Starting with the 23.4.5 version, Citrix Workspace app for iOS supports a couple more configurations using AppConfig-based key-value pairs to configure the Citrix Workspace app. Previously, administrators could configure Store URLs. Now, administrators can restrict end users to modify Store URLs and control how the app appears.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

The following are the details:

Configuration key	Value type	Configuration value
url	String	The store URL. For example, <code>prodcwa.cloud.com</code>
storeType	Integer	<ul style="list-style-type: none">(default) If set to 1, users can view the native or the default store loading. - If set to 2, users can view the store inside a web interface.
restrict_user_store_modification	Boolean	<ul style="list-style-type: none">If set to true, users can't modify the store (add/delete/edit). - If set to false, users can modify the store. Note: If the flag is set to true, all the existing stores are deleted before adding a UEM -configured store.

Support for configuring device name through UEM

Starting with the 24.3.5 version, Citrix Workspace app for iOS enables administrators to assign and identify device names based on user groups through Unified Endpoint Management (UEM).

To configure the device name using UEM, do the following steps:

Note:

For demonstrative purposes, Microsoft Intune is used as the UEM solution in this example. The steps below and the UI shown differ depending on your UEM provider.

1. Sign in to your UEM provider.
2. Add Citrix Workspace app that you want to manage by your UEM provider. You can upload the app by using your UEM provider's portal to enable management by your UEM provider. Alternatively, you can link to the app in the App Store.

3. Create an app configuration policy for your app.
4. Add a key and value pair to the XML property list and fill in the following values:
 - key: deviceName
 - value type: String
 - value: Name of the device (for example, MY_IPHONE_Device)

Configuration key	Value type	Configuration value	
url	String	prodcwa.cloud.com	...
deviceName ✓	String ▾	MY_IPHONE_DVICE ✓	...
<input type="text"/>	Select one ▾	<input type="text"/>	

Peripheral devices

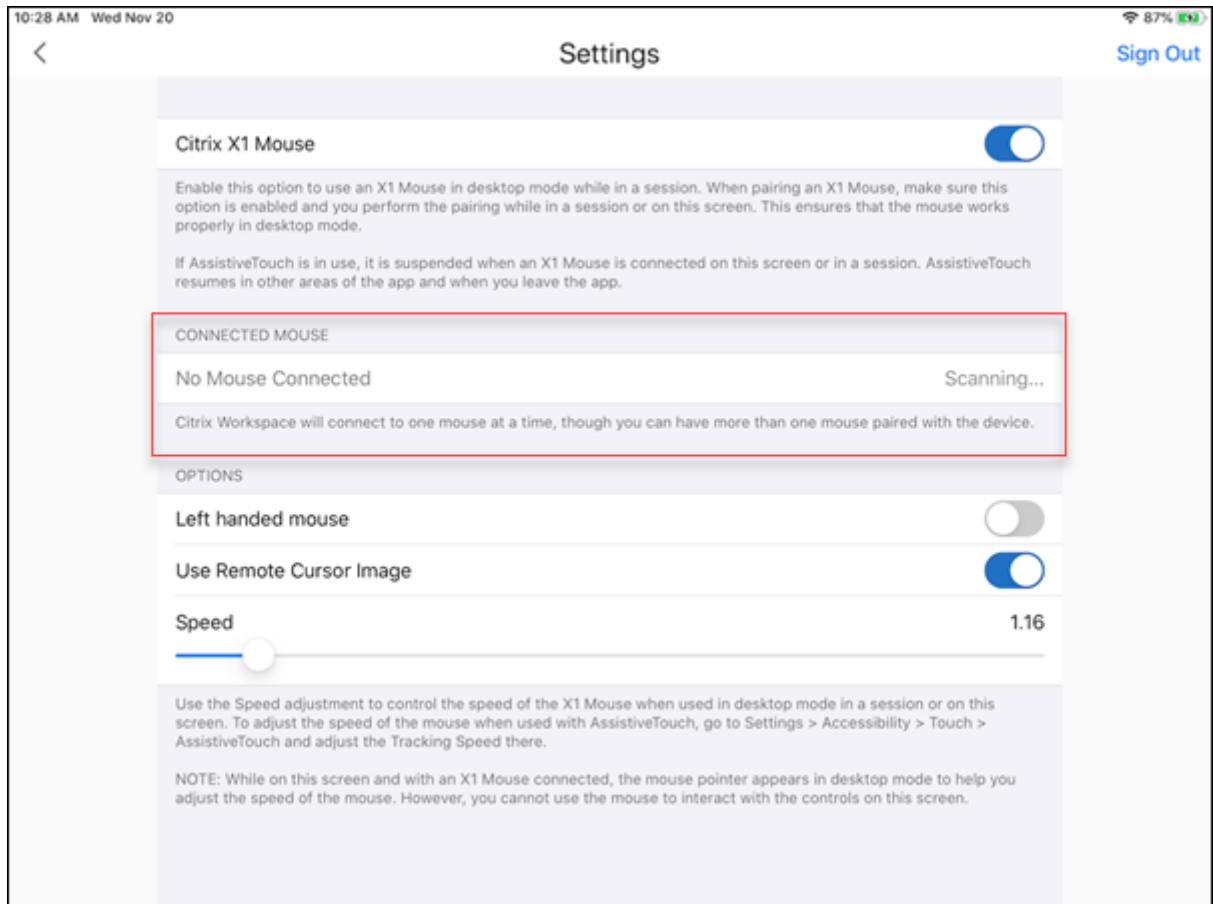
June 28, 2024

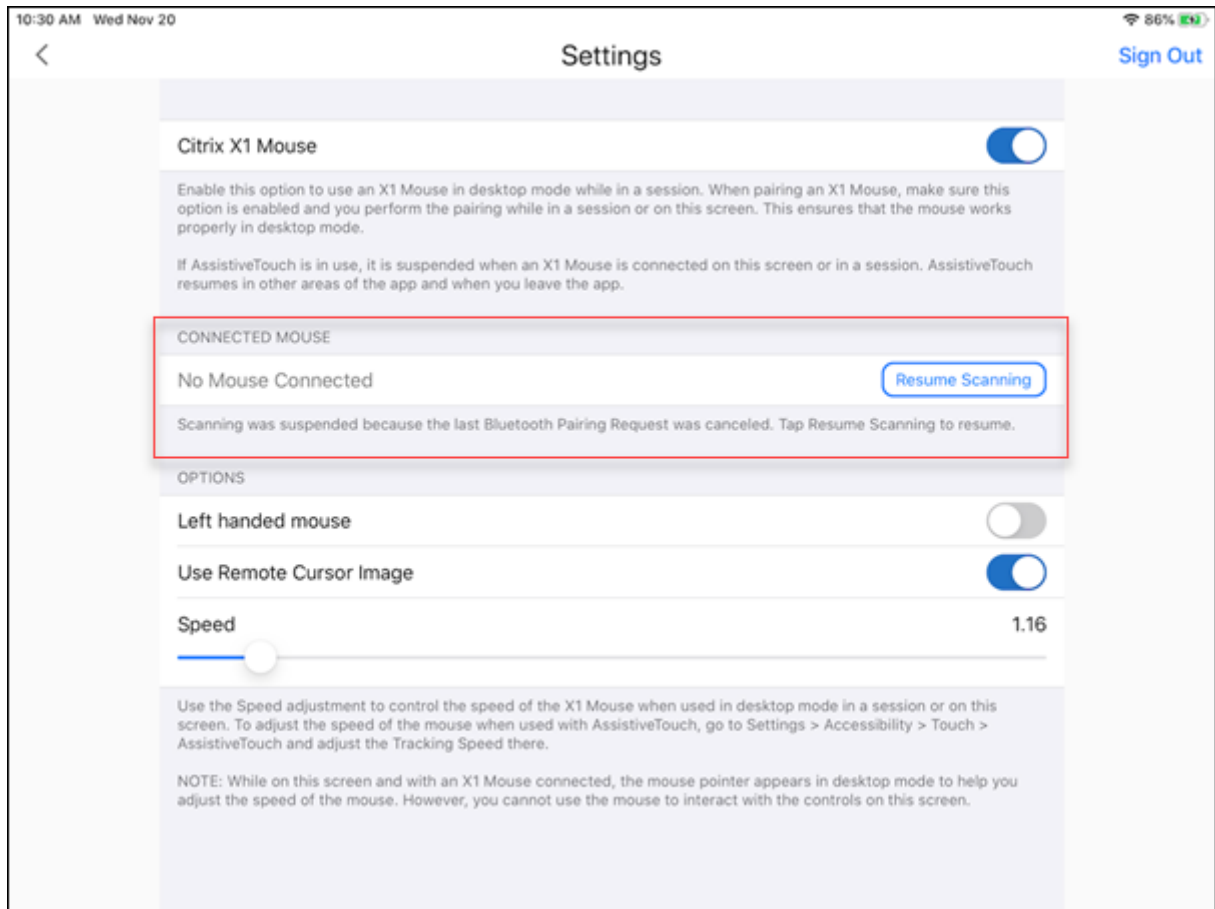
Citrix X1 Mouse

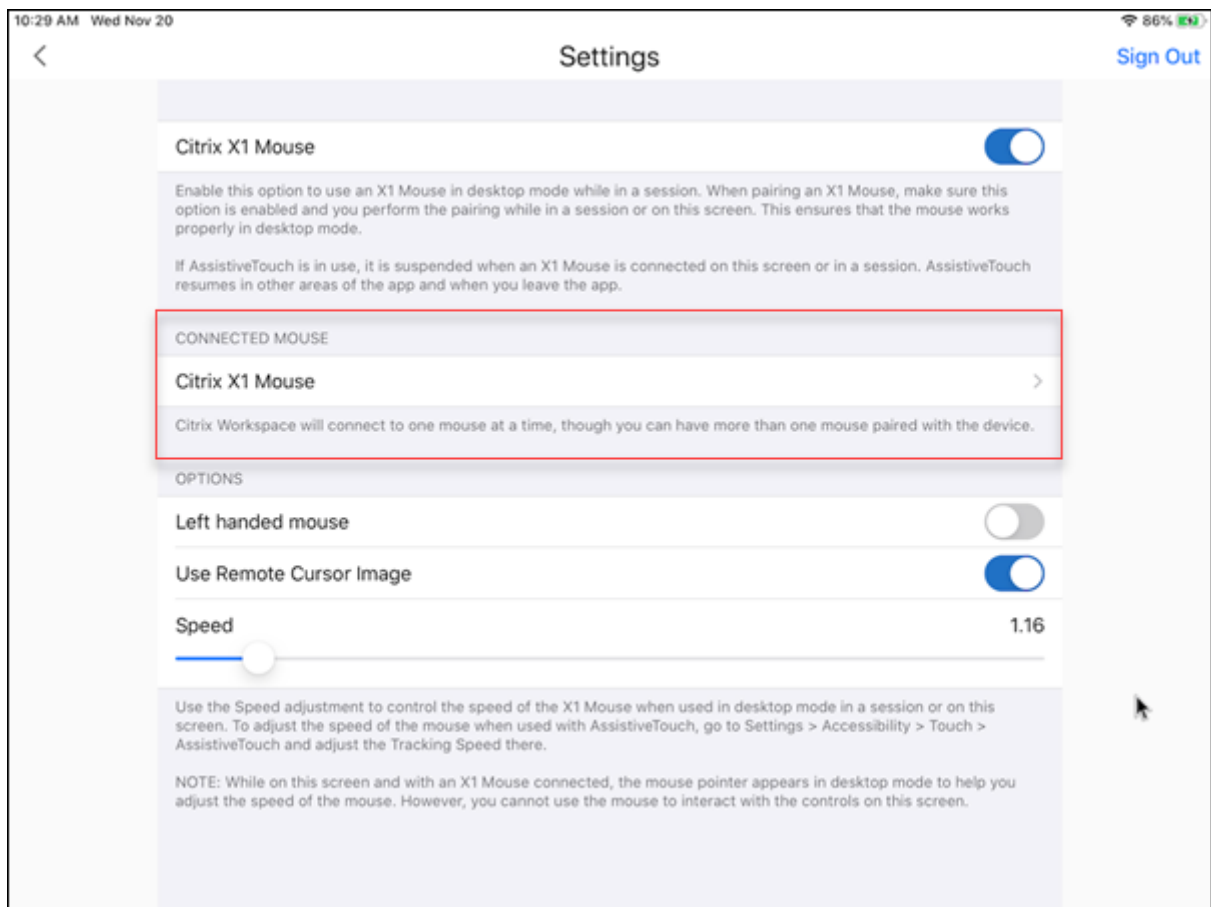
Citrix X1 Mouse pairing and connection status

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

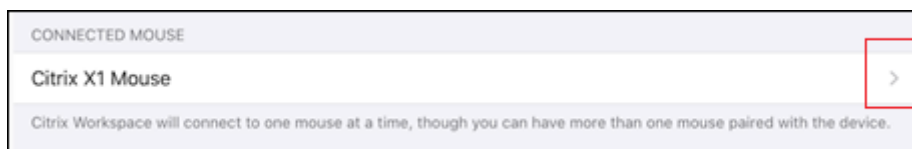
- Pair the Citrix X1 Mouse. You can also pair an X1 Mouse when you are in a session.
- View the connection status.



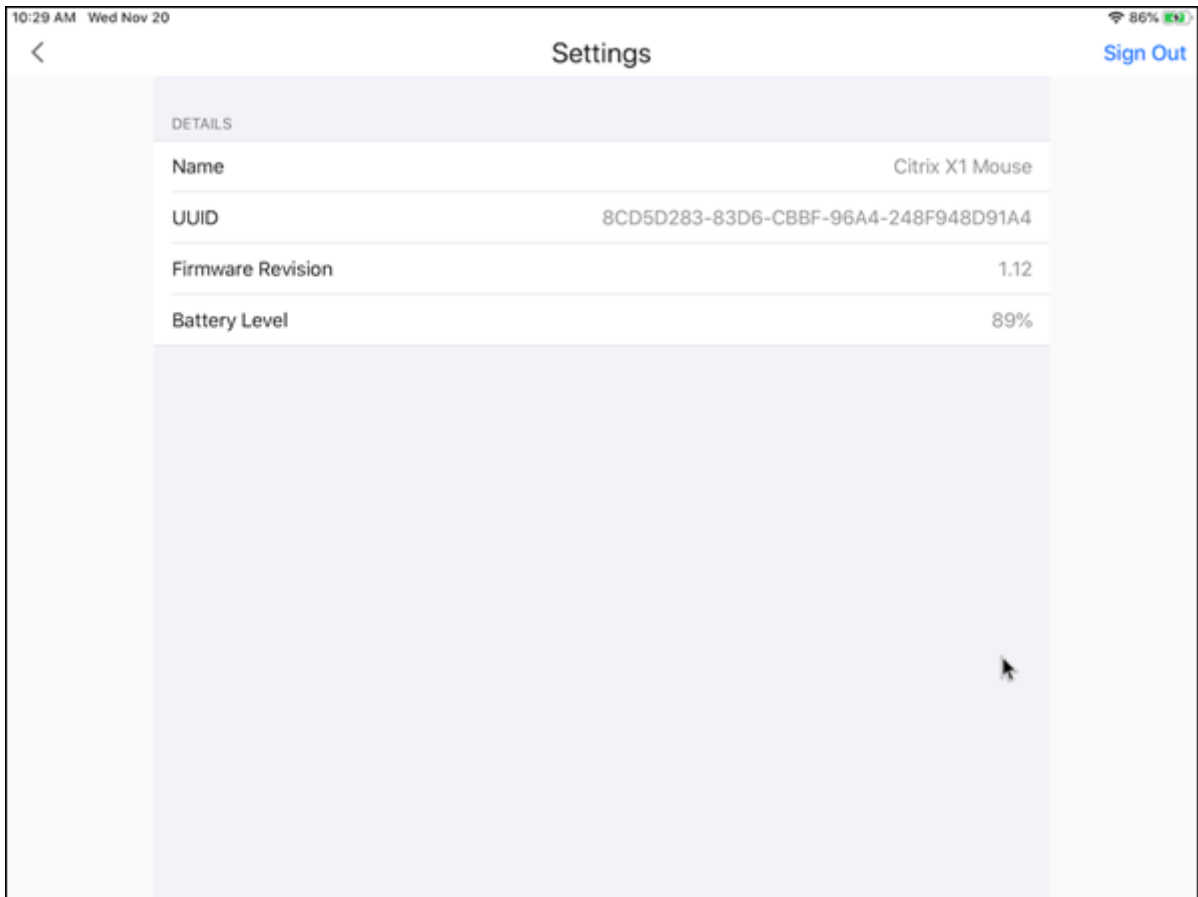




- View the Citrix X1 Mouse properties such as **Name**, **UUID**, **Firmware Revision**, and **Battery Level**. To do so, tap the Citrix X1 Mouse entry under **CONNECTED MOUSE**.



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 in the following cases:

- 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.

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.

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:

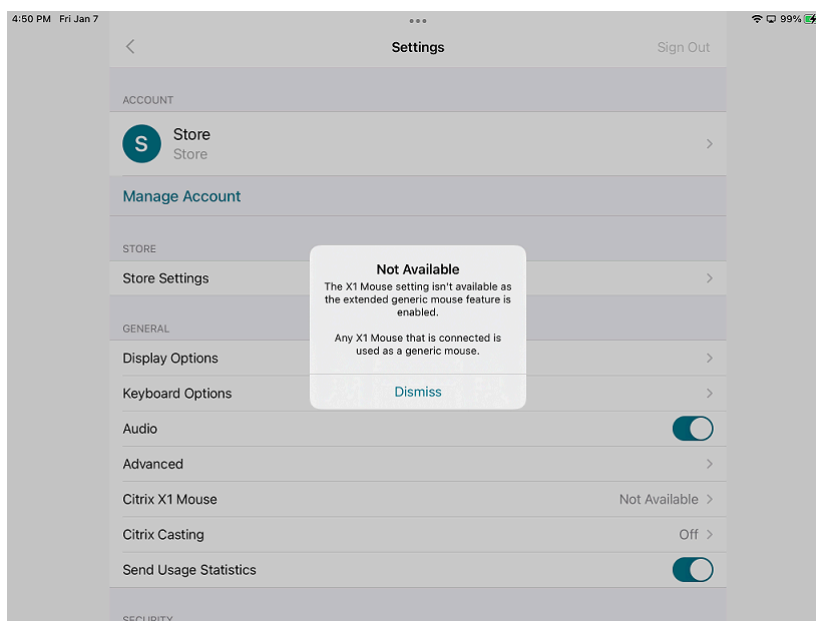
- adapters
- iPad
- other hardware used

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 blue-tooth mouse.

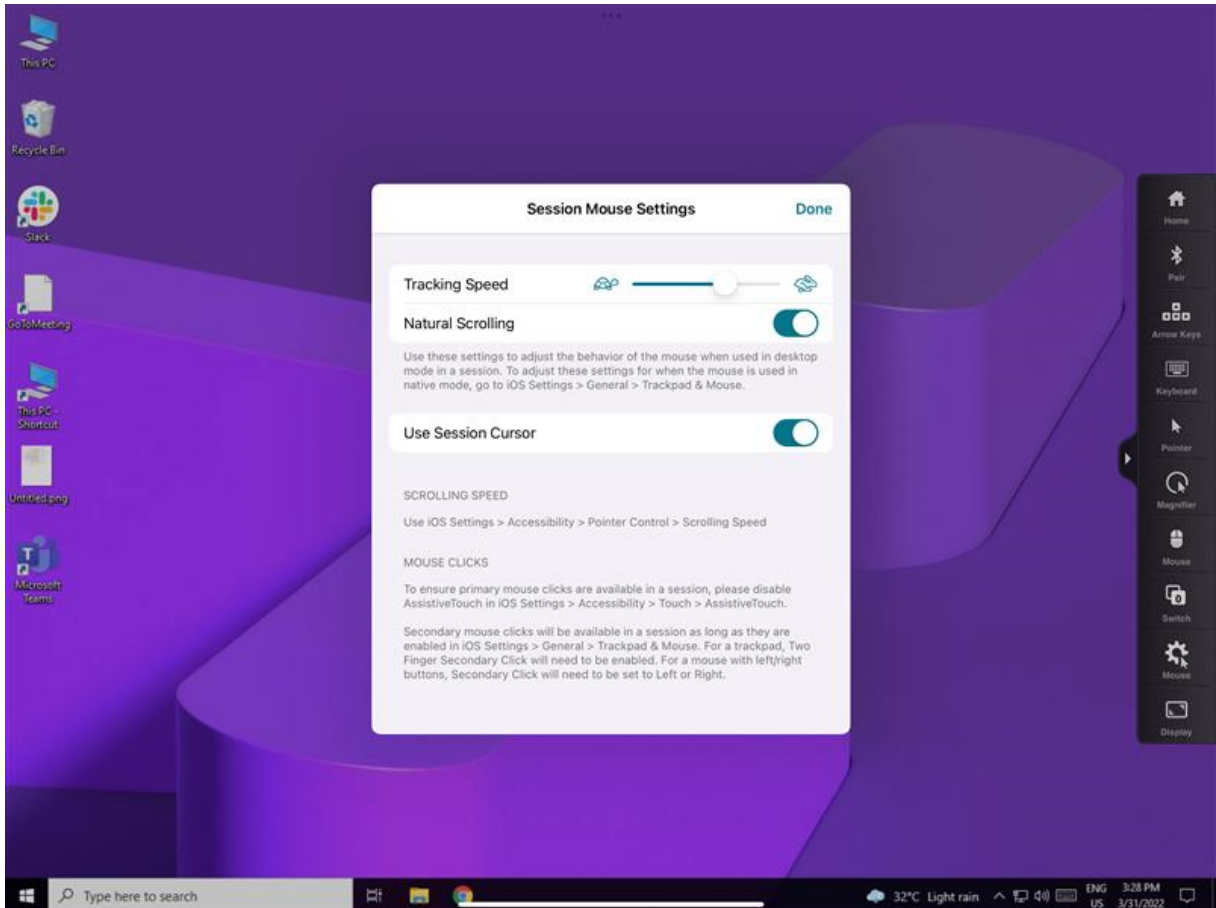


Generic Mouse icon

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]

Keyboard support

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**.

Prerequisites

- For Linux VDA, enable Client keyboard layout sync and IME improvement policy.
- For Windows VDA, enable Unicode Keyboard Layout Mapping, Client Keyboard Layout Sync, and IME Improvement policies.
- The VDA must be version 7.16 or later.

Keyboard layout support for Windows VDA & Linux VDA

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
Belarusian(Belarus)	Belarusian(Belarus)	Belarusian(Belarus) Keyboard	by
Bulgarian	Bulgarian	Bulgarian (Typewriter) keyboard	bg
Chinese (Simplified)	Chinese (Simplified, China)	Citrix IME - Chinese (Simplified, China)	zh
Chinese (Traditional)	Chinese (Traditional, Taiwan)	Citrix IME - Chinese (Traditional, Taiwan)	tw
Croatian	Croatian (Croatia)	Croatian keyboard	hr
Czech	Czech	Czech keyboard	cz
Danish	Danish	Danish keyboard	df
Dutch	Dutch (Netherlands)	United States-International keyboard	us
Dutch(Belgium)	Dutch	Belgian (Period) Keyboard	be
English (Australia)	English (Australia)	US keyboard	us
English (Canada)	English (Canada)	US keyboard	us

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
English (UK)	English (United Kingdom)	United Kingdom keyboard	gb
English(US)	English (United States)	US keyboard	us
Estonian	Estonian	Estonian keyboard	ee
Finnish	Finnish	Finnish keyboard	fi
French (Canada)	French (Canada)	French Keyboard	fr
French (Switzerland)	French (France)	Swiss French Keyboard	ch
French(French)	French (France)	French Keyboard	fr
German (Austria)	German (Austria)	German keyboard	at
German (Switzerland)	German (Switzerland)	Swiss German keyboard	ch
German(Germany)	German (Germany)	German keyboard	at
Greek	Greek	Greek keyboard	gr
Hungarian	Hungarian	Hungarian keyboard	hu
Icelandic	Icelandic	Icelandic keyboard	is
Irish	Irish		ie
Italian	Italian (Italy)	Italian keyboard	it
Japanese	Japanese	Citrix IME - Japanese	jp
Korean	Korean	Citrix IME - Korean	kr
Latvian	Latvian	Latvian keyboard	lv
Norwegian	Norwegian (Bokmål)	Norwegian keyboard	no
Polish	Polish	Polish (Programmers) keyboard	pl
Portuguese (Brazil)	Portuguese (Brazil)	Portuguese (Brazil ABNT) keyboard	br
Portuguese (Portugal)	Portuguese (Portugal)	Portuguese keyboard	pt
Romanian	Romanian (Romania)	Romanian (legacy) keyboard	ro
Russian(Russia)	Russian	Russian keyboard	ru
Slovak	Slovak	Slovak keyboard	sk

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
Slovenian	Slovenian	Slovenian keyboard	si
Spanish (Mexico)	Spanish (Mexico)	Latin American keyboard	latam
Spanish (Spain)	Spanish (Spain)	Spanish keyboard	es
Swedish(Sweden)	Swedish (Sweden)	Swedish keyboard	se
Turkish	Turkish	Turkish F keyboard	tr
Ukrainian	Ukrainian	Ukrainian keyboard	ua

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

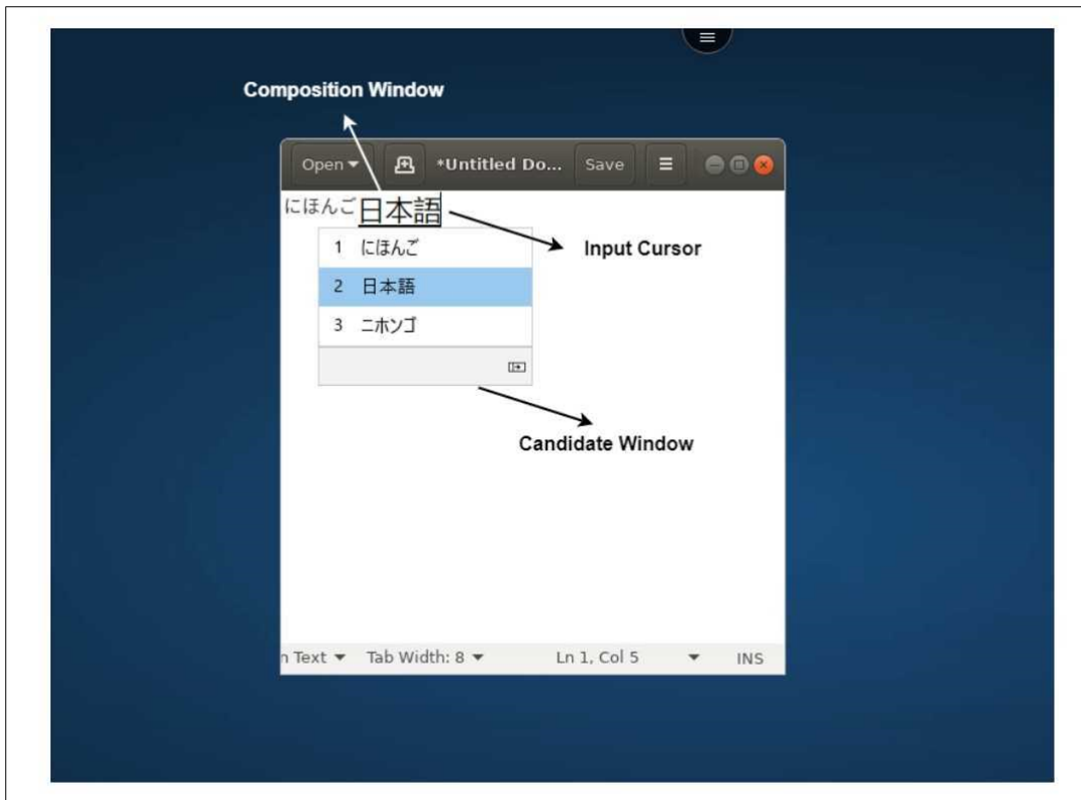
Extended keyboard enhancements

Starting with the 23.5.0 version, extended keyboard functionality is enhanced to provide a better user experience. The following are the enhancements:

- Pin or unpin the extended toolbar UI.
- Rotate the extended toolbar in sync with screen rotation.
- Support Windows icon key and 3-key combination shortcuts.
- Improve experience in multiple monitor use case scenarios.
- Auto open or collapse the extended toolbar UI.
- Improve the experience for Stage Manager mode (on iPad with M1 chip).

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.

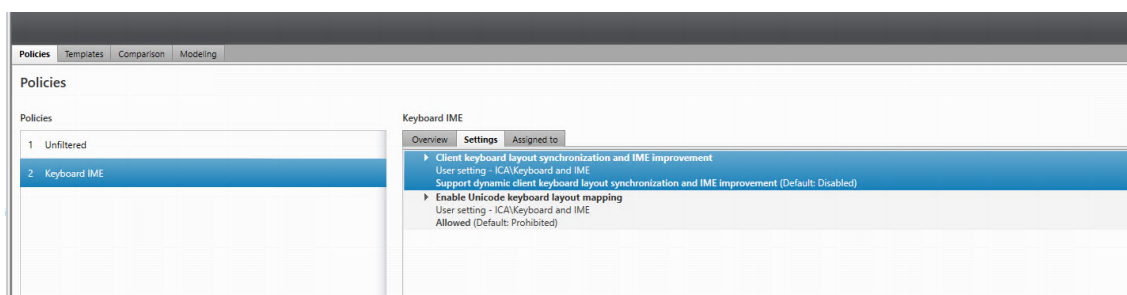
Currently, you can use this feature on the sessions hosted on Windows VDAs and supports both soft keyboards and external physical keyboards.

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. This feature allows you to compose CJK characters at the cursor position when you are in a session with your client IMEs. The feature is available for the Windows VDA environments. 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 the **Settings > Keyboard Options > Keyboard Layout Sync** option from Citrix Workspace app.

Support for scancode input mode

Starting with the 24.1.0 release, you can select **Scancode** as the keyboard input mode while using an external physical keyboard. This feature is helpful when you use iOS devices with an external Windows PC's standard keyboard. With **Scancode**, you can use the keyboard layout of the VDA instead of the iOS's keyboard. In this way, you can completely follow the input style of the external Windows keyboard instead of iOS. It is beneficial when typing in East-Asian languages, as it significantly improves the overall user experience. The end user might find themselves using the keyboard layout of the server instead of the client. For more understanding, see the [Use Case](#) section in this article.

To use the **Scancode** feature, do the following steps:

1. Open Citrix Workspace app for iOS and navigate to **Settings > Keyboard Options**.
2. Tap **Input mode for external keyboards**.
3. Select one of the following options:
 - **Scancode**: Sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.

- **Unicode:** Sends the key from the client-side keyboard to VDA and VDA generates the same character in VDA. Applies client-side keyboard layout.

By default, **Unicode** is selected as the input mode for both software or touch keyboard and external keyboard.

4. Tap **Scancode**.

When you are in a session, you can switch the remote, server, or VDA keyboard layout and input with the remote, server, or VDA keyboard layout.

Use case For example, consider a scenario where you're using a US international keyboard layout that is connected to your iOS device.

When you choose **Scancode** and type the key next to the CapsLock on your external keyboard, the **scancode 1E** is sent to the VDA. The VDA then uses **1E** to display the character **a**.

If you choose **Unicode** and type the key next to CapsLock on your external keyboard, the character **a** is sent to the VDA. So, even if the VDA uses another keyboard layout that has a different character in the same position, the character **a** appears on the screen.

Note:

Unicode is the preferred mode for typing when you use a touch keyboard on your mobile devices. Because the keys on a touch keyboard generally don't generate a scancode.

Enhancements to external keyboard shortcut support

Starting with the 24.1.0 version, Citrix Workspace app for iOS now enables you to use more shortcuts from external keyboards when in a remote desktop or app session. The following are important improvements made to external keyboard shortcuts:

- Support for Windows keyboard specific keys such as **Insert**, **Delete**, and number pad.
- When you keep a key pressed down and don't release it, the remote desktop/app responds correctly.
- Support shortcuts with more than three keys.

In addition, you can now configure the specific key for **Alt** by using the following options via **Settings > Keyboard Options > Assign Specific Key for Alt:**

- **Option or Alt (left):** Sends **Alt** using **Option (left) or Alt (left)**.
- **Command or Windows (left):** Sends **Alt** using **Command (left) or Windows (left)** keys.
- **Option or Alt (left and right):** Sends **Alt** using the **Option or Alt (left and right)** key.

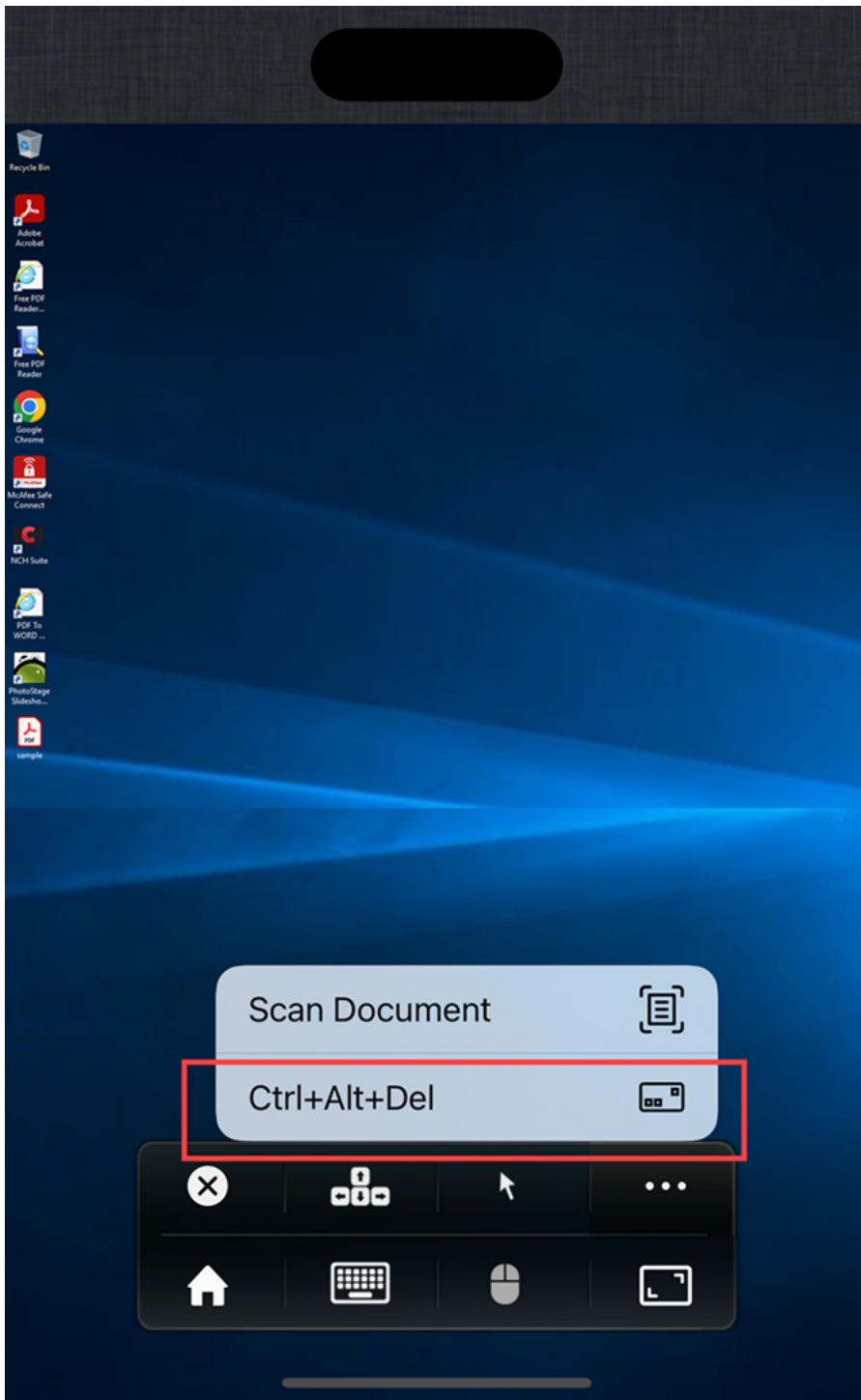
Assigning specific key for Alt option helps to avoid conflict between the macOS **Option** key and the Windows **Alt** key.

Limitations The following iOS system shortcuts are currently not supported:

- **Command (Windows)-H**: Go to the Home screen.
- **Command (Windows)-Space bar**: Show or hide the Search field.
- **Command (Windows)-Tab**: Switch to the next most recently used app among your open apps.
- **Command (Windows)-Shift-3**: Take a screenshot.
- **Command (Windows)-Shift-4**: Take a screenshot and immediately open Markup to view or edit it.
- **Command (Windows)-Option (Alt)-D**: Show or hide the Dock.
- **Command (Windows)-Ctrl-Q**: Lock the device.
- **AltGr** in the Europe keyboard is not supported. If you want to enter special characters with **AltGr**, use the following shortcuts instead:
 - macOS **Option+*** shortcut or
 - Windows OS **Alt + number pad shortcut**.

Addition of Ctrl+Alt+Del shortcut to Session Toolbar

Starting with the version, the session toolbar now has an option to perform the **Ctrl+Alt+Del** function with the tap of a button. This option facilitates users to sign out, switch users, lock the system, or access the Task Manager.



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 the camera or microphone.

Also, microphone and camera access per store 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.

Rear camera support

Starting with the 23.2.0 version, Citrix Workspace app for iOS now supports switching the camera position from front to rear and the other way around within an HDX session.

When you invoke the camera in the virtual session, a camera floating button appears on the screen to allow the switching of the camera position. You can also move the floating button freely around the screen and place it anywhere.

To switch the camera position between the front and rear positions in the virtual sessions, do the following steps:

1. Open a client app that captures video.
2. Start the video recording.
3. Tap the camera floating button that appears on the screen to switch between front and rear camera.

Note:

The client app settings have no effect on the camera within an HDX session. You must use the camera floating button that is enabled by Citrix to switch the camera position.

Known issues:

The floating button is partially or fully obstructed when the Casting feature or the Document Scan feature is enabled.

Graphics and Display

Improved graphics performance

Starting with the 24.1.0 version, Citrix Workspace app for iOS supports hardware accelerated H.264 video encoding or decoding. The multimedia engine of Citrix HDX now uses Apple's Video Toolbox framework for encoding and decoding. This framework compresses and decompresses video faster and in real time. This enhancement reduces the load on the CPU during multimedia usage.

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**.

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 the [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 the [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 Citrix Ready workspace hub

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](#).

Support for document scanner

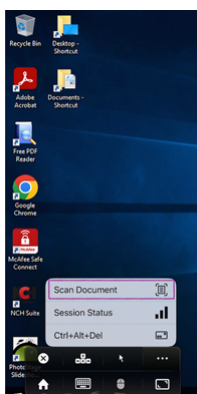
Starting with the 24.5.0 version, Citrix Workspace app for iOS supports the document scanner feature. With this feature, you can now scan and save multiple documents, all within the desktop session. This feature is enabled by default.

Prerequisites

- Client drive mapping (CDM) must be enabled for the store.
- The document scanner feature requires read and write access on your device. To enable access, follow these steps:
 1. From your profile, tap **Application Settings > Store Settings**.
 2. Tap your current store.
 3. Tap **Device Storage** and then select **Full Access**.

To scan documents using the document scanner, do the following steps:

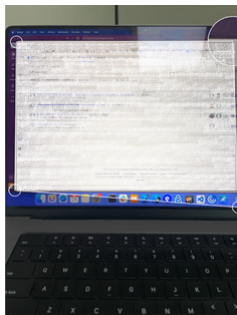
1. From the in-session toolbar, tap the ellipsis menu and select **Scan Document**. The camera app opens.



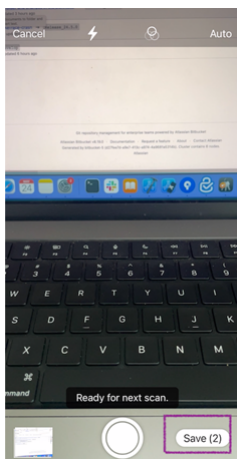
2. Tap the shutter button to capture the photo. If you choose to capture again, tap **Retake**.



- Optional: Crop the scanned document. After cropping to the required size, tap **Keep Scan**. The camera app opens again to allow you to capture more images.



- After capturing the required images, tap **Save**.



- Select the file format option to save the scanned document in the required format.

via cable or network. The AirPrint enabled printers are listed along with the other available printers once users initiate a print command.

To print using an AirPrint enabled printer, users must ensure the following.

- The required printer must be AirPrint compatible and AirPrint enabled.
- The user's device must be connected to the same Wi-Fi network as the AirPrint enabled printer.

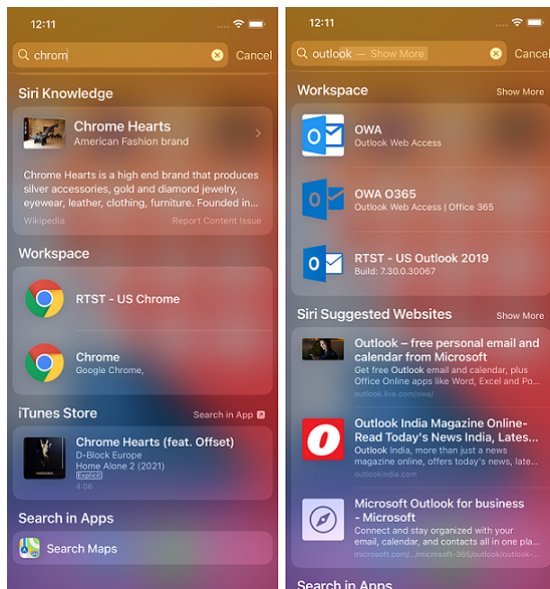
This functionality is available for iOS platforms on both cloud and on-premises environments.

User Experience

June 28, 2024

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.

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.

Long press functionality to access resource

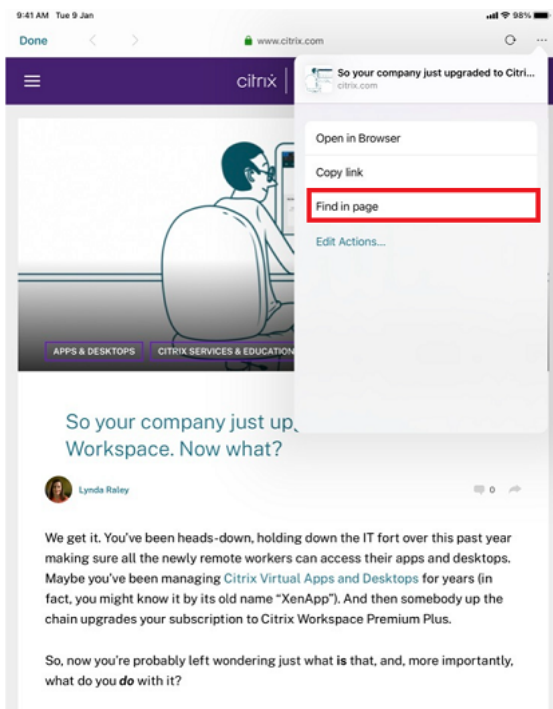
You can now long-press the Citrix Workspace app icon and access your most recently launched resource. You can now quit the Citrix Workspace app and access your most recently launched resource.

Find in page enhancement

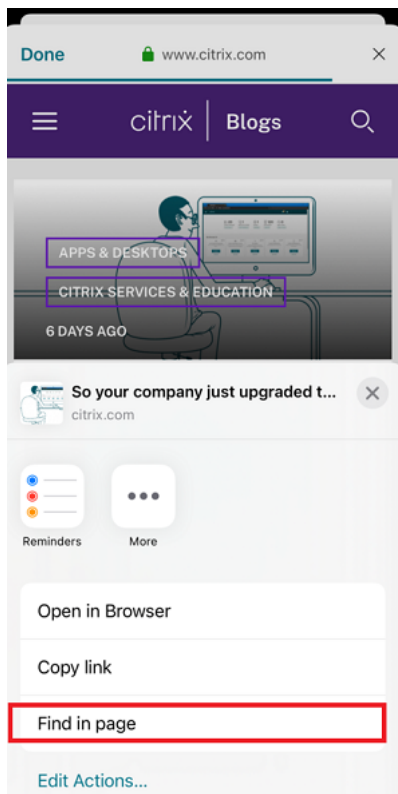
The Find in page enhancement lets you search for words or phrases. This usability enhancement is applicable within your Web and Software-as-a-Service (SaaS) apps.

To search:

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

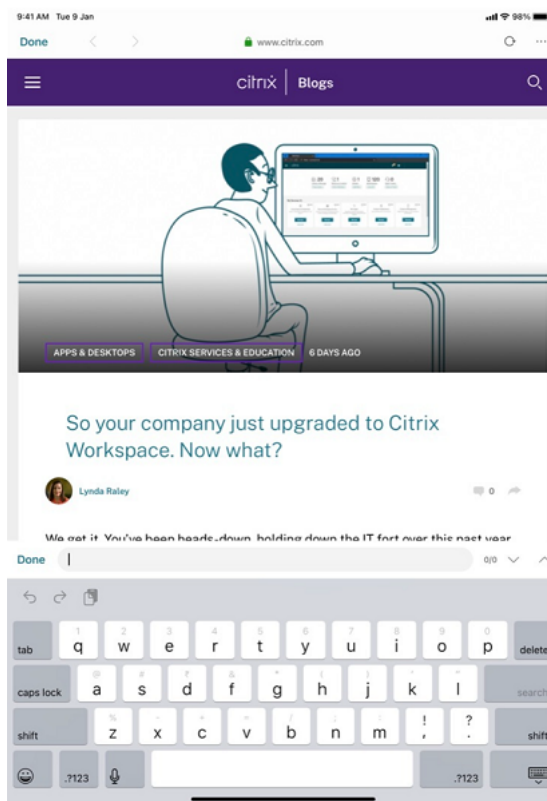


On your iPhone, tap the ellipsis (...) button on the lower-right corner and then select **Find in page**.

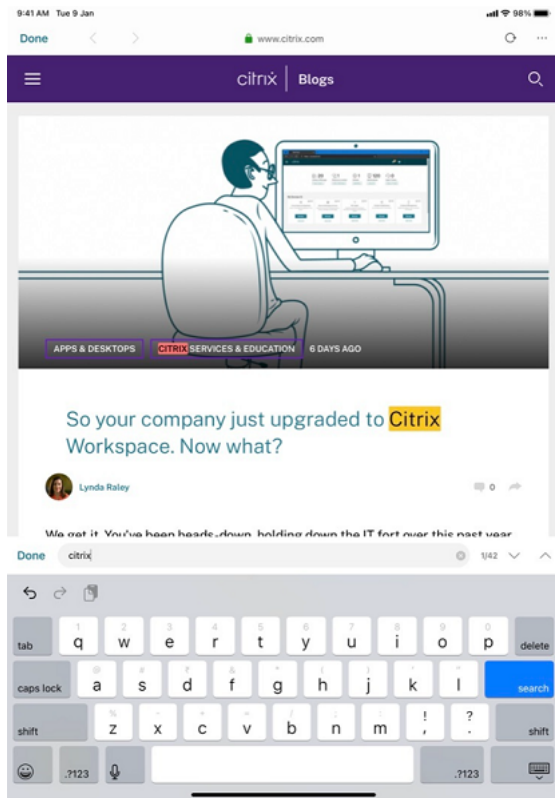


The on-screen keyboard appears.

Citrix Workspace app for iOS



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



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.

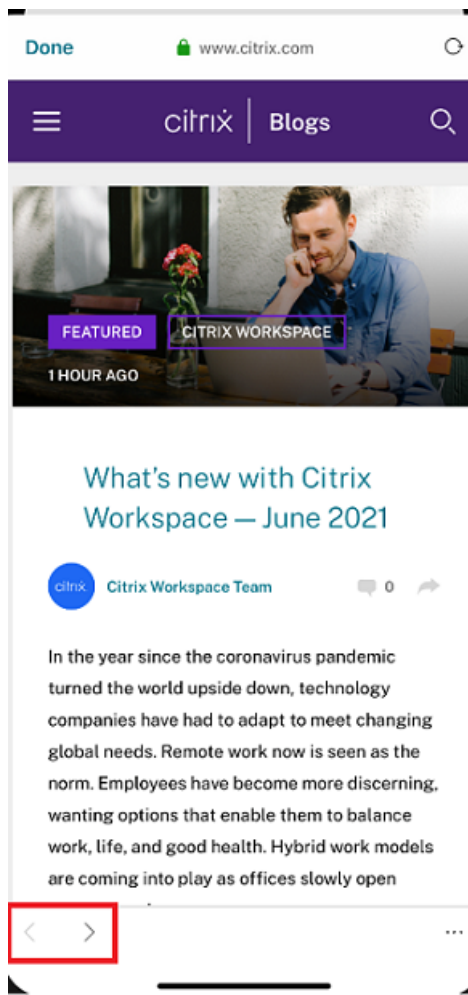
Notes:

- 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.

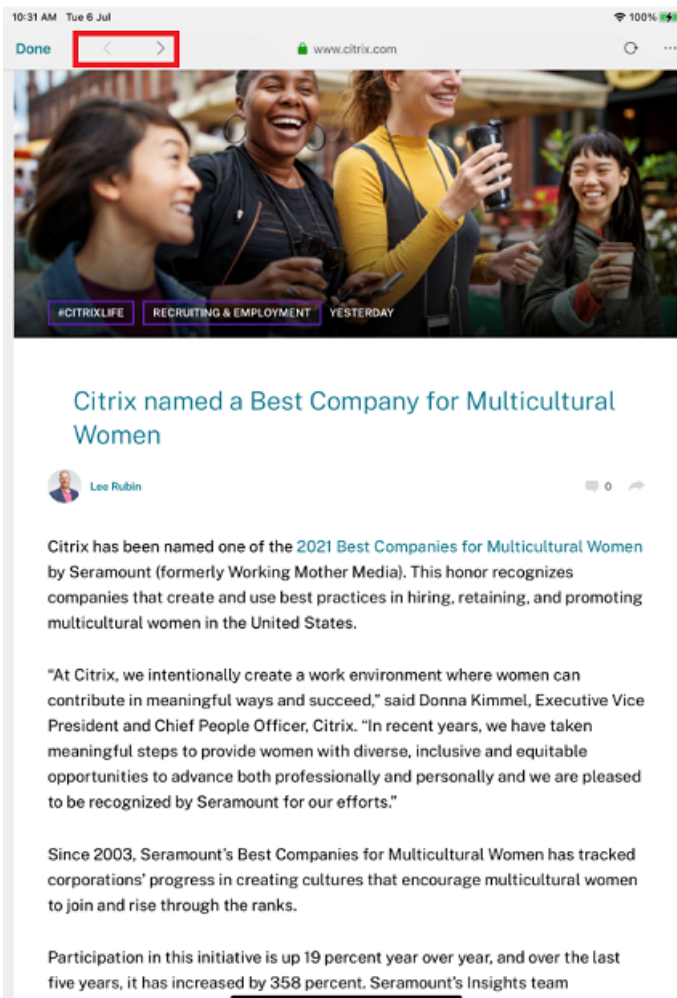
Switch between SaaS and web apps

The usability enhancement lets you navigate back and forth within web and Software-as-a-Service (SaaS) apps.

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.



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.

Siri integration

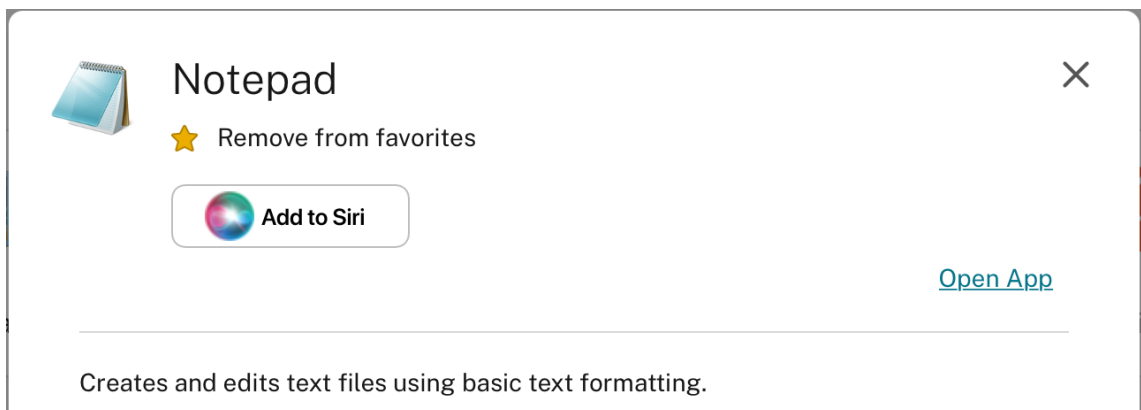
You can interact with Siri to launch resources like apps and desktops without launching Citrix Workspace app each time.

To configure

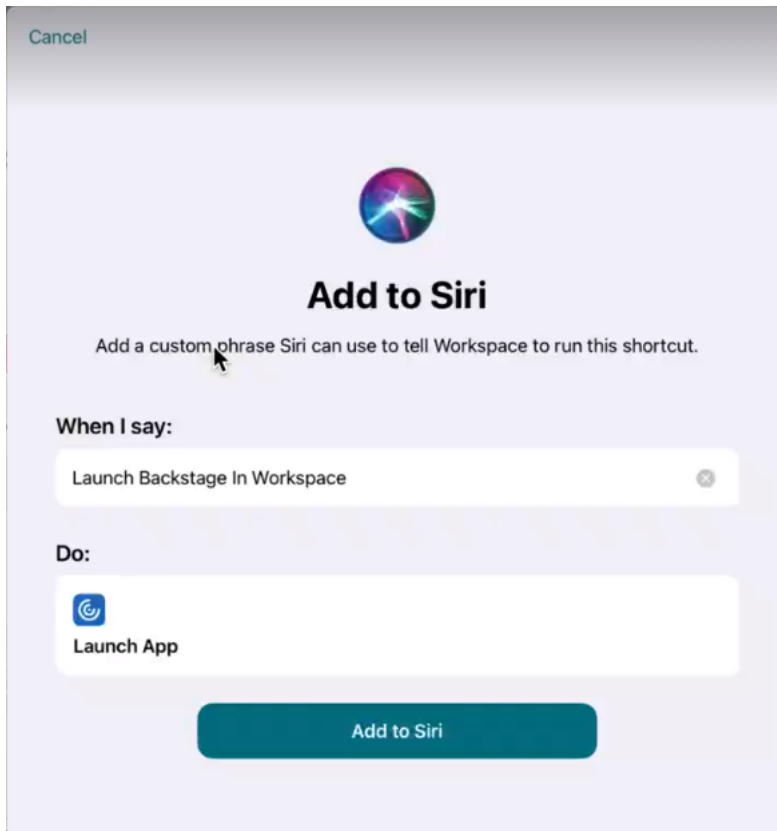
1. Launch Citrix Workspace app and tap **Apps** or **Desktops**. Select the resource that you want to add to the Siri shortcut.
2. Tap ellipsis (...). A dialog box appears.

Note:

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



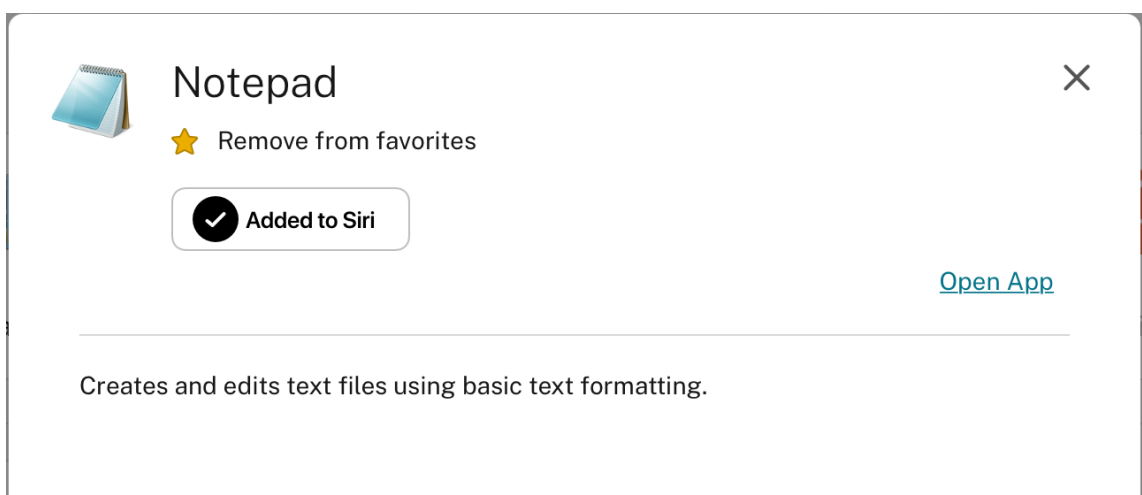
3. Tap **Add to Siri**. The **Add to Siri** dialog box appears.



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.

Support for separate session window from Citrix Workspace app

Starting with the 24.1.0 version, Citrix Workspace app for iOS introduces a separate session window that makes multitasking more efficient and user-friendly. With this feature, you can have a desktop-like experience. When the Separate Session Window feature is enabled, you may simply drag & drop sessions onto the connected external monitors. As a result, the iPad's main monitor can be used to multitask with other apps.

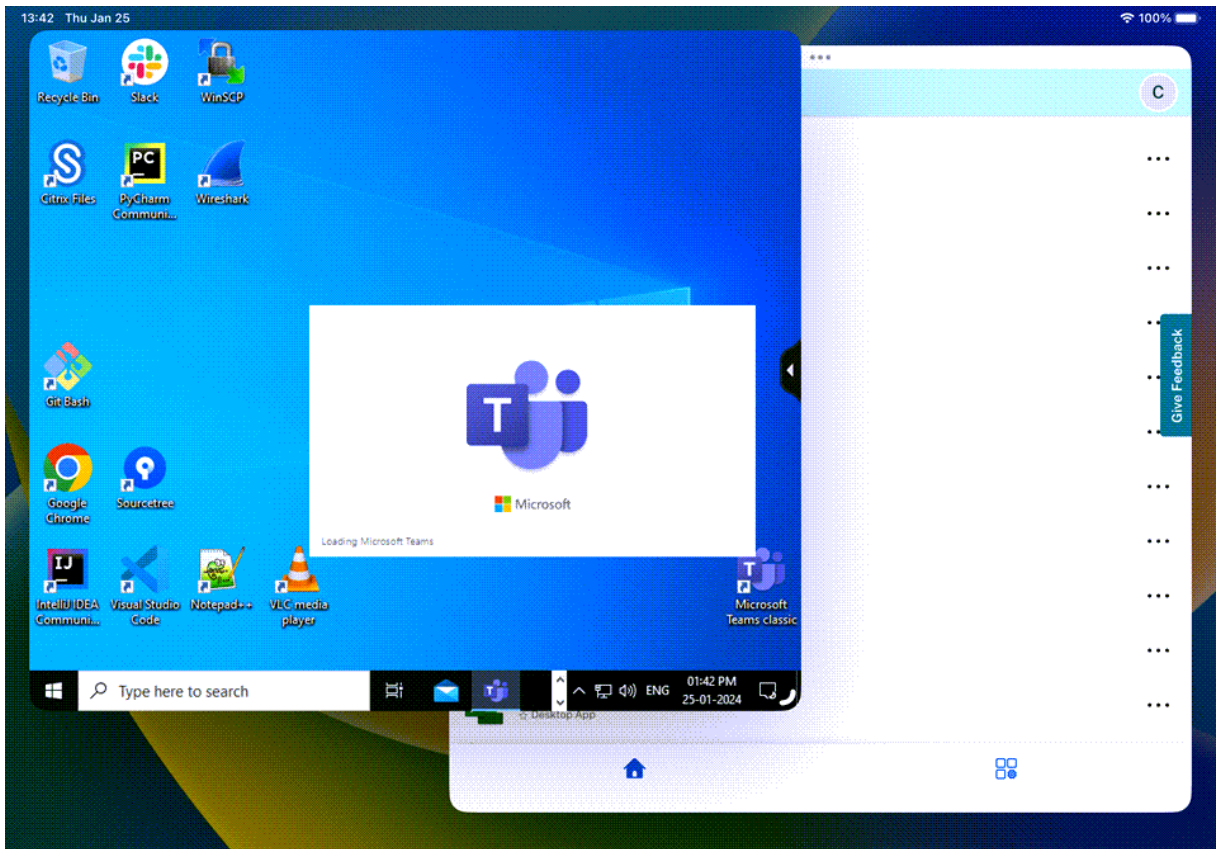
The following improvements are included with this feature:

- When you click the **Home** button on the session menu bar, the Citrix Workspace UI window opens instead of closing the HDX session window. This enhancement allows you to use the Citrix Workspace UI and the HDX session at the same time. If you start a new session from the Citrix Workspace UI, the existing one is automatically disconnected.
- When you click the **Display Options** button on the session menu bar, a setting window appears on top of the HDX session. This window allows you to adjust the session resolution instead of the Citrix Workspace UI settings.

Note:

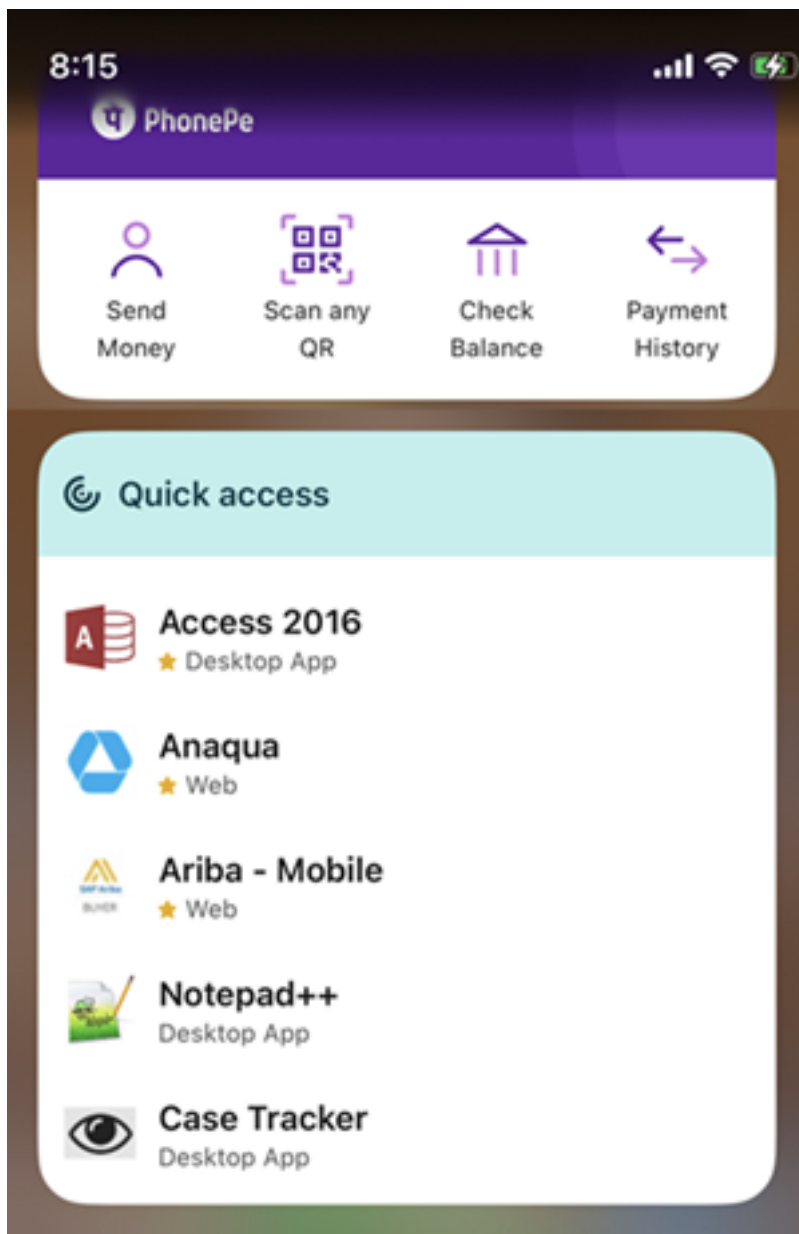
This feature is supported only on devices that support the Stage Manager feature. All iPhone devices and some iPad devices are not supporting this feature. For more information about the State Manager feature, see [Turn Stage Manager on or off on your iPad](#) in the Apple support documentation.

To configure the separate session window feature, navigate to **Settings -> Advanced -> Multitasking** and select **Separate Session Window**.



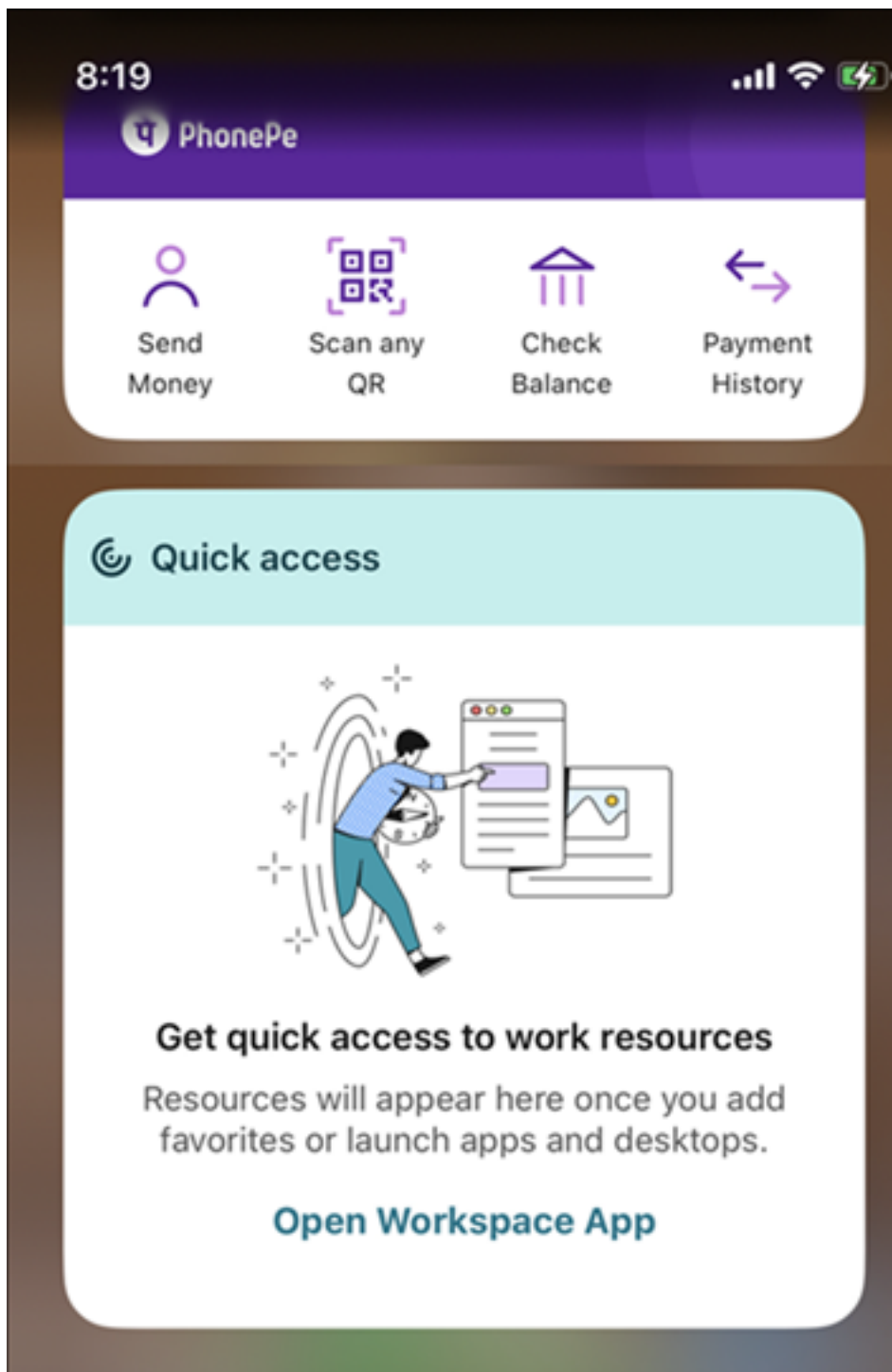
View apps and desktops as widgets

Starting with the 23.11.0 version, end users can now launch their virtual apps and desktops directly from their iPhones and iPads. They do not need to open the Citrix Workspace app to start an app or desktop session. A user can have a maximum of five virtual apps and desktops as widgets.



The widgets are created automatically as per the following criteria:

- Three Favorite and two recently opened apps or desktops are displayed as widgets
- If there are no Favorite apps or desktops, up to five recently opened apps and desktops are displayed as widgets
- If there are no recently opened apps or desktops, up to five Favorite apps or desktops are displayed as widgets
- If no apps or desktops have been added as Favorite yet and no apps or desktops were opened recently, users are prompted to open the Citrix Workspace app for iOS. They can then mark certain apps or desktops as Favorites.



Webview for Web and SaaS apps

February 28, 2024

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.

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. It improves productivity and gives a better performance in rendering the 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

- consistent 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.

Password management

February 28, 2024

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.

How to use

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 save password

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 saved 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 monitor 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 server that 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, **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.

Authenticate

June 28, 2024

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`.

The authentication is completed when the user extracts the user name and domain, and provides the required information (such as password). 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 that you use the Web Interface for traditional SSL-based Citrix Virtual Apps connections, where you can configure the Citrix Gateway.

Configure the XenApp farm for Citrix Workspace app for mobile devices to support connections from the 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 checkbox), 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, if it is an intermediate certificate, then 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.

Support to switch web browser for authentication

Starting with the 23.2.0, administrators can now switch the browser being used for the authentication process from embedded browser to system browser on iOS or iPad devices, when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment.

Configure Rewrite policy for authentication process Administrators can switch the browser being used for the authentication process from embedded browser to system browser. It is only possible when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment. To configure an advanced authentication policy, 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\").EQ(\")"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 more capabilities such as:

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

Embedded browser is used as the default browser for authentication if the administrator hasn't 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:

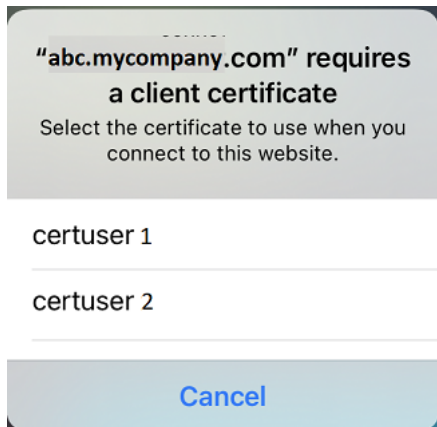
NetScaler Gateway	Global App Configuration Service	Browser used for authentication
System	System	System
System	Embedded	System
Embedded	System	System
Embedded	Embedded	Embedded
No Configuration	System	System
No Configuration	Embedded	Embedded

Support certificate-based authentication for on-premises stores

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. You can switch 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.

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
 - Type-C CCID-compliant readers
 - twocanoes smart card utility reader
- Supported VDA Smart Card Middleware
 - ActiveIdentity
- 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.

Support for Type C-based Generic Readers

Starting with the 23.12.0 version, Citrix Workspace app for iOS now supports Type-C CCID compliant readers for Smart Card authentication. Previously, only lightning port-based readers were supported. The inclusion of Type-C smart card readers within the Citrix Workspace app offers dual advantages: users can authenticate through Citrix Workspace app and seamlessly use the smart card within their virtual desktop sessions.

Support for the twocanoes smart card utility reader

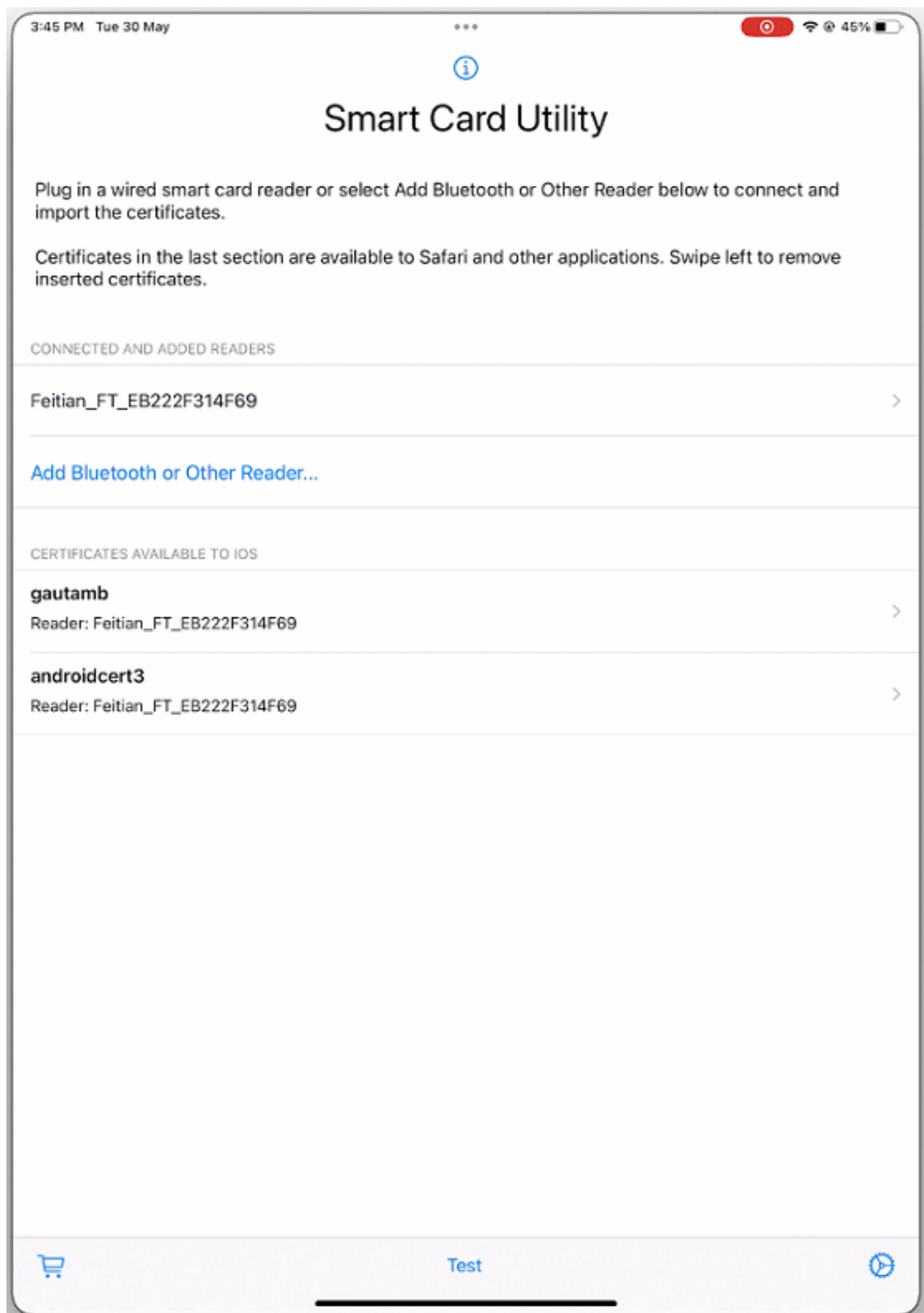
Starting with the 24.3.5 version, Citrix Workspace app for iOS supports the twocanoes smartcard utility readers. For more information about supported smart card readers, see [Smart Cards](#).

Note:

The twocanoes smart card utility USB-C reader is supported for both Citrix Workspace app login and virtual session login. However, the twocanoes smart card utility Bluetooth reader is supported only for Citrix Workspace app login and not for virtual session login.

To configure the twocanoes smart card utility Bluetooth reader, do the following steps:

1. Download and install the Smart Card Utility app from the App store. For more information, see [Smart Card Utility Bluetooth Reader Quick Start](#) in the twocanoes knowledge base.
2. Make sure that the Bluetooth on your device is turned on and the smart card is inserted into the reader.
3. Open the Smart Card Utility app.

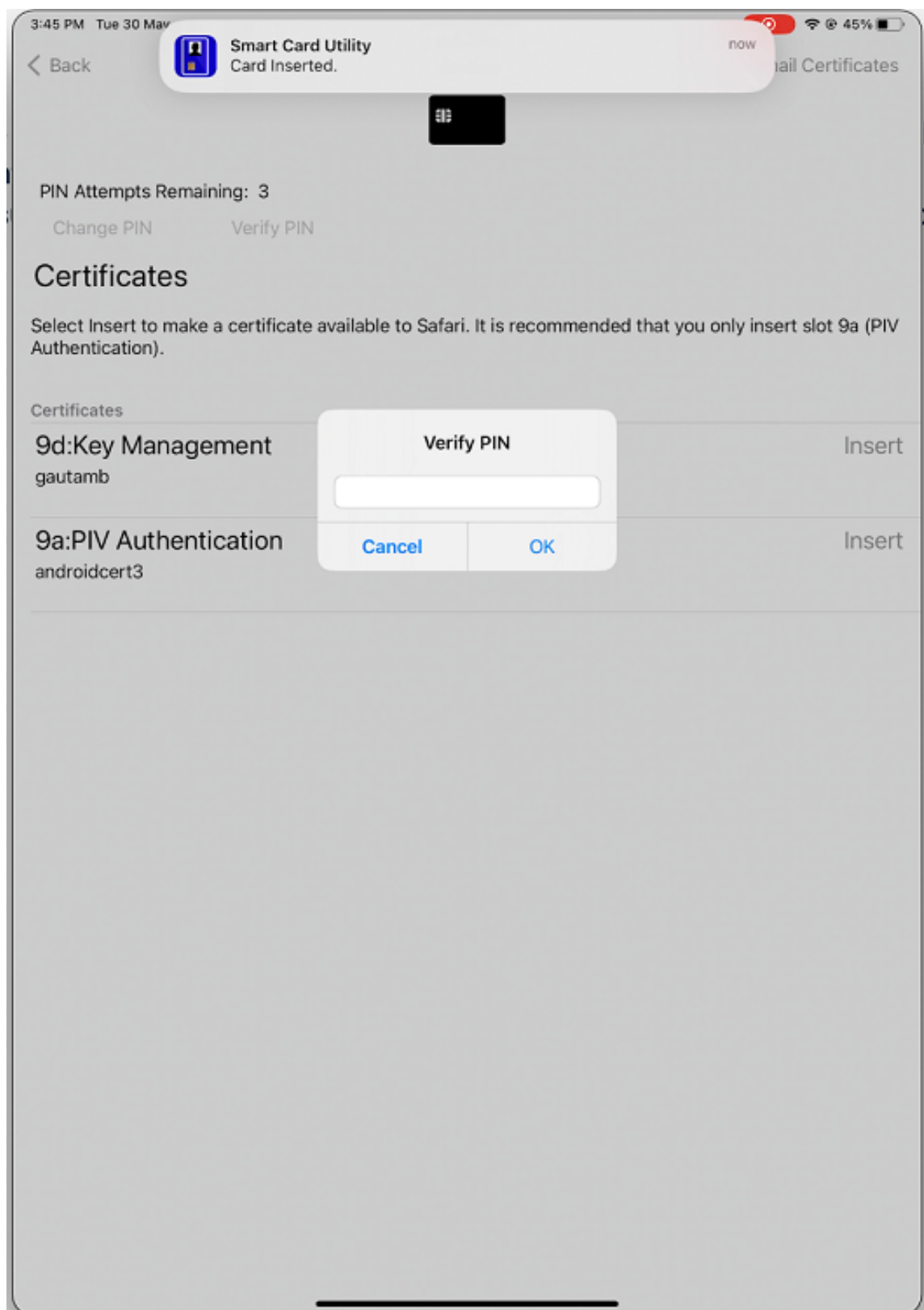


4. If you are using the Bluetooth reader, then tap **Add Bluetooth or Other Reader...** and select

your reader to connect.

Note:

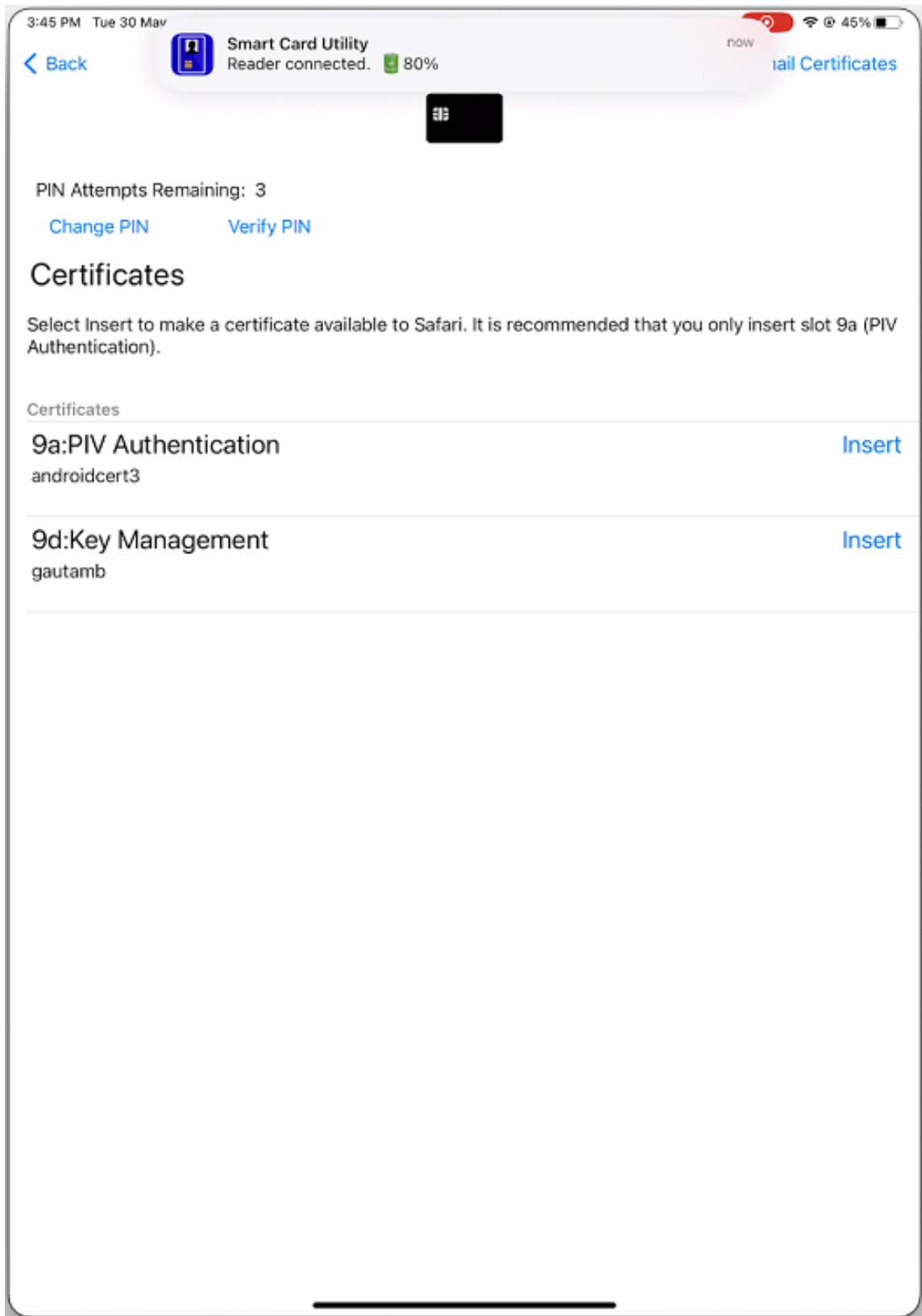
If the reader is enabled with pin pairing, then you must enter the **PIN** when prompted. The **PIN** is available on the backside of the reader.



5. Tap **Insert** on the required certificate to copy it to the keychain interface.

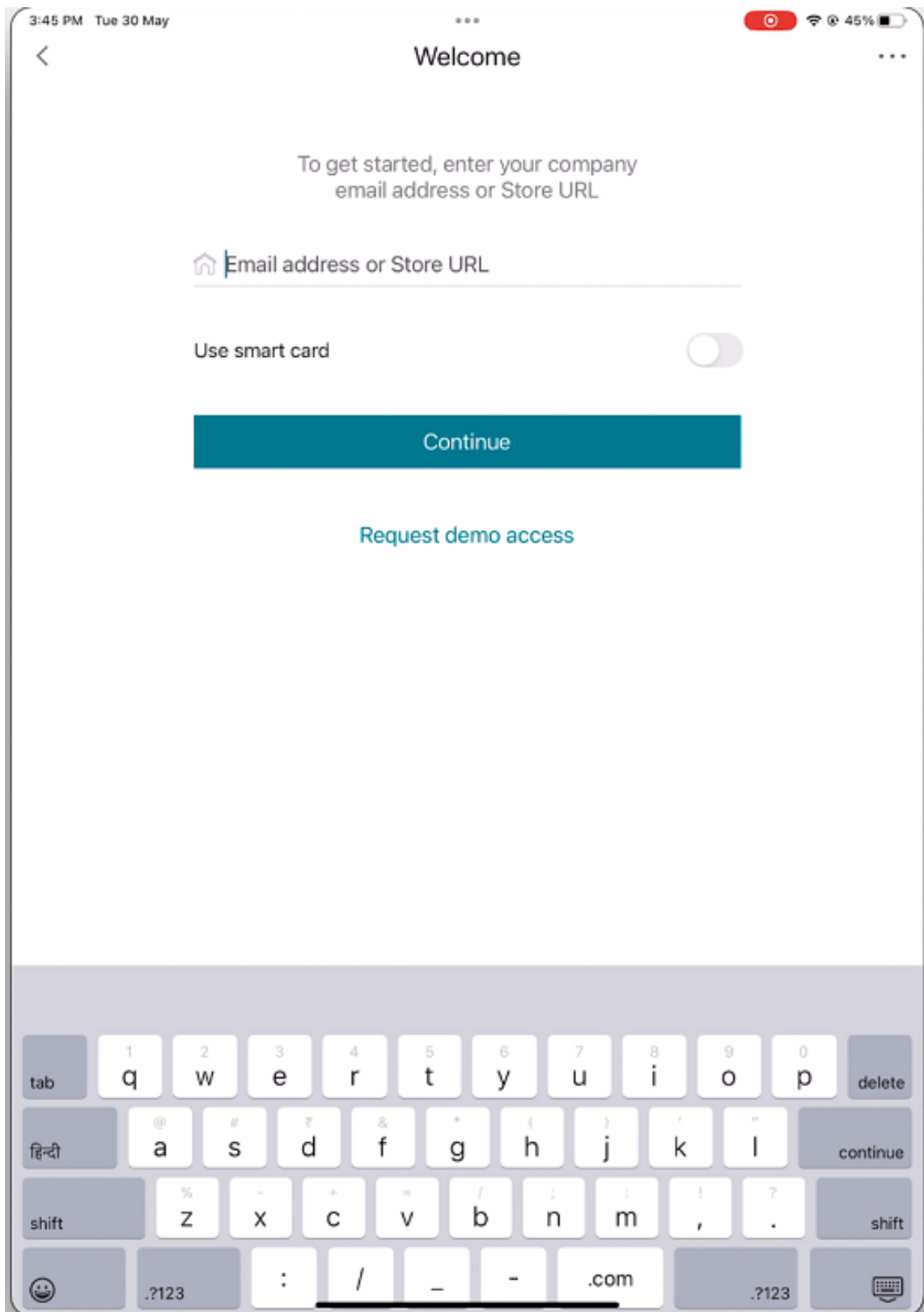
Note:

The Smart Card Utility app has implemented a cryptokit extension provided by Apple to write certificates to the keychain interface in the form of tokens. For more information, see [Configure Smart Card Authentication](#) in the Apple developer documentation.

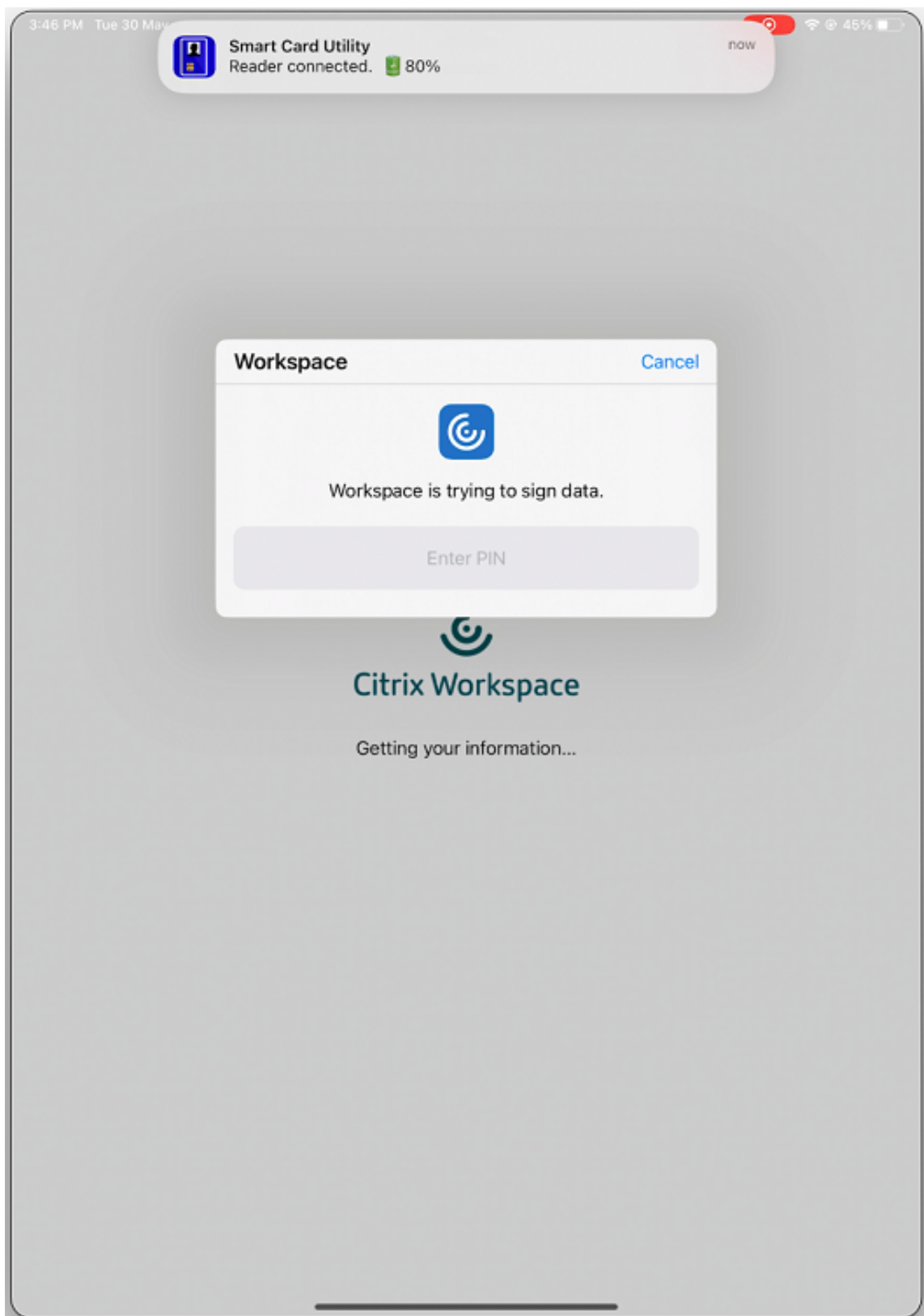


6. Make sure that the reader remains connected to the device.

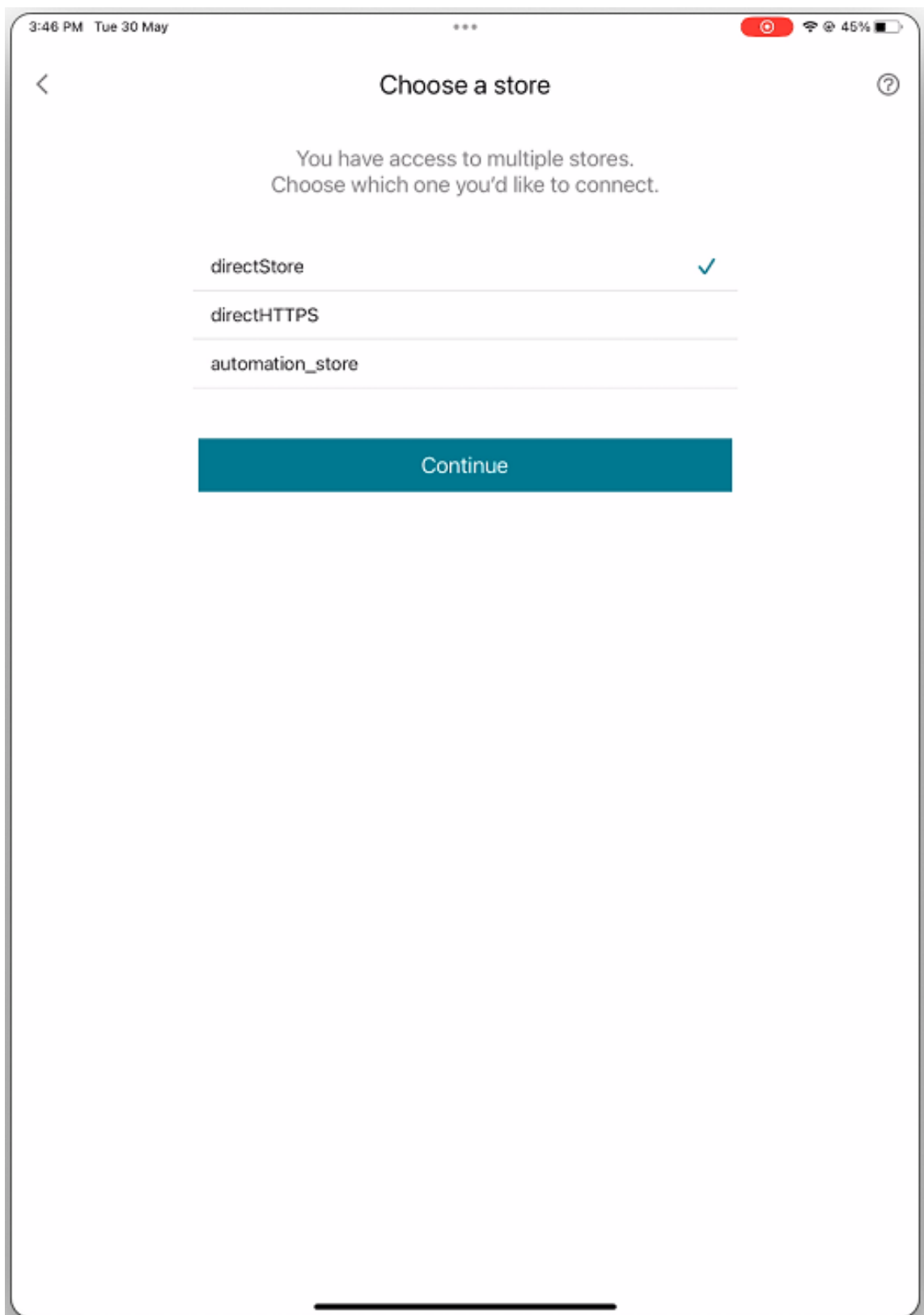
7. Open Citrix Workspace app and enter the store URL that is configured with smart card authentication.



8. On the Certificates screen, select the required certificate and enter the smart card PIN provided by your IT administrator to sign in.



9. If you have access to multiple stores, then select the required store and tap **Continue**.



10. After successful authentication, you are signed in to the Citrix Workspace app.

YubiKey support for smart card authentication

Starting with the 23.12.0 version, you can now perform smart card authentication using YubiKey. This feature provides a single-device authentication experience for Citrix Workspace app and for the virtual sessions and published apps in the VDA session. It eliminates the need to connect smart card readers or other external authenticators. It simplifies the end-user experience as YubiKey supports a wide variety of protocols, such as OTP, FIDO and so on.

To sign in to Citrix Workspace app, end users need to insert the YubiKey into their iPhone or iPad, turn on the Smart card toggle, and provide their Store URL.

Note:

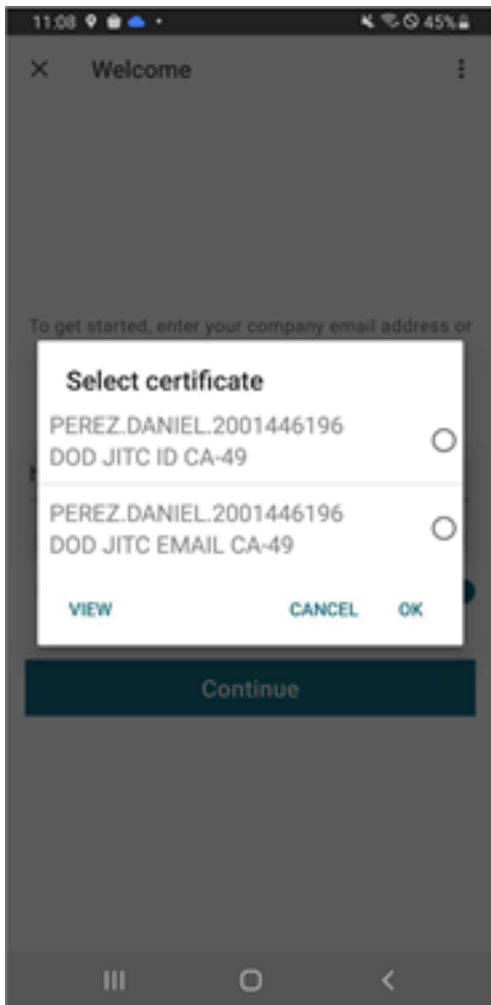
This feature supports only direct connection to Citrix Workspace app on StoreFront deployments and not through Citrix Gateway. The YubiKey support for smart card authentication through Citrix Gateway will be available on the future release.

Citrix Workspace app for iOS supports only the YubiKey 5 series. For more information on YubiKey, see [YubiKey 5 series](#).

Support for multiple certificates in smart card authentication

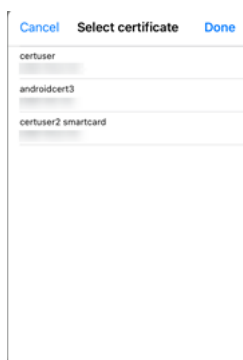
Previously, Citrix Workspace app for iOS displayed the certificate available on the first slot of the connected smart card.

Starting with the 24.1.0 version, Citrix Workspace app for iOS displays all the certificates available on the smart card. This feature allows you to select the required certificate while authenticating through smart card authentication.



View all certificates available on smart card

Starting with the 23.7.5 version, Citrix Workspace app for iOS now displays multiple certificates available on the smart card and allows you to select the certificate for smart card-based authentication. The required certificate can be selected from the **Select certificate** page once the smart card toggle has been enabled.



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 are 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 can't be edited. Delete and create the card.
- A PIN can be invalid up to ten times. If it is invalid after ten tries then the virtual smart card gets deleted.
- When you select derived credentials, the virtual smart card overrides a physical smart card.

User-agent string for WKWebView

Starting with the 23.3.5 version, the user-agent string used during some of the network requests initiated through WKWebView now includes the Citrix Workspace app identifier by default.

Therefore, it has been changed from:

```
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
```

To one of the following:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone  
(iPhone example)
```

Or

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad  
(iPad example)
```

nFactor authentication

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide multiple proofs of identification 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.

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:

While performing advanced (nFactor) authentication for Citrix Workspace app on iPhone or iPad, the authentication process is redirected to an embedded WebView. The resultant user agent string might vary slightly based on the OS version, the CWA build version, the device model, and the AuthManager version. For example, consider the following user agent strings for iPhone and iPad.

For iPhone:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X) AppleWebKit /605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/16.2 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone AuthManager/3.3.0.0
```

For iPad:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0
```

This feature is in preview. It can be enabled on request using the [Podio link](#) or by contacting Citrix Technical Support. However, it will eventually be rolled out to every customer after the preview has ended.

Note:

- The version or device model information might vary based on the environment.
- To apply Citrix Workspace app for iOS-specific user agent-based policies during authentica-

tion, use the following keywords:

- iOS
- CWA
- CWACapable

Support for FIDO2-based authentication when connecting to HDX session

Starting with the 23.9.0 version, Citrix Workspace app for iOS now supports password-less authentication within a Citrix Virtual Apps and Desktops session using FIDO2-based authentication methods. This feature allows users to sign in to a WebAuthn-supported website in browsers such as Google Chrome or Microsoft Edge using FIDO2-supported Yubico security keys. Simply opening a WebAuthn-supported website triggers password-less authentication.

Only lightning port-based devices are supported (devices with USB-C or USB 4 ports aren't supported). Signing in to the Citrix Workspace app or desktop session using password-less authentication isn't supported.

For more information about the prerequisites, see [Local authorization and virtual authentication using FIDO2](#) in the Citrix Virtual Apps and Desktops documentation.

Support for authentication using FIDO2 when connecting to a cloud store

Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Touch ID, and Face ID only). This feature is enabled by default.

Note:

FIDO2 authentication is supported with the Chrome custom tabs by default. If you are interested in using FIDO2 authentication with WebView, register your interest using this [Podio form](#).

Support for configuring storage of authentication tokens on the on-premises deployment

Citrix Workspace app for iOS now provides an option to configure the storage of authentication tokens on the local disk for on-premises stores. With this feature, you can disable the storage of the authentication token for the enhanced security. After disabling, when the system or session restarts, you need to authenticate again to access the session.

To disable the storage of authentication tokens on the on-premises deployment using the administration config file, 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">`
3. Before the `</account>` tag, navigate to the properties of that user account and add the following:

```
1     <properties>
2         <property name="TokenPersistence" value="false" />
3     </properties>
4 <!--NeedCopy-->
```

The following is an example of the web.config file:

```
1     <account id="#####" name="Store
2         Service"
3         description="" published="true" updaterType="None"
4         remoteAccessType="StoresOnly">
5         <annotatedServices>
6             <clear />
7             <annotatedServiceRecord serviceRef="1__Citrix_Store">
8                 <metadata>
9                     <plugins>
10                        <clear />
11                    </plugins>
12                    <trustSettings>
13                        <clear />
14                    </trustSettings>
15                    <properties>
16                        <clear />
17                        <property name="TokenPersistence" value="false"
18                            />
19                    </properties>
20                </metadata>
21            </annotatedServiceRecord>
22        </annotatedServices>
23        <metadata>
24            <plugins>
25                <clear />
26            </plugins>
27            <trustSettings>
28                <clear />
29            </trustSettings>
30            <properties>
31                </properties>
32        </metadata>
33    </account>
34 <!--NeedCopy-->
```

Reauthentication after session timeout

Starting with the 23.3.0 version, you are now prompted to reauthenticate to the Citrix Workspace app if your session has expired since your last sign-in. You are prompted for two-factor authentication or a username and password when connecting to the Citrix Workspace app from the web or a native client.

Secure

June 28, 2024

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 a 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're 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're 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're 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're 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 the 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 are 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 100 s 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 applications can use the root certificate using TLS.

Support for Transport Layer Security 1.3 Starting with the 23.9.0, Citrix Workspace app for iOS now supports Transport Layer Security (TLS) 1.3 that boosts performance and efficiency. TLS 1.3 provides robust security with its strong cipher suites and one-time session keys.

End users can enable it on Citrix Workspace app for iOS as follows.

1. Go to **Advanced settings > TLS Versions**.
2. Select **TLS 1.3 version**.

XenApp and XenDesktop Site

To configure the XenApp and XenDesktop Site:

Important:

- Citrix Workspace app uses XenApp and XenDesktop Sites, which support Citrix Secure Gateway 3.x.
- Citrix Workspace app uses Citrix Virtual Apps websites, which support Citrix Secure Gateway 3.x.
- XenApp and XenDesktop Sites supports only single-factor authentication.
- Citrix Virtual Apps websites support 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've created the XenApp and XenDesktop Site using the default path (`/Citrix/PNAgent`), enter the Secure Web Gateway FQDN: `FQDNofSecureGateway.companyName.com`
 - If you've 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`

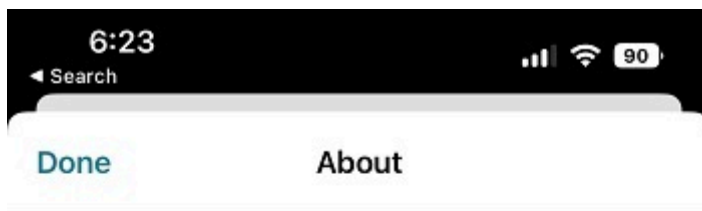
2. If you're manually configuring the account, then clear the Citrix Gateway option **New Account** dialog.

Troubleshoot

April 11, 2024

How to check app's version

To check your Citrix Workspace app version, open your app. Tap **Settings** > **About**. The version information is displayed on your screen.



24.1.0.10 (2401)

© 1990-2024 Cloud Software Group, Inc.
All Rights Reserved.

[Third Party Notices](#)

[User Agreements](#)



How to upgrade Citrix Workspace app to the latest version

You can upgrade to the latest version of Citrix Workspace app from the App Store. Search for Citrix Workspace app and tap the **Upgrade** button.

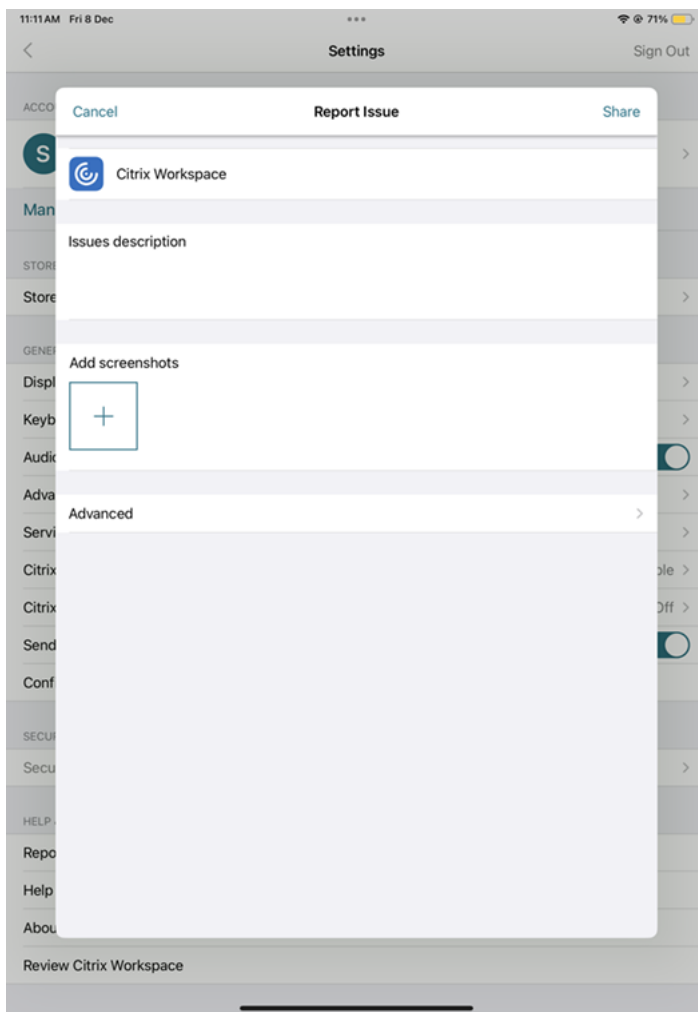
How to reset Citrix Workspace app

You can reset your Citrix Workspace app using one of the following methods:

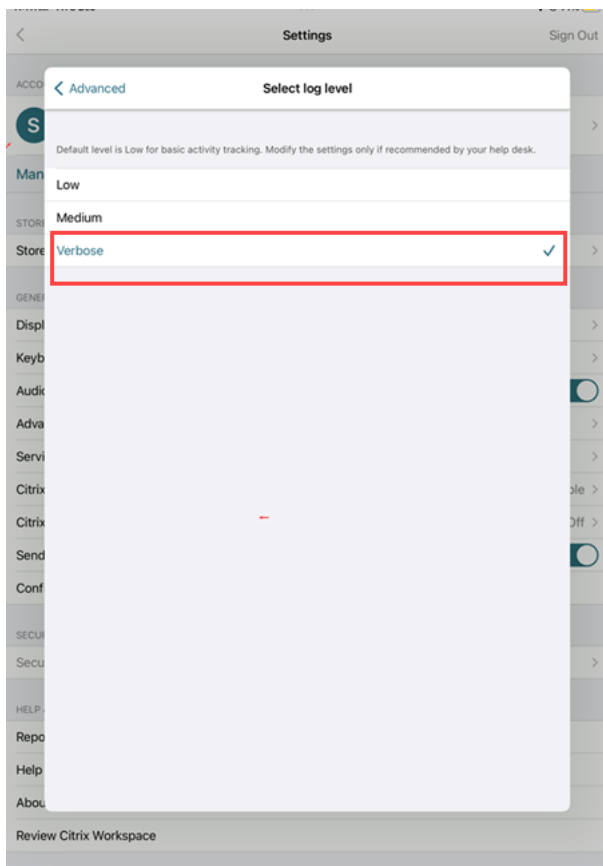
- Delete any existing accounts from Citrix Workspace app
- Clear the Citrix Workspace app storage data
- Uninstall Citrix Workspace app and install the latest Citrix Workspace app for iOS that has the latest fix.

How to collect logs

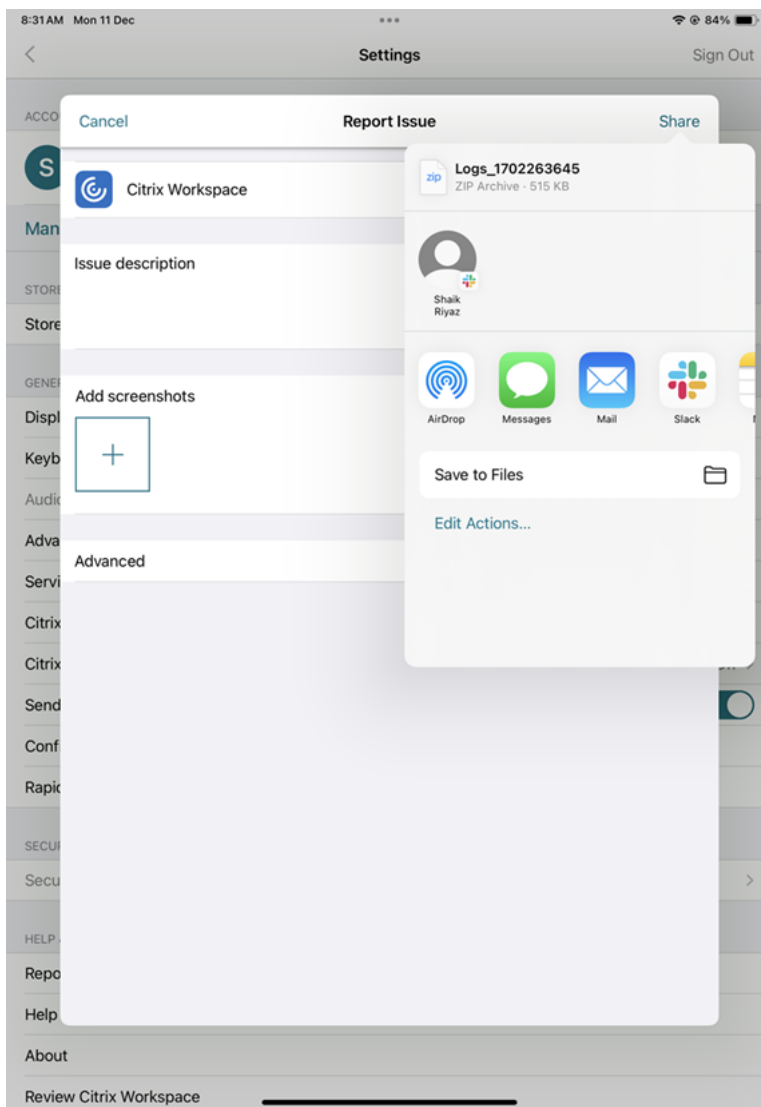
1. Open your Citrix Workspace app and navigate to **Settings**.
2. Under **Help & Support**, select **Report Issue**.



3. Reproduce your issue.
4. On the Select log level page, select **Verbose**.



5. On the **Select Log location** page, select **Both Console & File**.
6. Share the zip file with Citrix.



How to request for enhancements

You can send in your requests for enhancements by filling out [this form](#).

How to access technical preview features

You can request for Technical Preview features using a Podio form that is unique to each feature. You can find this form attached with the Technical preview announcement in the [Product Documentation](#).

How to provide feedback on EAR

To provide feedback on the EAR version, tap [here](#).

Common issues and troubleshooting tips

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. The issue occurs when you use 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.

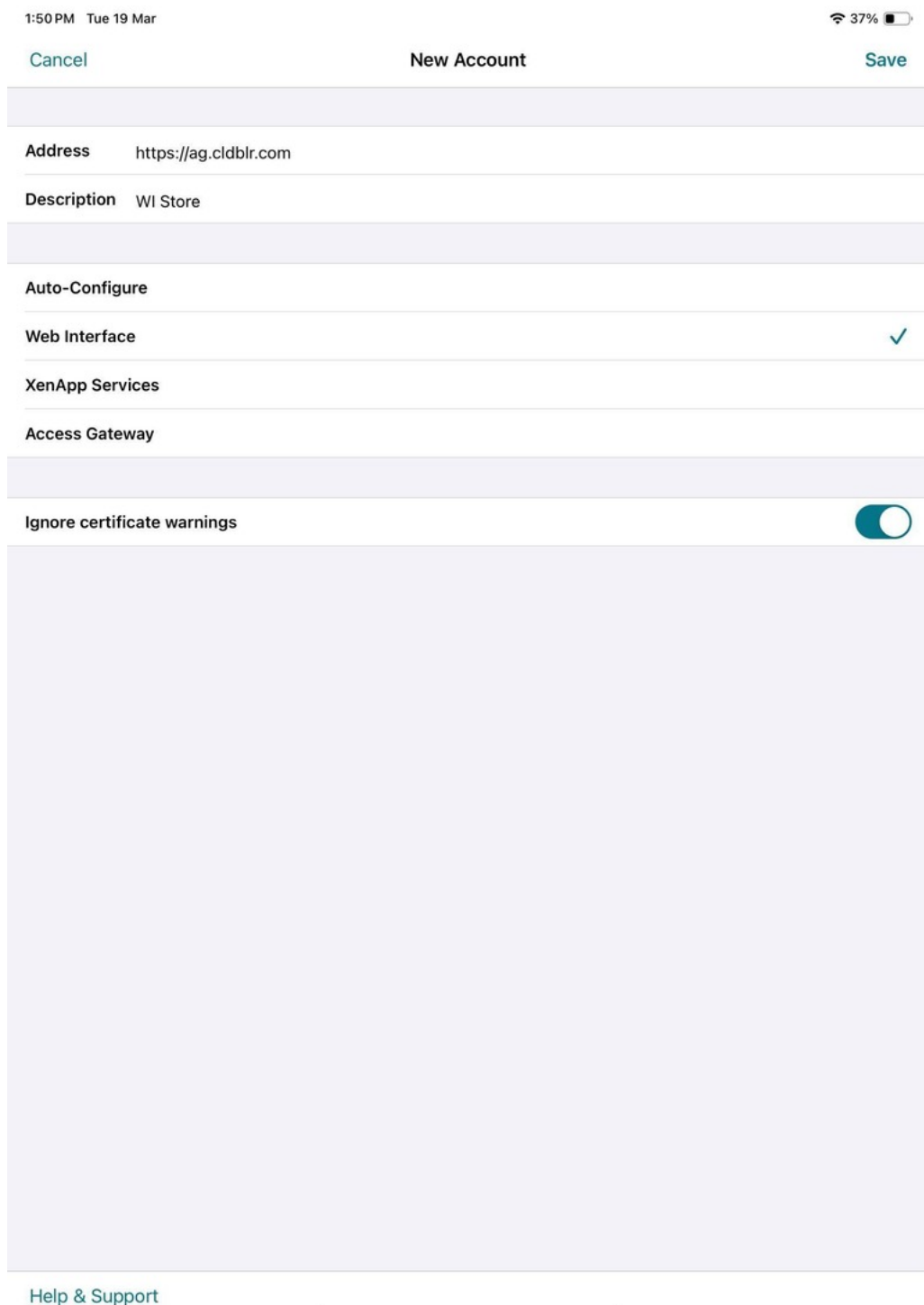
For suggestions about how to create policies to improve audio quality, see Knowledge Center article [CTX123543](#).

Failed to launch desktop and app sessions for customized store experience

You might fail to launch desktop and app sessions from Citrix Workspace app if you have customized store experience. The auto-discovery of store type is supported only for e-mail addresses and not for store URLs. It is recommended to use email address or Web-interface login mode if you have a customized store. For more information, see [Manual setup](#) and [Configuring email-based account discovery](#).

To configure an account manually through Web-interface login mode, do the following steps:

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 the **Web Interface** connection. This connection mode displays a Citrix Virtual Apps web-site similar to a Web browser. This UI is also known as Web View.



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 by 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.

Note:

You must enter the user credentials for each connection, as they are not saved in the Web interface login mode.

FAQs

How to improve the video performance on virtual app and virtual desktop for low-powered or mobile devices

For information on how to improve and configure virtual desktop video performance using the MaxFramesPerSecond registry value or using HDX policies, depending on your Citrix Virtual Apps and Desktops version, see the Knowledge Center article [CTX123543](#).

I can't see my apps or desktops after signing on to Citrix Workspace app

Contact your company's help desk or your IT Support team administrator for further assistance.

How to troubleshoot slow connections

If you face any of the following issues, follow the steps mentioned in the following **Workaround** section.

- Slow connections to the Citrix Virtual Apps and Desktops site
- Missing app icons
- Recurring Protocol Driver Error messages

Workaround Disable Citrix PV Ethernet Adapter properties for the network interface on Citrix Virtual Apps server, Citrix Secure Web Gateway, and Web Interface server.

The Citrix PV Ethernet Adapter properties include the following properties that are enabled by default. You need to disable all of these properties.

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

Note:

Server restart isn't required. This workaround applies to the Windows Server 2003 and 2008 32-bit. This issue does not affect the Windows Server 2008 R2.

Troubleshoot issue with Numeric keys and special characters

If numeric keys or Chinese IME characters do not function as expected, you need to disable the Unicode Keyboard option.

To disable the Unicode Keyboard option:

1. Navigate to **Settings > Keyboard Options**.
2. Set **Use Unicode Keyboard** to **Off**.

Citrix Workspace app for iOS

June 10, 2024

Citrix Workspace app for iOS is client software available for download from the App Store. It enables you to access and run virtual desktops and hosted applications delivered by Citrix Virtual Apps and Desktops.

iOS is the operating system for Apple mobile devices such as iPads and iPhones. Citrix Workspace app for iOS runs on devices using the iOS operating system, such as iPhone X, iPad mini, and iPad Pro.

Language support

Citrix Workspace app for iOS is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for iOS, see [Language support](#).

Deprecation

The announcement in this article gives you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they're withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

Deprecated items aren't removed immediately. Citrix continues to support them in this release but they'll be removed in the future.

Item	Deprecation announced in	Removed in	Alternative
Support for DTLS 1.0 protocol	Citrix Workspace app for iOS version 24.5.0	-	DTLS 1.2 protocol
Support for TLS 1.0 and TLS 1.1 protocols	Citrix Workspace app for iOS version 24.4.0	-	TLS 1.2 or TLS 1.3 protocol
XenApp Services (also known as PNAgent)	Citrix Workspace app for iOS version 23.7.5	-	Within Citrix workspace app, connect to stores using the store URL rather than the XenApp Services URL.
iOS operating system version 14	Citrix Workspace app for iOS version 23.10.0	Target: Citrix Workspace app for iOS 23.12.0	Upgrade to the latest available version of iOS
iOS operating system version 13.x	Citrix Workspace app for iOS version 22.9.5	Target: December 2022 and version 22.12.0	Upgrade to the latest available version of iOS
iOS operating system version 11.x and 12.x	Citrix Workspace app for iOS version 21.12.0	Target: Aug 2022 and version 22.8.0	Upgrade to the latest available version of iOS
iOS operating system version 10.x	Citrix Workspace app for iOS version 21.1.5	Release following 21.1.5	Use Citrix Workspace app for iOS version 21.1.5 or earlier

Notes:

- Existing Citrix Workspace app users on deprecated platform versions can't upgrade to the latest release (from the App Store) of the Citrix Workspace app.
- New Citrix Workspace app users on deprecated platform versions can only be able to down-

load an older compatible version from the App Store.

- Users on deprecated platform versions don't get any new features or security patches that come with every newer release of the Citrix Workspace app.



© 2024 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).