Citrix Workspace app for iOS

Contents

About this release

September 6, 2019

What's new

What's new in 1909

iOS 13 support

Citrix Workspace app for iOS is supported on iOS 13.

> **Important:**
>
> - The CR01 app is not supported on iOS 13. If you are using the CR01 app, Citrix recommends that you do not upgrade to iOS 13.
> - In iOS 13, launching sessions from the Safari web browser has changed. For more information, see the help documentation.

On iOS 13, you can now use the X1 Mouse in full desktop mode while in a session, and use it in iOS native mouse mode when you leave the session or leave the app.

What's new in 1908

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

What's new in 1907.5

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

What's new in 1907

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

What's new in 1906

Session roaming on iPad

Session roaming is also now available on iPad devices. For more information, see the help documentation for iOS devices.

Keyboard layout synchronization

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

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

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

What's new in 1905.5

Support for session roaming

Session roaming is now available on iPhone and iPod touch devices when using a cloud store. For more information, see the help documentation for iOS devices.

What's new in 1905

Enhancement to workspace hub

Citrix Workspace app integrates a new procedure for adding or removing a workspace hub from the trusted list on iOS devices. For more information, see Security Connection.

Host to client redirection

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

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

When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs.
If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA.
When host to client redirection is disabled, users open the URLs with web browsers or multimedia players on the server VDA.
When host to client redirection is enabled, users cannot disable it.

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

For more information, see General content redirection.

What's new in 1904.5

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

What's new in 1904.2

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

What's new in 1904

Enhancements

- You can view the list of recently used SaaS or Web apps under the Recent tab for apps and desktops.
- Citrix Ready workspace hub supports a Secure Sockets Layer (SSL) connection between mobile devices and the hub for security purposes. You need to set a Fully Qualified Domain Name (FQDN) either manually or automatically to uniquely identify each device. For more information, see Security connection in the Citrix Ready workspace hub documentation.

What's new in 1903

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

What's new in 1902

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

What's new in 1901

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

What's new in 1812

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

What's new in 1811

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

What's new in 1810.2

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

> **Note:**
>
> For more information on configuring Citrix Ready workspace hub internal beacons, see Knowledge Center article CTX218708.

What's new in 1810.1

Support for 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 Citrix Ready workspace hub in Citrix Workspace app for iOS, see Configure Citrix Ready workspace hub.

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

What's new in 1810

Support for Purebred derived credentials

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

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

For information on configuring derived credentials, see Derived credentials.

What's new in 1809

iOS 12 support

Citrix Workspace app for iOS fully supports iOS 12.

What's new in 1808

Updated end user help

The end user help located within the app has been completely rewritten and updated to reflect all the changes to Citrix Workspace app for iOS.

Fixed issues

Fixed issues in 1909

- When you use the mouse pointer to double-click an app or a file, the app or the file opens twice. [LD1160]
- Citrix Workspace app for iOS Versions 1904 and 1905 sometimes exit unexpectedly. [RFIOS-4301]
- This release addresses connectivity and discovery issues with the Citrix X1 Mouse. [RFIOS-4529]

Fixed issues in 1908

- When the Citrix Workspace app moves from the background to the foreground, the following error message appears: "Reconnected to server". [RFIOS-4510]
- When the Citrix Workspace app moves from the background to the foreground, any window that is open using the published desktop moves on the screen and the screen resolution appears odd. This issue occurs when you use the Citrix Workspace app version 1904.2 or later. [RFIOS-4401]
- After you configure Face ID authentication on the device, the following issue might occur: When you refresh the list of apps and desktops, the Citrix Workspace app might exit unexpectedly. [LD1633]
- After you disconnect or reconnect a session, the Citrix X1 Mouse might fail to be rediscovered. Also, occasionally, drag-and-drop mouse actions are unsuccessful. [RFIOS-4487]

Fixed issues in 1907.5

- When your Active Directory (AD) password expires, the Sign in page does not alert you about it. [LD1849]

Fixed issues in 1907

- On an iPad, when two resources have the same display name and one of them is already in a session, launching the other resource might fail. [LD1467]
- When an active user session times out, the session might fail to relaunch and the following error message appears:

  "The address given did not provide a valid app list. Please check the address, gateway settings, and your network connection."

  The issue occurs due to incorrect communication between the Citrix Workspace app and the Citrix Gateway.
- On a smart keyboard, when you press the Shift key and scroll using the Citrix X1 mouse, the vertical scroll is unsuccessful. [LD1284]

Fixed issues in 1906

- If you try to launch an app or desktop locally, while roaming the same app or desktop from a cloud store to a workspace hub, your roaming session ends. [WH-2128].
- The search bar on the iPad is truncated when switched to the Landscape mode. [RFIOS-2310]
- When you rotate the device to Landscape mode, the **Settings** menu might display abnormally. This issue occurs when you minimize the Citrix Workspace app screen while in multi-task mode. [RFIOS-3066]

Fixed issues in 1905.5

- After you sign on to StoreFront using the Safari web browser, the virtual desktop or application might fail to open. [RFIOS-4178]

Fixed issues in 1905

This release also addresses a number of issues that help to improve overall performance and stability.

Fixed issues in 1904.5

- When you log on to Citrix Workspace app for the first time, your login might fail and the following error message appears:

  "Cannot Connect to Server. Try again."

  [RFIOS-3588]
- Unable to get the current latitude and longitude report details. [RFIOS-3668]
- Deleting client certificates from **Account Settings** might cause Workspace app to exit unexpectedly. [RFIOS-4212]

Fixed issues in 1904.2

- When you tap the "arrow" icon on the custom toolbar, the custom arrow keys are invisible. [RFIOS-4233]

Fixed issues in 1904

- You can add PNAgent accounts seamlessly. [RFIOS-3342]
- You can view the WiFi SSID on certain connection related error messages. With the help of the WiFi SSID, you can ensure that you are on the same network as the Citrix Ready workspace hub you are trying to connect to. [WH-1903]
- When the active directory (AD) password has expired, resetting your AD password from Citrix Workspace app fails with an error. [RFIOS-3241]
- In sessions running on a Japanese language VDA, pressing the Option (Alt) + Return keys allows you to input a new line in a cell in Microsoft Excel while retaining the IME mode. [RFIOS-4046]
- When you reconnect a device and the VDA, the display becomes unresponsive for 10 to 20 seconds after the device recovers from sleep mode. [RFIOS-4146]
- With Google two-factor authentication, logging on to Citrix Workspace app from an iOS device fails and the following error message appears:

  Incorrect user name, password or passcode

  [RFIOS-4064]

Fixed issues in 1903

- When using Version 1810 of Citrix Workspace app on an iPhone X, the keyboard symbol disappears when the client device is in landscape view. [LD0619]

- When using Version 1812 of Citrix Workspace app on a non-English system, the **Add new account** field label appears in English. [LD1066]
- The Citrix X1 Mouse becomes unresponsive when the client device is idle for a long time. [LD0842]
- The Citrix Workspace app splash screen dialog is suppressed in version 1903 and later. [RFIOS-3509]

Fixed issues in 1902

- When Enlightened Data Transport (EDT) protocol is used, the display becomes unresponsive for 10 to 20 seconds after the device recovers from sleep mode. [LD0854]
- When you enter username and password for authentication, the keyboard layout switches to a different language when using the password field. [LD0588]

Fixed issues in 1901

- When an external Apple Bluetooth keyboard is connected and you press Shift + 0 to type the ")" symbol, the session is disconnected. [RFIOS-3658]

Fixed issues in 1812

- The text on the screen appears to be spaced incorrectly if the screen resolution is set to "Auto-fit Low" with a resolution of 1024x1366. [LC9808]
- When Citrix Gateway is pointing to the Web Interface, Stores might not enumerate correctly and you might have issues when adding the Store account. [RFIOS-3342]
- When you attempt to remove mandatory apps from the **Favorite Apps** list, Citrix Workspace app does not display an alert message. [RFIOS-1556]
- When the virtual keyboard appears, the X1 mouse coordinates can offset to display an incorrect selection. [RFIOS-3418]
- When you sign in to a PNAgent account, the page does not display a screen asking you to enter your domain credentials. This issue occurs if you missed entering the domain credentials initially. [RFIOS-2944]
- After upgrading to Citrix Workspace app for iOS 1809, when you launch a published app, a **Certificate not trusted** error message appears. [RFIOS-3368]

Fixed issues in 1811

- Digital signatures might not get captured correctly. To fix the issue, add the *HandleDoubleTapLocally=no* parameter into the default.ica file to disable the behavior.

  To modify the default.ica file on the StoreFront or on the Web Interface server, see the Knowledge Center article CTX116357 for detailed steps. [LD0629]

Fixed issues in 1810.2

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

Fixed issues in 1810.1

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

Fixed issues in 1810

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

Fixed issues in 1809

- Users might not be able to log on to the Store when upgrading from Citrix Receiver to Citrix Workspace app. [RFIOS-3233]

Fixed issues in 1808

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

Known issues

Known issues in 1909

- On iOS 13 devices which are using Japanese, Chinese or Korean language keyboards, the **Command-C** and **Command-V** keyboard shortcuts are unsuccessful. [RFIOS-4620]

Known issues in 1908

No new issues have been observed in this release.

Known issues in 1907.5

No new issues have been observed in this release.

Known issues in 1907

No new issues have been observed in this release.

Known issues in 1906

No new issues have been observed in this release.

Known issues in 1905.5

- If you try to launch an app or desktop locally while roaming the same app or desktop from a cloud store to a workspace hub, your roaming session ends. [WH-2128].

Known issues in 1905

No new issues have been observed in this release.

Known issues in 1904.5

No new issues have been observed in this release.

Known issues in 1904.2

No new issues have been observed in this release.

Known issues in 1904

No new issues have been observed in this release.

Known issues in 1903

- After you sign on to StoreFront using the Safari web browser, the virtual desktop or application might fail to open. [RFIOS-4178]

Known issues in 1902

No new issues have been observed in this release.

Known issues in 1901

No new issues have been observed in this release.

Known issues in 1812

No new issues have been observed in this release.

Known issues in 1811

- Finger taps might not register correctly when using the **Auto-fit High** setting on an iPad Pro 12.9". As a workaround, change the Display Options in Citrix Workspace app to another setting. [RFIOS-1766]

Known issues in 1810.2

- Finger taps might not register correctly when using the **Auto-fit High** setting on an iPad Pro 12.9". As a workaround, change the Display Options in Citrix Workspace app to another setting. [RFIOS-1766]
- When switching networks, sessions might not reconnect or relaunch. As a workaround, close and relaunch Citrix Workspace app. [RFIOS-3246]
- Sessions might not launch, displaying HdxSdkErrorDomain_Session error 8. As a workaround, close and relaunch Citrix Workspace app. [RFIOS-3374]

Known issues in 1810.1

No new issues have been observed in this release.

Known issues in 1810

No new issues have been observed in this release.

Known issues in 1809

No new issues have been observed in this release.

Known issues in 1808

- When using a smart card on an iPhone, launching an app after logging off displays a constant loading status. As a workaround, relaunch the app. [RFIOS-2550]
- When using a smart card, session sign out might not work correctly after upgrading to Citrix Workspace app for iOS. As a workaround, relaunch the app. [RFIOS-3076]

Prerequisites for installing

September 6, 2019

System requirements and compatibility

Device requirements

- Citrix Workspace app version 1808 and later for iOS supports iOS 10, 11, and 12.
- This software update has been validated on the following devices:
  - iPhone 5x models, iPhone 6x models, iPhone 7x models, iPhone 8x models, and only iPhone X model.
  - All iPad models (including iPad Pro) except for iPad 1 and iPad 2 which are not supported.
- External display support
  - iPhone - as supported by iOS.
  - iPad - as supported by iOS (does not use the whole screen).

Server requirements

Ensure you install all the latest hotfixes for your servers.

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

  StoreFront:

- StoreFront 3.6 or later (recommended). Citrix Workspace app for iOS 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 for iOS 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 for iOS.

- StoreFront configured with a Workspace for Web site

  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 Services sites
- Web Interface on Citrix Gateway (browser-based access only using Safari)

  You must 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
  - Citrix XenApp 6.5 for Windows Server 2008 R2

Connections, certificates, and authentication

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

	Workspace for Web using browsers	StoreFront Services site (native)	StoreFront XenApp Services site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes			

	Workspace for Web using browsers	StoreFront Services site (native)	StoreFront XenApp Services site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor authentica-tion (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 Web sites and for deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

For connections to the Web Interface 5.4, Citrix Workspace app for iOS 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 Services site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface XenApp Services site
Anonymous	Yes			
Domain	Yes	Yes	Yes*	

	Web Interface (browsers)	Web Interface XenApp Services site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface XenApp Services site
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

When a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the device to successfully access Citrix resources using Citrix Workspace app for iOS.

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

Manually installed certificate

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

1. Make sure you have 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 are asked to import the root certificate.

Wildcard certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app for iOS 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 the Knowledge Base article that matches your edition:

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition

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

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

Joint Server Certificate Validation Policy

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

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

When validating a server certificate, Citrix Workspace app for iOS now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous releases, Citrix

Workspace app for iOS then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

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

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

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

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

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

> **Important**
>
> Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there are currently two certificates ("DigiCert"/"GTE CyberTrust Global Root", and "DigiCert Baltimore Root"/"Baltimore CyberTrust Root") that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available ("DigiCert Baltimore Root"/"Baltimore CyberTrust Root"). If you configure "GTE CyberTrust Global Root" at the gateway, Citrix Workspace app for iOS connections on those user devices will fail. Consult the certificate authority's documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.

Then, Citrix Workspace app for iOS will use these two certificates. It will then search for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as "Example Root Certificate"), the connection succeeds. Otherwise, the connection fails. Note that this configuration supplies the intermediate certificate that Citrix Workspace app for iOS needs, but also allows Citrix Workspace app for iOS to choose any valid, trusted, root certificate.

Now suppose a gateway is configured with these certificates:

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

A web browser may ignore the wrong root certificate. However, Citrix Workspace app for iOS will not ignore the wrong root certificate, and the connection will fail.

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

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

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

Avoid configuring the gateway to use the cross-signed intermediate certificate, as Citrix Workspace app for iOS will select the earlier root certificate:

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

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

- “Example Server Certificate”

In this case, if Citrix Workspace app for iOS cannot locate all the intermediate certificates, the connection will fail.

Get started

September 6, 2019

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 Services sites and Citrix Virtual Apps and Desktops 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 for iOS, enabling 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 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.
  - Ensure that you include meaningful descriptions for published applications because these descriptions are visible to users in Citrix Workspace app for iOS.
  - You can emphasize published applications for your mobile device users by listing the applications in the Featured list of Citrix Workspace app for iOS. To populate this list on Citrix Workspace app for iOS, edit the properties of applications published on your servers and append the KEYWORDS:Featured string to the value of the Application description field.
  - To enable the screen-to-fit mode that adjusts the application to the screen size of mobile devices, edit the properties of applications published on your servers and append the KEYWORDS:mobile string to 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 you provide 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 deployment does not have a Web site or Citrix Virtual Apps and Desktops Site, create one. The name of the site and how you create

it depends on the version of Web Interface you have installed. For instructions on how to create one of these sites, see the "Creating Sites" topic for your version of Web Interface.

Manual setup

In general, when Citrix Workspace app for iOS connects to Citrix Gateway, Citrix Workspace app for iOS attempts to locate a XenApp Services site or Citrix Virtual Apps Web site 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 in the upper right corner and then in the Accounts screen, tap the 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. Additional fields appear on the screen.
3. In the Address field, type the secure URL of the site or Citrix Gateway to which you want to connect (for example, agee.mycompany.com).
4. Select one of the following connection options. The remaining fields on the screen change, depending on your selection.
   - Web Interface - Select for Citrix Workspace app for iOS to display a Citrix Virtual Apps Web site similar to a Web browser. This is also known as Web View.
   - XenApp Services - Select for Citrix Workspace app for iOS to locate a specific XenApp Services site for which authentication through Citrix Gateway is not configured. In the additional options that appear on this screen, provide site logon credentials.
     - <StoreFront FQDN>: If there are multiple stores, a list will be presented and the user can choose the store to add.
     - <StoreFront FQDN>/citrix/<Store Name>: This will add the StoreFront store <Store Name>.
     - <StoreFront FQDN>/citrix/PnAgent/config.xml: This will add the default legacy PNAgent store.
     - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: This will add the legacy PNAgent store associated with <Store Name>.
   - Citrix Gateway - Select for Citrix Workspace app for iOS to connect to a XenApp Services 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 are 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 12.
> - Citrix Workspace app for iOS supports only XenApp Services 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 enumerate and aggregate desktops and applications from Citrix Virtual Apps and Desktops sites and Citrix Virtual Apps farms, making these resources available to users.

1. Install and configure StoreFront. For details, see the StoreFront product documentation. For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for iOS.
2. Configure stores for StoreFront as you would for other Citrix Virtual Apps and Desktops 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) containing 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 Web sites 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 multiple stores that you can manually distribute to your users.
   - Manual configuration. You can directly inform users of the Citrix Gateway or store URLs needed to access their desktops and applications. For connections through Citrix Gateway, users also need to know the product edition and required authentication method. Af-

ter installation, users type these details into Citrix Workspace app for iOS, which attempts to verify the connection and, if successful, prompts users to log on.

- 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 (for example, users who connect from the internet of from remote locations), configure authentication through Citrix Gateway.

- When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition versions from 9.3, and Citrix Gateway versions through 12.

To configure Citrix Workspace app for iOS to access apps

1. If you want to configure Citrix Workspace app for iOS to automatically access apps when creating an account, in the Address field, type the matching URL of your store, such as storefront.organization.com.
2. Select the **Use Smartcard** option when you are using a smart card to authenticate.
3. For manual configuration (accessible by tapping Options>Manual Setup), continue by completing the remaining fields and select the Citrix Gateway authentication method, such as enabling the security token, selecting the type of authentication, and saving the settings.

> **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.

Web Interface

To configure the Web Interface site, users with iPhone and iPad devices can launch applications through your Web Interface site and the built-in Safari browser on the mobile device. Configure the Web Interface site the same as you would for other Citrix Virtual Apps applications. If no XenApp Services 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.

Web Interface 5.x is supported by the built-in Safari browser.

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 Web sites.

> **Important:**
>
> In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not 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 for iOS determines the Access Gateway or

StoreFront server, or AppController virtual appliance associated with the email address 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 is not supported if Citrix Workspace app for iOS is connecting to a Web Interface deployment.

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 Web sites, users can also obtain Citrix Workspace app for iOS provisioning files from those sites.

For more information, see the StoreFront documentation.

Provide users with account information to enter manually

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

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

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

Configuration

September 6, 2019

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 is not available.

To override password saving

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

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

Use the Save Password feature

Citrix Workspace app for iOS 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 everytime you open Citrix Workspace app for iOS.

> **Note:**
>
> The save password functionality currently works with the PNA protocol. It does not work with StoreFront *native* mode; however, this functionality works when StoreFront enables PNA *legacy* mode.

Configure StoreFront PNA legacy mode

To configure StoreFront PNA legacy mode 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, setup, and uninstall Citrix StoreFront.

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 you want to configure.
5. Click **Configure XenApp Service Support**.
6. Enable **Legacy Support**, and Click **OK**.
7. Navigate to the template configuration file located at c:\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\.
8. Make a backup of Config.aspx.
9. Open the original Config.aspx file.
10. Edit the line <EnableSavePassword>**false**</EnableSavePassword> to change the **false** value to **true**.
11. Save the edited Config.aspx file.
12. On the StoreFront server, run PowerShell with administrative rights.
13. In the PowerShell console:

    a. cd "c:\Program Files\Citrix\Receiver StoreFront\Scripts"

    b. Type "Set-ExecutionPolicy RemoteSigned"

    c. Type ".\ImportModules.ps1"

    d. Type "Set-DSServiceMonitorFeature –ServiceUrl" `https://localhost:443/StorefrontMonitor`

14. If you have a StoreFront group, run the same commands on all the members in the group.

Configure Citrix Gateway to save passwords

> **Note:**
>
> This configuration uses Citrix Gateway load balance servers.

To configure Citrix Gateway to support the save password functionality:

1. Log in to the Citrix Gateway management console.
2. Follow the Citrix best practices to create a certificate for your load balance virtual server(s).
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** (this is 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 Group**s 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; a list of monitors (those configured on Citrix Gateway) appears.
15. Click the radio button beside the monitor(s) 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.
18. Select the **Server Based** radio button; a list of server members (those configured on Citrix Gateway) appears. Click the radio button beside the StoreFront server(s) you created earlier.
19. Enter 443 for the port number and specify a unique number for the Hash ID, then click **Create**, then click **Done**. If everything has been configured properly, the **Effective State** should show a green light, indicating that monitoring is functioning properly.
20. Navigate to Traffic Management -> Load Balancing -> Virtual Servers and click **Add**. Enter a name for the server and select **SSL** as the protocol.
21. Enter the IP address for the StoreFront load-balanced server and click **OK**.
22. Select the **Load Balancing Virtual Server Service Group** binding, click the arrow then add the Service Group created previously. Click **OK** twice.
23. Assign the SSL certificate created for the Load Balance virtual server. Select **No Server Certificate**.
24. Select the Load Balance server certificate from the list and click **Bind**.
25. Add the domain certificate to the Load Balance Server. Click **No CA certificate**.

26. Select the domain certificate and click **Bind**.
27. On the right side of the screen, select **Persistence**.
28. Change the Persistence to **SOURCEIP** and set the time out to **20**. Click **Save,** then click **Done**.
29. On your domain DNS server, add the load balance server (if not already created).
30. Launch Citrix Workspace app for iOS on your iOS device and enter the full XenApp URL.

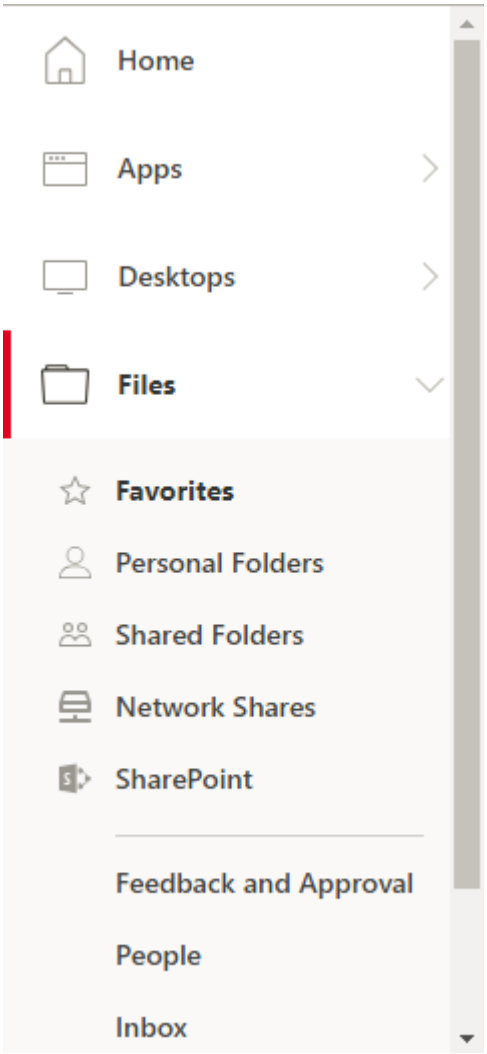
Content Collaboration Service integration

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

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

> **Note:**
>
> Citrix Content Collaboration integration in Citrix Workspace app is not supported on Windows Server 2012 and Windows Server 2016 due to a security option set in the operating system.

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



Limitations

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

Citrix Ready workspace hub

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

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

Configure

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

Known limitation

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

Session sharing

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

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

Authenticate

September 6, 2019

Client certificate authentication

> **Important:**
>
> - When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition Version 9.3 and later, and NetScaler Gateway through Version 11.
> - Client certificate authentication is supported by Citrix Workspace app for iOS.
> - Only Access Gateway Enterprise Edition 9.x and 10.x (and subsequent releases) support client certificate authentication.

> - Double-source authentication types must be CERT and LDAP.
> - Citrix Workspace app for iOS also supports optional client certificate authentication.
> - Only P12 formatted certificates are supported.

Users logging on 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.

To authenticate users based on the client-side certificate attributes, client authentication should be enabled on the virtual server and the client certificate should be requested. You must bind a root certificate to the virtual server on Citrix Gateway.

When users log on to the Citrix Gateway virtual server, after authentication, the user name and domain information is extracted from the specified field of the certificate. This information must be in the certificate's **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** field. It is in the format "username@domain."If the user name and domain are extracted successfully, and the user provides the other required information (for example, a password), then the user is authenticated. 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 Services site

If you do not already have a XenApp Services site created, in the Citrix Virtual Apps console or Web Interface console (depending on the version of Citrix Virtual Apps you have installed), create a XenApp Services site for mobile devices.

Citrix Workspace app for iOS for mobile devices uses a XenApp Services site to get information about the applications a user has rights to and presents them to the app running on the device. This is similar to the way you use the Web Interface for traditional SSL-based Citrix Virtual Apps connections for which a Citrix Gateway can be configured.

Configure the XenApp Services site for Citrix Workspace app for iOS for mobile devices to support connections from a Citrix Gateway connection.

1. In the XenApp Services 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 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 two authentication policies: Cert and LDAP.

1. Create a session policy on Citrix Gateway to allow incoming Citrix Virtual Apps connections from Citrix Workspace app for iOS, and specify the location of your newly created XenApp Services site.

    - Create a session policy to identify that the connection is from Citrix Workspace app for iOS. 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 this is not a global setting (you selected the Override Global check box), ensure that the ICA Proxy field is set to ON.

      In the Web Interface Address field, type the URL including the config.xml for the XenApp Services site that the device users use, such as //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 (on the Certificate tab, open SSL Parameters, and for Client Authentication, set Client Certificate to Mandatory.

    > **Important:**
    >
    > If the server certificate used on Citrix Gateway is part of a certificate chain (with an intermediate certificate), ensure that the intermediate certificates are also installed correctly on Citrix Gateway. For information about installing certificates, see 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 is completed successfully, the user name and domain are extracted from the certificate and any policies specified for that user are applied.

1. From Citrix Workspace app for iOS, open the Account, and in the Server field, type the matching FQDN of your Citrix Gateway server, such as GatewayClientCertificateServer.organization.com. Citrix Workspace app for iOS 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, the certificate must be downloaded and installed by Citrix Workspace app for iOS only.
3. After selecting a valid certificate, the user name and domain fields on the logon screen is pre-populated using the user name information from the certificate, and a user types the remaining 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 for iOS proceeds with the connection and provides the user with the logon screen.
5. After users complete the initial log on, they can start applications without providing the certificate again. Citrix Workspace app for iOS stores the certificate for the account and uses it automatically for future logon requests.

Smart cards

Citrix Workspace app for iOS provides support for SITHS smart cards for in-session connections only.

If you are using FIPS Citrix Gateway devices, configure your systems to deny SSL renegotiations. For details, see How to configure the -denySSLReneg parameter.

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 (4th generation) and Tactivo for iPad (3rd generation) and iPad 2 Firmware version 3.8.0
  - BaiMobile® 301MP and 301MP-L Smart Card Readers
    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

RSA SecurID authentication

RSA SecurID authentication for Citrix Workspace app for iOS is supported for Secure Web Gateway configurations (through the Web Interface only) and 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 for iOS registers the URL scheme com.citrix.securid only.

If users have installed both the Citrix Workspace app for iOS 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 for iOS on their devices.

To import an RSA SecurID soft token

To use an RSA Soft Token with the Citrix Workspace app for iOS, have your users follow this procedure.

The policy for PIN length, type of PIN (numeric only, alphanumeric), and limits on PIN reuse are specified on the RSA administration server.

Your users should only need to do this once, after they have successfully authenticated to the RSA server. After your users verify their PINs, they are are also authenticated with the StoreFront server, and it presents 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 for iOS 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 will see a message that the token was successfully imported.
4. Close the import message, and in Citrix Workspace app for iOS, click the **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 may have changed it to comply with their security policies.)
7. At the top left, click **Log On**. After you click **Log On**, you are prompted to create a new PIN.
8. Enter a PIN from 4 to 8 digits and click **OK**.

9. You are then prompted to verify your new PIN. Re-enter your PIN and click **OK**. After clicking OK, you will be able to access your apps and desktops.

Next Token Code

If you configure Citrix Gateway for RSA SecurID authentication, Citrix Workspace app for iOS supports Next Token Code. With this feature enabled, if a user enters three (by default) incorrect passwords, the Citrix Gateway plug-in prompts the user to wait until the next token is active before logging on. 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 for iOS is available. When connecting to a Store that allows derived credentials, users can log on to Citrix Workspace app for iOS using a virtual smart card. This feature is supported only on on-premises deployments.

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

To enable derived credentials in Citrix Workspace app for iOS:

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

Then, 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 desired authentication certificate from the list.
9. Tap **Import Key**.
10. Repeat steps 5–9 for the Digital Signature Certificate and the Encryption Certificate, if desired.
11. Tap **Save**.

You can import up to three 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 inside of a VDA session.

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

Known limitations

- Users can only have one active card at a time.
- Once a virtual smart card is created, it cannot be edited. To make changes to the virtual smart card, users must delete the card and create a new card.
- A PIN can be invalid up to 10 times. After the tenth attempt, the virtual smart card gets deleted.
- When derived credentials are selected, the virtual smart card that was created earlier overrides a physical smart card when a smart card is needed in a session.

Secure

September 6, 2019

To secure the communication between your server farm and Citrix Workspace app for iOS, you can 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 for iOS and servers. Citrix Workspace app for iOS supports SOCKS and secure proxy protocols.
- Secure Web Gateway. You can use Secure Web Gateway with Web Interface to provide a single, secure, encrypted point of access through the Internet to servers on internal corporate networks.
- SSL Relay solutions with Transport Layer Security (TLS) protocols.
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Citrix Workspace app for iOS 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 for iOS.

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 for iOS and the server. No configuration of Citrix Workspace app for iOS is required if you are using the Secure Web Gateway in Normal mode and users are connecting through the Web Interface.

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

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

- The fully qualified domain name (FQDN) of the Secure Web Gateway server.
- The port number of the Secure Web Gateway server. Note that Relay mode is not supported by Secure Web Gateway Version 2.0.

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

- Host name
- Intermediate domain
- Top-level domain

For example, my_computer.example.com is a 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 generally 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 for iOS and servers. Citrix Workspace app for iOS supports both SOCKS and

secure proxy protocols.

When communicating with the Citrix Virtual Apps and Desktops server, Citrix Workspace app for iOS uses proxy server settings that are configured remotely on the Web Interface server.

When communicating with the Web server, Citrix Workspace app for iOS uses the proxy server settings that are configured for the default web browser on the user device. You must configure the proxy server settings for the default web browser on the user device accordingly.

Firewall

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

If the firewall is configured for Network Address Translation (NAT), you can use Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your Citrix Virtual Apps and Desktops server is not 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 for iOS supports TLS 1.0, 1.1 and 1.2 with the following cipher suites for TLS connections to XenApp/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 for iOS running on iOS 9 and later 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 may also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

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

Note:

Citrix Workspace app for iOS uses platform (iOS) crypto for connections between Citrix Workspace app for iOS 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 use TLS to secure communications between TLS-enabled Citrix Workspace app for iOS and Citrix Virtual Apps and Desktops, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate.

iOS comes with about 100 commercial root certificates preinstalled, but if you want to use a different certificate, you can obtain one from the Certificate Authority and install it on each user device.

Depending on your organization's policies and procedures, you may want to 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 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 and can be used by TLS-enabled clients and by any other application using TLS.

XenApp Services site

To configure the XenApp Services site:

> **Important:**
>
> - Citrix Secure Gateway 3.x is supported by Citrix Workspace app for iOS using XenApp Services sites.
> - Citrix Secure Gateway 3.x is supported by Citrix Workspace app for iOS using Citrix Virtual Apps Web sites.
> - Only single-factor authentication is supported on XenApp Services sites, and both single-factor and dual factor are supported on Citrix Virtual Apps Web sites.
> - You must use Web Interface 5.4, which is supported by all built-in browsers.

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

If you are using a Citrix Secure Gateway connection, do not configure Citrix Gateway settings on Citrix Workspace app for iOS.

Citrix Workspace app for iOS uses a XenApp Services site to get information about the applications a user has rights to and presents them to Citrix Workspace app for iOS running on the device. This is similar to the way you use the Web Interface for traditional SSL-based Citrix Virtual Apps connections for which a Citrix Gateway can be configured. XenApp Services sites running on the Web Interface 5.x have this configuration ability built in.

Configure the XenApp Services site to support connections from a Citrix Secure Gateway connection:

1. In the XenApp Services 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 for this site (//XenAppServerName/Citrix/PNAgent). The default path enables your users to specify the FQDN of the Secure Web Gateway they are connecting to instead of the full path to the config.xml file that resides on the XenApp Services site (such as //XenAppServerName/CustomPath/config.xml).

To configure the Citrix Secure Gateway

1. On the Citrix Secure Gateway, use the Citrix Secure Gateway Configuration wizard to configure the Citrix Secure Gateway to work with the server in the secure network hosting the XenApp Service site. After selecting the Indirect option, enter the FQDN path of your Secure Web Gateway Server and continue the wizard steps.
2. Test a connection from a user device to verify that the Secure Web Gateway is configured correctly for networking and certificate allocation.

To configure the mobile device

1. When adding a Citrix Secure Gateway account, enter the matching FQDN of your Citrix Secure Gateway server in the **Address** field:
   - If you created the XenApp Services site using the default path (/Citrix/PNAgent), enter the Secure Web Gateway FQDN: FQDNofSecureGateway.companyName.com
   - If you customized the path of the XenApp Services site, enter the full path of the config.xml file, such as: FQDNofSecureGateway.companyName.com/CustomPath/config.xml
2. If you are manually configuring the account, then turn off the Citrix Gateway option **New Account** dialog.

Troubleshoot

September 6, 2019

App switcher not working

Apps must be published by the IT administrator on the same server. Otherwise, app switching will not work.

Applications open in different sessions

This server-side issue can occur even when application sharing is enabled. This is an intermittent issue, and there is no workaround.

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 expose 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 remains in a disconnected state. Although the user can reconnect at a later time, you can ensure disconnected sessions are rendered inactive after a specific interval. To do this, 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 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 onto 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 cannot 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 onto 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, HDX audio to Citrix Workspace app for iOS might lose quality when using audio plus video. This issue occurs when the Citrix Virtual Apps and Desktops HDX policies cannot 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.

Demo accounts available from Citrix Cloud

Users who do not currently have an account can create a demo user account at the Citrix Cloud demo site at http://cloud.citrix.com/.

Citrix Cloud offers users the ability to experience the power of Citrix solutions without having to set up and configure their own environment. Citrix Cloud demo environment uses a number of key Citrix solutions including Citrix Virtual Apps and Desktops and Citrix Gateway.

However, in this demo environment, data is not saved, and when you disconnect, you might not get able to get back to your session.

Numeric keys

If users have issues with numeric keys not working correctly in published applications, they can try disabling the Unicode keyboard in Citrix Workspace app for iOS. To do this, from the Settings tab, tap **Keyboard Options**, and for Use Unicode Keyboard, toggle the switch to **Off**.

Slow connections

If you experience slow connections to the XenApp Services site, or issues such as missing application icons or “Protocol Driver Error” messages, as a workaround, on the Citrix Virtual Apps server and Citrix Secure Web Gateway or Web Interface server, disable the following Citrix PV Ethernet Adapter Properties for the network interface (all enabled by default):

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

No server restart is needed. This workaround applies to Windows Server 2003 and 2008 32-bit. Windows Server 2008 R2 is not affected by this issue.

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