



# Citrix Workspace app for Android

## Contents

<b>About this release</b>	<b>3</b>
<b>Prerequisites for installing</b>	<b>7</b>
<b>Install</b>	<b>13</b>
<b>Get started</b>	<b>14</b>
<b>Configure</b>	<b>18</b>
<b>Authenticate</b>	<b>24</b>
<b>SDK and API</b>	<b>25</b>

## About this release

June 17, 2019

### What's new

#### What's new in 1906

##### Supported API version

Chrome OS supports only Android API Version 21 and later.

Additionally, this release addresses issues that help to improve overall performance and stability.

#### What's new in 1905

Version 2.8 of the Citrix HDX RTME is embedded with the Citrix Workspace app 1905 and later for Android. For more information, see the [HDX RealTime Optimization Pack 2.8](#) documentation.

#### What's new in 1904.1

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

#### What's new in 1904

##### Embedded Citrix HDX RealTime Media Engine

In earlier releases, the Citrix HDX RealTime Media Engine (RTME) was installed separately using an apk from Google Play.

With this release, the Citrix HDX RTME is embedded with the Citrix Workspace app installer.

This feature is supported on:

- Chromebooks running on x86 processors.
- Devices running on Android 6.0 or later.

For more information, see the [HDX RealTime Media Engine](#) documentation.

#### What's new in 1903.1

This release addresses a number of issues that help to improve overall performance and stability. For more information, see [Fixed issues](#).

### **What's new in 1903**

This release addresses a number of issues that help to improve overall performance and stability. For more information, see [Fixed issues](#).

### **What's new in 1902.1**

This release addresses a number of issues that help to improve overall performance and stability. For more information, see [Fixed issues](#).

### **What's new in 1902**

#### **Support for unauthenticated users**

With this release, Citrix Workspace app supports unauthenticated (anonymous) users. Anonymous users can now launch Citrix Virtual Apps and Desktops sessions successfully.

### **What's new in 1901**

This release addresses a number of issues that help to improve overall performance and stability. For more information, see [Fixed issues](#).

## **Fixed issues**

### **Fixed issues in 1906**

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

### **Fixed issues in earlier releases**

#### **Fixed issues in 1905:**

- This fix restricts the number of characters that you can use to set the client name to 15. This restriction allows for permanent device CAL licenses to be assigned by the license server. [LD0409]
- The store fails to load when you switch from WiFi to mobile data or vice versa. [RFANDROID-3780]
- When your mobile device is set to the Turkish language, no apps are listed on the Apps tab. [RFANDROID-3852]

#### **Fixed issues in 1904:**

- Starting a session after waking a device docked on Samsung DeX can cause Citrix Workspace app for Android to become unresponsive and the following error message appears:

“Cannot Connect to Server.”

[RFANDROID-2607]

- When switching between apps, Citrix Workspace app for Android might become unresponsive when returning to the app. [RFANDROID-2906]
- The menu icon does not work when the app is resized to a lower resolution. [RFANDROID-3110]
- Unable to copy a large file between the mapped client drive and the session. [RFANDROID-3785]

#### **Fixed issues in 1903.1:**

- A toast notification does not appear at logoff. [RFANDROID-3082]
- In a Citrix Cloud setup, the **Try again** dialog appears continuously and does not work even when the user confirms the action. [RFANDROID-3108]
- On a mobile device, when you are accessing applications other than Citrix Workspace app, the following message appears randomly.

“Cannot connect to Server, Try Again.”

[RFANDROID-3172]

#### **Fixed issues in 1903:**

- When you run an HDX session on a Samsung DeX device, a blue screen appears. [RFANDROID-2913]
- HDX sessions running on Android 9 devices might appear corrupted when you set the color depth to either **8-bit** or **16-bit** in Citrix Studio. [RFANDROID-2914]
- When you try to change the password, the previously logged in username appears instead of the currently logged in username. [RFANDROID-3042]
- When you move an extended session to the background, the session continues to be displayed on the external monitor. [RFANDROID-3122]

#### **Fixed issues in 1902.1:**

- When you launch a session with EDT enabled, a black screen appears. [LD0739]
- When you change the options for the Extended Keyboard settings, the selection might not be reflected in your session. [RFANDROID-2387]
- When you undock an Android device from Samsung DeX in an active session, the Num Lock keys are not synchronized. [RFANDROID-2875]

#### **Fixed issues in 1902:**

- On an Android 7 device with a physical keyboard attached, the soft keyboard does not appear when you tap the **Keyboard** option in the session toolbar. [RFANDROID-1442]

- In a multi-store StoreFront setup, the **Add Account** dialog displays stores that were added previously. [RFANDROID-1903]
- When you try to add a Citrix Cloud account, the **Authentication** dialog does not appear long enough to enter the details. [RFANDROID-2884]
- When you try to switch between apps in a session, the following error message appears:  
“Cannot connect to the Server. Try Again”.  
When you tap **Try Again**, the connection is restored. [RFANDROID-2910]

### Fixed issues in 1901:

- When you tap the **Details** option of an app that has a long name (for example, 64 characters), the app name appears as spilt over and the ellipsis does not appear. [RFANDROID-1894]
- The username is not autopopulated when you access the Citrix Secure Hub app using the Citrix Workspace app. [RFANDROID-2885]
- When you tap **Refresh**, the install status of the app is not updated and is displayed incorrectly. [RFANDROID-2886]

### Known issues

#### Known issues in 1906

No new issues have been observed in this release.

#### Known issues in earlier releases

##### Known issues in 1904.1:

- The following error message appears when attempting to import the RSA soft token.  
“Unknown Error”  
[LD1085]

##### Known issues in 1904:

- Citrix Workspace app does not support Citrix Cloud store configuration on devices running on Android 5 or earlier. Upgrade to Version 5.1 or later. [RFANDROID-3804]

##### Known issues in 1903.1:

- Citrix Workspace app for Android does not support the custom EDT MSS stack parameter. [LD1096]

### **Known issues in 1903:**

No new issues have been observed in this release.

### **Known issues in 1902.1:**

- In a session running on Samsung DeX, apps do not extend to full screen when maximized. [RFANDROID-3105]

### **Known issues in 1902:**

No new issues have been observed in this release.

### **Known issues in 1808:**

- When you are running the Citrix Workspace app for Android on a Chrome OS, the screen resolution on the VDA is different than what is set on the client. A gray bar is noticed too. [RFANDROID-2478]
- Users who upgrade to Citrix Workspace app and connect to a branded Workspace store do not see any resources. As a workaround, log off and back in to Citrix Workspace app. [RFANDROID-2505]

## **Third party notices**

Citrix products often include third party code licensed to Citrix for use and redistribution under an open source license. In an effort to better inform its customers, Citrix publicizes open source code included within Citrix products in an open source licensed code list.

For information about Open Source Licensed Code, see [Open Source Licensed Code](#).

## **Prerequisites for installing**

June 17, 2019

## **System requirements and compatibility**

### **Device requirements**

Citrix Workspace app for Android supports Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat), 8.x (Oreo), and 9.x (Pie).

For best results, update Android devices to the latest Android software.

Citrix Workspace app for Android 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 Android directly.

**Important:**

If a Tech Preview version of Citrix Workspace app for Android is installed, uninstall it before installing the new version.

**Server requirements**

StoreFront:

- StoreFront 2.6 or later

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

- StoreFront configured with a Workspace for Web site

Provides access to StoreFront stores from a web browser. For the limitations of this deployment, see the StoreFront documentation.

Web Interface (not supported for Citrix Virtual Apps and Desktops 7 and later deployments):

- Web Interface 5.4 with Web Interface sites
- Web Interface 5.4 with XenApp Services sites

Web Interface on Citrix Gateway:

You must enable the rewrite policies provided by Citrix Gateway.

Citrix Virtual Apps and Desktops (any of the following products):

- Citrix Virtual Apps 7.5 or later
- XenApp 6.5 for Windows Server 2008 R2
- Citrix Virtual Apps and Desktops 7.x or later

**Connections, certificates, and authentication**

Citrix Workspace app for Android supports HTTP, HTTPS, and ICA-over-TLS connections to a Citrix Virtual Apps server through any one of the following configurations.

For LAN connections:

- StoreFront 2.6 or later
- Web Interface 5.4
- XenApp Services (formerly Program Neighborhood Agent) site.



For secure remote connections (any of the following products):

- Citrix Gateway 11 and later (including VPX, MPX, and SDX versions)
- XenMobile is supported only with versions 9 and 10.

### **TLS Certificates**

When securing remote connections using TLS, the mobile device verifies the authenticity of the remote gateway's TLS certificate against a local store of trusted root certificate authorities. The device automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

### **Private (Self-signed) Certificates**

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

**Note:**

When 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 selects to continue through the warning, a list of applications is displayed; however, application fails to launch.

### **Wildcard Certificates**

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

### **Intermediate Certificates and Citrix Gateway**

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway server certificate. See the Knowledge Center article that matches your edition of the Citrix Gateway:

[CTX114146](#) and [CTX124937](#)

### **Joint Server Certificate Validation Policy**

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

### **Important:**

Before installing this version of Citrix Workspace app for Android, confirm that the certificates at the server or Citrix Gateway are correctly configured as described here. Connections might fail if:

- the server or Citrix Gateway configuration includes a wrong root certificate.
- the server or Citrix Gateway configuration does not include all intermediate certificates.
- the server or Citrix Gateway configuration includes an expired or otherwise invalid intermediate certificate.
- the server or Citrix Gateway configuration includes a cross-signed intermediate certificate.

When validating a server certificate, Citrix Workspace app for Android uses **all** the certificates supplied by the server (or Citrix Gateway) when validating the server certificate. It 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 Citrix Gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app for Android connection to fail.

Suppose that a Citrix 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 Android:

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

Then, Citrix Workspace app for Android checks that all these certificates are valid. Citrix Workspace app for Android also checks that it already trusts “Example Root Certificate”. If Citrix Workspace app for Android 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 Android 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.

**Note:**

Some servers and Citrix Gateway never send the root certificate, even if configured. Stricter validation is then not possible.

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

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

Then, Citrix Workspace app for Android uses 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. This configuration supplies the intermediate certificate that Citrix Workspace app for Android needs, but also allows Citrix Workspace app for Android to choose any valid, trusted, root certificate.

Now suppose that a Citrix Gateway is configured by using these certificates:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Wrong Root Certificate”

Citrix Workspace app for Android reads the wrong root certificate, and the connection fails.

Some certificate authorities use more than one intermediate certificate. In this case, the Citrix 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”

Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and an 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.

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 as “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 Citrix Gateway to use the cross-signed intermediate certificate, because it selects the earlier root certificate:

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

It is not recommended to configure the Citrix Gateway by using only the server certificate:

- “Example Server Certificate”

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

### Authentication

**Note:**

RSA SecurID authentication is not supported for Citrix Secure Web Gateway configurations. To use RSA SecurID, use Citrix Gateway.

Citrix Workspace app for Android supports authentication through Citrix Gateway using the following methods, depending on your edition:

- No authentication (Standard and Enterprise versions only)
- Domain authentication
- RSA SecurID, including software tokens for Wi-Fi and non-Wi-Fi devices
- Domain authentication paired with RSA SecurID
- SMS Passcode (one-time PIN) authentication
- Smartcard authentication

**Note:**

Smart card authentication on Web Interface sites is not supported.

Citrix Workspace app for Android now supports the following products and configurations.

Supported smart card readers:

- BaiMobile 3000MP USB Smart Card Reader

Supported smart cards:

- PIV cards
- Common Access Cards

Supported configurations:

- Smart card authentication to Citrix Gateway with StoreFront 2 or 3 and Citrix Virtual Apps and Desktops 7.x and later or XenApp 6.5 and later
- Smart card authentication to Citrix Gateway with Web Interface 5.4.2 and Citrix Virtual Apps and Desktops 7.x and later or XenApp 6.5 or later

**Note:**

Other token-based authentication solutions can be configured using RADIUS. For SafeWord token authentication, see [Configuring SafeWord Authentication](#).

## Install

June 17, 2019

### HDX RealTime Media Engine

Citrix HDX RTME plug-in is embedded with the Citrix Workspace app installer.

The HDX RealTime Media Engine (RTME) is a plug-in to the Citrix Workspace app for Android to support clear, crisp high-definition audio-video calls. You can seamlessly participate in audio-video or audio-only calls to and from HDX RealTime Media Engine users.

HDX RTME integrates Citrix Workspace app on the endpoint device and performs media processing directly on the user device, offloading the server for maximum scalability, minimizing network bandwidth consumption and ensuring optimal audio-video quality.

**Note:**

- HDX RTME for Citrix Workspace app for Android is supported only on Chromebooks with Intel Core Processor.
- You must uninstall the existing version of HDX RTME to install the latest version available with the Citrix Workspace app.

To enable the HDX RTME from Citrix Workspace app, go to **Settings > Advanced** and select **Enable RealTime Media Engine**.

By default, this setting is set to **Off**.

Citrix Workspace app for Android does not support the following HDX RTME features:

- Camera encoding USB Video Class (UVC) 1.1.
- Device enumeration and switching from Skype for Business settings. Only default devices are used.
- G722.1C, RTAudio, and RTVideo codecs.

- Human interface devices, auto gain control, and Call Admission Control.
- In **Fallback** mode, webcam and audio devices are not available because of limitations in Citrix Workspace app for Android.

For more information about HDX RealTime Media Engine, see [HDX RealTime Optimization Pack](#) documentation.

### Installing Citrix Workspace app on an SD card

Citrix Workspace app for Android is optimized for local installation on user devices. However, if devices have insufficient storage, users can install Citrix Workspace app for Android on an external SD card and mount it on the device to launch published apps on their mobile devices. This support is provided by default and no additional configuration is required.

To launch an app using the SD card, select the app from the list of Citrix Workspace app on the user device, and then select Move to SD card.

If users opt to install Citrix Workspace app for Android on an external SD card to launch apps, the following issues exist:

- Mounting a USB storage device while the SD card is mounted on the mobile device causes the SD card to become unavailable, and if apps were running, they stop running when the USB device is mounted.
- Some AppWidgets (such as the home screen widgets) are not available when an app is running from the SD card. After unmounting the SD card, users must restart the AppWidgets.

If users install Citrix Workspace app for Android locally on their user devices, they can move Citrix Workspace app for Android to the SD card when needed.

## Get started

June 17, 2019

When creating a new account, in the **Address** field, enter the matching URL of your store, such as storefront.organization.com.

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.

When adding an account using an automatic configuration you can enter the FQDN of a StoreFront server or Citrix Gateway, or you can alternatively use an email address to create a new account. You are then prompted to enter the user credentials before logging on.

For more information about configuring access to StoreFront through Citrix Gateway, see:

[Configure and manage stores](#)

[Integrating StoreFront with Citrix Gateway](#)

## **Email-based account discovery**

You can configure Citrix Workspace app to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Workspace app for Android installation and configuration. Citrix Workspace app for Android determines the Citrix Gateway or StoreFront server 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 is connected to a Web Interface deployment.

## **Provision 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 Android automatically. After installing Citrix Workspace app for Android, users simply open the .cr file on the device to configure Citrix Workspace app for Android. If you configure Workspace for Web sites, users can also obtain Citrix Workspace app for Android provisioning files from those sites.

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

## **Provide users with account information to enter manually**

If you are 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: server-name.company.com.
- To access using Citrix Gateway, provide the Citrix Gateway address and required authentication method.

See the [Citrix Gateway](#) documentation for more information.

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

## **Provide access to Citrix Virtual Apps and Desktops**

Citrix Workspace app requires configuration of either Web Interface or StoreFront to deliver apps, desktops and files from your Citrix Virtual Apps and Desktops deployment.

### **Web Interface**

There are two types of Web Interface sites: XenApp Services (formerly Program Neighborhood Services) sites and XenApp websites. Web Interface sites enable user devices to connect to the server.

### **StoreFront**

You can configure StoreFront to provide authentication and resource delivery services for Citrix Workspace app, enabling you to create centralized enterprise stores to deliver desktops and applications through Citrix Virtual Apps and Desktops, and Worx Mobile Apps and mobile apps you have prepared for your organization through XenMobile.

Authentication between Citrix Workspace app and a Web Interface site or a StoreFront store can be handled using a variety of solutions:

- Users inside your firewall can connect directly to Web Interface or StoreFront.
- Users outside your firewall can connect to StoreFront or the Web Interface through Citrix Gateway.
- Users outside your firewall can connect through Citrix Gateway to StoreFront.

### **Connect through Citrix Gateway**

Citrix Gateway 11 and later are supported by Citrix Workspace app for Android for access to:

- Web Interface 5.4 XenApp Services Sites and XenApp Web Sites
- StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 and 3.11 stores

You can create multiple session policies on the same virtual server depending on the type of connection (such as ICA, CVPN, or VPN) and type of Workspace deployment (Workspace for Web or locally installed Citrix Workspace app). All of the policies can be achieved from a single virtual server.

When users create accounts on Citrix Workspace app, they should enter the account credentials, such as their email address or the matching FQDN of your Citrix Gateway server. For example, if the connection fails when using the default path, users should enter the full path to the Citrix Gateway server.



## Citrix Endpoint Management

To enable remote users to connect through Citrix Gateway to your XenMobile deployment, you can configure Citrix Gateway to work with [AppController](#) or StoreFront (both components of XenMobile). The method for enabling access depends on the edition of XenMobile in your deployment:

Enabling access to XenMobile 9:

### [Client Certificate Authentication](#)

Enabling access to XenMobile 10:

### [Citrix Gateway and Citrix Endpoint Management](#)

If you deploy XenMobile in your network, allow connections from remote users to [AppController](#) by integrating XenMobile and [AppController](#). This deployment allows users to connect to [AppController](#) to obtain their web, Software as a Service (SaaS), and mobile apps, and access documents from ShareFile. Users connect through either Citrix Workspace app or the Citrix Gateway Plug-in.

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

To deploy windows and custom apps to your users, you must wrap the apps by using the MDX Toolkit. You can find more information here:

### [MDX Toolkit](#)

## Connecting to StoreFront

Citrix Workspace app for Android supports launching sessions from Workspace for Web, provided that the web browser works with Workspace for Web. If launches do not occur, configure your account through Citrix Workspace app for Android directly.

### Tip

When Workspace for Web is used from a browser, sessions are not launched automatically when downloading an .ICA file. The .ICA file must be opened manually shortly after its downloaded for the session to be launched.

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Workspace app. Create stores that enumerate and aggregate desktops and applications from XenDesktop sites and XenApp, making these resources available to users.

For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for Android.

Configure stores for StoreFront just as you would Citrix Virtual Apps and Desktops . No special configuration is needed for mobile devices. 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 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. After installation, users enter these details into Citrix Workspace app, which attempts to verify the connection and, if successful, prompts users to log on.

### **Connecting to Web Interface**

Citrix Workspace app can launch applications through your Web Interface site. Configure the Web Interface site just as you would for other Citrix Virtual Apps and Desktops apps and desktops. No special configuration is needed for mobile devices.

Citrix Workspace app supports Web Interface version 5.4 only. In addition, users can launch applications from Web Interface 5.4 using the Firefox mobile browser.

#### **To launch applications on the Android device:**

From the device, users log into the Web Interface site using their normal logon and password.

For more information about configuring Web Interface sites see, [Configuring Web Interface](#).

## **Configure**

June 17, 2019

### **Citrix Casting**

Citrix Casting 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.

Using Citrix Casting, you can:

- Roam your session without launching a VDA session on the mobile devices.
- View the list of available workspace hubs by tapping **View hub list** from the **Workspace hub** dialog.

### Configure Citrix Casting

Citrix Casting is enabled on Citrix Workspace app when all the following system requirements are met:

- Citrix Workspace app 1809 for Android or later installed
- Bluetooth enabled
- Location enabled
- Mobile device and workspace hub using the same Wi-Fi network

To turn on the Citrix Casting feature, tap **Settings** and **Citrix Casting** on your device.

### Known Limitation

- Web Interface does not support session roaming. Therefore, do not select the **Add account type as Web Interface** option.

For more information about Citrix Ready workspace hub in Citrix Workspace app for Android, see [Configure Citrix Ready workspace hub](#).

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

### Content Collaboration Service integration

This release introduces integration of Citrix Content Collaboration Service with Citrix Workspace app. 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.

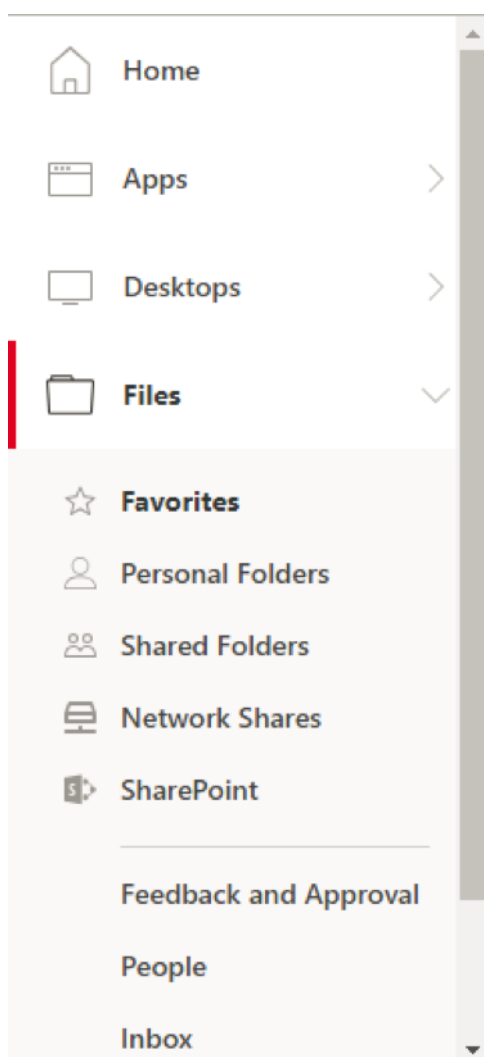
**Note:**

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.

**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.

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



**Keyboard layout synchronization**

Citrix Workspace app for Android offers separate options to enable the client IME and keyboard layout synchronization under **Settings**.

The **Enable client IME** option allows you to type the double-byte characters (such as Chinese, Japanese, and Korean characters) directly at the insertion point in a session.

The **Sync Keyboard** option allows automatic keyboard layout synchronization between the VDA and the client device.

On a fresh install and by default, the **Enable client IME** option is set to **On** for Japanese, Chinese, and Korean languages and the **Sync Keyboard** option is set to **Off**.

To enable dynamic keyboard layout synchronization, set both the **Enable client IME** and **Sync Keyboard** options to **On**.

Notes:

- The VDA must be version 7.16 or later.
- Administrators must enable the enhanced support for Asian languages feature on the VDA. By default, the feature is enabled. However, on Windows Server 2016 VDA, you must add a new key called **DisableKeyboardSync** and set the value to 0 in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme` to enable the feature.
- Administrators must enable the unicode keyboard layout mapping feature on the VDA. By default, the feature is disabled. To enable it, create the **CtxKlMap** key under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` and set DWORD value `EnableKlMap = 1` under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap`.

Limitations:

- This feature works only on soft keyboards on the devices, not on external keyboards.
- Certain mobile devices might not fully support keyboard layout synchronization, such as the Nexus 5x
- The keyboard layout can only be synced from the client to the server. When changing the server-side keyboard layout, the client keyboard layout cannot be changed.
- When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality cannot be confirmed.
- Remote applications that run with elevated privileges (for example, applications you run as an administrator) can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.

## USB smart card

Citrix Workspace app provides support for USB smart card readers with StoreFront, Web Interface-based site, or a PNA site. You can use USB smart cards for the following purposes when enabled:

- Smart card logon - Authenticates users to Citrix Workspace app.
- Smart card application support - Enables smart card-aware published applications to access local smart card devices.

Citrix Workspace app supports this feature on all Android devices listed by [Biometric Associates](#).

Citrix Workspace app supports the following types of USB smart cards:

- Personal Identity Verification (PIV) cards
- Common Access Cards (CAC) cards

USB smart card is supported on Android operating system 6.0(Marshmallow) to Version 7.12(Nougat). Android operating system Version 8.0(Oreo) and 9.0(Pie) are not supported. This is a third-party limitation.

You can also enable USB smart card authentication from **Settings > Manage Accounts**.

### Configuring USB smart card

#### Prerequisite:

- Download and install the Android PC/SC-Lite service from the Google Play Store.
1. Connect the USB smart card reader to the mobile device. For information about connecting smart card readers, refer to the smart card reader specifications provided by the manufacturer.
  2. Add a smart card enabled StoreFront account.
  3. On the Citrix Workspace app logon page, tap **Add Account**. Tap the **Use Smartcard** option.
  4. To edit an existing account to use the USB smart card authentication, tap **Accounts > Edit** and tap the **Use Smartcard** option.

### File type association

As a prerequisite for this feature to work, go to the Citrix Workspace app settings and set the **Use device storage** option to **Full Access**. An additional option, **Ask every time** is also available so that you are prompted for permission before accessing your device storage in a session.

#### Note:

**Ask every time** option is a per-session setting. It does not carry forward to the next session.

When you select **Ask every time**, any system-generated access to your device storage might cause the **Use device storage** prompt to appear (for example, at logoff). This is expected behavior.

Citrix Workspace app reads and applies the settings configured by administrators in Citrix Studio.

To apply FTA in a session, ensure that users connect to the Store server where the FTA is configured.

On the user device, select the file you want to launch File Explorer and click Open. The Android operating system provides an option to launch the file using Citrix Workspace app (applying the FTA

configured by the administrator) or a different application. Depending on your earlier selection, a default application might or might not be set. You can change the default application using the Change default option.

**Note:**

This feature is available only on StoreFront and requires Citrix Virtual Apps and Desktops Version 7 or later.

### File type association (FTA) with Google Drive

When using a Chromebook, you can access files residing on Google Drive from Citrix Workspace app using the file type association (FTA) feature. You can seamlessly use Android applications available on Chromebooks to access these files. For example, if you save a .doc file to Google Drive, you can open the file using an Android application (in this case, Microsoft Word) on the Chromebook from within Citrix Workspace app.

**Note:**

Only Chromebook devices support FTA with Google Drive.

### Enabling access to files on Google Drive:

1. Download the Citrix File Access component (FileAccess.exe) from the [Citrix Workspace app for Chrome download page](#) and install it on the VDA.
2. Using Citrix Studio, configure the appropriate file type associations (FTAs) for published applications. FTAs can be configured from the respective application properties or settings. For more information about how to set FTA, see Knowledge Center article [CTX218743](#).
3. In a Citrix Virtual Apps and Desktops session, open the default browser, add the following URL to the trusted sites: <https://accounts.google.com> and <https://ssl.gstatic.com>.
4. On the Chromebook device, select the file you want to launch. Tap **Open** and select Citrix Workspace app from the list.

### Known issues and limitations

1. Smart card authentication might be slower than password authentication. For example, after disconnecting from a session, wait for approximately 30 seconds before attempting to reconnect. Reconnecting to a disconnected session too quickly might cause Citrix Workspace app to turn unresponsive.
2. Smart card authentication is not supported on XenApp Services Sites.
3. Some users might have a global PIN number for smart cards; however, when users log on using a smart card account, they must enter the PIV PIN and not the global smart card PIN. This is a third-party limitation.

4. Citrix recommends that you exit and restart the Citrix Workspace app session after you log off from the smart card account.
5. Multiple USB smart cards are not supported.
6. You can access only MIME file formats supported by Microsoft Office, Adobe Acrobat reader and Notepad applications using the file type association feature.

## Authenticate

June 17, 2019

### RSA SecurID

If you configure the Citrix Gateway for RSA SecurID authentication, the Citrix Workspace app for Android supports Next Token Mode. 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.

For more information, see [Authentication and Authorization](#) section in the Citrix Gateway documentation.

**Tip:**

RSA SecurID authentication is not supported on Citrix Secure Web Gateway configurations. To use RSA SecurID, use Citrix Gateway.

### Installing RSA SecurID Software Tokens

An RSA SecurID Software Authenticator file has an .sdtid file extension. Use the RSA SecurID Software Token Converter to convert the .sdtid file to an XML-format 81-digit numeric string. Obtain the latest software and information from the RSA Web site.

Follow these general steps:

1. On a computer (not a mobile device), download the converter tool [here](#). Follow the instructions on the web site and in the readme included with the converter tool.
2. Paste the converted numeric string into an email and send it to user devices.
3. On the mobile device, make sure that the date and time are correct, which is required for authentication to occur.
4. On the device, open the email and click the string to start the software token import process.



After the software token is installed on the device, a new option appears in the Settings list to manage the token.

**Note:**

On mobile devices that do not associate the .sdtid file with Citrix Workspace app for Android, change the file extension to .xml and import it.

### 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.

- If you enable password saving, Citrix Workspace app 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 prompts users to enter passwords every time they connect.

**Note:**

You cannot store the password on StoreFront direct connections.

### To override saved passwords

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.

## SDK and API

June 17, 2019

## Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) provides support for writing server-side applications and client-side drivers for additional virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers. This version of the SDK provides support for writing new virtual channels for Citrix Workspace app for Android. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Android Virtual Driver AIDL Interfaces: **IVCService.aidl** and **IVCCallback.aidl**, used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels.
- A helper class **Marshall.java** designed to make writing your own virtual channels easier.
- Working source code for three virtual channel sample programs that demonstrate programming techniques.

The Virtual Channel SDK requires the WFAPI SDK to write the server-side of the virtual channel. For more information on SDK, see [Citrix Virtual Channel SDK for Citrix Workspace app for Android](#).



**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

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, 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).