Citrix Workspace app for Android

Contents

About this release

July 14, 2020

What's new in 20.7.0

User interface enhancement

Starting with this release, you can now remove the store account details from the **Edit** option. Click **Remove account** to remove the account details.

What's new in 20.6.5

Update to cyrptography

This feature is an important change to the secure communication protocol. Cipher suites with the prefix TLS_RSA_ doesn't offer forward secrecy and are considered weak.

In this release, the `TLS_RSA_` cipher suites have been removed. This release supports advanced `TLS_ECDHE_RSA_` cipher suites. If your environment isn't configured with the `TLS_ECDHE_RSA_` cipher suites, you cannot luanch the client because of weak ciphers.

The following advanced cipher suites are supported:

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

TLS v1.0 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS v1.2 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

What's new in 20.6.0

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

What's new in 20.5.0

Option to disable display of error messages

You can now disable the display of the following error message related to network monitoring:

"Connection might be temporarily slow."

Go to **Advanced** and select **Disable network monitoroting messages** option to disable the error message relating to network issues in a session

What's new in 20.4.5

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

What's new in 20.4.0

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

What's new in 20.3.0

Starting with 20.3.0, the Citrix Workspace app consumes Version 2.9 of the Citrix HDX RealTime Media Engine (RTME).

> **NOTE:**
>
> You do not need to install HDX RTME to use Skype for Business, you only need the Citrix Workspace app. If HDX RTME is already installed on the Chromebook device, you must uninstall it.

To enable HDX RTME from the Citrix Workspace app:

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

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

For more information, see the HDX RealTime Optimization Pack 2.9 documentation.

Auto-redirection of USB devices

With this release, Citrix Workspace app lets you redirect USB devices automatically when you connect them. When you connect a USB device, a prompt appears, asking you for permission. After you grant the permission, the USB device is redirected automatically.

> **Note:**
>
> This feature is available on-demand only and works only if the USB device redirection feature is enabled.

What's new in 20.2.0

This release addresses issues to improve the Session reliability and Auto-client reconnection feature, overall Citrix Workspace app performance, and stability.

What's new in 20.1.5

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

What's new in 20.1.0

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

What's new in 1912.5

USB device redirection

Generic USB redirection allows redirection of USB devices from client devices into virtual desktop sessions. With this feature, end users can utilize a wide selection of generic USB devices in their Citrix Virtual Desktops sessions as if the USB devices were physically plugged into the clients.

Generic USB redirection works at a low level and redirects USB request and response messages between client machines and virtual desktops. The feature prevents the need for compatible device drivers on the client machine and the server's ability to support them.

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

This feature is available only on demand.

Limitations:

- Only one USB device is supported at a time.
- Audio and video USB devices are not currently supported.

Auto-launch of ICA file

In earlier releases, you had to manually launch the Workspace app session from the downloaded ICA file to start a session.

Starting with Version 1912.5, you can launch your published apps and desktops by clicking the resource. This feature requires StoreFront (on-premises) Version 1912 or later.

> **Note:**
>
> - This feature is supported only on Chromebook devices and only for HTTPS store URLs.
> - When you select an app or desktop, do not select the **Remember my choice** option in the prompt.

Enhanced session launch

In earlier releases, published app and desktop sessions launched in the store enumeration window itself. To interact with the store enumeration window, you had to disconnect or sign off from the session.

Starting with Version 1912.5, published apps and desktops launch in a separate window. This helps you to use and interact with the store enumeration window without having to disconnect or sign off from the session.

> **Note:**
>
> - This feature is supported only on Chromebook devices.
> - This feature is not supported on tablets, phones, and Samsung DeX.

Limitations:

- After changing any user settings, you must relaunch the session for the changes to take effect.
- Apps and desktop are named 'Workspace' in the taskbar - not after the session.
- Only one session can be used at a time.

What's new in 1911

Workspace with intelligence

This version of Citrix Workspace app for Android is optimized to take advantage of the upcoming intelligent features when they are released. For more information, see Workspace Intelligence Features - Microapps.

What's new in 1910.5

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

What's new in 1910

64-bit compliance

Citrix Workspace app for Android is now 64-bit compliant.

Depending on your Android operating system, the respective binaries are installed.

To know about the installed version, go to **Settings**> **About**.

Battery status indicator

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

> **Note:**
>
> Battery status indicator is not displayed for server VDA.

What's new in 1909.5

Android version support

Citrix Workspace app now supports only Android OS Version 7 (Nougat) and later. Citrix recommends that you use the Workspace app only on the supported version to realize the app's full functionality.

> **Note:**
>
> Citrix Workspace app Version 1909.5 does not support Android OS versions earlier than 7.0.

You can continue to use Citrix Workspace app Version 1909 and later. However, upgrades to later versions will not be available.

What's new in 1909

Support for configuration using Google policy

You can now configure Citrix Workspace app from the Google Admin Console using Google policy. This feature is supported on Chromebook devices only.

Using Google policy, you can add one or more stores by adding the store URL.

For more information, see Google Policy.

EDT MSS stack parameter

Citrix Workspace app for Android now supports the custom EDT MSS stack parameter.

For more information, see Knowledge Center article CTX231821.

What's new in 1908

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

What's new in 1907.5

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

What's new in 1907.1

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

What's new in 1907

Client drive mapping enhancement

Citrix Workspace app informs the server of the available client drives. By default, client drives are mapped to server drive letters so they appear to be directly connected to the session. These mappings are available only for the current user during the current session.

> **Note:**
>
> This feature is supported only on versions of Android running SDK version 24 and later.

Client drive mapping (CDM) allows plug-and-play storage devices in a session. This means that you can use mass storage devices (For example, pen drives), to copy and paste documents between the pen drive and the user device.

Limitations:

- Android APIs are observed to be slow, which delays certain operations.
- CDM for external storage is not supported on Pixel devices.
- File type association is not supported on external storage devices.

Known issue:

- The Workspace app screen might shift between foreground and background when you plug in an external storage device.

What's new in 1906.1

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

What's new in 1906

Supported API version

Chrome OS supports only Android API Version 21 and later.

Also, 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.

> **Note:**
>
> Only Citrix Workspace app is needed to use Skype for Business. You do not need to install HDX RTME. If HDX RTME is already installed on the Chromebook device, you must uninstall it.

To enable HDX RTME from Citrix Workspace app:

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

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

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 several issues that help to improve overall performance and stability. For more information, see Fixed issues.

What's new in 1903

This release addresses various issues that help to improve overall performance and stability. For more information, see Fixed issues.

What's new in 1902.1

This release addresses several 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 several issues to improve overall performance and stability. For more information, see Fixed issues.

Fixed issues

Fixed issues in 20.7.0

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

Fixed issues in earlier releases

Fixed issues in 20.6.5:

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

Fixed issues in 20.6.0:

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

Fixed issues in 20.5.0:

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

Fixed issues in 20.4.5:

- HDX RealTime Optimization Pack might not be optimizing Skype for Business during the initial launch. As a workaround, relaunch Citrix Workspace app. (RFANDROID-5383)
- On a 3D Pro-enabled VDA, a gray screen might appear for some time at logon. (RFANDROID-5471)

Fixed issues in 20.4.0:

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

Fixed issues in 20.3.0:

- Attempts to launch SaaS apps might fail in a session running in Kiosk mode in cloud deployments. [RFANDROID-5137]

Fixed issues in 20.2.0:

- In cloud deployments, the splash screen is scrollable. [RFANDROID-5023]
- Attempts to launch a session in Kiosk mode might fail. [RFANDROID-5133]

Fixed issues in 20.1.5:

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

Fixed issues in 20.1.0:

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

Fixed issues in 1912.5:

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

Fixed issues in 1911:

- In cloud deployments, when you select an uninstalled app from the **All apps** list, you are redirected to the Google Play store. Regardless of the action in the store, the app displays a **Reinstall** flag against it on the **All apps** screen. [RFANDROID-4294]
- The authentication dialog disappears during the app switch when copying the VIP token code. [RFANDROID-4670]
- Unable to send Google Admin policy configurations using the Google Admin console to Citrix Workspace app. [RFANDROID-4678]

Fixed issues in 1910.5:

- Third-party custom applications might sign you out from Citrix Workspace app. [RFANDROID-2477]

- Pinning shortcuts to the home screen might not work on accounts using cloud deployments. [RFANDROID-4567]
- In cloud deployments, Citrix Secure Hub might not read the authentication token from Citrix Workspace app. Instead, Citrix Secure Hub displays the **WebView** authentication dialog. [RFANDROID-4628]
- When you change the screen orientation from portrait to landscape or the opposite and then click the **Battery** icon in the notification area, the battery status is displayed along with the following Toast message:

  "Scroll mode"

  This issue is observed intermittently.

  [RFANDROID-4656]

Fixed issues in 1910:

- In a cloud setup, the user credentials dialog becomes unresponsive for some time and a "Try Again" dialog appears. After you click **Try Again**, you log on successfully. The issue occurs when you log out of Citrix Workspace app, exit the app, and then log back in. [RFANDROID-4589]
- In a cloud setup, the Store list page appears instead of the user credentials dialog. This issue occurs when you log out of Citrix Workspace app, exit the app, and the log back in. [RFANDROID-4590]

Fixed issues in 1909.5:

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

Fixed issues in 1909:

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

Fixed issues in 1908:

- The Native One Time Password (OTP) feature does not work with the Citrix Workspace app. [RFANDROID-4305]
- In a cloud setup, when the user login token expires, the webpage becomes unresponsive and the following error message appears:

  "Please wait"

  [RFANDROID-4257]
- In a cloud setup, when the user login token expires, the user authentication dialog appears repeatedly. [RFANDROID-4354]

Fixed issues in 1907.5:

- If the display is set to **Optimized for high resolution** or if you zoom in during a session, the mouse pointer might shift by a few pixels. [RFANDROID-4258]

Fixed issues in 1907.1:

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

Fixed issues in 1907:

- On an Android-based thin-client device, right-clicking the mouse results in a backspace. [LD1751]

Fixed issues in 1906.1:

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

Fixed issues in 1906:

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

Fixed issues in 1905:

- This fix restricts the number or 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 Wi-Fi to mobile data or the opposite way. [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 user name appears instead of the currently logged in user name. [RFANDROID-3042]
- When you move an extended session to the background, the session remains 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 user name 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 20.7.0

No new known issues have been observed in this release.

Known issues in earlier releases

Known issues in 20.6.5:

No new known issues have been observed in this release.

Known issues in 20.6.0:

No new known issues have been observed in this release.

Known issues in 20.5.0:

No new known issues have been observed in this release.

Known issues in 20.4.5:

No new known issues have been observed in this release.

Known issues in 20.4.0:

No new known issues have been observed in this release.

Known issues in 20.3.0:

- On a Samsung DeX device, you might not be able to cancel USB device redirection if you dismiss the permission prompt without clicking the **Cancel** button. [RFANDROID-5397]

Known issues in 20.2.0:

- Attempts to launch a session fail with an error message when you disable the **Session Reliability** policy on an SSL-enabled VDA. [RFANDROID-5065]
- Attempts to launch SaaS apps might fail in a session running in Kiosk mode in cloud deployments. [RFANDROID-5137]
- Client reconnection attempts do not work and the following error message appears:

  “General problem, try connecting again.”

  The issue occurs on Citrix Gateway-configured stores if the **Session Reconnect** option is disabled and the **Automatic Client Reconnect** option is enabled on the Controller.

  [RFANDROID-5138]

- Attempts to reconnect fail when you click **Connect** in the **Auto Client Reconnect** dialog. The issue occurs in sessions connected to Citrix XenApp and XenDesktop Version 7.6 CU 8. [RFANDROID-5151]

Known issues in 20.1.5:

- In a multiple store-cloud setup, deleting a store might not remove the Store details. The Store remains listed until the user removes the Workspace app from the **Recent** tab. [RFANDROID-5043]

Known issues in 20.1.0:

No new known issues have been observed in this release.

Known issues in 1912.5:

No new known issues have been observed in this release.

Known issues in 1912.5:

- Deep linking is not functional in Incognito mode. [RFANDROID-4864]
- When you select the **Remember my choice** option during session launch, the Chrome browser exists unexpectedly. [RFANDROID-4865]

Known issues in 1911:

No new known issues have been observed in this release.

Known issues in 1910.5:

No new known issues have been observed in this release.

Known issues in 1910:

No new known issues have been observed in this release.

Known issues in 1909.5:

No new known issues have been observed in this release.

Known issues in 1909:

No new known issues have been observed in this release.

Known issues in 1908:

No new known issues have been observed in this release.

Known issues in 1907.5:

No new known issues have been observed in this release.

Known issues in 1907.1:

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 1906.1:

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 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. 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.

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

Citrix Workspace app for Android Third-Party Notices

Copied!
Failed!

Prerequisites for installing

July 12, 2020

System requirements and compatibility

Device requirements

Citrix Workspace app for Android supports Android 7.x (Nougat), 8.x (Oreo), 9.x (Pie), and 10.x (Android Q).

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

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

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

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 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
- 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)

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 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 “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”

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

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.

> **Note:**
>
> Other token-based authentication solutions can be configured using RADIUS. For SafeWord token authentication, see Configuring SafeWord Authentication.

Copied!
Failed!

Install, Upgrade

July 14, 2020

Upgrade

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

- Download the Citrix Workspace app from the Citrix Download page and install the app to upgrade from Citrix Receiver to Citrix Workspace app.
- Upgrade your Citrix Workspace app using Google Play.

For information about the features available in Citrix Workspace app for Android, see Citrix Workspace app Feature Matrix.

For the documentation of Citrix Receiver for Android, see Citrix Receiver.

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 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 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.

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.

Enable HDX RTME from Citrix Workspace app:

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

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

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.

Copied!
Failed!

Get started

July 12, 2020

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

Complete 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 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 an 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

Google policy

Starting with Citrix Workspace app Version 1909 for Android, you can configure Citrix Workspace app from the Google Admin Console using the Google policy. This feature is supported on Chromebook devices only.

Using the Google policy, you can add one or more stores by adding the store URL.

Known issues:

- This feature is not supported on Android Version 5.0 and earlier.
- When you download the ICA file from a web browser and launch the session, the store added using the Google policy is not applied. Instead, Citrix Workspace app launches the downloaded ICA file.

Sample file of Google policy:

```
{

  ”v1”: {

    ”stores”: [
      {

        ”url”: <”https://xyz.example.com>
        ”is_web_interface_enabled”:false
      }
,
    {

        ”url”: <https://xyz.example.com>
        ”is_web_interface_enabled”:false
      }

    ]
   }

}
```

> **Note:**
>
> Provide the complete store URL and not only the name of the domain.

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.

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 websites, 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 that you distribute the following information to enable them to connect to their hosted and desktops successfully:

- The StoreFront URL or XenApp and XenDesktop Site hosting resources; for example: servername.company.com.
- 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 StoreFront to deliver apps, desktops and files from your Citrix Virtual Apps and Desktops deployment.

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 XenMobile Apps and mobile apps you have prepared for your organization through XenMobile.

Authentication between Citrix Workspace app and a StoreFront store can be handled using various solutions:

- Users inside your firewall can connect directly to StoreFront.
- Users outside your firewall can connect to StoreFront through Citrix Gateway.
- Users outside your firewall can connect through Citrix Gateway to StoreFront.

Connecting to StoreFront

Citrix Workspace app for Android supports launching sessions from Workspace for Web, if 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 it's 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.

Connect through Citrix Gateway

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

- XenApp and XenDesktop 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, clientless VPN, or VPN) and type of Workspace deployment (Workspace for Web or locally installed Citrix Workspace app). 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

Workspace app enables users to access apps, files, and other resources delivered by Citrix Endpoint Management. For more information, see Integration with Citrix Workspace experience

Copied!
Failed!

Configure

July 16, 2020

USB device redirection

The generic USB redirection feature allows redirection of arbitrary USB devices from client machines to Citrix Virtual Apps and Desktops. With this feature, the client devices can interact with a wide selection of generic USB devices in a session.

The USB redirection policy must be set to **Allowed** on the Controller. For information about configuring USB redirection in Citrix Studio, see Configure generic USB redirection in Citrix Virtual Apps and Desktops documentation.

Prerequisites:

For printers and scanners:

Install the vendor-specific drivers on the device. When the installation is complete, the vendor software might ask you to reconnect the USB device. Reconnect the USB device to redirect it.

For Chromebooks:

By default, USB devices (for example, pen drives) are blocked by the Chrome operating system. You must whitelist the devices using the Google admin console for managed Chromebooks.

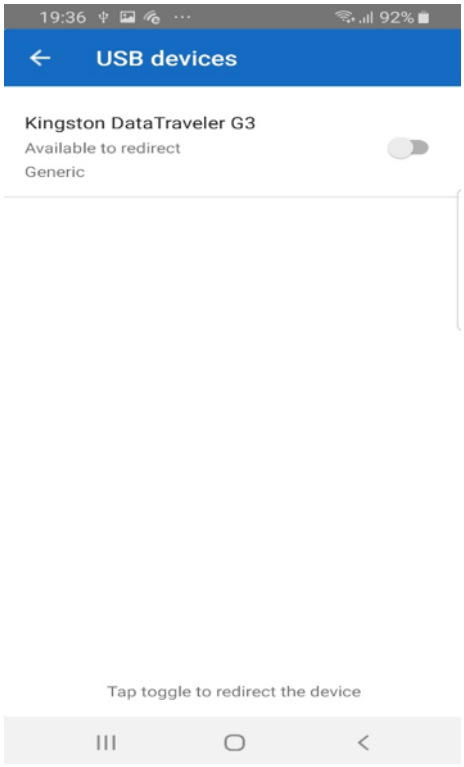
For information on how to whitelist USB devices in a Chromebook, see Knowledge Center article CTX200825.

> **Note:**
>
> Depending on the redirected USB device and the network latency, it might take some time for the device to be visible in the Windows Explorer.

Configuring USB redirection on mobiles phones, tablets, and Samsung DeX

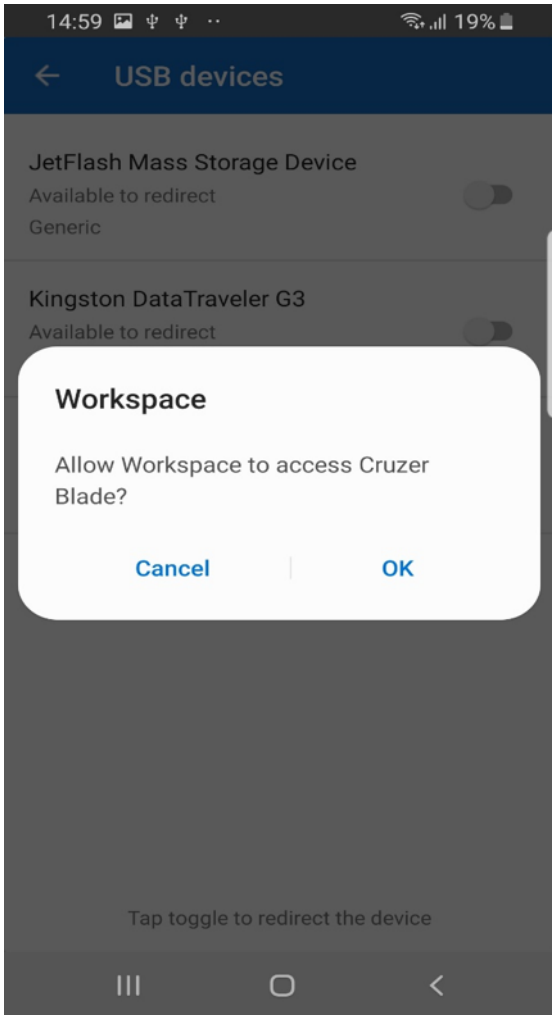
1. Add a USB redirection policy-enabled store and launch a session.
2. Click the session toolbar icon as displayed in the dialog below:

3. Click the **USB Icon** in the session toolbar.
4. Connected USB devices are listed in the USB devices window as shown below:



5. To redirect a particular USB device, click the Toggle option against the device.

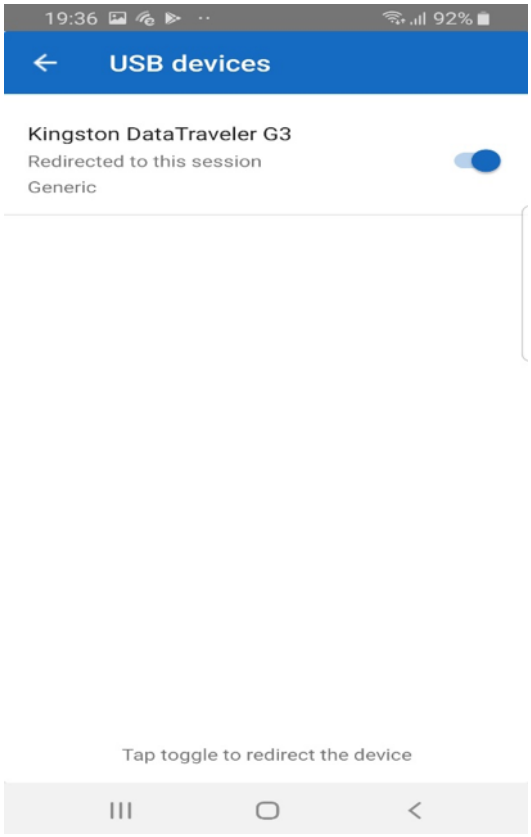
   A Workspace permission dialog appears.



6. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.

   > **Note:**
   >
   > This step is mandatory to redirect the USB device.

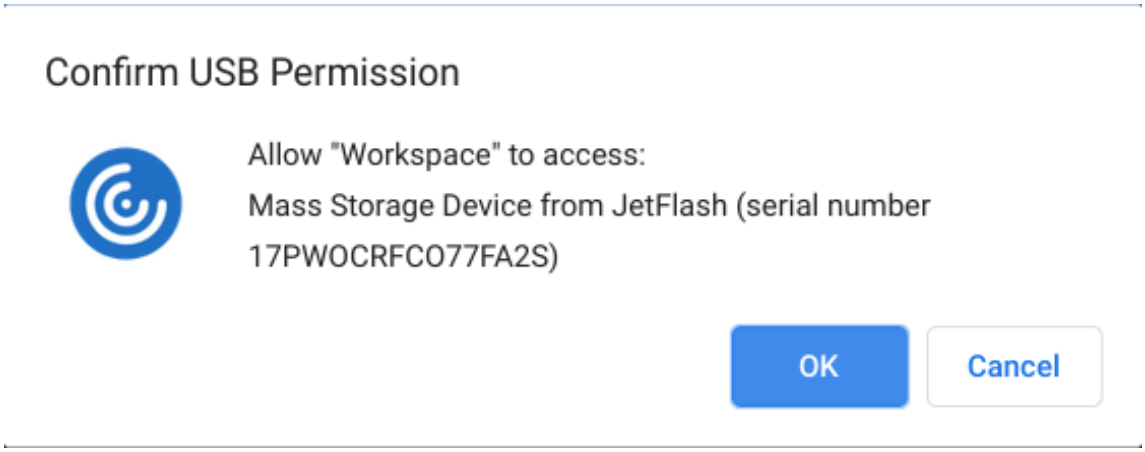
   The USB device is redirected and the status is displayed as shown below:



Configuring the USB redirection feature on Chromebooks

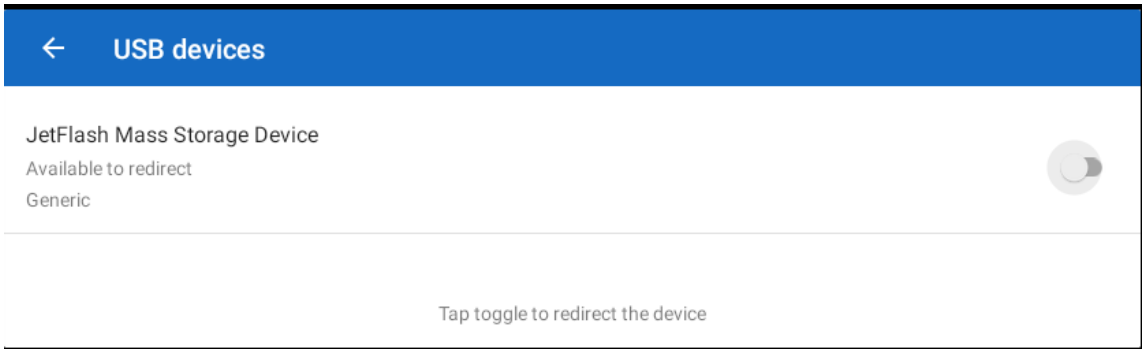
1. Add a USB redirection policy-enabled store and launch a session.
2. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.

> **Note:**
>
> Granting permission is a mandatory step and the prompt appears only on a fresh install.



3. Connect the USB device.
4. Click the toolbar icon and then the USB icon on the session toolbar.

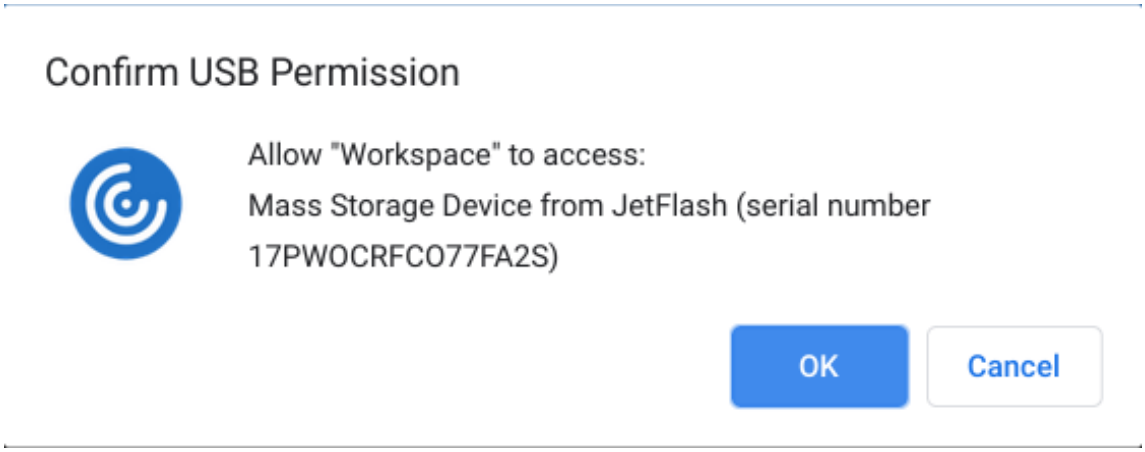
Connected USB devices are listed as shown below:



> **Note:**
>
> If a USB device isn't listed, ensure that you have whitelisted it.

For information on how to whitelist USB devices on a Chromebook, see Knowledge Center article CTX200825.

5. To redirect the USB device, click the **Toggle** option against the device to be redirected.
6. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.



The USB device is redirected and the status is updated. Dismiss the dialog to continue using the redirected USB device.

> **Note:**
>
> - If a pen drive is redirected, it appears as listed in a session.

> • If a printer or scanner is redirected, it is displayed in the **Devices** section in the control panel.

Tested USB devices

Device	Manufacturer	Model
Printer	HP	LaserJet P2014
Scanner	HP	Scanjet G3010
Scanner	Canon	CanoScan LiDE 700F
Space Navigator	3Dconnexion	
Printer	Brother	QL-580N
Scanner	HP	Scanjet 200

Known issues:

- Only one USB device is supported at a time.
- Audio and video USB devices are not currently supported.

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 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.

For more information about the Citrix Ready workspace hub in Citrix Workspace app, see Configure the Citrix Ready workspace hub.

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

Content Collaboration Service integration

Citrix Content Collaboration (formerly ShareFile) enables you to easily and securely exchange documents, send large documents by email, and securely handle document transfers to third parties. There are many ways to work using Citrix Content Collaboration, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

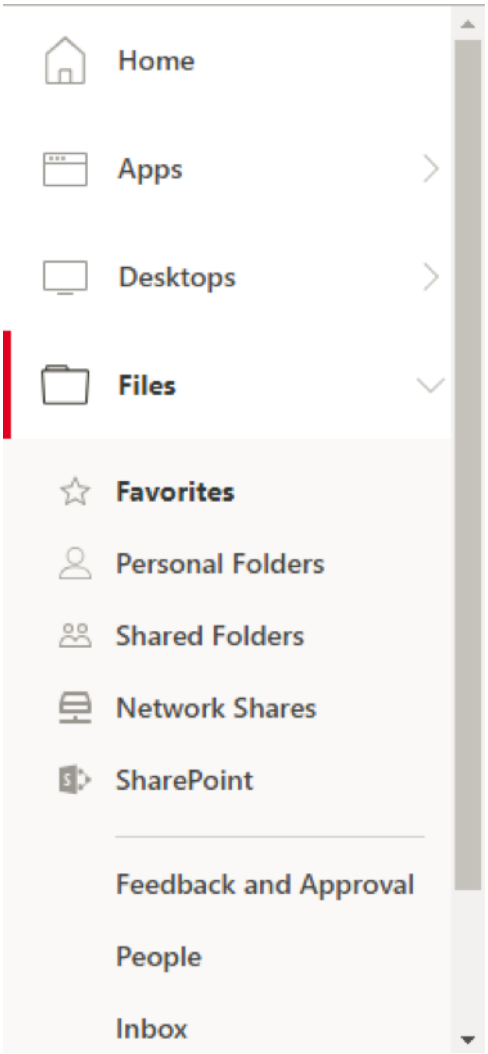
You can access Citrix Content Collaboration using the **Files** tab in the Citrix Workspace app. You can view the **Files** tab only if the Content Collaboration Service is enabled in the Citrix Cloud console. For information, see Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

> **Note:**
>
> Citrix Content Collaboration integration 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 Citrix Workspace app:



Keyboard layout synchronization

Citrix Workspace app 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**.

Note:

- 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. 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.

Copied!
Failed!

Authenticate

July 16, 2020

RSA SecurID

> **Note:**
>
> Citrix Workspace app has deferred support for **Next Token Mode** because of a third-party dependency. We will update this description as information about the supportability become available.

With this feature enabled, if you entere three incorrect passwords, the Citrix Gateway plug-in prompts you to wait until the next token is active before logging on. The RSA server can disable a user's account if a user logs on too many times with an incorrect password.

For more information, see the 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 name 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 website.

Follow these general steps:

1. On a computer (not a mobile device), download the converter tool here. Follow the instructions on the website and 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 required for authentication.
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, change the file name extension to .xml and import it.

Copied!
Failed!

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.

Copied!
Failed!

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