Citrix Workspace app for Android
## Contents

- **About this release** 3
- **Features in Technical Preview** 16
- **Prerequisites for installing** 25
- **Install, Upgrade** 30
- **Get started** 30
- **Configure** 36
- **Configure Citrix Workspace app using Unified Endpoint Management solutions** 53
- **Peripherals** 55
- **Extend display** 58
- **User experience** 61
- **Session experience** 68
- **Store experience** 82
- **Authenticate** 83
- **Secure** 86
- **Troubleshoot** 89
- **SDK and API** 92
About this release

November 3, 2023

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

Note:
Looking for features in Technical Preview? We have curated a list so that you can find them in one place. Explore our Features in Technical Preview page and share your feedback using the attached Podio form link.

What’s new in 23.10.5

Support for external microphone

Previously, Citrix Workspace app for Android supported audio redirection through the device’s microphone only.

Starting with the 23.10.5 version, Citrix Workspace app for Android supports external microphones. Microphones can be USB or Bluetooth-based peripheral devices.

After you connect a USB or a Bluetooth microphone, the audio redirects from the external microphone to the session. When you remove the external microphone from the device, the audio automatically redirects to the device’s microphone.

This feature is helpful when you connect an external microphone, for example, to a:

- phone
- tablet
- smart TV
- external monitor in a conference room.

Fixed issues in 23.10.5

There are no fixed issues in this release.

Known issues in 23.10.5

There are no new known issues.

Note:
For a complete list of issues in the earlier releases, see the Known issues section.
Earlier releases

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

23.10.0

What’s new

Screenshot detection and prevention through Unified Endpoint Management solutions

Starting with the 23.10.0 version, administrators can prevent end users from taking screenshots at the Citrix Workspace app level.

This feature prevents sensitive or private information leaks. Administrators can configure this feature using an AppConfig-based key-value pair:

- key: restrictScreenshot
- value type: Boolean
- value:
  - If set to true, end users can’t take screenshots.
  - If set to false, end users can take screenshots.

Fixed issues in 23.10.0

There are no fixed issues in this version.

23.9.5

What’s new

Addition of Ctrl+Alt+Del shortcut in session toolbar

Starting from the 23.9.5 version, the session toolbar has a new option to do the Ctrl+Alt+Del function with the tap of a button.

This option helps users to sign out, switch users, lock the device, or access the Task Manager.
Support for full-screen mode for app sessions

Previously, when you started an app session, you could view it in windowed mode.

Starting from the 23.9.5 version, Citrix Workspace app for Android introduces a new option to view the app session in full-screen mode. This feature is helpful when you:

- start a session in full immersion mode with touch devices
- try to duplicate the screen and cast it
- view the Citrix Workspace app on a smaller screen.

To enable the option, go to Citrix Workspace app for Android Settings > Advance > Fullscreen Window and toggle on. The following screenshot displays the option:
Citrix Workspace app for Android

Accessibility and TalkBack

Citrix Workspace app provides an enhanced user experience with the TalkBack feature. The TalkBack feature helps end users who have difficulty seeing the screen. The narrator reads the screen elements aloud when using the UI.

To use the Android talkback feature, end users must enable it from Android Settings > Accessibility > Talkback.

For more information, see Accessibility and TalkBack in the help documentation.

Technical preview

- Separate session window from Citrix Workspace app for Samsung DeX

For the complete list of Technical Preview features, see the Features in Technical Preview page.

Fixed issues in 23.9.5

- In a multimonitor setup, when you tap the extend icon on the session toolbar, a gray bar might appear at the bottom of the extended session. The issue occurs when you start a session on the Samsung DeX, with some of the Samsung tablets as the external monitor. [CVADHELP-23269]
23.8.0

What’s new

Support for Android 14

Citrix Workspace app for Android 23.8.0 supports Android 14. Upgrading to Citrix Workspace app version to 23.8.0 ensures continuous support for devices that are updated to Android 14.

Support for FIDO2-based authentication

Starting with the 23.8.0 version, Citrix Workspace app for Android now supports password-less authentication within a Citrix Virtual Apps and Desktops session using FIDO2-based authentication methods.

For more information, see Support for FIDO2-based authentication.

Support for Transport Layer Security 1.3

Citrix Workspace app for Android now supports Transport Layer Security (TLS) 1.3. It boosts performance and efficiency. TLS 1.3 provides robust security with its strong cipher suites and one-time session keys.

For more information, see Support for Transport Layer Security 1.3.

For more information on help documentation, see TLS version.

Support for full-screen display

Starting with the 23.8.0 version, the H264 codec supports improved video rendering in full screen mode. If you’re a frequent consumer of videos or heavily depend on video content, this feature is recommended for you. It’s designed to improve your video experience for performance, video quality, and resource utilization.

For more information see, Support for full-screen display.

Managing predictive text

The predictive text helps in a better typing experience by suggesting words that you can type next. When you enable this feature during an app or desktop session, it’s possible for passwords to show up on the prediction ribbon. To control this behavior this feature is disabled by default.

Notes:

- On your device’s default keyboard settings, if the Predictive text option is disabled, you can’t use this feature even when you enable it through Citrix Workspace app for Android.
- In a session, when the CJK input layout is set as a default on the GBoard keyboard, the...
English layout appears instead of the CJK layout. To view the CJK keyboard layout, go to app Settings > Keyboard and enable the Predictive text option. [CVADHELP-23667]

Technical preview

- Add many stores using UEM

For the complete list of Technical Preview features, see the Features in Technical Preview page.

Fixed issues in 23.8.0

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

23.7.5

What's new

Support for store configuration using unified endpoint management solutions

Citrix Workspace app for Android now supports remote configuration of your Workspace Store URL using unified endpoint management solutions. As an administrator, you can manage store URLs remotely using the AppConfig-based key-value pairs using unified endpoint management solutions.

To configure your Workspace Store URL using unified endpoint management solutions, follow these steps:

Note:

- This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.

Configure your store using mobile device management

Citrix Workspace app for Android supports remote configuration of your Workspace Store URL using unified endpoint management solutions.

To remotely configure your Workspace Store URL using existing unified endpoint management solutions, follow these steps:

1. Sign in to your unified endpoint management solutions provider.
2. Create an app configuration policy for your app.
3. Add a new key and value pair to the XML property list and fill in the following values:

   - key: url
   - value type: String
   - value: your store URL (for example, prodcwa.cloud.com)
Citrix Workspace app for Android

**Note:**

- For demonstrative purposes, Microsoft Intune is used as the unified endpoint management solution in this example. The UI shown differs depending on your unified endpoint management solutions provider.

**Settings**

<table>
<thead>
<tr>
<th>Configuration key</th>
<th>Value type</th>
<th>Configuration value</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>String</td>
<td>prodowa.cloud.com</td>
</tr>
</tbody>
</table>

**Limitations in the feature**

- If a cloud store is already set up and the administrator configures a new cloud store, your existing cloud store and any associated data or settings are deleted. You receive a notification to inform you of the deletion in Citrix Workspace. You must then sign in again so that the new cloud store is added to Citrix Workspace.
- To apply new configurations, you must close and open Citrix Workspace app.

**Support to configure store type**

Starting with the 23.6.0 version, Citrix Workspace app for Android supports configuring store type using the AppConfig-based key-value pair to configure the Citrix Workspace app. Now, administrators can control how the app appears.

The following is the key-value pair:

- **key**: storeType
- **value type**: Integer
- **value**:
  - If set to 1 (default), users can view the native or the default store loading.
  - If set to 2, users can view the store inside a web interface.

**Note:**

This feature doesn’t require enablement.

**Control store configurations using unified endpoint management solutions**

The Citrix Workspace app for Android started supporting remote configuration of the Workspace Store URL using unified endpoint management solutions from the 23.4.5 version. As an administrator, you...
can manage store URLs remotely using AppConfig-based key-value pairs using unified endpoint management solutions.

For more information, see Support for store configuration using unified endpoint management solutions.

Starting with the 23.7.5 version, administrators can configure if end users can modify store URLs using an AppConfig-based key-value pair:

- **key**: restrict_user_store_modification
- **value type**: Boolean
- **value**:
  - If set to true, end users can’t modify the store (add or delete or edit).
  - If set to false, end users can modify the store.

**Note:**

If the flag restrict_user_store_modification is set to true, all the existing stores are deleted before adding a new unified endpoint management-configured store.

**Fixed issues**

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

**23.6.5**

**What’s new**

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

**Fixed issues**

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

**23.6.0**

**What’s new**

**Support to configure store type [Technical Preview]**

Starting with the 23.6.0 version, Citrix Workspace app for Android supports configuring store type using the AppConfig-based key-value pair to configure the Citrix Workspace app. Now, administrators can control how the app appears.
The following is the key-value pair:

- **key**: storeType
- **value type**: Integer
- **value**: 
  - If set to 1 (default), users can view the native or the default store loading.
  - If set to 2, users can view the store inside a web interface.

**Note:**
This feature doesn't require enablement.

**Fixed issues in 23.6.0**
- There are no fixed issues in this release.

**23.4.5**

**What's new**

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

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

For more information, see the Global App Configuration service documentation.
For more information on how to configure, see Global App Configuration service channel support.

**Support for store configuration using Unified Endpoint Management solutions [Technical Preview]**
Citrix Workspace app for Android now supports remote configuration of your Workspace Store URL using unified endpoint management solutions. As an administrator, you can manage store URLs remotely using the AppConfig-based key-value pairs using unified endpoint management solutions.

To configure your Workspace Store URL using unified endpoint management solutions, follow these steps:
Citrix Workspace app for Android

**Note:**
- This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.

**Configure your store using unified endpoint management solutions**

Citrix Workspace app for Android supports remote configuration of your Workspace Store URL using unified endpoint management solutions.

To remotely configure your Workspace Store URL using existing unified endpoint management solutions, follow these steps:

1. Sign in to your unified endpoint management solutions provider.
2. Create an app configuration policy for your app.
3. Add a new key and value pair to the XML property list and fill in the following values:
   - **key:** url
   - **value type:** String
   - **value:** your store URL (for example, prodcwa.cloud.com)

**Note:**
- For demonstrative purposes, Microsoft Intune is used as the unified endpoint management solution in this example. The UI shown differs depending on your unified endpoint management solutions provider.

<table>
<thead>
<tr>
<th>Configuration key</th>
<th>Value type</th>
<th>Configuration value</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>String</td>
<td>prodcwa.cloud.com</td>
</tr>
</tbody>
</table>

**Limitations**

- If a cloud store is already set up and the administrator configures a new cloud store, your existing cloud store and any associated data or settings are deleted. You receive a notification to inform you of the deletion in Citrix Workspace. You must then sign in again so that the new cloud store is added to Citrix Workspace.
- To apply new configurations, you must close and open Citrix Workspace app.

**Support for front and rear camera redirection**
Citrix Workspace app for Android

Citrix Workspace app for Android now allows you to switch the camera position from front to rear and conversely, within the HDX session. Both 32-bit and 64-bit applications are supported.

A floating button appears when you invoke the camera. A single tap on the floating button to switch between the front and rear camera positions. You can also move the floating button freely around the screen and place it anywhere.

**Known issues in the feature**

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

**Fixed issues**

- There are no fixed issues in this release.

**23.3.5**

**What’s new**

This release addresses a few issues that help to improve overall performance and stability. In addition, this release enhances the user experience related to the frequency of the Rate your experience pop-up.

**Technical preview**

- Introducing picture-in-picture mode
- Rapid scan

For the complete list of Technical Preview features, see the Features in Technical Preview page.

**Fixed issues in 23.3.5**

There are no fixed issues in this release.

**23.3.0**

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

**Fixed issues**

There are no fixed issues in this release.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
23.2.0

What’s new

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

Fixed issues

There are no fixed issues in this release.

23.1.0

What’s new

Support for webcam redirection

You can now redirect the front camera of your device into the session. Both 32-bit and 64-bit applications are supported. By default, the auto-redirection of the webcam is enabled.

Fixed issues

- A few apps and desktop sessions fail to start. The following error message appears: “Try connecting again”. [HDX-47308]

Known issues

Known issues in 22.6.5

- When you open a Web app or a SaaS app, the taskbar buttons and ellipsis do not work as expected. The issue occurs after you toggle on Web Interface in the Add Account screen. [RFANDROID-10266]

Known issues in 21.4.0

No new known issues have been observed in this release.

Note:

When you’re enrolled in the Work profile in Citrix Workspace app, launching your sessions using the Chrome browser from an ICA file in the Personal profile no longer works. However, the issue isn’t present with Citrix Secure Web on adding the ICA file URL in the exclusion list.
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 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]

Limitations

- While starting Web and SaaS apps from within the Citrix Workspace app, if the app uses Google IdP and requires the end user to sign in then the authentication will fail with the error message “Access Denied”.

Technical preview

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

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

Legacy documentation

For product releases that have reached End of Life (EOL), see Legacy documentation.
Features in Technical Preview

November 9, 2023

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

Separate session window from Citrix Workspace app for Samsung DeX

This feature is in technical preview from 23.9.5 release.

Previously, when you started a virtual app or a desktop session, it opened in the Citrix Workspace app UI window. With this arrangement the end users had to tap the Home icon from the session toolbar and disconnect the session to access another app or desktop from Citrix Workspace app. The single window mode restricted the desktop experience on the Samsung DeX.

Starting from the 23.9.5 version, Citrix Workspace app introduces a separate session window that makes multi-tasking more efficient and user-friendly. With this feature, you can have a desktop-like experience.

For example, when you open the Google Chrome browser, it opens as a separate window as shown in the following screenshot.

![Separate session window example](image)

Known limitations in the feature

Only one session window is supported. In other words, the existing session window closes when opening a new session window.
Notes:
• This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.
• You can provide feedback for this technical preview by using the Podio form.

Add many stores using UEM

This feature is in technical preview from 23.8.0 release.
Administrators can now use Unified Endpoint Management (UEM) solutions to configure many stores for managed Android devices.

Note:
• You can provide feedback for this technical preview by using the Podio form.

The details for each store can be added to a JSON file. This JSON file can then be uploaded while configuring the app configuration policy. The details include:

• store URL

• store type (optional)

  Note:
  – If the store type isn’t provided, then the default interface is considered as native.

• store name (optional)

  Note:
  – UEM supports one cloud store and many on-premises stores.

The JSON file must be in a key-value format. For more information, refer to the following sample JSON data:

  Note:
  • The sample JSON data is related to Microsoft Intune. The JSON data might vary for other UEM solutions.

```json
{
  "kind": "androidenterprise#managedConfiguration",
  "productId": "app:com.citrix.Receiver",
  "managedProperty": [
    {
      "key": "stores",
```
"valueBundleArray": [
    {
        "managedProperty": [
            {
                "key": "url",
                "valueString": "test.cloud.com"
            },
            {
                "key": "storeType",
                "valueInteger": 1
            },
            {
                "key": "displayName",
                "valueString": "StoreFront1"
            }
        ],
        "managedProperty": [
            {
                "key": "url",
                "valueString": "test2.cloud.com"
            },
            {
                "key": "storeType",
                "valueInteger": 2
            },
            {
                "key": "displayName",
                "valueString": "StoreFront2"
            }
        ]
    }
]
```
] } ]
} ,
{
  "key": "restrict_user_store_modification",
  "valueBool": false
}
}
<!--NeedCopy-->  

Notes:

- (default) If the integer is set to 1, users can view the native or the default store loading.
- If the integer is set to 2, users can view the store inside a web interface.

To upload the JSON file that contains store configurations, select Enter JSON data from the Configuration settings format drop-down list.
Introducing picture-in-picture mode

This feature is in technical preview from 23.3.5 release.

Citrix Workspace app for Android supports picture-in-picture (PiP) mode, enabling you to shrink your desktop session, SaaS app, or web app, to a floating window. You can move this window freely around the screen and place anywhere. PiP mode frees up the home screen of the Citrix Workspace app for you to complete other tasks.

To use this feature:

- In your desktop session, tap the **Home** button on the session toolbar.
  
  or

- While using a SaaS or web app, tap the **ellipsis menu (…) > Minimize.**
Tap on the floating window to view the app in full screen and close the app by tapping the X icon on the floating window. The floating window appears automatically in full screen when you minimize another app.

Note:
- This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.

The PiP feature is supported on both on-premises and cloud deployments. However, for cloud deployments, you can:

- minimize web apps to a PiP window.
- switch between a desktop session and a web app by tapping on the floating window.

Note:
You can keep only two apps active at a time. One in full screen mode and the other minimized as a PiP:
- 2 web or SaaS apps
- 1 web or SaaS app and 1 virtual app or desktop session

Rapid scan

This feature is in technical preview from 23.3.5 release.

If you’re signed into Citrix Workspace app, you can use the Rapid scan feature to scan many documents and transfer those scanned documents into the desktop session.

Note:
- This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.

Prerequisites

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

How to use the feature

To scan the documents:
1. From the in-session toolbar, tap the rapid scan icon.

2. Tap **ADD IMAGE** to start scanning.

   ![](image)

   To scan a document, tap 'Add image'

   ![](image)

   The camera app opens and you can start taking the photos.

3. (Optional) Crop the scanned document. After cropping to the required size, tap **CROP**.
4. Choose from the options to save the file in the required format.

5. Tap **Save**.

All the scanned documents are accessible inside the folder **CitrixRapidScanDocuments** on the external storage of your device. You can access the scanned documents through:
Citrix Workspace app for Android

- File manager on your device
- Client drive mapping (CDM) on your virtual desktop.

**DPI Matching**

*This feature is in technical preview from 22.12.0 release.*

The DPI matching feature ensures that the DPI scaling setting present in a remote desktop matches your device’s DPI setting. In general, the display clarity depends not only on resolution but also on the density of the pixels (DPI).

Previously, the sessions were rendered by resolution settings and those sessions weren’t clear even on high-DPI mobile phones or tablets.

Starting with the 2212 release, a new UI is introduced to achieve DPI matching. On your device, go to Citrix Workspace app for Android > Settings > General > Display > Session Resolution > and select the Match client DPI option.

You can now connect an Android phone, or an Android tablet to an external monitor, or a TV and the session display scales according to the optimal DPI settings. You can use the Samsung DeX mode.
too. In other words, the Citrix Workspace app attempts to match the display resolution and DPI scale settings of the Android device to the Citrix session automatically.

This feature enhances the user experience by rendering the sessions according to the DPI of the phone or tablet. The session icons, text, and image clarity are now sharper and more comfortable to read. By default, the DPI matching feature is disabled.

Note:
- This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.

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

This feature is in technical preview from 22.3.5 release.

This feature simplifies the configuration of SSO for internal web apps and SaaS apps while using third-party identity providers (IdPs).

The enhanced SSO experience reduces the entire process to a few commands. It eliminates the mandatory prerequisite to configure Citrix Secure Private Access in the IdP chain to set up SSO. It also improves the user experience, provided the same IdP is used for authentication to both the Workspace app and the particular web or SaaS app being launched.

You can register for this technical preview by using this Podio form.

**Prerequisites for installing**

November 9, 2023

**System requirements and compatibility**

**Device requirements**

Citrix Workspace app supports Android versions 7 and later.

For the best results, update Android devices to the latest Android operating system.

You can start Citrix Workspace app sessions from Workspace for Web, when the web browser is compatible with Workspace for Web. If you’re unable to start the session, configure your account through Citrix Workspace app directly.
Important:
If a Technical 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 limitations of this deployment, see the StoreFront documentation.

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
- Citrix Virtual Apps and Desktops 7.x or later

Connections and certificates

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 12.1 and later (including VPX, MPX, and SDX versions).

TLS Certificates

When you secure remote connections using TLS, the mobile device does the following:

1. Authenticates the remote gateway’s TLS certificate against a local store of trusted root certificate authorities.
2. 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**

When you install a private certificate on the remote gateway, make sure the root certificate of the organization's certificate authority is installed on the mobile device. This configuration helps you to access Citrix resources successfully using Citrix Workspace app for Android.

*Note:*

When you can’t verify the gateway’s certificate upon connection, because the root certificate isn’t 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, an 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 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 verifies if the certificates are trusted. If the certificates aren’t 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 the Citrix Workspace app for Android connection to fail.

Suppose that a Citrix Gateway is configured with these valid certificates. It’s recommended for customers who require stricter validation. They can enforce 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 verifies if all these certificates are valid. Citrix Workspace app for Android also verifies if it already trusts an “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 fail. Consult the certificate authority’s documentation to determine which root certificate can 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, without the root certificate, is normally recommended:

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

Citrix Workspace app for Android uses these two certificates. It then searches 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”
Citrix Workspace app for Android

- “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. It’s intended for situations when more than one root certificate is found, and an earlier root certificate is still in use at the same time as a later root certificate. In this case, there are 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). It differentiates the cross-signed intermediate certificate from an ordinary intermediate certificate (such as “Example Intermediate Certificate 2”).

This configuration, without 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 isn’t recommended to configure the Citrix Gateway by using only the server certificate:

- “Example Server Certificate”

When Citrix Workspace app for Android can’t locate all the intermediate certificates, the connection fails.
Install, Upgrade

September 20, 2023

Upgrade

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

• Upgrade your Citrix Workspace app using Google Play.

• Download the Citrix Workspace app from the Citrix Download page and install the app to upgrade from Citrix Receiver to Citrix Workspace app.

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.

Get started

November 9, 2023

Request demo access

You can now experience the Citrix Workspace on mobile devices in a easy way. Potential users and anyone interested now have free demo access of the Citrix Workspace app for Android.

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

To request demo access:

1. Tap Request demo access on the Citrix Workspace app Sign in screen.
2. The Citrix request demo access webpage appears.

3. Enter your required details like name, company, address, phone number, city, work email address, and then tap **Submit Request**.

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

**Account**

To create an account do the following:
1. Enter a valid store URL or your email address in the **Address** field. For example, store-front.organization.com. Fill the other fields with necessary details.
2. Enter the user credentials.

**Access to StoreFront through Citrix Gateway**

For 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 isn't 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 isn't applied. Instead, Citrix Workspace app launches the downloaded ICA file.

**Sample file of Google policy:**

```json
{
  "v1": {
    "stores": [
      {
        "url": "https://xyz.example.com",
        "is_web_interface_enabled": false
      },
      {
        "url": "https://xyz.example.com",
        "is_web_interface_enabled": false
      }
    ]
  }
}
```
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. It then prompts the user to sign in, to access their hosted applications, desktops, and data.

Provision file

You can use StoreFront to create provisioning files that have connection details for accounts. You can 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 get 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

When you provide users with account details that they need to enter manually, make sure you distribute the following information. The following information enables users to connect to their hosted desktops successfully:

- The StoreFront URL or XenApp and XenDesktop Site hosting resources; for example: server-name.company.com.
- To access using Citrix Gateway, provide the Citrix Gateway address and the required authentication method.
See the Citrix Gateway documentation for more information.

When a user enters the details for a new account, Citrix Workspace app tries 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 and Citrix DaaS**

Citrix Workspace app requires configuration of StoreFront to deliver apps, desktops, and files from your Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment.

**StoreFront**

You can configure StoreFront to provide authentication and resource delivery services for Citrix Workspace app, which enables you to create centralized enterprise stores to deliver:

- Desktops and applications through Citrix Virtual Apps and Desktops or Citrix DaaS.
- XenMobile Apps and mobile apps you’ve 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 is compatible 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 aren't launched automatically when downloading an .ICA file. The .ICA file must be opened manually, right 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 count 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.
Citrix Workspace app for Android

Configure stores for StoreFront just as you would Citrix Virtual Apps and Desktops and Citrix DaaS. No special configuration is needed for mobile devices.

**Connect through Citrix Gateway**

Citrix Workspace app for Android supports Citrix Gateway 11 and later with 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 following:

- the type of connection (such as ICA, clientless VPN, or VPN)
- the type of Workspace deployment (Workspace for Web or locally installed Citrix Workspace app).

The policies can be achieved from a single virtual server.

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

**VPN functionality**

You can access the internal Web, Software-as-a-Service (SaaS) apps, and websites hosted by your company - regardless of your access location. You can access these resources, hosted by your company, without a VPN connection. This feature is available only for customers on cloud stores.

**Allow access to manage all files**

We’ve introduced the permission option – **Allow access to manage all files**. We recommend that you enable this permission for optimal performance. Your files remain secure.
Per-store microphone access

The client-selective trust feature allows Citrix Workspace app to trust access from a VDA session. You can grant access to local client drives and hardware devices like microphones and webcams.

Previously, your setting for microphone access was applied on all configured stores.

Now, Citrix Workspace app requires the end user’s permission to access the microphone. The selected setting for microphone access is applied on a per-store basis. Provide the permission to access the microphone as follows:

1. Long press on the Citrix Workspace app icon and tap the App info icon.
2. Tap **Permissions**.

3. Tap **Microphone**.
4. Select **Allow only while using this app**.

Now, you can access the microphone while using Citrix Workspace app.

Configure the access levels as follows:

1. Open the Citrix Workspace app and select **Settings > Store settings**.
2. Under the **Set permissions for** option, select a store from the drop-down menu.
3. Enable **Microphone**.

Now, the microphone is enabled and you can use it while using Citrix Workspace app in your Android device.

**Per-store location access**

The client-selective trust feature allows Citrix Workspace app to trust access from a VDA session.

Previously, your setting for location access was applied on all configured stores.

Starting with the version 21.3.0, Citrix Workspace app requires the end user’s permission to access the location. The selected setting for location access is applied on a per-store basis. Provide the permission to access the location as follows:

1. Long press on the Citrix Workspace app icon and tap the **App info** icon.
2. Tap **Permissions**.

3. Tap **Location**.
4. Select **Allow only while using this app**.

Now, you can access the location while using Citrix Workspace app.

Configure the access levels as follows:

1. Open the Citrix Workspace app and select **Settings > Store settings**.

2. Under the **Set permissions for** option, select a store from the drop-down menu.
3. **Enable Location.**

Now, location is enabled and you can use it while using Citrix Workspace app in your Android device.

**Per-store camera access**

The client-selective trust feature allows Citrix Workspace app to trust access from a VDA session. You can grant access to local client drives and hardware devices like microphones and webcams. Previously, your setting for camera access was applied on all configured stores.

Now, Citrix Workspace app requires the end user’s permission to access the camera. The selected setting for camera access is applied on a per-store basis. Provide the permission to access the camera as follows:

1. Long press on the Citrix Workspace app icon and tap the **App info** icon.
2. Tap **Permissions**.

3. Tap **Camera**.
4. Select **Allow only while using this app**.

Now, you can access the camera while using Citrix Workspace app.

Configure the access levels as follows:

1. Open the Citrix Workspace app and select **Settings > Store settings**.
2. Under the **Set permissions for** option, select a store from the drop-down menu.
Citrix Workspace app for Android

3. Enable **Camera**.

Now, the camera is enabled and you can use it while using Citrix Workspace app in your Android device.

**Feature flag management**

If an issue occurs with Citrix Workspace app in production, we can disable an affected feature dynamically in Citrix Workspace app even after the feature is shipped. To do so, we use feature flags and a third-party service called LaunchDarkly.

You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly through specific URLs or IP addresses, depending on your policy requirements.

You can enable traffic and communication to LaunchDarkly in the following ways:

**Enable traffic to the following URLs**

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com
- app.launchdarkly.com

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
**List IP addresses in an allow list**

If you must list IP addresses in an allow list, for a list of all current IP address ranges, see LaunchDarkly public IP list. You can use this list to verify if your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Status page.

**LaunchDarkly system requirements**

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

- LaunchDarkly service.
- APNs listener service

**Provision to disable LaunchDarkly service**

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

On the cloud setup, administrators can disable the LaunchDarkly service. Administrator can set the `enableLaunchDarkly` attribute to **False** in the Global App Configuration Service.

```json
{
  "assignedTo": [
    "AllUsersNoAuthentication"
  ],
  "category": "Third Party Services",
  "settings": [
    {
      "name": "Enable Launch Darkly",
      "value": "true"
    }
  ],
  "userOverride": false
}
```

For more information, see the Global App Configuration Service documentation.

On the on-premises deployment, do the following:
Citrix Workspace app for Android

1. Use a text editor to open the **web.config** file, which is typically at `C:\inetpub\wwwroot\Citrix\Roaming` directory.

2. Locate the user account element in the file (Store is the account name of your deployment).
   For example, `<account id=... name="Store">`. Before the `</account>` tag, navigate to the properties of that user account:

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

3. Add the **enableLaunchDarkly** tag and set the value as **false**.
   ```xml
   <property name="enableLaunchDarkly" value="false"/>
   ```

   **Note:**
   Most of the features are behind a feature flag, and LaunchDarkly controls them. In the environments where it is disabled, you have to wait for a minimum of 90 days to avail the feature.

**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’re 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), which is an expected behavior.

Citrix Workspace app reads and applies the settings configured by administrators in Citrix Studio. To apply FTA in a session, make sure that end 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 that are on the 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, and then 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 in the feature

1. Smart card authentication might be slower than password authentication. For example, after disconnecting from a session, wait for approximately 30 seconds before you attempt to reconnect. Reconnecting to a disconnected session too quickly might cause Citrix Workspace app to turn unresponsive.
2. Smart card authentication isn’t supported on farms.
3. Some users might have a global PIN number for smart cards. However, when users sign in using a smart card account, they must enter the PIV PIN and not the global smart card PIN, which 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 aren’t supported.
Citrix Workspace app for Android

6. You can access only MIME file formats supported by Microsoft Office, Adobe Acrobat reader, and Notepad applications using the file type association feature.

Customer Experience Improvement Program (CEIP)

<table>
<thead>
<tr>
<th>Data collected</th>
<th>Description</th>
<th>What we use it for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration and usage data</td>
<td>The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app and automatically sends the data to Google Analytics for Firebase.</td>
<td>This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app.</td>
</tr>
</tbody>
</table>

Additional Information

Citrix handles your data in accordance with the terms of your contract with Citrix. Your data is protected as specified in the Citrix Services Security Exhibit. This exhibit is available on the Citrix Trust Center.

You can disable sending CEIP data to Citrix and Google Analytics for Firebase (except for the two data elements collected for Google Analytics for Firebase indicated by an * in the following table) by:

1. Launch the Citrix Workspace app and select Settings.
2. Select Advanced Preferences.
   The Advanced Preferences dialog appears.
3. Clear the option Send Usage statistics.

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

The specific CEIP data elements collected by Google Analytics for Firebase are:

<table>
<thead>
<tr>
<th>Operating system version*</th>
<th>Workspace app version*</th>
<th>Authentication configuration</th>
<th>Device information</th>
</tr>
</thead>
</table>

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
## Migration from on-premises to cloud account

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

To configure:

1. Navigate to the **Global App Configuration Store Settings API** URL and enter the cloud Store URL. For example, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.

2. Navigate to **API Exploration > SettingsController > postDiscoveryApiUsingPOST** > click **POST**.

3. Click **INVOKE API**.

4. Enter and upload the payload details. Enter the StoreFront store expiry date in the epoch timestamp in milliseconds format.

For example,

```json
1 "migrationUrl": [
2 {  
3  
4 }
```
5. Click **EXECUTE** to push the service.

**End user Experience for this feature**

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

**Note:**

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

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

**Note:**

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

**Use the latest version**

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

When you tap **Update**, the update happens in the background, and you can continue using the app. You can view the progress on the Snackbar. After the download is complete the following dialog box appears:

Tap **Relaunch now** to use the latest version. If you tap **Do it later**, the prompt to restart the app appears in the next app launch.

**Global App Configuration service channel support**

Starting with the 23.4.5 release, administrators can use the Global App Configuration service to define settings and test them before rolling out the configuration to all end users. This process ensures that
Citrix Workspace app for Android

features and functionalities are well-tested before production.

Note:

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

For more information, see the Global App Configuration service documentation.

**How to use this feature**

To test configurations:

1. Navigate to Citrix Workspace app **Settings > Advanced > App configuration**
2. Select **Test channel**.

You can now start the test.

Note:

- Make sure that the app configurations are present on the Test channel. For assistance, contact your organization’s administrator.
Configure Citrix Workspace app using Unified Endpoint Management solutions

November 9, 2023

Support for store configuration using unified endpoint management solutions

Citrix Workspace app for Android now supports remote configuration of your Workspace Store URL using unified endpoint management solutions. As an administrator, you can manage store URLs remotely using the AppConfig-based key-value pairs using unified endpoint management solutions.

To configure your Workspace Store URL using unified endpoint management solutions, follow these steps:

Configure your store using unified endpoint management solutions

Citrix Workspace app for Android supports remote configuration of your Workspace Store URL using unified endpoint management solutions.

To remotely configure your Workspace Store URL using existing unified endpoint management solutions, follow these steps:

1. Sign in to your unified endpoint management solutions provider.
2. Create an app configuration policy for your app.
3. Add key and value pair to the JSON property list and fill in the following values:
   
   • **key**: url
   • **value type**: String
   • **value**: your store URL (for example, prodcwa.cloud.com)

   **Note:**
   
   • For demonstrative purposes, Microsoft Intune is used as the unified endpoint management solution in this example. The UI shown differs depending on your unified endpoint management solutions provider.

<table>
<thead>
<tr>
<th>Configuration key</th>
<th>Value type</th>
<th>Configuration value</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>String</td>
<td>prodcwa.cloud.com</td>
</tr>
</tbody>
</table>
Limitations

- If a cloud store is already set up and the administrator configures a new cloud store, your existing cloud store and any associated data or settings are deleted. You receive a notification to inform you of the deletion in Citrix Workspace. You must then sign in again so that the new cloud store is added to Citrix Workspace.
- To apply new configurations, you must close and open Citrix Workspace app.

Support to configure store type

Starting with the 23.6.0 release, Citrix Workspace app for Android supports configuring store type using the AppConfig-based key-value pair to configure the Citrix Workspace app. Now, administrators can control how the app appears.

The following is the key-value pair:

- **key**: storeType
- **value type**: Integer
- **value**: 
  - If set to 1 (default), users can view the native or the default store loading.
  - If set to 2, users can view the store inside a web interface.

**Note:**
This feature doesn’t require enablement.

Control store configurations using unified endpoint management solutions

The Citrix Workspace app for Android started supporting remote configuration of the Workspace Store URL using unified endpoint management solutions from the 23.4.5 version. As an administrator, you can manage store URLs remotely using AppConfig-based key-value pairs using unified endpoint management solutions.

For more information, see Support for store configuration using unified endpoint management solutions.

Starting with the 23.7.5 version, administrators can configure if end users can modify store URLs using an AppConfig-based key-value pair:

- **key**: restrict_user_store_modification
- **value type**: Boolean
- **value**: 
  - If set to **true**, end users can’t modify the store (add or delete or edit).
Citrix Workspace app for Android

- If set to **false**, end users can modify the store.

**Note:**
If the flag `restrict_user_store_modification` is set to **true**, all the existing stores are deleted before adding a new unified endpoint management-configured store.

**Screenshot detection and prevention through Unified Endpoint Management solutions**

Starting with the 23.10.0 version, administrators can prevent end users from taking screenshots at the Citrix Workspace app level. This feature prevents sensitive or private information leaks. Administrators can configure this feature using an AppConfig-based key-value pair:

- **key**: restrictScreenshot
- **value type**: Boolean
- **value**:
  - If set to true, end users can’t take screenshots.
  - If set to false, end users can take screenshots.

**Peripherals**

November 3, 2023

**Client drive mapping**

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. So, you can use mass storage devices (For example, pen drives) to copy and paste documents between the pen drive and the user device.

**Feature limitations:**

- Android APIs are observed to be slow, which delays certain operations.
- CDM for external storage isn’t supported on Pixel devices.
Citrix Workspace app for Android

- File type association isn't supported on external storage devices.

**Known issue in the feature:**

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

**Client Drive Mapping enhancement**

Earlier a selected choice of device storage was applied on all configured stores.

Starting with the release 20.8.0, Citrix Workspace app allows you to select dedicated device storage for every configured store.

You get a prompt to select the type of device storage along with the store details at session launch. You can do one of the following:

- Select one of the device storage options and click **OK** - The choice is applied only to the current session. A prompt appears to select the type of device storage at every launch.
- Select one of the device storage options, select **Do not ask again**, and click **OK** - The choice is applied for all session launches for that store. No further prompts appear.
- Select **Cancel** - You’re prompted to select a type of device storage at every launch and within a session as well. The session does not have access to the device storage.

**Note:**

This feature applies only on direct ICA launches and Citrix Gateway configured stores. Stores with end-to-end SSL setup are 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.

The 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.
Citrix Workspace app for Android

**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 the [Citrix Ready workspace hub documentation](#).

**USB smart card**

Citrix Workspace app supports 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 cards are supported on the Android operating system from version 7.x through 11.x.

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

**Configuring a 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.
Support for webcam redirection

You can now redirect the front camera of your device into the session. Both 32-bit and 64-bit applications are supported. By default, the auto-redirection of the webcam is disabled.

Support for front and rear camera redirection

Citrix Workspace app for Android now allows you to switch the camera position from front to rear and conversely, within the HDX session. Both 32-bit and 64-bit applications are supported.

A floating button appears when you invoke the camera. A single tap on the floating button to switch between the front and rear camera positions. You can also move the floating button freely around the screen and place it anywhere.

Known issues in the feature

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

Support for external microphone

Previously, Citrix Workspace app for Android supported audio redirection through the device’s microphone only.

Starting with the 23.10.5 version, Citrix Workspace app for Android supports external microphones. Microphones can be USB or Bluetooth-based peripheral devices.

After you connect a USB or a Bluetooth microphone, the audio redirects from the external microphone to the session. When you remove the external microphone from the device, the audio automatically redirects to the device’s microphone.

This feature is helpful when you connect an external microphone, for example, to a:

- phone
- tablet
- smart TV
- external monitor in a conference room.

Extend display

November 9, 2023
Citrix Workspace app for Android

Support for Zebra workstation connect

With this release, we introduce compatibility with Zebra tablet features - desktop launcher and experience in desktop mode. The user experience of the Android tablet is mirrored on the client monitor with the Zebra Workspace Connector.

Citrix Workspace app supports the following Zebra devices:

- EC50, EC55, ET56 Mobile Computers
- TC52x,
- TC57x,
- TC52ax,
- TC52x-HC
- TC52ax-HC

For more information on managing the zebra device, see Manage Zebra Android devices in the Citrix Endpoint Management documentation.

Multi-display support on Samsung DeX

Samsung DeX (Desktop eXperience) is available on some high-end Samsung handheld devices. The DeX feature enables you to extend your device into a desktop-like experience by connecting a keyboard, mouse, and monitor.

You can connect your DeX-enabled device and the external display to extend the desktop session onto the external display. The external display must support the DeX protocol. You can either extend or display different content on the Samsung DeX screen and the external display.

Important:

- This feature applies only to the Samsung DeX platform and not for ChromeOS or other Android devices.
- This feature is only for Citrix desktop sessions and not for app sessions.
- The Extend icon is available only on the DeX screen. Start the desktop session from the DeX screen.
- The external display resolution depends on the Samsung DeX device, the external display, and the other hardware used.

Configure Extend mode

To enable the Extend mode:

1. Connect the device that has the Samsung DeX protocol to the external monitor using the cable. You can also connect the Samsung DeX capable device to the Samsung monitor. The Samsung monitor must support the DeX protocol in the wireless mode.
Citrix Workspace app for Android

Note:
The setup works best with USB type-c HDMI and USB-C Dock adapters.

2. Open Citrix Workspace app and start a desktop session from the Samsung DeX screen.

3. Navigate to the toolbar and tap the **Extend** icon.

   Tip:
   To remove the screen extension, tap the **Extend** icon again.

4. Use the drag and drop feature to move the application window to the external monitor.

   Limitation:
   Release the mouse pointer at the screen edge when you drag a window to another display. Continue the drag and drop action using a mouse from the target display to move the window.

   Note:
   • You can rotate the device screen to suit your needs.
   • Adjust the font size for readability in session display settings under the **Scale and layout** section.

Configure display arrangement

To configure the display arrangement:

Prerequisite:
Configure the display arrangement before you start the session.

1. Open Citrix Workspace app and navigate to the **Settings icon > Settings > General > Display > Display Arrangement.**
2. Select a suitable option.
   The device display appears either on the right or on the left.

   **Important:**
   - The Samsung DeX screen is the primary display.
   - Only one screen can display the Citrix Workspace app UI.
   - You can plug in only one external display.
   - Citrix Workspace app closes when you start a session.

**User experience**

**Inactivity timeout for Citrix Workspace app sessions**

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

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

When you’ve reached the specified time-out value, the end-user experience is as follows depending on the authentication type configured:
Citrix Workspace app for Android

- After the inactivity timeout, you’ll receive a prompt to provide biometric authentication to access the Citrix Workspace app again.

- If you can cancel the biometric authentication prompt, the following message appears:

  Citrix Workspace app is locked.
  You must authenticate to continue to use the Workspace app.

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

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

**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.”

To disable the error message relating to network issues in a session, go to Advanced and select the Disable network monitoring messages option.

**User interface enhancement**

- Starting with the 20.7.0 release, you can remove the store account details from the Edit option. Click Remove account to remove the account details.

- Starting with the 20.7.5 release, the Recent tab displays the native mobile apps along with the published apps and desktops.

- Starting with the 20.10.0 release, Citrix Workspace app supports Google Play’s current target API requirements for Android 10.

- Starting with the 20.10.0 release, you receive a notification about a non-secure connection when you try to add an HTTP store.

- Starting with the 21.3.5 release, you can navigate back and forth within web and Software-as-a-Service (SaaS) apps.

  The navigation buttons appear at the bottom left of your workspace web and SaaS app session of your mobile phone.
The navigation buttons appear at the top left of your SaaS app session of your tablet.

- Starting with the 21.4.0 release, you can search for words or phrases within your web and Software-as-a-Service (SaaS) apps.

To search, follow these steps.

1. Tap the ellipsis button on the bottom right and select **Find in page**.
2. The keyboard appears.
3. On typing, your search result appears (for example, the word “imagine”).

- Starting with the 21.6.0 release, you can download text, audio, and video files (with and without direct links). For text, audio, and video files with direct links, download directly by tapping the link. You can preview the audio and video files before downloading them.

To download files without direct links, tap the ellipsis button on the bottom right and select Download.
After the download completes, a notification indicates that the file is saved in your downloads folder.
• Starting with the 21.8.5 release, we now support Android 12 Beta 4 in the Citrix Workspace app for Android. Upgrading to Citrix Workspace app version 21.8.5 ensures uninterrupted support for devices that are updated to Android 12 Beta 4.

• Starting with the 21.9.0 release, the Citrix Workspace app supports Android 12 Beta 4. If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

• Starting with the 22.2.0 release, you can access a list of recently launched apps for quick access when you use the long-press gesture on the Citrix Workspace app icon.

Google Assistant integration

You can interact with the Google Assistant to launch resources like apps and desktops without launching the Citrix Workspace app each time. All the recently accessed resources are listed under Google Assistant shortcuts. Select the ones that you prefer to add as a shortcut.

To configure:

1. Launch the Citrix Workspace app and open a resource you want to add as the shortcut.
2. Open Google Assistant settings from your device.
Accessing Google Assistant settings can vary depending upon the Android version and the Android device you use.

As a tip, use the voice command to open the Google Assistant settings.

3. Scroll and tap **Shortcuts**.

4. Tap **Citrix Workspace app** and select the resource you want to add as a shortcut.

You can now use voice commands to launch the resource.

5. (Optional) You can edit and update the voice command.

---

**Session experience**

November 9, 2023

**Enlightened Data Transport (EDT)**

In earlier releases, session launches were unsuccessful when Enlightened Data Transport (EDT) connections can’t be established between Citrix Gateway and the VDA. Starting with the 21.5.0 release, unsuccessful EDT connections fall back to TCP.
**EDT stack parameters enabled by default**

Starting with the 21.7.0 release, the EDT stack parameters are enabled by default. As a result, we've removed the EDT Stack Parameters option from Settings > Advanced.

To date, the option to disable EDT stack parameters was available to users. With this option available, not all clients were following custom EDT Maximum Segment Size (MSS) requirements consistently. As a result, fragmentation occurred with degradation in HDX performance and issues in establishing sessions for these clients. With EDT stack parameters newly enabled by default, the overall user experience and satisfaction is now enhanced.

**Parallel connection**

Starting with the 21.7.0 release, we've are introducing the EDT and TCP parallel connection feature. The feature results in decreased connection times.

Earlier, when establishing a connection, the Citrix Workspace app would try to connect using EDT. Unsuccessful EDT connection attempts would fall back to TCP causing the following issues that are now addressed:

- Increased connection time in fallback scenarios.
- Session reliability and Auto client reconnect tended to favor TCP.
- Required a connection break to try TCP again.

**MTU Discovery capabilities added to EDT**

We've added Maximum Transmission Unit Discovery capabilities to Enlightened Data Transport (EDT). As a result, you can now enjoy a consistently stable HDX experience, delivered by EDT.

Earlier, EDT failed in several scenarios such as VPN, Wi-Fi, 4G or 3G connections, and on Microsoft Azure, caused by packet loss because of packet size.

When you tried to launch a session, packet fragmentation caused sessions to drop. As a workaround, it was necessary to adjust the EDT MSS (Maximum Segment Size) in the StoreFront file, which meant extra configuration. The addition of MTU Discovery capabilities added to EDT resolves and addresses these issues.

MTU Discovery capabilities added to EDT work in sessions hosted on 1912 VDA and later.

**Auto-launch of ICA file**

You can launch your published apps and desktops by clicking the resource. This feature requires StoreFront (on-premises) Version 1912 or later.
Citrix Workspace app for Android

**Note:**

- Auto-launch of ICA files is supported only on Chromebook devices and only for HTTPS store URLs.
- Don’t select the **Remember my choice** option when you launch a resource.

**Enhanced session launch**

Published apps and desktops are launched in separate windows. This enhancement helps you to use and interact with the store enumeration window without having to disconnect or log off from the session.

**Note:**

- This feature is supported only on Chromebook devices.
- This feature isn’t 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.

**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 isn’t displayed for server VDA.

**Embedded Citrix HDX RealTime Media Engine**

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**.
Citrix Workspace app for Android

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

This feature is supported on:

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

**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.

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

**USB device redirection**

Starting with Version 20.9.0, the USB redirection feature is fully functional and ready for general availability. By default, the USB redirection feature is disabled.

This feature allows the redirection of arbitrary USB devices from client machines to Citrix Virtual Apps and Desktops and Citrix DaaS. It allows you to interact with a wide selection of generic USB devices in a session, as if they were physically plugged into it.

As a prerequisite to manage this feature using the Citrix Global App Config Service, set the USB redirection feature to Enabled on the Delivery Controller. For more information on how to configure USB redirection on the Delivery Controller, see the Generic USB devices section in the Citrix Virtual Apps and Desktops documentation.

The Citrix Global App Configuration Service gives Citrix administrators the ability to deliver Citrix Workspace service URLs and Citrix Workspace app settings through a centrally managed service.

The USB redirection feature is integrated with and configurable through the Citrix Global App Config Service. You can manage the feature using the Citrix Global App Config Service for non-domain joined networks.

For information on configuring the feature using this method, see Global App Configuration Service in the developer’s documentation.

**Note:**

This feature is ready for general availability starting with Version 20.9.0. In Versions 20.8.1 and earlier, it’s available on-demand only.

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

**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, the Chrome operating system blocks the USB devices (for example, pen drives). Allow the list of devices using the Google admin console for managed Chromebooks.

For information on how to allow the list of 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 mobile 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 follows:
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 follows:
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 follows:
Citrix Workspace app for Android

Note:
If a USB device isn’t listed, verify that you’ve whitelisted it.

For information on how to allow list of 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’s displayed in the **Devices** section in the control panel.

**Tested USB devices**

<table>
<thead>
<tr>
<th>Device</th>
<th>Manufacturer</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer</td>
<td>HP</td>
<td>LaserJet P2014</td>
</tr>
<tr>
<td>Scanner</td>
<td>HP</td>
<td>Scanjet G3010</td>
</tr>
<tr>
<td>Scanner</td>
<td>Canon</td>
<td>CanoScan LiDE 700F</td>
</tr>
<tr>
<td>Space Navigator</td>
<td>3Dconnexion</td>
<td></td>
</tr>
<tr>
<td>Printer</td>
<td>Brother</td>
<td>QL-580N</td>
</tr>
<tr>
<td>Scanner</td>
<td>HP</td>
<td>Scanjet 200</td>
</tr>
</tbody>
</table>

**Known issues:**
Citrix Workspace app for Android

- Only one USB device is supported at a time.
- Audio and video USB devices aren’t currently supported.

**Auto-redirection of USB devices**

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 supports only if the USB device redirection feature is enabled.

**Enhancements to audio redirection**

Previously, audio redirection in a desktop session required multiple levels of microphone settings, and the steps to set the permissions weren’t intuitive. Now, microphone permission settings are simplified and are user friendly. You can also enable the permissions while you are in a session.

By default, the audio toggle under **Citrix Workspace app > Settings > Audio** is enabled. The session can now detect the speaker that is already connected. Administrators can enable or disable audio redirection using the **Global App Configuration Service**.

**Note:**
By default, the microphone permission is disabled on both the Citrix Workspace app setting and on the store setting page.

You might come across one of the following scenarios when either the Citrix Workspace app or the store disables the microphone:

- When both Citrix Workspace app and Store settings disable the microphone permission, the **Allow Workspace to record audio** pop-up message appears as you start the desktop session and use the microphone. Tap **While using the app**.
- When Citrix Workspace app enables, but Store settings disable the microphone permission, the **Allow access to microphone** pop-up message appears as you start the desktop session and use the microphone. Tap **Allow**.

**Keyboard layout synchronization**

Citrix Workspace app allows you to enable the keyboard layout synchronization under **Settings > General > Keyboard > Keyboard Layout Sync.**
The **Keyboard Layout Sync** option allows automatic keyboard layout synchronization between the VDA and the client device.

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

To enable dynamic keyboard layout synchronization, set the **Keyboard Layout Sync** option to **On**.

When the **Keyboard Layout Sync** option is disabled, both the VDA-side (remote) IME and the client-side IME take effect depending on your device's current input method. For example, if the client-side IME is in English and the VDA-side IME is in Japanese, the VDA-side IME (remote) takes effect.

When the **Keyboard Layout Sync** option is enabled, the client-side IME takes precedence. If you change the input language at the client-side IME, the VDA-side IME changes accordingly. For example, if you change the client-side IME to Japanese, the VDA-side IME automatically changes to Japanese. At the same time, Japanese IME on your client device is used during the session.

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

**Feature Limitations:**
- This feature works only on soft keyboards on the devices, not on external keyboards.
- Keyboard layout synchronization does not support Gboard (the Google Keyboard).
- The keyboard layout can only be synced from the client to the server. When changing the server-side keyboard layout, the client keyboard layout can't 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 can't be confirmed.

**Keyboard layout support for Windows VDA and Linux VDA**

<table>
<thead>
<tr>
<th>Keyboard layout on Android</th>
<th>Keyboard Language</th>
<th>Keyboard Layout on Windows</th>
<th>Keyboard Layout on Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belarusian (Belarus)</td>
<td>Belarusian (Belarus)</td>
<td>Belarusian (Belarus) Keyboard</td>
<td>by</td>
</tr>
<tr>
<td>Bulgarian</td>
<td>Bulgarian</td>
<td>Bulgarian (Typewriter) keyboard</td>
<td>bg</td>
</tr>
<tr>
<td>Chinese (Simplified)</td>
<td>Chinese (Simplified, China)</td>
<td>Citrix IME - Chinese (Simplified, China)</td>
<td>zh</td>
</tr>
</tbody>
</table>

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Keyboard layout on Android</th>
<th>Keyboard Language</th>
<th>Keyboard Layout on Windows</th>
<th>Keyboard Layout on Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese (Traditional)</td>
<td>Chinese (Traditional, Taiwan)</td>
<td>Citrix IME - Chinese (Traditional, Taiwan)</td>
<td>tw</td>
</tr>
<tr>
<td>Croatian</td>
<td>Croatian (Croatia)</td>
<td>Croatian keyboard</td>
<td>hr</td>
</tr>
<tr>
<td>Czech</td>
<td>Czech</td>
<td>Czech keyboard</td>
<td>cz</td>
</tr>
<tr>
<td>Danish</td>
<td>Danish</td>
<td>Danish keyboard</td>
<td>df</td>
</tr>
<tr>
<td>Dutch</td>
<td>Dutch (Netherlands)</td>
<td>United States-International keyboard</td>
<td>us</td>
</tr>
<tr>
<td>Dutch (Belgium)</td>
<td>Dutch</td>
<td>Belgian (Period) Keyboard</td>
<td>be</td>
</tr>
<tr>
<td>English (Australia)</td>
<td>English (Australia)</td>
<td>US keyboard</td>
<td>us</td>
</tr>
<tr>
<td>English (Canada)</td>
<td>English (Canada)</td>
<td>US keyboard</td>
<td>us</td>
</tr>
<tr>
<td>English (UK)</td>
<td>English (United Kingdom)</td>
<td>United Kingdom keyboard</td>
<td>gb</td>
</tr>
<tr>
<td>English (US)</td>
<td>English (United States)</td>
<td>US keyboard</td>
<td>us</td>
</tr>
<tr>
<td>Estonian</td>
<td>Estonian</td>
<td>Estonian keyboard</td>
<td>ee</td>
</tr>
<tr>
<td>Finnish</td>
<td>Finnish</td>
<td>Finnish keyboard</td>
<td>fi</td>
</tr>
<tr>
<td>French (Canada)</td>
<td>French (Canada)</td>
<td>French Keyboard</td>
<td>fr</td>
</tr>
<tr>
<td>French (Switzerland)</td>
<td>French (France)</td>
<td>Swiss French Keyboard</td>
<td>ch</td>
</tr>
<tr>
<td>French (France)</td>
<td>French (France)</td>
<td>French Keyboard</td>
<td>fr</td>
</tr>
<tr>
<td>German (Austria)</td>
<td>German (Austria)</td>
<td>German keyboard</td>
<td>at</td>
</tr>
<tr>
<td>German (Switzerland)</td>
<td>German (Switzerland)</td>
<td>Swiss German keyboard</td>
<td>ch</td>
</tr>
<tr>
<td>German (Germany)</td>
<td>German (Germany)</td>
<td>German keyboard</td>
<td>at</td>
</tr>
<tr>
<td>Greek</td>
<td>Greek</td>
<td>Greek keyboard</td>
<td>gr</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hungarian</td>
<td>Hungarian keyboard</td>
<td>hu</td>
</tr>
<tr>
<td>Icelandic</td>
<td>Icelandic</td>
<td>Icelandic keyboard</td>
<td>is</td>
</tr>
<tr>
<td>Irish</td>
<td>Irish</td>
<td></td>
<td>ie</td>
</tr>
<tr>
<td>Italian</td>
<td>Italian (Italy)</td>
<td>Italian keyboard</td>
<td>it</td>
</tr>
<tr>
<td>Keyboard layout on Android</td>
<td>Keyboard Language</td>
<td>Keyboard Layout on Windows</td>
<td>Keyboard Layout on Linux</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Japanese</td>
<td>Japanese</td>
<td>Citrix IME - Japanese</td>
<td>jp</td>
</tr>
<tr>
<td>Korean</td>
<td>Korean</td>
<td>Citrix IME - Korean</td>
<td>kr</td>
</tr>
<tr>
<td>Latvian</td>
<td>Latvian</td>
<td>Latvian keyboard</td>
<td>lv</td>
</tr>
<tr>
<td>Norwegian</td>
<td>Norwegian (Bokmål)</td>
<td>Norwegian keyboard</td>
<td>no</td>
</tr>
<tr>
<td>Polish</td>
<td>Polish</td>
<td>Polish (Programmers) keyboard</td>
<td>pl</td>
</tr>
<tr>
<td>Portuguese (Brazil)</td>
<td>Portuguese (Brazil)</td>
<td>Portuguese (Brazil ABNT) keyboard</td>
<td>br</td>
</tr>
<tr>
<td>Portuguese (Portugal)</td>
<td>Portuguese (Portugal)</td>
<td>Portuguese keyboard</td>
<td>pt</td>
</tr>
<tr>
<td>Romanian</td>
<td>Romanian (Romania)</td>
<td>Romanian (legacy) keyboard</td>
<td>ro</td>
</tr>
<tr>
<td>Russian (Russia)</td>
<td>Russian</td>
<td>Russian keyboard</td>
<td>ru</td>
</tr>
<tr>
<td>Slovak</td>
<td>Slovak</td>
<td>Slovak keyboard</td>
<td>sk</td>
</tr>
<tr>
<td>Slovenian</td>
<td>Slovenian</td>
<td>Slovenian keyboard</td>
<td>si</td>
</tr>
<tr>
<td>Spanish (Mexico)</td>
<td>Spanish (Mexico)</td>
<td>Latin American keyboard</td>
<td>latam</td>
</tr>
<tr>
<td>Spanish (Spain)</td>
<td>Spanish (Spain)</td>
<td>Spanish keyboard</td>
<td>es</td>
</tr>
<tr>
<td>Swedish (Sweden)</td>
<td>Swedish (Sweden)</td>
<td>Swedish keyboard</td>
<td>se</td>
</tr>
<tr>
<td>Turkish</td>
<td>Turkish</td>
<td>Turkish F keyboard</td>
<td>tr</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>Ukrainian</td>
<td>Ukrainian keyboard</td>
<td>ua</td>
</tr>
</tbody>
</table>

**Service continuity**

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services.

For more information, see the Service continuity section in the Citrix Workspace documentation.

**App switch**

This feature enables an end user to switch between many published apps that are in the same session. When you tap the Switch icon, you can scroll to select an app and the app that is in focus is highlighted. You can view the app title, preview image, and window title.
Citrix Workspace app for Android

When you open or close an app, the app count updates accordingly. If some apps are opened in another session, the app count includes all the opened ones.

![App count update](image)

**Support for full-screen display**

Starting with the 23.8.0 version, the H264 codec supports improved video rendering in full screen mode. If you’re a frequent consumer of videos or heavily depend on video content, this feature is recommended for you. It’s designed to improve your video experience for performance, video quality, and resource utilization.

**Configuration**

On the DDC machine set the policy **Use video codec for compression** to **For the entire screen** to improve video compression up to 60FPS.

![Configuration setting](image)

**Addition of Ctrl+Alt+Del shortcut in session toolbar**

Starting from the 23.9.5 version, the session toolbar has an option to do the Ctrl+Alt+Del function with the tap of a button. This option facilitates users to sign out, switch users, lock the device, or access the Task Manager.
Support for full-screen mode for app sessions

Previously, when you started an app session, you could view it in windowed mode.

Starting from the 23.9.5 version, Citrix Workspace app for Android introduces a new option to view the app session in full-screen mode. This feature is helpful when you:

- start a session in full immersion mode with touch devices
- try to duplicate the screen and cast it
- view the Citrix Workspace app on a smaller screen.

To enable the option, go to Citrix Workspace app for Android [Settings] > [Advance] > [Fullscreen Window] and toggle on. The following screenshot displays the option:
Accessibility and TalkBack

Citrix Workspace app provides an enhanced user experience with the TalkBack feature. The TalkBack feature helps end users who have difficulty seeing the screen. The narrator reads the screen elements aloud when using the UI.

To use the Android talkback feature, end users must enable it from Android Settings > Accessibility > Talkback.

For more information, see Accessibility and TalkBack in the help documentation.

Known issues in the feature

- When you attach an external keyboard to your device:
  - To use the CapsLock key as the narrator key, the action might not work as expected. As a workaround, press the Insert key. [HDX-55347]
  - To use the key combination Win+Ctrl+Enter to enable the narrator, the action doesn’t take effect inside the virtual desktop session. As a workaround, use the Win key or the Start menu and enter the word Narrator. [HDX-55380]

Store experience

September 20, 2023
Unauthenticated users

Citrix Workspace app supports unauthenticated (anonymous) users. Anonymous users can launch Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sessions successfully.

Security settings

Citrix recommends using stores that are secure. Besides, it’s a good practice to have HTTP strict transport security (HSTS) setting enabled for secure stores.

Do the following steps to enable the HSTS setting:

1. In Citrix StoreFront, under Stores, click the link of the particular store to enable the security settings.
2. The Manage Receiver for Web Sites dialog box appears.
3. Click Configure.
4. The Edit Receiver for Web site dialog box appears.
5. Click the Advanced Settings tab and select Enable strict transport security.

Authenticate

November 3, 2023

Smart cards

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
- SMS Passcode (one-time PIN) authentication
- Smart card authentication

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

**Smart card readers:**

- BaiMobile 3000MP USB Smart Card Reader

**Smart cards:**

- PIV cards
- Common Access Cards
Citrix Workspace app for Android

Configurations:

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

Note:

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

How to use smart cards

Prerequisite

- Install C4E app from play store to use smart cards. Contact android@citrix.com for licenses.

To use smart cards to access apps:

1. If you want to configure Citrix Workspace app automatically to access apps when you create an account, in the Address field, enter the valid URL of your store. For example:
   - StoreFront.organization.com
   - netscalervserver.organization.com

2. Insert the smart card along with the supported reader to your Android device. The Citrix Workspace app automatically detects the smart card.
3. Select the **Use Smartcard** option to authenticate.

**Note:**
- Your access to the store stays valid for approximately one hour. After that time, you must sign in to refresh your access or start other apps.

**Support for FIDO2-based authentication**

Starting with the 23.8.0 version, Citrix Workspace app for Android now supports password-less authentication within a Citrix Virtual Apps and Desktops session using FIDO2-based authentication methods.

This feature allows users to sign in to a WebAuthn-supported website in browsers. For example, Google Chrome or Microsoft Edge using FIDO2-supported platform authenticators such as fingerprint, and device PIN. Simply opening a WebAuthn-supported website triggers password-less authentication.

Signing in to the Citrix Workspace app or desktop session using password-less authentication isn’t supported on FIDO 2.
Citrix Workspace app for Android

Note:

- Roaming authenticators such as YubiKey, or Smart Card aren’t supported in Citrix Workspace app for Android.

For more information about the prerequisites for this feature, see Local authorization and virtual authentication using FIDO2 in the Citrix Virtual Apps and Desktops documentation.

Secure

September 25, 2023

ProGuard enabled for security

We’ve enabled ProGuard to make Citrix Workspace for Android secure through obfuscation. ProGuard renames different parts of the code to prevent inspection of stack traces and makes the Workspace app secure. ProGuard also reduces the app size by shortening the names of app classes, methods, and fields.

Cryptography

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.

The TLS_RSA_ cipher suites have been removed. The releases 20.6.5 and later supports advanced TLS_ECDHE_RSA_ cipher suites. If your environment isn’t configured with the TLS_ECDHE_RSA_ cipher suites, you can’t launch 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
TLS v1.3 supports the following cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

**Support for Transport Layer Security 1.3**

Citrix Workspace app for Android now supports Transport Layer Security (TLS) 1.3. It boosts performance and efficiency. TLS 1.3 provides robust security with its strong cipher suites and one-time session keys.

End users can enable it on Citrix Workspace app for Android as follows:

1. Go to Citrix Workspace app **Settings > TLS version**.
2. Tap the **Select protocol version** option and select **TLS v1.3**.
Citrix Workspace app for Android

For more information, see Cryptography
For more information on help documentation, see TLS version.

Troubleshoot

September 20, 2023

How to collect logs

To collect logs, follow these steps.

1. Tap Settings.

2. Under Help and Support, tap Send feedback to Citrix (Includes logs).
3. Tap **Workspace**.

1. Under **Report an issue**, tap **Log Options**.
2. Then, tap **Level**.

3. Select **Low**, **Medium**, or **Verbose** level. (Default level is low for basic activity tracking. Modify the level only if recommended by your help desk).

**How to provide feedback**

You can send us feedback about Citrix Workspace app for Android and report issues using the same interface. To send feedback:

1. Click Settings > **Send feedback to Citrix**.

   The **Report an issue** dialog appears.
Using the Report an issue dialog, you can:

- Request help from Support
- Report an issue
- Send issue logs

SDK and API

November 9, 2023

Citrix Virtual Channel Software Development Kit (SDK)

The Citrix Virtual Channel SDK supports writing server-side applications and client-side drivers for other 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 supports 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 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 the SDK documentation, see Citrix Virtual Channel SDK for Citrix Workspace app for Android.