



Citrix Workspace app for Android

Contents

| | |
|---|------------|
| Citrix Workspace app for Android | 2 |
| About this release | 2 |
| Features in Technical Preview | 10 |
| Citrix Workspace app for Android 24.8.0 - Preview | 12 |
| Prerequisites for installing | 12 |
| Install, Upgrade | 17 |
| Get started | 17 |
| Configure | 21 |
| Configure Citrix Workspace app using Unified Endpoint Management solutions | 37 |
| Peripherals | 52 |
| Extend display | 59 |
| User experience | 62 |
| Session experience | 69 |
| Store experience | 89 |
| Authenticate | 89 |
| Secure | 93 |
| Troubleshoot | 97 |
| SDK and API | 105 |
| Deprecation | 106 |

Citrix Workspace app for Android

March 11, 2024

Citrix Workspace app for Android provides on-the-go tablet and phone access to:

- Virtual apps and desktops.
- Touch-enabled apps for low-intensity use of tablets as alternatives to desktop computers.

The preferred method to update or install Citrix Workspace app for Android is from [Google Play](#) using an Android device. Automatic updates are allowed when new versions are available.

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

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

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

Language support

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

Legacy documentation

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

About this release

July 25, 2024

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 24.7.0

Support for adaptive audio

Citrix Workspace app for Android supports HDX adaptive audio. This feature is designed to provide users with exceptional audio quality and low latency.

For more information about configuration and limitations, see [Support for adaptive audio](#).

Add many stores using UEM

Administrators can now use Unified Endpoint Management (UEM) solutions to configure many stores for managed Android devices.

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.

For more information about the configuration, see [Add many stores using UEM](#).

Jailbroken devices

Your users can compromise the security of your deployment by connecting with jailbroken Android devices. Jailbroken devices are those devices whose owners have modified them, usually with the effect of bypassing certain security protections. When Citrix Workspace app for Android does a basic detection of a jailbroken Android device, the app displays an alert to the user.

For more information, see [Jailbroken devices](#).

Enhancement to support desktop-like experience in a single session on Samsung DeX

Previously, Citrix Workspace app supported seamless multi-tasking and provided users with a desktop-like experience. It allows you to open multiple apps within the same session to run simultaneously. These apps opened in separate windows.

Starting from the 24.7.0 release, end users can open a separate window for session-sharing apps. This feature supports more than one local window, thus facilitating multi-tasking. Each window has a name for each virtual app. Users can open multiple virtual apps and native DeX apps on the DeX screen only. Active virtual apps and native DeX apps show up as active apps in the bottom taskbar with respective app names, on the DeX Screen only.

For more information, see [Enhancement to support desktop-like experience in a single session on Samsung DeX](#).

Support for App Protection

Starting with the Citrix Workspace app for Android 24.7.0 version, the App Protection feature is supported.

App Protection is a feature for the Citrix Workspace app that provides enhanced security when using Citrix Virtual Apps and Desktops published resources. This feature restricts the ability of clients to be compromised by screen-capturing malware. Also, prevents unauthorized screen captures, recordings, mirroring, screen sharing, and app switching.

Anti-screen capture feature is available for authentication processes, web or SaaS apps, and Citrix Virtual Apps and Desktops. Citrix Workspace app for Android doesn't allow you to take screenshots. When you try to capture a screen, you get a prompt that you aren't allowed to take screenshots.

The admins can choose to enable anti-screen capture for the following:

- Virtual Apps and Desktops
- Web and SaaS apps
- Authentication screens

Starting with the Citrix Workspace app for Android 24.7.0 version, the anti-screen capture feature is available by default. However, to enable the feature, do the configuration steps mentioned at the [Configuration](#) section.

Disclaimer:

App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). This means that App Protection policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.

Prerequisites

- Citrix Virtual Apps and Desktops Version 1912 LTSR or later.
- StoreFront version 1912 LTSR or Workspace.
- Citrix Workspace app for Android version 24.7.0 or later.
- A valid App Protection license

Limitations

- The App Protection policies are downloaded for each store. If a store has the policies downloaded and you are moving to another store for which the policies aren't downloaded, the anti-screen capture feature isn't protected in the new store.

- The anti-screen capture feature is not supported on the authentication screens when **ChromeCustomTab** is used. However, this feature is supported when using native authentication or WebView. The **ChromeCustomTab** is enabled by default on the Cloud stores and you can change it to WebView by changing the `AndroidWebViewType` to `webview` using the PowerShell module. For more information, see [Set-WorkspaceCustomConfigurations](#).

For more information, see:

- [System requirements](#)
- [Anti-screen capture](#)
- [Behavior when you open an app with anti-keylogging in Citrix Workspace app for Android](#)

Fixed issues in 24.7.0

There are no fixed issues in the release.

Known issues in 24.7.0

There are no new known issues in the release.

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](#).

24.5.0

What's new

Support for authentication using FIDO2 when connecting to a cloud store Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Face recognition, and Fingerprint only). This feature is compatible with Android version 9 and later.

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

Note:

This feature is enabled by default.

Document scanner If you're signed into Citrix Workspace app, you can use the document scanner feature to scan many documents and transfer those scanned documents to the virtual desktop session.

Note:

- This feature is enabled by default.

Prerequisites

- [Client drive mapping \(CDM\)](#) must be enabled for the store.
- Document scanner 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**.

For more information about how to use this feature, see [Document scanner](#) in the help documentation.

Deprecation announcement Starting with the 24.5.0 version, Citrix Workspace app for Android doesn't support Android OS versions 9, 10, and 11. For the best results, update Android devices to the latest Android operating system.

For more information, see [Deprecation](#).

Technical Preview

- [Audio redirection with external microphones](#).
- [Single sign-on for Microsoft Entra ID enabled VM](#)

Fixed issue

There are no fixed issues in this release.

24.4.0

What's new

This release addresses areas that improve overall performance and stability.

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

Fixed issues

Attempts to install Citrix Workspace app version 24.1.0 fail with an incompatible error. The issue occurs on certain Zebra devices that don't have a camera. [CVADHELP-24843]

24.3.5

What's new

This version includes enhancements to the log collection. The log file now contains more comprehensive information that can assist IT administrators and customer support teams in analyzing the scenario better.

Push Citrix Workspace app settings through UEM Previously, you could configure the store URL in the Citrix Workspace app.

Starting with this release, you can configure the Citrix Workspace app settings on the managed devices through any unified endpoint management (UEM) solutions tool that is deployed in your infrastructure.

Note:

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

For more information about configuration, see [Push Citrix Workspace app settings through UEM](#).

Fixed issues

There are no fixed issues in the release.

24.3.0

What's new

Support for biometric authentication after inactivity After the inactivity timer expires, the end user is asked to authenticate themselves using biometric features such as facial recognition and fingerprint scanning.

The most robust form of biometric authentication available to the end user depends on the OEM of their device, and they are prompted accordingly.

For more information about configuring inactivity timer, see [Inactivity timeout for Citrix Workspace app sessions](#).

Fixed issues

There are no fixed issues in the release.

Known issues

Known issues in 24.5.0

- When you start a virtual desktop session on a DeX-enabled device and click the **Extend** button from the session toolbar, the session gets disconnected, and the extended screen window closes.

The issue occurs on the external monitor setup when you use Citrix Workspace app for Android version 24.4.0 and a Samsung Galaxy Tab S9 Ultra with OneUI 6.0 device. [HDX-65584]

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-10263]

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 tapping the **Cancel** button. [RFANDROID-5397]

Known issues in 20.2.0

Attempts to reconnect fail when you tap **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 fails 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](#)

Deprecation

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

Legacy documentation

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

Features in Technical Preview

July 24, 2024

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

List of features in Technical Preview

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

| Title | Available from version | Enablement form (Click the icon) | Feedback form (Click the icon) |
|---|------------------------|---|---|
| Single sign-on for Microsoft Entra ID enabled VM | 24.5.0 |  |  |
| Audio redirection with external microphones | 24.5.0 |  |  |
| Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps | 22.3.5 |  |  |

Single sign-on for Microsoft Entra ID enabled VM

This feature is in technical preview from 24.5.0 release.

Citrix Workspace app for Android supports users signing in to Azure AD-joined VM devices using single sign-on authentication. For the first launch of Azure AD-joined virtual machines (VMs) in Citrix Workspace app, users are prompted to enter Azure account credentials for authentication. The subsequent VDA sign-ins happen automatically without prompting for credentials until the authentication token expires.

Notes:

- This feature is applicable only for Azure AD joined cloud stores.
- By, default, this feature is disabled. 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](#).

Audio redirection with external microphones

This feature is in technical preview from 24.5.0 release.

Previously, you could use only one audio device in the session. Starting with the 24.5.0 version, Citrix Workspace app for Android displays all available local audio devices in a session with their names. In addition, plug-and-play audio devices are also supported.

Notes:

- By, default, this feature is disabled. 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](#).

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](#).

Technical Preview to General Availability (GA)

| Feature name | General availability version |
|---|------------------------------|
| DPI matching | 24.1.0 |
| Push Citrix Workspace app settings through UEM | 24.3.5 |
| Document scanner | 24.5.0 |
| Support for adaptive audio | 24.7.0 |
| Support for multi-window session sharing apps on Samsung DeX | 24.7.0 |
| Separate session window from Citrix Workspace app for Samsung DeX | 24.7.0 |
| Add many stores using UEM | 24.7.0 |

Citrix Workspace app for Android 24.8.0 - Preview

July 24, 2024

Citrix Workspace app for Android 24.8.0 - Preview is coming soon. Look forward to the new features and resolved issues in the upcoming 24.8.0 release.

The generally available version of Citrix Workspace app for Android is 24.7.0. For more information on the current release, see [About this release](#).

Prerequisites for installing

May 31, 2024

System requirements and compatibility

Device requirements

Citrix Workspace app supports Android versions 12 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”
- “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

March 11, 2024

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](#)

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.

Configure stores for StoreFront just as you configure 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.

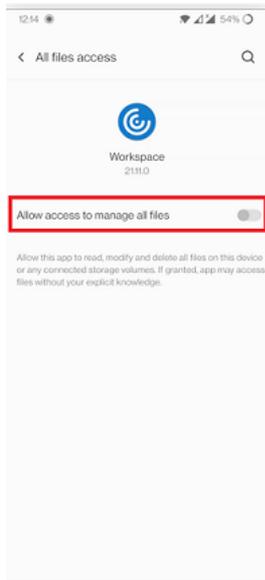
When your users create accounts on Citrix Workspace app, they need to enter their email address or the matching FQDN of your Citrix Gateway server. For example, if the connection fails when using the default path, enter the full path to the Citrix Gateway server.

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.



Configure

May 3, 2024

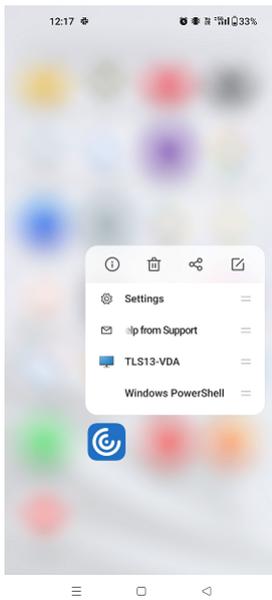
Microphone access for every store

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.

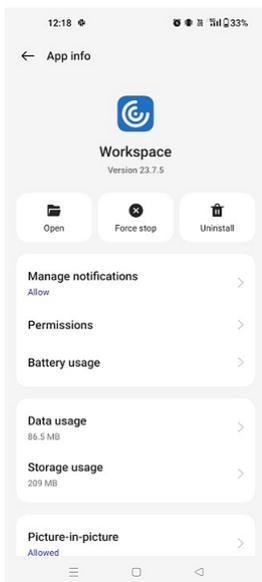
Previously, your setting for microphone access was applied on all configured stores.

Now, Citrix Workspace app requires the end user's permission for every store to access the microphone. Provide the permission to access the microphone as follows:

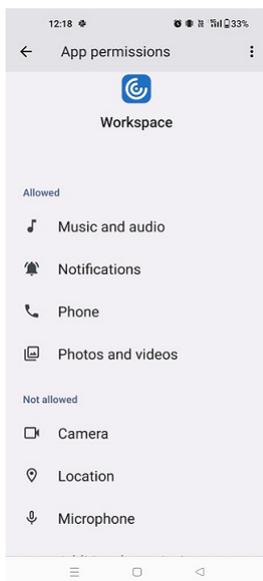
1. Long press on the Citrix Workspace app icon and tap the **App info**  icon.



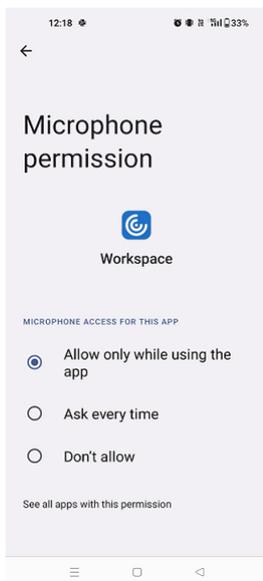
2. Tap **Permissions**.



3. Tap **Microphone**.



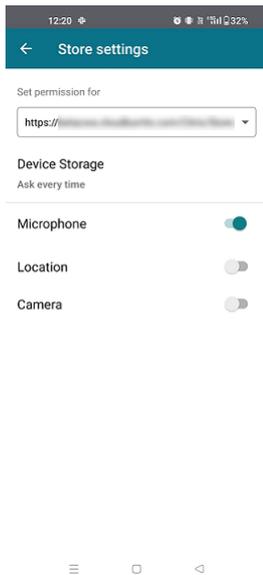
4. Select **Allow only while using this app**.



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.

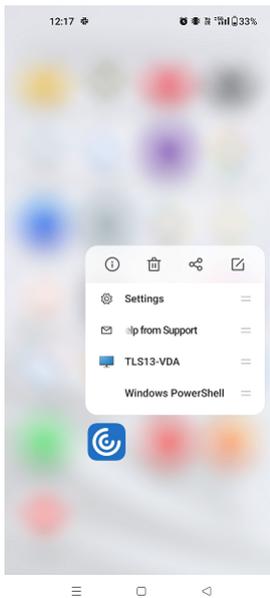
Location access for every store

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

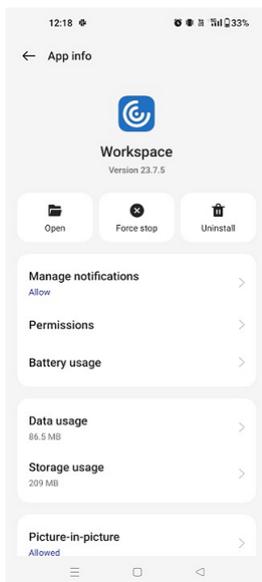
Previously, your setting for location access was applied on all configured stores.

Starting with the version 21.3.0, Citrix Workspace app requires the end user's permission for every store to access the location. Provide the permission to access the location as follows:

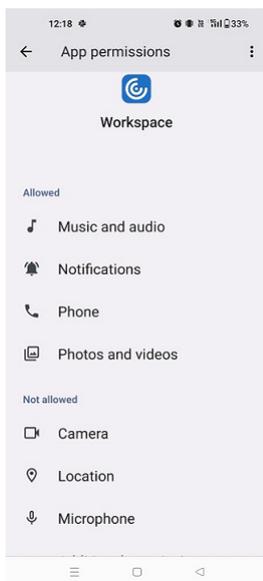
1. Long press on the Citrix Workspace app icon and tap the **App info**  icon.



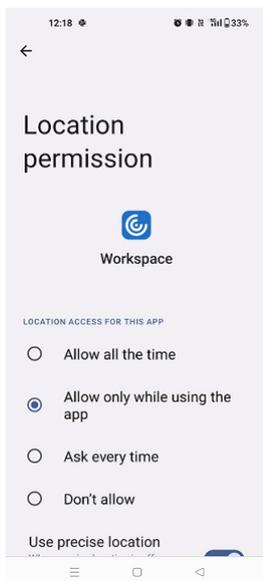
2. Tap **Permissions**.



3. Tap **Location**.



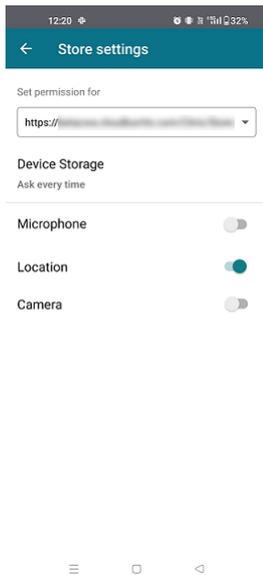
4. Select **Allow only while using this app**.



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.

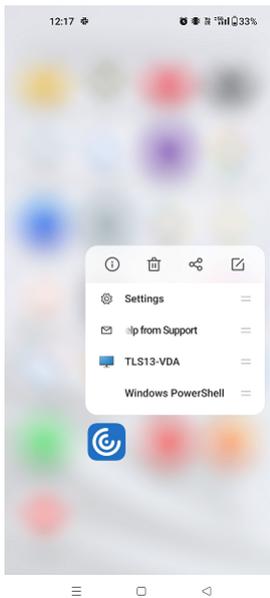
Camera access for every store

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.

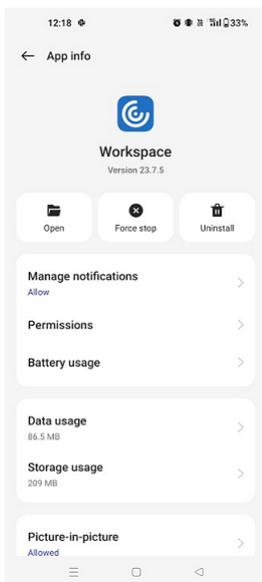
Previously, your setting for camera access was applied on all configured stores.

Now, Citrix Workspace app requires the end user's permission for every store to access the camera phone. Provide the permission to access the camera as follows:

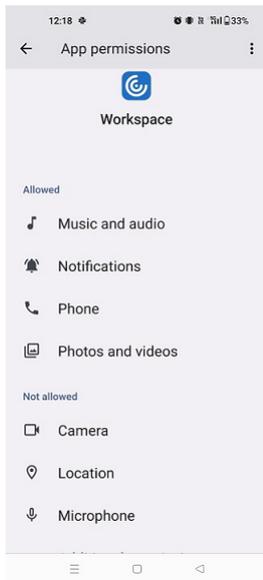
1. Long press on the Citrix Workspace app icon and tap the **App info**  icon.



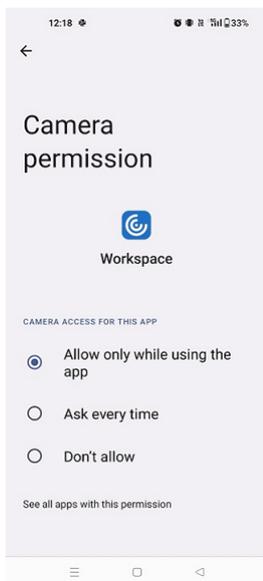
2. Tap **Permissions**.



3. Tap **Camera**.



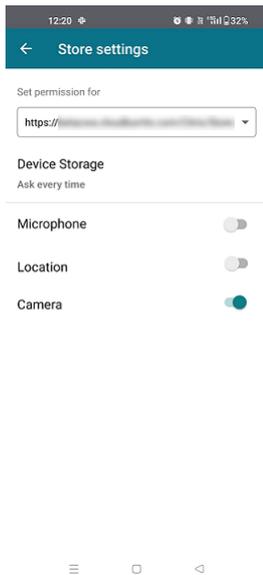
4. Select **Allow only while using this app**.



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.



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

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.

```
1      {
2
3          "assignedTo": [
4              "AllUsersNoAuthentication"
5          ],
6          "category": "Third Party Services",
7          "settings": [
8              {
9
10                 "name": "Enable Launch Darkly",
11                 "value": "true"
12             }
13         ],
14         "userOverride": false
15     }
16 }
```

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

On the on-premises deployment, do the following:

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

2. Locate the user account element in the file (Store is the account name of your deployment).

For example, `<account id=... name="Store">`. Before the `</account>` tag, navigate to the properties of that user account:

```
1 <properties>
2 <clear/>
3 </properties>
```

3. Add the **enableLaunchDarkly** tag and set the value as **false**.

```
<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 setting that applies for each session. 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 tap **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.

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.
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)

| Data collected | Description | What we use it for? |
|------------------------------|---|---|
| Configuration and usage data | The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app and automatically sends the data to Google Analytics for Firebase. | This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app. |

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:

| | | | |
|---|---------------------------------------|------------------------------------|--|
| Operating system version* | Workspace app version* | Authentication configuration | Device information |
| Session launch method | Citrix store type | Client drive-mapping configuration | |
| Session information | <code>Receiverconfig.txt</code> usage | USB redirection configuration | HDX RTME user info |
| HTTP and HTTPS connection configuration | ICA connections protocol info | Workspace app review action | Disable Firebase Configuration |
| Number of stores added | Screen capture action | RSA feature user actions | StoreFront Vs Workspace app user count |
| App update action | Operating system update | Screen view action | App remove |
| Web view connections | App clear data | App execution | App session start |

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 > tap POST**.

3. Tap **INVOKE API**.
4. Enter and upload the payload details. Enter the StoreFront store expiry date in the epoch timestamp in milliseconds format.

For example,

```
1  "migrationUrl": [  
2  {  
3  
4  
5  "url": "<cloud store url>"  
6  "storeFrontValidUntil": "<epoch timestamp in milliseconds>",  
7  }  
8  
9  ] ,
```

5. Tap **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 end users are on a lower version of Citrix Workspace app than the playstore version, the in-app prompt asks users 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 features and functionalities are well-tested before production.

Note:

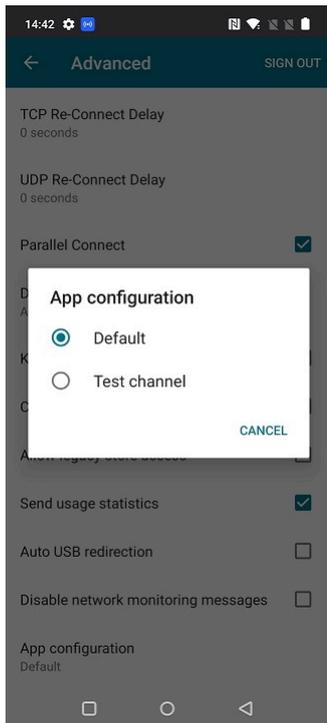
- The Citrix Workspace app for Android supports the **Default** and **Test channel** configurations. By default, all users are on the **Default** channel.

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

July 24, 2024

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 the key-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.

Settings [Edit](#)

| Configuration key | Value type | Configuration value |
|-------------------|------------|---------------------|
| url | String | prodcwa.cloud.com |

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).
 - ☒ 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.

Push Citrix Workspace app settings through UEM

Previously, you could configure the store URL in the Citrix Workspace app.

Starting with this release, you can configure the Citrix Workspace app settings on the managed devices through any unified endpoint management (UEM) solutions tool that is deployed in your infrastructure.

Note:

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

Configurations

The following JSON data is a sample from MS Intune that displays how to configure this feature.

```
1 {
2
3   "kind": "androidenterprise#managedConfiguration",
4   "productId": "app:com.citrix.Receiver",
5   "managedProperty": [
6     {
7
8       "key": "stores",
9       "valueBundleArray": [
10        {
11
12          "managedProperty": [
13            {
14
15              "key": "url",
16              "valueString": ""
17            }
18          ],
19          {
20
21            "key": "storeType",
22            "valueInteger": 1
```

```
23         }
24     ,
25     {
26         "key": "displayName",
27         "valueString": ""
28     }
29     ]
30     }
31     ]
32     }
33     ]
34     ]
35     }
36     ,
37     {
38         "key": "url",
39         "valueString": "prodcwa.cloud.com"
40     }
41     ,
42     {
43         "key": "storeType",
44         "valueInteger": 1
45     }
46     ,
47     {
48         "key": "displayName",
49         "valueString": ""
50     }
51     ,
52     {
53         "key": "restrict_user_store_modification",
54         "valueBool": false
55     }
56     ,
57     {
58         "key": "restrictScreenshot",
59         "valueBool": true
60     }
61     ,
62     {
63         "key": "appSettings",
64         "valueBundleArray": [
65             {
66                 "managedProperty": [
67                     {
68                         "key": "appSettings",
69                         "valueBundleArray": [
70                             {
71                                 "key": "appSettings",
72                                 "valueBundleArray": [
73                                     {
74                                         "key": "appSettings",
75                                         "valueBundleArray": [
```

```

76         "key": "name",
77         "valueString": ""
78     }
79     ,
80     {
81         "key": "value",
82         "valueString": ""
83     }
84     ,
85     {
86         "key": "userOverride",
87         "valueBool": false
88     }
89     ]
90 }
91 ]
92 ]
93 ]
94 ]
95 ]
96 ]
97 ]
98 ]
99 ]

```

Key value pair table

The following table provides the key value pair information:

| Setting | Description | Key | Value | Value type | Default Value |
|-----------------|--|---------------------------|--------|------------|-----------------|
| Audio | Allows users to control the audio and microphone connection within the app or desktop. | audioRecordingSettingsKey | record | String | Play and record |
| Predictive text | Enables text suggestions while the user is typing. | predictiveText | FALSE | Boolean | FALSE |

| Setting | Description | Key | Value | Value type | Default Value |
|---|---|----------------------|-------|------------|---------------|
| Extended keyboard | Enables support for the Extended keyboard in a session. | showExtendedKeyboard | TRUE | Boolean | TRUE |
| Generic USB Redirection | Enables automatic redirection of arbitrary USB devices from the client device to the VDA. | autoUSB | TRUE | Boolean | FALSE |
| Session Disconnect User Confirmation (Ask before exiting) | Prompts a confirmation dialog that allows the user to confirm before disconnecting any session. | askBeforeExiting | TRUE | Boolean | TRUE |
| Clipboard Redirection (Clipboard) | Allows the user to use clipboard operations, such as, Cut, Copy, and Paste in a session. | clipboardAccess | TRUE | Boolean | FALSE |

Citrix Workspace app for Android

| Setting | Description | Key | Value | Value type | Default Value |
|-------------------------------|---|-----------------------------|----------------|------------|---------------|
| Adaptive Transport (EDT) | Enables Enlightened Data Transport as a preferred protocol over TCP to optimize data transport. | edtSetting | TRUE | Boolean | TRUE |
| Display Orientation | Allows users to select the display orientation based on the device position. | displayOrientationKey | landscape mode | String | Automatic |
| Keep Display On | Keeps the display active and the screen on. | keepscreenOnKey | TRUE | Boolean | FALSE |
| Strict Certificate Validation | Enforces stricter control on the server certificate validation. | strictcertificatevalidation | TRUE | Boolean | FALSE |
| Legacy Store Access | Allows users to access earlier versions of the store. | allowlegacystoreaccess | TRUE | Boolean | FALSE |
| RealTime Media Engine | Enables support for high definition audio and video calls. | RTMEOAccess | TRUE | Boolean | FALSE |

Citrix Workspace app for Android

| Setting | Description | Key | Value | Value type | Default Value |
|-----------------------------|---|---------------------------|---|------------|---------------|
| Auto USB Redirection | Enables automatic redirection of arbitrary USB devices from the client device to the VDA. | autoUSB | TRUE | Boolean | FALSE |
| Network Monitoring Messages | Disables alert messages that provide details on the network performance. | DisableChannelMissWarning | FALSE | Boolean | FALSE |
| Extended Keys | Shortcuts to be used for the session keyboard. | key_map | ["strAltTab", "strAlt", "strBackspace", "strAltF4"] | MultiList | null |
| LaunchDarkly | Enables the LaunchDarkly flag on the Citrix Workspace app features. | enableLaunchDarkly | TRUE | Boolean | TRUE |

The following is an example JSON data. Here the example displays different setting values such as:

- Boolean
- Integer
- String
- List of strings

```
1 {
2
3   "kind": "androidenterprise#managedConfiguration",
4   "productId": "app:com.citrix.Receiver",
5   "managedProperty": [
6     {
7
8       "key": "stores",
```

```
9         "valueBundleArray": [  
10             {  
11                 "managedProperty": [  
12                     {  
13                         {  
14                             "key": "url",  
15                             "valueString": ""  
16                         }  
17                     },  
18                     {  
19                         {  
20                             "key": "storeType",  
21                             "valueInteger": 1  
22                         }  
23                     },  
24                     {  
25                         {  
26                             "key": "displayName",  
27                             "valueString": ""  
28                         }  
29                     }  
30                 ]  
31             }  
32         ]  
33     },  
34     {  
35         "key": "url",  
36         "valueString": "your_store_url"  
37     },  
38     {  
39         "key": "storeType",  
40         "valueInteger": 1  
41     },  
42     {  
43         "key": "displayName",  
44         "valueString": ""  
45     },  
46     {  
47         "key": "restrict_user_store_modification",  
48         "valueBool": false  
49     },  
50     {  
51         "key": "restrict_user_store_modification",  
52         "valueBool": false  
53     },  
54     {  
55         "key": "restrict_user_store_modification",  
56         "valueBool": false  
57     },  
58     {  
59         "key": "restrict_user_store_modification",  
60         "valueBool": false  
61     },  
62     {  
63         "key": "restrict_user_store_modification",  
64         "valueBool": false  
65     }  
66 ]  
67 }
```

```
62
63     "key": "restrictScreenshot",
64     "valueBool": true
65   }
66 ,
67   {
68
69     "key": "appSettings",
70     "valueBundleArray": [
71       {
72
73         "managedProperty": [
74           {
75
76             "key": "name",
77             "valueString": "showExtendedKeyboard"
78           },
79         ,
80         {
81
82           "key": "value",
83           "valueString": "false"
84         },
85         ,
86         {
87
88           "key": "userOverride",
89           "valueBool": false
90         }
91       ]
92     }
93   },
94   {
95
96     "managedProperty": [
97       {
98
99         "key": "name",
100        "valueString": "enterRegion"
101      },
102    ,
103    {
104
105      "key": "value",
106      "valueString": "-40"
107    },
108    ,
109    {
110
111      "key": "userOverride",
112      "valueBool": false
113    }
114  ]
115 }
```

```
115
116     ]
117   }
118 ,
119   {
120     "managedProperty": [
121       {
122         "key": "name",
123         "valueString": "displayOrientationKey"
124       },
125       {
126         "key": "value",
127         "valueString": "Landscape mode"
128       },
129       {
130         "key": "userOverride",
131         "valueBool": false
132       }
133     ]
134   },
135   {
136     "managedProperty": [
137       {
138         "key": "name",
139         "valueString": "askBeforeExiting"
140       },
141       {
142         "key": "value",
143         "valueString": "true"
144       },
145       {
146         "key": "userOverride",
147         "valueBool": false
148       }
149     ]
150   },
151   {
152     "managedProperty": [
153       {
154         "key": "name",
155         "valueString": "askBeforeExiting"
156       },
157       {
158         "key": "value",
159         "valueString": "true"
160       },
161       {
162         "key": "userOverride",
163         "valueBool": false
164       }
165     ]
166   },
167   {
```

```
168
169         "managedProperty": [
170             {
171                 "key": "name",
172                 "valueString": "key_map"
173             },
174             {
175                 "key": "value",
176                 "valueString": "['strAltTab','strAlt','strBackspace','strAltF4']"
177             },
178             {
179                 "key": "userOverride",
180                 "valueBool": true
181             }
182         ]
183     }
184 ]
185 }
186 ]
187 }
```

Add many stores using UEM

Administrators can now use Unified Endpoint Management (UEM) solutions to configure many stores for managed Android devices.

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.

```
1 {
2
3   "kind": "androidenterprise#managedConfiguration",
4   "productId": "app:com.citrix.Receiver",
5   "managedProperty": [
6     {
7
8       "key": "stores",
9       "valueBundleArray": [
10        {
11
12          "managedProperty": [
13            {
14
15              "key": "url",
16              "valueString": "test.cloud.com"
17            },
18            {
19
20              "key": "storeType",
21              "valueInteger": 1
22            },
23            {
24
25              "key": "displayName",
26              "valueString": "1"
27            }
28          ]
29        }
30      ]
31    },
32    {
33
34      "managedProperty": [
35        {
36
37          "key": "url",
38          "valueString": "test2.cloud.com"
39        }
40      ]
41    }
42  ]
43 }
```

```
41         }
42     ,
43     {
44         "key": "storeType",
45         "valueInteger": 2
46     }
47 ,
48 {
49     "key": "displayName",
50     "valueString": "2"
51 }
52 ]
53 }
54 ]
55 }
56 ]
57 }
58 ]
59 }
60 ,
61 {
62     "key": "restrict_user_store_modification",
63     "valueBool": false
64 }
65 ]
66 }
67 ]
68 }
```

Note:

- (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.

Home > Apps | App configuration policies >

Create app configuration policy

✔ Basics ✔ **Settings** ③ Assignments ④ Review + create

Permissions
Permissions granted here will override the "Default app permissions" policy for the selected apps.
[Learn more about Android runtime permissions](#)

+Add
Not configured

Configuration Settings
Configuration settings format ⓘ

Download JSON template

1

Connected apps
Enable users to connect this app across the work and personal profiles ⓘ
Enabled **Not configured**

This setting only works for personally-owned and corporate-owned work profile

Previous **Next**

Peripherals

July 24, 2024

Scancode input mode for external keyboard

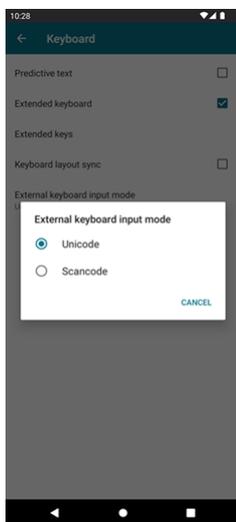
Starting with the 24.1.0 release, you can select Scancode as the keyboard input mode while using an external physical keyboard. This feature is helpful when you use Android devices with an external Windows PC's standard keyboard. Similar to using the Samsung DeX feature.

With Scancode, you can use the keyboard layout of the VDA instead of the Android's soft keyboard. In this way, you can completely follow the input style of Windows instead of Android. It's beneficial when typing in East-Asian languages, as it significantly improves the overall user experience. The end user might find themselves using the keyboard layout of the server instead of the client. For more understanding, see the Use Case section in this article.

How to use the feature

To use the scancode feature:

1. Open Citrix Workspace app for Android and navigate to **Settings > General > Keyboard**.
2. Tap **External keyboard input mode**.



3. Select one of the following options:
 - **Scancode** - Sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
 - **Unicode** - Sends the key from the client-side keyboard to VDA and VDA generates the same character in VDA. Applies client-side keyboard layout.

By default, **Unicode** is selected as the external keyboard input mode.

4. Tap **Scancode**.

When you are in a session, you can switch the remote keyboard using the IME feature and input in the server keyboard layout.

Use case

For example, consider a scenario where you're using a US international keyboard layout connected to your Android device.

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

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

Note:

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

Support for external webcam

Citrix Workspace app for Android now supports externally connected webcams within your sessions. Connect a USB webcam and use it for video conferencing by tapping the camera icon, then select the external webcam name. It enhances the session experience by using the resources available to end users.

Note:

The external webcam's name appears only after an external camera is detected.



The next time you use a video conferencing app, the system remembers your preference and uses the camera preference accordingly. For example, if you had completed the last video call with an external webcam preference, next time the external webcam is selected by default.

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

Note:

- When you remove the external camera, the floating multiple-camera icon  changes to a flip button . The **Select Camera** dialog closes if it's open and the external camera view on the VDA becomes unresponsive.
- This feature is applicable on both on-premises and cloud deployments.

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.

In addition, if the CDM setting is set to full access or read access, you can utilize the device's internal storage as a mapped drive to the session.

Feature limitations:

- Android APIs are observed to be slow, which delays certain operations.
- CDM for external storage isn't supported on Pixel devices.
- 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 tap **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 tap **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.

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:

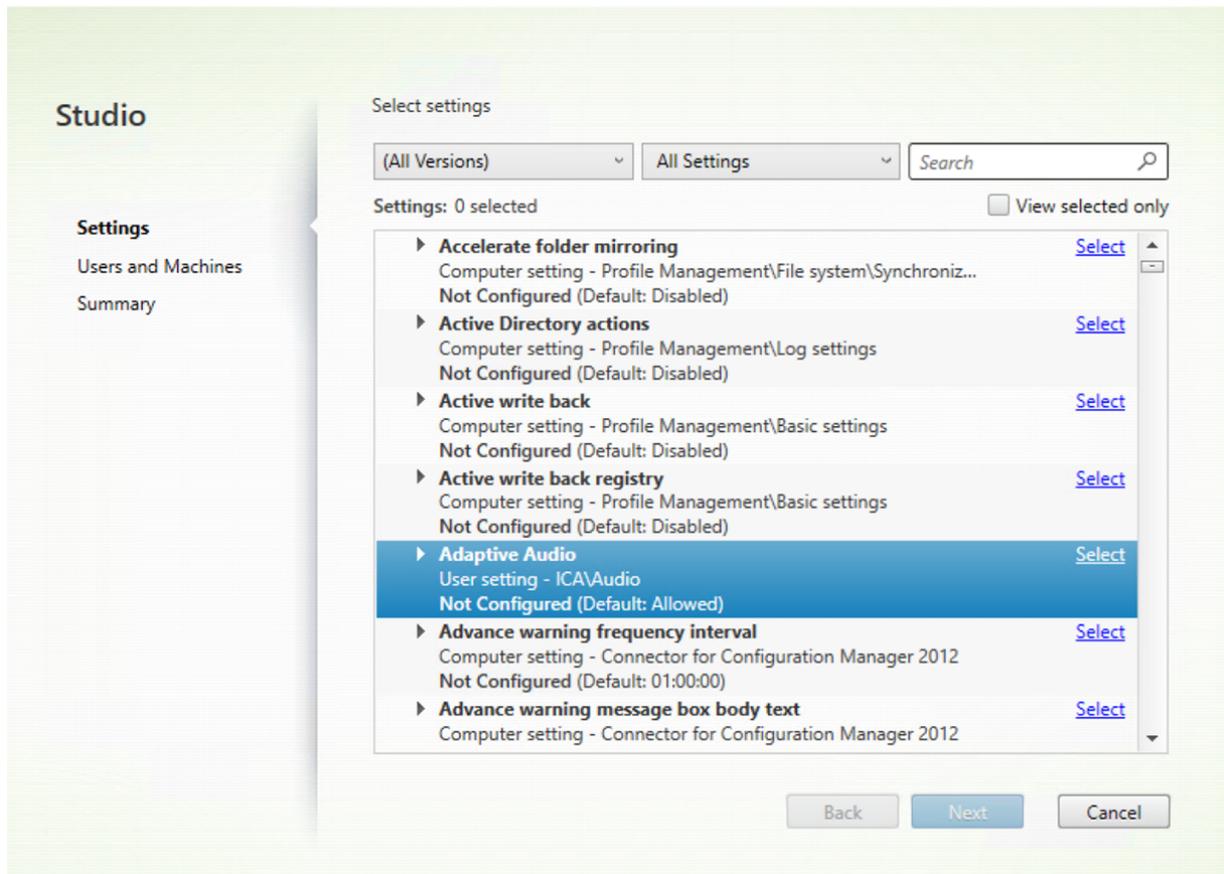
- phone
- tablet
- smart TV
- external monitor in a conference room.

Support for adaptive audio

Citrix Workspace app for Android supports HDX adaptive audio. This feature is designed to provide users with exceptional audio quality and low latency.

You can configure this feature by enabling the **Adaptive Audio** policy.

Create Policy



Feature limitation

In a session, when you play audio on one device and then switch to another device, you might experience difficulty hearing the audio properly. As a workaround, you can pause the audio and wait for about 5-10 seconds, after which the voice is audible. [HDX-67047]

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

Extend display

March 5, 2024

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 Analytics for Performance 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.

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.

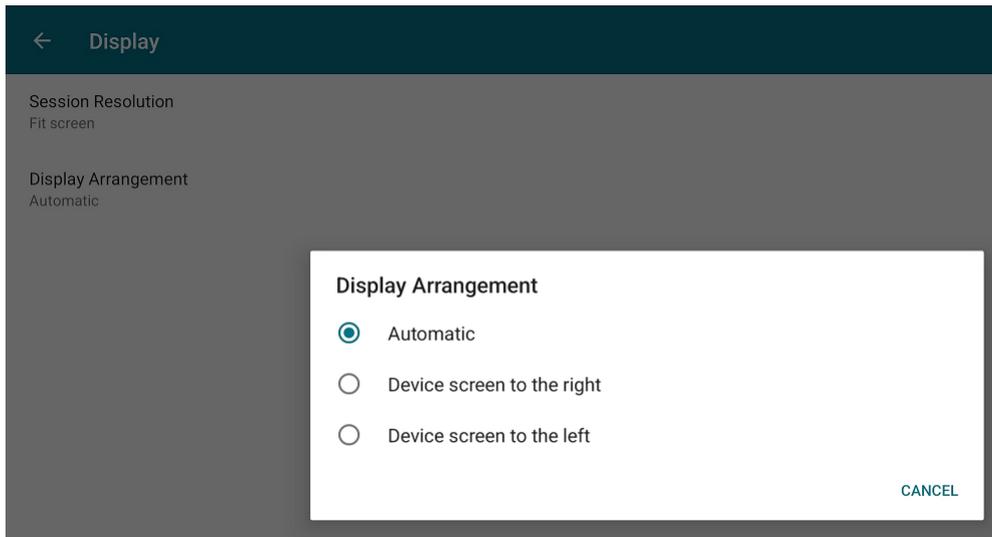
Configure display arrangement

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

March 11, 2024

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. The administrator can configure the **inactivityTimeoutInMinutesMobile** property by using a PowerShell module. Tap [here](#) to download the PowerShell modules for Citrix Workspace app configuration.

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

- After the inactivity timeout, you'll receive a prompt to provide biometric authentication to access the Citrix Workspace app again.
- If you can cancel the biometric authentication prompt, the following message appears:

Citrix Workspace app is locked.

You must authenticate to continue to use the Workspace app.

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

Note:

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

Support for biometric authentication after inactivity

After the inactivity timer expires, the end user is asked to authenticate themselves using biometric features such as facial recognition and fingerprint scanning.

The most robust form of biometric authentication available to the end user depends on the OEM of their device, and they are prompted accordingly.

For more information about configuring inactivity timer, see [Inactivity timeout for Citrix Workspace app sessions](#).

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.”

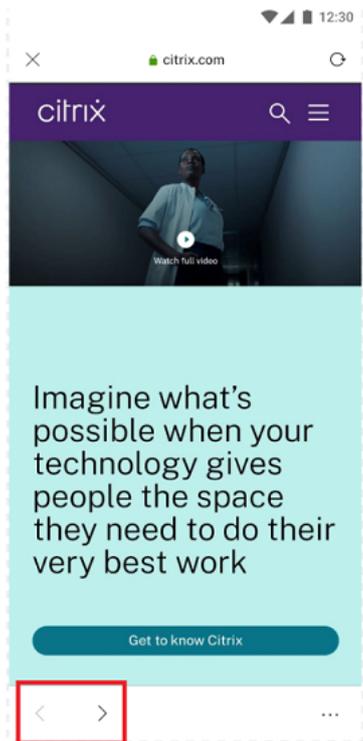
To disable the error message relating to network issues in a session, go to **Advanced** and select the **Disable network monitoring messages** option.

User interface enhancement

- Starting with the 20.7.0 release, you can remove the store account details from the **Edit** option. Tap **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.

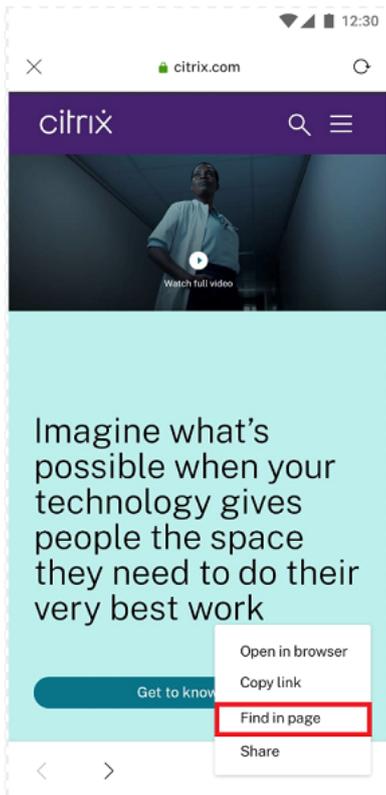


The navigation buttons appear at the top left of your SaaS app session of your tablet.

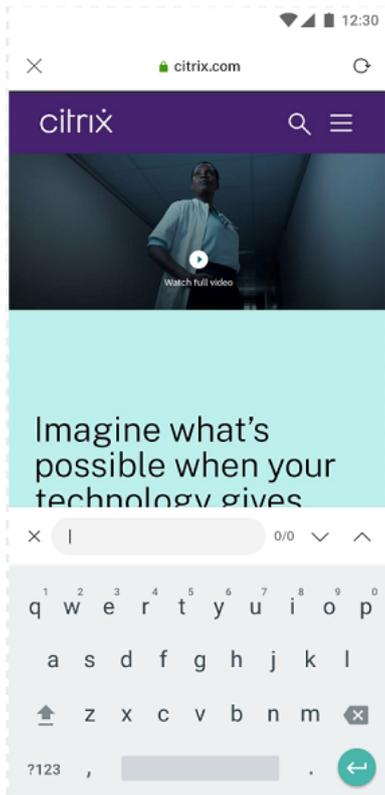
- Starting with the 21.4.0 release, you can search for words or phrases within your web and Software-as-a-Service (SaaS) apps.

To search, follow these steps.

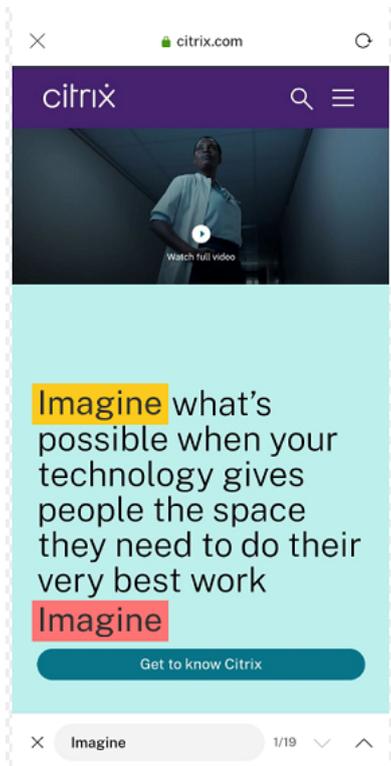
1. Tap the ellipsis button on the bottom right and select **Find in page**.



1. The keyboard appears.



1. 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**.

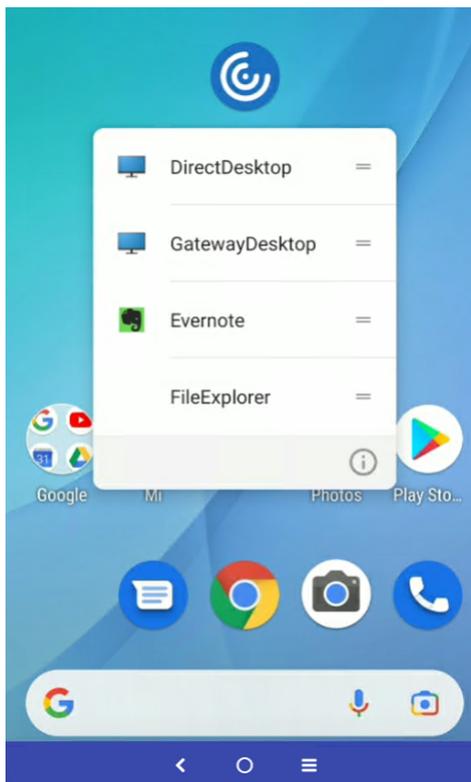
Citrix Workspace app for Android



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:

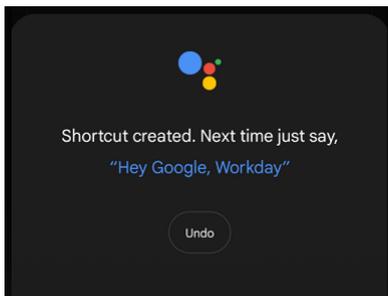
1. Launch the Citrix Workspace app and open a resource you want to add as the shortcut.
2. Open Google Assistant settings from your device.

Note:

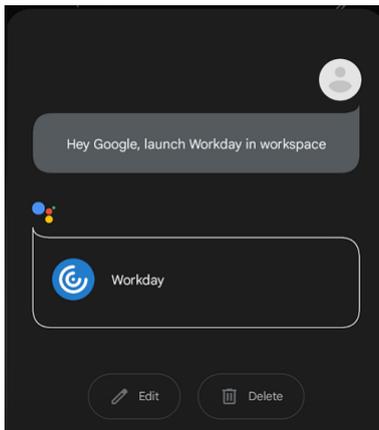
Accessing Google Assistant settings can vary depending upon the Android version and the Android device you use.

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

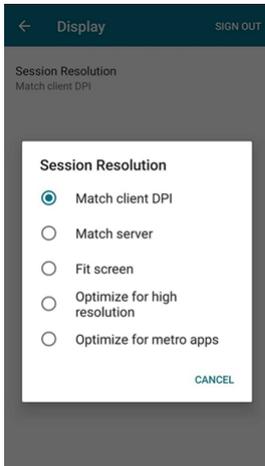
July 24, 2024

DPI matching

The DPI matching feature ensures that the virtual session gets rendered according to the DPI of the device. Previously, even on high-DPI mobile phones and tablets, the DPI of the device wasn't consid-

ered for session display. Starting with the 24.1.0 release, a new display setting helps to achieve DPI matching.

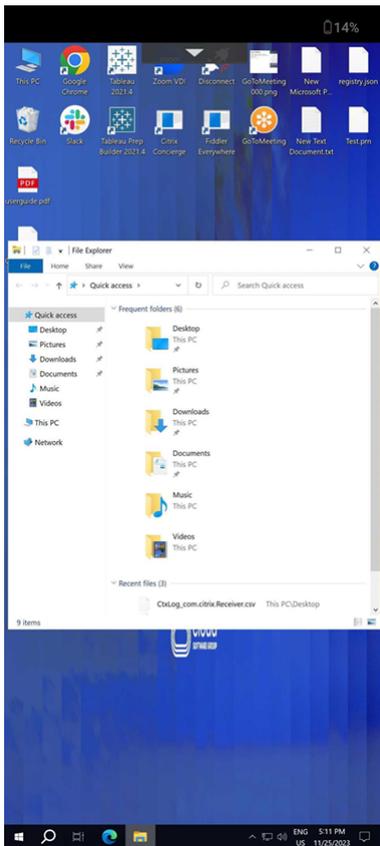
On your device, go to Citrix Workspace app for Android **Settings > General > Display > Session Resolution >** and select the **Match client DPI** option.



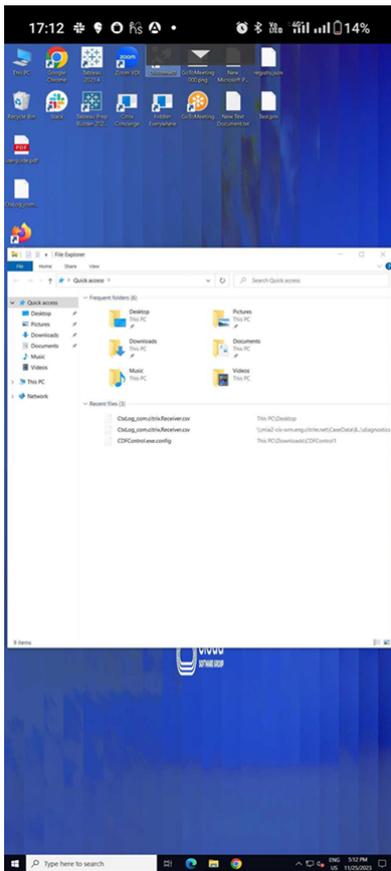
In other words, the Citrix Workspace app attempts to match the display resolution and DPI scale settings of the Android device to the Citrix session automatically. This feature enhances the user experience by displaying the sessions according to the DPI of the phone or tablet. The session icons, text, and image clarity are now sharper and more comfortable to read.

For example, when you select the **Match client DPI** option, the session icons, text, and images are clear.

Citrix Workspace app for Android



On the contrary, when you select the **Fit screen** option, the session icons, text, and images are smaller in size.



Note:

When you connect an external monitor, the session continues to render with the primary device's DPI because of Android's limitation.

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're introducing the EDT and TCP parallel connection feature. The feature results in decreased connection times.

Earlier, when establishing a connection, the Citrix Workspace app tried to connect using EDT. Unsuccessful EDT connection attempts 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 tapping the resource. This feature requires StoreFront (on-premises) Version 1912 or later.

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.

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.

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.

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:

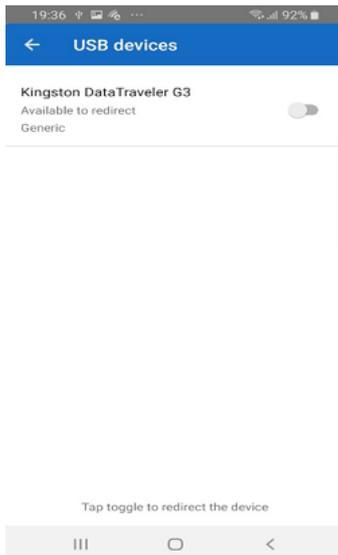
Install the vendor-specific drivers on the device. When the installation is complete, the vendor software might ask you to reconnect the USB device. Reconnect the USB device to redirect it.

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

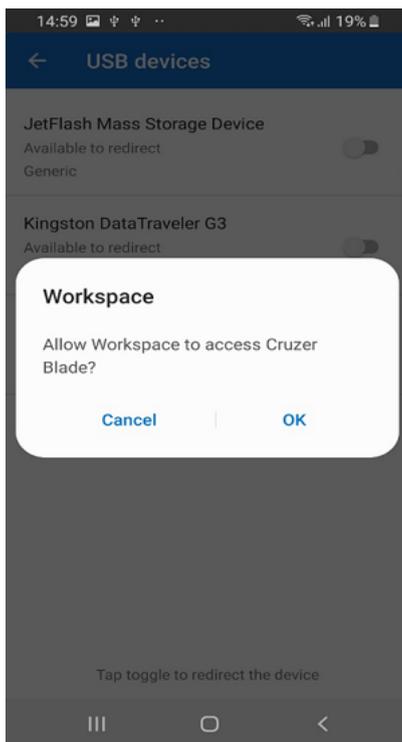
1. Add a USB redirection policy-enabled store and launch a session.
2. Tap the session toolbar icon as displayed in the dialog below:



3. Tap 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, tap the Toggle option against the device.
A Workspace permission dialog appears.

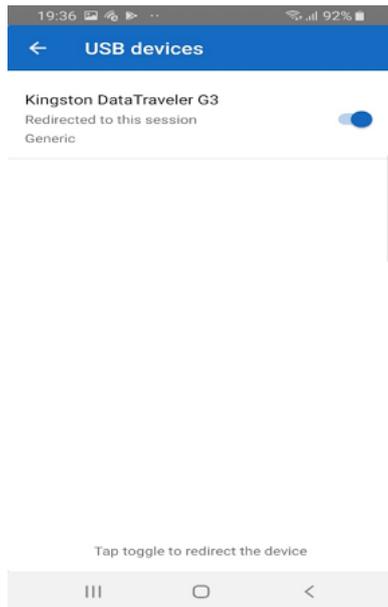


6. Tap **OK** to grant permission for the Citrix Workspace app to redirect the device.

Note:

This step is mandatory to redirect the USB device.

The USB device is redirected and the status is displayed as follows:



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

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

Known issues:

- Only one USB device is supported at a time.
- Audio and video USB devices 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

| Keyboard layout on Android | Keyboard Language | Keyboard Layout on Windows | Keyboard Layout on Linux |
|----------------------------|-------------------------------|--|--------------------------|
| Belarusian(Belarus) | Belarusian(Belarus) | Belarusian(Belarus) Keyboard | by |
| Bulgarian | Bulgarian | Bulgarian (Typewriter) keyboard | bg |
| Chinese (Simplified) | Chinese (Simplified, China) | Citrix IME - Chinese (Simplified, China) | zh |
| Chinese (Traditional) | Chinese (Traditional, Taiwan) | Citrix IME - Chinese (Traditional, Taiwan) | tw |

| Keyboard layout on Android | Keyboard Language | Keyboard Layout on Windows | Keyboard Layout on Linux |
|----------------------------|--------------------------|--------------------------------------|--------------------------|
| Croatian | Croatian (Croatia) | Croatian keyboard | hr |
| Czech | Czech | Czech keyboard | cz |
| Danish | Danish | Danish keyboard | df |
| Dutch | Dutch (Netherlands) | United States-International keyboard | us |
| Dutch(Belgium) | Dutch | Belgian (Period) Keyboard | be |
| English (Australia) | English (Australia) | US keyboard | us |
| English (Canada) | English (Canada) | US keyboard | us |
| English (UK) | English (United Kingdom) | United Kingdom keyboard | gb |
| English(US) | English (United States) | US keyboard | us |
| Estonian | Estonian | Estonian keyboard | ee |
| Finnish | Finnish | Finnish keyboard | fi |
| French (Canada) | French (Canada) | French Keyboard | fr |
| French (Switzerland) | French (France) | Swiss French Keyboard | ch |
| French(French) | French (France) | French Keyboard | fr |
| German (Austria) | German (Austria) | German keyboard | at |
| German (Switzerland) | German (Switzerland) | Swiss German keyboard | ch |
| German(Germany) | German (Germany) | German keyboard | at |
| Greek | Greek | Greek keyboard | gr |
| Hungarian | Hungarian | Hungarian keyboard | hu |
| Icelandic | Icelandic | Icelandic keyboard | is |
| Irish | Irish | | ie |
| Italian | Italian (Italy) | Italian keyboard | it |
| Japanese | Japanese | Citrix IME - Japanese | jp |
| Korean | Korean | Citrix IME - Korean | kr |
| Latvian | Latvian | Latvian keyboard | lv |

| Keyboard layout on Android | Keyboard Language | Keyboard Layout on Windows | Keyboard Layout on Linux |
|----------------------------|-----------------------|-----------------------------------|--------------------------|
| Norwegian | Norwegian (Bokmål) | Norwegian keyboard | no |
| Polish | Polish | Polish (Programmers) keyboard | pl |
| Portuguese (Brazil) | Portuguese (Brazil) | Portuguese (Brazil ABNT) keyboard | br |
| Portuguese (Portugal) | Portuguese (Portugal) | Portuguese keyboard | pt |
| Romanian | Romanian (Romania) | Romanian (legacy) keyboard | ro |
| Russian(Russia) | Russian | Russian keyboard | ru |
| Slovak | Slovak | Slovak keyboard | sk |
| Slovenian | Slovenian | Slovenian keyboard | si |
| Spanish (Mexico) | Spanish (Mexico) | Latin American keyboard | latam |
| Spanish (Spain) | Spanish (Spain) | Spanish keyboard | es |
| Swedish(Sweden) | Swedish (Sweden) | Swedish keyboard | se |
| Turkish | Turkish | Turkish F keyboard | tr |
| Ukrainian | Ukrainian | Ukrainian keyboard | ua |

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.

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.

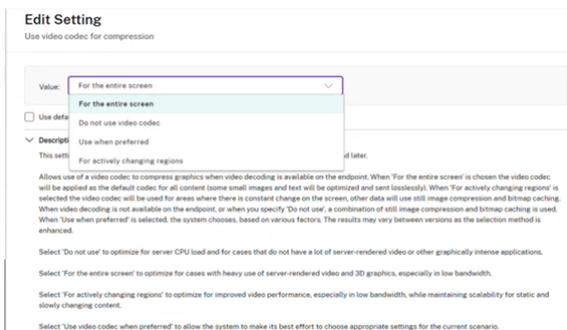


Support for full-screen display

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.

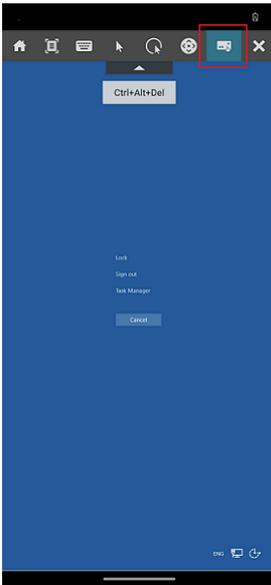
Configuration

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



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.



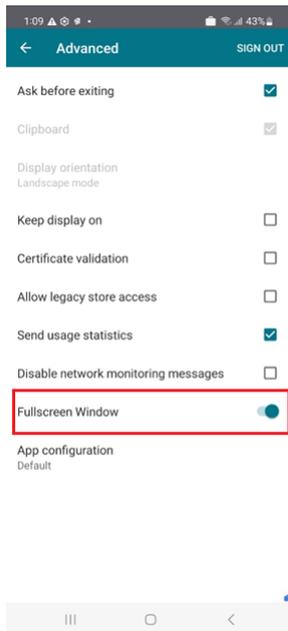
Support for full-screen mode for app sessions

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

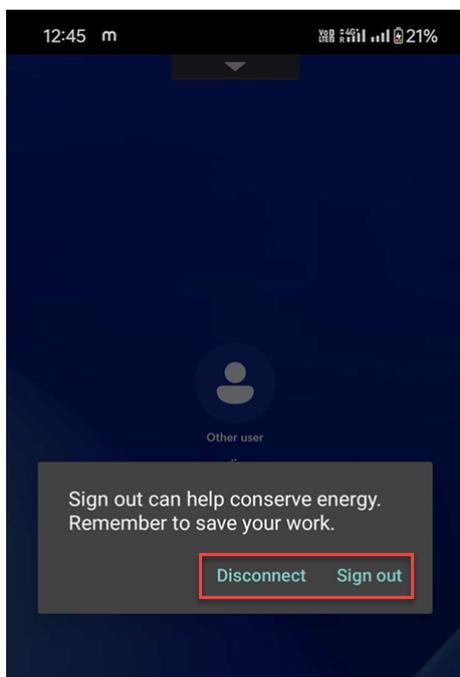
- When you attach an external keyboard to your device:
 - To use the CapsLock key as the narrator key, the action might not work as expected. As a workaround, press the Insert key. [HDX-55347]
 - To use the key combination Win+Ctrl+Enter to enable the narrator, the action doesn't take effect inside the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

Sustainability initiative from Citrix Workspace app

Previously, virtual desktops were left in a disconnected state when users closed them by tapping the home button. This consumed unnecessary energy and power resources.

Starting from the 24.2.0 version, we have introduced a sustainability initiative that encourages users to conserve energy that might be used due to running unused virtual desktops.

With this feature enabled, when users tap on the **X** icon to disconnect the session, a prompt is displayed to sign out from the desktop session. This feature can be helpful in enterprises that use Windows OS policies to shut down VMs when no users are logged in.



End users can exit from the session in two ways:

- **Sign out** to save energy. This sustainability action shuts down the virtual machine and conserve energy. End users must make sure to save their work before signing out.
- **Disconnect** to close the virtual desktop session window. However, the virtual session remains active until the next sign-in. End users can resume their work easily.

As an administrator, you can customize the sustainability message. For more information on how to enable and customize this feature, see the [Sustainability initiative from Citrix Workspace app](#) article in Citrix Workspace app for Windows documentation.

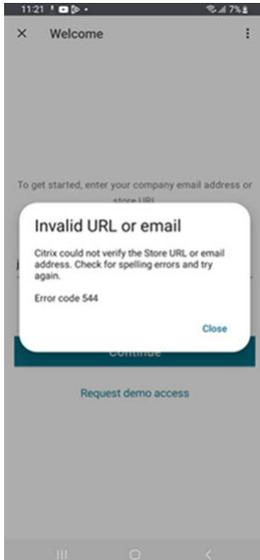
Improved error messages

Previously, error messages had insufficient actionable descriptions.

Starting with the 23.12.0 release, error messages include a clear and user-friendly title, a specific description for each error, and error codes where possible. Error codes help administrators to troubleshoot the issue. The improved messages to end users provide enough details to troubleshoot

problems. If there are any unresolved issues, we suggest users reach out to their IT administrator for further assistance.

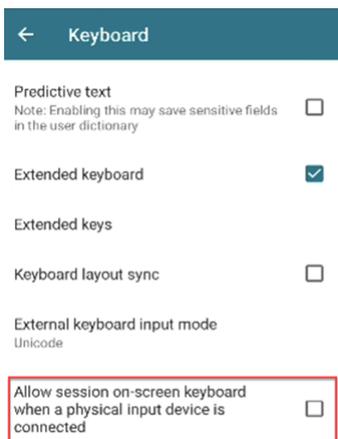
For example, when the user is unable to sign in, the following error message appears:



Soft keyboard support for barcode scanner

Previously, when barcode scanners (for example, Zebra scanners) were detected in a session, the soft keyboard didn't appear. The issue was because it was identified as an external keyboard.

Starting with the 24.2.0 version, the soft keyboard appears when barcode scanners are connected as a physical input device. A new keyboard setting is added to support this feature. End users can go to Citrix Workspace app **Setting > Keyboard >** and select **Allow session on-screen keyboard when a physical input device is connected** option.



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]

Document scanner

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

Note:

- This feature is enabled by default.

Prerequisites

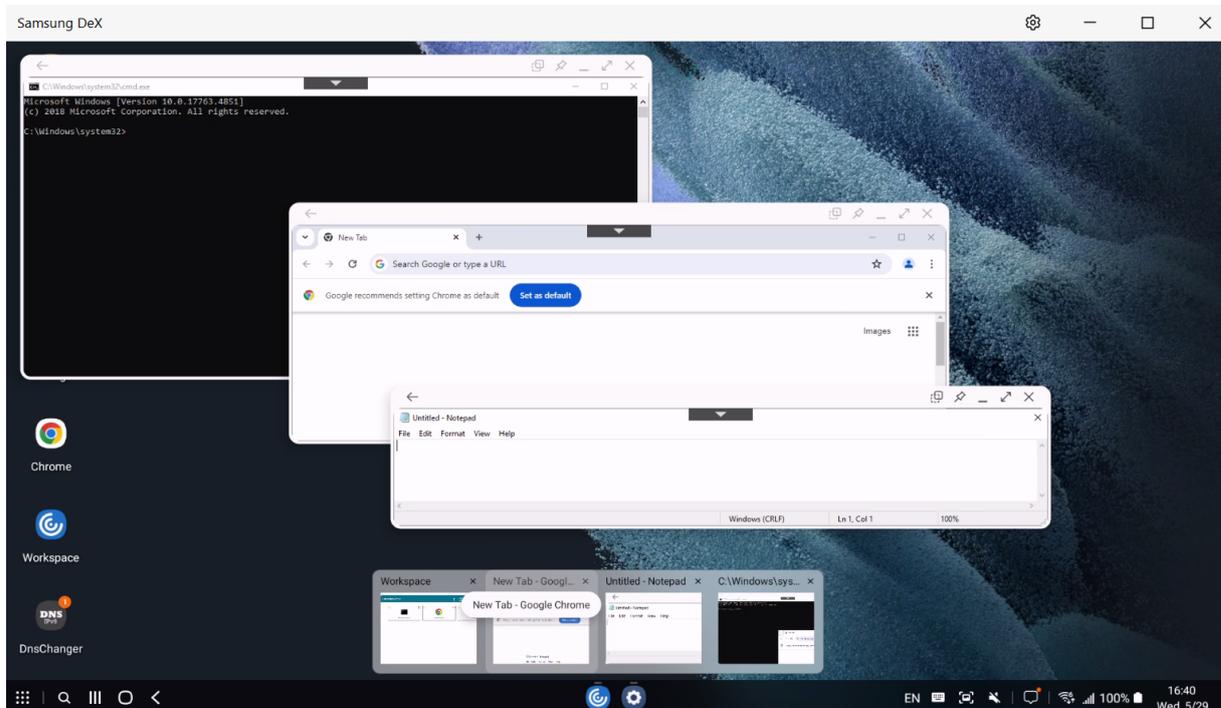
- [Client drive mapping \(CDM\)](#) must be enabled for the store.
- Document scanner requires read and write access on your device. To enable access, follow these steps:
 1. From your profile, tap application **Settings > Store settings**.
 2. Tap your current store.
 3. Tap **Device Storage** and then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

For more information about how to use this feature, see [Document scanner](#) in the help documentation.

Enhancement to support desktop-like experience in a single session on Samsung DeX

Previously, Citrix Workspace app supported seamless multi-tasking and provided users with a desktop-like experience. It allows you to open multiple apps within the same session to run simultaneously. These apps opened in separate windows.

Starting from the 24.7.0 release, end users can open a separate window for session-sharing apps. This feature supports more than one local window, thus facilitating multi-tasking. Each window has a name for each virtual app. Users can open multiple virtual apps and native DeX apps on the DeX screen only. Active virtual apps and native DeX apps show up as active apps in the bottom taskbar with respective app names, on the DeX Screen only.



Note:

The first app you start might take a minute to sign in to the session and load your user profile.

Users can do the following:

- Click the pin button on the upper-right of the window to pin the app window. The pinned window always stays on top.
- Access the session toolbar button on all the app windows.
- Minimize, maximize, move, and close the app window.
- Switch apps and multi-task using mouse clicks, double-clicks, drag, and keyboard strokes.

Feature limitations

- Server-oriented window size change isn't supported. In other words, if the size of the server-side window is set or limited, any requests to change the size from the client side aren't successful. This setting results in a discrepancy between the local and remote window graphics.

- The client-side window has a minimum window size. For instance, the minimum size of a window on a 1920x1080 resolution DeX screen is 220x220 with the title bar, and the available rectangle size is 220x189.
- Certain menu options might extend and appear out of the parent app boundary. The extended menu options might appear in the other app windows.
- The preview image of an app in the taskbar might overlap and cover another app's preview.

Store experience

March 11, 2024

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**, tap the link of the particular store to enable the security settings.
2. The **Manage Receiver for Web Sites** dialog box appears.
3. Tap **Configure**.
4. The **Edit Receiver for Web site** dialog box appears.
5. Tap the **Advanced Settings** tab and select **Enable strict transport security**.

Authenticate

July 24, 2024

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

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

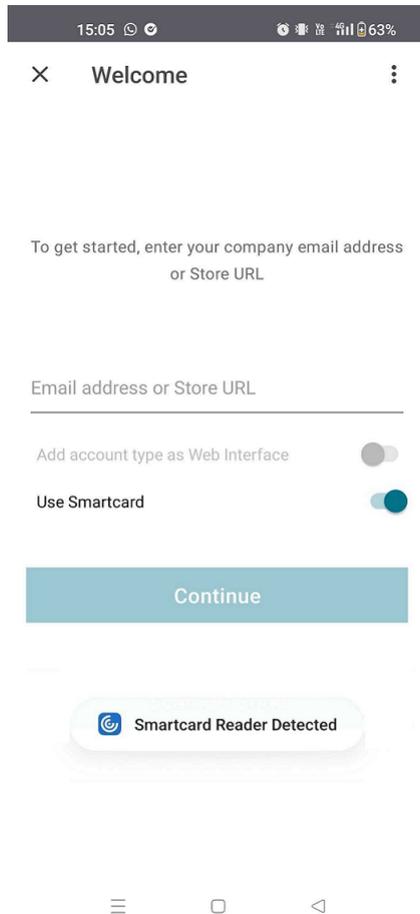
Prerequisite

- Install [C4E app from play store](#) to use smart cards. Contact email address: 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:
 - .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 when connecting to HDX session

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.

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.

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.

For more information, see [Inactivity timeout for Citrix Workspace app sessions](#).

Support for biometric authentication after inactivity

After the inactivity timer expires, the end user is asked to authenticate themselves using biometric features such as facial recognition and fingerprint scanning.

The most robust form of biometric authentication available to the end user depends on the OEM of their device, and they are prompted accordingly.

Support for authentication using FIDO2 when connecting to a cloud store

Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Face recognition, and Fingerprint only). This feature is compatible with Android version 9 and later.

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

Note:

This feature is enabled by default.

Secure

July 24, 2024

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:

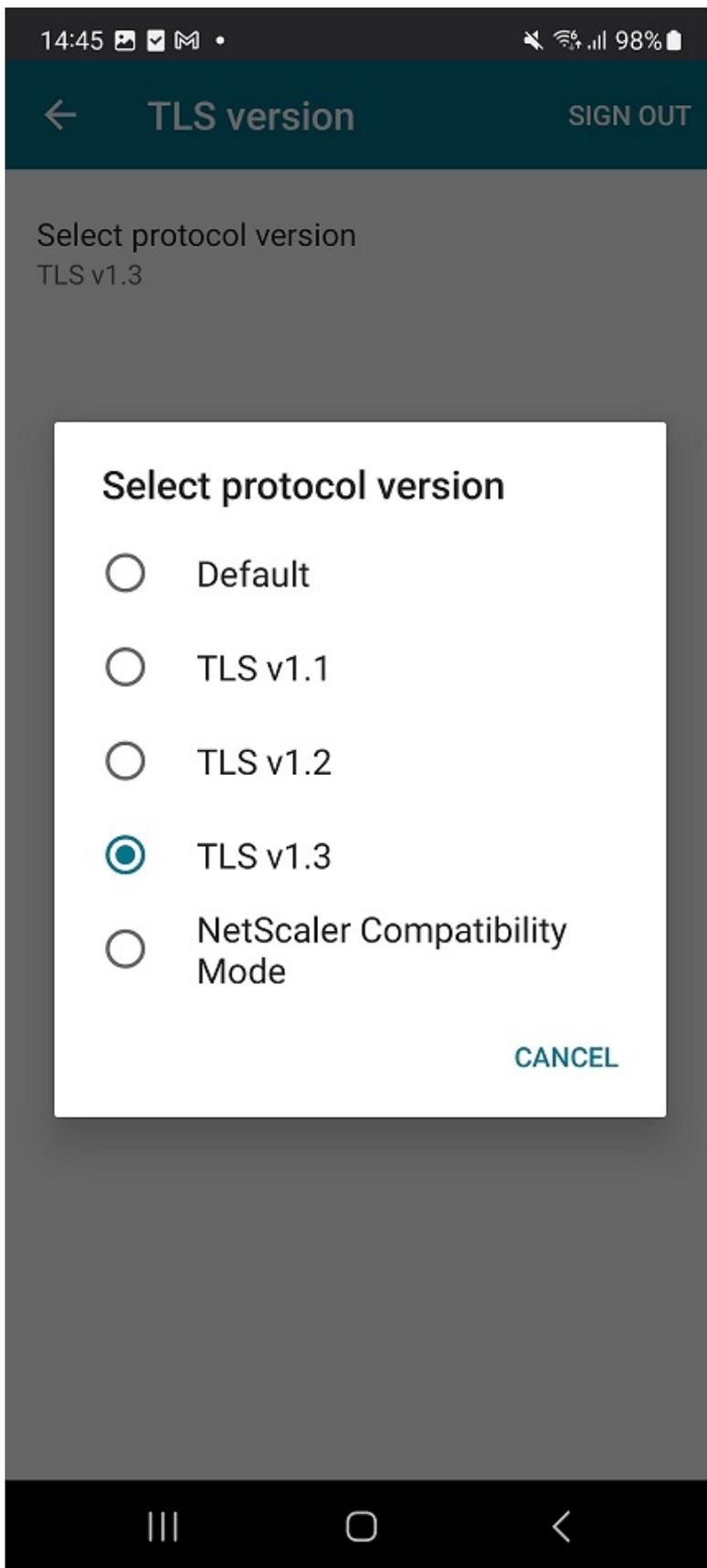
- `TLS_AES_256_GCM_SHA384`
- `TLS_AES_128_GCM_SHA256`

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**.

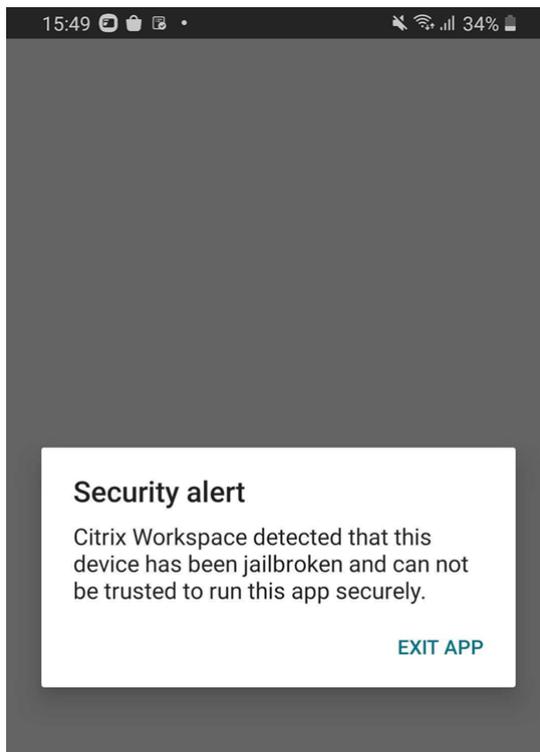


For more information, see [Cryptography](#)

For more information on help documentation, see [TLS version](#).

Jailbroken devices

Your users can compromise the security of your deployment by connecting with jailbroken Android devices. Jailbroken devices are those whose owners have modified them, usually with the effect of bypassing certain security protections. When Citrix Workspace app for Android does a basic detection of a jailbroken Android device, the app displays an alert to the user.



To further help secure your environment, you can configure StoreFront or Web Interface to help prevent detected jailbroken devices from running apps.

Requirements:

- Citrix Workspace app for Android 24.7.0 or later.
- Access to StoreFront or Web Interface through an administrator account.

To help prevent detected jailbroken devices from running apps:

1. Sign in to your StoreFront or Web Interface server as a user with administrator privileges.
2. Find the file **default.ica**, which is in one of the following locations:

- `C:\\inetpub\\wwwroot\\Citrix*storename* conf` (Microsoft Internet Information Services)
 - `C:\\inetpub\\wwwroot\\Citrix*storename*\\App_Data` (Microsoft Internet Information Services)
 - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. Under the section **[Application]**, add the following: `AllowJailBrokenDevices=OFF`
 4. Save the file and restart your StoreFront or Web Interface server.

After you restart the StoreFront server, users who see the alert about jailbroken devices can't start the apps from your StoreFront or Web Interface server

To allow detected jailbroken devices to run apps:

If you don't set `AllowJailBrokenDevices`, the default is to display the alert to jailbroken device users but still allow them to open applications.

If you want to allow your users to run applications on jailbroken devices specifically, set `AllowJailBrokenDevices=ON`.

When you set `AllowJailBrokenDevices` to ON, your users see the alert about using a jailbroken device, but they can run applications through StoreFront or Web Interface.

Troubleshoot

March 11, 2024

How to check app's version

To know which version of Citrix Workspace app you're using, see the article [How to check app's version](#) in the help documentation.

How to upgrade to the latest version

To upgrade the Citrix Workspace app to the latest version manually, do the following:

1. Open Play Store.
2. Search for Citrix Workspace.

If an update is available, tap **Update**.

Update the app automatically

By default, apps are updated automatically when the following conditions are met:

- The device is connected to a Wi-Fi network.
- The device is charging.
- The device is idle (not actively used).
- The Citrix Workspace app isn't running in the foreground.

Note:

The Google Play Store checks for app updates once a day. So, it can take up to 24 hours before an app update is added to the update queue. After an app is added to the queue, it will be automatically updated the next time when the conditions are fulfilled.

How to reset Citrix Workspace app

To reset the app, you can do one of the following:

- Clear the Citrix Workspace app storage data. Go to Android device **Settings** > **Apps** > select **Citrix Workspace app** > **Storage** > **Clear Cache**.
- or
- Uninstall Citrix Workspace app and install the latest Citrix Workspace app for Android from [Google Play](#) that has the latest fix.

Note

Deleting existing accounts from Citrix Workspace app resets the account and not Citrix Workspace app itself.

How to collect logs

Log collection is important as it can help identify issues. For more information, see the article [How to collect logs](#) in the help documentation.

How to provide feedback

You can send us feedback about Citrix Workspace app for Android and report issues using the same interface. For more information, see the article [How to provide feedback](#) in the help documentation.

How to request for enhancements

To request for Citrix Workspace app for Android feature enhancements, fill the [Podio form](#).

How to access technical preview features

To know about the features that are in technical preview, see [Features in Technical Preview](#).

How to provide feedback on EAR

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

Common issues and troubleshooting tips

Application unavailable in app store

If you're unable to use Google Play Store to install Citrix Workspace app for Android, as an alternative, you can download the app from the [Citrix Downloads](#) page.

Installation failures

When Citrix Workspace app isn't supported by default on Android TV, reach out to us through [enhancement requests](#).

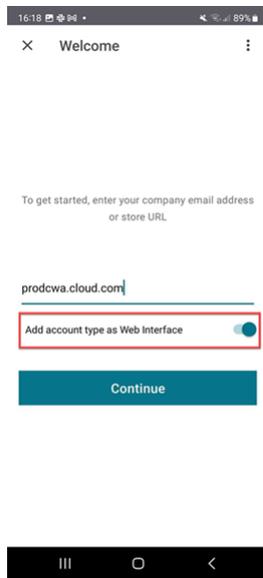
Authentication and store addition

If you observe issues about authentication or store addition, check for the following.

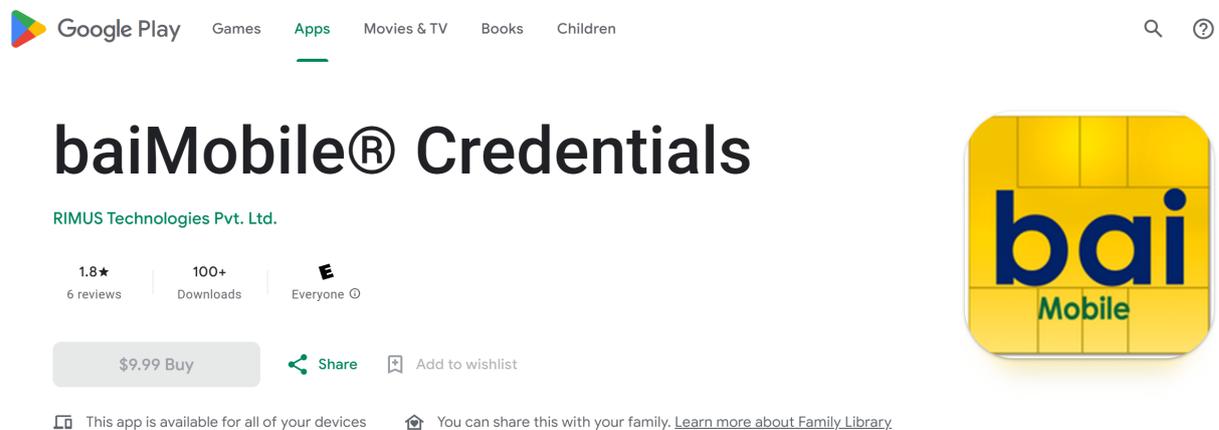
Invalid input You might have entered:

- invalid credentials
- incorrect store URL
- typos while entering the credentials and the store URL
- HTTP instead of HTTPS.

Web Interface mode You can also try to use **Web Interface** mode. On the first page of the app, tap **Get started**. On the **Welcome** page, enter the store URL and enable **Add account type as Web Interface**.



Smart card If the smart card authentication isn't working, install the **baiMobile Credentials** app. If the baiMobile Credentials app detects your smart card, contact us to look into the issue further.



NetScaler policy configurations To troubleshoot connection issues, see the [NetScaler Gateway for mobile devices](#) Knowledge Center article.

Session launch

To view session statistics:

- from the session toolbar, tap the mouse pointer icon four times
or
- run `ctxsession -v` command in session terminal.

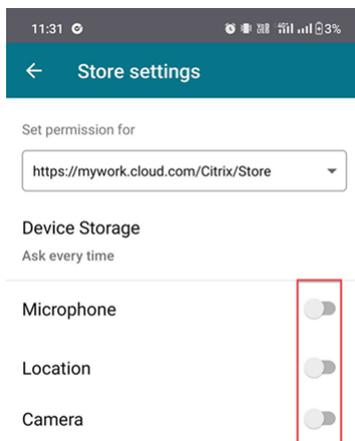
Failed to launch desktop To troubleshoot, see the following Knowledge Center articles:

- [Error code 2524](#)
- [Error code 2523](#)
- [Error code 2502](#)
- [Error code 2517](#)

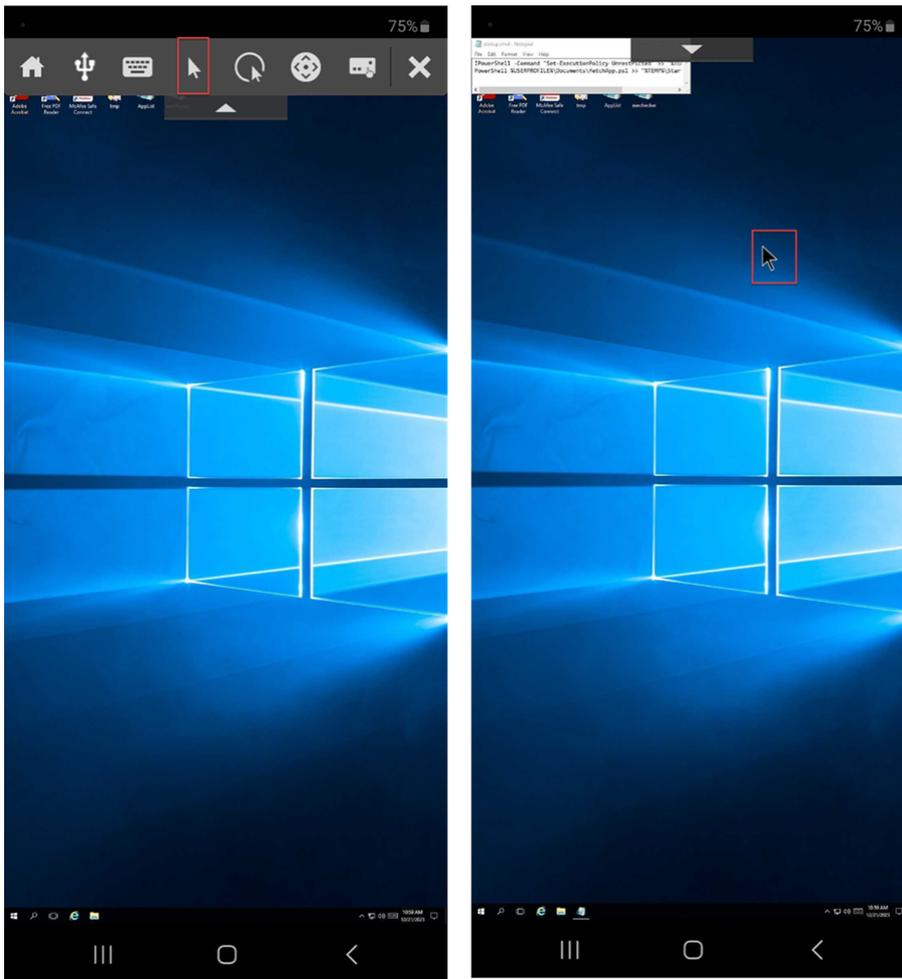
Permissions to access peripherals

Enable proper setting permissions.

Client Selective Trust Enable settings for Microphone, Location, and Camera. Go to Citrix Workspace app **Settings > Store settings** and enable CST settings for a selected store.

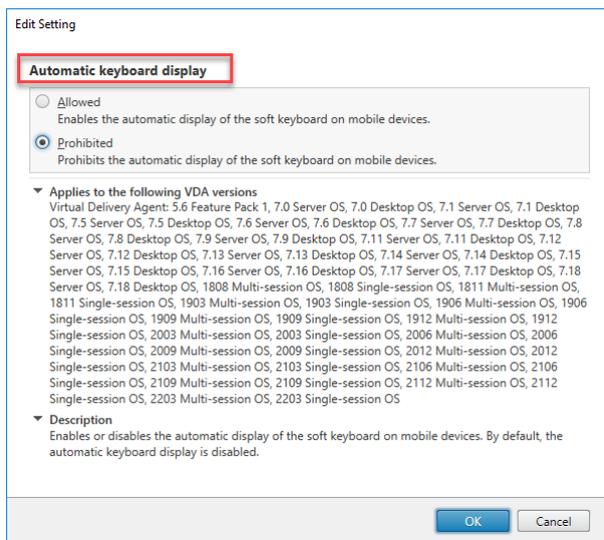


Enable mouse pointer After you start a session, tap on the toolbar and tap the mouse pointer icon to enable the mouse pointer.



Enable Keyboard If your organization's administrator hasn't enabled the automatic keyboard display feature by default, contact your organization's administrator for further assistance.

Administrators must enable the **Automatic keyboard display** policy in the DDC setting.



FAQs

- How to improve the virtual app and virtual desktop's video user experience for low-powered devices or mobile devices?
 - For more information see, [Video user experience](#) Knowledge Center article.
- Accessing Resources - I can't see my apps or desktops after signing into Citrix Workspace app?
 - Contact your company's help desk or your IT Support team administrator for further assistance.
- How to troubleshoot slow connections?
 - Follow the workaround if you experience any of the following issues:
 - slow connections to the Citrix Virtual Apps and Desktops site
 - missing application icons
 - recurring **Protocol Driver Error** messages

Workaround:

- Disable **Citrix PV Ethernet Adapter** properties for the network interface on the:
 - Citrix Virtual Apps server
 - Citrix Secure Web Gateway
 - Web Interface server
- The **Citrix PV Ethernet Adapter** properties include (all enabled by default):

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

No server restart is needed. This workaround applies to the Windows Server 2003 and 2008 32-bit. This issue does not affect the Windows Server 2008 R2.

- Issue with Numeric keys and special characters
 - If the numeric keys or Chinese IME characters do not work properly, disable the **Unicode Keyboard** option. To do so, go to **Settings > Keyboard Options >** and set **Use Unicode Keyboard** to **disabled**.

Troubleshooting error codes

The following table gives you the list of error codes and a probable solution:

| Error code | Knowledge Center article |
|---|--|
| Error code 437 | https://support.citrix.com/article/CTX463401 |
| Error code 41E | https://support.citrix.com/article/CTX235177 |
| Error code 546 or 547 | https://support.citrix.com/article/CTX231798 |
| Error code 518 | https://support.citrix.com/article/CTX277571 |
| Error code 42B | https://support.citrix.com/article/CTX260992 |
| Error code 548 | https://support.citrix.com/article/CTX250706 https://support.citrix.com/article/CTX578359 |
| Incorrect server address + Error code 548 | https://support.citrix.com/article/CTX554245 |
| Error code 451 | https://support.citrix.com/article/CTX256708 |
| General error | https://support.citrix.com/article/CTX219073 |
| Try connecting again | Disable the UDP option. Go to app Settings > Advance > EDT |

Errors messages and description

The following table gives you the list of errors and description. The probable solution is to contact [Citrix Technical support](#) for further assistance:

| Error | Description |
|---|---|
| SessionManager.Launch.EngineLoadFailed | The ICA Engine failed to load/initialize. |
| SessionManager.Launch.ConnectionFailed | The ICA Engine terminated before connecting. |
| SessionManager.Launch.LogonFailed | Session disconnected without completing login |
| SessionManager.LeaseResolution.Failed | Unable to attempt lease launch. |
| SessionManager.clxmtp.SoftDeny | Engine CLXMTP negotiation failed (soft deny). |
| SessionManager.clxmtp.SoftDeny_Implicit | Engine CLXMTP connection failed (implicit soft deny). |
| Transport.Connect.NoCGP_Fail | Failed to connect (CGP disabled). |
| Transport.Connect.FallbackFail | Failed to connect, tried the ICA fallback. |
| Transport.Connect.Fail | Connection is unavailable. |

SDK and API

March 11, 2024

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](#).

Deprecation

May 28, 2024

The announcements in this article give you advanced notice of platforms, Citrix products, and features that are being phased out. Using these announcements, you can make timely business decisions.

Citrix monitors customer use and feedback to determine when they're withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

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

| Item | Deprecation | | Alternative |
|---|---|---|---|
| | announced in Citrix Workspace app version | Removed in Citrix Workspace app version | |
| Android operating systems earlier than version 12.0 | 24.5.0 | 24.7.0 | Android version 12.0 and later are supported |
| Support for TLS 1.0 and TLS 1.1 protocols | 24.4.0 | Future release | TLS 1.2 or TLS 1.3 protocol |
| XenApp Services (also known as PNAgent) | 24.3.5 | Future release | Within workspace app, connect to stores using the store URL rather than the XenApp Services URL |
| Android operating systems earlier than version 9.0 | 24.1.0 | 24.3.0 | Android version 9.0 and later are supported |
| Citrix Workspace app for Android on ChromeOS | 23.8.0 | 23.12.0 | To use Citrix Workspace app on ChromeOS, install the extension . |
| Workspace with intelligence | - | 23.2.0 | - |

| Item | Deprecation | | Alternative |
|--|--|--|--|
| | announced in Citrix Workspace app version | Removed in Citrix Workspace app version | |
| Support for Android Enterprise | - | 23.2.0 | - |
| Mobile Workspace Experience | - | 23.2.0 | - |
| RSA SecurID Authentication | 2008 | - | - |
| Android operating systems earlier than Version 7.0 | 1903 | 1906 | Version 7.0 (Nougat) and later are supported |



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).