Citrix Workspace™ app for Linux

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix Workspace app for Linux 3

About this release 4

Features in Technical Preview 87

Citrix Workspace app for Linux 2608 - Preview 102

System requirements and compatibility 116

Install, Uninstall, and Update 132

Store configuration 141

App experience 157

App preferences 158

Data collection and monitoring 162

Security and authentication 164

Security 164

Secure communications 172

Authentication 183

Connectivity 206

HDX™ and Multimedia 210

Graphics and display 211

Audio 227

Multimedia 234

Optimization for Microsoft Teams 241

Browser content redirection 251

Server-client content redirection 254

ICA® Settings Reference 256

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bidirectional content redirection 256

Devices 257

Mouse 258

Cursor 259

Touch screen 260

Keyboard 262

USB 281

SANE redirection 299

Webcams 300

Client-drive mapping 306

Printer 311

Session experience 314

SDK and API 335

Storebrowse 337

Troubleshooting 349

Deprecation 394

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app for Linux

August 14, 2026

Citrix Workspace app for Linux is a software client that provides access to your desktops, applications, and data easily and securely from many types of Linux devices. Citrix Workspace app provides access from your desktop, Citrix Workspace user interface, or web browsers.

Working with a Citrix-enabled IT infrastructure, Citrix Workspace app gives you the mobility, convenience, and freedom you need to get your work done.

For detailed information about the features, fixed issues, and known issues, see the About this Release page.

You can use Citrix Workspace app on PCs, tablets, and thin clients. By using Citrix StoreFront™ with Citrix Workspace app, your organization can provide self-service access to applications and desktops. And that access comes with a common user interface, regardless of the following:

- Endpoint device hardware
- Operating system
- Form factor

For information about the features available in Citrix Workspace app for Linux, see Citrix Workspace app feature matrix.

For information about deprecated items, see the Deprecation page.

Language support

Citrix Workspace app for Linux is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for Linux, see Language support.

Earlier versions

- Citrix Workspace app 2604 for Linux (PDF Download)
- Citrix Workspace app 2601 for Linux (PDF Download)
- Citrix Workspace app 2508.10 for Linux (PDF Download)
- Citrix Workspace app 2508 for Linux (PDF Download)
- Citrix Workspace app 2505 for Linux (PDF Download)
- Citrix Workspace app 2503 for Linux (PDF Download)
- Citrix Workspace app 2411 for Linux (PDF Download)
- Citrix Workspace app 2408 for Linux (PDF Download)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspace app 2405 for Linux (PDF Download)
- Citrix Workspace app 2402 for Linux (PDF Download)
- Citrix Workspace app 2311 for Linux (PDF Download)
- Citrix Workspace app 2309 for Linux (PDF Download)
- Citrix Workspace app 2308 for Linux (PDF Download)
- Citrix Workspace app 2307 for Linux (PDF Download)
- Citrix Workspace app 2305 for Linux (PDF Download)
- Citrix Workspace app 2303 for Linux (PDF Download)
- Citrix Workspace app 2302 for Linux (PDF Download)
- Citrix Workspace app 2211 for Linux (PDF Download)
- Citrix Workspace app 2209 for Linux (PDF Download)
- Citrix Workspace app 2207 for Linux (PDF Download)
- Citrix Workspace app 2205 for Linux (PDF Download)
- Citrix Workspace app 2203 for Linux (PDF Download)
- Citrix Workspace app 2202 for Linux (PDF Download)
- Citrix Workspace app 2112 for Linux (PDF Download)
- Citrix Workspace app 2111 for Linux (PDF Download)
- Citrix Workspace app 2109 for Linux (PDF Download)
- Citrix Workspace app 2108 for Linux (PDF Download)
- Citrix Workspace app 2106 for Linux (PDF Download)
- Citrix Workspace app 2104 for Linux (PDF Download)
- Citrix Workspace app 2103 for Linux (PDF Download)
- Citrix Workspace app 2101 for Linux (PDF Download)

Documentation for this product version is provided as a PDF because it isn't the latest version. For the most recently updated content, see the Citrix Workspace app for Linux current documentation.

> **Note:**
>
> Links to external websites found in the preceding PDF take you to the correct pages, but links to other sections within the PDF are no longer usable.

Legacy documentation

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

About this release

September 15, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Learn about new features, enhancements, fixed issues, and known issues for Citrix Workspace app for Linux.

> **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 form link.
> - ARM64 continues to be supported in Citrix Workspace app for Linux 2604.

What's new in 2604.10

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

Fixed issues in 2604.10

- After a session locks automatically, the Browser Content Redirection overlay might retain keyboard focus, causing typed input to go to the redirected browser tab instead of the session. [CVADHELP-33859]

Known issues in 2604.10

There are no new known issues.

Earlier releases

2604

What's new

The following is a list of features that are available in Citrix Workspace app 2604 for Linux:

- Enhanced Browser Content Redirection with Server-Side Certificate Validation
- Entra ID single sign-on for NetScaler Gateway stores
- Removal of Citrix Enterprise Browser
- Google Chrome support for FIDO2 authentication
- Enhanced Call Connect times with UCSDK Optimization
- Service continuity for connectorless workloads
- Shortcuts menu for macOS VDA
- Scanner workflow optimization

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- EDT Lossy support with Secure HDX 2.0
- Removal of ARM64 support
- Dual VCSDK binary sets for Linux (Technical Preview)
- Dual CWA package sets for Linux (Technical Preview)

Enhanced Browser Content Redirection with Server-Side Certificate validation

Starting with Citrix Workspace app 2604 for Linux, Browser Content Redirection is further enhanced with certificate validation support. When accessing a redirected website from the client, the client overlay browser may not trust the certificate from the server or the MitM proxy. In such cases, BCR can now validate the Host or Proxy certificates against the VDAs certificate store.

For more information, see Server-side certificate validation document.

Requirements This feature is enabled by default, and no configuration is necessary once the following requirements are met:

- CVAD 2507 LTSR or later, or CVAD 2511 CR or later
- CWA Linux 2604 or later
- Browser Redirection Extension (Chrome or Edge) 25.11 or later

Entra ID single sign-on for NetScaler Gateway stores

Starting with Citrix Workspace app 2604 for Linux, you can configure Entra ID single sign-on (SSO) for on-premises stores that are accessed through a NetScaler Gateway. This enhancement lets users launch virtual apps and desktops without re-entering their Entra ID credentials.

Install dependencies Install the following packages if they are not already present on the endpoint.

For Ubuntu or Debian:

```
sudo apt install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

For RHEL or Fedora:

```
sudo dnf install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

For openSUSE:

```
sudo zypper install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Entra ID SSO All Entra ID SSO settings are available in `/opt/Citrix/ICAClient/config/AuthManConfig.xml`.

Edit the file with root privileges:

```
sudo vi /opt/Citrix/ICAClient/config/AuthManConfig.xml
```

Configure the following settings as needed:

- `PersistCookies`: Persists Entra ID SSO cookies in memory when the authentication window closes. The default value is **`false`**.
- `AADSSOEnabled`: Enables or disables Entra ID SSO. The default value is **`true`**.
- `AADSSOWithFido2AuthenticationEnabled`: Uses the system browser for authentication instead of the built-in WebKitGTK window. The default value is **`false`**.
- `SharedAuthContextEnabled`: Persists Entra ID cookies across app launches in the same user session. The default value is **`false`**.
- `EnableBypassGateway`: Reuses the AAD-issued gateway cookie (`NSC_AAAC`) to bypass interactive NetScaler Gateway authentication. The default value is **`false`**.

Example:

```
<PersistCookies>true</PersistCookies>

<key>AADSSOEnabled</key>
<value>true</value>

<key>AADSSOWithFido2AuthenticationEnabled</key>
<value>false</value>

<key>SharedAuthContextEnabled</key>
<value>true</value>

<key>EnableBypassGateway</key>
<value>true</value>
```

How it works

Self-Service UI Launch Citrix Workspace app for Linux from the application menu or by running:

```
/opt/Citrix/ICAClient/selfservice
```

Use the following workflow:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sign in to the NetScaler Gateway store.
2. Launch an application or desktop.
3. Complete Entra ID authentication in the WebKitGTK window the first time that you launch a resource.
4. Start the session without entering credentials again on the VDA.

When `PersistCookies` is **`true`**, Citrix Workspace app reuses the Entra ID session for subsequent launches in the same session. When `EnableBypassGateway` is **`true`**, the NetScaler Gateway authentication step is also skipped by reusing the `NSC_AAAC` cookie that was obtained during the Entra ID sign-in flow.

Storebrowse `storebrowse` provides the same Entra ID SSO experience from the command line.

Use the following workflow:

1. Add the NetScaler Gateway store:

```
/opt/Citrix/ICAClient/util/storebrowse --addstore "https://gateway
    .example.com"
```

2. List the configured stores:

```
/opt/Citrix/ICAClient/util/storebrowse --liststore
```

3. List the published applications:

```
/opt/Citrix/ICAClient/util/storebrowse -E "https://gateway.example
    .com/Citrix/Store/discovery"
```

4. Launch an application:

```
/opt/Citrix/ICAClient/util/storebrowse -L "Citrix.MPS.Desktop.
    Notepad" "https://gateway.example.com/Citrix/Store/discovery"
```

5. Complete Entra ID authentication when the authentication window appears on the first launch.

On the first launch, an Entra ID authentication window appears. After the user authenticates, Citrix Workspace app acquires the SSO token and embeds it in the session so that the VDA does not prompt for credentials. If `EnableBypassGateway` is **`true`**, the gateway authentication step is skipped by reusing the `NSC_AAAC` cookie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Shared workstation mode For kiosk or shared Linux thin-client deployments, enable shared user mode:

```
/opt/Citrix/ICAClient/util/storebrowse -c SharedUserMode=True
```

Authentication methods

Built-in window By default, Citrix Workspace app uses a WebKitGTK window for Entra ID authentication. No additional software is required beyond the standard dependencies. When `SharedAuthContextEnabled` is **`true`**, the built-in window uses the same cookie context as the store webview. Cookies are stored in a persistent SQLite database that WebKitGTK manages. Each authentication attempt uses a 30-second timeout.

System browser Set `AADSSOWithFido2AuthenticationEnabled=`**`true`** to use the system browser
instead of the built-in window. The browser redirects back to Citrix Workspace app through the `ctxaadsso://` protocol handler.

Use the system browser in the following cases:

- Your organization requires FIDO2 security key authentication.
- Conditional Access policies require a specific browser.
- Browser-based smart card or certificate authentication is required.

Supported browsers are Google Chrome, Chromium, Mozilla Firefox, and Microsoft Edge for Linux. Citrix Workspace app registers the `ctxaadsso://` protocol handler automatically during installation by using the desktop file at `/opt/Citrix/ICAClient/desktop/ctxaadsso.desktop`.

Removal of Citrix Enterprise Browser

Starting with Citrix Workspace app 2604 for Linux, the Citrix Enterprise Browser (CEB) is removed from the CWA-L package, along with the related setup components. For FIDO2 sign-ins, authentication now occurs in the system default web browser instead of CEB. This change simplifies the sign-in experience and aligns it with standard browser-based authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Chrome support for FIDO2 authentication

Starting with Citrix Workspace app 2604 for Linux, you can use Google Chrome for FIDO2 cloud authentication.

To configure Google Chrome for FIDO2 authentication, add the following setting to `AuthManConfig.xml`:

```
<FIDO2AuthBrowser>google-chrome</FIDO2AuthBrowser>
```

Enhanced call connects times with UCSDK Optimization

Starting with Citrix Workspace app 2604 for Linux, the Smart Sync feature introduced in Unified Communications SDK (UCSDK) 5.0.0 accelerates call connection times by streamlining communication between the VDA and the client endpoint. This enhancement delivers faster call setup across the board, with the most significant performance improvements in high-latency network environments.

For more information, see UCSDK documentation.

Service continuity for connectorless workloads

Starting with Release 2604, Citrix Workspace app for Linux supports Service Continuity for connectorless workloads. This enhancement helps users maintain access to their connectorless resources during an outage.

For information about how to configure Service Continuity, see Service continuity.

Shortcuts menu for macOS VDA

Starting with Citrix Workspace app 2604 for Linux, users connecting to a macOS VDA can access the **Shortcuts** menu in the session toolbar for quick access to common operating system actions without requiring complex keyboard shortcuts or trackpad gestures.

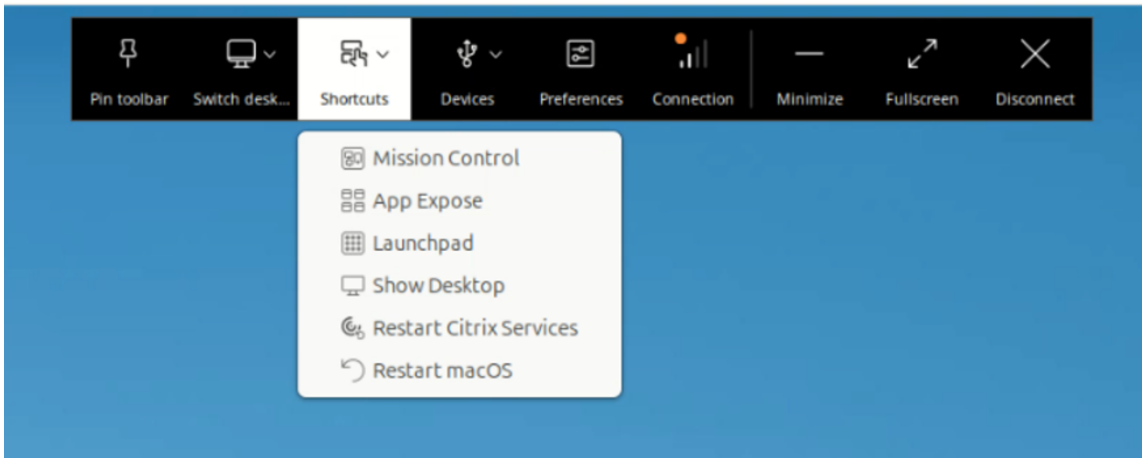
> **Note:**
>
> The **Shortcuts** menu appears only when the endpoint is connected to a macOS VDA.

The **Shortcuts** menu includes the following options:

- Mission Control
- App Expose
- Launchpad

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Show Desktop
- Restart Citrix Services
- Restart macOS



Scanner workflow optimization

Starting with Citrix Workspace app 2604 for Linux, scanner redirection improves scan performance by caching **SANE** initialization and device-list responses to reduce repeated communication between components. It also improves recovery from scanner faults, such as paper jams, to help prevent pipe read blocks, and uses the latest `IcaGenScan` SDK APIs.

EDT Lossy support with Secure HDX 2.0

Starting with Citrix Workspace app 2604 for Linux, direct CWA-to-VDA connections now support Enlightened Data Transport (EDT) Lossy with Secure HDX 2.0. Previously, EDT Lossy was available only with Datagram Transport Layer Security (DTLS) or HDX Direct.

Removal of ARM64 support

Starting with version 2604, Citrix Workspace app for Linux no longer supports ARM64.

Technical Preview

- Dual VCSDK binary sets for Linux
- Dual CWA package sets for Linux

For more information, see the Features in Technical Preview page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- For Boot-to-VDI sessions, the system time displayed on the lock screen might become frozen and not update after logout, which can cause confusion on shared client devices. [CVADHELP-31860]
- When the Boot-to-VDI login screen remains inactive for some time, you might see an `AM_ERROR_AUTH_CANCELLED_BY_USER` message or a similar message instead of a clear login timeout message prompting you to reconnect and sign in again. [CVADHELP-32070]
- You might notice that launching Citrix Workspace app a second time while sign-in to a Citrix Cloud or Workspace store is still in progress makes the app unresponsive or displays a blank window. [CVADHELP-31992]
- Nuance PowerMic devices redirected into an HDX session after session launch might have non-functional HID buttons inside the session, such as in Dragon Medical One. [HDX-101227]
- On Linux clients such as eLux and Ubuntu, a phantom drive letter, such as `D:\`, might appear in the session through dynamic Client Drive Mapping (CDM) even when no USB storage device is connected. [CVADHELP-32425]
- In multi-monitor fullscreen sessions, repeatedly clicking **Extend to all displays** might cause the toolbar to expand and move off-screen, making both the toolbar and its collapsed notch inaccessible. [CVADHELP-31897]
- On eLux thin clients, a session window might move to the wrong monitor when a monitor is connected or disconnected, or when the laptop lid is closed and reopened. [HDX-104082]
- A seamless window might disappear immediately after it pops up when it carries all three style attributes simultaneously: `WS_POPUP`, `WS_EX_TOOLWINDOW`, and `WS_EX_NOINHERITLAYOUT`. [CVADHELP-30425]
- When a proxy is configured to use the NTLM authentication protocol, the connection might fail with the following error message: **No Supported Authentication Method**. [CVADHELP-31646]
- Launching a published or hosted application on Citrix Workspace app for Linux might fail with the following error message: **Network data corrupted - HDX has detected corrupted server data** when connecting to a legacy VDA such as XenApp/XenDesktop 7.15 LTSR. [CVADHELP-32516]
- Citrix Workspace app might crash in certain environments when excessive logging fills local disk partitions. [CVADHELP-32595]
- On eLux thin clients, after a smartcard is removed and reinserted, the session window might close and disappear during reconnect, even though the virtual desktop still shows the session as connected. [CVADHELP-32510]

Known issues

- You might find that certain pop-up windows of a custom web application fail to open or render correctly in a desktop session. This issue occurs when the VDA switches the desktop into multi-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

touch mode, which suppresses the synthetic mouse events that the web application's pop-up logic relies on. As a workaround, do the following:

1. Edit `/opt/Citrix/ICAClient/config/module.ini`.
2. Under the `[ICA 3.0]` section, set `MultiTouch=Off`.
3. Reconnect the session for the change to take effect. [CVADHELP-32531]

- Citrix Workspace app might stop responding and the session disconnects when you set the noise suppression level to **High** in the in-session audio preferences. This issue occurs on devices whose processor does not support the AVX-512 instruction set. As a workaround, set the noise suppression level to **Off** or to any level other than **High**. [HDX-107685]

2601

What's new

The following features are available in this release:

- Seamless Integration of Endpoint Analysis (EPA)
- Entra ID single sign-on (SSO) from web browsers
- Single sign-on (SSO) through cookie sharing for on-premises stores
- Microsoft Edge support for FIDO2 and Entra ID SSO
- FIDO2 authentication timeout configuration
- Identity Provider (IDP) logout on Workspace (WSP) inactivity timeout
- Automatic Maximum Transmission Unit (MTU) adaptation
- Enhanced keyboard settings
- Transparent key pass-through on Wayland and XWayland
- Improved session reconnection experience
- Extended logging support
- Modular Browser Content Redirection
- Force Gateway route for StoreFront discovery
- Audio Quality Enhancer for reliable transport

Seamless Integration of Endpoint Analysis (EPA)

Starting with version 2601, Citrix Workspace app for Linux prompts administrators to install the Endpoint Analysis (EPA) plug-in and installs it only when it detects an older EPA version; equal or newer versions remain unchanged.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Entra ID single sign-on (SSO) from web browsers

Starting with version 2601, Citrix Workspace app for Linux supports Entra ID single sign-on (SSO) from web browsers through the Citrix Web Extension. This feature is enabled by default.

For more information, see Entra ID single sign-on (SSO) from web browsers.

Single sign-on (SSO) through cookie sharing for on-premises stores

Starting with version 2601, Citrix Workspace app for Linux extends Single Sign-On (SSO) support to on-premises stores, including both direct StoreFront stores and those accessed through a gateway. This enhancement delivers seamless authentication for on-premises environments by applying cookie sharing through the Credential Insertion SDK.

SSO support for cloud-based stores was added in version 2508 using the `CitrixSSOnSDK::LogonSsoCookies` API to inject validated cookies. The same SDK and API are now used for on-premises stores as well.

For stores behind a gateway, authentication occurs during the store addition phase. Therefore, cookies must be injected into AuthManager's cache before adding the store, and the AuthManager daemon must be running. To ensure AuthManager is running, execute `storebrowse --liststore`. This command lists existing stores and starts the AuthManager daemon if it is not already running.

In addition to injecting cookies obtained from identity providers, you can optionally inject an AAAC cookie for stores behind a gateway. Injecting an AAAC cookie prompts AuthManager to directly initiate a Gateway session.

For more information on cookie sharing, see the Credential Insertion SDK documentation.

Microsoft Edge support for FIDO2 and Entra ID SSO

Starting with version 2601, Citrix Workspace app for Linux adds support for using Microsoft Edge for:

- FIDO2 authentication
- Entra ID Single Sign-On (SSO) using the system browser

For more information, see Microsoft Edge support for FIDO2 and Entra ID SSO.

FIDO2 authentication timeout configuration

Starting with version 2601, Citrix Workspace app for Linux provides a configuration option to control the browser-based FIDO2 authentication timeout.

For more information, see FIDO2 authentication timeout configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identity Provider (IDP) logout on Workspace (WSP) inactivity timeout

Starting with version 2601, Citrix Workspace app for Linux adds support for logging out of the Identity Provider (IDP) during user logoff and when a Workspace (WSP) inactivity timeout occurs. This opt-in feature helps ensure complete session termination across the authentication chain while preserving existing logout behavior unless enabled.

For more information, see Identity Provider (IDP) logout on Workspace (WSP) inactivity timeout.

Automatic Maximum Transmission Unit (MTU) adaptation

Starting with version 2601, Citrix Workspace app for Linux supports dynamic adjustment of the session's Maximum Transmission Unit (MTU). This feature automatically detects and adjusts the MTU during a session if the network path changes. This feature is disabled by default.

For more information, see Automatic Maximum Transmission Unit (MTU) adaptation.

Enhanced keyboard settings

Starting with version 2601, Citrix Workspace app for Linux introduces enhanced keyboard settings that provide improved control over system shortcuts and keyboard input modes. These enhancements include UI settings for system shortcut pass-through (transparent key pass-through) and an automatic mode for keyboard input that dynamically selects the best input method based on the VDA type.

For more information, see Enhanced keyboard settings.

Transparent key pass-through on Wayland and XWayland

Starting with version 2601, Citrix Workspace app for Linux supports reliable transparent key pass-through on Wayland and XWayland. System-level keyboard shortcuts (for example, Alt+Tab) pass through to the HDX session and are not intercepted by the local Linux desktop.

Improved session reconnection experience

Starting with version 2601, this feature enhances the end-user experience during session timeouts caused by inactivity or network interruptions. Users can reconnect directly from the timeout screen for both desktop and app sessions, and also reconnect after the Auto-Client-Reconnect (ACR) phase. This feature is enabled by default.

For more information, see Improved session reconnection experience.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Extended logging support

Starting with version 2601, Citrix Workspace app for Linux adds a configuration option to enable extended logging for easier diagnostics.

For more information, see Extended logging support.

Modular Browser Content Redirection

Starting with Citrix Workspace app 2601 for Linux, Browser Content Redirection (BCR) is managed as a modular component, decoupled from the main Citrix Workspace app (CWA) for Linux. This new modular architecture allows the BCR component to be updated or uninstalled independently of the CWA. As a result, security fixes can be delivered more quickly, and new BCR capabilities can be adopted without waiting for a full CWA release cycle.

The BCR component continues to be installed by default with Citrix Workspace app for Linux, ensuring a consistent user experience. Additionally, standalone BCR packages are available for situations that require independent updates or interim patches outside the regular Citrix Workspace app release cycle.

Force Gateway route for StoreFront discovery

Starting with version 2601, Citrix Workspace app for Linux introduces the ability to force Gateway routing for StoreFront discovery while accessing on-premises stores behind a Gateway. With this option, administrators can override the default route decision and ensure that StoreFront traffic is always proxied through the Gateway when a mapping is configured.

This option can be useful in environments where the beacons do not function as expected, or where administrators prefer not to modify beacon configuration in Citrix StoreFront.

To enable this option:

1. Navigate to `AuthManConfig.xml` file.
2. Set the value as follows:

```
<ForceGatewayRoute>true</ForceGatewayRoute>
```

Technical Preview in 2601

- Audio Quality Enhancer for reliable transport

For more information, see the Features in Technical Preview page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- You might have noticed unexpected behavior where certain browser keyboard shortcuts could launch a non-sandboxed browser window during a Browser Content Redirection (BCR) session. The affected shortcuts are now blocked and can no longer trigger this action. [CVADHELP-30447]
- You might have noticed an issue where Bloomberg keyboard special function keys (top row green keys) did not function correctly in ICA sessions. The keys now work as expected. [HDX-97528]
- You might have noticed that when adding a NetScaler Gateway URL in Citrix Workspace app 2508.10 for Linux on Ubuntu 24.04 platforms, an HTTP error could occur and prevent successful addition. [CVADHELP-30718]
- When you attempt to add a store through an external gateway in Citrix Workspace app for Linux, the operation might fail. [CVADHELP-31534]
- You might have noticed that after disconnecting or logging off in Citrix Workspace app 2508 for Linux on eLux, users could be unable to reconnect or launch a new session because multiple lingering storebrowse processes created after session launch prevented successful reconnection.[CVADHELP-30529]

Known issues

- You might find that uninstalling Citrix Workspace app for Linux does not automatically remove the ctxbcr Debian package if it was installed to upgrade the BCR component. As a workaround, manually remove the `ctxbcr` package using the command `sudo dpkg -r ctxbcr`. [HDX-1000982]
- When you use Jabber with CWAL 2601.0.150, self video might not appear in the Jabber video settings menu and could display on the Linux desktop instead. During Jabber calls, the caller might not see their own or the participant's video, while the participant can see both. [HDX-101366]

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.

2508.10

What's new

The following feature is available in this release:

- Entra ID SSO support for cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Entra ID SSO support for cloud

Starting with version 2508.10, Citrix Workspace app for Linux supports Microsoft Entra ID single sign-on (SSO) on endpoint devices running **Ubuntu 22.04** and **Ubuntu 24.04**. Use Microsoft Entra ID credentials to sign in to Citrix Cloud stores and access Citrix Virtual Apps and Desktops with SSO, without repeated credential prompts.

The following launch methods are supported for Citrix Cloud stores:

- Citrix Native UI (Self-Service)
- Citrix Store browse

For more information on implementing Microsoft Entra ID SSO with Citrix Workspace app for Linux, see Entra ID SSO support for cloud.

For more information about Citrix support for Microsoft Entra ID SSO, see Microsoft Microsoft Entra ID single sign-on.

Fixed issues

- The SAML authentication window might appear behind the active VDI session on some Linux desktops when the VDI is set to Fullscreen, causing the window to become inaccessible and blocking sign-in. Eventually, this disrupts the saving of the session layout. This is most frequently observed on eLux (MATE or Marco). [CVADHELP-29227]
- The session might fail to launch successfully when attempting to load the custom virtual driver (Cisco Webex Meetings VDI). [HDX-95265]
- When you configure device rules with a **Deny** rule in **Client USB device redirection rules** policy setting in Studio, certain devices that have been allowlisted in the same policy setting for passthrough into an HDX session with an **ALLOW** rule fail to get redirected. [HDX-95546]
- You might experience a white screen issue when launching a session with multiple monitors. Add `ToolbarLayoutInitEnabled=False` to the `wfclient.ini` file under the `WFClient` section to resolve the issue. [CVADHELP-30429]

Known issues

There are no new known issues.

2508

What's new

The following features are available in this release:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Mandate end users to authenticate and access apps and desktops through native app
- Addition of DisableClientAppManagement flag
- SSO to Citrix Workspace™ app through cookie sharing using Credential Insertion SDK
- Ubuntu 24.04+ webkit2gtk dependency resolution
- Hardware acceleration in Browser Content Redirection
- Keyboard settings change take effect without reconnect
- Audio Quality Enhancer to improve audio performance
- Enhanced Connection Strength Indicator
- Background blur for webcam redirection using UI
- Support for H.264 hardware decoding for seamless apps
- Support for H.264 hardware decoding
- Browser Profile Sharing in Browser Content Redirection (Tech Preview)
- Support for EDT timeout configuration
- NFC support for FIDO2 Authentication
- GACS supports Citrix Workspace app for Linux
- Enhanced file transfer capabilities for Linux clients
- PDF Universal Printing
- Smart card authentication support for Boot-to-VDI (Tech Preview)
- Audio Quality Enhancer for EDT loss tolerant mode
- SANE redirection

Mandate end users to authenticate and access apps and desktops through native app

Starting with version 2508, admins can require Linux users to access Citrix Workspace exclusively through the native app. When enabled, users who try to access the store URL or use third-party browsers are automatically redirected to the Citrix Workspace app. This ensures users benefit from all native app features and enjoy a seamless experience.

For more information, see Mandate end users to authenticate and access apps and desktops through native app.

SSO to Citrix Workspace app through cookie sharing using Credential Insertion SDK

Citrix Workspace app for Linux now supports SSO for cloud-based stores through cookie sharing using the Credential Insertion SDK. The new API `CitrixSSOnSDK::LogonSsoCookies` allows clients to inject validated cookies from identity providers like Okta into the SSO cache. This feature enables seamless desktop and app launches without requiring domain credentials, eliminating redundant login steps and improving user experience. The single authentication path strengthens security by reducing repeated credential handling and maintaining consistent authentication.

For more information, see Credential Insertion SDK documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Addition of DisableClientAppManagement flag

Citrix Workspace app for Linux introduces a new configuration flag called DisableClientAppManagement. This flag allows for improved control over client app behavior.

For more information, see Addition of DisableClientAppManagement flag.

Ubuntu 24.04+ webkit2gtk dependency resolution

Ubuntu 24.04 (Noble Numbat) and newer versions no longer include the webkit2gtk-4.0 library in the default repositories and it is replaced with webkit2gtk-4.1.

For more information, see Ubuntu 24.04+ webkit2gtk dependency resolution.

Hardware acceleration in Browser Content Redirection

Starting with the Citrix Workspace app for Linux 2508 version, the hardware acceleration is now enabled by default in Browser Content Redirection (BCR).

For more information, see Hardware acceleration in Browser Content Redirection.

Keyboard settings change take effect without reconnect

Starting with this release, keyboard setting changes take effect immediately without needing to reconnect or restart the session. This enhancement allows users to modify keyboard settings within the UI and apply them in real-time during an active HDX session with Citrix Workspace app for Linux.This feature improves user experience by eliminating the need for session interruptions when adjusting keyboard configurations, enabling seamless workflow continuity.

Audio Quality Enhancer to improve audio performance

Starting with version 2508, the audio quality enhancer is enabled by default for adaptive audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Both adaptive audio and loss tolerant mode for audio must be enabled for this feature to work.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced Connection Strength Indicator

Starting with version 2508, Citrix Workspace app for Linux features an improved Connection Strength Indicator that provides better connectivity insights and user control. The enhanced indicator helps you monitor network performance, identify connectivity problems quickly, and take corrective action before issues impact your work.

For more information, see Enhanced Connection Strength Indicator.

Background blur for webcam redirection using UI

Starting with version 2508, you can enable background blur for webcam redirection using the graphical user interface (GUI).

For more information, see Background blur for webcam redirection using UI.

Support for H.264 hardware decoding for seamless apps

Starting with the 2508 version, Citrix Workspace app for Linux supports H.264 hardware decoding for seamless apps, using the GPU on the client device.

For more information, see Support for H.264 hardware decoding for seamless apps.

Support for H.264 hardware decoding

Starting with the 2408 version, Citrix Workspace app for Linux supports the GPU that can be used for H.264 decoding wherever it's available at the client. H.264 video codec must be supported and enabled on both the VDA and Citrix Workspace app.

For more information, see Support for H.264 hardware decoding.

Support for EDT timeout configuration

Starting with the version 2508, the configuration mechanism in Citrix Workspace app was enhanced to use the timeout setting from the VDA. This eliminates the need to configure the timeout on the client device. Also, the default EDT timeout was changed from 25 seconds to 10 seconds to allow for faster detection of network interruptions. For more information, see Configure EDT timeout.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NFC support for FIDO2 Authentication

Starting with the 2411 version, you can use the FIDO2-supported NFC card for a Tap-and-Go experience, which is an end-to-end single sign-on (SSO) solution. This means that you can use an NFC card to authenticate to a Citrix® store and then a pre-configured virtual desktop or virtual app will automatically open using SSO.

For more information on configuring this feature, see NFC support for FIDO2 Authentication.

GACS supports Citrix Workspace app for Linux

Starting with the 2408 version, you can manage the Citrix Workspace app settings for user groups using the Configuration profile in Global App Configuration service (GACS). With this feature, you can manage settings for specific user groups rather than applying them to all users accessing the store.

For more information on configuring settings for configuration profile, see Manage settings for user group using configuration profile.

Enhanced file transfer capabilities for Linux clients

Previously, you were able to copy and paste files and folders only between two virtual desktops. Starting with the Citrix Workspace app for Linux version 2508, you can copy files and folders from client to VDA.

For more information, see Clipboard.

PDF Universal Printing

Starting with the 2405 version, Citrix Workspace app for Linux supports the PDF universal printing. You can print as PDF once you configure either or both of the following options:

1. Provide a single PDF Universal Printer created in each session.
2. Use the Universal Print Driver (UPD) for regular auto-created printers.

For more information, see the PDF Universal Printing.

Audio Quality Enhancer for EDT loss tolerant mode

Starting with version 2508, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio .

For more information, see Audio Quality Enhancer for EDT loss tolerant mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SANE redirection

Starting with version 2508, Citrix Workspace app for Linux supports scanner redirection. You can connect a scanning device to the local endpoint and redirect it to a virtual session. This feature lets you access scanned files within the Citrix Workspace app session and upload documents to other apps that are accessible through Citrix Workspace app.

For more information, see SANE redirection.

Technical Preview

- Smart card authentication support for Boot-to-VDI
- Browser Profile Sharing in Browser Content Redirection

For more information, see the Features in Technical Preview page.

Fixed issues

- You might notice that apps become unresponsive when closing dialog windows. [CVADHELP-28893]
- The camera might freeze and flicker in Microsoft Teams optimization windows when the Citrix Workspace app toolbar is disabled and OpenGL rendering is enabled. [CVADHELP-28651]
- Keyboard input might be redirected to the Citrix Viewer session when an external monitor displaying the session is unplugged and a local application has focus on the primary monitor. [CVADHELP-29352]
- Seamless windows might display incorrect layering and experience interaction issues when multiple windows overlap or pop-up windows are present. [CVADHELP-28657]
- When you use USB audio devices in a Multi-Session OS session with Citrix Workspace app for Linux version 2503, audio redirection might fail due to incompatible USB protocols. [CVADHELP-29240]
- Some Fullscreen desktop sessions might fail to launch when the Mirror monitor feature is enabled in the local Linux system and desktop session initialization is attempted. [HDX-92829]

Known issues

- When you access web applications, such as Google Meet, through Chromium Embedded Framework-based Browser Content Redirection, certain UI elements might not respond to interactions. As a workaround, refresh the page to restore UI element functionality. [HDX-94506]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you configure device rules with a **Deny** rule in **Client USB device redirection rules** policy setting in Studio, certain devices that have been allowlisted in the same policy setting for passthrough into an HDX session with an **ALLOW** rule fail to get redirected. [HDX-95546]

2505

What's new

The following features are available in this release:

- Supporting Linux distributions
- App Protection support for eLux 7
- Improved proxy handling with FQDN support
- Enhancement to Fullscreen or Extend button behavior
- New storebrowse commands to create an autostart entry for boot-to-virtual-desktop
- Loss tolerant mode for graphics (Technical Preview)

Supporting Linux distributions

Citrix Workspace™ app for Linux version 2505 is supported on the following Linux distributions:

- openSUSE 15.6 x86-64
- RHEL 9.4 x86-64
- Ubuntu 2204 x86-64
- Ubuntu 2404 x86-64
- Raspberry Pi OS Bullseye, arm64
- Debian 11.9 x86-64
- Debian 12 to 12.6 x86-64

App Protection support for eLux® 7

Starting with this release, Citrix Workspace app for Linux supports App Protection on eLux 7. This integration provides enhanced security by helping protect against keylogging and screen capture threats when accessing virtual apps and desktops from eLux 7 devices. With App Protection enabled, organizations can better safeguard sensitive information and ensure compliance with security policies, even on thin client endpoints running eLux 7. For more information about App Protection, see the App Protection documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved proxy handling with FQDN support

Starting with 2505 version, Citrix Workspace app sends the Fully Qualified Domain Name (FQDN) of the target host in the CONNECT request to the proxy server when the target host is addressable by an FQDN.

Previously, Citrix Workspace app only sent the resolved IP address of the target host. This enhancement enables the proxy server to handle DNS resolution, supporting scenarios that require custom DNS configurations for specific domains.

Enhancement to Fullscreen or Extend button behavior

Starting with the 2505 version, the Fullscreen or Extend button adjusts display behavior based on the current configuration.

For more information, see Enhancement to Fullscreen or Extend button behavior.

New storebrowse commands to create an autostart entry for boot-to-virtual-desktop

Starting with 2505 version, to create an autostart entry for boot-to-virtual-desktop on endpoints, use the storebrowse command with the following syntax, depending on your Citrix Workspace app version:

For Citrix Workspace app version 2503:

```
./desktoplock <storeURL> <resourceName>
```

For Citrix Workspace app version 2505 and later:

```
./desktoplock --storeUrl <storeURL> --resource <resourceName>
```

For more information, see Configure Boot-to-Virtual-Desktop using script.

Technical Preview in 2505

- Loss tolerant mode for graphics

For more information, see the Features in Technical Preview page.

Fixed issues

- For sessions connected to a Linux or Mac VDA over TCP, the Connection Strength Indicator on the toolbar might incorrectly display a “Poor”status, even when the actual connection quality is good. [HDX-88899]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- During FIDO2 authentication, if you wait too long before scanning the displayed QR code, the QR code might expire. After expiration, there is no option to refresh or regenerate the QR code from the current screen. As a result, you cannot proceed with the login and must close and restart the authentication process to try again. [CVADHELP-27853]
- When using a Cloud Store with long-lived tokens disabled, you might experience authentication failures after logging in. This issue is particularly evident on Thin Client devices, where a "Session Launch Failed"error is displayed. [CVADHELP-27583]
- You might be prompted to re-authenticate on the redirected Browser Content Redirection (BCR) page, even if you have already authenticated on the VDA side in another tab. [CVADHELP-27449]
- You might be unable to launch a second seamless application if the Windows VDA is not configured to use the CP1252 character encoding (Windows Western European standard). [CVADHELP-27803]

Known issues

There are no new known issues.

2503

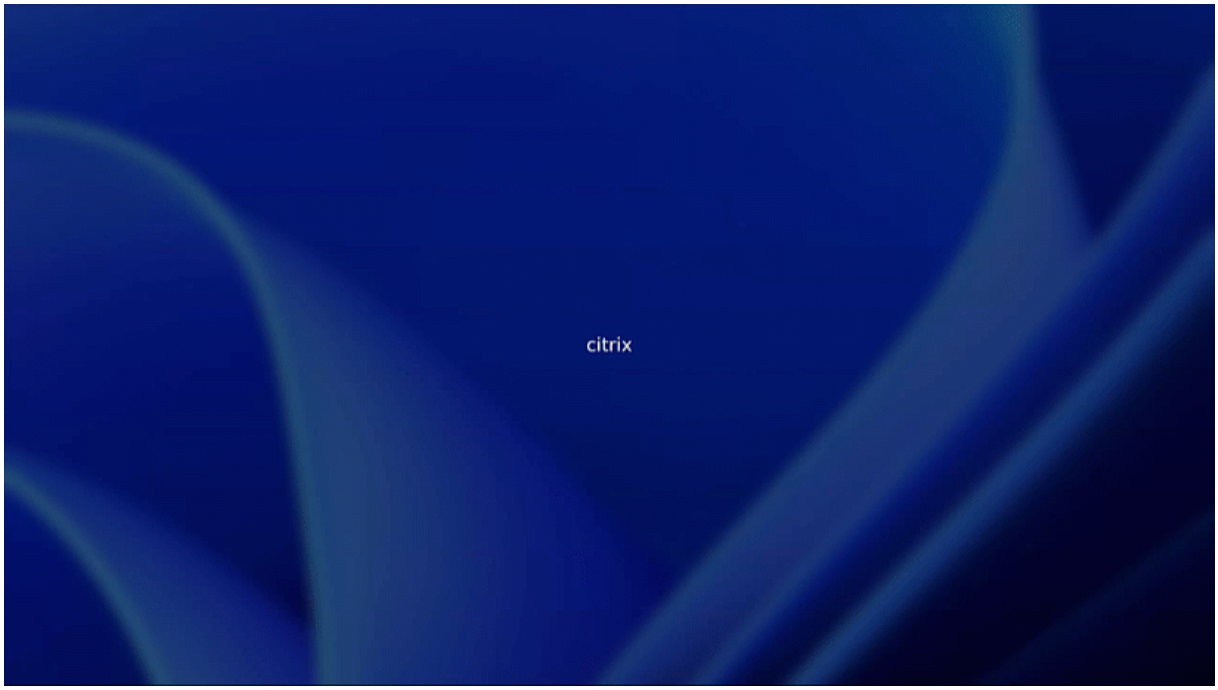
What's new

The following features are available in this release:

- Boot to Virtual Desktop
- Seamless Integration of deviceTRUST®
- Integration with eLux 7
- New command for storebrowse
- Connection strength indicator on Desktop Viewer toolbar
- On-screen keyboard enhancement for multi-touch
- Enhanced multi-monitor custom layout
- Enhanced battery status indicator
- Default audio device selection
- Bidirectional content redirection supports OAuth redirection
- Improved audio performance in Microsoft Teams
- Support for H.264 hardware decoding for seamless apps (Technical Preview)
- Enhanced keyboard and IME diagnostics tool

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Boot to Virtual Desktop Starting with 2503 version, Citrix Workspace app for Linux supports directly booting into a Virtual Desktop from the endpoint device. This feature simplifies the sign-in process for Citrix virtual desktops and is particularly beneficial for users who primarily work within the virtual environment during their workday.



For more information, see Boot to Virtual Desktop.

Seamless Integration of deviceTRUST Starting with 2503 version, Citrix Workspace app for Linux includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management.

For more information, see Seamless Integration of deviceTRUST.

Integration with eLux 7 This release introduces same-day availability and integration of the latest Citrix Workspace app with eLux 7. To download eLux 7, including Citrix Workspace app 2503 for Linux, visit the Downloads page.

New command for storebrowse Introducing a new command `-eu` to accept the End-User License Agreement (EULA) through the command line. This command bypasses the need for explicit user consent through the GUI.

For more information, see Accept End-User License Agreement (EULA).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connection strength indicator on Desktop Viewer toolbar Starting with 2503 version, Citrix Workspace app for Linux now supports the Connection Strength Indicator (CSI) on the Desktop Viewer toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

For more information, see Connection strength indicator on Desktop Viewer toolbar.

On-screen keyboard enhancement for multi-touch Starting with 2503 version, the on-screen keyboard functionalities are enhanced to better work with the multi-touch feature. This enhancement allows end users to use the digital on-screen keyboard on their device instead of relying on an additional external physical keyboard.

For more information, see Manage On-screen keyboard for multi-touch.

Enhanced multi-monitor custom layout Starting with 2503 version, we provide you with an enhanced multi-monitor experience that includes:

- A stable Citrix® session experience when using a full-screen session through the Custom Layout feature.
- Start a session with the saved monitor layout.

For more information, see Multi-monitor custom layout.

Enhanced battery status indicator Starting with 2503 version, the battery status indicator feature is compatible with CMB and ADP battery types. This enhancement allows users with devices using these newer battery technologies to also monitor battery life and prevent unexpected power loss during virtual desktop sessions, boosting user productivity.

For more information, see Battery status indicator.

Default audio device selection Starting with 2503 version, you can now select your preferred audio devices directly in the Desktop Viewer toolbar. This feature offers a more customized audio experience with the following key features when connected to a virtual desktop.

For more information, see Default audio device selection.

Bidirectional content redirection supports OAuth redirection Starting with 2503 version, Bidirectional content redirection supports OAuth redirection. For more information about the feature, see Bidirectional content redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved audio performance in Microsoft Teams Starting with 2503 version, the audio subsystem used in the HDXRTCMediaEngine has been replaced with a newer system. As a result, Microsoft Teams now provides better audio performance, enhancing the overall user experience during calls and meetings.

Enhanced keyboard and IME diagnostics tool Starting with version 2411, a new self-service command line tool hosted in Windows Virtual Desktop app is supported by Citrix Workspace app for Linux to diagnose keyboard and Input Method Editor (IME) related issues. This tool meets various user requirements, provides platform versatility, and caters to personalized needs. The keyboard and IME functions depend on different configurations and capabilities in Virtual Delivery Agent and Citrix Workspace app. Incorrect settings in the Virtual Desktop Agent or client side might result in unexpected input behavior.

For more information, see Enhanced keyboard and IME diagnostics tool.

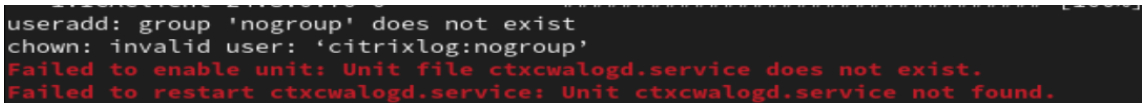
Technical previews

- Support for H.264 hardware decoding for seamless apps

For more information, see the Features in Technical Preview page.

Fixed issues

- You might encounter an installation error when installing Citrix Workspace for Linux on RHEL 9.

  [RFLNX-10747]

- For users running Citrix Workspace app for Linux version 2503 with Linux VDA versions lower than 2503, opening an app session on an external monitor might result in continuous flickering. [HDX-82101]
- For users running Citrix Workspace app for Linux version 2503 with Linux VDA versions lower than 2503, opening an app session on an external monitor mightn't display the session window properly in full screen. Instead, black borders might appear between the monitor bezels and the app session window. [HDX-82079]
- When the DTLS protocol setup fails, the microphone doesn't work when using UDP audio. [HDX-82340]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users experience difficulty configuring USB devices to automatically redirect to the session when the toolbar was not visible and the DDC version was lower than 2212. This issue occurrs because the `DesktopApplianceMode` key was deprecated starting with the 2405 release, following the introduction of Composite USB device redirection using DDC policies feature. This issue is now fixed by reintroducing the `DesktopApplianceMode` key, restoring the previous method for USB device redirection. [HDX-82090]

2411

What's new

The following features are available in this release:

- Supporting Linux distributions
- NFC support for FIDO2 authentication (Technical Preview)
- Echo cancellation
- Noise suppression
- Connection Strength Indicator on Desktop Viewer toolbar (Technical Preview)
- Enhanced desktop launch and screen resizing experience
- Multi-monitor custom layout (Technical Preview)
- Audio Quality Enhancer for Adaptive Audio (Technical Preview)
- Sustainability initiative from Citrix Workspace app
- Bidirectional content redirection
- HDX direct
- Customization of Desktop Viewer toolbar
- Support for WebHID API in UCSDK
- Support synchronizing Swedish keyboard layout

Supporting Linux distributions Citrix Workspace app for Linux version 2411 is supported on the following Linux distributions:

- RHEL 9.4 x86-64
- Ubuntu 2204 x86-64
- Ubuntu 2404 x86-64
- Raspberry Pi OS Bullseye, arm64
- Debian 11.9 x86-64
- Debian 12 to 12.6 x86-64

For more information, see System requirements and compatibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Echo cancellation Citrix Workspace app now supports echo cancellation feature designed to enhance real-time user experiences. This feature is enabled by default starting with the 2411 version.

For more information, see Echo cancellation.

Noise suppression With this release, Citrix Workspace app now offers improved audio redirection with enhanced noise suppression. This feature reduces background noise, ensuring clearer and more accurate speech, improving the overall communication experience.

For more information on enabling this feature, see Enable noise suppression.

Enhanced desktop launch and screen resizing experience With this release, Citrix Workspace app for Linux ensures an improved desktop launch and resizing experience. You'll experience a seamless, flicker-free transition to your desktop without intermediate screens.

For more information, see Enhanced desktop launch and screen resizing experience.

Sustainability initiative from Citrix Workspace app This feature helps conserve energy by reminding end users to sign out of the unused VMs when not required. When this feature is enabled, a prompt appears to sign out from the desktop session when a user closes a virtual desktop.

For more information, see Sustainability initiative from Citrix Workspace app.

Bidirectional content redirection With this release, admin can use the bidirectional content redirection feature that allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions.

For more information, see Bidirectional content redirection.

HDX direct When accessing Citrix-delivered resources, HDX Direct allows both internal and external client devices to establish a secure direct connection with the session host if direct communication is possible.

> **Note:**
>
> Starting with 2411 version, this feature is enabled by default.

For more information, see HDX direct documentation for Citrix Virtual Apps and Desktops.

Customization of Desktop Viewer toolbar With this release, you can customize the options on the **Desktop Viewer** toolbar using Global App Configuration service (GACS) or the `.ini` file.

For more information see, Customization of Desktop Viewer toolbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for WebHID API in UCSDK With this release, Citrix Workspace app for Linux supports the WebHID API to redirect Human Interface Device (HID) devices from endpoint to Unified Communication SDK application on the VDI. It complies to the HID standard for bi-directional communication between the application based on UCSDK and the HID devices connected to the endpoint.

For more information, see Support for WebHID API in UCSDK.

Support synchronizing Swedish keyboard layout With this release, Citrix Workspace app for Linux supports the Swedish (no support for dead keys) keyboard layout for Windows VDA.

For more information, see Keyboard layout support for Windows VDA and Linux VDA.

Technical previews in 2411

- NFC support for FIDO2 authentication
- Connection Strength Indicator on Desktop Viewer toolbar
- Multi-monitor custom layout
- Audio Quality Enhancer for Adaptive Audio

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

Fixed issues in 2411

- The installation of DEB packages is failing due to a dependency issue. Run the following command to resolve the issue:

  ```
  sudo apt-get install -f
  ```

  > **Note:**
  >
  > This fix is applicable for all DEB packages.

  [RFLNX-11883]

- The installation of RPM packages is failing due to a dependency issue. Run the following command to resolve the issue:

  ```
  sudo dnf install -y <ICAClient package>
  ```

  > **Note:**
  >
  > This fix is applicable for all RPM packages.

  [RFLNX-11878]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might notice that SaaS apps fail to open and display the following error message:

  "curl_easy_perform() failed: SSL connect error in /var/log/citrix/ICAClient.log."

  [RFLNX-10891]

- When App Protection is enabled, Microsoft Teams optimization might become unresponsive, causing issues with screen sharing. [HDX-71222]
- WebCam redirection uses additional bandwidth constraints for each resolution to ensure interactivity and image quality. [HDX-67168]
- When you install Citrix Workspace app for Linux using the Debian package Manager on Ubuntu version 22.04, you get the following error:

  "A dependency job for AppProtectionService-install.service failed. See 'journalctl -xe'for details."

  You get this error even though App Protection is successfully installed. [RFLNX-9995]

- For users who access Windows virtual desktop through Citrix Workspace app for Linux, they might be prompted with the Windows login screen when clicking multiple apps quickly one after another within the desktop session. [CVADHELP-26189]
- Browser content redirection fails when users close and restart the Microsoft Edge browser within a published desktop session opened through Citrix Workspace app for Linux. [CVADHELP-25418]

2408

What's new

The following features are available in this release:

- Support for RHEL 9.4 x86-64, Ubuntu 2204 x86-64, Raspberry Pi OS Bullseye-arm64, Debian 11.9 x86-64
- Enhanced virtual desktop screen resizing experience
- Enhanced Desktop Viewer toolbar
- Customize toolbar
- Accessibility support for enhanced Desktop Viewer toolbar
- Performance optimization for graphics
- Endpoint Analysis support for multi-factor (nFactor) authentication
- Enhancement to Storebrowse commands
- Multiple webcam resolutions support
- Fast smart card
- Improved loading experience for shared user mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Support for Optimized Microsoft Teams on ARM64 devices
- Version upgrade for Chromium Embedded Framework
- App protection
- Provision to manage multiple proxy servers
- Support for Cryptography Next Generation smartcards
- GACS supports Citrix Workspace app for Linux [Technical Preview]
- NFC support for FIDO2 Authentication [Technical Preview]
- Enhanced Unified Communications SDK API [Technical Preview]
- Support for WebHID API in UCSDK [Technical Preview]
- Support integrated windows authentication for browser content redirection [Technical Preview]
- Support for H.264 and H.265 hardware decoding [Technical Preview]
- Clipboard Support for HTML-formatted text [Technical Preview]

Support for RHEL 9.4 x86-64, Ubuntu 2204 x86-64, Raspberry Pi OS Bullseye-arm64, Debian 11.9 x86-64

Citrix Workspace app for Linux version 2408 is supported on the following Linux distributions:

- RHEL 9.4 x86-64
- Ubuntu 2204 x86-64
- Raspberry Pi OS Bullseye, arm64
- Debian 11.9 x86-64

For more information, see System requirements and compatibility.

Enhanced virtual desktop screen resizing experience

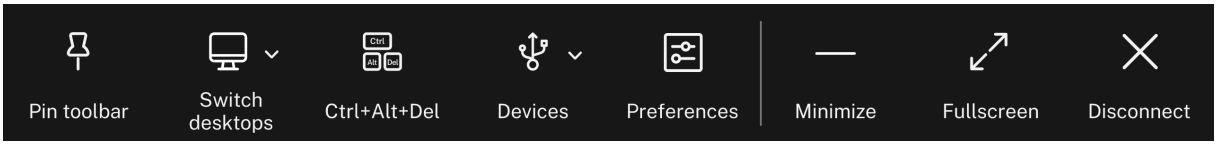
Starting with the 2408 version, Citrix Workspace app for Linux ensures a smooth transition and prevents black screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

For more information, see the Enhanced virtual desktop screen resizing experience documentation.

Enhanced Desktop Viewer toolbar

Starting with the 2408 version, Citrix Workspace app for Linux provides an enhanced Desktop Viewer toolbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The enhanced Desktop Viewer toolbar provides the following options:

- Show or hide toolbar - Click this button to show or hide the Desktop Viewer toolbar
- Switch desktop - Click this button to see the available open desktops. You can switch to another desktop by clicking the desktop that you want to access. The opened desktop shows in the front.
- Ctrl+Alt+Del - Click this button to access the shortcuts. The available shortcut is Ctrl+Alt+Del.
- Devices - Click this button to access the options in the **Devices** section.
- Preferences - Click this button to access the options in the **Preferences** section.
- Minimize - Click this button to minimize the virtual session.
- Fullscreen or Restore - Click the "Fullscreen"button to expand the desktop session to full screen. Click the "Restore"button to restore the full screen session to the previous window mode.
- Disconnect / Sign out - Click this button to sign out or to disconnect from a virtual session.

For more information, see the Enhanced Desktop Viewer toolbar documentation.

Customize toolbar

Previously, you could completely disable the **Desktop Viewer** toolbar. However, you couldn't enable or disable a few options on the toolbar. Starting with the 2408 release, you can customize the Citrix Workspace app toolbar by adding and removing options on the toolbar.

For more information, see the Customize toolbar documentation.

Accessibility support for enhanced Desktop Viewer toolbar

Starting with the 2408 version, you can access the enhanced Desktop Viewer toolbar using the keyboard of your endpoint devices. With this feature, you can invoke the toolbar, navigate through the options, and select the required options using the keyboard shortcuts.

For more information, see the Accessibility support for enhanced Desktop Viewer toolbar documentation.

Performance optimization for graphics

Citrix Workspace app 2408 ** version supports OpenGL library that improves the performance of graphics usage within an HDX session.

For more information, see the Performance optimization for graphics documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Endpoint Analysis support for multi-factor (nFactor) authentication

Starting with this release, Citrix Workspace app supports Endpoint Analysis (EPA) for multi-factor authentication, enhancing compliance and security. For example, if EPA and LDAP are configured as part of multi-factor authentication, Citrix Workspace app detects and runs the EPA app for authentication along with the LDAP authentication.

Previously, Citrix Workspace app did not support invoking the EPA app, resulting in an "Access Denied"error. This release supports EPA invocation, allowing the authentication process to proceed smoothly.

The new feature ensures comprehensive endpoint security checks, compliance with organizational policies, and regulatory requirements. It reduces the risk of unauthorized access and improves overall network integrity.

For more information, see Endpoint Analysis support for multi-factor (nFactor) authentication.

Enhancement to Storebrowse commands

Starting with the 2408 version, the following Storebrowse commands are updated for extra functionality:

- `-a`: Previously, this command added a store and all linked accounts for the given URL. With this release, it adds a store for a given URL.
- `-as`: This new command adds a store and all linked accounts for the given URL.

For more information, see Add a store documentation.

Multiple webcam resolutions support

Previously, only the VGA resolution was supported for webcam redirection.

Starting with the 2408 release, Citrix Workspace app for Linux supports high-definition webcam streaming for all webcam resolutions that are available on the client side. If media type negotiation fails, HDX now defaults back to the default VGA resolution (640 x 480 pixels). For more information, see the Multiple webcam resolutions support documentation.

Fast smart card

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN environments.

Fast smart cards are supported on Windows VDA only.

For more information, see the Fast smart card documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved loading experience for shared user mode

The time taken to load the store is reduced and thus the loading experience for the shared user mode is improved.

> **Note:**
>
> This feature is applicable only on StoreFront™ stores.

This feature is disabled by default. For more information,see the Improved loading experience for shared user mode documentation.

Support for Optimized Microsoft Teams on ARM64 devices

Starting with the 2408 version, the Optimized Microsoft Teams feature is supported on ARM64 architecture-based endpoint devices running Citrix Workspace app for Linux.

For more information, see the Support for Optimized Microsoft Teams on ARM64 devices documentation.

Provision to manage multiple proxy servers

Previously, Citrix Workspace app did not support the usage of multiple proxy servers. Startign with the 2405 version, you can use multiple proxy servers that allow the HDX sessions to select appropriate proxy servers for accessing specific resources. This selection is based on the proxy rules configured in the Proxy Auto-Configuration (PAC) file. Using this file, you can manage the network by mentioning which network traffic must be sent through a proxy server and which must be sent directly.

This feature is disabled by default. For more information, see Provision to manage multiple proxy servers.

Support for Cryptography Next Generation smartcards

With this release, Citrix Workspace app supports the new Personal Identification Verification (PIV) smartcard that uses Elliptic Curve Cryptography (ECC) algorithm. This type of smartcard works based on Cryptography Next Generation.

This enhancement is part of Fast smart card. For more information, see Fast smart card section.

Version upgrade for Chromium Embedded Framework

The version of the Chromium Embedded Framework (CEF) is upgraded to 128.0.6613.120. This upgraded version includes fixes for known security vulnerabilities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App Protection

Configure allow list for the apps which use LD_Preload functionalities App Protection blocks the launch of a protected session if other apps running use LD_PRELOAD. If there are genuine apps or if approved by the admin, you can use the allow list feature. To permit the use of other apps which use LD_PRELOAD, you must configure the allow list.

For more information, see the Allow list with LD_Preload functionalities documentation.

Technical previews

- GACS supports Citrix Workspace app for Linux
- NFC support for FIDO2 Authentication
- Enhanced Unified Communications SDK API
- Support for WebHID API in UCSDK
- Support integrated windows authentication for browser content redirection
- Support for H.264 and H.265 hardware decoding
- Clipboard Support for HTML-formatted text

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

Fixed issues

- When you exit the network printer settings, you might notice that the Citrix Workspace app for Linux shifts focuses incorrectly to a previous window. [CVADHELP-25465]
- When you access the Windows VDA session through Citrix Workspace app for Linux, you might notice that the keyboard stops responding inside the virtual session. [CVADHELP-25073]
- You might notice that the lease files are not getting downloaded while running the command `/storebrowse -o <full store url>`. [HDX-65544]
- When you set `ConnectionBar=0` in ~/.ICAClient/All_Regions.ini, you might notice that the USB devices are not auto-redirected to the virtual session. [HDX-68850]
- When you run the ‘storebrowse -WT‘ command, you might notice that the launched sessions did not sign out successfully. [RFLNX-11597]
- When Plug and Play (PnP) is enabled, you might fail to switch webcam from the apps that shows only one camera with a generic name “Citrix HDX Web Camera”. [HDX-67792]

2405

What’s new

The following features are available in this release:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Support for RHEL9 x64 , Ubuntu 2204 x86-64, RaspiOS-bullseye-arm64 , Debian 11x86-64
- Enhanced system logs for browser content redirection
- Improved loading experience for shared user mode
- UI option to manage monitor plug and play feature
- Support for authentication using FIDO2 when connecting to cloud stores
- Composite USB device redirection using DDC policies
- Enhanced the user interface for seamless login experience
- Support for multiple passkeys in HDX session
- Version upgrade for Chromium Embedded Framework
- Deprecation announcement of PNAgent support
- Deprecation announcement of SUSE
- Deprecation notice

Support for RHEL9 x64 , Ubuntu 2204 x86-64, RaspiOS-bullseye-arm64 , Debian 11x86-64 Citrix Workspace app for Linux version 2405 is supported on following distributions:

- RHEL9 x64
- Ubuntu 2204 x86-64
- Raspberry Pi OS Bullseye, arm64
- Debian 11x86-64

For more information, see System requirements and compatibility.

Enhanced system logs for browser content redirection With the enhancements to the system logs, browser content redirection now allows admins to monitor the feature status. For more information, see Browser content redirection.

Improved loading experience for shared user mode Starting with the 2405 version, the time taken to load the store is reduced. With this feature, the loading experience for the shared user mode is improved.

> **Note:**
>
> This feature is applicable only on on-premises stores.

This feature enabled by default. For more information, see Improved loading experience for shared user mode.

Support for authentication using FIDO2 when connecting to cloud stores Starting with Citrix Workspace app for Linux version 2405, users can authenticate using passwordless FIDO2 security keys

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when signing in to cloud stores. The security keys support different types of security inputs such as security pins, biometrics, card swipe, smart card, Public Key Certificates, and so on. For more information, see FIDO2 Authentication.

Administrators can configure the type of browser to authenticate to Citrix Workspace app. For more information, see Support for authentication using FIDO2 when connecting to cloud stores.

UI option to manage monitor plug and play feature Previously, you had to enter `MultiMonitorPnPEnable=True` in the [WFClient] section of the `$HOME/.ICAClient/wfclient.ini` file to enable the monitor plug and play feature.

With this release, a new UI option, the **Automatically extend desktop session to external monitors** checkbox is available to enable or disable the monitor plug and play feature. For more information, see UI option to manage monitor plug and play feature.

```
1 ![Audio preferences](/en-us/citrix-workspace-app-for-linux/media/audio-
    preferences.png)
```

Composite USB device redirection using DDC policies Previously, the composite USB device redirection was managed on the client side. There was no option to manage it on VDA.

Starting with the 2405 release, you can manage the composite USB device redirection on VDA using the DDC policies. The rules set on the VDA take preferences over the rules set on the client. Client can interpret the value set on VDA.

With this release, Citrix Workspace app for Linux supports the following policies which helps you to manage the usage of the composite USB device redirection:

- Client USB device redirection
- Client USB device redirection rules
- Client USB device redirection rules (Version 2)
- Allow existing USB devices to be automatically connected
- Allow newly arrived USB devices to be automatically connected

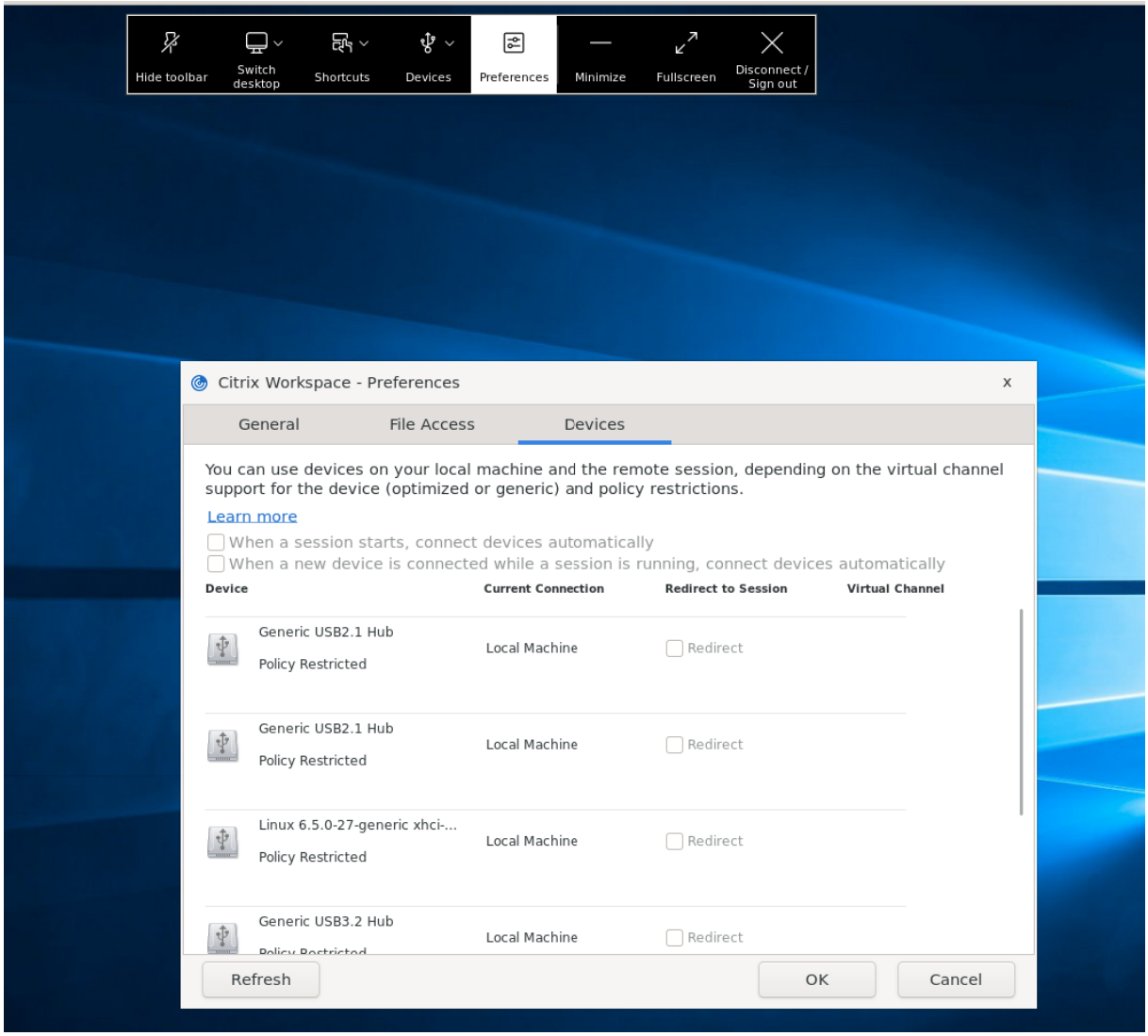
> **Note:**
>
> To configure the preceding polices, users can refer to the documents see Client USB device redirection document.

Desktop Viewer's updates according to the polices

- If the **Client USB device redirection** policy is set to *Prohibited* on DDC, the **Devices** on the toolbar will be set to insensible and the **Devices** option on the **Citrix Workspace app - Preferences** screen won't be visible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Based on the values set for **Allow existing USB devices to be automatically connected** and **Allow newly arrived USB devices to be automatically connected** policies, the following checkboxes might be enabled or disabled on the **Devices** option on the **Citrix Workspace app - Preferences** screen:
  - **When a session starts, connect devices automatically**
  - **When a new device is connected while a session is running, connect devices automatically**

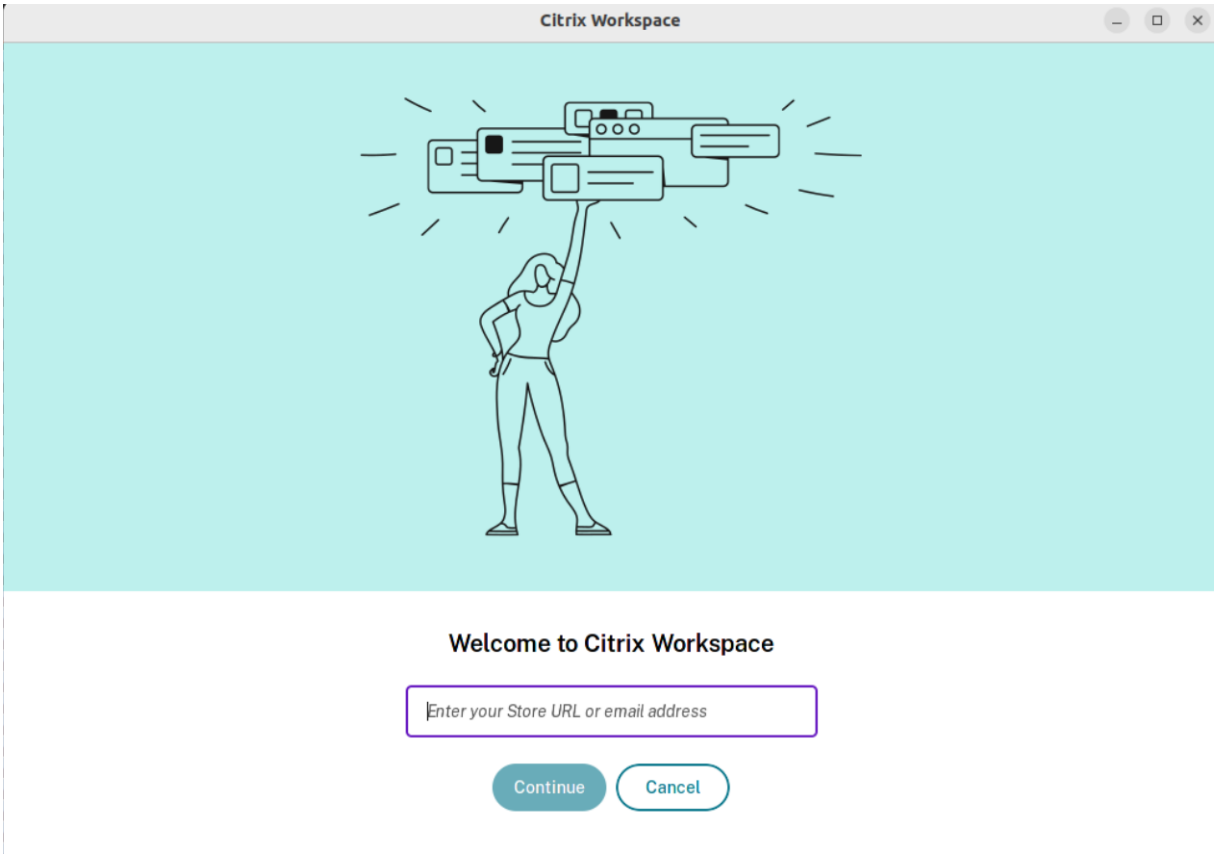


Enhanced the user interface for seamless login experience Starting with the 2405 release, Citrix Workspace app for Linux's user interface has been enhanced to be more modern and provides seamless login experience for first time users.

Previously, Citrix Workspace app for Linux were using two different GTK windows for store addition

© 1997–2026 Citrix Systems, Inc. All rights reserved.

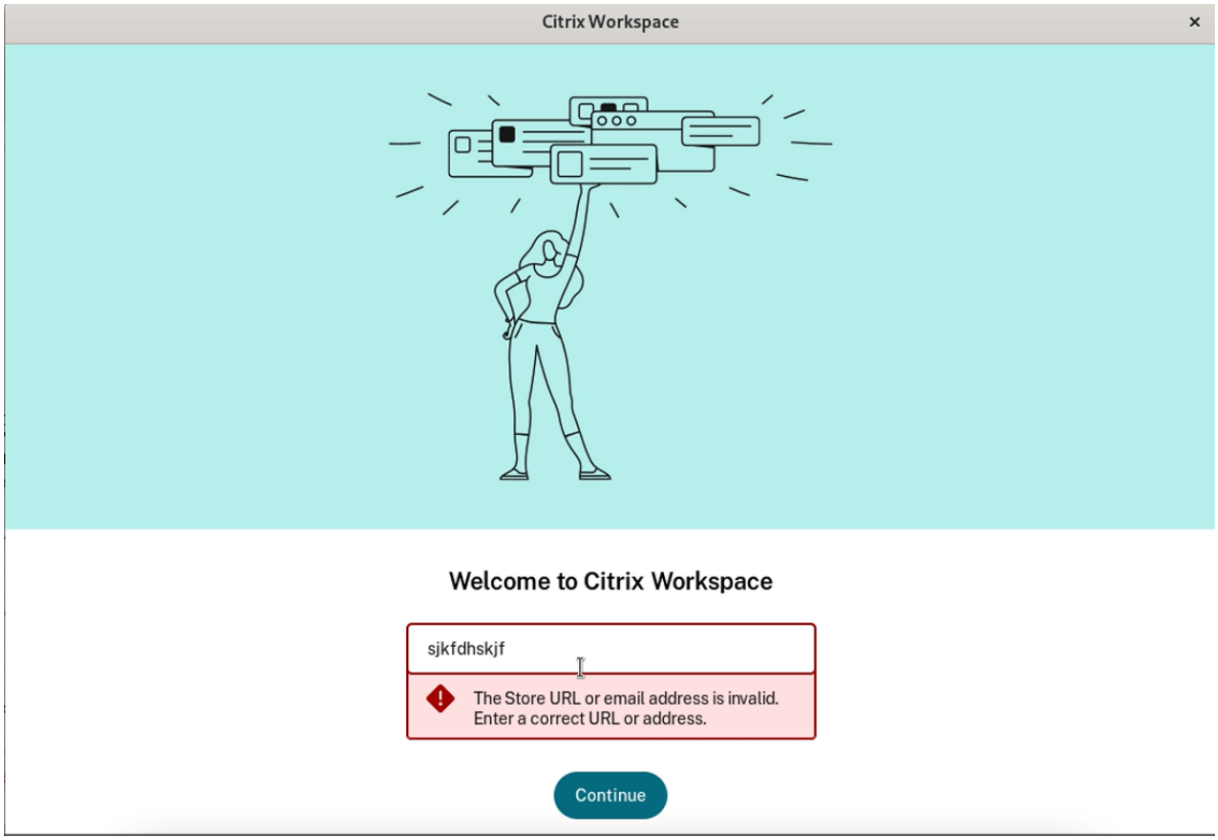
and enumeration of the resources. With this release, Citrix Workspace app displays the Welcome page with the option to add the store using the store url, e-mail id, or fully qualified domain name (FQDN).



This feature also includes the following enhancements to the UI:

After completing the installation, the option to login now or skip login for later is displayed.
If the user enters invalid store url, invalid or incomplete e-mail id, or invalid IP adress, an intuitive error message is displayed based on the input.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

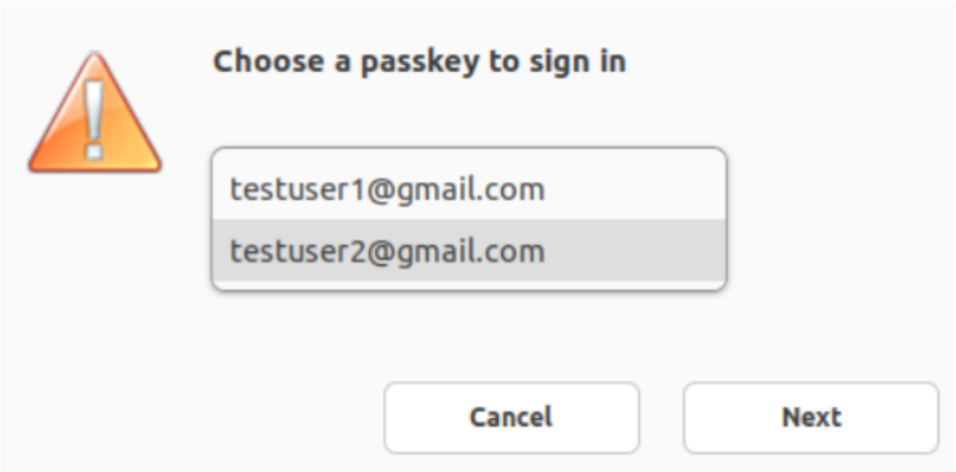


For more information, see Enhanced the user interface for adding store.

Support for multiple passkeys in HDX session Previously, when there were multiple passkeys associated with a security key or FIDO2 device, you were not having an option to select an appropriate passkey. By default, the first passkey was used for authentication.

Starting with the 2405 version, you can select an appropriate passkey from the Citrix Workspace app UI. This feature is enabled by default.
When there are multiple passkeys, the first one is selected as default. However, you can select the appropriate passkey as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Version upgrade for Chromium Embedded Framework The version of the Chromium Embedded Framework (CEF) is upgraded to 124. This upgraded version includes fixes for known security vulnerabilities.

Deprecation announcement of PNAgent support Starting from the 2405 release, support for XenApp® Services URLs (also known as PNAgent) for connecting to stores is deprecated. Alternatively, you can connect to stores using the store URL. For reference, see:

Deprecation page in the Citrix Workspace app for Linux documentation.

Deprecation notices in the StoreFront documentation.

Deprecation announcement of SuSE Starting from the 2405 version, the support for SuSE is deprecated and will be removed in the future release. For more information, see Deprecation.

Deprecation notice Starting with the 2405 version, support for the following items is deprecated and removed:

- ArmHF
- SoftwareMouse
- invert-cursor
- Raspberry Pi 3/3B support
- GDI
- GTK2
- VDSCARD.DLL

For more information, see Deprecation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Technical previews

- PDF Universal Printing
- Provision to manage multiple proxy servers
- Support for Cryptography Next Generation smartcards
- Multiple webcam resolutions support
- HDX direct
- Performance optimization for graphics
- AI-based noise suppression

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

Fixed issues

- When you install Citrix Workspace app for Linux 2402 version, the set log fields might not be populated correctly. This issue occurs when you install or upgrade Citrix Workspace app for Linux on a machine where Citrix Workspace app was already present. [RFLNX-11045]
- When you change the default `KeyboardSync` to *Off* setting in `module.ini`, typing characters with dead keys like circumflex ^, might cause the wfica process to fail. [HDX-63237]
- You might face visual artifacts in an app session. This issue occurs when you drag the app session to the edge of a screen to make it to a maximum window. [HDX-53648]
- You can't do screen sharing from chat using Optimized Microsoft Teams 2.1. [HDX-62703]
- You might notice that the echo cancellation is disabled if the Share System audio feature is enabled. [HDX-65123]
- You might notice the text overlap on the **Add Mapped Drive** window that opens from the **Preferences > File** menu for the non-English language UI of Citrix Workspace app for Linux. [RFLNX-11321]
- You might notice that the **Citrix Log Collection Utility** does not open more than once when accessed from the app indicator by navigating to **Troubleshooting > Collect logs**. [RFLNX-10911]
- The self-service user interface might stop responding when the session launch fails. [RFLNX-11195]
- Citrix Workspace app for Linux might fail to read the name of the Dell Wyse thin clients. [CVADHELP-23136]
- You might face visual artifacts when dragging the app window or connection bar in the virtual desktop session running on the thin client endpoints. [CVADHELP-24516]
- If you set the gRPCEnabled flag to false, the browser content redirection feature might stop responding when you run the storebrowse -K command after signing in and launching a session. From the 2405 version, the Storebrowse -K functionality are changed as follows:
    - Functionality of `storebrowse -k` is included in `storebrowse -K`. `storebrowse -k` is deprecated now.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - When you set `gRPCEnabled = false`, the authamangerdaemon process is not killed.
  - The sign out option is removed from `storebrowse -K`. To sign out of the session, use `storebrowse -WT`. [CVADHELP-25162]

- You might notice that 'UtilDaemon'crashes when the 'getCustomStoreUrls'command is executed. [RFLNX-11327]
- When using the snipping tool in a virtual desktop session to snap screenshots, you might notice that the gray out doesn't function properly on the extended monitors. [CVADHELP-24534]
- You might notice that the session sharing feature for the seamless app session is not working properly. When you launch the virtual app, the app is launched in a new session instead of sharing the existing session. [CVADHELP-25042]
- Citrix Workspace app for Linux might fail to read the name of the Dell Wyse thin clients. [CVADHELP-23136]

2402

What's new

The following features are available in this release:

- Synchronize multiple keyboards at session start
- Enhancement for composite USB auto-redirection
- Loss tolerant mode for audio
- Support for Audio volume synchronization
- Version upgrade for Chromium Embedded Framework
- Support for GTK3
- Availability of Credential Insertion SDK for cloud stores
- Improved UI for error messages
- Introduction of a new command in Storebrowse
- Send feedback on Citrix Workspace app
- Configure UDP port range for Microsoft Teams optimization
- Enhanced Desktop Viewer toolbar [Technical Preview]
- Customize toolbar [Technical Preview]
- Sustainability initiative from Citrix Workspace app [Technical Preview]
- Include system audio while screen sharing [Technical Preview]

Synchronize multiple keyboards at session start Previously, only the active keyboard on the client was synchronized with VDA after the session started in full-screen mode. In this scenario, if you configured **Sync only once - when session launches** on your Citrix Workspace app, and you had to change to a different keyboard, you have to manually install the keyboard on your remote desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature is used mostly when the client side keyboard input mode is scancode input mode. Users can select a keyboard layout in a remote session as the active keyboard layout which is synchronized from the client keyboard layout list.

Starting with the 2402 version, all available keyboards on the Linux client are synchronized with VDA after the session starts in full-screen mode. You can select the required keyboard from the list of installed keyboards on the VDA, after the session starts in full-screen mode.

For more information, see Synchronize multiple keyboards at session start.

Enhancement for composite USB auto-redirection Previously, you had to set **DesktopApplianceMode** to *True* in the configuration file to auto-redirect USB devices when a session starts.

With this release, you are able to manage device connection settings from a UI on the Citrix Workspace app for Linux, without having to depend on configuration files.

For more information, see Enhancement for composite USB auto-redirection.

Loss tolerant mode for audio Starting with the 2402 version, Citrix Workspace app supports loss tolerant mode (EDT lossy) for audio redirection. This feature improves the user experience for real-time streaming when users are connecting through networks with high latency and packet loss. By default, this feature is enabled.

For more information, see Loss tolerant mode for audio.

Support for Audio volume synchronization Starting with the 2402 version, Citrix Workspace app for Linux supports synchronization of audio volume between the VDA and your audio devices. You can now tune the volume using the VDA audio volume slider and have the same volume on your device and the other way around. This feature is enabled by default.

For more information, see Support for Audio volume synchronization.

Version upgrade for Chromium Embedded Framework The version of the Chromium Embedded Framework (CEF) is upgraded to 120. This upgraded version includes fixes for known security vulnerabilities.

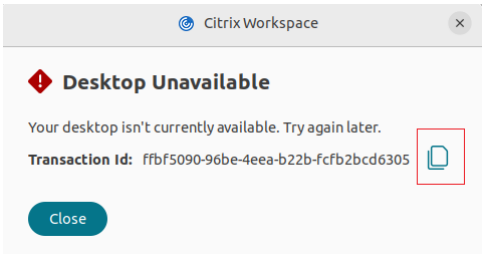
Support for GTK3 Previously, the `configmgr`, `conncenter`, and `setlog` executables within Citrix Workspace app were using GTK2. With this release, these executables are migrated to GTK3.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Availability of Credential Insertion SDK for cloud stores Previously, using the Credential Insertion SDK, you could authenticate only on on-premises stores. With this release, you can now authenticate users on the Self-Service plug-in using SSO on cloud stores.
For more information, see Availability of Credential Insertion SDK for cloud stores

Improved UI for error messages The error messages UI is improved. Previously, the `UIDialog` library was used to display error messages. From this release, the gtk library is‘ used in error messages. This enhancement improves the user experience.

Also, a transaction ID along with a copy to clipboard button is available for the user’s convenience.



Send feedback on Citrix Workspace app The **Send Feedback** option allows you to inform Citrix about any issues that you might run into while using Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

For more information, see Send feedback on Citrix Workspace app.

Introduction of a new command in Storebrowse A new command `-lt` is introduced to list out all types of enabled authentication methods for StoreFront. This command supports using the credential insertion SDK.

For more information, see List authentication methods.

Configure UDP port range for Microsoft Teams optimization With this release, you can specify the minimum and maximum range of UDP ports for Microsoft Teams optimization. If the UDP Port cannot be allocated for any reason, the WebRTC falls back to TCP. This feature helps you to use the minimum ports that you require.

For more information, see Configure UDP port range for Microsoft Teams optimization.

Technical previews

- Customize toolbar
- Sustainability initiative from Citrix Workspace app

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Include system audio while screen sharing

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

Fixed issues

- Unified Communications SDK (UC SDK) API might be unresponsive during reopening of an app within Citrix Workspace app. [HDX-59993]
- You might fail to redirect the Android phone as a generic USB redirection. [HDX-52166]
- The name of the audio devices are truncated to 32 characters while passing from Citrix Workspace app to VDA. As a result, the device might not be recognized in the client session by some apps. [HDX-53405]
- Sometimes, Citrix Workspace app session might disconnect on thin clients. [CVADHELP-24787]
- When the File Type Association feature and client drive mapping feature are enabled, you might notice that the file saved on the client machine is blank when opened using a published app. [CVADHELP-24496]
- You might face intermittent session disconnects on Dell Wyse thin clients. This issue occurs for users who uses the smartcard for authentication. [CVADHELP-23776]
- You might notice that the NITGEN FDU06M/S fingerprint sensor device isn't supported for generic USB redirection. [CVADHELP-23852]
- You might notice that the Thales DactyID20 fingerprint sensor device isn't supported for generic USB redirection. [CVADHELP-24076]
- When you use FIDO2 authentication, you might notice that you can open the second tab and open local files using the shortcut keys. [CVADHELP-24605]
- You might notice that the client machine might reboot when you highlight or select text on the second monitor. This issue occurs if the `InvertCursorEnabled` parameter is set to *True*. [CVADHELP-24106]
- Citrix Workspace app might fail to respond while you are in a session. This issue occurs randomly when you use a smartcard for authentication. [CVADHELP-23895]
- Citrix Workspace app for Linux might close abruptly when you configure a cloud store on StoreFront. [RFLNX-10976]

2311

What's new

The following features are available in this release:

- Support for DPI matching
- Support for IPv6 UDP with DTLS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Support for IPv6 TCP with TLS
- Multi-touch support
- Enhancement to multiple monitors
- Version upgrade for Chromium Embedded Framework
- Multimedia Redirection support for ARM64 devices
- Enhancement to Storebrowse commands
- Addition of a new library
- Collecting user activity logs
- Fast smart card [Technical Preview]
- Loss tolerant mode for audio [Technical Preview]
- Improved loading experience for shared user mode [Technical Preview]
- Support for audio volume synchronization [Technical Preview]
- App Protection compatibility with HDX optimization for Microsoft Teams [Technical Preview]

Support for DPI matching The display resolution and DPI scale values set in the Citrix Workspace app match to the corresponding values in the virtual apps and desktops session. You can set the required scale value in the Linux client, and the scaling of the VDA session is updated automatically.

DPI scaling is mostly used with large-size and high-resolution monitors. This feature helps to display the following in a size that can be viewed comfortably:

- Applications
- Text
- Images
- Other graphical elements

> **Note:**
>
> The DPI matching feature supports only GNOME, KDE, and Xfce desktop environments.

This feature is disabled by default. You can enable this feature using the command-line interface or GUI. For more information, see Support for DPI matching.

Support for IPv6 UDP with DTLS Previously, DTLS connections between Citrix Workspace app for Linux and Virtual Delivery Agents (VDAs) were supported over the IPv4 network only.

With this release, Citrix Workspace app supports DTLS connections over both IPv4 and IPv6.

This feature is enabled by default.

For more information, see Support for IPv6 UDP with DTLS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for IPv6 TCP with TLS Previously, TLS connections between Citrix Workspace app for Linux and Virtual Delivery Agents (VDAs) were supported over the IPv4 network only.

With this release, Citrix Workspace app supports TLS connections over both IPv4 and IPv6.

This feature is enabled by default.

For more information, see Support for IPv6 TCP with TLS.

Multi-touch support The multi-touch support feature in Citrix Workspace app for Linux supports multi-touch devices. This feature allows devices to receive input from the touch screen. The input includes touch gestures and interactions using a pen or a stylus device. You can interact with multi-touch screens while using apps or desktops in an HDX session.

For more information, see Multi-touch support.

Enhancement to multiple monitors When using multiple monitors, if you dock or undock your primary endpoint machine from a docking station, the session extends to the monitors automatically with the updated layout. Also, when you start a session with multiple monitors, the session is extended to those monitors. If you add or remove monitors, the session is adapted to the newly available screens.

> **Note:**
>
> This feature supports a primary monitor and one secondary monitor only.

By default, this feature is disabled. For more information, see Enhancement to multiple monitors.

Version upgrade for Chromium Embedded Framework The version of the Chromium Embedded Framework (CEF) is upgraded to 117. This version upgrade helps to resolve security vulnerabilities.

Multimedia redirection support for ARM64 devices The multimedia redirection feature is supported on ARM64 architecture-based endpoint devices running Citrix Workspace app for Linux. For more information, see Support for ARM64 architecture.

Enhancement to Storebrowse commands The following Storebrowse commands are enhanced for extra functionality:

- `-l` - Previously, this command was listing only single stores added to an account. With this release, this command lists multi-stores as well.
- `-a` - Previously, this command adds a single store and returns the URL of the store. With this release, along with the existing functionality, this command adds all URLs when multiple accounts are available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `-K` - Previously, this command was only terminating all the `Storebrowse` daemons. With this release, the `-K` command helps to sign out from the StoreFront, cloud stores, or NetScaler® Gateway.

Improved loading experience for shared user mode The time taken to load the store is reduced and thus the loading experience for the shared user mode is improved.

> **Note:**
>
> This feature is applicable only on StoreFront stores.

This feature is disabled by default. For more information, see Improved loading experience for shared user mode.

Addition of a new library With this release, a new library `UIDialogLib3.so` that supports gtk 3 is added in Citrix Workspace app.

> **Note:**
>
> The `UIDialogLib3.so` is installed as part of Citrix Workspace app for Linux 2311 version installation.

Collecting user activity logs You can collect the user activity logs. Activities related to most of the `Storebrowse` commands are saved in the log file. You can find the log files within the following location:

```
${ HOME } /.ICAClient/logs/userActivitylog/
```

By default, the user activity logs are enabled. For more information, see Collecting user activity logs.

Technical previews

- Loss tolerant mode for audio
- Improve audio performance during audio loss
- Support for Audio volume synchronization
- Fast smart card
- App Protection compatibility with HDX optimization for Microsoft Teams

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The video image might be stretched in an optimized Microsoft Teams video call. To enable this fix, add the `AdaptResolutionAllowCroppingVideo` parameter in your `config.json` file as follows:

```
/var/.config/citrix/hdx_rtc_engine/config.json
{

"AdaptResolutionAllowCroppingVideo"
: 1
 }
```

  If the preceding config.json file doesn't exist, create it.

  [HDX-55028]

- After visiting a browser content redirected site, if you sign out from the user session, an error message might appear. [HDX-55087], [HDX-52897]
- When you right-click the system tray icon of the published app, you might notice that the pop-up menu appears away from the system tray icon. [CVADHELP-22224]
- You might notice that the Epic Hyperspace opens partially off screen after you upgrade from Citrix Virtual Apps and Desktops 7.15 CU4 to 19.12 CU5 and upgrade the Epic Hyperspace to the November 2021 version. [CVADHELP-21563]

2309

What's new

The following features are available in this release:

- Support for ARM64 architecture
- Support for authentication using FIDO2 when connecting to on-premises stores
- Support for 32-bit cursor
- Copy and paste files and folders between two virtual desktops
- Screen pinning in custom web stores
- Keyboard input mode enhancements
- Support for extended keyboard layouts
- Enhancement to multiple monitors [Technical Preview]
- Improved error messages
- Enhancement to log collection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for ARM64 architecture Citrix Workspace app for Linux supports ARM64 architecture-based devices. For this feature, we have included binaries that allow to install Citrix Workspace app on ARM64-based devices in the installer package. The prerequisites and system requirements remain the same as installing the app on other architectures.

> **Note:**
>
> The following features aren't supported on Citrix Workspace app for Linux when using ARM64 architecture-based devices:
>
> - Optimized Microsoft Teams
> - Optimized Skype for Business (RTOP/RTME)
> - Browser Content Redirection (BCR)

Support for authentication using FIDO2 when connecting to on-premises stores Users can authenticate using passwordless FIDO2 security keys when signing in to on-premises stores through Citrix Workspace app for Linux. The security keys support different types of security inputs such as security pins, biometrics, card swipe, smart card, Public Key Certificates, and so on. For more information about FIDO2, see FIDO2 Authentication.

Administrators can configure the type of browser to authenticate to Citrix Workspace app. For more information, see Support for authentication using FIDO2 when connecting to on-premises stores.

Support for 32-bit cursor Previously, when you were using the custom 32-bit cursor, a black box might appear around the cursor.

Starting with Citrix Workspace app for Linux version 2212, support for the 32-bit cursor was enabled by default. As a result, the black box around the cursor issue is resolved.

With this release, you can disable the support for the 32-bit cursor. For this enhancement, a new parameter named `Cursor32bitSupport` is added in the `wfclient.ini` file.

For more information, see Support for 32-bit cursor.

Copy and paste files and folders between two virtual desktops Previously, you can copy only text between two virtual desktops. With this release, you can copy and paste files and folders between two virtual desktops. In the Linux Virtual Delivery Agent, the maximum transfer of data in one single copy-paste operation is 200 MB. For more information, see File copy and paste documentation.

This feature is enabled by default. For more information, see Copy and paste files and folders between two virtual desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Screen pinning in custom web stores The screen pinning in custom web stores allows you to save the selection for multi-monitor screen layout in custom web stores.

For more information, see Screen pinning in custom web stores.

Keyboard input mode enhancements Previously, you were able to enable different keyboard input modes only by updating the `KeyboardEventMode` value in the configuration file. There was no UI option to select the keyboard input mode.

Starting with Citrix Workspace app 2209, you can configure different keyboard input modes from the newly introduced **Keyboard input mode settings** section. You can select **Scancode** or **Unicode** as keyboard input mode.

For more information, see Keyboard input mode enhancements.

Support for extended keyboard layouts The Scancode keyboard input mode supports the following extended keyboard layouts:

- Japanese 106 keyboard
- Portuguese ABNT/ABNT2 keyboards
- Multimedia keyboards

For more information, see Support for extended keyboard layouts.

Improved error messages Previously all error messages were having a default error code and a description that isn't specific to the error. Currently, the error messages are improved to include the **Error code**, **Transaction ID**, and **Description** fields specific to the error.

For more information, see Improved error messages.

Enhancement to log collection With this release, the following enhancements are available:

- Citrix Log Collection Utility
- Disable DS logs

Citrix Log Collection Utility The Citrix Log Collection Utility helps you collect both new and existing logs. This utility specifically collects verbose logs and saves all logs in a tar.gz file.

For more information, see Citrix Log Collection Utility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disable collecting DS logs DS logs collects all logs. If you don't require the `dslogs`, you can disable it by adding the `DsLogsDisabled` key in the Authmanconfig.xml file:

For more information, see Disable DS logs.

Optimized Microsoft Teams updates

Upcoming Microsoft Teams Single-Window EOL On January 31, 2024, Microsoft will retire the Microsoft Teams support for Single-window UI when using VDI Microsoft Teams optimization and support only the Multi-Window experience. You must use a version of Citrix Virtual Apps and Desktops and Citrix Workspace app that support the Multi-Window feature to continue using certain optimized Microsoft Teams functionalities. For more information, see Upcoming Microsoft Teams Single-Window EOL.

Deprecation announcement of the SDP format (Plan B) from WebRTC Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use a version of Citrix Workspace app that supports the Unified Plan to continue using certain optimized Microsoft Teams functionalities. For more information, see Deprecation announcement of the SDP format (Plan B) from WebRTC.

Technical Preview

- Enhancement to multiple monitors

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

Fixed issues

- In Microsoft Teams, while you share a screen or app and resize it, the aspect ratios displayed might not be correct on the recipients (other meeting participants) side. This issue also occurs when you share screens or apps that are ordered using the Snap Windows feature option. [HDX-54395]
- After visiting a browser content redirected site, if you sign out from the user session, an error message might appear. [HDX-55087]
- You might face issues while sharing an app screen over the Optimized Microsoft Teams call. This issue occurs due to out of memory while sharing the app. [HDX-53442]
- Microsoft Teams admin might fail to get the current location of the Citrix Workspace app running on the endpoint. This issue occurs when the dynamic e911 feature is supported and the chassis ID is added for Microsoft Teams E911 configuration instead of subnet address. [CVADHELP-22752]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2308

What's new

HTTPS protocol support for proxy server Previously, you could connect to a proxy server only using the SOCKS protocol. From Citrix Workspace app for Linux 2308 onwards, you can connect to a proxy server using the HTTPS protocol also.

For more information on how to open a desktop using an HTTPS protocol, see HTTPS protocol support for proxy server.

Support for MJPEG webcams With this release, MJPEG webcams are supported in the H264 stream. The Webcam compresses MJEPG internally which provides better image quality and a higher frame rate. This feature is enabled by default. However, if Webcam doesn't support MJPEG, this feature is disabled.

Supports system certificate paths for SSL connection Previously, Citrix Workspace app supported only the `opt/Citrix/ICAClient/keystore` path as system certificate path. This path was a hardcode path to store Citrix predefined certificates. However, sometimes, certificate authority (CA) certificates are placed in the system certificates path in different linux distributions. To add these system certificate paths, customers had to make a soft link and replace `/opt/Citrix/ICAClient/keystore`.

With this release, Citrix Workspace app supports multiple system certificate paths. The following are the default system certificate paths supported for SSL connection:

```
"/var/lib/ca-certificates",
"/etc/ssl/certs",
"/system/etc/security/cacerts",
"/usr/local/share/cert",
"/etc/pki/tls/certs",
"/etc/openssl/certs",
"/var/ssl/certs",
ICAROOT() + "/keystore/cacerts"
```

In addition to the default system certified path, you can also add your own certified path by adding the `Certpath` field in the `AuthManConfig.xml` file.

For more information, see Supports system certificate paths for SSL connection.

Enhanced virtual channel SDK The virtual channel SDK for Citrix Workspace app for Linux is enhanced with the addition of new APIs for I/O functions and window positioning. For more information, see the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Client Side Media Player (CSMP)
- Virtual driver feature flag functions
- Virtual driver viewport functions
- Programming reference

Support for keyboard shortcut to switch between Full-screen and Window mode Previously, you had to use either the **Window** or **Full-screen** button on the Desktop Viewer to toggle between **Full-screen** and **Window** mode.

Starting with this release, you can use a keyboard shortcut Ctrl+F2 to switch between **Full-screen** and **Window** mode. For example, when the desktop session is in **Full-screen** mode, if you press "Ctrl+F2" , the desktop session exits from the **Full-screen** mode.

This feature is disabled by default.

For more information, see Support for keyboard shortcut to switch between Full-screen and Window mode.

Support for secondary ringer You can use the Secondary ringer feature to select a secondary device on which you want to get the incoming call notification when Microsoft Teams is optimized. For example, consider that you have set a speaker as the Secondary ringer and your endpoint is connected to the headphone. In this case, Microsoft Teams sends the incoming call signal to the speaker even though your headphones are the primary peripheral for the audio call itself. You can't set a secondary ringer in the following cases:

- When you aren't connected to more than one audio device
- When the peripheral isn't available (for example, a Bluetooth headset)

Added support for playing short tones in optimized Microsoft Teams Earlier, with the secondary ringtone feature enabled, short tones such as beeps or notifications were playing repeatedly. For example, the tone that was played when a guest joins the Microsoft Teams meeting was repeated. The only workaround was to quit and restart Microsoft Teams. This issue resulted in a poor end-user experience.

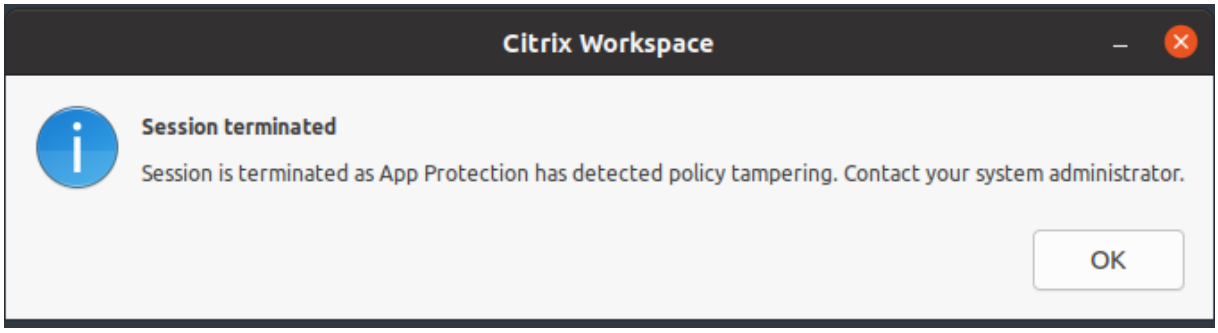
With this release, Citrix Workspace app supports playing the short tones as desired. This support also enables the secondary ringtone feature.

Prerequisites:

Update to the latest version of Microsoft Teams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy tampering detection Policy tampering detection feature prevents the user from accessing the Virtual App or Desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered. If policy tampering is detected, the virtual app or desktop session is terminated displaying the following error message:



For more information about the policy tampering detection feature, see Policy tampering detection.

Technical Preview

- Webcam redirection and service continuity support for ARM64 devices
- Multi-touch support

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

Fixed issues

- In a second hop scenario, you might be disconnected from the application that uses the Topaz USB Signature Pad or any other USB devices. This issue occurs when using the generic USB redirection feature in both hops. [CVADHELP-23053]
- After you upgrade Citrix Workspace app for Linux to 2206 or later versions, you might fail to sign in to Citrix Workspace app. This issue occurs only in the shared user mode when you sign in for the second or subsequent time. [CVADHELP-22775]
- When the Browser Content Redirection (BCR) feature is enabled, you might face disk space issues on thin clients. This issue occurs because the local cache of the redirected webpage is saved locally. [CVADHELP-21764]
- You might notice false HDMI audio devices detected inside the session. [CVADHELP-18849]
- When you install the 64-bit rpm package of Citrix Workspace app for Linux, you might get another requirements to install the library package that are required for 32-bit. [CVADHELP-23347]
- You might not be able to enter text in the search box of redirected browser content on the YouTube website when accessed in Full screen mode. This issue occurs with the Citrix Workspace app for Linux version 2106 or later. [CVADHELP-20399]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might need to authenticate twice when connecting to a PNA store by using `Storebrowse -E` or `-S` command. This issue occurs with the Citrix Workspace app for Linux version 2205 or later. [CVADHELP-22917]
- When you use the shortcut key "Ctrl + Alt + Enter", the keyboard might stop responding on pressing the "Enter"key. This issue occurs only in the Linux VDA desktop session started from Citrix Workspace app for Linux. [CVADHELP-22930]
- The white cursor isn't clearly displayed on a dark blue or black background. This issue occurs in Citrix Workspace app for Linux version 2307. [HDX-52458]
- You might fail to use the session in **Full-screen** mode on both monitors, when the secondary monitor is plugged in after a session is started. [HDX-52816]
- You might not be able to redirect a USB storage device to an app or desktop in a double hop session. [HDX-52155]
- You might see a blank page for the content redirected using the Browser Content redirection feature on Chrome. This issue occurs when you access an allowed site with Citrix Workspace app for Linux 2305. [HDX-50561]

2307

What's new

Script to verify system requirements for Windows Media Player redirection With this release, a new bash script is introduced to verify the configuration required for the Windows Media Player redirection feature in the Citrix Workspace app for Linux. This feature helps to reduce troubleshooting time for the Windows Media Player redirection feature. To verify the configuration, you can use the same rave_troubleshooting.sh available at System diagnostic script for RAVE.

Background blurring and replacement for Citrix Optimized Microsoft Teams Prerequisite:

Ensure that you have installed the `wget`.

With this release, Citrix Optimized Microsoft Teams in Citrix Workspace app for Linux now supports background blurring and background replacement. You can use this feature by selecting **More** > **Apply Background Effects** when you are in a meeting or in a P2P call.

For more information, see Background blurring and background effects.

Technical Preview

- HTTPS protocol support for proxy server
- Support for `IPv6` UDT with DTLS
- App Protection support for ARM64 devices

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Fixed issues

- You might fail to start a session in Citrix Workspace app version 2303 when the `AllowMultistream` value is set to True on Ubuntu 22.04. [HDX-49916]
- The DNS polling for CAS data collection might occur for direct ICA® launch and for CAS disabled stores. [CVADHELP-20018], [CVADHELP-12344]
- When you open Avaya WorkPlace, a black border is retained on the virtual apps or desktops screen. [CVADHELP-21558]
- When you use tools like the Snipping Tool, a shadow of the cursor might appear on virtual apps and desktops. [CVADHELP-22336]

2305

What's new

Enhancement to support keyboard layout synchronization for `GNOME 42` With this release, Citrix Workspace app for Linux supports keyboard layout synchronization for desktops like Ubuntu 22.04 which uses the `GNOME 42` desktop environment and later versions.

For more information, see the Keyboard layout synchronization section.

Client IME for East Asian languages Client Input Method Editor (IME) feature enhances input and display experience with Chinese, Japanese, and Korean (CJK) language characters in Citrix Workspace app for Linux. You can choose to use the Client IME when:

- you have a favorite IME in Linux Client or,
- IME isn't available from the remote server.

For more information, see Client IME for East Asian languages.

Addition of client-side jitter buffer mechanism This feature ensures clear audio even when the network latency fluctuates. By default, this feature is enabled.
To disable this feature, navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file and edit `JitterBufferEnabled=FALSE`.

Webcam redirection for 64-bit With this release, webcam redirection is supported for 64-bit applications. For more information, see Webcams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for more than 200 groups in Azure AD With this release, an Azure AD user who is part of more than 200 groups can view apps and desktops assigned to the user. Previously, the same user wasn't able to view these apps and desktops.

> **Note:**
>
> Users must sign out from Citrix Workspace app and sign in back to enable this feature.

Support for App Protection on Ubuntu 22.04 Starting with Citrix Workspace app for Linux version 2305, you can start protected virtual apps and desktops from the Citrix Workspace app on Ubuntu 22.04.

Enhancement to sleep mode for optimized Microsoft Teams call Previously, when you are in an optimized Microsoft Teams meeting, if there is no mouse or keyboard interaction, Citrix Workspace app or the optimized Microsoft Teams screen might go into sleep mode.

Starting with this release, Citrix Workspace app or the optimized Microsoft Teams screen doesn't go into sleep mode even if there is no mouse or keyboard interaction during an optimized Microsoft Teams meeting.

Improved experience for optimized Microsoft Teams video conference calls Starting with this release, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved. This enhancement is achieved by adapting to the proper resolution for the best call experience for all callers.

With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on) depending on several factors including endpoint capability, network conditions, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle. As a result, gives all users the optimum video experience.

Technical Preview

- Copy and paste files and folders between two virtual desktops
- Support for ARM64 architecture
- Support for IPv6 TCP with TLS
- Enhancement on 32-bit cursor support
- Support for authentication using FIDO2 when connecting to on-premises stores
- Hardware acceleration support for optimized Microsoft Teams

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The recorded audio might play fast when the app for recording uses the Microsoft Windows API MME (Multimedia Extension). For example, if you record audio for 20 seconds, it might play for 15 seconds. [CVADHELP-22162]
- The size of the `.NSAP_Data` file within the `.ICAClient` folder might grow beyond the maximum size and might affect the thin client's operations. This issue occurs when HDX Insight is enabled on NetScaler. [CVADHELP-22616]
- Opening protected sessions from Mozilla Firefox fails on IGEL distribution when using hybrid launch. [CVADHELP-22436]
- You might get an SSL error when you open an app or a desktop from Citrix Workspace app for Linux version 2209. [HDX-49324]
- Citrix Workspace app for Linux might stop responding when Universal Windows Platform (UWP) apps within VDI attempt to authenticate using FIDO2. [HDX-48942]
- When you select an image icon in the optimized Microsoft Teams, a gzip file is automatically downloaded. You might not be able to apply this image as a background image in optimized Microsoft Teams. [HDX-51694]
- You might fail to authenticate to Citrix Workspace app for Linux version 2303 using a smartcard. This issue occurs on Red Hat, Ubuntu 22.04, and Debian 11 Linux distributions. [RFLNX-9620]
- If you quit the Citrix Workspace app from the App indicator, the app might stop responding and you might get the following error message:

  "GLib (gthread-posix.c): Unexpected error from C library during 'pthread_setspecific': Invalid argument."[RFLNX-9445]
- You might get an undefined error with `libAnalyticsInterface.so` and might fail to share the Google Analytics data from Citrix Workspace app.[RFLNX-9705]

2303

What's new

Persistent login The Persistent login feature enables you to stay logged in for up to the duration (2–365 days) configured by your admin. When this feature is enabled, you need not provide login credentials for the Citrix Workspace app during the configuration period.

With this functionality, the SSO to Citrix DaaS sessions is extended up to a period of 365 days. This extension is based on the lifetime of Long-Lived Tokens. Your credentials are cached by default for 4

© 1997–2026 Citrix Systems, Inc. All rights reserved.

days or Lifetime whichever is lower. And then extended when you become active within these 4 days by connecting to the Citrix Workspace app.

For more information, see Persistent login.

Support for authentication using FIDO2 in HDX session With this release, you can authenticate within an HDX session using password-less FIDO2 security keys. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. For more information about FIDO2, see FIDO2 Authentication.

> **Note:**
>
> If you're using the FIDO2 device through USB redirection, remove the USB redirection rule of your FIDO2 device from the `usb.conf` file in the `$ICAROOT/` folder. This update helps you to switch to the FIDO2 virtual channel.

By default, FIDO2 authentication is disabled.

For more information, see Support for authentication using FIDO2.

Improved audio echo cancellation support Starting with this release, Citrix Workspace app supports echo cancellation. This feature is designed for real-time user cases, and it improves the user experience. The echo cancellation feature supports low quality, medium quality, and adaptive audio. Citrix recommends using adaptive audio for better performance.

For more information, see Improved audio echo cancellation support

Inactivity timeout for Citrix Workspace app The inactivity timeout feature signs you out of the Citrix Workspace app based on a value that the admin sets. Admins can specify the amount of idle time that is allowed before a user is automatically signed out of the Citrix Workspace app. You're automatically signed out when no activity from the mouse, keyboard, or touch occurs for the specified interval of time, within the Citrix Workspace app window. The inactivity timeout does not affect the already running Citrix Virtual Apps and Desktops and Citrix DaaS sessions or the StoreFront stores.

The inactivity timeout value can be set starting from 10 minutes to 1440 minutes. The interval to change this timeout value must be in a multiple of 5. For example: 10, 15, 20, or 25 minutes. By default, the inactivity timeout isn't configured.

> **Note:**
>
> This feature is applicable only on cloud deployments.

For more information on how to configure InactivityTimeoutInMinutes, see Inactivity Timeout for Citrix Workspace app section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Background blurring for webcam redirection Citrix Workspace app for Linux now supports background blurring for webcam redirection.

For more information, see Background blurring for webcam redirection.

Configure path for Browser Content Redirection overlay Browser temp data storage Starting with Citrix Workspace app 2303 version, you are requested to configure the temp data storage path for the CEF based browser.

For more information, see Configure path for Browser Content Redirection overlay Browser temp data storage.

Support for new PIV cards With this release, Citrix Workspace app supports the following new Personal Identification Verification (PIV) cards:

- IDEMIA next-generation smartcard
- DELL TicTok Smartcard

Performance optimization for smartcard driver Citrix Workspace app 2303 version includes performance related fixes and optimizations for the `VDSCARDV2.DLL` smartcard driver. These enhancements help to outperform version 1 `VDSCARD.DLL`.

Microsoft Teams enhancements

Configuring a preferred network interface Starting with the Citrix Workspace app 2303 version, you can now configure a preferred network interface for media traffic. With this enhancement, if you have multiple network connections and the performance of the default one isn't good, you can change to another network.

For more information, see Configuring a preferred network interface.

Fixed issues

- When you access Hyperspace over Citrix Virtual Apps™, the sign-in page that is specific to Hyperspace might appear on top of the apps that are already started. [CVADHELP-20368]
- When you access a second application, the current session might close and the session might restart. The data from the previous session might not be present and the data is updated as if the session started at the time the second application was started. This issue doesn't occur when you start the initial application in a session. [CVADHELP-21914]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might not be able to update the 24-hour time format under the **Selfservice** > **Profile** > **Account Setting** > **Regional Setting** > **Time format** section. This issue occurs only in a cloud store. [CVADHELP-20866]
- The session might close abruptly after you unplug the USB device while you drag multiple files from the VDA session to the USB device. This issue occurs only on Ubuntu. [HDX-30219]
- You might experience performance issues when signing in to the Citrix Workspace app using a smart card with the VDSCARDV2.DLL driver version. This issue occurs on eLux distributions only. [HDX-44314]

2302

What's new

Support for Korean language Citrix Workspace app for Linux is now available in the Korean language.

Performance optimization for Citrix Workspace app Starting with this release, the performance of Citrix Workspace app for Linux is improved when authenticating using AuthManLite.

Technical Preview

- Screen pinning in custom web stores
- Inactivity Timeout for Citrix Workspace app

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

Fixed issues

- You might experience conflict for the ctxcwalogd.service in the Citrix Workspace app for Linux with the ctxcwalogd.service in the Linux VDA. [HDX-44569]
- You might fail to apply a background image successfully in the optimized Microsoft Teams meeting. This issue occurs in specific operating systems including HP ThinPro OS. [HDX-47166]

2212

What's new

Support for multiple audio devices Starting with this release, Citrix Workspace app displays all available local audio devices in a session with their names. In addition, plug-and-play is also supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multiple audio devices redirection feature is enabled by default. To disable this feature, set the value for `AudioRedirectionV4` to False in the module.ini file.

Support for audio recording Starting with this release, the audio recording feature is enabled by default. The devices to record audio appear when a session starts.

To disable this feature, set the value for `AllowAudioInput` to False in the wfclient.ini file.

Technical Preview

- Support for 32-bit cursor
- Addition of client-side jitter buffer mechanism

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

Fixed issues

- You might not find a valid smartcard certificate after you remove the smartcard and insert again. [CVADHELP-20787]
- You might fail to sign in to Citrix Workspace app using the TicTok smartcard. [CVADHELP-20578]
- You might fail to sign in to Citrix Workspace app using the smartcard from IDEMIA. [CVADHELP-20652]
- The Citrix Workspace app might stop responding when audio redirection is using the Speex codec with multiple audio devices enabled. [CVADHELP-21212]
- When you sign out from the Citrix Workspace app and sign in again, the Citrix Workspace app starts without entering the sign-in credentials. This issue occurs only in cloud deployments and if the `longLivedTokenSupport` parameter value is set to *True*. [RFLNX-9160]
- Transaction ID error messages might appear when you start a session. For example: “The option “-transactionid”is invalid”. [HDX-45618]
- When you install Citrix Workspace app and start the session with root privileges, the session might exit. [HDX-46967]
- When you install and start Citrix Workspace app, the following error message might appear:

  “The X request 130.1 caused error:”10: BadAccess(Attempt to access private resource denied”. [HDX-44416]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2211

What's new

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

Fixed issues

- The VDA might crash after redirecting the Audio interface of the device. This issue occurs when you enable the "Client USB device redirection"policy on DDC and attach composite USB devices to the endpoint, such as the USB Headset. [HDX-44117]
- The QWERTY keyboard of Bloomberg 4 might be locked to the session after using the USB redirection. [HDX-44555]
- You might fail to register and use your YubiKey devices with the PIN code on Citrix Workspace app. [HDX-44951]
- When the snap-store process runs in the background, you might not be able to start protected apps and desktops. [APPP-110]

2209

What's new

Microsoft Teams enhancements

- **App sharing enabled:** Starting with Citrix Workspace app 2209 for Linux and Citrix Virtual Apps and Desktops 2109, you can share an app using the Screen sharing feature in Microsoft Teams.
- **Enhancements to high DPI support:** When the high DPI feature is enabled and you're using 4K monitors, Microsoft Teams video overlays are in the desired position and of the correct size. Irrespective of your display settings such as single or multi-monitor arrangements, overlays always appear correctly and aren't scaled up or appear in an undesired position. To enable this enhancement, ensure that the `DPIMatchingEnabled` parameter in the `wfclient.ini` configuration file is set to **True**. For more information, see Support for DPI matching.
- **WebRTC SDK upgrade:** The version of the WebRTC SDK that is used for the optimized Microsoft Teams is upgraded to version M98.

Upgraded version of compatibility libraries Starting with this release, Citrix Workspace app for Linux is compatible with the following libraries:

- `glibc` 2.27 or later
- `glibcxx` 3.4.25 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App Protection update

> **Note:**
>
> App Protection isn't supported on Ubuntu 22.04 prior to Citrix Workspace app version 2305. As a result, if you install the App Protection module on Ubuntu 22.04, you might not be able to start virtual apps and desktops in the Citrix Workspace app. For more information on App Protection, see App Protection.

Technical Preview

- Keyboard input mode enhancements
- Support for extended keyboard layouts
- Support for authentication using FIDO2 in HDX session

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

Fixed issues

- When the App Protection feature is enabled, the anti-keylogging functionality might not work for the Authentication Manager interface that loads the webpage in a separate window. [RFLNX-9004]
- After upgrading to Citrix Workspace app 2007 for Linux, adding a Store using `Storebrowse` might take a long time. This issue occurs because the Store attempts to contact the app config service that is unreachable. [CVADHELP-20618]
- When you connect to a cloud store from the self-service user interface, a spinning wheel might appear on the sign-in page. [CVADHELP-20039]
- When you start two apps from two different delivery groups, there might be a delay in starting the second app. [CVADHELP-18198]

2207

What's new

Enhancement to improve audio quality Previously, the maximum output buffering value to play the audio smoothly was 200 ms in Citrix Workspace app. Because of this value set, 200 ms latency was added in the playback scenario. This maximum output buffering value had an impact on interactive audio applications as well.

With this enhancement, the maximum output buffering value is decreased to 50 ms in Citrix Workspace app. As a result, the user experience on the interactive audio application is improved. Also, the Round trip time (RTT) is decreased by 150 ms.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with this release, you can select the appropriate playback threshold and pulse audio pre-buffer to improve the audio quality. For this enhancement, the following parameters are added in the [ClientAudio] section of the `module.ini` file:

- `PlaybackDelayThreshV4` –To specify the initial level of output buffering in milliseconds. Citrix Workspace app tries to maintain this level of buffering throughout a session's duration. The default value of the `PlaybackDelayThreshV4` is 50 ms. This parameter is valid only when `AudioRedirectionV4` is set to **True**.
- `AudioTempLatencyBoostV4` –When the audio throughput undergoes a sudden spike or isn't enough for an unstable network, this value increases the output buffering value. This increase in the output buffering value provides smooth audio. However, the audio might be slightly delayed. The default value of `AudioTempLatencyBoostV4` is set to 100 ms. This parameter is only valid when `AudioRedirectionV4` is set to **True** and `AudioLatencyControlEnabled` is set to **True**. By default, the value of `AudioLatencyControlEnabled` is set to True.

For more information on how to enable this enhancement, see the **Enhancement to improve audio quality** section in the Audio documentation.

Composite USB device redirection Starting with this release, Citrix Workspace app allows splitting of composite USB devices. A composite USB device can perform more than one function. These functions are accomplished by exposing each of those functions using different interfaces. Examples of composite USB devices include HID devices that consist of audio and video input and output.

Currently composite USB device redirection is available in desktop session only. The split devices appear in the Desktop Viewer.

Earlier when a device was unplugged and plugged in during a session, the device was redirected automatically. As a result, the device was auto connected to the VDA. With this release, you are required to enable auto-redirection manually through configuration file settings. Auto-redirection of composite USB devices is disabled by default.

For more information on configuring composite USB device redirection, see the **Composite USB device redirection** section in the USB documentation.

Technical Preview

- Support for DPI matching
- Improved audio echo cancellation support

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- When you launch a desktop in full-screen mode using the Lightweight X11 Desktop Environment (LXDE) and disconnect from the network, you get a **Connection to <XXX> has been lost error** message with a **Quit** option on the dialog. The message appears if the Auto Client Reconnect (ACR) or Session Reliability (SR) policy is expired. When you click **Quit**, the user desktop disappears. However, if you click anywhere else on the screen, the **Quit** button might never appear on the dialog. You must manually exit the user desktop by pressing the **Esc** or **Enter** key. [CVADHELP-17478]
- Citrix Workspace app for Linux might interpret URLs containing the string, **cloud** (for example <*xxx-yyy-cloud.com*>) as cloud domain URLs even if they represent on-premises URLs. [CVADHELP-19480]
- The session might disconnect while you try to use the HDX webcam. The issue occurs only in VDA version 2203. [CVADHELP-20223]
- Copying and pasting content between published applications, VDI sessions, or a VDI session and a published application might fail. The session or the application might become unresponsive for some time. [CVADHELP-19899]
- You might experience the session disconnection issues when connected through the Citrix Workspace app for Linux 2205 version endpoints. This issue occurs if you configure the lock screen using the **Force a specific default lock screen image** policy setting with certain types of JPEG file type and apply to the Citrix VDA 2203. [CVADHELP-21572]
- When you preview a video using a webcam in the Skype, the preview might show a black screen. [HDX-37860]
- HDX RealTime Webcam video compression does not support camera with MJPEG video format in Citrix Workspace app. [HDX-40352]
- While sharing the screen or an app during the Microsoft Teams call, your peers might see visual artifacts. This issue occurs due to unstable frame rates, such as incorrect video playback (frozen or transient black frames). This release includes improved frame rates or sampling rates that help to reduce visual artifacts. [HDX-38032]
- The video or an image in Citrix Workspace app might not render correctly. This issue occurs when Citrix Workspace app is used along with VDA version 2109 or later. [HDX-40287]
- When you launch `wfica` with the `-span o` command, the session might fail to launch and span across all available monitors. Similarly, when you launch `wfica` with the `-span h` command, the list of the monitors currently connected to the user device might fail to print. For more information, see command reference. [HDX-32519]
- When an SSL error occurs on one protocol during a TCP and EDT/UDP connection attempt, both connections might fail because of the race condition. This SSL error can occur if the TLS configuration differs between the protocols, and the client cannot connect via one protocol. [RFLNX-8747]
- When you try to connect remotely to a machine that has Citrix Workspace app with App Protec-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tion installed, the x11vnc server crashes and the connection fail. As a result, you might not be able to connect remotely to the machine through the x11vnc server. [RFLNX-8933]

- When you add a store with default settings, the `Storebrowse` enumeration might fail. This issue occurs only in the Debian 32-bit OS. [RFLNX-8743]
- You might get an error message when you install the Citrix Workspace app with App Protection feature enabled on 32-bit Linux machines. [RFLNX-8809]
- When you add a store using the `storebrowse -a` command and enumerate using the `storebrowse -E` command, the `Storebrowse` enumeration might fail. This issue occurs only in the Raspberry Pi OS. [RFLNX-8803]

2205

What's new

Authentication enhancement for `Storebrowse` Starting with this release, the authentication dialog is present inside Citrix Workspace app and the store details are displayed on the logon screen. This feature provides a better user experience. The authentication tokens are encrypted and stored so that you don't need to reenter credentials when your system or session restarts.

You can also toggle the authentication enhancement for `Storebrowse` feature off or on using the `StorebrowseIPC` key in the `AuthmanConfig.xml` file. By default, the toggle functionality is disabled.

The authentication enhancement supports `storebrowse` for the following operations:

- `Storebrowse -E`: Lists the available resources.
- `Storebrowse -L`: Launches a connection to a published resource.
- `Storebrowse -S`: Lists the subscribed resources.
- `Storebrowse -T`: Terminates all sessions of the specified store.
- `Storebrowse -Wr`: Reconnects the disconnected yet active sessions of the specified store. The [r] option reconnects all the disconnected sessions.
- `storebrowse -WR`: Reconnects the disconnected yet active sessions of the specified store. The [R] option reconnects all the active and disconnected sessions.
- `Storebrowse -s`: Subscribes the specified resource from a given store.
- `Storebrowse -u`: Unsubscribes the specified resource from a given store.
- `Storebrowse -q`: Launches an application using the direct URL. This command works only for StoreFront stores.

> **Note:**
>
> - You can continue to use the remaining `storebrowse` commands as used earlier (using AuthMangerDaemon).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - The authentication enhancement is applicable for cloud deployments only.
> - With this enhancement, the persistent login feature is supported.

For more information, see the Authentication enhancement.

Email-based auto-discovery of store You can now provide your email address in Citrix Workspace app to automatically discover the store associated with the email address. If there are multiple stores associated with a domain, by default the first store returned by the Global App Configuration Service is added as the store of choice. Users can always switch to another store if necessary.

For more information, see the **Email-based auto-discovery of store** section at Adding store URL to Citrix Workspace app documentation.

Technical Preview

- Persistent Login

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

Fixed issues

- The DNS server in a customer environment with limited internet access might not resolve the URL, `clientstream.launchdarkly.com`. As a result, Citrix Workspace app sends many DNS queries (>1000 within three seconds per day) to the URL. [CVADHELP-19559]
- When the App Protection feature is enabled, the anti-keylogging functionality might not work for the Authentication Manager interface that uses the `UIDialogLibWebKit3.so` library. This issue is resolved in the "GNOMEandKDE' desktop environment. [RFLNX-8027]
- Attempting to print from a VDA session running on Raspberry Pi ARMHF client version 3 or 4 might make the session unresponsive. [CVADHELP-18506]
- When you launch the self-service user interface with the default settings, the following error message might appear:

  "Response for Secondary Token request is not 200/400/404 42"

  This issue occurs on Fedora 35. [RFLNX-8603]

2203

What's new

Support for EDT `IPv6` Starting with this release, Citrix Workspace app supports EDT `IPv6`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for TLS protocol version 1.3 Starting with this release, Citrix Workspace app supports the Transport Layer Security protocol (TLS) version 1.3.
For more information, see TLS.

Custom web stores Starting with 2203, you can access your organization's custom web store from the Citrix Workspace app.

> **Note:**
>
> The Pinning multi-monitor screen layout feature isn't supported in the custom web store.

For more information, see Custom web stores.

Authentication enhancement experimental feature Starting with this release, the authentication enhancement supports `storebrowse` for the following operations:

- `Storebrowse -E` to list the available resources.
- `Storebrowse -L` to launch a connection to a published resource.
- `Storebrowse -S` to list the subscribed resources.

> **Note:**
>
> You can continue to use the remaining `storebrowse` commands in the `AuthMangerDaemon` and will be supported with authentication enhancement in the future release.

For more information, see Authentication enhancement for `Storebrowse`.

Keyboard layout synchronization enhancement Keyboard layout synchronization enables you to switch among preferred keyboard layouts on the client device. This feature is disabled by default. When enabled, the client keyboard layout automatically synchronizes to the Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session.

Starting with version 2203, Citrix Workspace app supports the following three different keyboard layout synchronization modes:

- **Sync only once - when session launches** –Based on the `KeyboardLayout` value in the `wfclient.ini` file, the client keyboard layout is synchronized to the server when the session launches. If the `KeyboardLayout` value is set to `0`, the system keyboard is synchronized to VDA. If the `KeyboardLayout` value is set to a specific language, the language-specific keyboard is synchronized to VDA. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, sign out and sign in to the app. The **Sync only once - when session launches** mode is the default keyboard layout selected for Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Allow dynamic sync** - This option synchronizes the client keyboard layout to the server when you change the client keyboard layout.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

For more information, see Keyboard layout synchronization.

Multi-window chat and meetings for Microsoft Teams You can use multiple windows for chat and meetings in Microsoft Teams, when optimized by HDX in Citrix Virtual Apps and Desktops 2112 or higher. You can pop out the conversations or meetings in various ways. For details about the pop-out window feature, see the New Meeting and Calling Experience in Microsoft Teams documentation.

If you're running an older version of Citrix Workspace app or Virtual Delivery Agent (VDA), remember that Microsoft will deprecate the single-window code in the future. However, you can upgrade to a version of the VDA or Citrix Workspace app that supports multiple windows (2203 and greater). To upgrade to a higher version, you will have a minimum of nine months after this feature is generally available.

> **Note:**
>
> This feature is available only after the roll-out of a future update from Microsoft Teams. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

Enhancement to auto-redirection of USB devices Earlier when a device was unplugged and plugged in during a session, the device was auto-redirected. As a result, the device was auto-connected to the VDA. With this release, you are required to enable auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default. For more information, see the USB section.

Fixed issues

- When you add a store and authenticate it to the Citrix Workspace app, the authentication window is loaded for the second time, even after successful authentication. This issue occurs when you first sign into the Citrix Workspace app after setting the `AuthManLiteEnabled` to **True**. [RFLNX-8694]
- After you install the Citrix Workspace app with App Protection feature enabled on the OS that uses `glibc 2.34` or later, the OS boot might fail on restarting the system. [RFLNX-8358]
- When you are using Microsoft Teams to make a P2P call or to attend a meeting, and wait for some time, the load for one CPU core might increase to 100% due to socket error. [HDX-38974]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspace app does not support the new version of Raspberry Pi OS based on the Debian bullseye. [HDX-37000]
- When you launch a session with the ICA file and sign off from the session, the expected return value that you receive from the `wfica` command-line is 0. However, instead of the expected value, the value that you receive is 2. This issue occurs in Citrix Workspace app version 2106 or later. [HDX-38916]
- In Citrix Workspace app, you might experience intermittent failures when answering or making a Microsoft Teams call. The following error message appears:

  "Call could not be established."

  [HDX-38819]

Known issues

Known issues in 2508

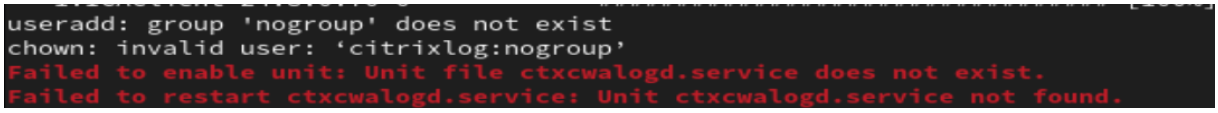
- When you access web applications, such as Google Meet, through Chromium Embedded Framework-based Browser Content Redirection, certain UI elements might not respond to interactions. As a workaround, refresh the page to restore UI element functionality. [HDX-94506]
- When you configure device rules with a **Deny** rule in **Client USB device redirection rules** policy setting in Studio, certain devices that have been allowlisted in the same policy setting for passthrough into an HDX session with an **ALLOW** rule fail to get redirected. [HDX-95546]

Known issues in 2503

- Some third-party scanners fail to scan in color and grayscale modes. This issue occurs when Citrix Workspace app and the scanner drivers use different versions of the JPEG library. [HDX-80932]

Known issues in 2411

- You might encounter an installation error when installing Citrix Workspace for Linux on RHEL 9.



As a workaround, do the following steps to install successfully:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Run the following command to create the 'nogroup'group:
   `sudo groupadd nogroup`
2. Run the following command to create the citrixlog user:
   `sudo useradd -g nogroup citrixlog`
3. Run the following command to change the ownership of the Citrix Workspace directory:
   `sudo chown citrixlog:nogroup /opt/Citrix/ICAClient`
4. Uninstall the previously installed Citrix Workspace app, and then reinstall it.

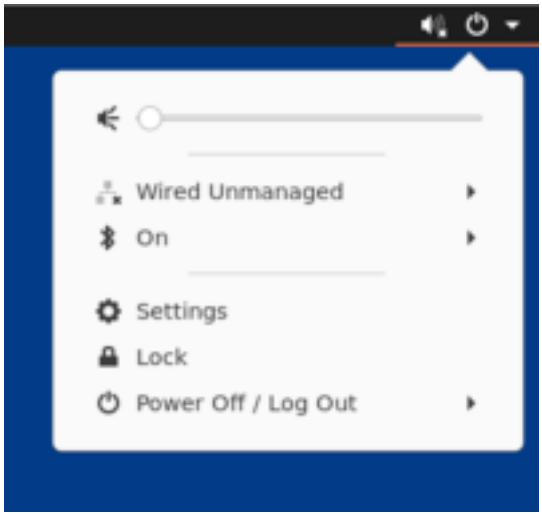
For more information, see Install.[RFLNX-10747]

- After successfully authenticating to the cloud store in Citrix Workspace for Linux, you might encounter a "No Connection"error within the workspace.



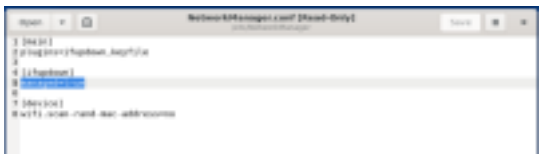
Resolution

This issue may be caused by the Network Manager configuration on your machine. Specifically, if the Network Manager shows "Wired Unmanaged,"follow the steps below to resolve the issue.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to /etc/NetworkManager.
2. Edit `NetworkManager.conf` file.
3. Set the managed field to **true**. Refer to the below screenshot:



4. Create a new configuration file (10-globally-managed-devices.conf) in this directory. `/etc/NetworkManager/conf.d`
5. Add Configuration to the New File and save this file:

```
[keyfile]
unmanaged-devices=*,except:type:ethernet,except:type:wifi,except:
   type:wwan
```

6. Run this command:
   `sudo service network-manager restart`
   If the service is not available, use this command instead
   `sudo systemctl restart NetworkManager.service`

After completing these steps, your network settings should be updated, and the "No Connection"issue should be resolved.



Known issues in 2408

- When you attempt to reconnect to the session quickly after disconnecting, with the Nuance PowerMic III device auto-redirected to the session, you might notice that the Nuance PowerMic III redirected to the session is delayed. This issue is limited to the Nuance PowerMic III device on the Linux platform. [CVADHELP-25048]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Google Earth might not be supported in BCR, and you might get the following the error message :

  "WebGL is not supported on your browser."

  As a workaround, use server-side rendering. HDX-71097.

- You might notice that SaaS apps fail to open and display the following error message:

  `curl_easy_perform()failed: SSL connect error in /var/log/citrix/ICAClient.log.`

  As a workaround, do the following:

  1. Navigate to the /etc/ssl/openssl.cnf file.
  2. For SSL v3.0.2 and older set the following value:
     `Options = UnsafeLegacyRenegotiation` [RFLNX-10891]

- You might encounter an installation error when installing Citrix Workspace for Linux on RHEL 9. As a workaround, do the following steps to install successfully:

  1. Run the following command to create the 'nogroup'group:
     `sudo groupadd nogroup`
  2. Run the following command to create the citrixlog user:
     `sudo useradd -g nogroup citrixlog`
  3. Run the following command to change the ownership of the Citrix Workspace directory:
     `sudo chown citrixlog:nogroup /opt/Citrix/ICAClient`
  4. Uninstall the previously installed Citrix Workspace app, and then reinstall it. For more information, see Install. [RFLNX-10747]

Known issues in 2405

- You might fail to take a screenshot using the PrintScreen (PrtSc) key in the keyboard. This issue occurs while any drop-down is expanded in the Citrix Workspace app UI. As a workaround, use a third-party app which can add delay to capture. For example, you can use the Gnome Screenshot for delaying the screen capture. [RFLNX-10986]
- You might notice that you cannot navigate the Desktop Viewer toolbar using the keyboard after switching between the virtual desktop sessions. This issue happens when you switch from one virtual desktop to another through the **Switch Desktop** menu in the Desktop Viewer toolbar using the keyboard. As a workaround, after switching to another desktop, click the **Windows** or **Alt+Tab** buttons twice. [HDX-63512]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 2402

- You might face visual artifacts in an app session. This issue occurs when you drag the app session to the edge of a screen to make it to a maximum window. As a workaround, use the maximize button to make the app session into a maximum window. [HDX-53648]
- When you change the default `KeyboardSync` setting to *Off* in the `module.ini` file, typing characters with dead keys like *circumflex* ^, might cause the `wfica` process to fail. As a workaround, change the `KeyboardSync` setting to *On*. [HDX-63237]
- When you install Citrix Workspace app for Linux 2402 version, the set log fields might not be populated correctly. As a workaround, delete the `ctxcwalogconf` and `ctxcwalogsocket` from the `/var/log/citrix/` path before installing Citrix Workspace app for Linux. This issue occurs when you install or upgrade Citrix Workspace app for Linux on a machine where Citrix Workspace app was already present. [RFLNX-11045]
- In the virtual desktop session, when you drag and place the seamless app above other apps, you might notice that any click on the app above is received by the app under it. As a workaround, after dragging the seamless app, move the cursor on the seamless app to avoid this issue. [HDX-63775]

Known issues in 2311

- After you start a session, if you remove one monitor from the three monitors that are arranged vertically, the session moves to window mode instead of full-screen mode. [HDX-55840]
- Citrix Workspace app for Linux doesn't support HTML5 redirection where the Fluendo hardware-based decoder is used. [CVADHELP-22564]
- You might notice that the following fingerprint sensor devices are not supported for generic USB redirection:

  - Thales DactyID20
  - NITGEN FDU06M/S

  [CVADHELP-24076], [CVADHELP-23852]

- You might notice that the following fingerprint sensor devices are not supported for generic USB redirection:

  - Thales DactyID20
  - NITGEN FDU06M/S

  [CVADHELP-24076], [CVADHELP-23852]

- You can't do screen sharing from chat using Optimized Microsoft Teams 2.1. [HDX-62667]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sometimes, you might fail to open SaaS apps and might get the following error message:

  "curl_easy_perform() failed: SSL connect error in /var/log/citrix/ICAClient.log."

  As a workaround, do the following:

  1. Verify the openSSL version using the following command:

     ```
     openssl version
     ```

  2. Navigate to the /etc/ssl/openssl.cnf file.

     a) For SSL v3.0.2 and older set the following value:

     ```
     Options = UnsafeLegacyRenegotiation
     ```

     a) For SSL v3.0.4 and later set the following value:

     ```
     Options = UnsafeLegacyServerConnect
     ```

  [RFLNX-10662]

Known issues in 2308

- After visiting a browser content redirected site, if you sign out from the user session, an error message might appear. You can ignore this error message. [HDX-55087]

Known issues in 2307

- When you install Citrix Workspace app for Linux using the Debian package Manager on Ubuntu version 22.04, you get the following error:

  A dependency job for AppProtectionService-install.service failed. See 'journalctl -xe' for details.

  You get this error even though App Protection is successfully installed. [RFLNX-9995]

Known issues in 2305

- When you use tools like the Snipping Tool, a shadow of the cursor might appear on virtual apps and desktops. [CVADHELP-22336]
- When you open Avaya WorkPlace, a black border is retained on the virtual apps or desktops screen. [CVADHELP-21558]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 2303

- When you install the Citrix Workspace app using the UI, you might not be able to install the App Protection feature on Ubuntu 20.04 and 22.04. As a workaround, install the app using the command-line interface. [APPP-1067]
- You might fail to start a session in Citrix Workspace app version 2303, when the `AllowMultistream` value is set to **True** on Ubuntu 22.04. [HDX-49916]
- You might fail to authenticate to Citrix Workspace app for Linux version 2303 using a smartcard. This issue occurs on Red Hat, Ubuntu 22.04, and Debian 11 Linux distributions. [RFLNX-9620]
- If you quit the Citrix Workspace app from the App indicator, the app might stop responding and you might get the following error message:

  "GLib (gthread-posix.c): Unexpected error from C library during 'pthread_setspecific': Invalid argument. "

  As a workaround, ensure that you use `glib` version 2.76 or later. [RFLNX-9445]

Known issues in 2211

- Transaction ID error messages might appear when you start a session. For example: "The option "-transactionid"is invalid". As a workaround, click **OK** to close the message box and proceed. [HDX-45618]
- When you install and start Citrix Workspace app, the following error message might appear:

  "The X request 130.1 caused error:"10: BadAccess(Attempt to access private resource denied"

  Click **Cancel** to proceed with the session.

  As a workaround, navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file and replace `IgnoreErrors=9,15` with `IgnoreErrors=9,15,32`. [HDX-44416]
- When you sign out from the Citrix Workspace app and sign in again, the Citrix Workspace app starts without entering the sign-in credentials. This issue occurs only in cloud deployments and if the `longLivedTokenSupport` parameter value is set to *True*. As a workaround, do the following:

  1. Navigate to the `/config/AuthManConfig.xml` file.
  2. Go to the [AuthManLite] section and update the following entry:

  ```
  <longLivedTokenSupport>false</longLivedTokenSupport>
  ```

  [RFLNX-9160]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 2209

- When you start a Microsoft Edge App session, the Microsoft Edge icon displays randomly for different scale. This error occurs if you have applied the following settings:

  - `DPIMatchingEnabled` value is set to **True**
  - Client scale in the display isn't set to 100%

  [HDX-39764]

- Attempts to start a server VDA session using smart card authentication might fail for a smart card with multiple users. As a workaround, reinsert the card. [HDX-44255]
- The VDA might crash after redirecting the interface of the device. This issue occurs when you enable the "Client USB device redirection"policy on DDC and attach composite USB devices to the endpoint, such as the USB Headset. Also, add the input value in the usb.conf file as `vid =** pid=** split=01 and intf=00,01`. After that you start the session from Citrix Workspace app and set redirect the interface of a device. [HDX-44117]
- The session launch might fail on the Raspberry Pi ARMHF OS based on Debian 11. Citrix recommends you to use Raspberry Pi ARM64 OS based on Debian 11 or older Raspberry Pi ARMHF OS based on Debian 10. [HDX-41729]
- When you remove a primary account, the sign-in credentials might not be deleted from the self-service cache. As a result, you might be able to sign in to the store without providing credentials. As a workaround, quit the selfservice to delete the credentials. [RFLNX-9051]
- After you provide the sign-in credentials and start selfservice, a white screen might appear. As a workaround, quit the selfservice and restart it. [RFLNX–8951]
- In OpenSUSE SLES 15, you might get a spinning wheel when you connect to a cloud store. [RFLNX–9109]
- You might fail to start Selfservice on RHEL9 and Fedora 36. As a workaround, ensure that the value of `AuthManLiteEnabled` is set to *False* in the `$ICAROOT/config/AuthManConfig.xml` file. [RFLNX-9128]

Known issues in 2207

- The DNS polling for CAS data collection might occur for direct ICA launch and for CAS disabled stores. [CVADHELP-20018]
- When using `storebrowse` commands, if you add and enumerate a second store, you might fail to launch the apps or desktops from the first store. As a workaround, you must enumerate the specific store again before launching any apps or desktops. [RFLNX-8953]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In a desktop session, when you play a video using Windows Media Player, the mouse cursor might disappear on the rave video. This issue occurs only if you have set the following policies in DDC as follows:
  - "Use video codec for compression"as "For actively changing regions"
  - "Windows Media redirection"as "Allowed"(Default setting)
  - "Browser Content Redirection"as "Allowed"(Default setting)
  - "InvertCursorEnabled"as "BOTH"and the following values are added in the ~/.ICAClient/wfclient.ini file:
    - InvertCursorEnabled=True
    - InvertCursorRefreshRate=60
    - InvertCursorMode=1

[HDX-37259]

Known issues in 2205

- You might experience the session disconnection issues when connected through the Citrix Workspace app for Linux 2205 version endpoints. This issue occurs if you configure the lock screen using the **Force a specific default lock screen image** policy setting with certain types of JPEG file type and apply to the Citrix VDA 2203. As a workaround, upgrade to the Citrix Workspace app version 2207 or later. [CVADHELP-21572]
- When an SSL error occurs on one protocol during a TCP and EDT/UDP connection attempt, both connections might fail because of the race condition. This SSL error can occur if the TLS configuration differs between the protocols, and the client cannot connect via one protocol. As a workaround, set the HDXoverUDP attribute to On or Off in the ICA file. [RFLNX-8747]
- HDX RealTime Webcam video compression does not support camera with MJPEG video format in Citrix Workspace app. [HDX-40352]
- The video or an image in Citrix Workspace app might not render correctly. This issue occurs when Citrix Workspace app is used along with VDA version 2109 or later. As a workaround, do the following.
  1. Sign into Citrix Studio.
  2. Edit the **Use video codec for compression** policy settings.
  3. Select the **For the entire screen** option from the **Value** drop-down list. [HDX-40287]
- When you add a store using the `storebrowse -a` command and enumerate using the `storebrowse -E` command, the `Storebrowse` enumeration might fail. This issue occurs only in the Raspberry Pi OS. As a workaround, do the following:
  1. Navigate to /opt/Citrix/ICAClient/config/AuthmanConfig.xml.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Add the following entry:

```
<StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
```

[RFLNX-8803]

- When you add a store with the default settings, the `Storebrowse` enumeration might fail. This issue occurs only in the Debian 32-bit OS. As a workaround, do the following:

  1. Navigate to /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Add the following entry:

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
```

  [RFLNX-8743]

- You might fail to install the Debian package of Citrix Workspace app on Ubuntu 22.04 LTS. The reason for this failure is that the `libidn11` package required for `ICAClient` isn't present on Ubuntu 22.04 LTS. As a workaround, install the `libidn11` independently on Ubuntu 22.04 LTS before installing the Debian package of Citrix Workspace app. [RFLNX-8839]

Known issues in 2203

- When launching a published Remote Desktop Protocol (RDP) application with multiple monitors in an Ubuntu endpoint, only one monitor displays content even though the client machine has multiple monitors. The "Use all my monitors for the remote session"checkbox in the display option of the RDP application is selected before connecting to a remote desktop through RDP. The issue occurs in the seamless mode and multi-monitor setup. [CVADHELP-16768]
- Citrix Workspace app does not pass the `Clientname` and `clientaddress` parameters to DDC during resource enumeration. As a result, `Set-BrokerAccessPolicyRule` filtered with client name or client IP might not work properly. [CVADHELP-17667]
- When you preview a video using the webcam in the Skype, the preview might show a black screen. [HDX-37860]

Known issues in 2112

- When you attempt to enter text, the cursor appears white. The issue occurs in a double-hop scenario when connected from a Linux end-point machine. [CVADHELP-16170]

Known issues in 2111

- When you log on to a cloud store, the screen might appear in white. [RFLNX-8337]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you try to launch Citrix Workspace app, the self-service user interface might fail to open, and the following error message appears:

  "User-defined signal 2"

  The issue occurs in the debug build and in Azure VM Debian 10. [RFLNX-8336]

Known issues in 2109

- When you uninstall the Citrix Workspace app, out of date cache files at `$HOME/.local/share/webkitgtk` might not be removed automatically. As a workaround, manually remove the cache files. [HDX-28187]
- Attempts to launch desktops or applications using the Citrix Workspace app might fail when the Multi-Port policy is enabled on DDC. [HDX-31016]
- Attempts to launch a session using smart card authentication might fail. The issue occurs with Citrix Workspace app for Linux version 2104 and later. As a workaround, manually enter the smart card credentials. [CVADHELP-18402]
- Attempts to reconnect to the session might occur only once during auto-client reconnection. As a result, the **Auto client reconnect** policy might not work as expected. [HDX-34114]
- When you close the progress bar that displays the progress of an application launch, the `wfica` process might fail. As a result, the application might launch and disappear from your screen. [HDX-34701]

Known issues in 2108

- If you're using Global Server Load Balancing (GSLB), the Domain Name System (DNS) responses might not get cached for Time-To-Live (TTL) duration. As a result, the authentication using WebView might fail. [RFLNX-3673]

Known issues in 2106

- In a desktop session, after a page is redirected using CEF-BCR, the keyboard focus shifts to the current mouse location. The issue occurs because of a third-party limitation on open source CEF. [RFLNX-7724]
- When you try to click the BCR overlay (for example, YouTube Search) with another application in the foreground, the browser page does not appear on the foreground. [RFLNX-7730]
- After a page is redirected using the CEF-BCR, when you close the redirected webpage, a segmentation fault is captured in the error logs. [RFLNX-7667]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 2103

- During a video call or screen sharing, Microsoft Teams might turn unresponsive and the call might end abruptly. [CVADHELP-16918]

Known issues in 2101

- Sometimes, Citrix Workspace app might not be able to render the incoming videos in Microsoft Teams. [RFLNX-6662]

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.

Third-party notices

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

Citrix Workspace app for Linux Third-Party Notices (PDF Download)

Experimental features

On occasion, Citrix releases experimental features as a mechanism for seeking customer feedback on the potential desirability of new technologies or features. Citrix does not accept support cases for experimental features but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. Citrix isn't committing to productizing experimental features and might withdraw them for any reason at any time.

Features in Technical Preview

June 29, 2026

Features in the 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 the technical preview. To provide feedback for any of these features, fill out the feedback form.

Title	Available from version	Feedback form (click the icon)
Dual VCSDK binary sets for Linux	2604	
Dual CWA package sets for Linux	2604	
Audio Quality Enhancer for reliable transport	2601	
Smart card authentication support for Boot-to-VDI	2508	
Browser Profile Sharing in Browser Content Redirection	2508	
Loss tolerant mode for graphics	2505	
Support for H.264 hardware decoding for seamless apps	2503	
Enhanced Unified Communications SDK API	2408	
Support integrated windows authentication for browser content redirection	2408	
Support for H.265 hardware decoding	2408	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Title	Available from version	Feedback form (click the icon)
Include system audio while screen sharing	2402	
App Protection compatibility with HDX optimization for Microsoft Teams	2311	
Hardware acceleration support for optimized Microsoft Teams	2305	
Support for Service continuity with Citrix Workspace Web Extension for Google Chrome	2109	

Dual VCSDK binary sets for Linux

Technical Preview from 2604 release	Feedback form.

Starting with Citrix Workspace app 2604 for Linux, the Virtual Channel SDK (VCSDK) package includes two Linux binary sets instead of one so that you can choose the build that matches your target environment.

Citrix Workspace app for Linux 2604 continues to use GCC 8. The VCSDK package also includes a GCC 11 build as a Technical Preview.

Folder	Built with	When to use
`linux64`	GCC 11	Technical Preview only. Requires `glibc` 2.35 or later.
`linux64_gcc8`	GCC 8	Recommended. Matches the main Citrix Workspace app 2604 for Linux build and supports older `glibc` versions.

For most use cases, use `linux64_gcc8`. Use `linux64` only for Technical Preview validation on systems with `glibc` 2.35 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dual CWA package sets for Linux

Technical Preview from 2604 release Feedback form.

Starting with Citrix Workspace app for Linux 2604, the package includes two Linux package sets instead of one so that you can choose the build that matches your target environment.

Package line	Built with	When to use
GCC 8 package line	GCC 8	Uses the renamed packages with the `gcc-8` suffix and supports older `glibc` versions.
GCC 11 package line	GCC 11	Technical Preview only. Uses the original package names. Use for newer runtime environments such as Ubuntu 24.04 and later. Requires `glibc` 2.35 or later.

The GCC 8 package line includes:

- `icaclient-gcc-8_26.04.0.49_amd64.deb`
- `ICAClient-rhel-gcc-8-26.04.0.49-0.x86_64.rpm`
- `ICAClient-suse-gcc-8-26.04.0.49-0.x86_64.rpm`
- `linuxx64-gcc-8-26.04.0.49.tar.gz`
- `ctxusb-gcc-8_26.04.49._amd64.deb`
- `ctxusb-gcc-8-26.04.0.-1.x86_49.rpm`

System requirements and compatibility Consider the following compatibility details when you choose a package line:

- The GCC 11 package line is intended for newer environments such as Ubuntu 24.04 and later.
- The GCC 8 package line can be used on Ubuntu 24.04 and earlier.
- The GCC 8 package line uses renamed packages with the `gcc-8` suffix and continues with `webkit2gtk-4.0` and `libsoup-2.4`.
- The GCC 11 package line uses the original package names.
- The GCC 11 package line uses updated dependency tracks such as `webkit2gtk-4.1` and `libsoup-3.0`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For GCC 11 builds, install the following packages if they are not already present:

```
sudo apt install libsoup-3.0-dev libwebkit2gtk-4.1-dev
```

RHEL 8 and RHEL 9 support only the GCC 8 package line because they use older `glibc` versions. ARM64 platforms, such as Raspberry Pi 4, support only the GCC 11 package line.

Audio Quality Enhancer for reliable transport

Technical Preview from 2601 release Feedback form.

Starting with version 2601, audio quality enhancer is also available for connections over reliable transport (that is, TCP and EDT-Reliable). Under poor network conditions, both audio playback and recording have a smoother experience with reduced latency.

To enable and disable this feature, see Audio quality enhancer for Linux VDA.

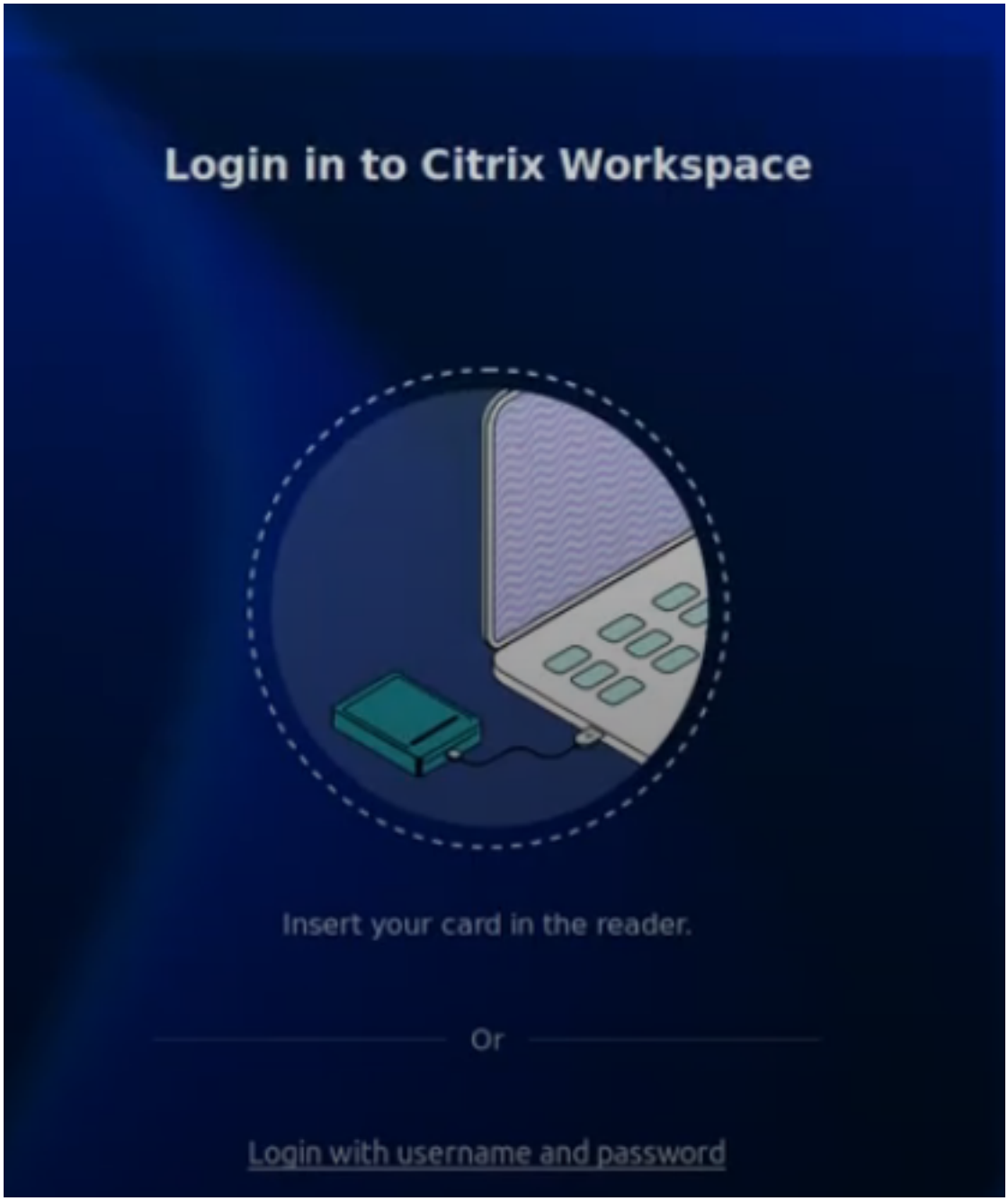
> **Note:**
>
> - Adaptive audio must be enabled for this feature to work.
> - This feature is disabled by default in Technical Preview (over reliable transport).
> - This feature must be enabled on both VDA and CWA.
> - This feature is supported with Linux VDA version 2511 and later, and Mac VDA version 2507 and later.

Smart card authentication support for Boot-to-VDI

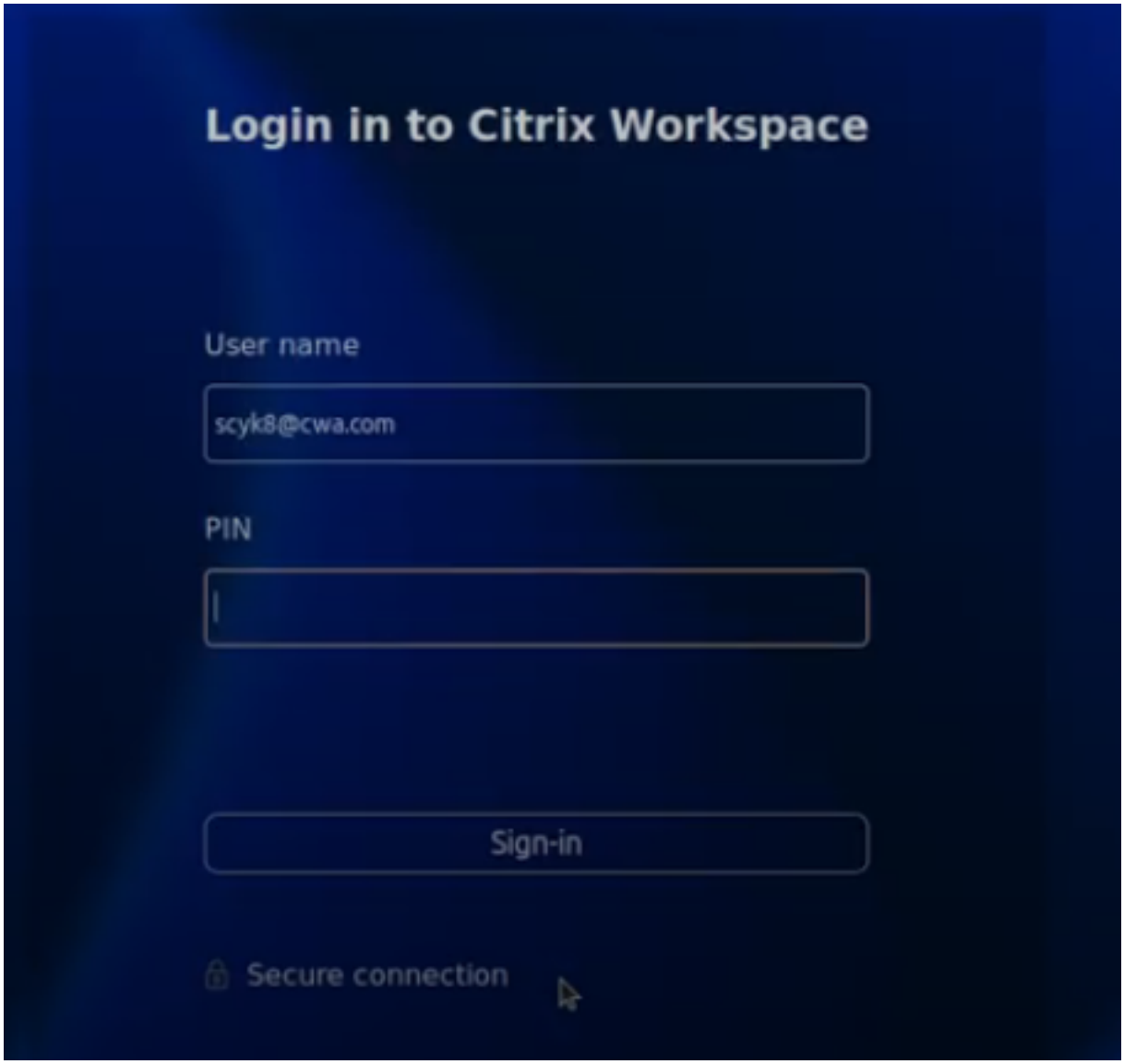
Technical Preview from 2508 release Feedback form.

Starting with this release, Boot-to-VDI supports smart card authentication with a new intuitive interface. For information on configuring smart card, see Boot to Virtual Desktop and Smart card sections in the documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> Features in the 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.

Browser Profile Sharing in Browser Content Redirection

Technical Preview from 2508 release	Feedback form.

BCR now offers a streamlined user experience with the new Profile Sharing feature, enabling VDA-side

© 1997–2026 Citrix Systems, Inc. All rights reserved.

authentication and cookie sharing. This enhancement eliminates redundant logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed. This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client. For more information, see Citrix Virtual Apps and Desktops™ documentation.

Requirements for Tech Preview::

- Citrix Virtual Apps and Desktops 2507
- Citrix Workspace App for Linux 2508
- Latest Browser Content Redirection Extension
- Microsoft Edge Extension
- Google Chrome Extension

Loss tolerant mode for graphics

Technical Preview from 2503 release Feedback form.

The loss tolerant mode for graphics feature enables Citrix Workspace™ app for Linux to use the loss tolerant mode for graphics in Citrix sessions, improving the video experience, particularly in poor network conditions.

Loss tolerant mode for graphics improves performance by allowing Citrix applications to handle video and graphics better, even when the network connection isn't strong. For users who work remotely or in areas with unreliable networks, this feature ensures that graphics-heavy applications remain usable without major performance issues like lag or pixelation.

With this feature, you can do the following:

- Access and use applications seamlessly, even in unstable network conditions, without major interruptions.
- Enjoy smoother visuals and quicker response times, leading to a more productive and less frustrating work environment.
- Work from anywhere without sacrificing application quality, regardless of network conditions.

This feature is disabled by default. To enable this feature, do the following:

1. Navigate to the $HOME/.ICAClient/wfclient.ini folder.
2. Go to the [Thinwire3.0] section.
3. Add the following entry:

```
LossTolerantModeEnabled=True
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for H.264 hardware decoding for seamless apps

Technical Preview from 2503 release Feedback form.

Starting with the 2503 version, Citrix Workspace app for Linux now supports H.264 hardware decoding for seamless apps, utilizing the GPU on the client device.

To enable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Go to the `[Thinwire3.0]` section.
3. Add the following entry:

```
TWIOpenGLEnabled=True
OpenGLEnabled=True
```

> **Note:**
>
> If hardware decoding acceleration is enabled, then:
>
> - The maximum window size supported by the client is 4096x4096 (approximately 4K).
> - For some Red Hat operating systems with Intel graphics, you might notice that "X11 rendering enabled"printed in `ICAClient.log` after launching a session. In such cases, you need to verify whether the intel-media-driver is installed.

Enhanced Unified Communications SDK API

Technical Preview from 2408 release Feedback form.

Starting with the 2408 version, Citrix Workspace app for Linux has enhanced support for UCSDK. With this feature, the UCSDK API can obtain more accurate deviceID and groupID for audio and video devices on Linux clients.

The deviceID is designed to identify devices of different models or the same model. With this feature, if you switch devices of the same model, the Optimized Microsoft Teams can now be enhanced to identify the change in the device with the deviceID information.

The groupID is designed to identify the microphone, speaker, and camera from the same physical devices. With this feature, Optimized Microsoft Teams can now be enhanced to group the microphone and camera of the same USB device together with the groupID information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This enhancement can provide a better multimedia conferencing and P2P call experience when using Optimized Microsoft Teams.

You can request access for this feature using this Enablement Form.

Support integrated windows authentication for browser content redirection

Technical Preview from 2408 release Feedback form.

Previously, the browser content redirection feature used a basic authentication method that required users to authenticate with their VDA credentials each time they accessed the web server.

Starting with the 2408 version, Citrix Workspace for Linux supports Integrated Windows authentication for browser content redirection that ensures single sign-on access to the web server.

For more information, see Single sign-on with Integrated Windows Authentication.

Support for H.265 hardware decoding

Technical Preview from 2408 release Feedback form

Starting with the 2408 version, Citrix Workspace app for Linux supports the GPU that can be used for H.265 decoding wherever it's available at the client. H.265 video codec must be supported and enabled on both the VDA and Citrix Workspace app. If your device doesn't support H.265 hardware decoding, then the session falls back to the H.264 video codec.

Prerequisites for H.265

- VDA 7.16 or later
- Use any of the following GPUs in VDA:
  - NVIDIA Maxwell generation GPU or later
  - Intel 6th generation GPU or later
  - AMD Raven generation GPU or later
- Enable the **Optimize for 3D graphics workload policy** on the VDA.
- Enable the **Use hardware encoding for video codec policy** on the VDA.

This feature is set to be disabled by default.

To enable this feature, complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Go to the [Thinwire3.0] section.
3. Add the following entry:

For H.265 hardware decoding:

```
OpenGLEnabled=True
H265Enabled=True
```

> **Note**
>
> If hardware decoding acceleration is enabled, then:
>
> - In the window mode, the maximum window size supported by the client is 4096x4096 (approximately 4K).
> - For some Red Hat operating systems with Intel graphics, you might notice that "Initialized h264 software decoding successfully"printed in `ICAClient.log` after launching a session. In such cases, you need to verify whether the intel-media-driver is installed.

Include system audio while screen sharing

Technical Preview from 2402 release Feedback form

Previously, the **Include computer sound** button wasn't enabled during screen sharing or app sharing. Starting with Citrix Workspace app version 2402, the **Include computer sound** button is enabled and you can use the system audio while sharing the screen. This feature allows you to share the audio playing on the VDA with users in a meeting or call.

> **Note:**
>
> This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, go to the Microsoft site and search for Microsoft 365 roadmap. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

This feature is disabled by default. To enable this feature, do the following on the client:

1. Navigate the `/var/.config/citrix/hdx_rtc_engine/config.json` file.
2. Add the following:

```
{


"ms_teams_share_system_audio": "true"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
5
6   }
```

3. Navigate to `config/module.ini` under the directory where Citrix Workspace app is installed. The default directory is: `/opt/Citrix/ICAClient/`.
4. Append the following key to the "[ClientAudio]"section:

```
1  EnableAudioListener=TRUE
```

To disable this feature, set the preceding parameters as follows:

```
1  ms_teams_share_system_audio": "false"
2  EnableAudioListener=FALSE"
```

Known limitation:

When you share with RAVE and BCR redirected apps or tabs, the audio from these apps or tabs might not be shared.

Known issue:

When you share a screen including computer sound, if multiple audio output devices are playing sound, one or more receivers might notice sound artifacts. [HDX-58342]

App Protection compatibility with HDX optimization for Microsoft Teams

Technical Preview from 2311 release Feedback form

Optimized Microsoft Teams supports screen sharing when Citrix Workspace app is enabled with App Protection in the Desktop Viewer mode only. When you click **Share content** in Microsoft Teams, the screen picker provides the following options:

- Window option to share any open app - This option is displayed only if the VDA version is 2109 or later.
- Desktop option to share the contents on your VDA desktop.

> **Note:**
>
> For Citrix Workspace app for Linux, the Desktop share option is disabled by default.

To enable the Desktop share option, add the `UseGbufferScreenSharing` parameter in your `config.json` file as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


      "UseGbufferScreenSharing":1

 }
```

Optimized Microsoft Teams enabled with App Protection also supports the Citrix virtual monitor layout which allows you to share each virtual monitor individually.

Limitations:

- Optimized Microsoft Teams enabled with App Protection doesn't support screen sharing on Published Desktops enabled with Local App Access (LAA).
- Client-rendered content such as Browser content using BCR can't be captured or shared. If you try to screen capture, it's displayed as a black screen.

Hardware acceleration support for optimized Microsoft Teams

Technical Preview from 2305 release Feedback form

Citrix Workspace app for Linux provides an improved performance experience for Microsoft Teams video calls.

Earlier only the CPU was used for encoding purposes. With this release, the GPU can also be used to encode the outgoing video frames and thus reduce CPU usage. This feature is of benefit when you use a thin client with limited CPU resources and a spare GPU.

Prerequisite:

Ensure you have the latest GPU driver. If not, install the latest GPU driver using the following command:

```
```
sudo apt install va-driver-all
```
```

This feature is disabled by default. To enable this feature, do the following:

1. Navigate to `/var/.config/citrix/hdx_rtc_engine/config.json` file.
2. Set the following configuration:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
  "VideoHwEncode": 1,  }
```

Support for Service continuity with Citrix Workspace Web Extension for Google Chrome

Technical Preview from 2109 release Feedback form

Support for service continuity with the Citrix Workspace Web Extension for Google Chrome is in a public technical preview. You can use the Workspace Web Extension for Google Chrome with Citrix Workspace app for Linux 2109. This extension is available at the Google Chrome web store. The Workspace app communicates with the Citrix Workspace Web extension using the native messaging host protocol for the browser extension. Together, the Workspace app and the Workspace Web extension use Workspace connection leases to give browser users access to their apps and desktops during outages. For more information, see Service continuity.

Technical Preview to General Availability (GA)

Service or feature	General availability version
GACS supports Citrix Workspace app for Linux	2508
NFC support for FIDO2 Authentication	2508
Support for H.264 hardware decoding	2508
PDF Universal Printing	2508
Clipboard Support for HTML-formatted text	2508
Multi-monitor layout selection	2503
Connection strength indicator on Desktop Viewer toolbar	2503
Support for WebHID API in UCSDK	2411
HDX direct	2411
Sustainability initiative from Citrix Workspace app	2411
Noise suppression	2411
Provision to manage multiple proxy servers	2408

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service or feature	General availability version
Support for Cryptography Next Generation smartcards	2408
Performance optimization for graphics	2408
Enhanced Desktop Viewer toolbar	2408
Customize toolbar	2408
Improved loading experience for shared user mode	2408
Fast smart card	2408
Multiple webcam resolutions support	2408
Loss tolerant mode for audio	2402
Support for Audio volume synchronization	2402
Support for DPI matching	2311
Support for IPv6 UDP with DTLS	2311
Support for IPv6 TCP with TLS	2311
Multi-touch support	2311
Enhancement to multiple monitors	2311
Support for authentication using FIDO2 when connecting to on-premises stores	2309
Support for 32-bit cursor	2309
Copy and paste files and folders between two virtual desktops	2309
Screen pinning in custom web stores	2309
Keyboard input mode enhancements	2309
Support for extended keyboard layouts	2309
Support for ARM64 architecture	2309
HTTPS protocol support for proxy server	2308
Addition of client-side jitter buffer mechanism	2305
Inactivity Timeout for Citrix Workspace app	2303
Support for authentication using FIDO2 in HDX session	2303

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service or feature	General availability version
Improved audio echo cancellation support	2303
Persistent login	2303

Citrix Workspace app for Linux 2608 - Preview

September 7, 2026

You can download Citrix Workspace app for Linux 2608 preview version from the Downloads page.

> **Note:**
>
> This is an Early Access Build shared for the purpose of testing or validation with the intent to make organizations ready for the upcoming release and is NOT advised to be deployed in production environments.

What's new

The following is a list of features that are available in Citrix Workspace app 2608 for:

- Image copy and paste from the client to the session
- Version upgrade for Chromium Embedded Framework
- Web page zoom synchronization for Browser Content Redirection
- Webcam device selection in Preferences
- Restart option on the Boot to virtual desktop screen
- Biometric user verification for security keys in an HDX session
- HDX Direct support for traditional direct connections
- Support for Ubuntu 26.04
- Improved session reconnection experience
- Improved Point of Presence (PoP) selection
- Enhanced virtual apps and desktops launch experience (Technical Preview)
- Dynamic smart card support

Image copy and paste from the client to the session

Starting with Citrix Workspace app 2608 for Linux, you can copy an image on the local Linux device and paste it into the virtual app or desktop session using the clipboard. This enhancement extends

© 1997–2026 Citrix Systems, Inc. All rights reserved.

clipboard redirection to support images, so you can move image content from the client to the session as easily as text.

This feature supports the following image formats:

- BMP
- JPEG
- PNG

Version upgrade for Chromium Embedded Framework

Starting with Citrix Workspace app 2608 for Linux, the version of the Chromium Embedded Framework (CEF) used by Browser Content Redirection (BCR) is upgraded to 148. This upgraded version incorporates the latest security and stability improvements.

Web page zoom synchronization for Browser Content Redirection

Starting with Citrix Workspace app 2608 for Linux, Browser Content Redirection (BCR) synchronizes the zoom level between the VDA browser and the client-rendered BCR overlay. This synchronization ensures that the web content is scaled consistently across the session.

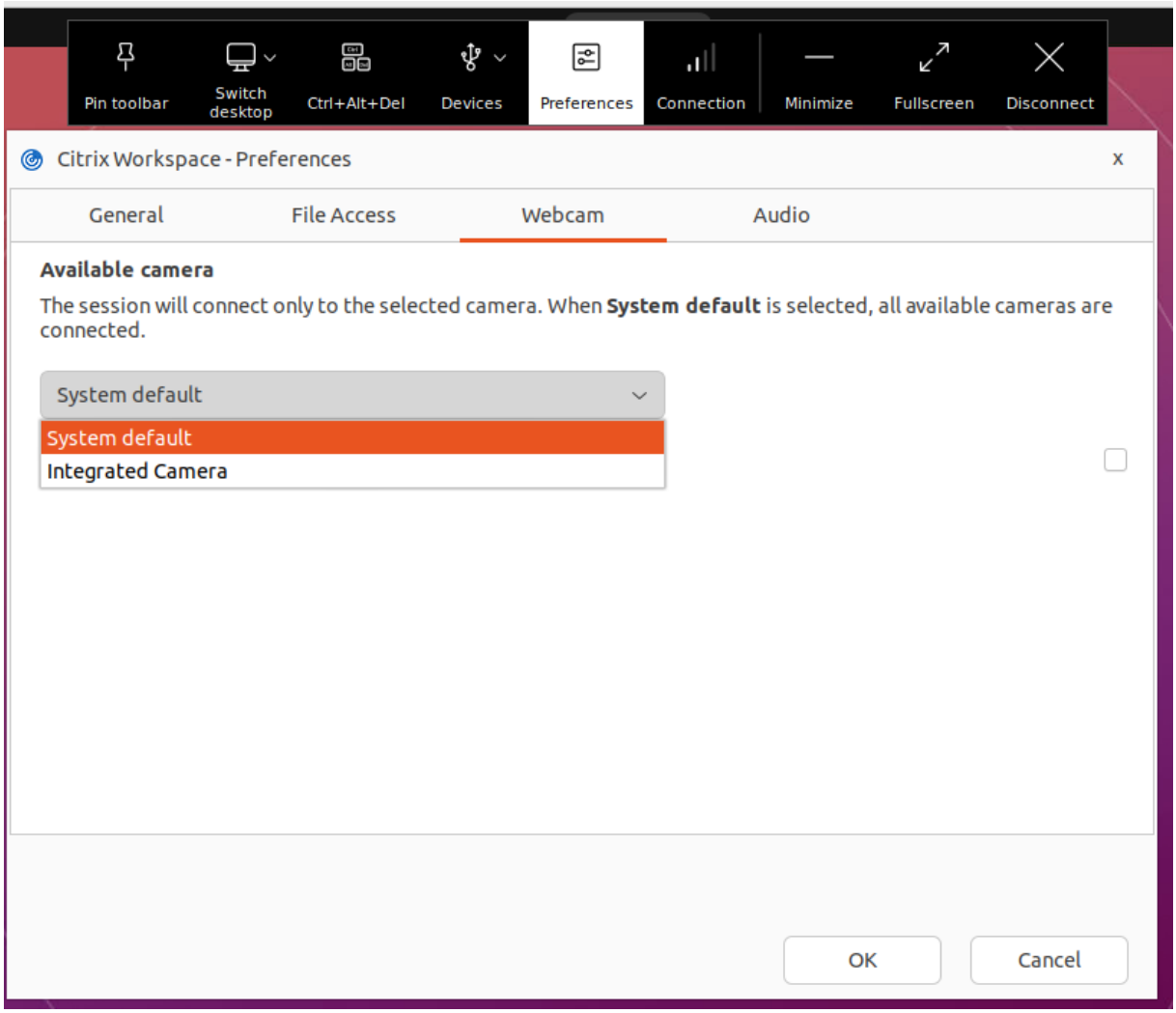
Webcam device selection in Preferences

Starting with Citrix Workspace app 2608 for Linux, a webcam device drop-down list is available in **Preferences**. The drop-down list shows all webcams connected to the local Linux device and allows you to select one of the following options:

- **System default (default)**: Redirects all available webcams to the session.
- **A specific webcam device**: Redirects only the selected webcam to the session.

The selected webcam preference is saved per resource and is automatically applied when you reconnect to the same resource.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Restart option on the Boot to virtual desktop screen

Starting with Citrix Workspace app 2608 for Linux, you can restart an endpoint directly from the **Boot to virtual desktop** screen using the new **Restart** button. Earlier, when a device was configured for Boot to virtual desktop (DesktopLock), this screen offered only the **Shut down** and **Network/Wi-Fi settings** options. To restart the device, for example, after OS updates, network changes, or troubleshooting, you had to shut it down and then power it on again locally or through a remote power-on command.

The **Restart** button now appears next to the **Shut down** button, so you can restart the endpoint in a single step. You can also show or hide each power button (**Shut down**, **Restart**, and **Network/Wi-Fi settings**) independently using the configuration keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User experience On the Boot to virtual desktop screen, the power buttons appear in the following order:

- **Shut down**: Powers off the endpoint device. This is the existing behavior.
- **Restart**: Restarts the endpoint device.
- **Network / Wi-Fi settings**: Opens the network settings. This is the existing behavior.

The **Restart** button is available on both the idle or lock screen and the error screen.

Configure the power buttons By default, the **Shut down**, **Restart**, and **Network/Wi-Fi settings** buttons are displayed. To hide any of these buttons, edit the `AuthManConfig.xml` file:

1. Open the `$ICAROOT/config/AuthManConfig.xml` file.
2. Set the required keys as shown in the following table.
3. Save the file. The change takes effect the next time the Boot to virtual desktop screen starts.

Setting	Controls	Default value	To hide the button
`DesktopLockShowShutdownButton`	Shut down button	**`true`** (shown)	Set to **`false`**
`DesktopLockShowRebootButton`	Restart button	**`true`** (shown)	Set to **`false`**
`DesktopLockShowWifiButton`	Network / Wi-Fi settings button	**`true`** (shown)	Set to **`false`**

For example, to hide the Network/Wi-Fi settings button and keep the Shut down and Restart buttons:

```
<DesktopLockShowShutdownButton>true</DesktopLockShowShutdownButton>
<DesktopLockShowRebootButton>true</DesktopLockShowRebootButton>
<DesktopLockShowWifiButton>false</DesktopLockShowWifiButton>
```

> **Note:**
>
> - A button is hidden only when its key is set to **`false`**. Any other value, or a missing or empty key, keeps the button visible. The values are case-insensitive.
> - When all three buttons are hidden, the entire power-button area is removed from the screen.

Default behavior and upgrade impact

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- After the upgrade, existing Boot to virtual desktop deployments get the **Restart** button automatically. No configuration is required.
- This feature is backward compatible. When you don't change the configuration, the **Shut down** and **Network/Wi-Fi settings** buttons appear as before, with the **Restart** button added alongside.

Biometric user verification for security keys in an HDX session

Starting with Citrix Workspace app 2608 for Linux, you can complete user verification with a fingerprint on FIDO2 biometric (BIO) security keys in an HDX session. When an app or a website in the session requests user verification, you can confirm your identity using the fingerprint sensor on the security key instead of entering the security key PIN.

Earlier, user verification always relied on the security key PIN. A biometric security key that had a fingerprint enrolled but no PIN was rejected, and a key that had both a fingerprint and a PIN always prompted for the PIN, which bypassed the fingerprint sensor.

Your biometric data never leaves the security key. Only the result of the verification is sent to the session.

No additional configuration is required for biometric security keys.

Prerequisites

- A FIDO2 security key that has a fingerprint sensor with at least one fingerprint enrolled.
- FIDO2 redirection enabled on the client. It is enabled by default starting with version 2505. For more information, see Support for authentication using FIDO2 in HDX session.

> **Note:**
>
> The fingerprint sensor is the preferred verification method. If the fingerprint is not recognized or on-device verification is locked out, and the security key also has a PIN, Citrix Workspace app prompts for the PIN and retries the operation.

Limitations

- You can not enroll or manage fingerprints on the security key using Citrix Workspace app. To enroll a fingerprint, use the security key vendor's tool, for example, Yubico Authenticator.
- Biometric verification applies only when the app or the website requests user verification as **required**. When user verification is requested as **preferred** or **discouraged**, the behavior is unchanged.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX Direct support for traditional direct connections

Starting with version 2608, Citrix Workspace app for Linux supports securing traditional direct connections through HDX Direct in both DaaS Local and DaaS Cloud environments. The relevant access scenarios are:

- Citrix Workspace with Direct Workload Connection enabled.
- Citrix Workspace with resource location connectivity set to Internal only.
- Citrix StoreFront accessed from inside the network.

For more information, see Traditional direct connections.

Support for Ubuntu 26.04

Starting with Citrix Workspace app 2608 for Linux, Ubuntu 26.04 (x86_64) is supported, in addition to the previously supported Ubuntu 22.04 and Ubuntu 24.04.

- This support applies to the GCC 11 build of Citrix Workspace app for Linux (`.deb` or `.tar.gz` package).

Prerequisites Some packages that are present by default on earlier Ubuntu releases are not installed by default on Ubuntu 26.04. Install these packages manually:

```
1 sudo apt install dbus-x11 gnome-keyring libsecret-1-0 net-tools
```

The following table lists these packages and the reason each one is required:

Package	Reason
`gnome-keyring`, `libsecret-1-0`	Secure storage of authentication tokens or credentials.
`dbus-x11`	D-Bus session support.
`net-tools`	Required runtime dependency that is not installed by default on Ubuntu 26.04.

> **Note:**
>
> Ubuntu 26.04 ships `webkit2gtk-4.1` by default, which the GCC 11 build uses. You don't have to install a separate WebKitGTK package.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved session reconnection experience

Starting with Citrix Workspace app 2608 for Linux, the session reconnection experience is improved with the following enhancements:

- **Reconnect during the Auto-Client-Reconnect (ACR) phase**. A reconnect option now appears while the ACR countdown is running, so you do not have to wait for the countdown to finish before you reconnect.
- **Automatic sign-in when your store session has expired**. If your sign-in to the store has expired by the time you reconnect, Citrix Workspace app starts the sign-in automatically. The reconnection screen displays **Verifying authentication** while sign-in is in progress. After you sign in successfully, the session is relaunched automatically, and you do not have to start the desktop or the app again manually.
- **Reconnection for hybrid-launched sessions**. You can now reconnect to desktop and app sessions that were started using hybrid launch, on both on-premises and cloud stores, after automatic reconnection fails. In earlier versions, hybrid-launched sessions were not supported. This capability is enabled by default.
- **Blurred session background**. While reconnection is in progress, or after it fails, the session content behind the reconnection screen is blurred and dimmed. This behavior keeps the reconnection options readable and prevents session content from being viewed while the session is disconnected.

These enhancements are enabled by default.

> **Note:**
>
> The reconnection timeout is paused while you are signing in. A sign-in that takes time, for example, when multifactor authentication is required, does not cause the reconnection to fail. If the sign-in is not completed within 30 minutes, the reconnection attempt fails, and you can select the reconnect option again.

Configure the reconnection options Administrators can control the reconnection options using the following settings in the `$HOME/.ICAClient/wfclient.ini` file:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting	Section	Default	Description
ManualReconnectEnabled	[WFClient]	True	Controls whether the reconnect option is available. When set to False, the reconnect option is hidden on all screens. The reason for the disconnection is still displayed.
ShowReconnectDuringACR	[WFClient]	True	Controls whether the reconnect option appears during the ACR phase. This setting is ignored when ManualReconnectEnabled is set to False.
ManualReconnectDuration	[WFClient]	86400	The time, in seconds, that the reconnect option stays available after reconnection fails. The default is 24 hours. Values outside the range 60-604800 are adjusted to the nearest limit.

To change a setting:

1. Open the $HOME/.ICAClient/wfclient.ini file.
2. Add the setting under the [WFClient] section. For example:

```
[WFClient]
ManualReconnectEnabled=False
```

3. Restart the session for the change to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved Point of Presence (PoP) selection

Starting with version 2608, Citrix Workspace app for Linux improves Gateway Service PoP selection for eligible Citrix Gateway Service sessions. When configured and session latency exceeds the defined threshold, the Citrix Workspace app for Linux can evaluate candidate PoPs associated with the Gateway Service FQDN and reconnect through a better-performing PoP. This enhancement helps improve session responsiveness when applicable.

This feature is disabled by default. To enable it, set: `AdaptiveGatewaySelectionEnabled=True` under the `[Network]` section of the `$HOME/.ICAClient/All_Regions.ini` file.

Enhanced virtual apps and desktops launch experience (Technical Preview)

Starting with Citrix Workspace app 2608 for Linux, you can enable a launch status indicator that shows real-time progress for app and desktop launches and for store operations. Progress appears as a stack of status cards in the bottom-right corner of the primary monitor. You can see how a launch is advancing instead of waiting with no feedback after selecting a resource.

The indicator covers the launch from the moment a resource is selected to the point where the session window appears on screen. Adding an account and refreshing apps produce their own cards.

This feature is disabled by default.

> **Note:**
>
> This feature is in Technical Preview. Citrix recommends that you use it in nonproduction or limited production environments.

Configure the launch status indicator The launch status indicator is disabled by default. To enable it, edit the `$ICAROOT/config/AuthManConfig.xml` file:

1. Open the `$ICAROOT/config/AuthManConfig.xml` file.
2. Set the required keys to **`true`**, as shown in the following table.
3. Save the file, and then restart Citrix Workspace app for the change to take effect.

Setting	Controls	Default
`LaunchStatusIndicatorEnabled`	Launch status indicator.	**`false`**
`LaunchStatusIndicatorPreAuthEnabled`	Cards for store operations, such as adding an account and refreshing apps.	**`false`**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, to enable both the launch status indicator and the store-operation cards:

```
<!-- LaunchStatusIndicatorEnabled - true, false -->
<key>LaunchStatusIndicatorEnabled</key>
<value>true</value>
<!-- LaunchStatusIndicatorPreLaunchEnabled - true, false -->
<key>LaunchStatusIndicatorPreLaunchEnabled</key>
<value>true</value>
```

> **Note:**
>
> `LaunchStatusIndicatorEnabled` controls the overall feature. When it is set to **`false`**, no cards appear for any operation. To show launch cards but not store-operation cards, set `LaunchStatusIndicatorEnabled` to **`true`** and leave `LaunchStatusIndicatorPreLaunchEnabl` set to **`false`**.

Known limitations

- Web and SaaS resources do not produce a status card, because they do not open an HDX session.
- The indicator supplements rather than replaces existing error messages in Citrix Workspace app.

Dynamic smart card support

Starting with Citrix Workspace app 2608 for Linux, you can use smart cards from different vendors on the same device without configuring a fixed driver. When you insert a card, Citrix Workspace app reads the card's Answer To Reset (ATR), selects the matching PKCS#11 driver, and loads that driver automatically. Cards that you insert or remove during authentication are detected in real time, so you can switch between cards from different vendors without any manual steps.

Earlier, Citrix Workspace app for Linux could use only a single, fixed PKCS#11 driver. As a result, only one smart card type worked at a time, and an administrator had to configure the driver in advance.

This feature applies to client-side smart card authentication to Citrix StoreFront or NetScaler Gateway. In-session ICA smart card redirection is a separate, existing capability that is unchanged.

This feature is enabled by default (`MultipleSmartCardSupported`=**`true`**), so you do not have to configure a driver value.

> **Note:**
>
> The fixed-driver setting `PKCS11module` in the `AuthManConfig.xml` file is deprecated. It is used only as a fallback when `MultipleSmartCardSupported` is set to **`false`**. For more information, see Revert to a single fixed driver.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

Requirement	Details
Citrix Workspace app for Linux	Installed at `/opt/Citrix/ICAClient/` (`$ICAROOT`).
PC/SC middleware	`pcsc-lite-libpcsclite.so` (or `libpcsclite.so.1`) must be present. If it is missing, smart card support is disabled.
PC/SC daemon	`pcscd` running, which is required for card reader insert and remove events.
A PKCS#11 driver	The `.so` file for your card, for example, `opensc-pkcs11.so` (OpenSC), `libykcs11.so` (YubiKey), or `libIDPrimePKCS11.so` (SafeNet). Installed under a standard PKCS#11 directory such as `/usr/lib64/pkcs11` or `/usr/lib/x86_64-linux-gnu/pkcs11`.
A supported smart card and reader	A USB reader and a card whose certificate is enabled for logon.

If the dependencies are not already present, install them as follows:

On Ubuntu or Debian:

```
sudo apt-get install pcscd libpcsclite1 opensc
sudo systemctl enable --now pcscd
```

On RHEL:

```
sudo dnf install pcsc-lite pcsc-lite-ccid opensc
sudo systemctl enable --now pcscd
```

Install the vendor PKCS#11 package instead of, or in addition to, `opensc` when your card is not supported by OpenSC. For example, install SafeNet Authentication Client for Gemalto IDPrime .NET cards.

How it works By default (`MultipleSmartCardSupported=true`), Citrix Workspace app does not load any PKCS#11 module at startup. When you insert a card, it reads the card's ATR, selects the matching driver, and loads that driver. If you later insert a different card, Citrix Workspace app switches to the driver for that card automatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app selects the driver from the following three sources, checked in priority order. It uses the first source that matches the card and does not check the remaining sources.

Priority	Source	Description
1	`smartcard_drivers.ini`	The ATR-to-driver mapping table, which contains `[card:Name]` sections and a `[fallback]` driver.
2	`~/.ICAClient/learned_drivers.json`	A cache that Citrix Workspace app updates after it successfully detects a driver for a card.
3	Auto-detect	Automatic detection that tests the installed driver files to find one that works with the card. This source is disabled by default.

Configure ATR-to-driver mappings The `smartcard_drivers.ini` file maps a card's ATR to its PKCS#11 driver. Citrix Workspace app uses only one file and does not merge the two files. When the system file is present, it takes precedence:

- `$ICAROOT/config/smartcard_drivers.ini` –The system default. This file is owned by root and is preferred.
- `$HOME/.ICAClient/smartcard_drivers.ini` –The per-user file, which is used only when the system file does not exist. This file is restricted for security. Citrix Workspace app ignores the `[library_paths]` section and any absolute driver paths, and accepts only driver file names that resolve within the standard system directories.

The file that ships with Citrix Workspace app already covers common cards, including YubiKey 5, 5 FIPS, and NEO, and Gemalto IDPrime MD, .NET, and .NET Astrid. It also includes an `opensc-pkcs11.so` fallback, so any card that OpenSC supports works without changes.

The file uses the following format:

```
[library_paths]
path1 = /usr/lib64/pkcs11
path2 = /usr/lib/x86_64-linux-gnu/pkcs11

[card:YubiKey_5]
driver = libykcs11.so
atr = 3BFD1300008131FE158073C021C057597562694B6579
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
8
9  [card:Gemalto_IDPrime_MD]
10 driver = opensc-pkcs11.so
11 atr = 3B7F9600008031B8658B0802
12
13 [fallback]
14 driver = opensc-pkcs11.so
```

To add a new card type, append a section with the driver and one or more ATR prefixes:

```
1  [card:MyNewCard]
2  driver = my-pkcs11-driver.so
3  atr = 3B12AB34CD
4  atr = 3B56EF7890
```

The following table describes the fields:

Field	Description
`driver`	The PKCS#11 driver. A driver file name is resolved through the `[library_paths]` section and the standard directories. Absolute paths are accepted only in the system file.
`atr`	The ATR hex prefix, which is not case-sensitive. Repeat this key to map more than one ATR to the same card.
#	A comment line, which Citrix Workspace app ignores.

Revert to a single fixed driver Dynamic, ATR-based selection is the default. If you need the legacy behavior, that is, a single, fixed PKCS#11 driver that is loaded at startup, you can turn off dynamic selection with the `MultipleSmartCardSupported` key in the `AuthManConfig.xml` file.

Value	Effect
`true` (default)	Citrix Workspace app selects the driver for each card dynamically from `smartcard_drivers.ini`.
`false`	Dynamic selection is turned off. Citrix Workspace app loads the single fixed driver that is named in the deprecated `PKCS11module` key at startup.

When `MultipleSmartCardSupported` is **`false`**, set the driver path in the deprecated `PKCS11module` key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<key>MultipleSmartCardSupported</key>
<value>false</value>
<key>PKCS11module</key>
<value>/usr/lib64/pkcs11/opensc-pkcs11.so</value>
```

Note:

- `PKCS11module` is deprecated. Citrix Workspace app reads it only when `MultipleSmartCardSuppor` =**`false`**. When `MultipleSmartCardSupported`=**`true`** (the default), Citrix Workspace app ignores it.
- If `MultipleSmartCardSupported`=**`false`** and `PKCS11module` is empty or unset, Citrix Workspace app does not load any PKCS#11 module and logs a warning. Smart card authentication does not work until you supply a driver path.
- In this mode, only one card type works at a time. This is the earlier behavior, which is retained only for backward compatibility. Keep `MultipleSmartCardSupported`=**`true`** unless you have a specific reason to use a single driver.

Use dynamic smart card support

1. Ensure that `pcscd` is running and the driver for your card is installed.
2. If your card is already covered by the `smartcard_drivers.ini` file or by the OpenSC fallback, no configuration is needed. Otherwise, add a `[card:Name]` entry as shown earlier.
3. Launch Citrix Workspace app or Self-Service and authenticate to your Citrix StoreFront or NetScaler Gateway store.
4. Insert the smart card when prompted, and then enter the PIN or select the certificate. Citrix Workspace app detects cards that you insert during authentication and loads the matching driver automatically.

Troubleshooting

Symptom	Resolution
Smart card support disabled appears in the logs.	`libpcsclite.so` is not installed or cannot be loaded. Install `pcsc-lite`.
No readers appear, or the card is not detected.	Confirm that `pcscd` is running (`systemctl status pcscd`), and that `pcsc_scan` lists the reader.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Symptom	Resolution
The card is detected, but no certificate or token appears.	The selected driver does not support the card. Add a `[card:Name]` entry that points to the correct vendor PKCS#11 driver. For example, Gemalto IDPrime .NET "Astrid"cards require SafeNet's `libIDPrimePKCS11.so`, not OpenSC.
Cards are not selected dynamically, or only one card type works.	Check whether `MultipleSmartCardSupported` is set to **`false`** in the `AuthManConfig.xml` file. In that mode, Citrix Workspace app loads only the fixed `PKCS11module` driver. Set it back to **`true`** for dynamic, multi-card selection.

Fixed issues

Known issues

- When you launch a seamless application from a Linux client configured with 300% dots per inch (DPI) scaling, the application window might display a non-seamless frame and the message **Please wait...Adjusting screen resolution** while the session window is being resized. This issue is specific to 300% DPI configurations on Linux clients. As a workaround, reduce the DPI scaling on the Linux client from 300% to 200% or 100%. [HDX-106160]
- On a Wayland desktop session, snapping a seamless application window to half the screen by dragging it to the top edge might cause the window to freeze and show a distorted or mirrored image. [HDX-101776]

  As a workaround, perform any of the following:
  - Click the affected window once to refresh it and return it to normal.
  - Use an Xorg desktop session instead of Wayland to avoid the issue.

System requirements and compatibility

March 5, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

Hardware requirements

Linux kernel:

- Version 2.6.29 or later

Disk space:

- A minimum of 55 MB
- An extra 110 MB if you expand/extract the installation package on the disk
- A minimum of 1 GB RAM for system-on-a-chip (SoC) devices that use HDX™ MediaStream Flash Redirection

Color video display:

- 256 color video display or greater

Supported Linux distributions

Citrix Workspace app for Linux are supported on following Linux distributions:

Citrix Workspace™ app version	Linux distribution
2601	openSUSE 15.6 x86-64 RHEL 8.10 x86-64 and 9.5 x86-64 Ubuntu 2204 x86-64 and 2404 x86-64 Raspberry Pi OS Bookworm, arm64 Debian 11.9 x86-64 and Debian 12 to 12.6 x86-64
2508	openSUSE 15.6 x86-64 RHEL 9.5x86-64 Ubuntu 2204 x86-64 and 2404 x86-64 Raspberry Pi OS Bookworm, arm64 Debian 11.9 x86-64 and Debian 12 to 12.6 x86-64
2505	openSUSE 15.6 x86-64 RHEL 9.5x86-64 Ubuntu 2204 x86-64 and 2404 x86-64

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace™ app version	Linux distribution
2503	Raspberry Pi OS Bookworm, arm64 Debian 11.9 x86-64 and Debian 12 to 12.6 x86-64 RHEL 9.5 x86-64 Ubuntu 2204 x86-64 and 2404 x86-64
2411	Raspberry Pi OS Bookworm, arm64 Debian 12.8 x86-64 RHEL 9.4 x86-64 Ubuntu 2204 x86-64 and 2404 x86-64
2408	Raspberry Pi OS Bullseye, arm64 Debian 11.9 x86-64 and 12 to 12.6 x86-64 RHEL 9.4 x86-64 Ubuntu 2204 x86-64
	Raspberry Pi OS Bullseye, arm64 Debian 11.9 x86-64

Support for Ubuntu 2404 To support Citrix Workspace app for Linux on Ubuntu 2404, backporting the `webkit2gtk` library is required. Follow the steps below to backport the library based on your architecture:

For x64 architecture:

1. Add the following packages for jammy:

   sudo apt-add-repository deb `http://us.archive.ubuntu.com/ubuntu` jammy main

   sudo apt-add-repository deb `http://us.archive.ubuntu.com/ubuntu` jammy-updates main

   sudo apt-add-repository deb `http://us.archive.ubuntu.com/ubuntu` jammy-security main

2. Install the library:

   ```
   sudo apt install libwebkit2gtk-4.0-dev
   ```

3. Post successful installation of the library `libwebkit2gtk-4.0-dev`, remove the the repositories:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sudo apt-add-repository -r deb http://us.archive.ubuntu.com/ubuntu jammy main

For arm64 architecture:

1. Add the following packages for jammy:

   sudo apt-add-repository deb [arch=arm64] http://us.archive.ubuntu.com/ubuntu jammy main

   sudo apt-add-repository deb [arch=arm64] http://us.archive.ubuntu.com/ubuntu jammy-updates main

   sudo apt-add-repository deb [arch=arm64] http://us.archive.ubuntu.com/ubuntu jammy-security main

2. Install the library:

   ```
   sudo apt install libwebkit2gtk-4.0-dev
   ```

3. Post successful installation of the library `libwebkit2gtk-4.0-dev`, remove the the repositories:

   sudo apt-add-repository -r deb [arch=arm64] http://us.archive.ubuntu.com/ubuntu jammy main

> **Note:**
>
> If this doesn't work due to dependencies, install `pixbuf-2.40` separately:
>
> ```
> sudo apt install libgdk-pixbuf-2.0-0=2.40.0+dfsg-3
> ```

Libraries and codec

Libraries:

- `glibcxx` 3.4.25 or later
- `glibc` 2.27 or later
- gtk 3
- gtk 2 (2.20.1 or later)
- libcap1 or libcap2
- `libva2`
- `libjson-c` (for instrumentation)
- X11 or X.Org (Wayland isn't supported)
- `udev` support
- Advanced Linux Sound Architecture (ALSA) libasound2
- PulseAudio
- `UIDialogLib3.so`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Self-service user interface:

- webkit2gtk 2.16.6 or later
- libxml2 2.7.8
- `libxerces-c` 3.1

Codec libraries:

- Speex
- Vorbis codec libraries

Red Hat Package Manager (RPM) based distribution requirements:

- `chkconfig`

Network requirements

Network protocol:

- TCP/IP

H.264 requirements

For x86 devices:

- A minimum processor speed of 1.6 GHz

For the HDX 3D Pro feature:

- A minimum processor speed of 2 GHz
- A native hardware with accelerated graphics driver

For ARM devices:

- A hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro

HDX MediaStream Flash Redirection

For all HDX MediaStream Flash Redirection requirements, see Knowledge Center article CTX134786.

We recommend that you test the article with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication requirements

cURL 7.68 or later with OpenSSL for cloud authentication.

Customer Experience Improvement Program (CEIP) integration requirements

- `zlib` 1.2.3.3
- `libtar` 1.2 or later
- `libjson` 7.6.1 or later

Smart card requirements

- Your smart card readers and published applications must be PC/SC industry standard compliant.
- Install the appropriate driver for your smart card.
- Install the PC/SC Lite package.
- Install and run the `pcscd` Daemon, which provides middleware to access the smart card using PC/SC.
- On a 64-bit system, both 64-bit and 32-bit versions of the "libpcsclite1"package must be present.

HDX RealTime webcam video compression requirements

- A `Video4Linux` compatible webcam
- `GStreamer` 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good"package

  Or,

- `GStreamer` 1.0 (or a later 1.x version), including the distribution's "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly", and "gstreamer-libav"packages

HDX MediaStream Windows Media redirection requirements

- `GStreamer` 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good"package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection

  Or,

- `GStreamer` 1.0 (or a later 1.x version), including the distribution's "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly", and "gstreamer-libav"packages

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Notes:**
>
> - If `GStreamer` isn't included in your Linux distribution, you can download it from the GStreamer page.
> - Use of certain codes (for example, as in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help.

Browser content redirection requirements

- webkit2gtk version 2.16.6

Philips SpeechMike requirements

- Visit the Philips website to install the relevant drivers

App Protection requirements

App Protection works best with the following Operating Systems along with the Gnome Display Manager:

- 64-bit Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- 64-bit Debian 9 and Debian 10
- 64-bit CentOS 7
- 64-bit RHEL 7
- ARMHF 32-bit Raspberry Pi OS (Based on Debian 10 (buster))
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

> **Note:**
>
> - If you're using Citrix Workspace app earlier than version 2204, the App Protection feature does not support the operating systems that use `glibc` 2.34 or later.
> - On Ubuntu 20.04.5 or later, when you double-click the `.deb` package file, the Snap Store installer opens. This installer doesn't support user prompts. So, you must install the Citrix Workspace app using the command line in a terminal or using other software installers like `gnome-software`, `gdebi`, and `synaptics`.

Endpoint Analysis (EPA) requirements

Endpoint Analysis (EPA) requires the following libraries:

- `libcurl4` version 7.68 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- libproxy1v5
- libglib2.0-0
- libxml2
- libpugixml1v5
- libgpgme11
- libwebkit2gtk-4.1-0

> **Note:**
>
> Endpoint Analysis (EPA) supports the following Operating Systems:
>
> - Ubuntu 22.04 and Ubuntu 24.04
> - ELUX 7

Microsoft Teams optimization requirements

Minimum version:

- Citrix Workspace app 2006

Software:

- GStreamer 1.0 or later and Cairo 2
- libc++-9.0 or later
- libgdk 3.22 or later
- OpenSSL 1.1.1d
- libnsl
- Ubuntu 20.04 or later

Hardware:

- A minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call
- A dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz

Authentication enhancement:

- Libsecret library
- libunwind-12 library

Service continuity requirements

Starting with Version 2106, you can install Service Continuity on the Debian version of Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the following commands from the terminal before installing Citrix Workspace app:

```
sudo apt-get update -y
```

Mandatory preinstalled libraries:

- libwebkit2gtk-4.0-37 version 2.30.1 or later
  - If you're using Debian, run the following command:

    ```
    1 sudo apt-get install libwebkit2gtk-4.0-37
    ```

  - If you're using RPM, run the following command:

    ```
    1 sudo yum install libwebkit2gtk-4*
    ```

  - For Ubuntu, RHEL, SUSE, Fedora, or Debian, Citrix recommends you to install the latest libwebkit2gtk-4.0-37 version 2.30.1 or later.
  - For the Raspberry Pi with Buster OS, Citrix recommends you to install the libwebkit2gtk-4.0-37 version 2.30.1.
- gnome-keyring version 3.18.3 or later
  - If you're using Debian, run the following command:

    ```
    1 sudo apt-get install gnome-keyring
    ```

  - If you're using RPM, run the following command:

    ```
    1 sudo yum install gnome-keyring
    ```

- Libsecret
  - If you're using Debian, run the following command:

    ```
    1 sudo apt-get install libsecret-1-0
    ```

  - If you're using RPM, run the following command:

    ```
    1 sudo yum install libsecret-1*
    ```

> **Notes:**
>
> Following the 1910 version, Citrix Workspace app works as expected only if the operating system meets the following GCC version criteria:
>
> - GCC version for x64 architecture: 4.8 or later
> - GCC version for ARMHF architecture: 4.9 or later
>
> Following the 2101 version, Citrix Workspace app works as expected only if the operating system

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> meets the following requirements:
>
> - GCC version 4.9 or later
> - `glibcxx` 3.4.20 or later
>
> Following the 2209 version, Citrix Workspace app works as expected only if the operating system meets the following requirement:
>
> `glibcxx` 3.4.25 or later

Compatibility matrix

Citrix Workspace app is compatible with all currently supported versions of the Citrix products.

For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the Citrix Product Lifecycle Matrix.

Server requirements

StoreFront

- You can use all currently supported versions of Citrix Workspace app to access StoreFront stores from both internal network connections and through Citrix Gateway:
  - StoreFront 1811 and later.
  - StoreFront 3.12.
- You can use StoreFront configured with the workspace for web. The workspace for web provides access to StoreFront stores from a web browser. For the limitations of this deployment, see Important considerations in the StoreFront documentation.

Connections and certificates

Connections

Citrix Workspace app for Linux supports HTTPS and ICA-over-TLS connections through any one of the following configurations.

- For LAN connections:
  - StoreFront using StoreFront services or workspace for web
- For secure remote or local connections:
  - Citrix Gateway 12.0 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway 10.1 and later
- NetScaler® Access Gateway Enterprise Edition 10
- Netscaler Access Gateway Enterprise Edition 9.x
- Netscaler Access Gateway VPX

For information about the Citrix Gateway versions supported by StoreFront, see System requirements of StoreFront.

Certificates

To ensure secure transactions between server and client, use the following certificates:

Private (self-signed) certificates If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the user device. This installation helps to access Citrix resources using Citrix Workspace app.

> **Note:**
>
> An untrusted certificate warning appears, if the remote gateway's certificate can't be verified upon connection. This verification might fail since the root certificate isn't included in the local key store. If you choose to continue through the warning, the apps are displayed but can't be launched. The root certificate must be installed in the client's certificate store.

Root certificates For domain-joined machines, use the Group Policy Object administrative template to distribute and trust CA certificates.

For non-domain joined machines, create a custom install package to distribute and install the CA certificate. Contact your system administrator for assistance.

Install root certificates on user devices To use TLS, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate. By default, Citrix Workspace app supports the following certificates.

Certificate	Issuing Authority
Class4PCA_G2_v2.pem	Verisign Trust Network
Class3PCA_G2_v2.pem	Verisign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate	Issuing Authority
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

Wildcard certificates Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app supports wildcard certificates, however they must only be used following your organization's security policy.

Alternatives to wildcard certificates, such as a certificate that includes the list of server names within the Subject Alternative Name (SAN) extension, can be considered. Both private and public certificate authorities issue such certificates.

Append intermediate certificate to Citrix Gateway If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway server certificate. For information, see Configuring Intermediate Certificates in the Citrix Gateway documentation.

If your StoreFront server fails to provide the intermediate certificates that match the certificate it's using, or you install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store:

1. Get one or more intermediate certificates separately in PEM format.

   > **Tip:**
   >
   > If you can't find a certificate in the .pem file extension, use the `openssl` utility to convert a certificate to the .pem file extension.

2. When you install the package (usually root):

   a) Copy one or more files to $ICAROOT/keystore/intcerts.

   b) Run the following command after you installed the package:

   ```
   $ICAROOT/util/ctx_rehash
   ```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

When validating a server certificate, Citrix Workspace app uses all the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Workspace app versions, it verifies that the certificates are trusted. If any certificate is untrusted, the connection fails.

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

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

If a gateway is configured with these valid certificates, use the following configuration for stricter validation. This configuration determines exactly which root certificate the Citrix Workspace app uses:

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

Citrix Workspace app verifies all these certificates are valid. Citrix Workspace app also verifies that it already trusts the Example Root Certificate. If Citrix Workspace app does not trust the 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 the GTE CyberTrust Global Root certificate at the gateway, Citrix Workspace app connections on those user devices fail. Consult the certificate authority's documentation to determine which root certificate must be used. Also note that root certificates even-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> tually expire, as do all certificates.
> - Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

If a gateway is configured with these valid certificates, we can use the following configuration, leaving out the root certificate:

- Example Server Certificate
- Example Intermediate Certificate

Citrix Workspace app uses these two certificates. It searches for a root certificate on the user device. If Citrix Workspace app finds a root certificate 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 needs, but also allows Citrix Workspace app to choose any valid, trusted, root certificate.

If a gateway is configured with these certificates:

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

A web browser might ignore the wrong root certificate. However, Citrix Workspace app does not ignore the wrong root certificate, and the connection fails.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is configured with all the intermediate certificates (but not the root certificate) such as:

- Example Server Certificate
- Example Intermediate Certificate 1
- Example Intermediate Certificate 2

> **Important:**
>
> - Some certificate authorities use a cross-signed intermediate certificate. This certificate is used where there's more than one root certificate, and an earlier root certificate is still in use 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 the *Class 3 Public Primary Certification Authority*. The later root certificate does not use a cross-signed intermediate certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To). But the cross-signed intermediate certificate has a different Issuer name (Issued By). This difference distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such as Example Intermediate Certificate 2).

This configuration, leaving out the root certificate and the cross-signed intermediate certificate, is recommended:

- Example Server Certificate
- Example Intermediate Certificate

Avoid configuring the 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 gateway with only the server certificate:

- Example Server Certificate

In this case, if Citrix Workspace app can't locate all the intermediate certificates, the connection fails.

Supports system certificate paths for SSL connection Previously, Citrix Workspace app supported only the `opt/Citrix/ICAClient/keystore` path as system certificate path. This path was a hardcode path to store Citrix predefined certificates. However, sometimes, certificate authority (CA) certificates are placed in the system certificates path in different linux distributions. To add these system certificate paths, customers had to make a soft link and replace `/opt/Citrix/ICAClient/keystore`.

With this release, Citrix Workspace app supports multiple system certificate paths. The following are the default system certificate paths supported for SSL connection:

```
"/var/lib/ca-certificates",
"/etc/ssl/certs",
"/system/etc/security/cacerts",
"/usr/local/share/cert",
"/etc/pki/tls/certs",
"/etc/openssl/certs",
"/var/ssl/certs",
ICAROOT() + "/keystore/cacerts"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In addition to the default system certified path, you can also add your own certified path by adding the `Certpath` field in the `AuthManConfig.xml` file as follows:

```
<!--Cert bundle file for Selfservice with AuthManLite. -->
<Certfile></Certfile>
<!--Cert folder path for Selfservice with AuthManLite.-->
<Certpath></Certpath>
```

This feature simplifies the certificate management process on the client side and improves the user experience. Citrix Workspace app for Linux supports multiple system certificate paths for SSL connection. This feature eliminates the need to create a soft link.

Workspacecheck

We provide a script, `workspacecheck.sh`, as part of the Citrix Workspace app installation package. The script checks whether your device meets all the system requirements in support of the functionalities of Citrix Workspace app. The script is in the `Utilities` directory of the installation package.

To run the workspacecheck.sh script

1. Open the terminal in your Linux machine.
2. Type `cd $ICAROOT/util` and press **Enter** to navigate to the `Utilities` directory of the installation package.
3. Type `./workspacecheck.sh` to run the script.

Out-of-support applications and operating systems

Citrix does not offer support in the context of applications and operating systems that are no longer supported by their vendors.

While attempting to address and resolve a reported issue, Citrix assesses whether the issue directly relates to an out-of-support application or operating system. To help in making that determination, Citrix might ask you to attempt to reproduce an issue using the supported version of the application or operating system. If the issue seems to be related to the out-of-support application or operating system, Citrix will not investigate the issue further.

Ubuntu 24.04+ webkit2gtk dependency resolution

Ubuntu 24.04 (Noble Numbat) and newer versions no longer include the webkit2gtk-4.0 library in the default repositories and it is replaced with webkit2gtk-4.1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The selfservice component of the Citrix Workspace app for Linux strictly depends on webkit2gtk-4.0. This mismatch prevents Citrix Workspace app from launching correctly on Ubuntu 24.04 and later versions.

To address this mismatch, Citrix Workspace app for Linux package now directly includes the webkit2gtk-4.0 library. This addition of the library ensures the dependency is met, allowing Citrix Workspace app for Linux to function consistently across all supported Ubuntu versions.

Install, Uninstall, and Update

September 7, 2025

You can install the Citrix Workspace app by downloading the file from the Citrix website at Downloads page.

Verify the version of the Citrix Workspace app

Perform the following steps to verify the current version of the Citrix Workspace app installed on your system:

1. Open a terminal window.
2. Run the following command:

   For Debian packages:

   ```
   dpkg --list | grep -i icaclient
   ```

   OR

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   ```

   For Red Hat packages:

   ```
   rpm -qa | grep -i icaclient
   ```

   OR

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   ```

   For Tarball packages:

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manual install

Download the following packages from the Citrix Downloads page.

Debian packages

Install the `Icaclient` package based on your OS architecture.

To use generic USB redirection, install one of the `ctxusb` packages based on your OS architecture. You can download the `ctxusb`package from the **USB Support Packages** section of Citrix Downloads page.

> **Note:**
>
> To avoid the compatibility issue, ensure that you install the same version of `Icaclient` and `ctxusb` packages.

Package name	Contents
Debian packages (Ubuntu, Debian, Linux Mint etc.)	
`icaclient_<version>_amd64.deb`	Self-service support, 64-bit x86_64
`icaclient_<version>_arm64.deb`	Self-service support, ARM 64
`ctxusb_<version>_amd64.deb`	USB package, 64-bit x86_64
`ctxusb_<version>_arm64.deb`	USB package, ARM 64

Install using a Debian package

> **Prerequisites:**
>
> Verify that you've installed all the required system requirements, as mentioned at the System requirements section.

When installing Citrix Workspace app from the Debian package on Ubuntu, open the packages in the Ubuntu Software Center.

In the following instructions, replace
packagename with the name of the package that you're trying to install.

This procedure uses a command line and the native package manager for Ubuntu, Debian, or Mint. You can also install the package by double-clicking the downloaded .deb package in a file browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This action typically starts a package manager that downloads any missing required software. If no package manager is available, Citrix® recommends you to use the **gdebi**, a command-line tool.

> **Note:**
>
> On Ubuntu 20.04.5 or later, when you double-click the `.deb` package file, the Snap Store installer opens. This installer doesn't support user prompts. So, you must install the Citrix Workspace app using the command line in a terminal or using other software installers like `gnome-software`, `gdebi`, and `synaptics`.

To install the package using the command line:

1. Log on as a privileged (root) user.
2. Open a terminal window.
3. Run the installation using one of the following commands:

   - `apt` –Use the following command to install the Citrix Workspace app with dependency:

     ```
     sudo apt install -f ./icaclient_<version>._amd64.deb
     ```

     To install the USB package, run the following command:

     ```
     sudo apt install -f ./ctxusb_<version>._amd64.deb
     ```

   - `dpkg -i` –Use the following command to install the Citrix Workspace app:

     ```
     sudo dpkg -i icaclient_<version>_amd64.deb
     sudo apt-get -f install
     ```

     To install the USB package, run the following command:

     ```
     sudo dpkg -i ctxusb_<version>_amd64.deb
     sudo apt-get -f install
     ```

   - `gdebi` –Use the following command to install the Citrix Workspace app:

     ```
     gdebi icaclient_<version>_amd64.deb
     ```

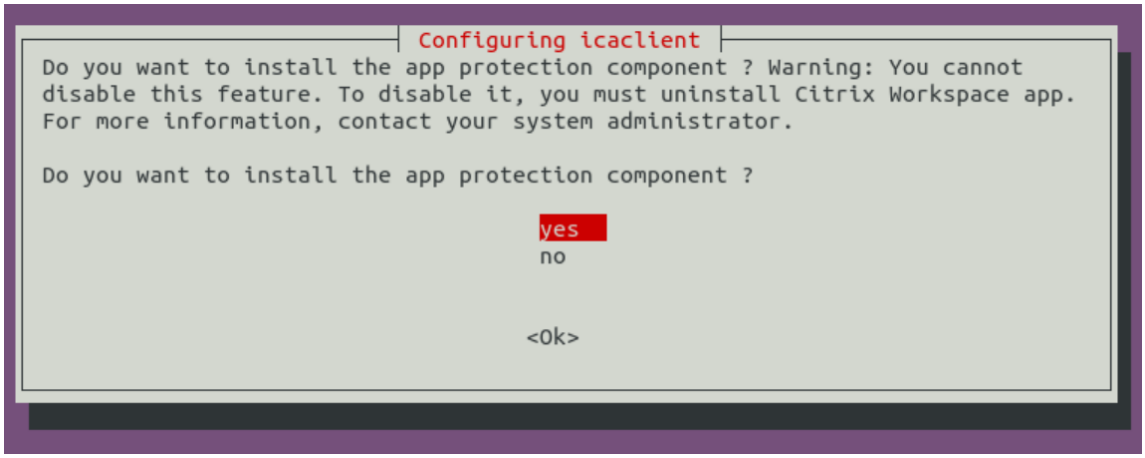
     To install the USB package, run the following command:

     ```
     gdebi ctxusb_<version>_amd64.deb
     ```

   > **Note:**
   >
   > The `ctxusb` package is optional to support the generic USB redirection feature

4. Starting with version 2101, the following interactive prompt appears asking you to install App Protection:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Select **Yes** to continue with the installation with the App Protection component.

   Silent installation of the App Protection component on Debian packages

   Starting with version 2102, App Protection is supported on the Debian version of Citrix Workspace app.

   For silent installation of the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

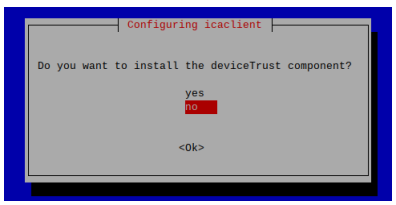
```
export DEBIAN_FRONTEND="noninteractive"
```

```
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
```

```
sudo debconf-show icaclient
```

```
sudo apt install -f ./icaclient_<version>._amd64.deb`
```

6. Starting with version 2503, the following interactive prompt appears asking you to install deviceTRUST®:



   Select **Yes**, and then click **Ok** to proceed with the installation of the deviceTRUST component.

   > **Note:**
   >
   > For more information on deviceTRUST, see Seamless Integration of deviceTRUST.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Red Hat packages

Install the ICAClient package based on your OS architecture.

To use generic USB redirection, install one of the ctxusb packages based on your OS architecture.

> **Note:**
>
> To avoid the compatibility issue, ensure that you install the same version of Icaclient and ctxusb packages.

Package name	Contents
Redhat packages (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-<version>.x86_64.rpm	Self-service support, Red Hat (including Linux VDA) based, 64-bit x86_64
ICAClient-suse-<version>.x86_64.rpm	Self-service support, SUSE based, 64-bit x86_64
ctxusb-<version>.x86_64.rpm	USB package, 64-bit x86_64

> **Note:**
>
> The SuSE 11 SP3 Full Package (Self-Service Support) RPM package is deprecated.

Install using an RPM package

If you're installing Citrix Workspace app from the RPM package on SUSE, use the YaST or Zypper utility. The RPM utility installs the .rpm package. An error occurs if the required dependencies are missing.

> **Tip:**
>
> RPM Package Manager does not install any missing required software.
>
> - For customers using SUSE, download and install the software using zypper install <file name> at a command line on OpenSUSE.
> - For customers using Red Hat, download and install the software using yum localinstall <filename>on Fedora/Red Hat.

To install from the RPM package

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Prerequisites:**
>
> Verify that you've installed all the required system requirements, as mentioned at the System requirements section.

1. Set up the EPEL repository.

   > **Note:**
   >
   > For RHEL and CentOS, install the EPEL repository before you can install the Linux VDA successfully. For information on how to install EPEL, see the instructions.

2. Log on as a privileged (root) user.
3. Open a terminal window.
4. Run the installation for the following three packages by typing Zypper in .

   > **Note:**
   >
   > - `ctxusb` is an optional package. Install the package to support Generic USB Redirection.
   > - `ctxappprotection` is an optional package. Install the package only if you want to install the App Protection component.

   For SUSE installations:

   - `zypper in ICAClient-suse-<version>.x86_64.rpm`
   - `zypper in ctxusb-<version>.x86_64.rpm`
   - `zypper in ctxappprotection-<version>.x86_64.rpm`

   For Red Hat installations:

   - `yum localinstall ICAClient-rhel-<version>.x86_64.rpm`
   - `yum localinstall ctxusb-<version>.x86_64.rpm`
   - `yum localinstall ctxappprotection-<version>.x86_64.rpm`

To install a missing package On a Red Hat based distribution (RHEL, CentOS, Fedora, and so on), add an EPEL repository (details can be found at https://docs.fedoraproject.org/en-US/epel/), if the following error message appears:

```
1 "... requires libwebkitgtk-1.0.so.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tarball packages

Install one of the following packages based on your OS architecture.

Package name	Contents
Tarballs (Script install for any distribution)	
`linuxx64-<version>.tar.gz`	64-bit Intel
`linuxarm64-<version>.tar.gz`	ARM 64

> **Note:**
>
> - If you want to customize the installation location, install Citrix Workspace app from the tarball package. If you want to install any required packages automatically, install Citrix Workspace app from the Debian package or the RPM package.
> - Do not use two different installation methods on the same machine. If you do, you might see error messages and unwanted behavior.

Install using a tarball package

> **Note:**
>
> The tarball package does not do dependency checks or install dependencies. All system dependencies must be resolved separately.

1. Open a terminal window.
2. Extract the contents of the `.tar.gz` file into an empty directory. For example, type: `tar xvfz packagename.tar.gz`.
3. Type `./setupwfc` and then press Enter to run the setup program.
4. Accept the default of 1 (to install Citrix Workspace app) and press **Enter**.
5. Type the path and name of the required installation directory and then press Enter. Or, press Enter to install Citrix Workspace app in the default location.

   The default directory for privileged (root) user installations is `/opt/Citrix/ICAClient`.

   The default directory for non-privileged user installations is `$HOME/ICAClient/platform`. Platform is a system-generated identifier for the installed operating system, for example, `$HOME/ICAClient/linuxx86` for the Linux/x86 platform).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If you specify a non-default location, set it in $ICAROOT in `$HOME/.profile` or `$HOME/.bash\\_profile`.

6. When prompted to continue, type `y` and then press Enter.
7. You can choose whether to integrate Citrix Workspace app into your desktop environment. The installation creates a menu option from which users can start Citrix Workspace app. Type `y` at the prompt to enable the integration.
8. If you have previously installed `GStreamer`, you can choose whether to integrate `GStreamer` with Citrix Workspace app, and support HDX MediaStream Multimedia Acceleration. To integrate Citrix Workspace app with `GStreamer`, type `y` at the prompt.

   > **Note:**
   >
   > On some platforms, installing the client from a tarball package can cause the system to become unresponsive after prompting you to integrate with `KDE` and `GNOME`. This issue occurs with the first-time initialization of gstreamer-0.10. If you encounter this issue, terminate the installation process (using the keys ctrl+c) and run the command `gst-inspect-0.10 -- gst-disable-registry-fork --version`. After running the command, you can rerun the tarball package without experiencing the issue.

9. If you log on as a privileged user (root), choose to install USB support for Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) published VDI applications. Type `y` at the prompt to install USB support.

   > **Note:**
   >
   > If you aren't logged on as a privileged user (root), the following warning appears:
   >
   > "USB support can't be installed by non-root users. Run the installer as root to access this install option."

10. When the installation completes, the main installation menu appears again. To exit setup, type 3 and then press Enter.

Uninstall

The environment variable ICAROOT must be set to the installation directory of the client. The default directory for non-privileged user installations is `$HOME/ICAClient/platform`. The platform variable is a system-generated identifier for the installed operating system, for example, `$HOME/ICAClient/linuxx86` for the Linux/x86 platform. Privileged user installation defaults to `/opt/Citrix/ICAClient`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Notes:**
>
> - To uninstall Citrix Workspace app, you must be logged in as the same user who does the installation.
> - When you uninstall the Citrix Workspace app, out of date cache files at `$HOME/.local/share/webkitgtk` might not be removed automatically. As a workaround, manually remove the cache files.

To uninstall Citrix Workspace app on the tarball package

1. Run the setup by typing `$ICAROOT/setupwfc` and press Enter.
2. To remove the client, type 2 and press **Enter**.

To uninstall Citrix Workspace app on Debian/Ubuntu Operating systems

1. Open a terminal window.
2. Run the installation using one of the following commands:

```
sudo apt remove icaclient -y
```

```
sudo apt autoremove -y
```

OR,

```
sudo apt remove icaclient -y
```

```
sudo apt purge icaclient -y
```

> **Note:**
>
> You can also remove the Debian package using your operating system's standard tools.

To uninstall Citrix Workspace app on Fedora/RHEL/CentOS Operating systems

1. Open a terminal window.
2. Run the installation using the following command:

```
yum remove icaclient -y
```

> **Note:**
>
> You can also remove the RPM package using your operating system's standard tools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify whether the uninstallation of the Citrix Workspace app is successful. For more information see, Verify the version of the Citrix Workspace app section.

Update

Before updating Citrix Workspace app, verify the current version of the Citrix Workspace app installed in your system. For more information see, Verify the version of the Citrix Workspace app section.

To update to a newer version of the Citrix Workspace app, download and install the latest Citrix Workspace app from Citrix Downloads. For the installation procedure, you can follow the steps mentioned at the following installation section:

- Debian packages
- Red Hat packages
- Tarball packages

If you have the Citrix Workspace app installed in your system, the system detects the existing app, and updates to a newer version. However, for Tarball packages, consider a scenario where you've installed the earlier version of the app in one folder and you've installed the newer version of the app in a different folder. In this scenario, both versions of the app might exist in your system.

The **Citrix Workspace** screen overlay appears on the first launch of the app, when you update, and when you uninstall and reinstall the app. Click **Got it** to continue using Citrix Workspace app, or click **Learn more** for more details.

Upgrade App Protection:

When App Protection is installed, upgrade is not supported. For more information, see Upgrade.

Store configuration

October 14, 2025

This article is a reference document to help you get started with Citrix Workspace app for Linux.

Verify the current version of the Citrix Workspace app installed in your system. For more information see, Verify the version of the Citrix Workspace app section.

Store

A **store** aggregates available applications and desktops for a user into a single place. A user can have multiple stores and switch across stores as needed. An admin delivers the store URL that has pre-configured resources and settings. You can access these stores through the Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on the store, see the StoreFront documentation.

Types of stores

You can add the following store types in the Citrix Workspace app:

- Workspace
- StoreFront
- Citrix Gateway Store
- Custom web store

Workspace

Citrix Workspace is a cloud-based enterprise app store that provides secure and unified access to apps, desktops, and content (resources) from anywhere, on any device. These resources can be Citrix DaaS, content apps, local and mobile apps, SaaS and Web apps, and browser apps. For more information, see Citrix Workspace Overview.

StoreFront

StoreFront is an on-premises enterprise app store that aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single easy-to-use store for users.

For more information, see StoreFront documentation.

Citrix Gateway Store

Configure Citrix Gateway to enable users to connect from outside the internal network. For example, users who connect from the Internet or from remote locations.

Custom web stores

Starting with 2203, you can access your organization's custom web store from the Citrix Workspace app.

To use this feature, if Global App Configuration Service is available:

The administrator must add the domain or the custom web store to the list of allowed URLs in the Global App Configuration Service. After you've added the domain or the custom web store, provide the custom web store URL or email address in the **Add Account** screen in the Citrix Workspace app. The custom web store opens in the native Workspace app window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about configuring web store URLs for end-users, see Global App Configuration Service.

> **Note:**
>
> The Pinning multi-monitor screen layout feature isn't supported in the custom web store.

To remove the custom web store, go to **Accounts** > **Add or Remove accounts**, select the custom web store URL, and click **Remove**.

As a prerequisite, you must enable the custom web store in the `AuthManConfig.xml` file. To enable it:

1. Navigate to the `$ICAROOT/config/AuthManConfig.xml` configuration file.
2. Add the following entries:

```
<key>AppConfigEnabled</key>
<value>true</value>
```

To use this feature, if Global App Configuration Service isn't available:

Perform the following configuration changes:

1. Navigate to the `$ICAROOT/config/AuthManConfig.xml` configuration file.
2. Add the following entries:

```
<key>AppConfigEnabled</key>
<value>false</value>
```

3. Add the list of URLs that must be considered for the custom web store in the following way.

```
<AllowedWebStoreCache>
<value><URL1></value>
<value><URL2></value>
..
<value>....</value>
</AllowedWebStoreCache>
```

> **Note:**
>
> You can only use the URLs listed in the `AuthManConfig.xml` file for the custom web store. You can add extra URLs in the`AuthManConfig.xml` file that you want to be considered for the custom web store.

Adding store URL to Citrix Workspace app

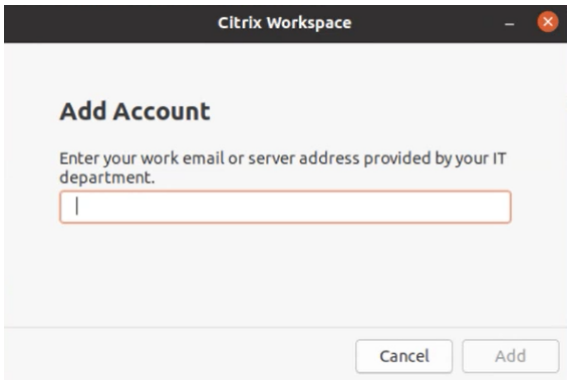
You can provide users with the account information that they need to access virtual desktops and applications using the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Providing users with account information to enter manually
- Configuring email-based auto-discovery
- Adding store through CLI

Provide users with account information to enter manually

After installing the Citrix Workspace app successfully and when you launch the app for the first time, the following screen appears. Users are required to enter an email or server address to access the apps and desktops. 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.



To enable users to set up accounts manually, be sure to distribute the information required to connect to their virtual desktops and applications.

- To connect to a Workspace store, provide the Workspace URL.
- To connect to a StoreFront store, provide the URL for that server. For example:`https://servername.company.com`.
- To connect through Citrix Gateway, provide users with the Citrix Gateway fully qualified domain name.

Email-based auto-discovery of store

You can now provide your email address in Citrix Workspace app to automatically discover the store associated with the email address. If there are multiple stores associated with a domain, by default the first store returned by the Global App Configuration Service is added as the store of choice. Users can always switch to another store if necessary.

To disable this feature, do the following:

1. Navigate to `$ICAROOT/config/AuthManConfig.xml` file.
2. Set the following entry to false.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<key>AppConfigEnabled</key>
<value>false</value>
```

Adding store through CLI

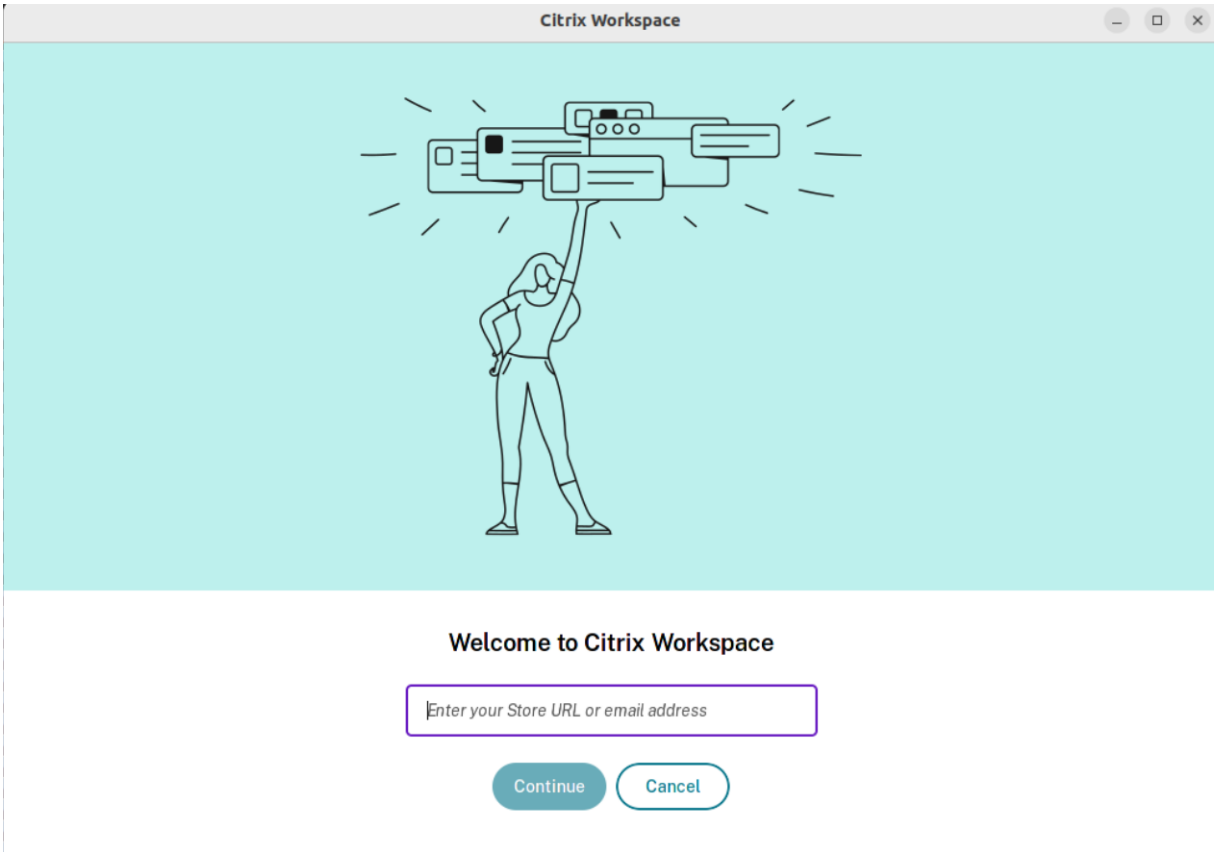
Install Citrix Workspace app for Linux as an administrator using the command-line interface.

For more information, see the `Storebrowse` section.

Enhanced the user interface for seamless login experience

Starting with the 2405 release, Citrix Workspace™ app for Linux's user interface has been enhanced to be more modern and provides seamless login experience for first time users.

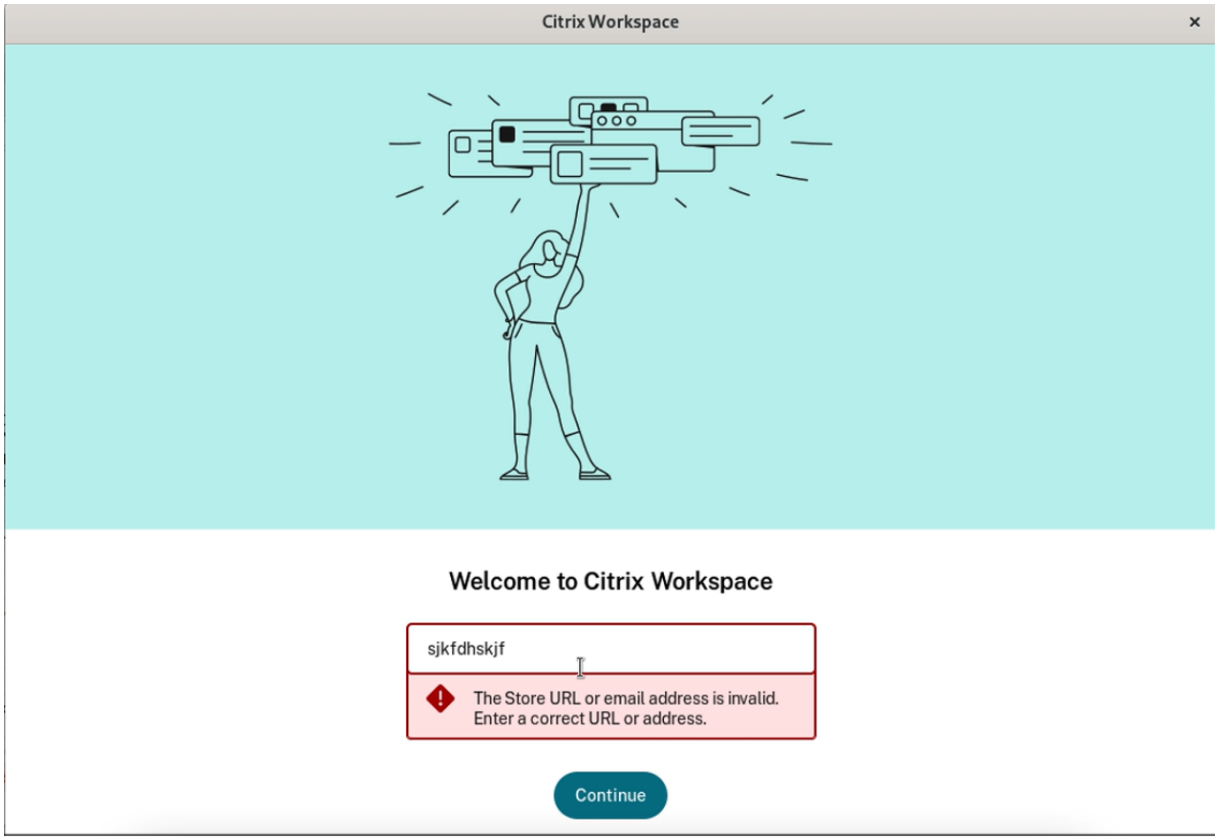
Previously, Citrix Workspace app for Linux were using two different GTK windows for store addition and enumeration of the resources. With this release, Citrix Workspace app displays the Welcome page with the option to add the store.



This feature also includes the following enhancements to the UI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After completing the installation, the option to login now or skip login for later is displayed.
If the user enters invalid store url, invalid or incomplete e-mail id, or invalid IP adress, an intuitive error message is displayed based on the input.



This feature is disabled by default.

To enable this feature, do the following:

1. Navigate to /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
2. Add the following entry:

```
<key>AccountConfigEnabled</key>

 <value>true</value>
```

Set up

You can download the installation package, customize the configuration, and then install the Citrix Workspace app.

You can modify the contents of the Citrix Workspace app package and then repackage the files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customize installation

1. Expand the Citrix Workspace app package file into an empty directory. The package file is called platform.major.minor.release.build.tar.gz (for example, `linuxx86-<version>.tar.gz` for the Linux/x86 platform).
2. Make the required changes to the Citrix Workspace app package. For example, you can add a TLS root certificate to use a certificate from the Certificate Authority that is not a part of the standard Citrix Workspace app installation.
3. Open the `PkgID` file.
4. Add the following line to indicate that the package was modified:

   MODIFIED=traceinfo

   where, `traceinfo` is information indicating who made the change and when.
5. Save and close the file.
6. Open the package file list, platform/platform.psf (for example, linuxx86/linuxx86.psf for the Linux/x86 platform).
7. Update the package file list to reflect the changes you made to the package. Not updating might cause an error when installing the new package. Changes can include updating the size of any files you modified, or adding new lines for any files you added to the package. The columns in the package file list are:

   - File type
   - Relative path
   - Subpackage (always set to `cor`)
   - Permissions
   - Owner
   - Group
   - Size
8. Save and close the file.
9. Use the tar command to rebuild the Citrix Workspace app package file. For example, `tar czf ../newpackage.tar.gz *`, where `newpackagez` is the name of the new Citrix Workspace app package file.

Latest `webkit` support

Citrix Workspace app for Linux requires libwebkit2gtk (2.16.6+).

libwebkit2gtk has the following advantages:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Improved UI experience. webkit2gtk is compatible with the browser content redirection feature. Use webkit2gtk Version 2.24 or later for an even better YouTube viewing experience.
- webkit2gtk Version 2.16.6 and later improves the sign-in experience and the time that it takes to sign in.
- The app works better with newer Linux distributions and provides with the latest `webkit` security fixes.

> **Note:**
>
> webkit2gtk isn't available on some Linux distributions. As a workaround, consider the following options:
>
> - Build webkit2gtk from the source before installing Citrix Workspace app 1906.
> - Move to a later Linux distribution that supports webkit2gtk 2.16.6 or later.

Launch

You can start Citrix Workspace app either at a terminal prompt or from one of the supported desktop environments.

Ensure that the environment variable `ICAROOT` is set to point to the actual installation directory.

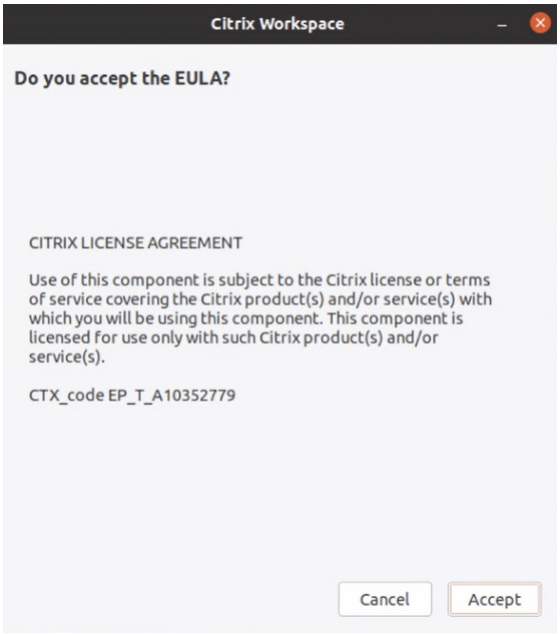
> **Tip:**
>
> The following instruction does not apply to installations made from the Web packages, and where the tarball is used. This instruction is applicable when the requirements for self-service haven't been met.

Terminal prompt

To start the Citrix Workspace app at the terminal prompt:

1. Type `/opt/Citrix/ICAClient/selfservice`
2. Press Enter (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Workspace app).
   The **Do you accept the EULA?** dialog box appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Accept** to continue with adding the store.

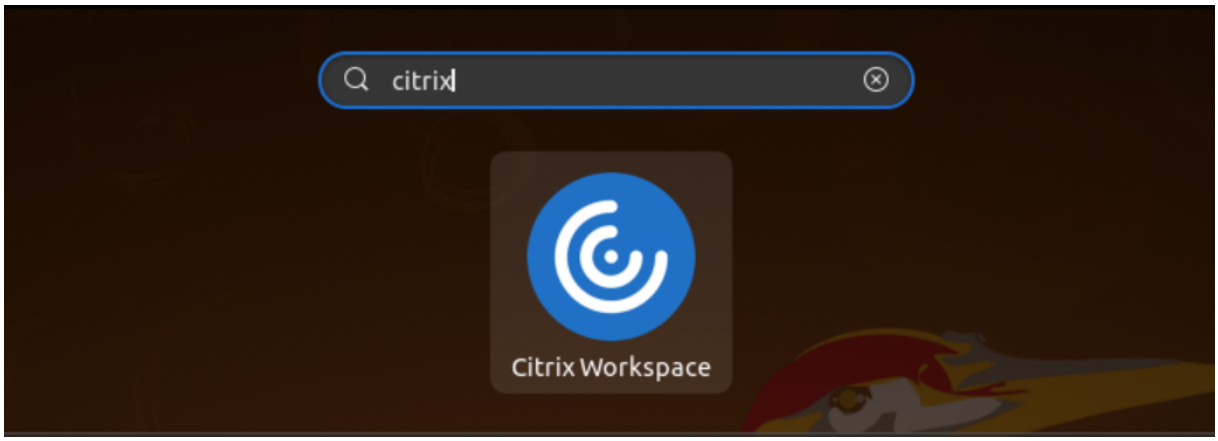
> **Note:**
>
> The **Do you accept the EULA?** dialog box appears only if you access the Citrix Workspace app for Linux first time after the installation.

Linux desktop

You can start the Citrix Workspace app from a desktop environment using a file manager.

On some desktops, you can also start Citrix Workspace app from a menu. Citrix Workspace app is available in different menus depending on your Linux distribution.

On Ubuntu, the Citrix Workspace app icon appears as follows:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Preferences

To set preferences, click **Preferences** from the Citrix Workspace app menu. You can control the following:

- How desktops are displayed
- Connect to different applications and desktops
- Manage file and device access

Manage an account

To access desktops and applications, you need an account with Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Your IT help desk might ask you to add an account to Citrix Workspace for this purpose. Or they might ask you to use a different Citrix Gateway or Access Gateway server for an existing account. You can also remove accounts from Citrix Workspace.

1. On the **Accounts** page of the **Preferences** dialog, do one of the following:
    - To add an account, click **Add**. Contact your system administrator for more information.
    - To change details of a store that the account uses, such as the default gateway, click **Edit**.
    - To remove an account, click **Remove**.
2. Follow the on-screen prompts. When prompted, authenticate to the server.

Desktop display

You can display desktops across the entire screen on your user device (full screen mode), which is the default, or in a separate window (windowed mode).

- On the **General** page of the **Preferences** dialog box, select a mode using the **Display desktop in** option.

Use the **You can enable Desktop Viewer** toolbar functionality to dynamically modify the window configuration of your remote session.

Desktop Viewer

Your requirements for the way users access virtual desktops can vary from user to user and might vary as your corporate needs evolve.

Use the Desktop Viewer when users interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop Viewer toolbar functionality allows the user to switch a session between windowed and full-screen session window, including multi-monitor support for the intersected monitors. Users can switch between desktop sessions and use more than one desktop using multiple Citrix Virtual Apps and Desktops™ or Citrix DaaS connections on the same user device. Buttons to minimize all desktop sessions, send the Ctrl+Alt+Del sequence, disconnect, and log off from the session are provided to manage a user's session conveniently.

Pressing **Ctrl+Alt+Break** displays the **Desktop Viewer** toolbar buttons in a pop-up window.

Enhanced Desktop Viewer toolbar Starting with the 2408 version, Citrix Workspace app for Linux provides an enhanced Desktop Viewer toolbar.



The enhanced Desktop Viewer toolbar provides the following options:

- Show or hide toolbar - Click this button to show or hide the Desktop Viewer toolbar
- Switch desktop - Click this button to see the available open desktops. You can switch to another desktop by clicking the desktop that you want to access. The opened desktop shows in the front.
- Ctrl+Alt+Del - Click this button to access the shortcuts. The available shortcut is Ctrl+Alt+Del.
- Devices - Click this button to access the options in the **Devices** section.
- Preferences - Click this button to access the options in the **Preferences** section.
- Minimize - Click this button to minimize the virtual session.
- Fullscreen or Restore - Click the "Fullscreen"button to expand the desktop session to full screen. Click the "Restore"button to restore the full screen session to the previous window mode.
- Disconnect / Sign out - Click this button to sign out or to disconnect from a virtual session.

You can float or rotate the toolbar as per your preference across the screen. By default, the new toolbar is available.

Customize toolbar Previously, you could completely disable the **Desktop Viewer** toolbar. However, you couldn't enable or disable a few options on the toolbar. Starting with the 2408 release, you can customize the Citrix Workspace app toolbar by adding and removing options on the toolbar.

To hide Devices option on the toolbar, do the following:

1. Navigate to the $HOME/.ICAClient/wfclient.ini file.
2. Go to the [WFClient] section and add the following entry as required to hide the options on the toolbar:

```
1    DevicesButtonVisible=False
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accessibility support for enhanced Desktop Viewer toolbar Starting with the 2408 version, you can access the enhanced Desktop Viewer toolbar using the keyboard of your endpoint devices. With this feature, you can invoke the toolbar, navigate through the options, and select the required options using the keyboard shortcuts.

Use the following keyboard shortcuts to access the toolbar:

- `Ctrl + Shift + t`: Show the toolbar and move focus to the first button.
- `Tab`: Navigate the options in the forward direction.
- `Space`: Select a menu.
- `Up` and `Down` arrow keys: Navigate across submenus.
- `Enter`: Select a submenu.
- `Esc`: When focus on sub-menu, quit the submenu. When focusing on the toolbar, remove the focus and quit the keyboard shortcut mode.

Modify or disable a keyboard shortcut combinations You can modify or disable a shortcut key combination as per your preference.

To modify a shortcut key combination:

For example, if you want to modify the shortcut `Ctrl + Shift + t`, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
2. Go to the `[WFClient]` section and add the following entry:

```
WCAGModeKeyCombination="Ctrl+Shift+W"
```

> **Note:**
>
> Make sure the new shortcut key doesn't conflict with other shortcuts.

To disable a shortcut key combination:

For example, if you want to disable the shortcut `Ctrl + Shift + t`, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
2. Go to the `[WFClient]` section and add the following entry with empty key:

```
WCAGModeKeyCombination=
```

Automatic session reconnects

Citrix Workspace app can reconnect to desktops and applications that are disconnected. For example, a network infrastructure issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the **General** page of the **Preferences** dialog box, select an option in **Reconnect apps and desktops.**

Access local files

A virtual desktop or application needs access to files on your device. You can control the extent to which this access happens.

1. On the **File Access** page of the **Preferences** dialog box, select a mapped drive and then one of the following options:
   - **Read and write** - Allow the desktop or application to read and write to local files.
   - **Read only** - Allow the desktop or application to read but not write to local files.
   - **No access** - Do not allow the desktop or application to access local files.
   - **Ask me each time** - Display a prompt each time the desktop or application access local files.
2. Click **Add**, specify the location, and select a drive to map to it.

Microphone and Webcam

To set up a microphone or a webcam, you can change the way a virtual desktop or application accesses your local microphone or webcam:

On the **Mic & Webcam** page of the **Preferences** dialog box, select one of the following options:

- **Use my microphone and webcam** - Allow the microphone and webcam to be used by the desktop or application.
- **Don't use my microphone or webcam** - Do not allow the microphone or webcam to be used by the desktop or application.

Connect

Citrix Workspace app provides users with secure, self-service access to virtual desktops and applications, and on-demand access to Windows, web, and Software as a Service (SaaS) applications. Citrix StoreFront or legacy webpages created with Web Interface manage the user access.

To connect to resources using the Citrix Workspace UI

The Citrix Workspace app home page displays virtual desktops and applications that are available to the users based on their account settings (that is, the server they connect to) and settings configured

© 1997–2026 Citrix Systems, Inc. All rights reserved.

by Citrix Virtual Apps and Desktops or Citrix DaaS administrators. Using the **Preferences** > **Accounts** page, you can configure the URL of a StoreFront server or, if email-based account discovery is configured, by entering the email address.

> **Tip:**
>
> If you use the same name for multiple stores on the StoreFront server, you avoid duplications by adding numbers. The names for such stores depend on the order in which they're added. For Citrix Workspace app, the store URL is displayed and uniquely identifies the store.

After connecting to a store, the self-service shows the tabs: **FAVORITES**, **DESKTOPS**, and **APPS**. To launch a session, click the appropriate icon. To add an icon to **FAVORITES**, click the **Details** link next to the icon and select A**dd To Favorites**.

Configure connection settings

You can configure some default settings for connections between Citrix Workspace app and Citrix Virtual Apps and Desktops or Citrix DaaS servers. You can also change these settings for individual connections, if necessary.

Although the tasks and responsibilities of administrators and users can overlap, the term "user"is used to distinguish user tasks from those tasks that an administrator performs.

Connect to resources from a command line or browser

You create connections to servers when you click a desktop or application icon on the Citrix Workspace app home page. Also, you can open connections from a command line or from a web browser.

To create a connection to a Program Neighborhood or StoreFront server using a command line Prerequisite:

Ensure that the store is known to Citrix Workspace app. If necessary, add it using the following command:

```
```
./util/storebrowse --addstore \<store URL\>
```
```

1. Get the unique ID of the desktop or application that you want to connect to. This ID is the first quoted string on a line acquired in one of the following commands:

   - List all desktops and applications on the server:

     ```
     ./util/storebrowse -E <store URL>
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- List the desktops and applications that you've subscribed to:

```
./util/storebrowse -S <store URL>
```

2. Run the following command to start the desktop or application:

```
./util/storebrowse -L <desktop or application ID> <store URL>
```

If you can't connect to a server, you might need to check your administrator for issues like server location or SOCKS proxy. For more information, see
proxy server.

To create a connection from a web browser Configuration for starting sessions from a web browser is typically carried out automatically during installation. Because of the wide variety of browsers and operating systems, some manual configuration can be required.

If you set up `.mailcap` and `MIME` files for Firefox, Mozilla, or Chrome manually, use the following file modifications. Using these modifications, the `.ICA` files start up the Citrix Workspace app executable, `wfica`. To use other browsers, modify the browser configuration accordingly.

1. Run the following commands for non-administrator installation of Citrix Workspace app. The settings of ICAROOT might be changed if they're installed to a non-default location. You can test the result with the command

   `xdg-mime query default application/x-ica`, which must return "wfica.desktop."

   ```
   export ICAROOT=/opt/Citrix/ICAClient
   ```

   ```
   xdg-icon-resource install --size 64 $ICAROOT/icons/000_Receiver_64.png Citrix Workspace app
   ```

   ```
   xdg-mime default wfica.desktop application/x-ica
   ```

   ```
   xdg-mime default new_store.desktop application/vnd.citrix.receiver.configure
   ```

2. Create or extend the file /etc/xdg/mimeapps.list (for administrator installation) or `$HOME/.local/share/applications/mimeapps.list` (`mimeapps.list`). The file must start with [Default Applications], and follow by:

   ```
   application/x-ica=wfica.desktop;
   ```

   ```
   application/vnd.citrix.receiver.configure=new_store.desktop;
   ```

   You might require to configure Firefox on its Preferences/Applications setting page.

   For "Citrix ICA® settings file content,"select:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “Citrix Workspace app Engine (default)”in the drop-down menu

  or

- “Use other …”and then select the file /usr/share/applications/wfica.desktop (for an administrator installation of Citrix Workspace app)

  or

- $HOME/.local/share/applications/wfica.desktop (for a non-administrator installation).

Connection Center

Users can manage their active connections using the Connection Center. This feature is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. With Connection Center, users can manage connections by:

- Closing an application.
- Logging off a session. This step ends the session and closes any open applications.
- Disconnecting from a session. This step cuts the selected connection to the server without closing any open applications (unless the server is configured to close applications on disconnection).
- Viewing connection transport statistics.

Manage a connection To manage a connection using the **Connection Center**:

1. On the Citrix Workspace app menu, click **Connection Center**.

   The servers that are used appear and active sessions are listed.

2. Do one of the following:

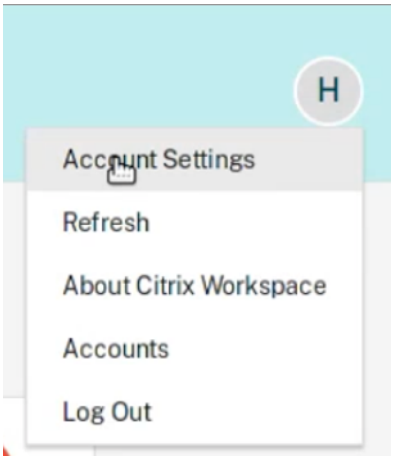
   - Select a server, disconnect or log off, or view its properties.
   - Select an application, close the window.

User Interface enhancement

Previously, the settings menu was available from the **Preferences** option in the Desktop Viewer.

Starting with version 2106, the settings menu appears in line with the Self-Service plug-in. The menu options are now improved to align with the look and feel of the native Citrix Workspace. This enhancement results in a seamless and a better user experience.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> This enhancement is available by default in Citrix Workspace app Version 2106 in cloud deployments.

To switch to the native and old style appearance, do the following:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and set the value of `WebUISettings` to **False**.

Addition of DisableClientAppManagement flag

Citrix Workspace app for Linux introduces a new configuration flag called DisableClientAppManagement. This flag allows for improved control over client app behavior.

The DisableClientAppManagement flag disables various Client App Management operations, including:

- GACS discovery calls
- Settings synchronization or retrieval related to client apps

By default, the DisableClientAppManagement flag is set to false, meaning that Client App Management operations are enabled. When set to true, the flag skips all related operations during runtime, creating a lighter or more restricted environment as needed.

This enhancement offers a configurable option to adapt the Citrix Workspace app's behavior based on specific deployment needs or system constraints.

App experience

January 22, 2024

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This section describes the following:

- App preferences
- Data collection and monitoring

App preferences

September 13, 2025

Settings

Configuration files

To change advanced or less common settings, you can modify Citrix Workspace app's configuration files. These configuration files are read each time `wfica` starts. You can update various files depending on the effect you want the changes to have.

If session sharing is enabled, an existing session might be used instead of a newly reconfigured one. This setting might cause the session to ignore changes you made in a configuration file.

Default settings

If you want to change the default for all Citrix Workspace app users, modify the `module.ini` configuration file in the `$ICAROOT/config` directory.

> **Note:**
>
> If an entry in `All\\_Regions.ini` is set to a specific value, the value for that entry in `module.ini` isn't used. The values in `All\\_Regions.ini` take precedence over the value in `module.ini`.

Template file

If the `$HOME/.ICAClient/wfclient.ini` file does not exist, `wfica` creates it by copying `$ICAROOT/config/wfclient.template`. When you change this template file, the changes are applied to all the Citrix Workspace app users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User settings

To apply configuration changes for a user, modify the `wfclient.ini` file in the user's `$HOME/.ICAClient` directory. The settings in this file apply to future connections for that user.

Validate configuration file entries

To limit the values for entries in `wfclient.ini`, specify the allowed options or ranges of options in `All\\_Regions.ini`.

If you specify only one value, that value is used. The `$HOME/.ICAClient/All\\_Regions.ini` file can match or reduce the possible values set in the `$ICAROOT/config/All\\_Regions.ini` file, it can't take away restrictions.

> **Note:**
>
> The value set in `wfclient.ini` takes precedence over the value in `module.ini`.

Parameters

The parameters listed in each file are grouped into sections. Each section begins with a name in brackets that indicates parameters that belong together; for example, `\[ClientDrive\]` for parameters related to client drive mapping (CDM).

Defaults are automatically supplied for any missing parameters except where indicated. If a parameter is present but not assigned a value then the default value is automatically applied. For example, consider the `InitialProgram` parameter is followed by an equal sign (=) and no value is provided. In this example, the default value (not to run a program after logging in) is applied.

Precedence

The `All\\_Regions.ini` file specifies parameters that the other files can set. It can restrict the values of parameters or set them exactly.

For any given connection, the files are checked in the following order:

1. `All\\_Regions.ini` - The values in this file override those values in:
    - The connections `.ICA` file
    - `wfclient.ini`
2. `module.ini` - The values in this file are used if they have not been set in `All\\_Regions.ini`, the connections `.ICA` file, or `wfclient.ini`. However, these values aren't restricted with the entries in `All\\_Regions.ini`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If no value is found in any of these files, the default in the Citrix Workspace app code is used.

> **Note:**
>
> There are exceptions to this order of precedence. For example, the code reads some values specifically from `wfclient.ini` for security reasons.

Creating custom user-agent strings in network request

Starting with the 2109 version, Citrix Workspace app introduces an option to append the User-Agent strings in the network request and identify the source of a network request. Based on this User-Agent strings request, you can decide how to manage your network request. This feature allows you to accept network requests only from trusted devices.

> **Note:**
>
> - This feature is supported on cloud deployments of Citrix Workspace app. Also, x86, x64, and ARMHF are the supported packages.

To customize the User-Agent strings, do the followings:

1. Locate the `$ICAROOT/config/AuthManConfig.xml` configuration file.
2. Add a value to the following entry:

```
<UserAgentSuffix> </UserAgentSuffix>
```

Example that includes App and Version in the customized text:

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

If you're adding App and AppVersion, separate them by a forward slash ("/").

- If the network request is from the UI-based Citrix Workspace app, the following User-Agent appears in the network requests:

  ```
  CWAWEBVIEW/CWAVersion App/AppVersion
  ```

- If the network request isn't from the UI-based Citrix Workspace app, the following User-Agent appears in the network requests:

  ```
  CWA/CWAVersion App/AppVersion
  ```

> **Notes:**
>
> - If you aren't adding AppVersion at the end of the UserAgentSuffix string, the Citrix Workspace app version is appended in the network requests.
> - Restart `AuthManagerDaemon` and `ServiceRecord` for the changes to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Folder

Configure special folder redirection

In this context, there are only two special folders for each user:

- The user's Desktop folder
- The user's Documents folder (My Documents on Windows XP)

Special folder redirection enables you to specify the locations of a user's special folders. As a result, these folders remain fixed across different server types and server farm configurations. It is important if, for example, a mobile user logs on to servers in different server farms. For static, desk-based workstations, where the user can log on to servers that reside in a single-server farm, special folder redirection is rarely necessary.

To configure special folder redirection:

Enable special folder redirection by making an entry in the module.ini file and specify the folder locations as follows:

1. Navigate to the `$ICAROOT/config/module.ini` file.
2. Go to the [ClientDrive] section and add the following entry:

   ```
   SFRAllowed=True
   ```

3. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
4. Go to the [WFClient] section and add the following entry:

   ```
   DocumentsFolder=documents
   DesktopFolder=desktop
   ```

   where documents and desktop are the UNIX file names, including the full path, of the directories to use as the users Documents and Desktop folders respectively. For example:

   DesktopFolder = $HOME/.ICAClient/desktop

   - You can specify any component in the path as an environment variable, for example, $HOME.
   - Specify values for both parameters.
   - The directories you specify must be available through client device mapping. That is, the directory must be in the subtree of a mapped client device.
   - Use the drive letters C or higher.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data collection and monitoring

September 7, 2025

Customer Experience Improvement Program (CEIP)

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

Additional information

Citrix handles your data following the terms of your contract with Citrix. Also, protects it as specified in the Citrix Services Security Exhibit available on the Citrix Trust Center.

Citrix also uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. You might review how Google handles data collected for Google Analytics.

Clear sending CEIP data to Citrix® and Google Analytics. For this activity, there is an exception for the data collected for Google Analytics indicated by * in the second table in the following section. You can do the following to clear sending CEIP data to Citrix and Google Analytics:

1. Navigate to the <ICAROOT>/config/module.ini folder and go to the CEIP section.
2. Select the entry EnableCeip and set it to Disable.
3. Restart all Citrix service components by running the following commands for the changes to take effect:

```
storebrowse -K
killall -9 UtilDaemon
```

> **Note:**
>
> After you set the EnableCeip key to Disable, you can disable sending the final two CEIP data elements collected by Google Analytics. These data elements are Operating System version and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Workspace app version. For this action, navigate to the following section and set the value as suggested:

Location: <ICAROOT>/config/module.ini

Section: GoogleAnalytics

Entry: DisableHeartBeat

Value: True

> **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 are:

Operating system version*	Workspace app version*	App name	Workspace app language
Session launch method	Compiler version	Hardware platform	Store configuration
Citrix Virtual Apps and Desktops™ Session Launch Status	Authentication configuration	Connection protocol	Browser Content Redirection feature usage
Connection Lease Details	App Protection configuration		

Support for NetScaler® App Experience (NSAP) virtual channel

Previously available as an experimental feature, the NSAP virtual channel feature is fully supported starting with version 2006. All HDX Insight data is sourced from the NSAP virtual channel exclusively and sent uncompressed. This approach improves the scalability and the performance of sessions. The NSAP virtual channel is enabled by default. To disable it, toggle the VDNSAP flag NSAP=Off in the module.ini file.

For more information, see HDX Insight in the Linux Virtual Delivery Agent documentation, and HDX Insight in the Citrix Application Delivery Management service documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for Citrix Analytics

Starting with the version 2006, Citrix Workspace app is updated to transmit data to the Citrix Analytics Service from ICA sessions that you launch from a browser.

For more information on how Citrix Analytics uses this information, see Self-Service Search for Performance and Self-service search for Virtual Apps and Desktops.

Citrix Workspace app for Linux is instrumented to securely transmit logs to Citrix Analytics when the app triggers certain events. The logs are analyzed and stored on Citrix Analytics servers when enabled. For more information about Citrix Analytics, see Citrix Analytics.

Security and authentication

January 22, 2024

This section describes the following:

- Security
- Secure communications
- Authentication

Security

September 7, 2025

App Protection

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

App Protection is an add-on feature that provides enhanced security when you use Citrix Virtual Apps and Desktops. The feature restricts the ability of clients to be compromised with keylogging and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

screen-capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information that are displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

> **Notes:**
>
> - This feature is supported when Citrix Workspace app is installed by using the tarball, Debian, and Red Hat Package Manager (RPM) packages. Also, x64 and ARM64 are the only supported architectures.
> - This feature is supported in on-premises deployments of Citrix Virtual Apps and Desktops. Also, in deployments using the Citrix Virtual Apps and Desktops Service with StoreFront.

App Protection requires that you install an add-on license on your License Server. A Citrix Virtual Desktops license must also be present. For information on Licensing, see the **Configure** section in the Citrix Virtual Apps and Desktops.

Starting with version 2108, the App Protection feature is now fully functional. The App Protection feature supports apps and desktop sessions and is enabled by default. However, you must configure the App Protection feature in the `AuthManConfig.xml` file to enable it for the authentication manager and the Self-Service plug-in interfaces.

Starting with this version, you can launch protected resources from Citrix Workspace app while Mozilla Firefox is running.

Prerequisite:

App Protection works best with the following operating systems along with the Gnome Display Manager:

- 64-bit Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- 64-bit Debian 9, Debian 10 and Debian 11
- 64-bit CentOS 7
- 64-bit RHEL 7
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

Installing the App Protection component:

When you install the Citrix Workspace app using the tarball package, the following message appears.

"Do you want to install the App Protection component? Warning: You can't disable this feature. To disable it, you must uninstall Citrix Workspace app. For more information, contact your system administrator. [default $INSTALLER_N]:"

Enter **Y** to install the App Protection component.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the App Protection component isn't installed.

Restart your machine for the changes to take effect. App Protection work as expected only after you restart your machine.

Installing the App Protection component on RPM packages:

Starting with Version 2104, App Protection is supported on the RPM version of Citrix Workspace app.

To install App Protection, do the following:

1. Install Citrix Workspace app.
2. Install the App Protection `ctxappprotection<version>.rpm` package from the Citrix Workspace app installer.
3. Restart the system for the changes to take effect.

Installing the App Protection component on Debian packages:

Starting with Version 2101, App Protection is supported on the Debian version of Citrix Workspace app.

For silent installation of the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
    install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
```

Starting with Version 2106, Citrix Workspace app introduces an option to configure the anti-keylogging and anti-screen-capturing functionalities separately for both the authentication manager and Self-Service plug-in interfaces.

Configuring App Protection for authentication manager:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    authmananti -A 1
     <key>AuthManAntiScreenCaptureEnabled</key>
     <value>true</value>
     <key>AuthManAntiKeyLoggingEnabled</key>
     <value>true</value>
```

Configuring App Protection for the Self-Service plug-in interface:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
   protection -A 4
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>
```

Known issues:

- When you minimize a protected screen, App Protection continues to run in the background.

Limitation:

- Sometimes, you can't launch protected resources when an application that is installed from the Snap Store is running. As a workaround, identify the application that causes the issue from the Citrix Workspace app log file. Also, close the application. For more information, see Configure allow list for the apps using LD_Preload functionalities
- When you're trying to take a screenshot of a protected window, the entire screen, including the non-protected apps in the background, are grayed out.

App Protection support for eLux® 7

Starting with this release, Citrix Workspace app for Linux supports App Protection on eLux 7. This integration provides enhanced security by helping protect against keylogging and screen capture threats when accessing virtual apps and desktops from eLux 7 devices. With App Protection enabled, organizations can better safeguard sensitive information and ensure compliance with security policies, even on thin client endpoints running eLux 7. For more information about App Protection, see the App Protection documentation.

Inactivity Timeout for Citrix Workspace app

The inactivity timeout feature signs you out of the Citrix Workspace app based on a value that the admin sets. From the 2303 version and later,admins can specify the amount of idle time that is allowed before a user is automatically signed out of the Citrix Workspace app. You're automatically signed out when no activity from the mouse, keyboard, or touch occurs for the specified interval of time, within the Citrix Workspace app window. The inactivity timeout does not affect the already running Citrix Virtual Apps and Desktops and Citrix DaaS sessions or the StoreFront stores.

> **Note:**
>
> This feature is applicable only on cloud deployments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
<key>ITOEnabled</key>
<value>true</value>
```

Admins can configure the timeout in Workspace Configuration. For more infomation, see Set inactivity timeout for Web and Workspace app desktop and mobile.

The end-user experience is as follows:

- A notification appears three minutes before you're signed out, with an option to stay signed in, or sign out.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click **Sign out** to end the session for the current store.

> **Note:**
>
> The inactivity timeout feature doesn't support distributions that have Wayland as the default graphics protocol. For distributions that have Wayland, uncomment either of the following: `WaylandEnable=false` in `/etc/gdm/custom.conf` or in `/etc/gdm3/custom.conf`.

Persistent login

From the Citrix Workspace app 2303 version and later, the persistent login feature enables you to stay logged in for up to the duration (2–365 days) configured by your admin. When this feature is enabled, you need not provide login credentials for the Citrix Workspace app during the configuration period.

With this functionality, the SSO to Citrix DaaS sessions is extended up to a period of 365 days. This extension is based on the lifetime of Long-Lived Tokens. Your credentials are cached by default for 4 days or Lifetime whichever is lower. And then extended when you become active within these 4 days by connecting to the Citrix Workspace app.

Configure the persistent login feature

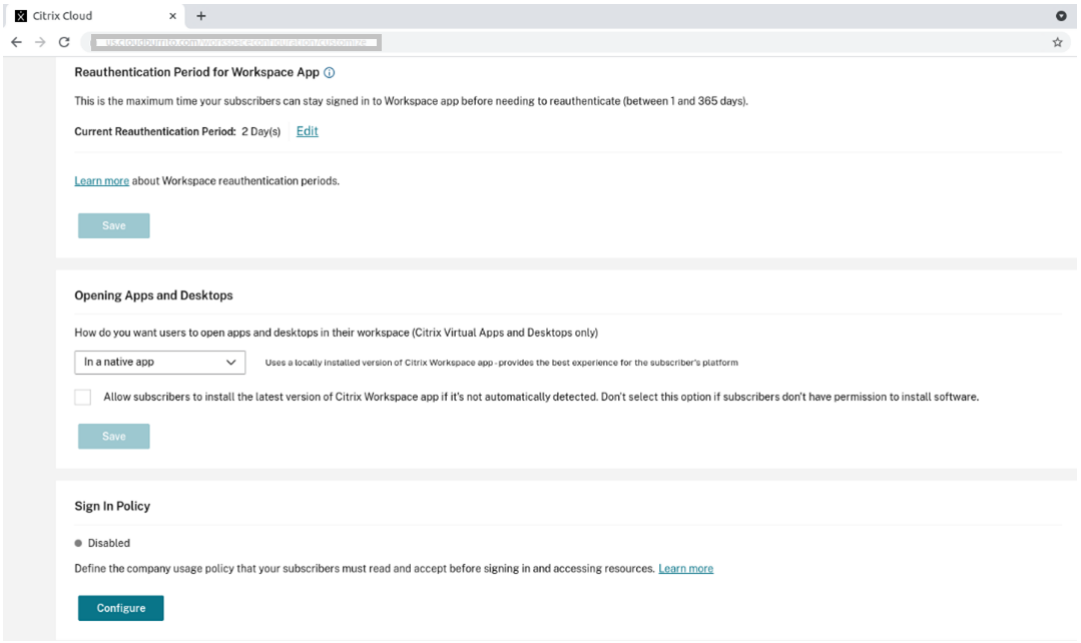
An admin needs to configure the persistent login on the Workspace environment using the following procedure:

1. Sign in to Citrix Cloud.
2. In the Citrix Cloud console, click the menu in the upper left corner of the screen.
3. Select the **Workspace Configuration** option > **Customize** > **Preferences**.
4. Scroll down to **Reauthentication Period for Workspace App**.
5. Click **Edit** next to the **Current Reauthentication Period** field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Enter the required days in the **Current Reauthentication Period** field.
7. You must enter two days or more in the **Current Reauthentication Period** field.

For more information, see the instructions in the **Reauthentication Period for Workspace App section** in the following image:

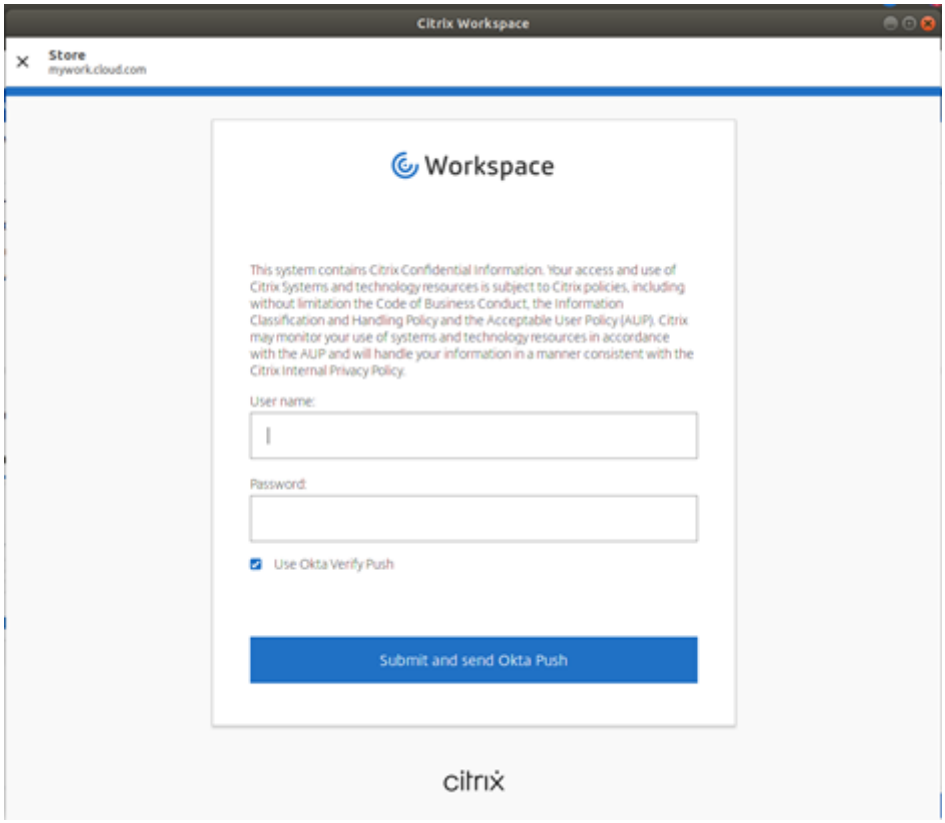


Experience with enhanced authentication

The persistent login window is embedded within the self-service window.

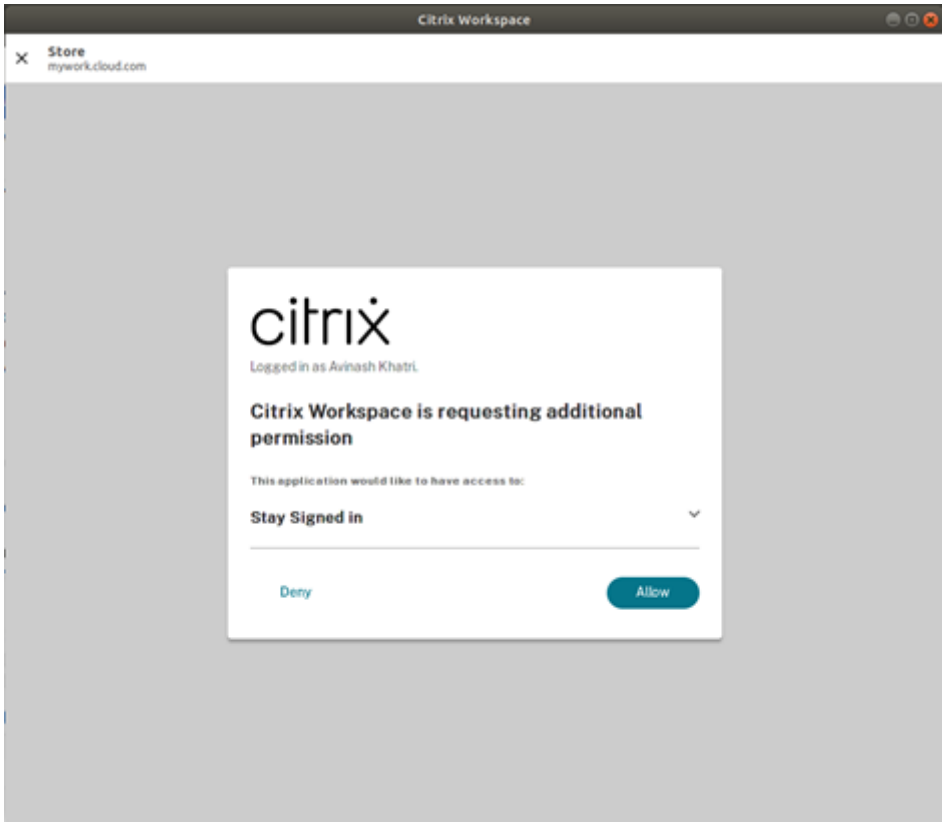
1. Access the Citrix Workspace app.
   The authentication window appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Sign in with your credentials.
   You are redirected to the Permission prompt to accept.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Allow**.

> **Note:**
>
> If you select **Deny** for consent, you would see a second login prompt and you need to sign in to Citrix Workspace app for every 24 hours.

Disable the persistent login feature

An admin can disable the persistent login feature in the Citrix Cloud UI or in the `AuthManConfig.xml` file. However, the value set in the `AuthManConfig.xml` file overrides the value set in the Citrix Cloud UI.

Using Citrix Cloud UI

1. Sign in to Citrix Cloud.
2. In the Citrix Cloud console, click the menu in the upper left corner of the screen.
3. Select the **Workspace Configuration** option > **Customize** > **Preferences**.
4. Scroll down to **Reauthentication Period for Workspace App**.
5. Click **Edit** next to the **Current Reauthentication Period** field.
6. Enter one day in the **Current Reauthentication Period** field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the AuthManConfig.xml file To disable the persistent login feature, do the following

1. Navigate to <ICAROOT>/config/AuthManConfig.xml file.
2. Set the values as follows:

```
<AuthManLite>
    <primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>
    <secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>
    <longLivedTokenSupport>true</longLivedTokenSupport>
    <nativeLoggingEnabled>true</nativeLoggingEnabled>
    <platform>linux</platform>
    <saveTokens>true</saveTokens>
    <compressedGroupsEnabled>true</compressedGroupsEnabled>
</AuthManLite>
```

Seamless Integration of deviceTRUST®

Starting with version 2503, deviceTRUST is included with Citrix Workspace app for unified deployment, ensuring seamless integration and management.

> **Note:**
>
> This feature is currently supported only on the Ubuntu operating system. Verify the Ubuntu versions as given in Supported Linux distributions.

The following are the behavior and specifications of the deviceTRUST integration:

- By default, Citrix Workspace app for Linux installs deviceTRUST using the packaged version included in the installer.
- The failure of deviceTRUST installation doesn't impact the installation of Citrix Workspace app.
- If you already have deviceTRUST Client Extension version 23.1 or earlier installed, it doesn't get updated or removed automatically. However, deviceTRUST Agent version 23.1 or earlier continue to work with the existing installation.

For more information on installing deviceTRUST component on Debian packages, see Install using a Debian package.

Secure communications

September 7, 2025

To secure the communication between your site and Citrix Workspace app, you can integrate your Citrix Workspace app connections using secure technologies such as Citrix Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix recommends using Citrix Gateway between StoreFront servers and user devices.

- A firewall: Network firewalls can allow or block packets based on the destination address and port. If you're using Citrix Workspace app through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.
- Trusted server.
- For Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments only (not applicable to XenDesktop 7): A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or Transport Layer Security (TLS) tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace app and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.
- For Citrix Virtual Apps and Desktops or Citrix DaaS deployments only: Citrix Secure Web Gateway or SSL Relay solutions with TLS protocols. TLS versions 1.0 through 1.2 are supported.

Provision to manage multiple proxy servers

Previously, Citrix Workspace app did not support the usage of multiple proxy servers. Startig with the 2408 version, you can use multiple proxy servers that allow the HDX sessions to select appropriate proxy servers for accessing specific resources. This selection is based on the proxy rules configured in the Proxy Auto-Configuration (PAC) file. Using this file, you can manage the network by mentioning which network traffic must be sent through a proxy server and which must be sent directly.

This feature is disabled by default. To enable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/All_Regions.ini` file.
2. Go to the `[Network\Proxy]` section and do the following:

    a) Update `ProxyType` to `Script`.
    b) Update `ProxyAutoConfigURL` to `file://file-path`, `https://serverfilepath`, or `http://server/filepath`.

    You must replace the preceding path with the real path that you want to use for connection.

When `Script` is added as `ProxyType`, the client retrieves a JavaScript based on the .pac file from the URL specified in the Proxy script URLs policy option. The .pac file is run to identify which proxy server must be used for the connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway

Citrix Gateway (formerly Access Gateway) secures connections to StoreFront stores. Also, lets administrators control, in a detailed way, user access to desktops and applications.

To connect to desktops and applications through Citrix Gateway:

1. Specify the Citrix Gateway URL that your administrator provides using one of the following ways:

   - The first time you use the self-service user interface, you're prompted to enter the URL in the Add Account dialog box.
   - When you later use the self-service user interface, enter the URL by clicking **Preferences** > **Accounts** > **Add**.
   - If you're establishing a connection with the `storebrowse` command, enter the URL at the command line.

   The URL specifies the gateway and, optionally, a specific store:

   - To connect to the first store that Citrix Workspace app finds, use a URL of the form, for example: `https://gateway.company.com`.
   - To connect to a specific store, use a URL of the form, for example: `https://gateway.company.com>?\<storename\`. This dynamic URL is in a non-standard form; do not include = (the equals sign character) in the URL. If you're establishing a connection to a specific store with `storebrowse`, you might need quotation marks around the URL in the `storebrowse` command.

2. When prompted, connect to the store (through the gateway) using your user name, password, and security token. For more information on this step, see the Citrix Gateway documentation.

   When authentication is complete, your desktops and applications are displayed.

Proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app and your Citrix Virtual Apps and Desktops or Citrix DaaS deployment.

Citrix Workspace app supports the SOCKS and HTTPS protocol, along with the following:

- Citrix Secure Web Gateway™ and Citrix SSL Relay, the secure proxy protocol
- Windows NT Challenge/Response (NTLM) authentication.

To configure a proxy to launch a desktop using the SOCKS protocol, do the following:

1. Navigate to the `~/.ICAClient/All_Regions.ini` configuration file.
2. Update the following attributes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Update `ProxyType`. You can use `SocksV5` as `ProxyType`.

b) Update `ProxyHost`. You can add `ProxyHost` in the following format:

`<IP>:<PORT>`. For example "10.122.122.122:1080".

> **Note:**
>
> - To use proxy, disable EDT. To disable EDT, set the `HDXoverUDP` attribute to *off* in the `[Network\UDT]` section of the `~/.ICAClient/All_Regions.ini` configuration file.
> - To ensure a secure connection, enable TLS.

HTTPS protocol support for proxy server

Previously, you could connect to a proxy server only using the SOCKS protocol. From Citrix Workspace app 2308 onwards, you can connect to a proxy server using the HTTPS protocol also.

To open a desktop using an HTTPS protocol, do the following:

1. Navigate to the ~/.ICAClient/All_Regions.ini configuration file.
2. Go to the [Network\UDT] section.
3. Set the following:

```
1 HDXoverUDP=Off
```

4. Go to the [Network\Proxy] section.
5. Update the following attributes:

    - Update ProxyType. You can use Secure as ProxyType.
    - Update ProxyHost. You can add ProxyHost in the following format:

    `<IP>:<PORT>`. For example "192.168.101.37:6153".

Secure proxy server

Configuring connections to use the secure proxy protocol also enables support for Windows NT Challenge/Response (NTLM) authentication. If this protocol is available, it's detected and used at run time without any additional configuration.

> **Important:**
>
> NTLM support requires the OpenSSL 1.1.1d and libcrypto.so libraries. Install these libraries on the user device. These libraries are often included in Linux distributions. You can also download

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> them from http://www.openssl.org/.

Secure Web Gateway and SSL

You can integrate Citrix Workspace app with the Citrix Secure Web Gateway or Secure Sockets Layer (SSL) Relay service. Citrix Workspace app supports the TLS protocol. TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Secure Web Gateway

You can use the Citrix Secure Web Gateway in Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app and the server. If you're using the Secure Web Gateway in **Normal** mode, Citrix Workspace app doesn't require any configuration.

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

- The fully qualified domain name (FQDN) of the Citrix Secure Web™ Gateway server.
- The port number of the Citrix Secure Web Gateway server.

> **Note:**
>
> Citrix Secure Web Gateway Version 2.0 doesn't support Relay mode.

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

- Host name
- Intermediate domain
- Top-level domain

For example: my_computer.my_company.com is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (my_company), and a top-level domain (.com). The combination of intermediate and top-level domain (my_company.com) is referred to as the domain name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the Citrix Virtual Apps and Desktops™ or Citrix DaaS server for TLS-secured communication. When the SSL Relay receives a TLS connection, it decrypts the data before redirecting it to the server.

If you configure SSL Relay to listen on a port other than 443, you must specify the non-standard listening port number to Citrix Workspace app.

You can use Citrix SSL Relay to secure communications:

- Between a TLS-enabled user device and a server

For information about configuring and using SSL Relay to secure your installation, see the Citrix Virtual Apps™ documentation.

TLS

Previously, the minimum TLS version supported was 1.0, and the maximum TLS version supported was 1.2. Starting with version 2203, the maximum TLS version supported is 1.3.

You can control the versions of the TLS protocol that can be negotiated by adding the following configuration options in the [WFClient] section:

- MinimumTLS=1.1
- MaximumTLS=1.3

These values are the default values, which are implemented in the code. Adjust them as you require.

> **Notes:**
>
> - These values are read whenever programs start. If you change them after starting self-service or `storebrowse`, type: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
> - Citrix Workspace app for Linux does not allow the use of the `SSLv3` protocol.
> - TLS 1.0/1.1 works only with the older VDI or Citrix Gateway which support them.

To select the cipher suite set, add the following configuration option in the [WFClient] section:

- SSLCiphers=GOV

This value is the default value. Other recognized values are COM and ALL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> As with the TLS version configuration, if you change this configuration after starting self-service or storebrowse you must type:
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

CryptoKit update

CryptoKit Version 14.2 is integrated with the OpenSSL 1.1.1d version.

Cryptographic update

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

The TLS_RSA_ cipher suites have been removed entirely. Instead, it supports the advanced TLS_ECDHE_RSA_ cipher suites.

If your environment isn't configured with the TLS_ECDHE_RSA_ cipher suite, client launches aren't supported because of weak ciphers. For client authentication, 1536-bit RSA keys are supported.

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)

DTLS v1.0 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS 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_EMPTY_RENEGOTIATION_INFO_SCSV

TLS v1.3 supports the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_AES_256_GCM_SHA384 (0x1302)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> From version 1903 and later, DTLS is supported from Citrix Gateway 12.1 and later. For information on DTLS supported cipher suites for Citrix Gateway, see Support for DTLS protocol

Cipher suites To enable different cipher suites, change the parameter `SSLCiphers` value to `ALL`, `COM`, or `GOV`. By default, the option is set to `ALL` in the `All_Regions.ini` file in the `$ICAROOT/config` directory.

The following sets of cipher suites are provided by ALL, GOV, and COM, respectively:

- ALL
  - all 3 ciphers are supported.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

For troubleshooting information, see Cipher suites.

Cipher suites with the prefix TLS_RSA_ do not offer forward secrecy. These cipher suites are now deprecated in the industry. However, to support backward compatibility with older versions of Citrix Virtual Apps and Desktops or Citrix DaaS, Citrix Workspace app includes an option to enable these cipher suites.

For better security, set the flag `Enable\\_TLS\\_RSA\\_` to **False**.

The following is the list of deprecated cipher suites:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Note:**
>
> The last two cipher suites use the RC4 algorithm and are deprecated because they're insecure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> You might also consider the TLS_RSA_3DES_CBC_EDE_SHA cipher suite to be deprecated. You can use flags to enforce all these deprecations.

For information on configuring DTLS v1.2, see the Adaptive transport section in the Citrix Virtual Apps and Desktops documentation.

Prerequisite:

If you're using version 1901 and earlier, do the following steps:

If `.ICAClient` is already present in the home directory of the current user:

- Delete `All\\_Regions.ini` file

Or

- To keep the `AllRegions.ini` file, add the following lines at the end of the [Network\SSL] section:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

If the `.ICAClient` folder isn't present in the home folder of the current user, it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the features is kept.

The following table lists the cipher suites in each set:
Table 1 –Cipher suite support matrix

> **Note:**
>
> All the preceding cipher suites are `FIPS-` and `SP800-52-` compliant. The first two are allowed only for (D)TLS1.2 connections. See **Table 1 –Cipher suite support matrix** for a comprehensive representation of cipher suite supportability.

Certificates

When you use a store with SAML authentication (using the `AUTHv3` protocol), the following error message appears: "Unacceptable TLS Certificate."

The issue occurs when you use Citrix Workspace app 1906 and later. For troubleshooting instructions, see the following Knowledge Center articles:

- CTX260336
- CTX231524
- CTX203362

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If your StoreFront server fails to provide the intermediate certificates that match the certificate it's using, or you install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store:

1. Get one or more intermediate certificates separately in PEM format.

   > **Tip:**
   >
   > If you can't find a certificate in PEM format, use the `openssl` utility to convert a certificate in CRT format to a .pem file.

2. As the user installs the package (usually root):

   a) Copy one or more files to $ICAROOT/keystore/intcerts.

   b) Run the following command as the user who installed the package:

   ```
   $ICAROOT/util/ctx_rehash
   ```

If you authenticate a server certificate that a certificate authority issued and not trusted in the user devices, follow these instructions before adding a StoreFront store:

1. Get the root certificate in PEM format.
   Tip: If you can't find a certificate in this format, use the `openssl` utility to convert a certificate in CRT format to a .pem file.
2. As the user who installed the package (usually root):

   a) Copy the file to $ICAROOT/keystore/cacerts.

   b) Run the following command:
   `$ICAROOT/util/ctx_rehash`

Enhancement to HDX™ Enlightened Data Transport Protocol (EDT)

In earlier releases, when `HDXoverUDP` is set to `Preferred`, data transport over EDT is used as primary with fallback to TCP.

Starting with Citrix Workspace app version 2103, when session reliability is enabled, EDT, and TCP are attempted in parallel during the following:

- Initial connection
- Session reliability reconnection
- Auto client reconnect

This enhancement reduces connection time when EDT is preferred. However, the required underlying UDP transport is unavailable and TCP must be used.

By default, after fallback to TCP, adaptive transport continues to seek EDT every five minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enlightened Data Transport (EDT) MTU discovery

Citrix Workspace app version 2109 supports Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT). It increases the reliability and compatibility of the EDT protocol and provides an improved user experience.

For more information, see the EDT MTU Discovery section in the Citrix Virtual Apps and Desktops documentation.

Support for EDT IPv6

Starting with Citrix Workspace app version 2203, EDT IPv6 is supported.

> **Note:**
>
> IPv6 is supported in both TCP and EDT. However, IPv6 isn't supported in TCP over TLS and in EDT over DTLS.

Support for IPv6 UDP with DTLS

Previously, DTLS connections between Citrix Workspace app for Linux and Virtual Delivery Agents (VDAs) were supported over the IPv4 network only.

Starting with the 2311 release, Citrix Workspace app supports DTLS connections over both IPv4 and IPv6.

This feature is enabled by default.

No additional configuration is required when you use IPv6 DTLS direct connection with VDA on Citrix Workspace app for Linux.

Support for IPv6 TCP with TLS

Previously, TLS connections between Citrix Workspace app for Linux and Virtual Delivery Agents (VDAs) were supported over the IPv4 network only.

Starting with the 2311 release, Citrix Workspace app supports TLS connections over both IPv4 and IPv6.

This feature is enabled by default.

No additional configuration is required when you use IPv6 TLS direct connection with VDA on Citrix Workspace app for Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication

September 30, 2026

Starting from Citrix Workspace app 2012, you can view the authentication dialog inside Citrix Workspace app and store details on the sign-in screen. This enhancement provides a better user experience.

Authentication tokens are encrypted and stored so that you don't need to reenter credentials when your system or session restarts.

> **Note:**
>
> This authentication enhancement is available only in cloud deployments.

Prerequisite:

Install the `libsecret` library.

This feature is enabled by default.

Authentication enhancement for `Storebrowse`

Starting with version 2205, the authentication dialog is present inside Citrix Workspace app and the store details are displayed on the logon screen for a better user experience. The authentication tokens are encrypted and stored so that you don't need to reenter credentials when your system or session restarts.

The authentication enhancement supports `storebrowse` for the following operations:

- `Storebrowse -E`: Lists the available resources.
- `Storebrowse -L`: Launches a connection to a published resource.
- `Storebrowse -S`: Lists the subscribed resources.
- `Storebrowse -T`: Terminates all sessions of the specified store.
- `Storebrowse -Wr`: Reconnects the disconnected yet active sessions of the specified store. The [r] option reconnects all the disconnected sessions.
- `storebrowse -WR`: Reconnects the disconnected yet active sessions of the specified store. The [R] option reconnects all the active and disconnected sessions.
- `Storebrowse -s`: Subscribes the specified resource from a given store.
- `Storebrowse -u`: Unsubscribes the specified resource from a given store.
- `Storebrowse -q`: Launches an application using the direct URL. This command works only for StoreFront stores.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - You can continue to use the remaining `storebrowse` commands as used earlier (using AuthMangerDaemon).
> - The authentication enhancement is applicable for cloud deployments only.
> - With this enhancement, the persistent login feature is supported.

Support for more than 200 groups in Azure AD

Starting with the 2305 release, an Azure AD user who is part of more than 200 groups can view apps and desktops assigned to the user. Previously, the same user wasn't able to view these apps and desktops.

To enable this feature, do the following:

1. Navigate to $ICAROOT/config/AuthManConfig.xml and add the following entries:

```
<compressedGroupsEnabled>true</compressedGroupsEnabled>
```

> **Note:**
>
> Users must sign out from Citrix Workspace app and sign in back to enable this feature.

Authentication enhancement for `Storebrowse` configuration

By default, the authentication enhancement feature is disabled.

If the gnome-keyring isn't available, the token is stored in the selfservice process memory.

To enforce storage of the token in memory, disable the gnome-keyring, using the following steps:

1. Navigate to `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Add the following entry:

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
```

Smart card

To configure smart card support in Citrix Workspace app for Linux, you must configure the StoreFront server through the StoreFront console.

Citrix Workspace app supports smart card readers that are compatible with PCSC-Lite and PKCS#11 drivers appropriately. By default, Citrix Workspace app now locates `opensc-pkcs11.so` in one of the standard locations. To add customized PKCS#11 drivers, see Add customized PKCS#11 drivers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app can find opensc-pkcs11.so in a non-standard location or another PKCS\\#11 driver. You can store the respective location using the following procedure:

1. Locate the configuration file: $ICAROOT/config/AuthManConfig.xml.
2. Locate the line <key>PKCS11module</key> and add the driver location to the <value> element immediately following the line.

> **Note:**
>
> If you enter a file name for the driver location, Citrix Workspace app navigates to that file in the $ICAROOT/PKCS\ #11 directory. You can also use an absolute path beginning with "/".

After you remove a smart card, configure the behavior of Citrix Workspace app by updating the SmartCardRemovalAction using the following steps:

1. Locate the configuration file: $ICAROOT/config/AuthManConfig.xml
2. Locate the line <key>SmartCardRemovalAction</key> and add noaction or forcelogoff to the <value> element immediately following the line.

The default behavior is noaction. No action is taken to clear stored credentials and generated tokens on removal of the smart card.

The forcelogoff action clears all credentials and tokens within StoreFront on removal of the smart card.

Limitation:

- Attempts to start a server VDA session using smart card authentication might fail for the smart card with multiple users. [HDX-44255]

Add customized PKCS#11 drivers

If your smartcard requires a custom PKCS#11 driver, do the following steps to add the driver path:

1. Navigate to the $ICAROOT/config/AuthManConfig.xml configuration file.
2. Locate the line <key>PKCS11module</key> and add the driver location to the <value> element immediately following the line. For example:

   /usr/lib/pkcs11/libIDPrimePKCS11.so.
3. Locate the configuration file: $ICAROOT/config/scardConfig.json.
4. Locate DefaultPKCS11Lib and change the default value to the customized driver path without /usr. For example:

   /lib/pkcs11/libIDPrimePKCS11.so

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling smart card support

Citrix Workspace app supports various smart card readers if smart card is enabled on both server and Citrix Workspace app.

You can use smart cards for the following purposes:

- Smart card logon authentication - Authenticates you to Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) servers.
- Smart card application support - Enables smart card-aware published applications to access the local smart card devices.

Smart card data is security sensitive and must be transmitted over a secure authenticated channel, such as TLS.

Smart card support has the following prerequisites:

- Your smart card readers and published applications must be PC/SC industry standard compliant.
- Install the appropriate driver for your smart card.
- Install the PC/SC Lite package.
- Install and run the `pcscd` Daemon, which provides middleware to access the smart card using PC/SC.
- On a 64-bit system, both 64-bit and 32-bit versions of the "libpcsclite1"package must be present.

For more information about configuring smart card support on servers, see Smart cards in the Citrix Virtual Apps and Desktops documentation.

Enhancement on smart card support

Starting with Version 2112, Citrix Workspace app supports the Plug and Play functionality for the smart card reader.

When you insert a smart card, the smart card reader detects the smart card in the server and client.

You can plug-and-play different cards at the same time, and all of these cards are detected.

Prerequisites:

Install the `libpcscd` library on the Linux client.

> **Note:**
>
> This library might be installed by default in the recent versions of most Linux distributions. However, you might need to install the `libpcscd` library in earlier versions of some Linux distributions, such as Ubuntu 1604.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To disable this enhancement:

1. Navigate to the <ICAROOT>/config/module.ini folder.
2. Go to the SmartCard section.
3. Set the DriverName=VDSCARD.DLL.

Support for new PIV cards

Starting with version 2303, Citrix Workspace app supports the following new Personal Identification Verification (PIV) cards:

- IDEMIA next-generation smartcard
- DELL TicTok Smartcard

Performance optimization for smartcard driver

Citrix Workspace app 2303 version includes performance related fixes and optimizations for the VDSCARDV2.DLL smartcard driver. These enhancements help to outperform version 1 VDSCARD.DLL.

Fast smart card

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN environments.

Fast smart cards are supported on Windows VDA only.

To enable fast smart card sign in on Citrix Workspace app:

Starting with the 2408 version, Fast smart card sign-in is enabled by default on the VDA and disabled by default on Citrix Workspace app. To enable the fast smart card feature, do the following:

1. Navigate to the [SmartCard] section in the /opt/Citrix/ICAClient/config/module.ini configuration file.
2. Add the following entry:

```
1 SmartCardCryptographicRedirection=On
```

To disable fast smart card sign in on Citrix Workspace app:

To disable fast smart card sign-in on Citrix Workspace app, remove the SmartCardCryptographicRedirect parameter from the [SmartCard] section in the /opt/Citrix/ICAClient/config/module.ini configuration file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for Cryptography Next Generation smartcards Staring with 2408 version, Citrix Workspace app supports the new Personal Identification Verification (PIV) smartcard that uses Elliptic Curve Cryptography (ECC) algorithm. This type of smartcard works based on Cryptography Next Generation.

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide extra proofs of identification to gain access.

Multifactor authentication makes authentication steps and the associated credential collection forms configurable by the administrator.

Native Citrix Workspace app supports this protocol by building on the Forms sign in support already implemented for StoreFront. The web sign-in pages for Citrix Gateway and Traffic Manager virtual servers also consume this protocol.

> **Note:**
>
> Multi-factor (nFactor) authentication supports only form-based authentication.

For more information, see SAML authentication and Multi-Factor (nFactor) authentication in the Citrix ADC documentation.

Endpoint Analysis support for multi-factor (nFactor) authentication

Starting with this release, Citrix Workspace app supports Endpoint Analysis (EPA) for multi-factor authentication, enhancing compliance and security. For example, if EPA and LDAP are configured as part of multi-factor authentication, Citrix Workspace app detects and runs the EPA app for authentication along with the LDAP authentication.

Previously, Citrix Workspace app did not support invoking the EPA app, resulting in an "Access Denied"error. This release supports EPA invocation, allowing the authentication process to proceed smoothly.

The new feature ensures comprehensive endpoint security checks, compliance with organizational policies, and regulatory requirements. It reduces the risk of unauthorized access and improves overall network integrity.

Prerequisites:

Ensure that the Endpoint Analysis app is installed on your system.

Supported Operating Systems:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- IGEL OS: EPA is already available.
- Ubuntu 18, 20, and 22: EPA is not pre-installed; you need to download and install EPA before proceeding with authentication. Download EPA for Ubuntu from the Citrix downloads page.

This feature is enabled by default and is used in conjunction with multi-factor authentication. For more information, see the multi-factor (nFactor) authentication documentation.

Support for authentication using FIDO2 in HDX session

Starting with the 2303 version, you can authenticate within an HDX session using password-less FIDO2 security keys. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. For more information about FIDO2, see FIDO2 Authentication.

> **Note:**
>
> If you're using the FIDO2 device through USB redirection, remove the USB redirection rule of your FIDO2 device. You can access this rule from the `usb.conf` file in the `$ICAROOT/` folder. This update helps you to switch to the FIDO2 virtual channel.

Starting with the 2505 version, FIDO2 authentication is enabled by default and requires no additional configuration. In earlier versions, FIDO2 authentication is disabled by default.

To change the default behavior, do the following:

1. Navigate to the `<ICAROOT>/config/module.ini` file.
2. Go to the `[ICA 3.0]` section.
3. Set the value as required:
    - To enable FIDO2 authentication, set `FIDO2=On`.
    - To disable FIDO2 authentication, set `FIDO2=Off`.
4. Launch a new session for the change to take effect.

This feature currently supports roaming authenticators (USB only) with PIN code and touch capabilities. You can configure FIDO2 Security Keys based authentication. For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.

When you access an app or a website that supports FIDO2, a prompt appears, requesting access to the security key. If you've previously registered your security key with a PIN, you must enter the PIN while signing in. The PIN can be a minimum of 4 and a maximum of 64 characters.

If you've registered your security key previously without a PIN, simply touch the security key to sign in.

Limitation:

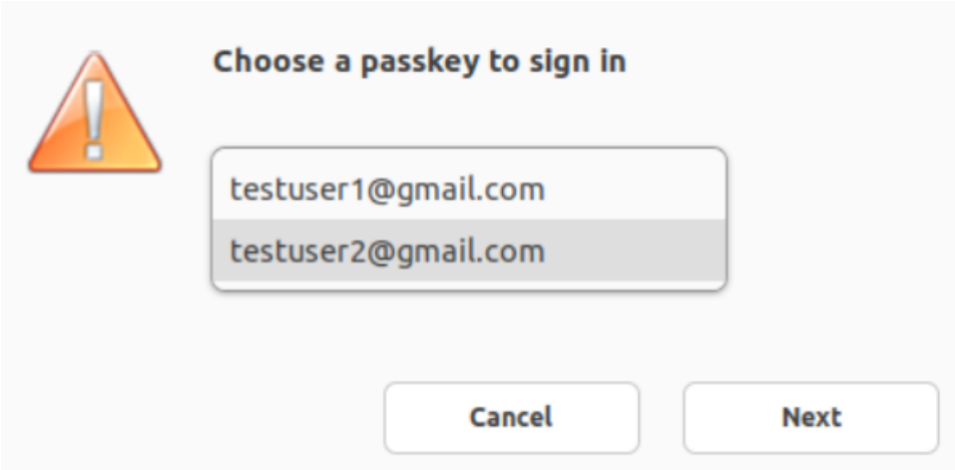
© 1997–2026 Citrix Systems, Inc. All rights reserved.

You might fail to register the second device to a same account using FIDO2 authentication.

Support for multiple passkeys in HDX session

Previously, when there were multiple passkeys associated with a security key or FIDO2 device, you were not having an option to select an appropriate passkey. By default, the first passkey was used for authentication.

Starting with the 2405 version, you can select an appropriate passkey from the Citrix Workspace app UI. This feature is enabled by default.
When there are multiple passkeys, the first one is selected as default. However, you can select the appropriate passkey as follows:



Support for authentication using FIDO2 when connecting to on-premises stores

Starting with Citrix Workspace app for Linux version 2309, users can authenticate using passwordless FIDO2 security keys when signing in to on-premises stores. The security keys support different types of security inputs such as security pins, biometrics, card swipe, smart card, Public Key Certificates, and so on. For more information about FIDO2, see FIDO2 Authentication.

Administrators can configure the type of browser to authenticate to Citrix Workspace app. To enable the feature, navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
1       <key>FIDO2Enabled</key>
2       <value>true</value>
```

To modify the default browser, navigate to `$ICAROOT/config/AuthManConfig.xml` and modify the browser settings as required. The possible values are `chromium`, `firefox`, and `chromium-browser`, and `Microsoft Edge`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<FIDO2AuthBrowser>firefox</FIDO2AuthBrowser>
```

Support for authentication using FIDO2 when connecting to cloud stores

Starting with Citrix Workspace app for Linux version 2405, users can authenticate using passwordless FIDO2 security keys when signing in to cloud stores. The security keys support different types of security inputs such as security pins, biometrics, card swipe, smart card, Public Key Certificates, and so on. For more information, see FIDO2 Authentication.

Administrators can configure the type of browser to authenticate to Citrix Workspace app.

To enable the feature, navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
<key>FIDO2Enabled</key>
<value>true</value>
```

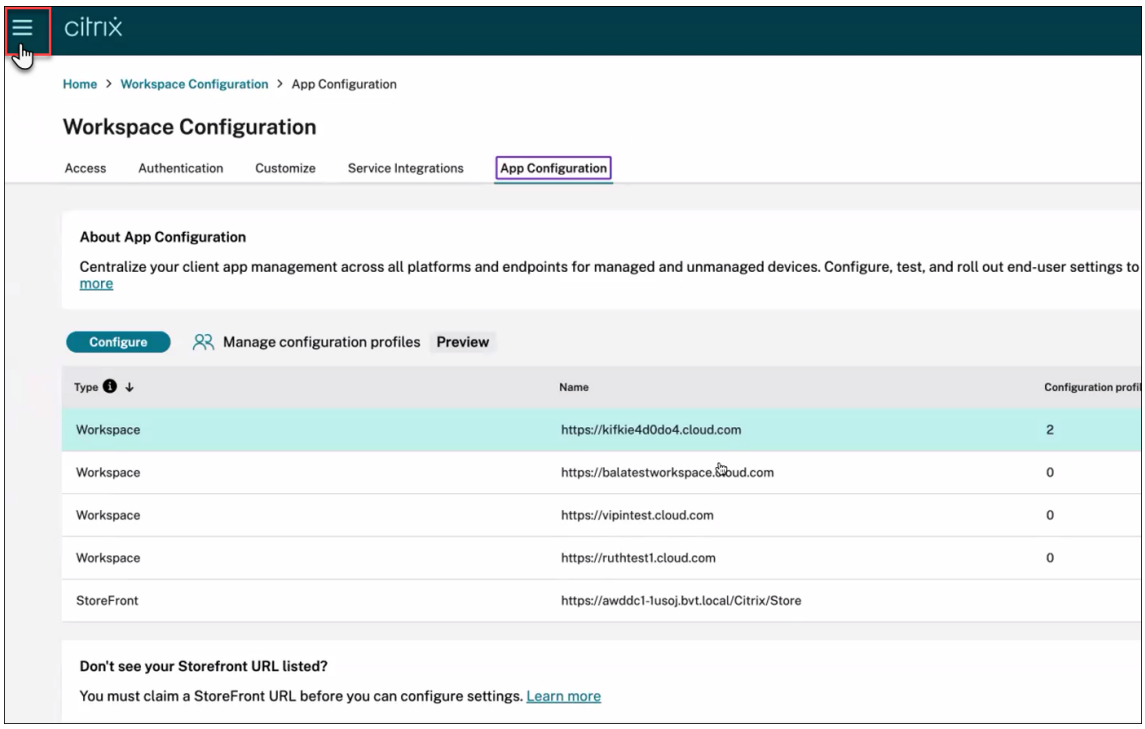
To modify the default browser, navigate to `$ICAROOT/config/AuthManConfig.xml` and modify the browser settings as required. The possible values are chromium, firefox, and chromium-browser.

```
<FIDO2AuthBrowser>firefox</FIDO2AuthBrowser>
```

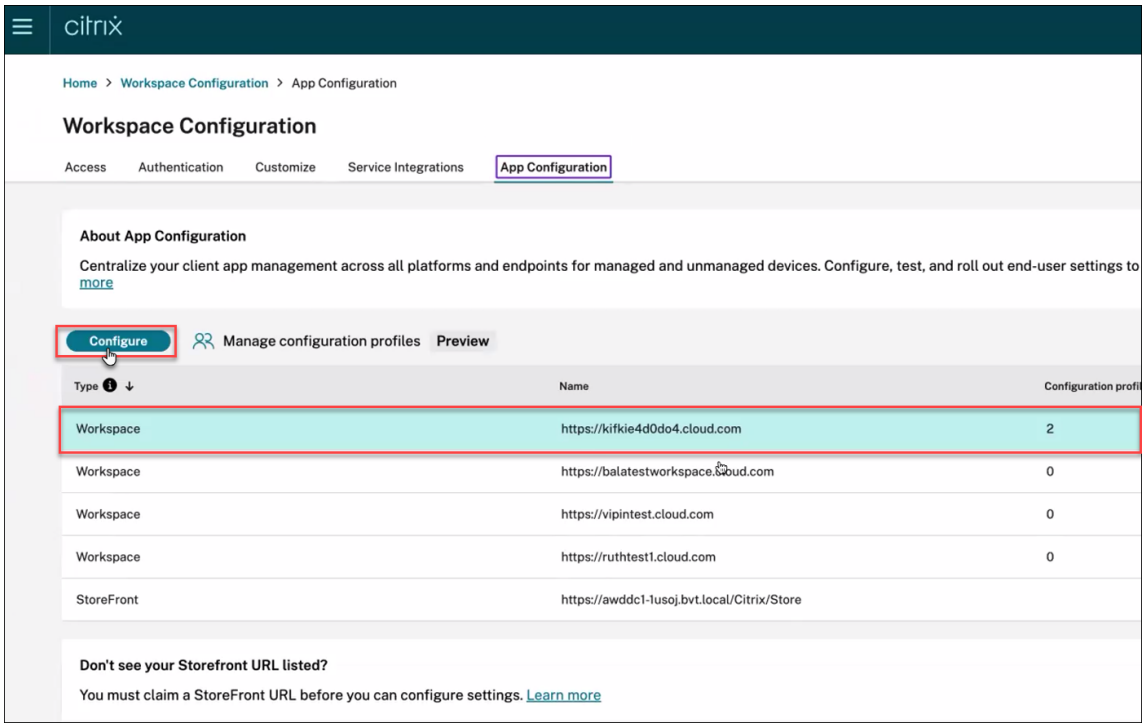
Using GACS configure FIDO2 authentication To enable the FIDO2 authentication for the store URL using GACS, perform the following steps:

1. Sign into **Citrix Cloud™**.
2. On the upper-left corner, click the hamburger icon, click **Workspace Configuration**, and then click **App Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

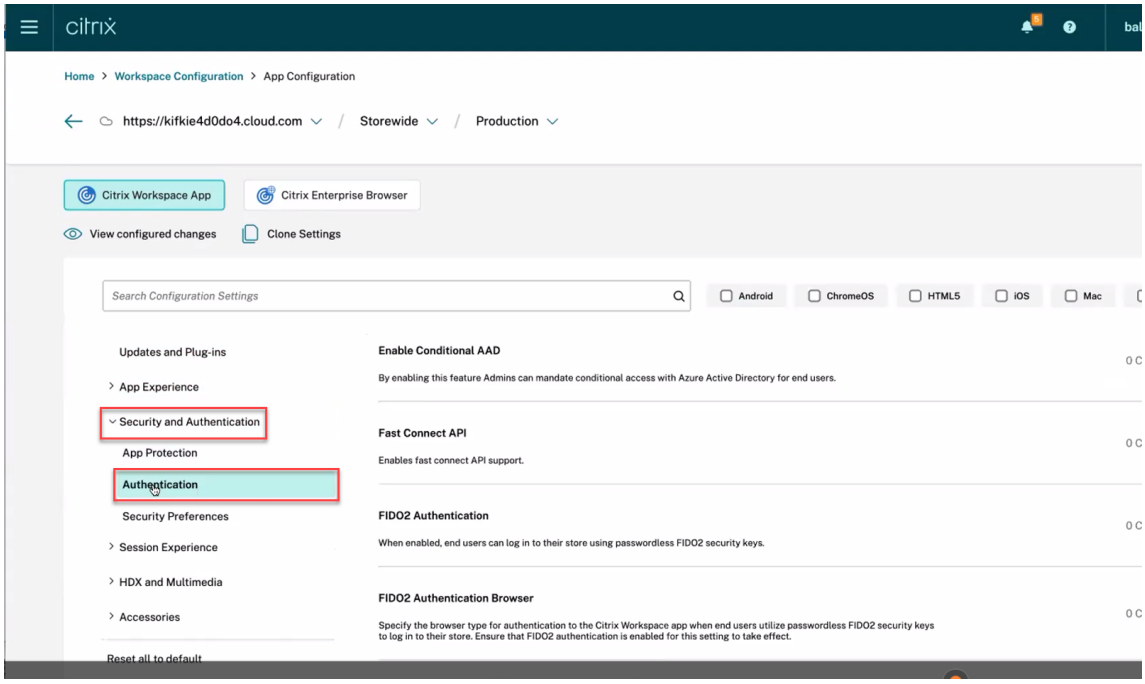


3. Click **Workspace**, and then click the **Configure** button.

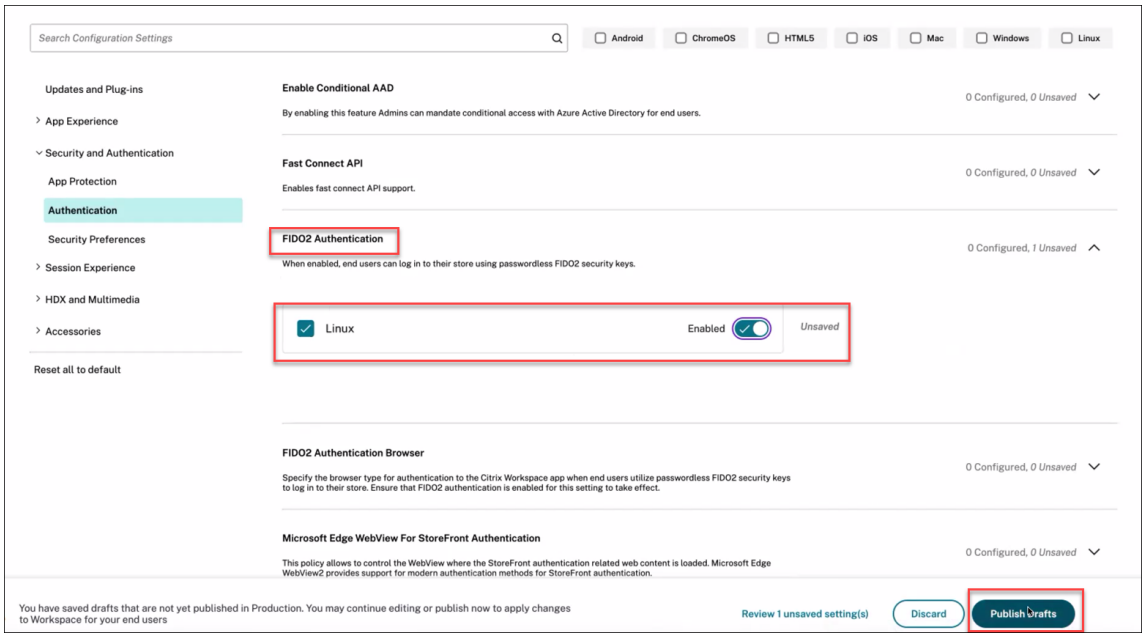


4. Click **Security and Authentication**, and then click **Authentication**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **FIDO2 Authentication**, select the **Linux** checkbox, and then switch the **Enabled** toggle.



6. Click **Publish Draft**.

Customized authentication

The following table provides a reference to the available customized authentication for Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utility	SDK	Authentication type	Libraries used	Binaries	Authentication type detection
Fast Connect	Credential insertion SDK	Username/password/smartcard/Domain passthrough	libCredentialInjectorSDK.so	wfica	Parameters- Used by third party authenticator integrations
Custom Dialog	Platform Optimization SDK	Username/password/smartcard	UIDialogLib and UIDialogLib-WebKit3.so	No	Auto detection - Used by thin clients partners
Storebrowse	Citrix Workspace app	Username/password	No	Storebrowse	Parameters

NFC support for FIDO2 Authentication

Starting with the 2411 version, you can use the FIDO2-supported NFC card for a Tap-and-Go experience, which is an end-to-end single sign-on (SSO) solution. This means that you can use an NFC card to authenticate to a Citrix® store and then a pre-configured virtual desktop or virtual app will automatically open using SSO.

For more information on configuring this feature, see the following sections:

Prerequisites

Hardware requirements:

- NFC-supported FIDO2 keys. For example, Yubikey5.
- NFC-supported FIDO2 readers that are compatible with Linux clients. For example, ACR1252U-M.

Software requirements:

The following software packages are required for this feature:

- **swig**
- **libpcsclite-devel** and **pcsc-lite** for CentOS or RHEL

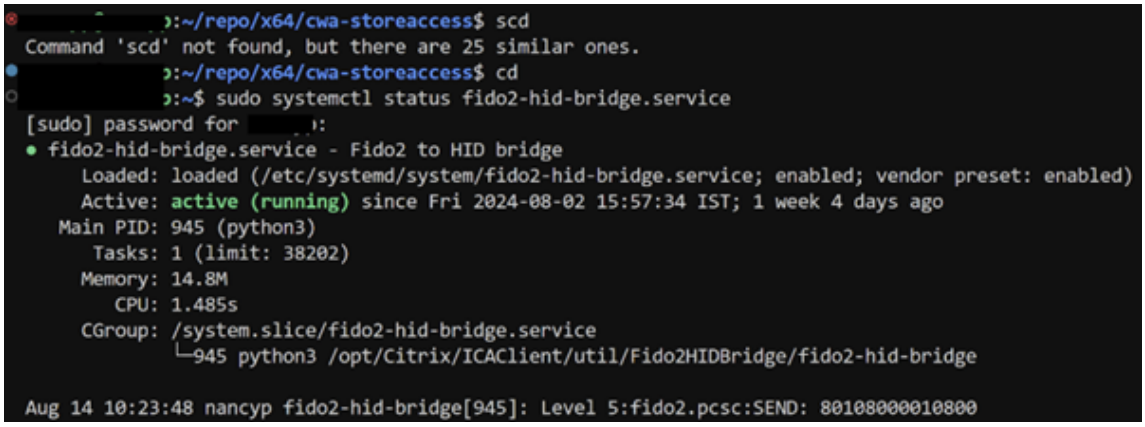
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **libpcsclite-dev** and **pcscd** for Ubuntu
- **python3** and **python3-pip**
- Python packages: `pyscard`, `uhid`, and `fido2`
- **Chromium browser** (if Citrix Enterprise Browser is not preferred). The preferred installer for the Chromium browser is the Debian package, which can be downloaded from the Chromium downloads page. It is not recommended to install Chromium as a snap.

> **Note:**
>
> - Administrators can install the above packages by running the `setupFIDO2Service.sh` script that is located at `<ICAROOT>/util/Fido2HIDBridge` as a sudo user. This `setupFIDO2Service.sh` script is an example for Ubuntu and RHEL OS. Admins can modify this script as required for their OS configuration.
> - This feature is not supported on the Ubuntu x86-64, RHEL x86-64, and ARM64 architectures.

How to enable this feature

1. Ensure that the `fido2-hid-bridge.service` is running, as it's usually installed with the Citrix Workspace app. If it isn't running, you can start it manually.



2. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

   `<key>FIDO2Enabled</key>`

   `<value>`**`true`**`</value>`

   Disable Long Lived Token as well:

   `<longLivedTokenSupport>`**`false`**`</longLivedTokenSupport>`

3. If required, modify the default browser by navigating to `$ICAROOT/config/AuthManConfig.xml` and updating the browser settings as required. The possible values are `CEB` and `chromium`. The default value is `CEB`.

   `<FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. To display the App Authenticator in full screen, add the following entry:

   ```
   <Fido2FullScreenMode>true</Fido2FullScreenMode>
   ```

   By default, the App Authenticator is displayed in the window mode.

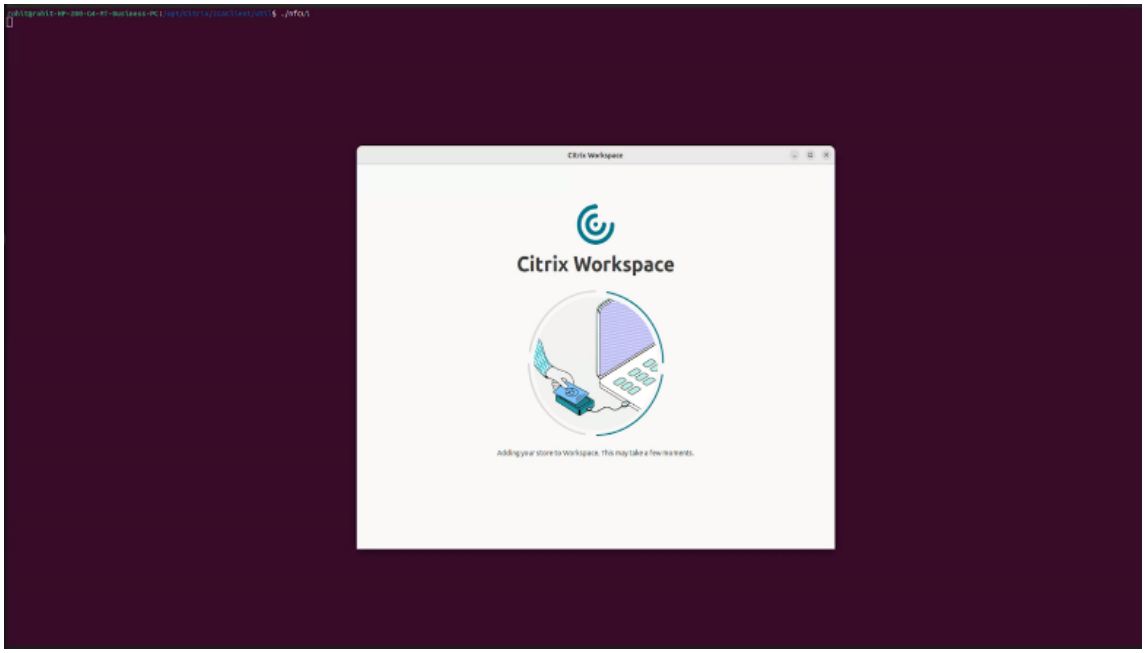
How to use this feature

1. Add `StoreURL` and `ResourceName` in `$ICAROOT/config/AuthManConfig.xml`:

   ```
   <StoreURL>test.cloud.com</StoreURL>
   ```

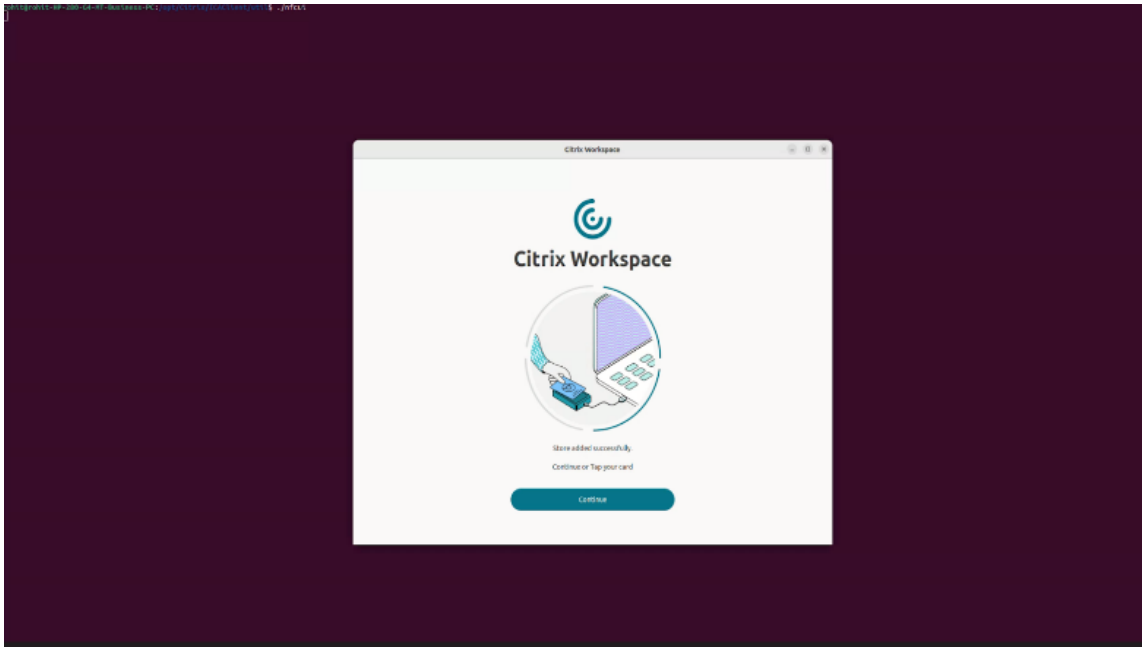
   ```
   <ResourceName>Notepad</ResourceName>
   ```

2. Navigate to `$ICAROOT/util` and run `nfcui`.



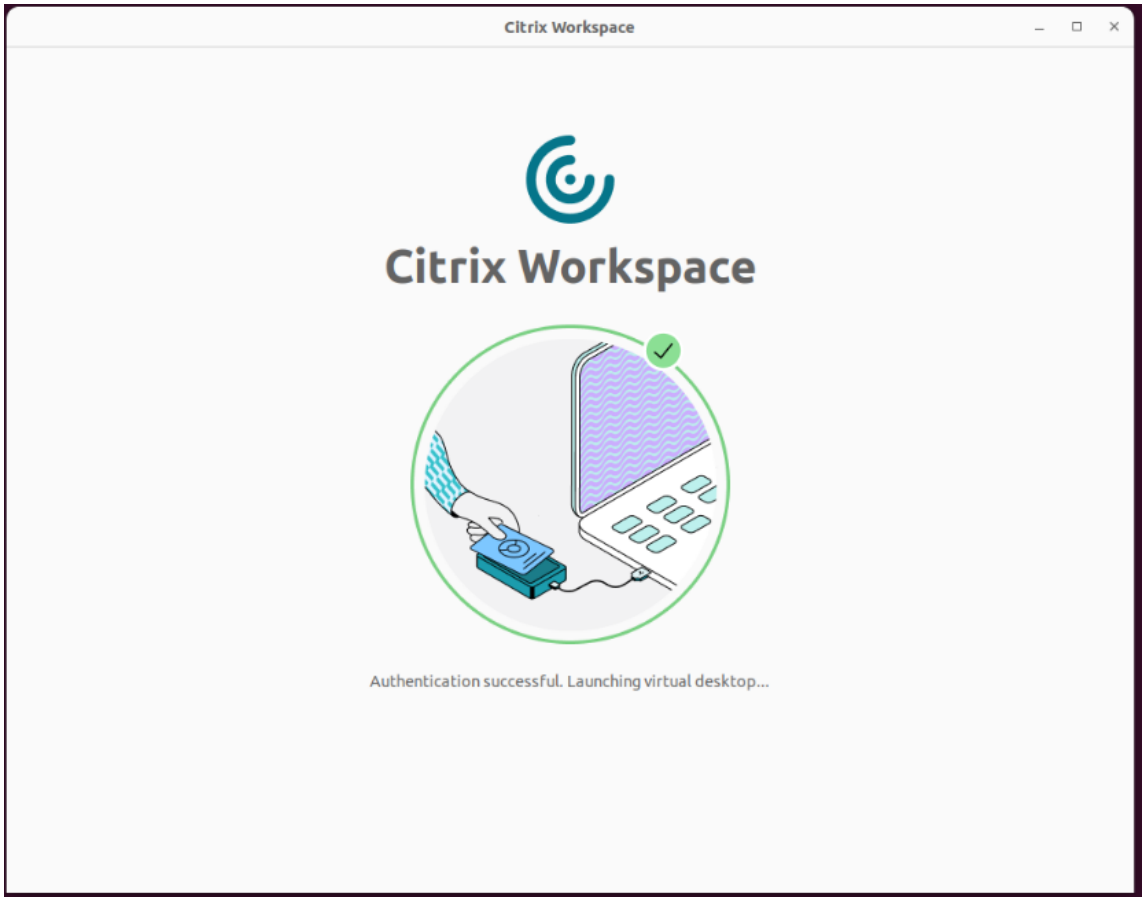
3. Once the store is added, either tap or click **Continue** for authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

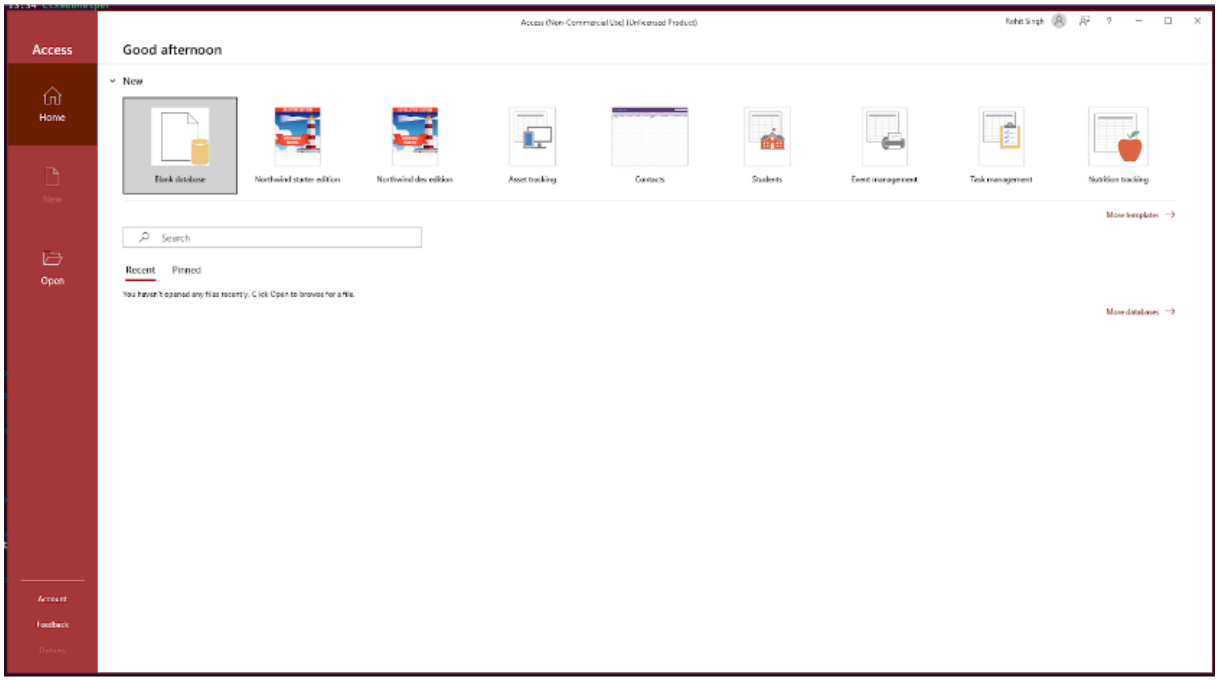


4. On the authentication page, enter the user credentials and click **Face**, **Fingerprint**, **PIN**, or **Security key** as the sign-in option.
5. Tap the NFC-supported FIDO2 key on the reader.
6. Enter the PIN for your security key, and click **Next**.
7. After successful authentication, click **Yes** on the **Stay signed in?** window.
8. Once authentication is completed, the configured VDA or the app is launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The application is successfully launched.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mandate end users to authenticate and access apps and desktops through native app

Starting with version 2508, admins can require Linux users to access Citrix Workspace exclusively through the native app. When enabled, users who try to access the store URL or use third-party browsers are automatically redirected to the Citrix Workspace app. This ensures users benefit from all native app features and enjoy a seamless experience.

If users attempt to connect using a browser and launch the HDX™ engine, they are prompted to add the store to the native client for future use. This feature gives admins greater control, enhances security by keeping authentication within the native app. Also, removes the need to download ICA files.

Admins can enable this feature in Citrix Cloud. Currently, it is supported only for Cloud stores.

For more information, see Mandate end users to authenticate and access apps and desktops through native app.

Storebrowse authentication path

For cloud stores, storebrowse authenticates over an interprocess communication (IPC) path. This path is required for Long Lived Token (LLT), DSAuth, and Microsoft Entra ID (formerly Azure AD) authentication to work correctly.

The IPC path is controlled by the `StorebrowseIPCDisabled` key in `$ICAROOT/config/AuthManConfig.xml`. To use a cloud store, make sure this key is either absent or set to **`false`**.

To enable the IPC path for a cloud store, do the following:

1. Open `$ICAROOT/config/AuthManConfig.xml`.
2. Find the `StorebrowseIPCDisabled` key, if it is present.
3. Remove the key, or set its value to **`false`**:

```
<dict>
    <StorebrowseIPCDisabled>false</StorebrowseIPCDisabled>
</dict>
```

4. Save the file, and then reconnect to the cloud store.

> **Note:**
>
> - If you applied the Raspberry Pi OS workaround from an earlier release, your configuration might still contain `StorebrowseIPCDisabled=true`. Remove this key before you connect to a cloud store.
> - In the same file, `AuthManLiteDisabled` takes precedence over `StorebrowseIPCDisabled`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> . For cloud store deployments, make sure `AuthManLiteDisabled` is also not set to **`true`**.

Entra ID SSO support for cloud

Starting with version 2508.10, Citrix Workspace app for Linux supports Microsoft Entra ID single sign-on (SSO) on endpoint devices running **Ubuntu 22.04** and **Ubuntu 24.04**. Use Microsoft Entra ID credentials to sign in to Citrix cloud stores and access Citrix Virtual Apps and Desktops with SSO, without repeated credential prompts.

Single sign-on with Microsoft Entra ID

Use SSO with Microsoft Entra ID credentials to access virtual apps and desktops on Entra joined or Entra hybrid joined session hosts.

Prerequisites

Install the following packages on the endpoint device:

- `gnome-keyring` (version 3.18.3 or later)

  For Ubuntu and Ubuntu-based distributions, run the following command:

  ```
  sudo apt-get install gnome-keyring
  ```

- `libsecret`

  For Ubuntu and Ubuntu-based distributions, run the following command:

  ```
  sudo apt-get install libsecret-1-0
  ```

> **Note:**
>
> When Citrix Long Lived Token (LLT) is enabled, Microsoft Entra ID SSO cookies must persist to maintain seamless authentication. To enable cookie persistence, configure the following setting in `AuthManConfig.xml` located at `/opt/Citrix/ICAClient`:
>
> ```
> <key>SharedAuthContextEnabled</key>
> <value>true</value>
> ```

Entra ID SSO using the system browser

To enable Entra ID SSO with the system browser, set the following keys in `AuthManConfig.xml` located at `/opt/Citrix/ICAClient`:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<key>AADSSOWithFido2AuthenticationEnabled</key>
<value>true</value>

<key>FIDO2Enabled</key>
<value>true</value>

<!-- FIDO2AuthBrowser options: CEB, chromium, firefox, chromium-browser
    -->
<FIDO2AuthBrowser>chromium</FIDO2AuthBrowser>
```

> **Note:**
>
> Entra ID SSO is supported with Firefox, Microsoft Edge, and Chromium.

Entra ID SSO using Storebrowse

To enable Entra ID SSO with Storebrowse:

1. Navigate to the utility directory:

   ```
   cd /opt/Citrix/ICAClient/util
   ```

2. Add the store:

   ```
   ./storebrowse -a <store_URL>
   ```

3. Enumerate and authenticate the store:

   ```
   ./storebrowse -E <full_store_URL>
   ```

4. Launch the resource:

   ```
   ./storebrowse -L <resourceID> <full_store_URL>
   ```

Entra ID single sign-on (SSO) from web browsers

Starting with version 2601, Citrix Workspace app for Linux supports Entra ID single sign-on (SSO) from web browsers through the Citrix Web Extension. This feature is enabled by default.

Prerequisites:

The following libraries are required:

- **gnome-keyring** version 3.18.3 or later

  If you are using Debian, run the following command:

  ```
  sudo apt-get install gnome-keyring
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you are using RPM, run the following command:

```
sudo yum install gnome-keyring
```

- **libsecret**

  If you are using Debian, run the following command:

  ```
  sudo apt-get install libsecret-1-0
  ```

  If you are using RPM, run the following command:

  ```
  sudo yum install libsecret-1*
  ```

Microsoft Edge support for FIDO2 and Entra ID SSO

Starting with version 2601, Citrix Workspace app for Linux adds support for using Microsoft Edge for:

- FIDO2 authentication
- Entra ID Single Sign-On (SSO) using the system browser

To configure Microsoft Edge for these flows, edit `AuthManConfig.xml` located at `/opt/Citrix/ICAClient/config/AuthManConfig.xml`.

Use Microsoft Edge as the browser for FIDO2 authentication:

```
<!-- FIDO2AuthBrowser - CEB, chromium, firefox, chromium-browser, edge -->
<FIDO2AuthBrowser>edge</FIDO2AuthBrowser>
```

Use Microsoft Edge as the system browser for Entra ID SSO:

```
<!-- SystemBrowser - CEB, chromium, firefox, chromium-browser, edge -->
<SystemBrowser>edge</SystemBrowser>
```

These settings ensure that both FIDO2 authentication and Entra ID SSO flow launch using Microsoft Edge.

FIDO2 authentication timeout configuration

Starting with version 2601, Citrix Workspace app for Linux provides a configuration option to control the browser-based FIDO2 authentication timeout.

To configure, open `/opt/Citrix/ICAClient/config/AuthManConfig.xml` and set the timeout (in seconds) using `FIDO2AuthTimeout`:

```
<!-- FIDO2AuthTimeout - Authentication timeout in seconds (default: 60, max: 180) -->
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<FIDO2AuthTimeout>60</FIDO2AuthTimeout>
```

> **Note:**
>
> Set the timeout to a value between 60 and 180 seconds, as required.

Identity Provider (IDP) logout on Workspace (WSP) inactivity timeout

Starting with version 2601, Citrix Workspace app for Linux adds support for logging out of the Identity Provider (IDP) during user logoff and when a Workspace (WSP) inactivity timeout occurs. This opt-in feature helps ensure complete session termination across the authentication chain while preserving existing logout behavior unless enabled.

To configure this feature, edit `AuthManConfig.xml` located at `/opt/Citrix/ICAClient/config/AuthManConfig.xml`.

Default setting:

```
<!-- EnableChainedLogoffOnTimeout - true, false -->
<EnableChainedLogoffOnTimeout>false</EnableChainedLogoffOnTimeout>
```

To enable the feature,

```
<!-- EnableChainedLogoffOnTimeout - true, false -->
<EnableChainedLogoffOnTimeout>true</EnableChainedLogoffOnTimeout>
```

> **Note:**
>
> This feature is disabled by default. Contact your admin to enable this feature if needed.

Entra ID single sign-on for NetScaler Gateway stores

Starting with Citrix Workspace app 2604 for Linux, you can configure Entra ID single sign-on (SSO) for on-premises stores that are accessed through a NetScaler Gateway. This enhancement lets users launch virtual apps and desktops without re-entering their Entra ID credentials.

Install dependencies

Install the following packages if they are not already present on the endpoint.

For Ubuntu or Debian:

```
sudo apt install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

For RHEL or Fedora:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sudo dnf install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

For openSUSE:

```
sudo zypper install gnome-keyring libsecret-1-0 libwebkit2gtk-4.0-37
```

Configure Entra ID SSO

All Entra ID SSO settings are available in `/opt/Citrix/ICAClient/config/AuthManConfig.xml`.

Edit the file with root privileges:

```
sudo vi /opt/Citrix/ICAClient/config/AuthManConfig.xml
```

Configure the following settings as needed:

- `PersistCookies`: Persists Entra ID SSO cookies in memory when the authentication window closes. The default value is **`false`**.
- `AADSSOEnabled`: Enables or disables Entra ID SSO. The default value is **`true`**.
- `AADSSOWithFido2AuthenticationEnabled`: Uses the system browser for authentication instead of the built-in WebKitGTK window. The default value is **`false`**.
- `SharedAuthContextEnabled`: Persists Entra ID cookies across app launches in the same user session. The default value is **`false`**.
- `EnableBypassGateway`: Reuses the AAD-issued gateway cookie (`NSC_AAAC`) to bypass interactive NetScaler Gateway authentication. The default value is **`false`**.

Example:

```
<PersistCookies>true</PersistCookies>

<key>AADSSOEnabled</key>
<value>true</value>

<key>AADSSOWithFido2AuthenticationEnabled</key>
<value>false</value>

<key>SharedAuthContextEnabled</key>
<value>true</value>

<key>EnableBypassGateway</key>
<value>true</value>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How it works

Self-Service UI Launch Citrix Workspace app for Linux from the application menu or by running:

```
/opt/Citrix/ICAClient/selfservice
```

Use the following workflow:

1. Sign in to the NetScaler Gateway store.
2. Launch an application or desktop.
3. Complete Entra ID authentication in the WebKitGTK window the first time that you launch a resource.
4. Start the session without entering credentials again on the VDA.

When `PersistCookies` is **`true`**, Citrix Workspace app reuses the Entra ID session for subsequent launches in the same session. When `EnableBypassGateway` is **`true`**, the NetScaler Gateway authentication step is also skipped by reusing the `NSC_AAAC` cookie that was obtained during the Entra ID sign-in flow.

Storebrowse `storebrowse` provides the same Entra ID SSO experience from the command line.

Use the following workflow:

1. Add the NetScaler Gateway store:

   ```
   /opt/Citrix/ICAClient/util/storebrowse --addstore "https://gateway.example.com"
   ```

2. List the configured stores:

   ```
   /opt/Citrix/ICAClient/util/storebrowse --liststore
   ```

3. List the published applications:

   ```
   /opt/Citrix/ICAClient/util/storebrowse -E "https://gateway.example.com/Citrix/Store/discovery"
   ```

4. Launch an application:

   ```
   /opt/Citrix/ICAClient/util/storebrowse -L "Citrix.MPS.Desktop.Notepad" "https://gateway.example.com/Citrix/Store/discovery"
   ```

5. Complete Entra ID authentication when the authentication window appears on the first launch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the first launch, an Entra ID authentication window appears. After the user authenticates, Citrix Workspace app acquires the SSO token and embeds it in the session so that the VDA does not prompt for credentials. If `EnableBypassGateway` is **`true`**, the gateway authentication step is skipped by reusing the `NSC_AAAC` cookie.

Shared workstation mode For kiosk or shared Linux thin-client deployments, enable shared user mode:

```
1 /opt/Citrix/ICAClient/util/storebrowse -c SharedUserMode=True
```

Authentication methods

Built-in window By default, Citrix Workspace app uses a WebKitGTK window for Entra ID authentication. No additional software is required beyond the standard dependencies. When `SharedAuthContextEnabled` is **`true`**, the built-in window uses the same cookie context as the store webview. Cookies are stored in a persistent SQLite database that WebKitGTK manages. Each authentication attempt uses a 30-second timeout.

System browser Set `AADSSOWithFido2AuthenticationEnabled`=**`true`** to use the system browser
instead of the built-in window. The browser redirects back to Citrix Workspace app through the `ctxaadsso://` protocol handler.

Use the system browser in the following cases:

- Your organization requires FIDO2 security key authentication.
- Conditional Access policies require a specific browser.
- Browser-based smart card or certificate authentication is required.

Supported browsers are Google Chrome, Chromium, Mozilla Firefox, and Microsoft Edge for Linux. Citrix Workspace app registers the `ctxaadsso://` protocol handler automatically during installation by using the desktop file at `/opt/Citrix/ICAClient/desktop/ctxaadsso.desktop`.

Connectivity

September 13, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connection

Configure connections

On devices with limited processing power or where limited bandwidth is available, there's a trade-off between performance and functionality. Users and administrators can choose an acceptable mixture of rich functionality and interactive performance. Making one or more of these changes, often on the server not the user device, can reduce the bandwidth that a connection requires and can improve performance:

- **Enable SpeedScreen Latency Reduction** - The SpeedScreen Latency Reduction improves performance over high latency connections. For this improvement, an instant feedback is provided to the user in response to typed data or mouse clicks. Use the SpeedScreen Latency Reduction Manager to enable this feature on the server. By default, in Citrix Workspace app, this feature is disabled for a keyboard. This feature is only enabled for the mouse on high latency connections. For more information, see the Citrix Workspace app for Linux OEM's reference guide.
- **Enable data compression** - Data compression reduces the amount of data transferred across the connection. This configuration requires more processor resources to compress and decompress the data, but it can increase performance over low-bandwidth connections. Use the **Citrix Audio Quality and Image Compression** policy settings to enable this feature.
- **Reduce the window size** - Change the window size to the minimum that is comfortable. On the farm set the Session Options.
- **Reduce the number of colors** - Reduce the number of colors to 256. On the Citrix Virtual Apps and Desktops™ or Citrix DaaS site, set the Session Options.
- **Reduce sound quality** - If audio mapping is enabled, reduce the sound quality to the minimum setting using the Citrix Audio quality policy setting.

For information about troubleshooting, see Connections in the troubleshooting section.

Automatic reconnection

This topic describes the HDX™ Broadcast auto-client reconnection feature. Citrix recommends that you use this feature with the HDX Broadcast session reliability feature.

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the HDX Broadcast auto-client reconnection feature, Citrix Workspace app for Linux can detect unintended disconnections of sessions and reconnect users to the affected sessions automatically.

When this feature is enabled on the server, users do not have to reconnect manually to continue working. Citrix Workspace attempts to reconnect to the session a set number of times until there is a successful reconnection or the user cancels the reconnection attempts. If user authentication is required,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a dialog box requesting credentials appears to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off. Users can reconnect only to disconnected sessions.

By default, Citrix Workspace app for Linux waits 30 seconds before attempting to reconnect to a disconnected session and attempts to reconnect to that session three times.

When connecting through an AccessGateway, ACR is not available. To protect against network dropouts, ensure that Session Reliability is enabled on the server, client, and configured on the AccessGateway.

For instructions on configuring HDX Broadcast auto-client reconnection, see your Citrix Virtual Apps and Desktops documentation.

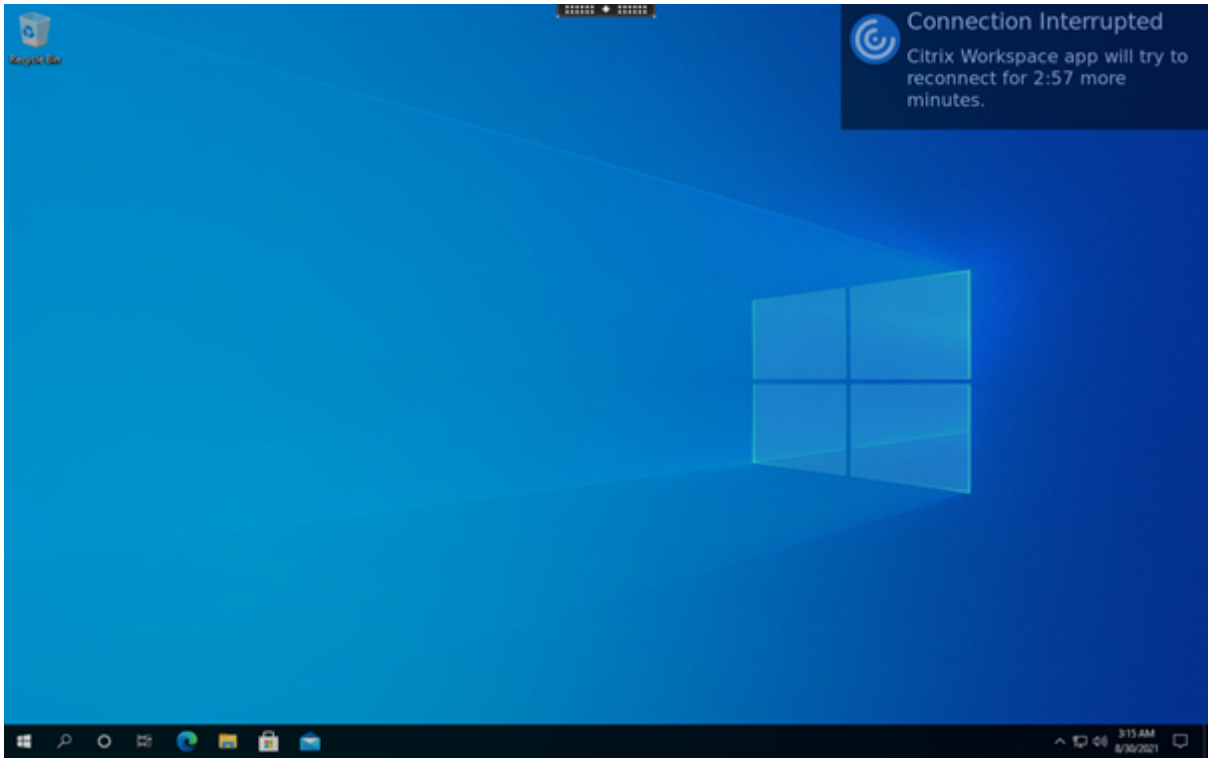
Session reliability

This topic describes the HDX Broadcast session reliability feature, which is enabled by default.

With HDX Broadcast session reliability, users continue to see a published application's window if the connection to the application experiences an interruption. For example, wireless users enter in a tunnel might lose their connection when they enter the tunnel. And, regain the connection when they emerge on the other side. During the downtime, key presses and all other interactions of a user are stored. Also, the app appears frozen. When the connection is re-established, these interactions are replayed into the application.

You can now see screen changes when the session reliability begins. With this enhancement, the session window is grayed out and a countdown timer displays the time until the next reconnection attempt occurs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Tip**
>
> You can alter the grayscale brightness used for an inactive session using the **Reconnection UI transparency level** policy. By default, this value is set to 80. The maximum value can't exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

When a session successfully reconnects, the countdown notification message disappears. You can interact with the desktop as usual.

Starting with the 2109 version, the session reliability notification is enabled by default.

To disable this enhancement:

1. Navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file.
2. In the [WFClient] section, modify the following setting:

```
SRNotification=False
```

> **Note:**
>
> This feature is supported only for Citrix Virtual Desktops.

When auto-client reconnection and session reliability are configured, session reliability takes precedence if there is a connection problem. Session reliability attempts to re-establish a connection to the existing session. It might take up to 25 seconds to detect a connection problem. And then takes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a configurable period (the default is 180 seconds) to attempt the reconnection. If session reliability fails to reconnect, then auto-client reconnect attempts to reconnect.

If HDX Broadcast session reliability is enabled, the default port used for session communication switches from 1494 to 2598.

Citrix Workspace users cannot override the server settings.

> **Important:**
>
> HDX Broadcast session reliability requires that another feature, the Common Gateway Protocol, is enabled (using policy settings) on the server. Disabling the Common Gateway Protocol also disables HDX Broadcast session reliability.

Using session reliability policies

The session reliability connections policy setting enables session reliability.

The session reliability timeout policy setting has a default of 180 seconds, or three minutes. If needed, you can extend the time session reliability to keep a session open. It does not prompt you for reauthentication.

> **Tip**
>
> As you extend the amount of time a session is kept open, you might get distracted and walk away from your device. This situation potentially leaves the session accessible to unauthorized users.

Incoming session reliability connections use port 2598. This default port is used unless you change the port number that is defined in the session reliability port number policy setting.

For information on configuring session reliability policies, see Session reliability policy settings.

> **Note:**
>
> Session reliability is enabled by default at the server. To disable this feature, configure the policy managed by the server.

HDX™ and Multimedia

September 7, 2025

This section describes the following:

- Graphics and display

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Audio
- Multimedia
- Browser content redirection
- Optimization for Microsoft Teams
- Server-client content redirection
- ICA Settings Reference
- Bidirectional content redirection

Graphics and display

March 2, 2026

Pinning multi-monitor screen layout

Starting with Version 2103, you can save the selection for multi-monitor screen layout. The layout is how a desktop session is displayed. Pinning helps to relaunch a session with the selected layout, resulting in an optimized user experience.

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

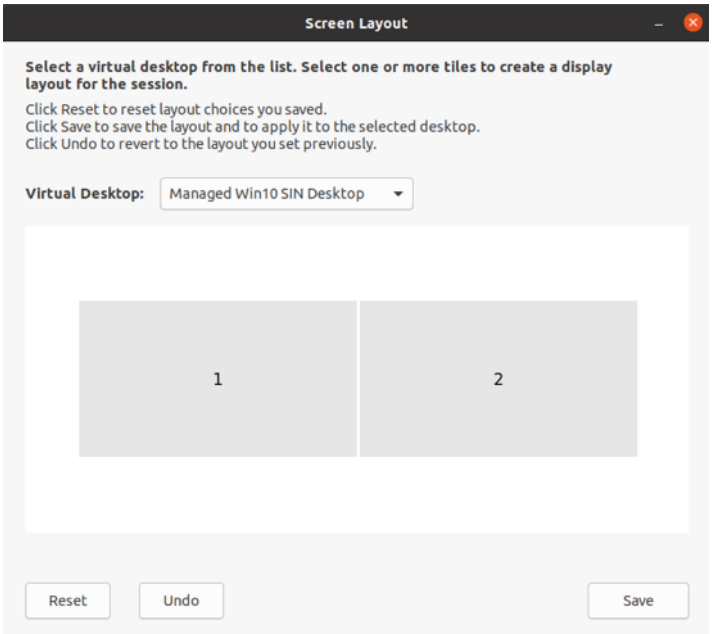
```
1       <key>ScreenPinEnabled</key>
2       <value>true</value>
```

Only after adding the preceding key, you can see the **Screen Layout** option in the **App indicator** icon. For more information about the app indicator icon, see App indicator icon.

To select the screen layout, click the app indicator icon in the taskbar, and select **Screen Layout**. The **Screen Layout** dialog appears.

Alternately, you can launch the **Screen Layout** dialog by pressing **Ctrl+m** keys when on the self-service window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select a virtual desktop from the drop-down menu. The layout selection is applied only to the desktop that you select.

Select one or more tiles to form a rectangular selection for the layout. The session then appears as per the layout selection.

Limitations:

- Enabling screen pinning disables the save layout feature in a session.
- This feature is applicable only on desktops that are marked as favorite.

Screen pinning in custom web stores

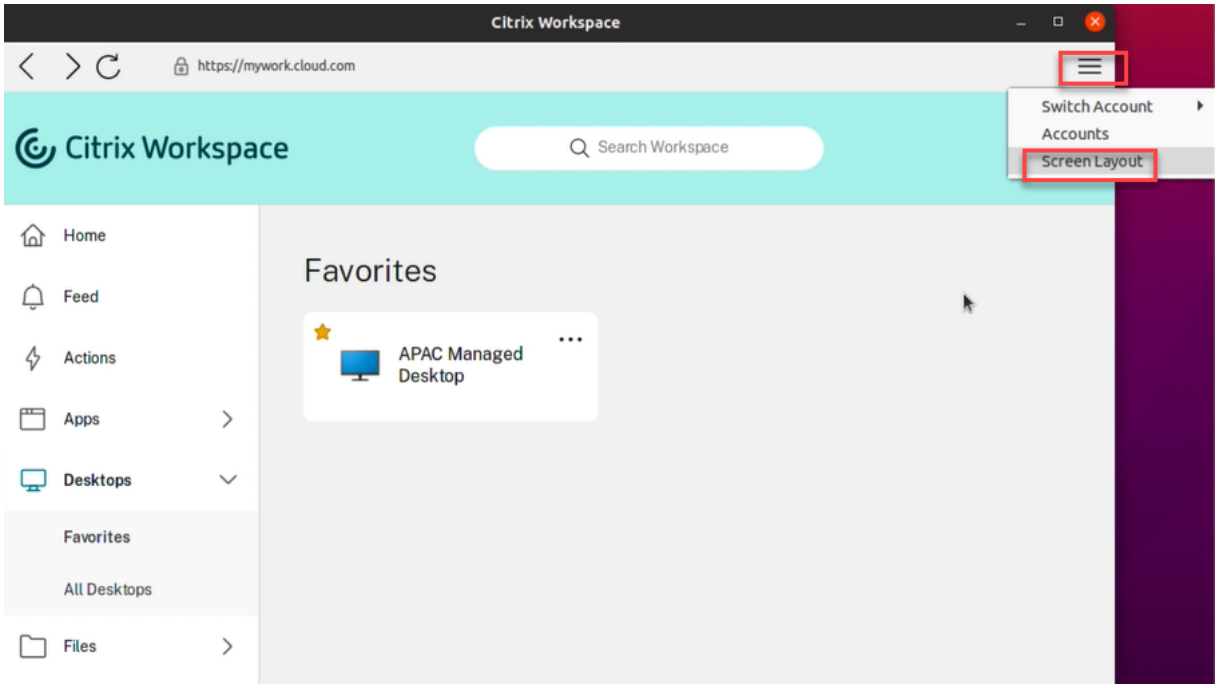
Starting with Citrix Workspace app version 2309, the screen pinning in custom web stores allows you to save the selection for multi-monitor screen layout in custom web stores.

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

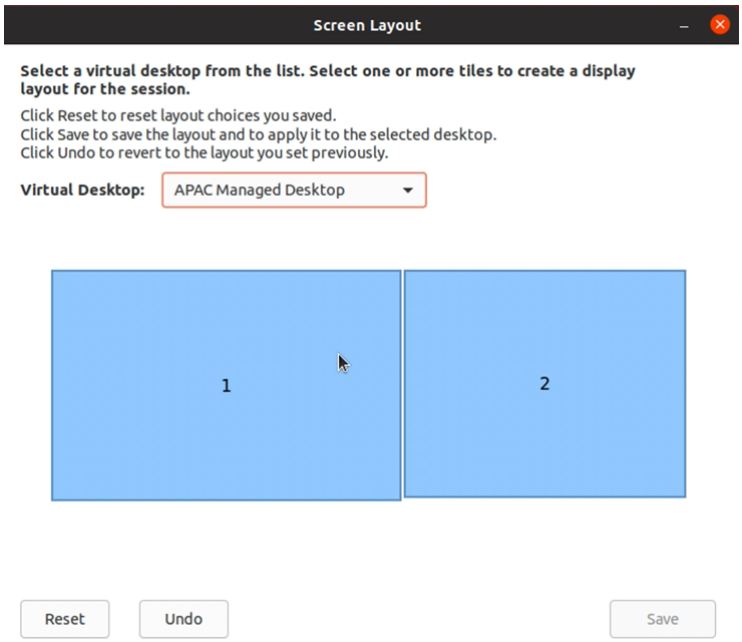
```
<key>ScreenPinEnabled</key>
<value>true</value>
```

Only after adding the preceding key, you can see the **Screen Layout** option in the Citrix Workspace app menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To select the screen layout, select **Screen Layout** in the Citrix Workspace app menu. The **Screen Layout** dialog box appears.



Select a virtual desktop from the drop-down menu. The layout selection is applied only to the desktop that you select.

Select one or more tiles to form a rectangular selection for the layout. The session then appears as per the layout selection.

Limitations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enabling screen pinning disables the save layout feature in a session.
- This feature is applicable only on desktops that are marked as favorite.

Support for DPI matching

The display resolution and DPI scale values set in the Citrix Workspace app match to the corresponding values in the virtual apps and desktops session. You can set the required scale value in the Linux client, and the scaling of the VDA session is updated automatically.

DPI scaling is mostly used with large-size and high-resolution monitors. This feature helps to display the following in a size that can be viewed comfortably:

- Applications
- Text
- Images
- Other graphical elements

> **Note:**
>
> The DPI matching feature supports only `GNOME`, `KDE`, and `Xfce` desktop environments.

This feature is disabled by default. You can enable this feature using the command-line interface or GUI.

Command-line interface

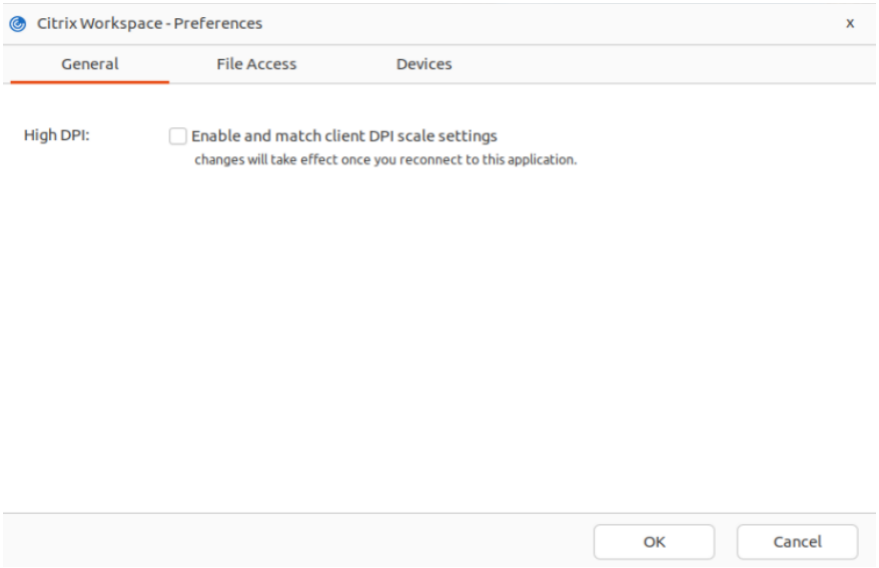
1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Go to the [WFClient] section and set the following entry:

```
1 DPIMatchingEnabled=TRUE
```

GUI

1. Go to **Menu** > **Preferences**. The **Citrix Workspace-Preferences** dialog appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Navigate to **General** tab.
3. Select the **Enable and match client DPI scale settings** checkbox.
4. Click **OK**.

> **Note:**
>
> The updated DPI scale settings take effect after you reconnect to Citrix Workspace app.

Limitation:

The DPI matching feature doesn't support the following:

- Fractional scaling on the client side.
- Desktop session that is extended to more than one monitor and when those monitors have different DPIs configured.

Multi-monitor layout persistence

This feature retains the session monitor layout information across endpoints. The sessions appear on the same monitor as configured.

Prerequisite:

This feature requires the following:

- StoreFront v3.15 or later.
- If `.ICAClient` is already present in the home folder of the current user:

  Delete the All_Regions.ini file

© 1997–2026 Citrix Systems, Inc. All rights reserved.

or

To retain the `All_Regions.ini` file, add the following lines at the end of the [Client Engine\Application Launching] section:

SubscriptionUrl=

PreferredWindowsBounds=

PreferredMonitors=

PreferredWindowState=

SaveMultiMonitorPref=

If the `.ICAClient` folder is not present then it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the feature is retained.

Use cases

- Launch a session on any monitor in windowed mode and save the setting.
  When you relaunch the session, it appears in the same mode, on the same monitor, and in the same position.
- Launch a session on any monitor in full-screen mode and save the setting.
  When you relaunch the session, it appears in full-screen mode on the same monitor.
- Stretch and span a session in windowed mode across multiple monitors and then switch to full-screen mode. The session continues in full-screen across all monitors. When you relaunch the session, it appears in full-screen mode, spanning across all monitors.

> **Notes:**
>
> - The layout is overwritten with every save, and the layout is saved only on the active StoreFront.
> - f you launch extra desktop sessions from the same StoreFront on different monitors, saving the layout in one session saves the layout information of all the sessions.

Using Citrix Virtual Desktops™ on dual monitor

1. Select the Desktop Viewer and click the down arrow.
2. Select **Window**.
3. Drag the Citrix Virtual Desktops screen between the two monitors. Verify that about half the screen is present in each monitor.
4. From the Citrix Virtual Desktop toolbar, select **Full-screen**.

   The screen extends to both the monitors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhancement to multiple monitors

When using multiple monitors, if you dock or undock your primary endpoint machine from a docking station, the session extends to the monitors automatically with the updated layout. Also, when you start a session with multiple monitors, the session is extended to those monitors. If you add or remove monitors, the session is adapted to the newly available screens.

> **Note:**
>
> This feature supports a primary monitor and one secondary monitor only.

By default, this feature is disabled.

Perform the following to enable this feature:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Go to the `[WFClient]` section.
3. Add the following entry:

```
1 MultiMonitorPnPEnabled=True
```

> **Note:**
>
> If you are using the 4K resolution monitor, during the multi-monitor plug and play, set `MonitorLayoutEventTimeout=4` on the `$HOME/.ICAClient/wfclient.ini` file in the `[WFClient]` section.

Limitation:

- When you change the monitor layout on your local machine after a session is started, the monitor layout inside the session might not change accordingly. [HDX-58023]

Fixed issue:

- When you manually switch the session from *Window* mode to *Full-screen* mode and then connect a second monitor, the session might fail to display correctly on the second monitor. [HDX-55370]

ICA-to-X proxy

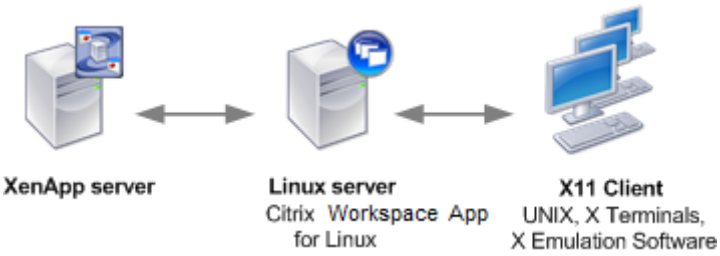
You can use a workstation running Citrix Workspace app as a server and redirect the output to another X11-capable device. You might want to do this task to deliver Microsoft Windows applications to X terminals or to UNIX workstations for which Citrix Workspace app isn't available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix Workspace app software is available for many X devices, and installing the software on these devices is the preferred solution in these cases. Running Citrix Workspace app in this way, as an ICA-to-X proxy, is also referred to as server-side ICA.

When you run Citrix Workspace app, you can think of it as an ICA-to-X11 converter that directs the X11 output to your local Linux desktop. However, you can redirect the output to another X11 display. You can run extra copies of Citrix Workspace app simultaneously on one system. In this case, each Citrix Workspace app sends its output to a different device.

This graphic shows a system with Citrix Workspace app for Linux set up as an ICA-to-X proxy:



To set up this type of system, you need a Linux server to act as the ICA-to-X11 proxy:

- If you have X terminals already, you can run Citrix Workspace app on the Linux server that usually supplies the X applications to the X terminals.
- If you want to deploy UNIX workstations for which Citrix Workspace app isn't available, you need an extra server to act as the proxy. This server can be a PC running Linux.

Applications are supplied to the final device using X11, using the capabilities of the ICA protocol. By default, you can use drive mapping only to access the drives on the proxy. This setting isn't a problem if you're using X terminals (which usually do not have local drives). If you're delivering applications to other UNIX workstations, you can either:

- NFS mounts the local UNIX workstation on the workstation acting as the proxy, then point a client drive map at the NFS mount point on the proxy.
- Use an NFS-to-SMB proxy such as SAMBA, or an NFS client on the server such as Microsoft Services for UNIX.

Some features aren't passed to the final device:

- USB redirection
- Smart card redirection
- COM port redirection
- Audio isn't delivered to the X11 device, even if the server acting as a proxy supports audio.
- Client printers aren't passed through to the X11 device. You access the UNIX printer from the server manually using LPD printing, or use a network printer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Redirection of multimedia input isn't supported. Because it requires a webcam on the machine that runs Citrix Workspace app, where the server acts as a proxy. However, redirection of multimedia output supports when `GStreamer` installed on the server acting as a proxy (untested).

To start Citrix Workspace app with server-side ICA from an X terminal or a UNIX workstation:

1. Use ssh or telnet to connect to the device acting as the proxy.
2. In a shell on the proxy device, set the **DISPLAY** environment variable to the local device. For example, in a C shell, type:

   ```
   setenv DISPLAY <local:0>
   ```

   > **Note:**
   >
   > If you use the command `ssh -X` to connect to the device acting as the proxy, you do not need to set the **DISPLAY** environment variable.

3. At a command prompt on the local device, type xhost <proxy server name>
4. Verify whether Citrix Workspace app is installed in the default installation directory. If not installed, verify that the environment variable ICAROOT is set to point to the actual installation directory.
5. Locate the directory where Citrix Workspace app is installed. At a command prompt, type `selfservice &`.

Font

ClearType font smoothing

ClearType font smoothing improves the quality of displayed fonts beyond the available quality through:

- traditional font smoothing or,
- anti-aliasing.

ClearType font smoothing is also known as subpixel font rendering. You can turn this feature on or off.

You can also specify the type of smoothing by doing the following:

1. Navigate to the [WFClient] section of the appropriate configuration file.
2. Edit the following setting:

   FontSmoothingType=number

   Where the number can take one of the following values:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Value	Behavior
0	The local preference on the device is used. The **FontSmoothingTypePref** setting defines this value.
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing

Both standard smoothing and ClearType smoothing can increase Citrix Workspace app's bandwidth requirements.

> **Important:**
>
> The server can configure `FontSmoothingType` through the `ICA` file. This value takes precedence over the value set in [WFClient].

If the server sets the value to 0, the following setting in the [WFClient] determines the local preference: FontSmoothingTypePref=number

Where a number can take one of the following values:

Value	Behavior
0	No smoothing
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing (default)

`Xcapture`

The Citrix Workspace app package includes a helper application, `Xcapture`. This application assists the exchange of graphical data between the server clipboard and non-ICCCM-compliant X Window applications on the X desktop. Users can use `Xcapture` to:

- Capture dialog boxes or screen areas and copy them between the user device desktop (including non-ICCCM-compliant applications) and an application running in a connection window
- Copy graphics between a connection window and X graphics manipulation utilities `xmag` or `xv`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To start `Xcapture` from the command-line:

At the command prompt, type `/opt/Citrix/ICAClient/util/xcapture` and press ENTER (where `/opt/Citrix/ICAClient` is the directory in which you installed Citrix Workspace app).

To copy from the user device desktop:

1. From the `Xcapture` dialog box, click **From Screen**. The cursor changes to a crosshair.
2. Choose from the following tasks:
    - Select a window. Move the cursor over the window that you want to copy and click the middle mouse button.
    - Select a region. Hold down the left mouse button and drag the cursor to select the area you want to copy.
    - Cancel the selection. Click the right mouse button. While dragging, you can cancel the selection by clicking the right button before releasing the middle or left mouse button.
3. From the `Xcapture` dialog box, click **To ICA**. The `Xcapture` button changes color to show that it is processing the information.
4. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from xv to an application in a connection window:

1. From xv, copy the information.
2. From the `Xcapture` dialog box, click From XV and then click To ICA. The `Xcapture` button changes color to show that it is processing the information.
3. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from an application in the connection window to xv:

1. From the application in a connection window, copy the information.
2. From the `Xcapture` dialog box, click From ICA and then click To XV. The `Xcapture` button changes color to show that it is processing the information.
3. When the transfer is complete, paste the information into xv.

UI option to manage monitor plug and play feature

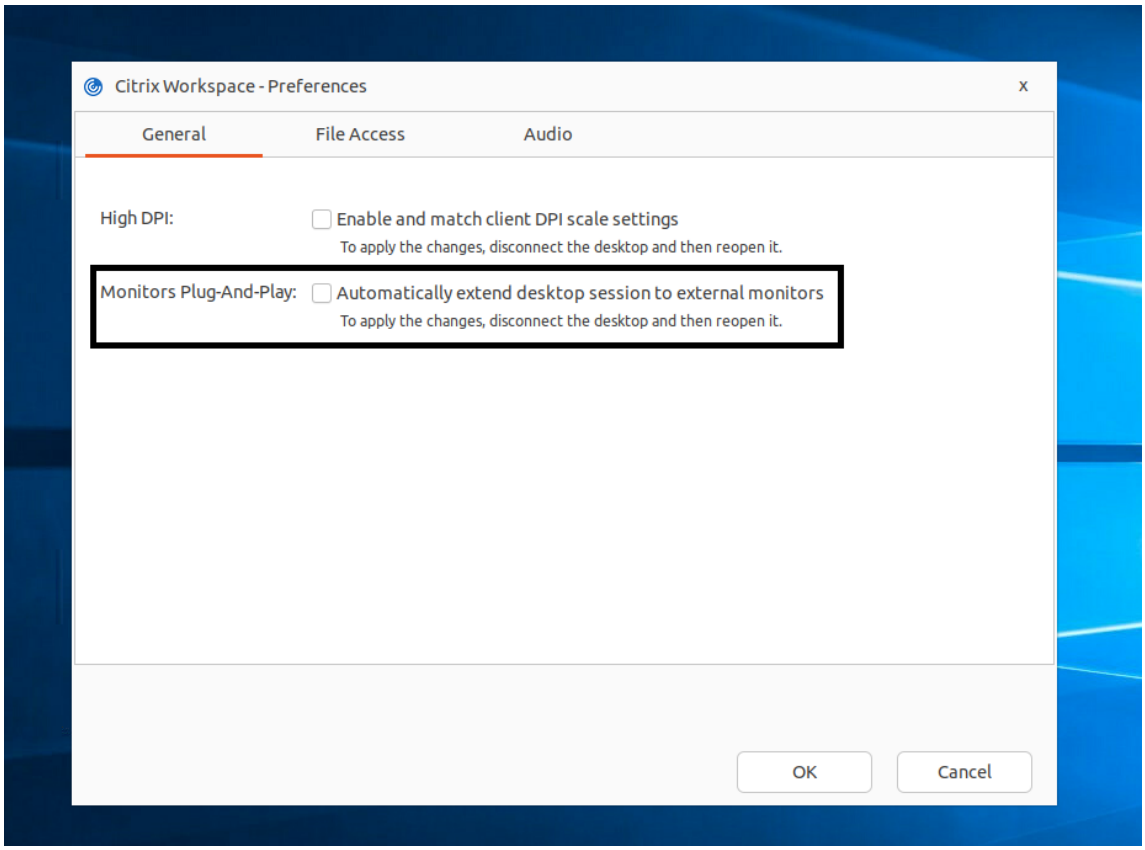
Previously, you had to enter `MultiMonitorPnPEnabled=True` in the [WFClient] section of the `$HOME/.ICAClient/wfclient.ini` file to enable the monitor plug and play feature.

Starting with the 2405 version, a new UI option, the **Automatically extend desktop session to external monitors** checkbox is available to enable or disable the monitor plug and play feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the **Automatically extend desktop session to external monitors** checkbox is not selected. To select this option, do the following:

1. Click **Desktop viewer** > **Preferences** > **General**.
2. Select the **Automatically extend desktop session to external monitors** checkbox.



3. Click **OK**. The change will take effect from the next-time you open the desktop session.

> **Note:**
>
> If you have disabled the feature through `All_Regions.ini` per machine, the **Automatically extend desktop session to external monitors** checkbox isn't visible.

Performance optimization for graphics

Citrix Workspace™ app 2408 version supports OpenGL library that improves the performance of graphics usage within an HDX session.

This feature is enabled by default starting with release 2503. To disable this feature, do the following:

1. Navigate to the $HOME/.ICAClient/wfclient.ini file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Go to the [Thinwire3.0] section and add the following entry:

```
OpenGLEnabled=False
```

Note

- To enable this feature, the operating system must support OpenGL 4.6.
- This feature is not supported on Linux based on Arm64 architectures.
- This feature is applicable only for the virtual desktop session.
- NVIDIA GPUs are not supported in this configuration.

Support for H.264 hardware decoding for seamless apps

Starting with the 2508 version, Citrix Workspace app for Linux supports H.264 hardware decoding for seamless apps, utilizing the GPU on the client device. This feature is enabled by default. To disable this feature, do the following:

1. Navigate to the $HOME/.ICAClient/wfclient.ini folder.
2. Go to the [Thinwire3.0] section.
3. Add the following entry:

```
OpenGLEnabled=False
```

Support for H.264 hardware decoding

Starting with the 2408 version, Citrix Workspace app for Linux supports the GPU that can be used for H.264 decoding wherever it's available at the client. H.264 video codec must be supported and enabled on both the VDA and Citrix Workspace app.

Prerequisites for H.264

- VDA 7.16 or later
- Use any of the following GPUs in VDA:
  - NVIDIA Maxwell generation GPU or later
  - Intel 6th generation GPU or later
  - AMD Raven generation GPU or later
- Enable the **Optimize for 3D graphics workload policy** on the VDA.
- Enable the **Use hardware encoding for video codec policy** on the VDA.

This feature is set to be enabled by default starting with release 2503.

To disable this feature, complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Go to the [Thinwire3.0] section.
3. Add the following entry:

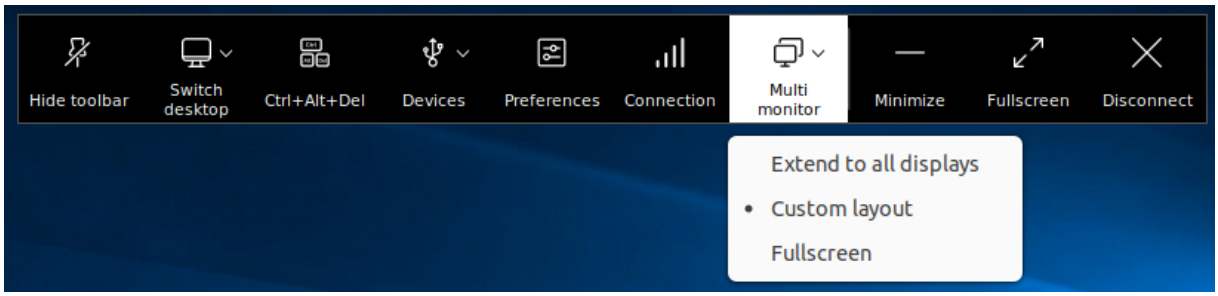
For H.264 hardware decoding:

```
OpenGLEnabled=False
```

> **Note**
>
> If hardware decoding acceleration is enabled, then:
>
> - In the window mode, the maximum window size supported by the client is 4096x4096 (approximately 4K).
> - For some Red Hat operating systems with Intel graphics, you might notice that "Initialized h264 software decoding successfully"printed in `ICAClient.log` after launching a session. In such cases, you need to verify whether the intel-media-driver is installed.

Multi-monitor custom layout

Starting with version 2411, the Multi-Monitor Selector (MMS) allows users to choose which displays to use in full-screen mode for desktop sessions only, not for seamless sessions. A new Multi-Monitor button has been added to the toolbar, which appears only when more than one screen is connected. This feature enhances the flexibility and usability of multi-monitor setups in desktop sessions, providing a more tailored and efficient user experience.



Starting with version 2503, we provide an enhanced multi-monitor experience when using a full-screen session through the Custom Layout feature. Additionally, you can save a monitor layout as per your preference and start a session with the saved layout.

This enhancement ensures a stable Citrix session experience in the following situations:

Unplugging or plugging in monitors:

Unplugging or plugging monitors into the system doesn't affect the stability of your full-screen Citrix session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you unplug a monitor that isn't used by a full-screen Citrix session: If you unplug an external monitor that isn't being used by a full-screen session, the session remains normal and available. The same applies when you plug the monitor back in.

When you unplug a monitor that is used by a full-screen Citrix session: When you unplug a monitor that is being used by a full-screen session, the session transfers to the next available monitor without interrupting the session progress. Once you plug the monitor back in, the session automatically restores to its previous state.

When you unplug a monitor when a full-screen Citrix session spans across more than one monitor: If your full-screen session spans across multiple monitors, unplugging a monitor causes the session to adjust to the remaining monitor(s), adapting their layout. When you plug the monitor back in, the session automatically restores back to its previous state.

Disconnecting and reconnecting monitors:

When your session monitor is disconnected due to network issues or other reasons, the full-screen session transfers to the next available monitor without affecting your work. Once the monitor is reconnected, the session automatically restores back to its previous state.

Prerequisites

The multi-monitor layout selection feature is enabled by default starting with Citrix Workspace app for Linux version 2505. To disable the multi-monitor layout selection feature:

1. Open the `$HOME/.ICAClient/wfclient.ini` file.
2. Navigate to the `[WFClient]` section.
3. Add the following entry:

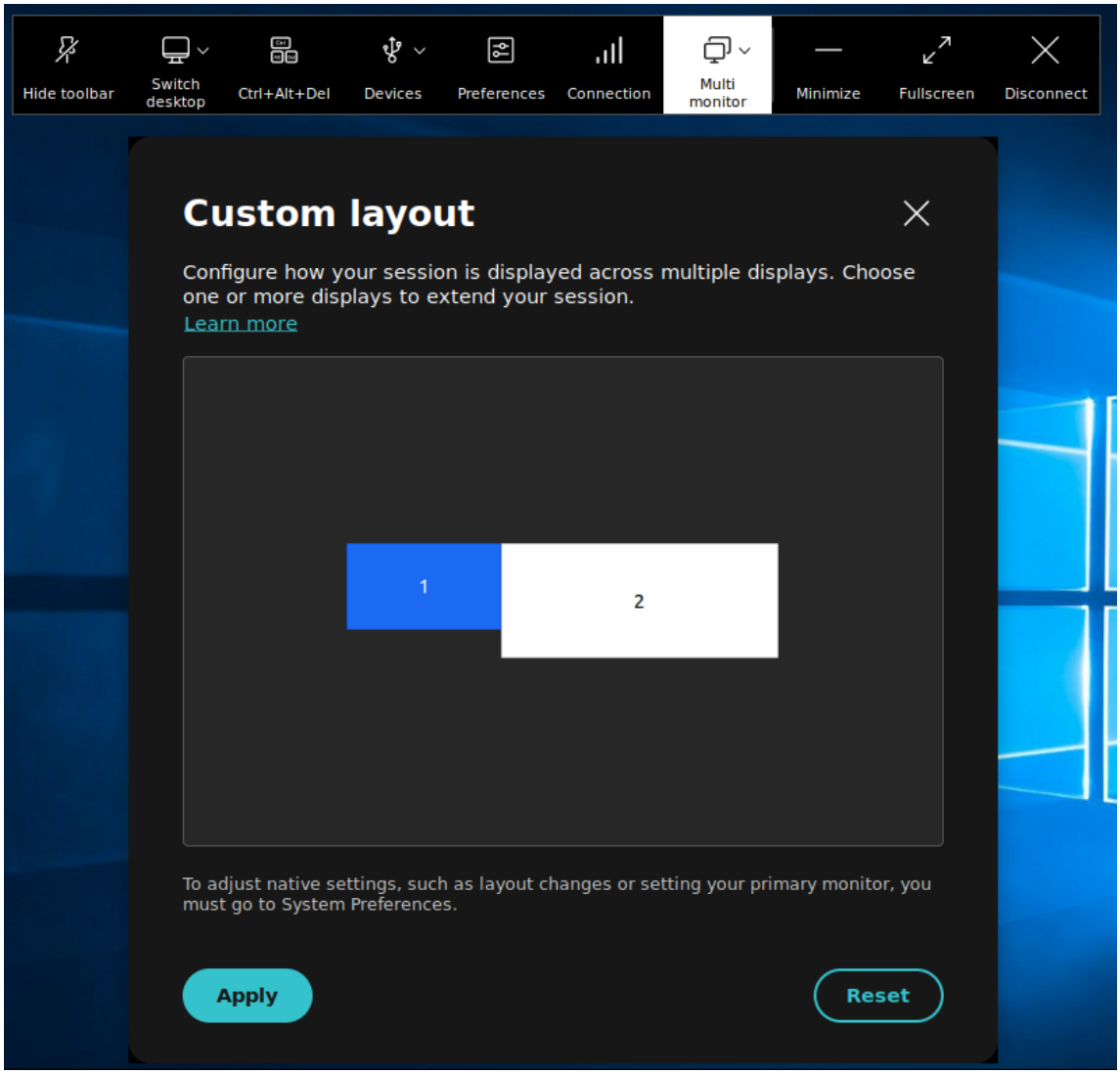
```
MultiMonitorSelectionEnabled=False
```

Multi-monitor menu options

The toolbar button includes three dropdown menu options for desktop sessions in full-screen mode:

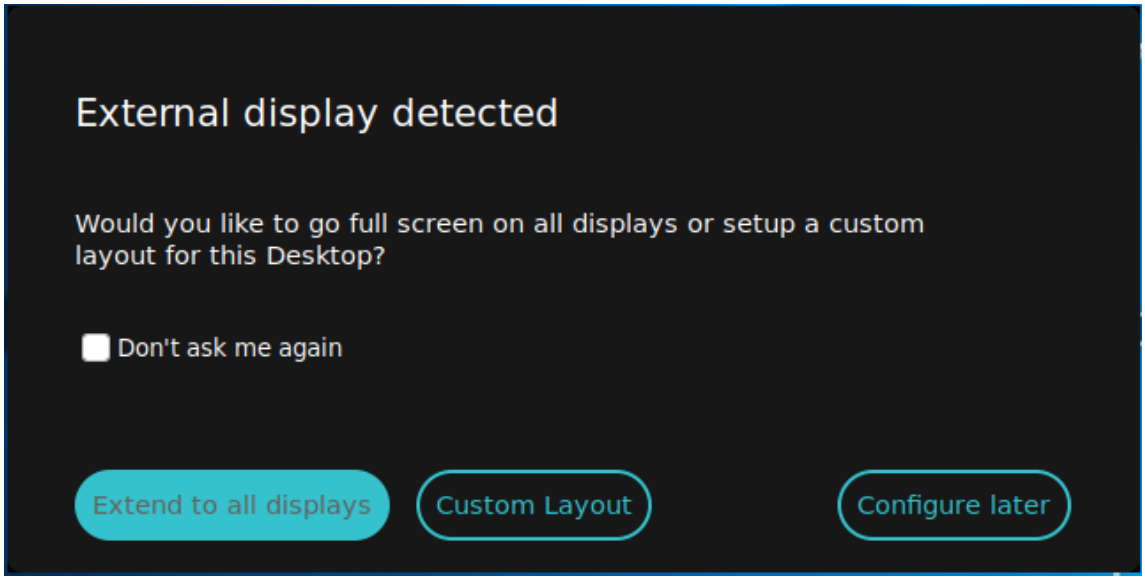
1. **Extend to All Displays**: The session switches to full-screen mode on all connected screens.
2. **Custom Layout**: This option opens a custom monitor selector displaying the layout of the Linux system. Users can click on the rectangles in the selector to choose which screens to use and then click **Apply**. The session then uses the selected screens in full-screen mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **Fullscreen**: The session switches to full-screen mode on the current single display where the toolbar is located or where the button is clicked.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When a new monitor is plugged in, a notification appears for the user to make a selection. Users can select the **Don't ask me again** checkbox to mute this notification.

Starting with 2503 release, to save a monitor layout, do the following:

1. Click the **Multi-monitor option** from the toolbar. For more information, see Multi-monitor menu options.
2. Select the **Don't ask me again** checkbox and then click **Extend to all displays** or **Custom Layout**.

The monitor layout is saved.

The user-customized layout is used first when the session is restarted or the monitor layout is changed.

- If you select **Extend to all displays**, the session always extends to all monitors in Fullscreen mode.
- If you select **Custom Layout**, the session extends to the selected monitors.

Audio

September 7, 2026

Client audio mapping enables applications that run on the Citrix Virtual Apps and Desktops or Citrix DaaS server to play sounds and record audio through a sound device that's installed on the user device. You can configure client audio mapping using policies. For more information, see the Citrix Virtual Apps and Desktops documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for audio recording

Starting with version 2212, the audio recording feature is enabled by default. The devices to record audio appear when a session starts.

To disable this feature, set the value for `AllowAudioInput` to *False* in the `wfclient.ini` file.

> **Note:**
>
> - The **Mic and Webcam** option in the **Preferences** dialog is disabled by default. For information on how to enable the mic and webcam, see Preferences.

Support for multiple audio devices

Citrix Workspace app for Linux supports multiple audio devices and redirects them to a session. Starting with version 2212, this feature is enabled by default.

With this feature:

- The PulseAudio library is used to access the audio devices, and multiple devices are supported.
- Multiple applications can use the audio devices at the same time.
- All local audio devices are displayed by name in the session and are available for selection. You can select a specific device or use the client's default device, which updates dynamically.
- Sessions update automatically when you plug in or unplug audio devices.

Known limitations:

- When you launch a session as the root user, PulseAudio might refuse the connection, and the session falls back to a single audio device. In this case, only one speaker and one microphone appear, named **Citrix HDX™ Audio**, which corresponds to the default device on the client side. Bluetooth and HDMI audio devices are not supported in this case.
- On Ubuntu 24.04 and later, HDMI audio devices might not be correctly detected or removed in the VDA when you plug in or unplug the HDMI device while the session is active. This issue occurs because of differences in PipeWire, the default audio engine in Ubuntu 24.04 and later, compared to its predecessor, PulseAudio. This issue affects machines that support both HDMI audio output and built-in speakers at the same time. The behavior is as follows:
  - When an HDMI device is plugged in before session launch, the device is redirected to the VDA as expected.
  - When an HDMI device is plugged in after session launch, the device is not redirected to the VDA correctly.
  - When an HDMI device is unplugged after session launch, the device remains in the VDA and cannot be used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When an HDMI device is unplugged and then reconnected after session launch, the device works as expected in the VDA.

Echo cancellation

Citrix Workspace™ app now supports echo cancellation feature designed to enhance real-time user experiences. The echo cancellation feature supports low quality, medium quality, and adaptive audio. Citrix recommends using adaptive audio for better performance.

> **Note:**
>
> Starting with the 2411 version, the echo cancellation feature is enabled by default.

During real-time user cases, it is recommended to turn on the echo cancellation if the speaker is used instead of the headset.

To disable this feature, do the following:

1. Navigate to the <ICAROOT>/config folder and open the module.ini file.
2. Go to the [ClientAudio] section and update the value of the EnableEchoCancellation parameter as follows:

   EnableEchoCancellation=False

Limitation:

By design, the echo cancellation feature is disabled for high quality audio. For more information on high quality audio, see the Citrix Virtual Apps and Desktops documentation.

Addition of client-side jitter buffer mechanism

Starting with version 2305, Citrix Workspace app ensures clear audio even when the network latency fluctuates. By default, this feature is enabled.

To disable this feature, navigate to the /opt/Citrix/ICAClient/config/module.ini configuration file and edit JitterBufferEnabled=FALSE.

Adaptive audio

Starting with version 2109, Citrix Workspace app supports adaptive audio. With adaptive audio, you don't need to manually configure the audio quality policies on the VDA. Adaptive audio optimizes settings for your environment and replaces obsolete audio compression formats to provide an excellent user experience. Adaptive audio is enabled by default. For more information, see Adaptive audio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with version 2112, adaptive audio works when using User Datagram Protocol (UDP) audio delivery.

Known limitation:

- Adaptive audio requires CPU processors that support Streaming SIMD Extensions (SSE) 4.x. Citrix Workspace app might be closed when adaptive audio is used with the CPU processor that doesn't support SSE 4.x.

Enabling UDP audio

UDP audio can improve the quality of phone calls made over the Internet. It uses UDP instead of TCP.

Starting with Version 2112, adaptive audio works when using UDP audio delivery. Also, from this version, Citrix Workspace app supports the Datagram Transport Layer Security (DTLS) protocol for UDP audio. As a result, you can access the UDP audio through Citrix Gateway. By default, this feature is disabled.

Starting with version 2202, Citrix Workspace app supports UDP audio through Citrix Gateway.

To enable UDP audio:

1. Navigate to the <ICAROOT>/config folder and open the module.ini file.
2. Set the following options in the [ClientAudio] section of module.ini:
    - Set EnableUDPAudio to **True**. By default, this value is set to **False**, which disables UDP audio.
    - Specify the minimum and maximum port numbers for UDP audio traffic using UDPAudioPortLow and UDPAudioPortHigh respectively. By default, ports 16500–16509 are used.
3. Set the following policies on the Domain Delivery Controller™ (DDC):
    - Set **Audio over UDP** to **Allowed**.
    - Set **Audio over UDP real-time transport** to **Enabled**.
4. By default, adaptive audio is enabled on the VDA and supports UDP audio. If you have disabled adaptive audio, set the following policy on the Domain Delivery Controller (DDC):
    - Set **Audio quality** to **Medium**.

    As a result, the resultant audio is of a medium quality, and it can support UDP audio.

To enable UDP audio through Citrix Gateway:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the <ICAROOT>/config folder and open the module.ini file.
2. Go to the [WFClient] section and set the following entry:

   EnableUDPThroughGateway=True

3. Go to the [ClientAudio] section and set the following entry:

   EnableUDPAudio=True

4. Set the following policies on the Domain Delivery Controller (DDC):

   - Set **Audio over UDP** to **Allowed**.
   - Set **Audio over UDP real-time transport** to **Enabled**.

5. By default, adaptive audio is enabled on the VDA and supports UDP audio. If you have disabled adaptive audio, set the following policy on the Domain Delivery Controller (DDC):

   - Set **Audio quality** to **Medium**.

Loss tolerant mode for audio

Starting with the 2402 version, Citrix Workspace app supports loss tolerant mode (EDT lossy) for audio redirection. This feature improves the user experience for real-time streaming when users are connecting through networks with high latency and packet loss. By default, this feature is enabled.

You need to use VDA version 2311 or later. For more information, see Support for audio over loss-tolerant mode in the Citrix Virtual Apps and Desktops documentation.

To disable this feature on Citrix Workspace app for Linux, set the value for EdtUnreliableAllowed to *FALSE* in the $ICAROOT/config/module.ini configuration file, and restart the session for the changes to take effect.

Support for Audio volume synchronization

Starting with the 2402 version, Citrix Workspace app for Linux supports synchronization of audio volume between the VDA and your audio devices. You can now tune the volume using the VDA audio volume slider and have the same volume on your device and the other way around. This feature is enabled by default.

You need to use VDA version 2308 or later. For more information, see Audio volume synchronization in the Citrix Virtual Apps and Desktops documentation.

To disable this feature on Citrix Workspace app for Linux, set the value for EnableVolumeSync to FALSE in the $ICAROOT/config/module.ini configuration file, and restart the session for the changes to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

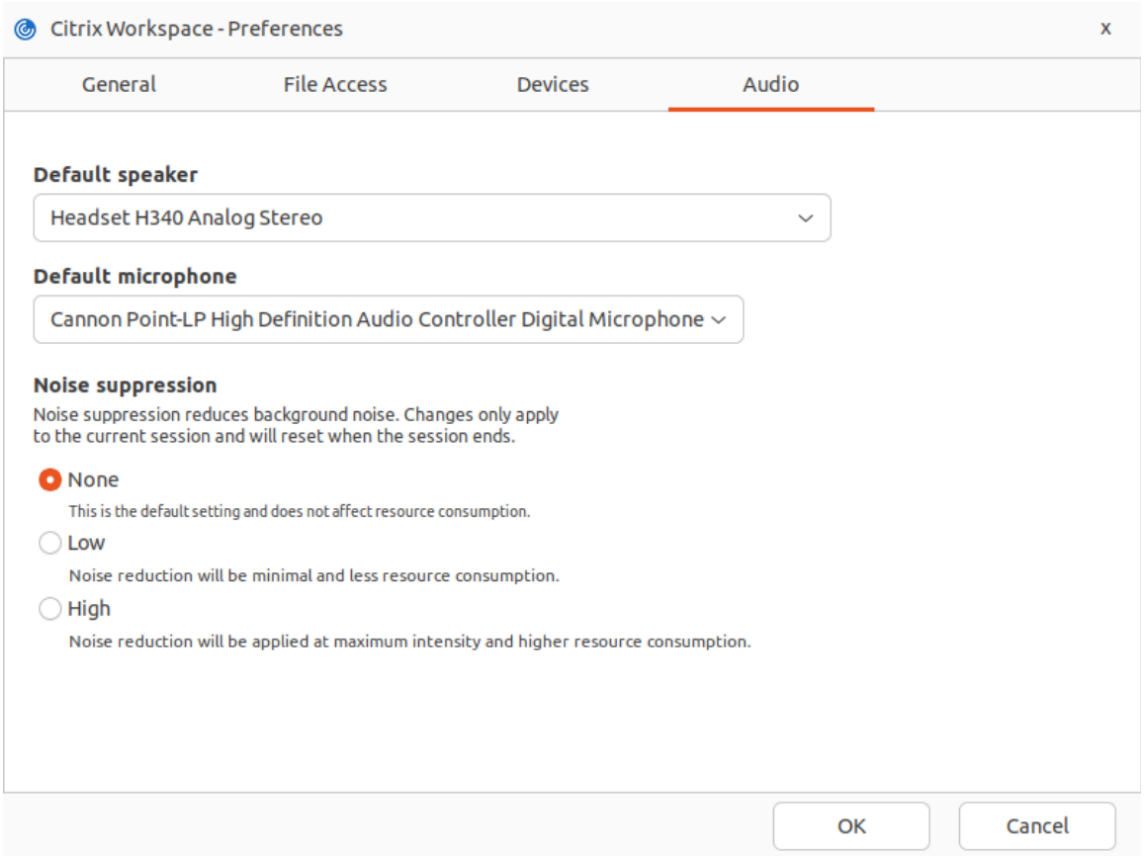
Enable noise suppression

Starting with the 2411 version, Citrix Workspace app now offers improved audio redirection with enhanced noise suppression. This feature reduces background noise, ensuring clearer and more accurate speech, improving the overall communication experience.

> **Note:**
>
> This feature is disabled by default.

To enable this feature, do the following:

1. Navigate to **Preferences** > **Audio** > **Noise Suppression**.



2. Select one of the options:

   - **None**: This is the default setting and doesn't use or affect resource consumption.
   - **Low**: Noise reduction is minimal and uses the least resource consumption.
   - **High**: Noise reduction is applied at maximum intensity with the best performance and uses higher resource consumption than the **Low** setting.

3. Click **OK**. The selected configuration is applied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - Changes apply only to the current session and reset once the session ends.
> - This feature is supported only on x64 and ARM64 Linux distributions. On x64 Linux, both **Low** and **High** options are available, while on ARM64 Linux, only the **Low** option is available due to CPU limitations on ARM devices.

Audio Quality Enhancer for EDT loss tolerant mode

Starting with the 2508 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Adaptive audio must be enabled for this feature to work.

Default audio device selection

Starting with 2503 version, you can now select your preferred audio devices directly in the Desktop Viewer toolbar. This feature offers a more customized audio experience with the following key features when connected to a virtual desktop.

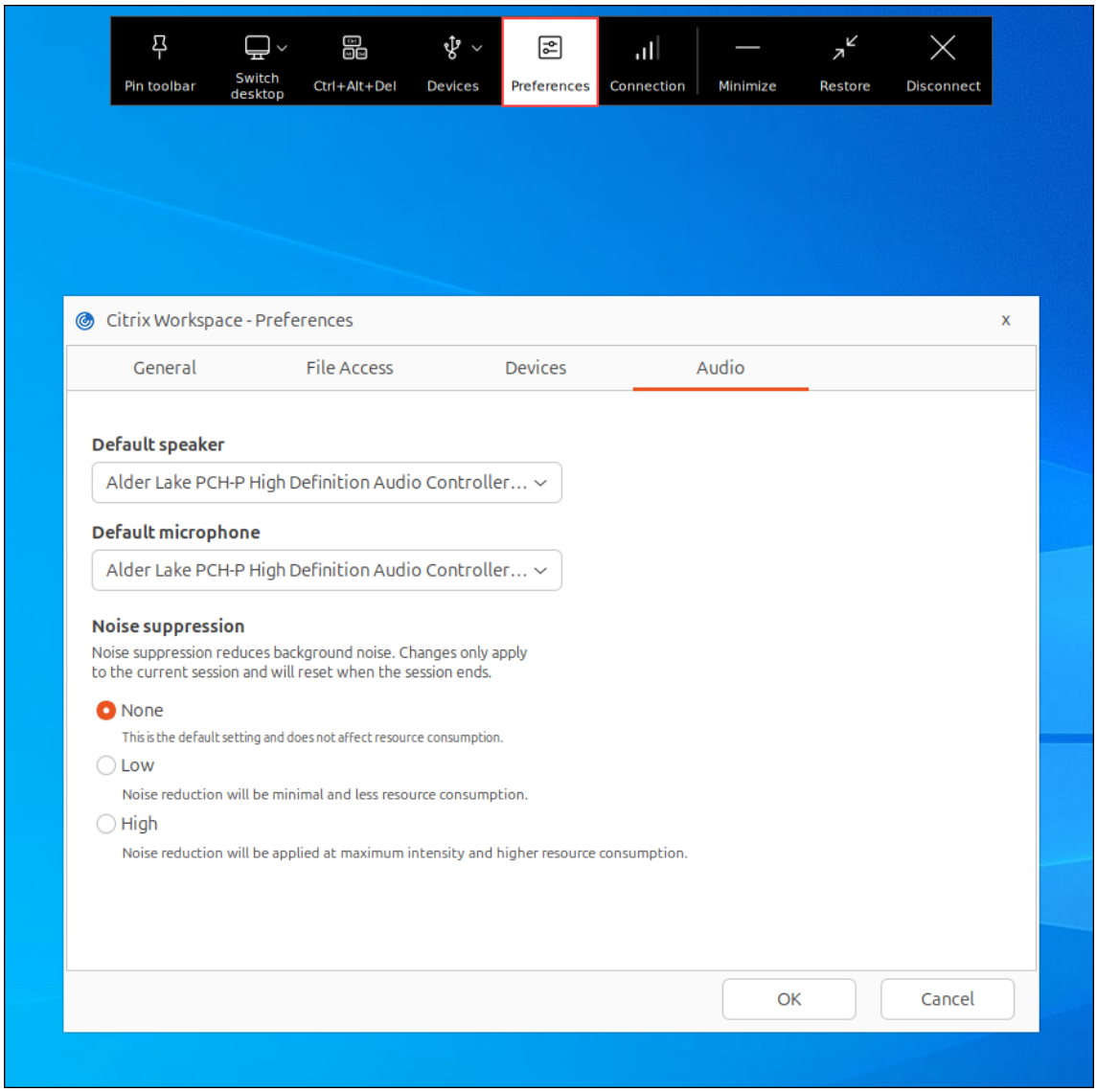
- **Device splitting:** You can assign different audio devices to different VDAs. For example, you can have two monitors with two different VDAs, each using a separate audio device (one loudspeaker and one headset).
- **Specific device selection:** The exact audio device can be selected for each active VDA from the **Preferences** section.
- **Configuration persistence:** The selected configuration is preserved for the next session, ensuring a seamless experience.

> **Note:**
>
> If you don't want the selected configuration to be preserved for the next session, you can adjust the settings accordingly in the Preferences section.
>
> This feature isn't applicable to a pooled desktop environment because each time a user signs in, they might be connected to a different VDA.

To select the specific audio device, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the **Preferences** section on the Desktop Viewer toolbar.



2. Select the device that you want from the **Default speaker** drop-down list.
3. Select the device that you want from the **Default microphone** drop-down list.
4. Click **OK** to save the changes.

Multimedia

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multimedia performance

The Citrix Workspace app includes a broad set of technologies that provide a high-definition user experience for today's media-rich user environments. These technologies improve the user experience when connecting to hosted applications and desktops, as follows:

- HDX MediaStream Windows Media Redirection
- HDX MediaStream Flash Redirection
- HDX RealTime Webcam Video Compression
- H.264

> **Note:**
>
> Citrix supports RTOP coexistence with Citrix Workspace app for Linux Version 1901 and later with `GStreamer 0.1`.

HDX™ MediaStream Windows Media Redirection

HDX MediaStream Windows Media Redirection overcomes the need for the high bandwidths required to provide multimedia capture and playback on virtual Windows desktops accessed from Linux user devices. Windows Media Redirection provides a mechanism for playing the media run-time files on the user device rather than on the server. As a result, reduces the bandwidth requirements for playing multimedia files.

Windows Media Redirection improves the performance of Windows Media Player and compatible players running on virtual Windows desktops. A wide range of file formats are supported, including:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAV sound files

Citrix Workspace app includes a text-based translation table, MediaStreamingConfig.tbl, for translating Windows-specific media format GUIDs into MIME types `GStreamer` can use. You can update the translation table to do the following:

- Add previously unknown or unsupported media filters/file formats to the translation table
- Block problematic GUIDs to force fall-back to server-side rendering.
- Add more parameters to existing MIME strings to allow for troubleshooting of problematic formats by changing a stream's `GStreamer` parameters
- Manage and deploy custom configurations that depend on the media file types supported by `GStreamer` on a user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With client-side fetching, you can also allow the user device to stream media directly from the URLs of the following form rather than streaming the media through a Citrix® server:

- <http://>
- <mms://>
- <rtsp://>

The server is responsible for directing the user device to the media, and for sending control commands (including Play, Pause, Stop, Volume, Seek). But the server does not handle any media data. This feature requires advanced multimedia GStreamer libraries on the device.

To implement HDX MediaStream Windows Media Redirection:

1. Install GStreamer 0.10, an open-source multimedia framework, on each user device that requires it. Typically, you install GStreamer before you install Citrix Workspace app to allow the installation process to configure Citrix Workspace app to use it.

   Most Linux distributions include GStreamer. Alternatively, you can download GStreamer from http://gstreamer.freedesktop.org.

2. To enable client-side fetching, install the required GStreamer protocol source *plugins* for the file types that users play on the device. You can verify that a plug-in is installed and operational using the gst-launch utility. If gst-launch can play the URL, the required plug-in is operational. For example, run gst-launch-0.10 playbin2 uri=<http://example-source/file.wmv> and check that the video plays correctly.

3. When installing Citrix Workspace app on the device, select the GStreamer option if you're using the tarball script (this step is done automatically for the .deb and .rpm packages).

Note about the client-side fetching feature:

- By default, this feature is enabled. You can disable it using the SpeedScreenMMACSFEnabled option in the Multimedia section of All-Regions.ini. With this option set to False, Windows Media Redirection is used for media processing.
- By default, all MediaStream features use the GStreamer playbin2 protocol. You can revert to the earlier playbin protocol for all MediaStream features except Client-Side Fetching. The Client-Side Fetching feature continues to use playbin2, using the SpeedScreenMMAEnablePlaybin2 option in the Multimedia section of the All-Regions.ini file.
- Citrix Workspace app does not recognize playlist files or stream configuration information files such as .asx or .nsc files. If possible, users must specify a standard URL that does not reference these file types. Use gst-launch to verify that a given URL is valid.

Note about GStreamer 1.0:

- By default, GStreamer 0.10 is used for HDX MediaStream Windows Media redirection. GStreamer 1.0 is used only when GStreamer 0.10 is not available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you want to use GStreamer 1.0, use the following instructions:

1. Find the install directory of the GStreamer plug-ins. Depending on your distribution, the OS architecture, and the way you install GStreamer, the installation location of the plug-ins varies. The typical installation path is /usr/lib/x86_64-linux-gnu/gstreamer-1.0 or $HOME/ .local/share/gstreamer-1.0.
2. Find the install directory of Citrix Workspace app for Linux. The default directory for privileged (root) user installations is /opt/Citrix/ICAClient. The default directory for non-privileged user installations is $HOME/ICAClient/platform (where the platform can be linuxx64, for example). For more information, see Install and set up.
3. Install libgstflatstm1.0.so by making a symbolic link in the GStreamer plug-ins directory: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so. This step might require elevated permissions, with sudo, for example.
4. Use gst_play1.0 as the player: ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play. This step might require elevated permissions, with sudo, for example.

- If you want to use GStreamer 1.0 in HDX RealTime Webcam Video Compression, use gst_read1.0 as the reader: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Enabling GStreamer 1.x

In releases earlier to 1912, GStreamer 0.10 was the default version supported for multimedia redirection. Starting with the 1912 release, you can configure GStreamer 1.x as the default version.

Limitations:

- When you play a video, the backward and forward options might not work as expected.
- When you launch the Citrix Workspace app on ARMHF devices, GStreamer 1.x might not work as expected.

To install GStreamer 1.x Install the GStreamer 1.x framework and the following plug-ins from https://gstreamer.freedesktop.org/documentation/installing/on-linux.html:

- Gstreamer-plugins-base
- Gstreamer-plugins-bad
- Gstreamer-plugins-good
- Gstreamer-plugins-ugly
- Gstreamer-libav

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To build binaries locally On some Linux OS distributions, for example, SUSE and openSUSE, the system might not find the GStreamer packages in the default source list. In this case, download the source code and build all binaries locally:

1. Download the source code from https://gstreamer.freedesktop.org/src/.
2. Extract the contents.
3. Navigate to the directory where the unzipped package is available.
4. Run the following commands:

```
$sudo ./configure
$sudo make
$sudo make install
```

By default, the generated binaries are available at */usr/local/lib/gstreamer-1.0/*.

For information about troubleshooting, see Knowledge Center article CTX224988.

To configure GStreamer 1.x To configure GStreamer 1.x for use with Citrix Workspace app, apply the following configuration using the shell prompt:

- $ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.
- $ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play

Where,

- ICACLIENT_DIR - The installation path of Citrix Workspace app for Linux.
- GST_PLUGINS_PATH - The plug-in path of GStreamer. For example, on a 64-bit Debian machine it is */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

Limitations:

- In releases earlier to Version 2106, the webcam redirection might fail and the session might get disconnected when using GStreamer version 1.15.1 or later.

HDX MediaStream Flash Redirection

HDX MediaStream Flash Redirection enables Adobe Flash content to play locally on user devices. This feature provides users with high definition audio and video playback, without increasing bandwidth requirements.

1. Verify that your user device meets the feature requirements. For more information, see System requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Add the following parameters to the [WFClient] section of `wfclient.ini` (for all connections made by a specific user). Or, add to the [Client Engine\Application Launching] section of `All \\_Regions.ini` (for all users of your environment):

   - **HDXFlashUseFlashRemoting=Ask**: **Never**; **Always**

     Enables HDX MediaStream for Flash on the user device. By default, this value is set to **Never**. Also, users are presented with a dialog box asking them if they want to optimize Flash content when connecting to webpages containing that content.

   - **HDXFlashEnableServerSideContentFetching=Disabled**; **Enabled**

     Enables or disables server-side content fetching for Citrix Workspace app. By default this value is set to **Disabled**.

   - **HDXFlashUseServerHttpCookie=Disabled**; **Enabled**

     Enables or disables HTTP cookie redirection. By default, this value is set to **Disabled**.

   - **HDXFlashEnableClientSideCaching=Disabled**; **Enabled**

     Enables or disables client-side caching for web content fetched by Citrix Workspace app. By default, this value is set to **Enabled**.

   - **HDXFlashClientCacheSize= [25-250]**

     Defines the size of the client-side cache, in MB. This value can be any size between 25 MB and 250 MB. When the size limit is reached, existing content in the cache is deleted to allow storage of new content. By default, this value is set to **100**.

   - **HDXFlashServerSideContentCacheType=Persistent**: **Temporary**; **NoCaching**

     Defines the type of caching used by Citrix Workspace app for content fetched using server-side content fetching. By default, this value is set to **Persistent**.

     Note: This parameter is required only if **HDXFlashEnableServerSideContentFetching** is set to **Enabled**.

3. Flash redirection is disabled by default. In /config/module.ini change FlashV2=Off to FlashV2=On to enable the feature.

HDX RealTime webcam video compression

HDX RealTime provides a webcam video compression option to improve bandwidth efficiency during video conferencing. This option ensures users experience optimal performance when using applications such as GoToMeeting with HDFaces, Skype for Business.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Verify that your user device meets the feature requirements.
2. Verify that the `Multimedia` virtual channel is enabled. To enable it, open the `$ICAROOT/config/module.ini` file, and check that `MultiMedia` in the [ICA3.0] section is set to `On`.
3. Enable audio input by clicking the **Use my microphone and webcam on the Mic & Webcam** page of the **Preferences** dialog.

Disable HDX RealTime webcam video compression

By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression. In some circumstances, however, you might require users to connect webcams using USB support. To do this connection, you must do the following:

- Disable HDX RealTime Webcam Video Compression
- Enable USB support for webcams

1. Add the following parameter to the [WFClient] section of the appropriate .ini file:

   AllowAudioInput=False

   For more information, see default settings.

2. Open the `usb.conf` file, typically available at `$ICAROOT/usb.conf`.
3. Remove or comment out the following line:

   > DENY: class=0e # UVC (default via HDX RealTime Webcam Video Compression)

4. Save and close the file.

H.264

Citrix Workspace app supports the display of H.264 graphics, including HDX 3D Pro graphics, that the Citrix Virtual Apps and Desktops 7 serves. This support uses the deep compression codec feature, which is enabled by default. The feature provides better performance of rich and professional graphics applications on WAN networks compared with the existing JPEG codec.

> **Note:**
>
> In H.264, the Citrix Workspace app for Linux supports YUV 420 format only and it doesn't support YUV 444 format.

Follow the instructions in this topic to disable the feature (and process graphics using the JPEG codec instead). You can also disable text tracking while still enabling deep compression codec support. This setting helps to reduce CPU costs while processing graphics that include complex images but relatively small amounts of text or non-critical text.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> To configure this feature, do not use any lossless setting in the Citrix Virtual Apps and Desktops or Citrix DaaS Visual quality policy. If you do, H.264 encoding is disabled on the server and does not work in Citrix Workspace app.

To disable deep compression codec support:

In the `wfclient.ini` file, set **H264Enabled** to **False**. This setting also disables text tracking.

To disable text tracking only:

With deep compression codec support enabled, in the `wfclient.ini` file set **TextTrackingEnabled** to **False**.

Optimization for Microsoft Teams

September 7, 2025

Optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops or Citrix DaaS and Citrix Workspace app. Optimization for Microsoft Teams is similar to HDX RealTime Optimization for Microsoft Skype for Business. The difference is that we bundle all the necessary components for Microsoft Teams optimization into the VDA and the Citrix Workspace app for Linux.

Citrix Workspace app for Linux supports audio, video, and screen-sharing features with Microsoft Teams optimization.

> **Note:**
>
> - Microsoft Teams optimization is supported only on Ubuntu 20.04 or later.
> - Microsoft optimization is supported in both Citrix Virtual Apps and Desktops™ and Citrix DaaS.
> - For Thin Clients that use Dell Wyse, use the **Citrix Configuration Editor** to edit any parameter in the `/var/.config/citrix/hdx_rtc_engine/config.json` file. For more information see the Dell documentation.

For information on how to enable log collection, follow the steps mentioned under Log collection for Microsoft Teams.

For information on system requirements, see Microsoft Teams optimization requirements.

For more information, see Optimization for Microsoft Teams and Microsoft Teams redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for Optimized Microsoft Teams on ARM64 devices

Starting with the 2408 version, the Optimized Microsoft Teams feature is supported on ARM64 architecture-based endpoint devices running Citrix Workspace app for Linux.

Limitation

- The second ringtone does not work when both USB microphone devices are selected on the Raspberry Pi 4B devices.
- The background effect is not supported for Linux Arm64 devices.
- When turned on both incoming and outgoing video, the resolution might degrade due to Pi performance limitations.
- The feature does not support human interface devices (HID).

You can provide feedback for this feature using this Feedback form.

Enhancement to audio configuration

If Microsoft Teams configures auto gain control and noise suppression options, Citrix-redirected Microsoft Teams honors the values as configured. Otherwise, these options are enabled by default. However, starting from Citrix Workspace app 2104, the echo cancellation option is disabled by default. The examples for audio issues include robotic voice, high CPU causing choppy audio, and so on. Starting from Citrix Workspace app 2112, admins can change the default settings to troubleshoot Audio issues by doing the following:

1. Navigate to the /var/.config/citrix/hdx_rtc_engine/config.json file.
2. Set the following options:
    - `EnableAEC` value to 1 to enable and 0 to disable echo cancellation
    - `EnableAGC` value to 1 to enable and 0 to disable auto gain control
    - `EnableNS` value to 1 to enable and 0 to disable noise suppression

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


      "EnableAEC":1,"EnableAGC":1,"EnableNS":1

 }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the call is established, monitor the webrpc log (/tmp/webrpc/<current date>/) for the following entries to verify that the changes took effect:

```
/tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
    14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
    constraints, aec=1, agc=1, ns=1
```

Encoder performance estimator for Microsoft Teams

The HdxRtcEngine is the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection. The HdxRtcEngine.exe can estimate the best outgoing video (encoding) resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 720p, and 1080p.

The performance estimation process uses macroblock code to determine the best resolution that can be achieved with the particular endpoint. The Codec negotiation during a call setup includes the highest possible resolution. The Codec negotiation can be between the peers, or between the peer and the conference server.

The following table lists the four performance categories for endpoints that have its own **maximum** available resolution:

Endpoint performance	Maximum resolution	Registry key value
Fast	1080p (1920x1080 16:9 @ 30 fps)	3
Medium	720p (1280x720 16:9 @ 30 fps)	2
Slow	360p (either 640x360 16:9 @ 30 fps, or 640x480 4:3 @ 30 fps)	1
Very slow	240p (either 320x180 16:9 @ 30 fps, or 320x240 4:3 @ 30 fps)	0

To set the outgoing video (encoding) resolution value, for example to 360p, run the following command from the terminal:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


    "OverridePerformance":1

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10   }
```

Log collection for Microsoft Teams

To enable log collection for Microsoft Teams:

1. Navigate to the /opt/Citrix/ICAClient/debug.ini file.
2. Modify the [HDXTeams] section as follows:

```
1  [HDXTeams]
2  ; Retail logging for HDXTeams 0/1 = disabled/enabled
3  HDXTeamsLogSwitch = 1
4  ; Debug logging; , It is in decreasing order
5  ; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
       LS_VERBOSE = 0
6  WebrtcLogLevel = 0
7  ; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
8  WebrpcLogLevel = 0
```

Log collection can also be enabled by adding the following line to the config.json file:

```
1  {
2
3  "WebrpcLogLevel": 0,"WebrtcLogLevel": 0
4   }
```

Adding the libunwind-12 library dependency for llvm-12

Starting with the 2111 release, a new dependency called the libunwind-12 library is added for llvm-12. However, by default, it does not exist in the original repository. Install the libunwind-12 library manually in the repository using the following steps:

1. Open the terminal.
2. Enter the following line to install the llvm repository key file:

```
1   wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key|sudo apt-key
        add
```

3. Enter the following line to configure the llvm repository source list:

```
1   sudo vim /etc/apt/sources.list
```

4. Add the following line:

```
1  deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
2  deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Run the following command to install the libunwind-12 library:

```
sudo apt-get update -y
sudo apt-get install libunwind-12
```

Configuring a preferred network interface

Starting with the Citrix Workspace app 2303 version, you can now configure a preferred network interface for media traffic. With this enhancement, if you have multiple network connections and the performance of the default one is not good, you can change to another network. To enable this enhancement:

1. Navigate to /var/.config/citrix/hdx_rtc_engine/config.json file.
2. Go to the following section:

```
        mkdir -p /var/.config/citrix/hdx_rtc_engine

         vim /var/.config/citrix/hdx_rtc_engine/config.json

        {


             ” NetworkPreference ” :1

          }
```

3. Update the “NetworkPreference:”value with one of the following values as required:
   - 1: Ethernet
   - 2: Wi-Fi
   - 3: Cellular
   - 4: VPN
   - 5: Loopback
   - 6: Any

By default and if no value is set, the WebRTC media engine chooses the best available route.

Configure UDP port range for Microsoft Teams optimization

With the 2402 release, you can specify the minimum and maximum range of UDP ports for Microsoft Teams optimization. If the UDP Port cannot be allocated for any reason, the WebRTC falls back to TCP. To enable this feature, add the following two new configuration items to the /var/.config/citrix/hdx_rtc_engine/config.json configuration file on the client device:

- PortRangeMin stands for minimum UDP port

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- PortRangeMax stands for maximum UDP port

Ensure that the following two conditions are met for this feature to take effect:

- You must set the minimum and maximum UDP port.
- The minimum port must be 10 numbers smaller than the maximum port.

To enable this feature, do the following on the client device:

1. Navigate to the `/var/.config/citrix/hdx_rtc_engine/config.json` config file.
2. Add the `PortRangeMin` and `PortRangeMax` numbers.

```
// config file /var/.config/citrix/hdx_rtc_engine/config.json

{

    "PortRangeMin" : 30000,
    "PortRangeMax" : 31000
 }
```

Enhancements to Microsoft Teams optimization

- Starting with version 2101 for Citrix Workspace app:
  - The Citrix Workspace app installer is packaged with the Microsoft Teams ringtones.
  - Audio output switches automatically to newly plugged-in audio devices, and an appropriate audio volume is set.
  - HTTP proxy support for anonymous authentication.
- Starting with version 2103 for Citrix Workspace app, the VP9 video codec is disabled by default.
- Starting with version 2104 for Citrix Workspace app, the echo cancellation feature is disabled by default. We recommend that you do not use your built-in speakers and microphone for calls. Use headphones instead. This fix aims to address choppy audio issues noticed on thin clients
- Starting with version 2106 for Citrix Workspace app:
  - Previously, when you clicked **Screen sharing**, preview of a default or main monitor was only available for screen sharing.

    With this version, a preview of all screens is displayed on the screen picker menu. You can select any screen for screen sharing in the VDA environment. A red square appears on the selected monitor and a small picture of the selected screen content appears on the screen picker menu.

    In seamless mode, you can select one from all screens to share. When the Desktop Viewer changes the window mode (maximized, restore, or minimize), the screen share stops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Starting with version 2112 for Citrix Workspace app:

  > **Note:**
  >
  > The following features are available only after the roll-out of a future update from Microsoft Teams. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

  - **Request control in Microsoft Teams**

    With this release, you can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other modifications to the shared screen.

    To take control when a screen is being shared, click **Request control** at the top of the Microsoft Teams screen. The meeting participant who's sharing the screen can either allow or deny your request.

    While you have control, you can make selections, edits, and other modifications to the shared screen. When you're done, click **Release control**.

    Limitations:

    - Users on a Linux client cannot *Give* control to other users. In other words, after the user on the Linux client starts sharing content, the option **Give control** is not present in the sharing toolbar. This is a Microsoft limitation.
    - The **Request Control** option is not available during the peer-to-peer call between an optimized user and a user on the native Microsoft Teams desktop client that is running on the endpoint. As a workaround (not applicable on the previous limitation for Linux client users), users can join a meeting to get the **Request Control** option.

  - **Support for dynamic e911**

    With this release, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it provides the capability to:

    - configure and route emergency calls
    - notify security personnel

    The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client that runs on the VDA.
    Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112 for Linux, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law. To support this feature, the LLDP library must be included in the Operating System distribution of the Thin Client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Starting with version 2203 for Citrix Workspace app:

  Multi-window chat and meetings for Microsoft Teams

  With this release, you can use multiple windows for chat and meetings in Microsoft Teams, when optimized by HDX in Citrix Virtual Apps and Desktops 2112 or higher. You can pop out the conversations or meetings in various ways. For details about the pop-out window feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings.

  If you're running an older version of Citrix Workspace app or Virtual Delivery Agent (VDA), remember that Microsoft will deprecate the single-window code in the future. However, you will have a minimum of nine months after this feature is GA to upgrade to a version of the VDA or Citrix Workspace app that supports multiple windows (2203 and greater).

  > **Note:**
  >
  > This feature is available only after the roll-out of a future update from Microsoft Teams. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

- Starting with version 2207 for Citrix Workspace app:

  - **App sharing enabled:** Starting with Citrix Workspace app 2209 for Linux and Citrix Virtual Apps and Desktops 2109, you can share an app using the Screen sharing feature in Microsoft Teams.

    Limitations:

    To support app sharing, make sure the following options aren't selected for the **Use Video Codec for Compression** policy:

    - Don't select the **For the Entire Screen** option.
    - Don't select **Use When Preferred** when the **Optimize for 3D Graphics Workloads** policy is enabled.

  - **Enhancements to high DPI support:** When the high DPI feature is enabled and you're using 4K monitors, Microsoft Teams video overlays are in the desired position and of the correct size. Irrespective of your display settings such as single or multi-monitor arrangements, overlays always appear correctly and aren't scaled up or appear in an undesired position. To enable this enhancement, ensure that the `DPIMatchingEnabled` parameter in the `wfclient.ini` configuration file is set to **True**. For more information, see Support for DPI matching.

  - **WebRTC SDK upgrade:** The version of the WebRTC SDK that is used for the optimized Microsoft Teams is upgraded to version M98.

- Starting with version 2305 for Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enhancement to sleep mode for optimized Microsoft Teams call**

  Previously, when you are in an optimized Microsoft Teams meeting, if there is no mouse or keyboard interaction, Citrix Workspace app or the optimized Microsoft Teams screen might go into sleep mode.

  Starting with the 2305 release, Citrix Workspace app or the optimized Microsoft Teams screen doesn't go into sleep mode even if there is no mouse or keyboard interaction during an optimized Microsoft Teams meeting.

- **Improved experience for optimized Microsoft Teams video conference calls**

  Starting with the 2305 release, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved by adapting to the proper resolution for the best call experience for all callers.

  With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on) depending on several factors that include endpoint capability, network conditions, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle thus giving all users the optimum video experience.

- Starting with version 2307 for Citrix Workspace app:

```
**Background blurring and replacement for Citrix Optimized
   Microsoft Teams**

**Prerequisite:**

Ensure that you have installed the `wget`.

Starting with version 2307 for Citrix Workspace app, Citrix
   Optimized Microsoft Teams in Citrix Workspace app for Linux
   now supports background blurring and background replacement.
   You can use this feature by selecting **More** > **Apply
   Background Effects** when you are in a meeting or in a P2P
   call.

For more information, see [Background blurring and background
   effects](/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms
   -teams#background-blurring-and-background-effects).
```

- Starting with version 2308 for Citrix Workspace app:

  - **Support for secondary ringer**

    You can use the Secondary ringer feature to select a secondary device on which you want to get the incoming call notification in an optimized Microsoft Teams. For example, consider that you have set a speaker as the Secondary ringer and your endpoint is connected to the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

headphone. In this case, Microsoft Teams sends the incoming call signal to the speaker even though your headphones are the primary peripheral for the audio call itself. You can't set a secondary ringer in the following cases:

- When you aren't connected to more than one audio device
- When the peripheral is not available (for example, a Bluetooth headset)

- **Added support for playing short tones in optimized Microsoft Teams**

  Earlier, short tunes, short tones such as beeps or notifications were playing repeatedly. For example, the tone that was played when a guest joins the Microsoft Teams meeting was repeated. The only workaround was to quit and restart Microsoft Teams. This issue resulted in a poor end-user experience.

  Starting with the 2308 release, Citrix Workspace app supports playing the short tones as desired. This support also enables the secondary ringtone feature.

  Prerequisites:

  Update to the latest version of Microsoft Teams.

Disable secondary ringer for Microsoft Teams

To disable the secondary ringer feature in the optimized Microsoft Teams, do the following steps:

1. Navigate to `/var/.config/citrix/hdx_rtc_engine/config.json`.
2. Add the following entry:

   ```
   ms_teams_secondary_audio_notifications:"false"
   ```

Support for WebHID API in UCSDK

Starting with the 2411 version, Citrix Workspace™ app for Linux supports the WebHID API to redirect Human Interface Device (HID) devices from endpoint to Unified Communication SDK application on the VDI. It complies to the HID standard for bi-directional communication between the application based on UCSDK and the HID devices connected to the endpoint. With this feature, your UCSDK application can access any HID devices such as keyboards, mice, headsets, and game controllers in the HDX™ session with an enhanced experience.

> **Note:**
>
> This feature is disabled by default.

To enable this feature, do the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to /var/.config/citrix/hdx_rtc_engine/config.json.
2. Add the following entry:

```
"EnableHID": 1
```

> **Note:**
>
> Starting from the 2411 release, Unified Communication SDK application (UCSDK) supports HID devices by default. To use HID support, we recommend that you check with your technology vendor to integrate UCSDK 4.0 or later.

Browser content redirection

September 7, 2026

Chromium Embedded Framework (CEF) for Browser Content Redirection

In releases earlier to Version 1912, BCR used a WebkitGTK+ based overlay to render the content. However, on thin clients, there were performance issues. Starting with Version 1912, BCR uses a CEF-based overlay. This functionality enriches the user experience for BCR. It helps offload network usage, page processing, and graphics rendering to the endpoint.

Starting with Version 2106, CEF-based browser content redirection is fully functional. The feature is enabled by default.

If needed, you can replace the libffmpeg.so file provided in the Workspace app package with a suitable libffmpeg.so file that has the required codecs, in the $ICAROOT/bcr/libffmpeg.so path.

> **Note:**
>
> This feature isn't supported on the ARMHF platform.
>
> Starting with the 2408 version, the version of the Chromium Embedded Framework (CEF) is upgraded to 128.0.6613.120. This upgraded version includes fixes for known security vulnerabilities.

Enabling CEF-based BCR

To enable CEF-based BCR:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the $ICAROOT/config/All_Regions.ini file where, $ICAROOT is the default installation directory of Citrix Workspace app.
2. Go to the [Client Engine\WebPageRedirection] section and set the following entry:

   UseCefBrowser=True

Limitation:

- Web apps that use pop-ups might not work when BCR is used.

Known issues:

- When you access web applications, such as Google Meet, through Chromium Embedded Framework-based Browser Content Redirection, certain UI elements might not respond to interactions. As a workaround, refresh the page to restore UI element functionality. [HDX-94506]
- When you set the UseCefBrowser option to **True** in the ~/.ICAClient/All_Regions.ini, the Japanese, Chinese (Simplified), and Korean IME might not work in the input fields. Citrix Workspace app for Linux does not support the Japanese, Chinese (Simplified), and Korean IME when using Secure SaaS with Citrix Embedded Browser.
- When you attempt to access a SharePoint URL using CEF-based BCR, you might receive an unknown certificate error. You can resolve this issue by verifying that the external client trusts the proxy's SSL certificate. [CVADHELP-24141]
- When you attempt to launch a webpage redirection using CEF-based BCR, you might receive an unknown certificate error. The issue occurs on Citrix Workspace app version 2106 and later. You can resolve this issue by ensuring that the root certificate trust for the website is imported to the linux pki store. For more information, see How to import self-signed certificate into nssdb?.

For information about BCR, see Browser content redirection in the Citrix Virtual Apps and Desktops documentation.

Configure path for Browser Content Redirection overlay Browser temp data storage

Starting with the Citrix Workspace app 2303 version, configure the temp data storage path for the CEF based browser. To configure the path, do the following:

1. Navigate to the $ICAROOT/config/All_Regions.ini file where, $ICAROOT is the default installation directory of Citrix Workspace app.
2. Go to the [Client Engline\WebPageRedirection] section and add the following entry:

```
1 CefCachePath=<folder for CEF based BCR tmp files>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hardware acceleration in Browser Content Redirection

Starting with the Citrix Workspace app for Linux 2508 version, the hardware acceleration is now enabled by default in Browser Content Redirection (BCR). This feature provides the following benefits:

- Faster graphics rendering - BCR leverages client-side GPU to delegate graphics-related tasks to the Graphics Processing Unit, delivering a more fluid and immersive user experience.
- Reduced CPU load - When the GPU handles hardware acceleration, it relieves the CPU of graphics-intensive tasks. The CPU can focus on other processes, improving overall system performance and multitasking efficiency.
- Enhanced video playbook - Hardware acceleration enables video playback to use dedicated rendering engines in modern GPUs, which process high-bitrate videos more efficiently.

This feature requires the following system requirements:

- GPU must support OpenGL version 2.0 or later, or DirectX version 9 or later
- Compatible GPUs include NVIDIA GeForce series, AMD Radeon GPUs, Intel Xe GPU Family, and similar hardware.

Modular Browser Content Redirection

Starting with Citrix Workspace app 2601 for Linux, Browser Content Redirection (BCR) is managed as a modular component, decoupled from the main Citrix Workspace app (CWA) for Linux. This new modular architecture allows the BCR component to be updated or uninstalled independently of the CWA. As a result, security fixes can be delivered more quickly, and new BCR capabilities can be adopted without waiting for a full CWA release cycle.

The BCR component continues to be installed by default with Citrix Workspace app for Linux, ensuring a consistent user experience. Additionally, standalone BCR packages are available for situations that require independent updates or interim patches outside the regular Citrix Workspace app release cycle.

Single sign-on support for Browser Content Redirection

Starting with Citrix Workspace App Linux 2601, Browser Content Redirection (BCR) offers streamlined user experience with single sign-on support, enabling VDA-side authentication and cookie sharing. This enhancement eliminates redundant logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed. This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client.

For more information, see Single sign-on support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Server-side certificate validation

Starting with Citrix Workspace app 2604 for Linux, Browser Content Redirection is further enhanced with certificate validation support. When accessing a redirected website from the client, the client overlay browser may not trust the certificate from the server or the MitM proxy. In such cases, BCR can now validate the Host or Proxy certificates against the VDAs certificate store.

For more information, see Server-side certificate validation document.

Requirements

This feature is enabled by default, and no configuration is necessary once the following requirements are met:

- CVAD 2507 LTSR or later, or CVAD 2511 CR or later
- CWA Linux 2604 or later
- Browser Redirection Extension (Chrome or Edge) 25.11 or later

Web page zoom synchronization

Starting with Citrix Workspace app 2608 for Linux, Browser Content Redirection synchronizes zoom levels between the VDA browser and the client-rendered BCR overlay, ensuring consistent scaling of web content.

Server-client content redirection

September 7, 2025

Server-client content redirection enables administrators to specify that URLs in a published application are opened in a local application. For example, opening a link to a webpage while using Microsoft Outlook in a session opens the required file using the browser on the user device.

Server-client content redirection enables administrators to give Citrix® resources more efficiently, by that provides better performance to the users. The following types of URL can be redirected:

- HTTP
- HTTPS
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Older Real Players)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The URL is opened using the server application when:

- Citrix Workspace app does not have an appropriate application
- Citrix Workspace app can't directly access the content

Server-client content redirection is configured on the server. This feature is enabled by default in Citrix Workspace app if the path includes the following:

- RealPlayer
- One of Firefox, Mozilla, or Netscape.

To enable server-client content redirection if RealPlayer and a browser aren't in the path:

1. Open the configuration file `wfclient.ini`.
2. In the [Browser] section, modify the following settings:

   Path=path

   Command=command

   The path is the directory where the browser executable is located. The command is the name of the executable used to handle redirected browser URLs, appended with the URL sent by the server. For example:

   `$ICAROOT`/`nslaunch` Netscape, Firefox, Mozilla

   This setting specifies the following:

   - The `nslaunch` utility is run to push the URL into an existing browser window.
   - Each browser in the list is tried in turn until content can be displayed successfully.

3. In the [Player] section, modify the following settings:

   Path=path

   Command=command

   The path is the directory where the RealPlayer executable is located. The command is the name of the executable used to handle the redirected multimedia URLs, appended with the URL sent by the server.

4. Save and close the file.

> **Note:**
>
> For both path settings, you need to specify the directory where the browser and RealPlayer executables are available. You do not need to specify the full path to the executables. For example, in the [Browser] section, the path might be set to /usr/X11R6/bin rather than /us-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> r/X11R6/bin/netscape. Also, you can specify extra directory names as a colon-separated list. If these settings aren't specified, the user's current $PATH is used.

To clear server-client content redirection from Citrix Workspace:

1. Open the `module.ini` configuration file.
2. Change the `CREnabled` setting to `Off`.
3. Save and close the file.

ICA® Settings Reference

September 7, 2025

The ICA Settings Reference page provides a list of registry settings and ICA file settings. This page allows administrators to customize the behavior of the Citrix Workspace app. You can also use the ICA Settings Reference page to troubleshoot an unexpected Citrix Workspace app behavior.

ICA Settings Reference (PDF download)

Bidirectional content redirection

September 7, 2025

Bidirectional content redirection allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions. This means:

- A URL entered in a browser running in the Citrix session can be opened using the client's default browser.
- Conversely, a URL entered in a browser running on the client can be opened in a Citrix session, either with a published app or desktop.

Citrix also offers host-to-client redirection and Local App Access redirection. However, it is recommended to use Bidirectional Content Redirection for most use cases.

For more information, see Bidirectional content redirection documentation for Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration

Prerequisites:

- Citrix Virtual Apps and Desktops™ version 2402 or later.
- Citrix Workspace™ app for Linux 2411 or later.

Bidirectional content redirection is configured entirely through Citrix Studio. For non-client configuration details, see the Bidirectional content redirection documentation for Citrix Virtual Apps and Desktops.

1. If upgrading from a previous version of Citrix Workspace App for Linux, confirm that `AllowBidirectionalContentRedirection=True` in `wfclient.ini`.
2. Install Chrome or Edge browser on the client.
3. If using Chrome, run the following command on the client:

   ```
   sudo cp /opt/Citrix/ICAClient/config/hdppkjifljbdpckfajcmlblbchhledln.json /opt/google/chrome/extensions/
   ```

   If using Edge, the equivalent will be automatically configured upon the first connection to a VDA.
4. Launch the client browser and enable `/install "Browser Redirection Extension"` when prompted.

Devices

April 22, 2026

This section describes the following:

- Mouse
- Cursor
- Keyboard
- USB
- Webcams
- Client drive mapping
- Printer
- SANE redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mouse

February 26, 2024

Relative Mouse

Relative Mouse support provides an option to interpret the mouse position in a relative rather than absolute manner. This capability is required for applications that demand relative mouse input rather than absolute.

> **Note:**
>
> This feature is available only in sessions running on Citrix Virtual Apps and Desktops 7.8 (or later) or Citrix DaaS. It's disabled by default.

To enable the feature:

In the file `$HOME/.ICAClient/wfclient.ini`, in the section [WFClient], add the entry RelativeMouse=1.

This step enables the feature but keeps it inactive until you activate it. For more information on enabling relative mouse features, see the Alternative Relative Mouse values section.

To activate the feature:

Type Ctrl/F12.

After the feature is enabled, type Ctrl/F12 again to synchronize the server pointer position with the client. The server and client pointer positions aren't synchronized when using Relative Mouse.

To deactivate the feature:

Type Ctrl-Shift/F12.

The feature is also switched off when a session window loses focus.

Alternative Relative Mouse values

Alternatively, consider using the following values for RelativeMouse:

- RelativeMouse=2 Enables the feature and activates it whenever a session window gains focus.
- RelativeMouse=3 Enables, activates, and keeps the feature activated always.
- RelativeMouse=4 Enables or disables the feature when the client-side mouse pointer is hidden or shown. This mode is suitable for automatically enabling or disabling the relative mouse for first-person gaming-style application interfaces.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To change the keyboard commands, add settings like:

- RelativemouseOnChar=F11
- RelativeMouseOnShift=Shift
- RelativemouseOffChar=F11
- RelativeMouseOffShift=Shift

The supported values for **RelativemouseOnChar** and **RelativemouseOffChar** are listed under [Hotkey Keys] in the `config/module.ini` file. You can find this file in the Citrix Workspace app installation tree. The values for **RelativeMouseOnShift** and **RelativeMouseOffShift** set the modifier keys to be used and are listed under the [Hotkey Shift States] heading.

Cursor

September 7, 2025

Support for cursor color inverting

Previously, the Citrix Workspace app displayed a dotted cursor that appeared the same in color to the black and white background of a text. As a result, it was difficult to locate the position of the cursor.

Starting with version 2112, the cursor color inverts based on the background color of a text. As a result, you can easily locate the position of the cursor in the text. By default, this feature is disabled.

Prerequisites:

- If `.ICAClient` is already present in the home folder of the current user:

  Delete `All_Regions.ini` file

  Or,

  To retain the `All_Regions.ini` file, add the following lines at the end of the [Virtual Channels\Thinwire Graphics] section:

  InvertCursorEnabled=

  InvertCursorRefreshRate=

  InvertCursorMode=

If the `.ICAClient` folder is not present then it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the feature is retained.

To enable this feature, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Go to the [Thinwire3.0] section and set the following entry:

   InvertCursorEnabled=True

> **Note:**
>
> The cursor does not invert when the value for the **Use video codec for compression** policy in Citrix Studio is set to `Do not use video codec`.

Support for 32-bit cursor

Previously, when you were using the custom 32-bit cursor, a black box might appear around the cursor.

Starting with Citrix Workspace app for Linux version 2212, support for the 32-bit cursor was enabled by default. As a result, the black box around the cursor issue is resolved.

Starting with Citrix Workspace app for Linux version 2309, you can disable the support for the 32-bit cursor. For this enhancement, a new parameter named `Cursor32bitSupport` is added in the `wfclient.ini` file.

To disable support for the 32-bit cursor, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Go to the [Thinwire3.0] section and set the following entry:

```
1 Cursor32bitSupport=False
```

Touch screen

March 17, 2025

Multi-touch support

The multi-touch support feature in Citrix Workspace app for Linux supports multi-touch devices. This feature allows devices to receive input from the touch screen. The input includes touch gestures and interactions using a pen or a stylus device. You can interact with multi-touch screens while using apps or desktops in an HDX session.
The supported actions and corresponding gestures on the touch screen are the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Select an item**: Tap on the touchpad.
- **Scroll**: Place two fingers on the touchpad and slide horizontally or vertically.
- **Zoom in or out**: Place two fingers on the touchpad and pinch in or stretch out.
- **Show more commands (similar to right-clicking)**: Tap the touchpad with two fingers, or press in the lower-right corner.

Known limitation:

- Doesn't support session reliability, which means no touch event cache is stored.
- Doesn't support on Linux VDA.

> **Note:**
>
> The preceding options might vary based on the Windows version that you are using.

Known issues:

- Multi-touch isn't supported on multi-monitors for which the display mode is set as **Join Displays** (extended mode). [HDX-52394]
- You might not be able to press a finger on the screen and hold it on the ASUS touch screen. [HDX-52521]

Manage On-screen keyboard for multi-touch

> **Note:**
>
> This feature is enabled by default.

Administrators can disable this feature as follows:

1. Navigate to the `$HOME/.ICAClient/All_Regions.ini` folder.
2. Go to the `[Virtual Channels\Keyboard]` section.
3. Modify the value of `EnhanceOSKForMT` as follows:

```
1 EnhanceOSKForMT=False
```

This feature supports the following environments:

- The default on-screen keyboard in Gnome.
- Florence and Onboard in X11-based desktop environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard

September 7, 2026

Keyboard behavior

To generate a remote Ctrl+Alt+Delete key combination:

1. Decide which key combination creates the Ctrl+Alt+Delete combination on the remote virtual desktop.
2. In the WFClient section of the appropriate configuration file, configure UseCtrlAltEnd:
    - True means that Ctrl+Alt+End passes the Ctrl+Alt+Delete combination to the remote desktop.
    - False (default) means that Ctrl+Alt+Enter passes the Ctrl+Alt+Delete combination to the remote desktop.

Generic redirection

Configuring the Bloomberg v4 keyboard through Generic USB Redirection on the client side:

As a prerequisite, the policy must be enabled in the Domain Delivery Controller™ (DDC).

1. Find the vid and pid of the Bloomberg keyboard. For example, in Debian and Ubuntu run the following command:

    ```
    lsusb
    ```

2. Go to $ICAROOT and edit the usb.conf file.
3. Add the following entry in the usb.conf file to allow the Bloomberg keyboard for USB redirection, and then save the file.

    ALLOW: vid=1188 pid=9545

4. Restart the `ctxusbd` daemon on the client. For example, in Debian and Ubuntu run the following command:

    ```
    systemctl restart ctxusbd
    ```

5. Launch a client session. Make sure that the session has focus while plugging in the Bloomberg v4 keyboard for redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can add the following configuration to disable the `selectconfiguration` command:
>
> `ALLOW: vid=1100 pid=0101 disableselectconfig=1`.
>
> The `selectconfiguration` is a command used in VDA to configure USB devices.

Selective redirection

This feature allows the use of the Bloomberg keyboard v4 and v5 interface across multiple sessions. This functionality provides flexibility to use the keyboard in all remote sessions except the fingerprint and audio interfaces. The fingerprint and audio interfaces are redirected to single sessions as before.

To enable the feature:

1. Edit the BloombergRedirection section as follows in the `$HOME/.ICAClient/wfclient.ini` file.

   ```
   1 BloombergRedirection=true
   ```

2. Do all the steps mentioned in Generic redirection.

To disable the feature:

1. Edit the BloombergRedirection section as follows in the `$HOME/.ICAClient/wfclient.ini` file.

   ```
   1 BloombergRedirection=false
   ```

2. Do all the steps mentioned in Generic redirection.

> **Note:**
>
> Setting the value to false reverts the functionality to the behavior present in earlier versions of the client, where all the interfaces are redirected to a single session.

Support for keyboard shortcut to switch between Full-screen and Window mode

Previously, you could use either the **Window** or **Full-screen** button on the Desktop Viewer to toggle between **Full-screen** and **Window** mode.

Starting with the Citrix Workspace app 2308 release, you can use a keyboard shortcut Ctrl+F2 to switch between **Full-screen** and **Window** mode. For example, when the desktop session is in **Full-screen** mode, if you press "Ctrl+F2", the desktop session exits from the **Full-screen** mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature is disabled by default.

To enable this feature:

1. If `.ICAClient` is already present in the home folder of the current user when the new Citrix Workspace app for Linux version is installed:

   Delete the All_Regions.ini file.
   Or
   Retain the All_Regions.ini file and add the following lines at the end of the [Client Engine\Application Launching] section:

   ```
   FullScreenShortcutSupport=*
   ```

2. Navigate to the /opt/Citrix/ICAClient/config/All_Regions.ini file and modify the value of FullScreenShortcutSupport as follows:

   ```
   FullScreenShortcutSupport=true
   ```

   By default, the keyboard shortcut is Ctrl+F2.

You can also customize the shortcut key. The shortcuts are composed of two different parts such as **KeyPassthroughEscapeShift** and **KeyPassthroughEscapeChar** in the `All_Regions.ini` file.

The two keys that you're using must be from the following list:

Name	Section	Value
KeyPassthroughEscapeShift	[Virtual Channels\Keyboard] in All_Regions.ini	[Alt, Ctrl, Shift, Alt+Ctrl, Alt+Shift, Ctrl+Shift, Alt+Ctrl+Shift], Default value: Ctrl
KeyPassthroughEscapeChar	[Virtual Channels\Keyboard] in All_Regions.ini	[F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Minus, Plus, Tab, Pause], Default value: F2, Note: Minus and Plus are the keys on the numeric pad.

For example, if you want to use "Ctrl+Shift+F3"as the keyboard shortcut, the configuration items must be as follows:

- KeyPassthroughEscapeShift=Ctrl+Shift
- KeyPassthroughEscapeChar=F3

Limitation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you use a keyboard combination that conflicts with the client OS shortcuts or contains a system shortcut, the **Full-screen** toggle might not work because the client OS takes precedence on using this shortcut. For example, if you use "Ctrl + F3"as a Linux OS system shortcut, you can't use "Ctrl + F3"or "Shift + Ctrl + F3"as the Citrix Workspace app **Full-screen** toggle.
- `Ctrl+Alt+F'*'` or `Alt+Ctrl+F'*'` (`F'*'` refers to F1-F12) are keyboard shortcuts used to switch between Virtual Terminals in Linux. These shortcuts must not be used for **Full-screen** toggle.
- Alt+Ctrl+Plus or Alt+Ctrl+Minus (Plus and Minus are the keys on the numerical keyboard) are mapped to the symbols XF86Next_VMode/XF86Prev_VMode in the Linux system and not available for shortcuts. So, these combinations must not be used for **Full-screen** toggle.

Keyboard layout synchronization

Keyboard layout synchronization enables you to switch among preferred keyboard layouts on the client device. This feature is disabled by default. After you enable this feature, the client keyboard layout automatically synchronizes to the virtual apps and desktops.

Starting with version 2203, Citrix Workspace app supports the following three different keyboard layout synchronization modes:

- **Sync only once - when session launches** –Based on the `KeyboardLayout` value in the wfclient.ini file, the client keyboard layout is synchronized to the server when the session launches. If the `KeyboardLayout` value is set to `0`, the system keyboard is synchronized to VDA. If the `KeyboardLayout` value is set to a specific language, the language-specific keyboard is synchronized to VDA. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, sign out and sign in to the app. Also, the changes take effect if you sign in again or reconnect to the VDA session. The **Sync only once - when session launches** mode is the default keyboard layout selected for the Citrix Workspace app.
- **Allow dynamic sync** - This option synchronizes the client keyboard layout to the server when you change the client keyboard layout.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

Prerequisite:

- Enable the Unicode Keyboard Layout Mapping feature on the Windows VDA. For more information, see Knowledge Center article CTX226335.
- Enable the Dynamic Keyboard layout sync feature on the Linux VDA. For more information, see Dynamic keyboard layout synchronization
- Keyboard layout synchronization depends on XKB lib.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you use a Windows Server 2016 or Windows Server 2019, navigate to the `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` registry path. And then, add a DWORD value with key name `DisableKeyboardSync` and set the value to `0`.
- If `.ICAClient` is already present in the home folder of the current user:

  Delete the All_Regions.ini file

  or

  To retain the `All_Regions.ini` file, add the following lines at the end of the[Virtual Channels\Keyboard] section:

  KeyboardSyncMode=

  KeyboardEventMode=

Configure keyboard layout

Citrix Workspace app provides both UI and configuration settings to enable the three different keyboard layout synchronization modes.

To configure keyboard layout synchronization using the graphical user interface:

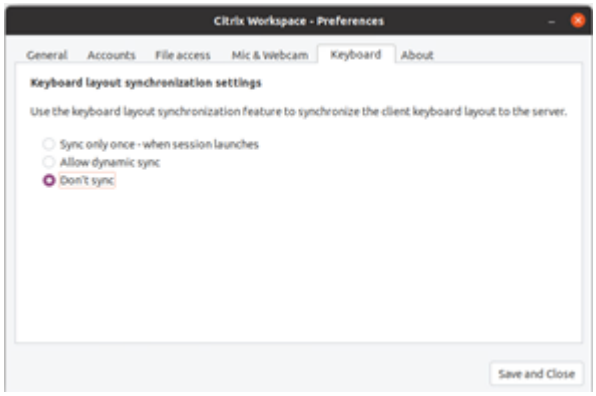
1. From the Citrix Workspace app icon in the notification area, select **Preferences**.

   Or,

   Open the terminal, navigate to the installation path, and run the following command:

   `util/configmgr`

   The **Citrix Workspace** –**Preferences** dialog appears.

2. Click the **Keyboard** tab.

   The **Keyboard layout synchronization settings** page appears.

3. Select from one of the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sync only once - when session launches** - Indicates that the keyboard layout is synced to the VDA only once at the session launch. Unicode keyboard input mode is the recommended option for the **Sync only once –when session launches** mode.
- **Allow dynamic sync** - Indicates that the keyboard layout is synced dynamically to the VDA when the client keyboard is changed in a session. Unicode keyboard input mode is the recommended option for the **Allow dynamic sync** mode.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server, irrespective of the keyboard layout that is selected in the client. Scancode keyboard input mode is the recommended option for the **Don't sync** mode. You must make sure that the client keyboard layout is the same as the keyboard layout on the VDA if you select Unicode for the **Don't Sync** option.

4. Click **Save and Close**.

To configure keyboard layout synchronization using configuration file settings:

Modify the `wfclient.ini` configuration file to enable the required keyboard layout.

Sync only once –when session launches:

With this feature enabled, when launching a session, the active keyboard layout on the client device is synchronized to VDA. Based on the `KeyboardLayout` value in the `wfclient.ini` file, the client keyboard layout is synchronized to the server when the session launches. If the `KeyboardLayout` value is set to `0`, the system keyboard is synchronized to VDA. If the `KeyboardLayout` value is set to a specific language, the language-specific keyboard is synchronized to VDA.

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardSyncMode=Once
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
```

Unicode keyboard input mode is the recommended option for the **Sync only once –when session launches** mode.

Allow dynamic sync:

With this feature enabled, when the keyboard layout changes on the client device during a session, the keyboard layout of the session changes correctly.

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
KeyboardSyncMode=Dynamic
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
```

Unicode keyboard input mode is the recommended option for the **Allow dynamic sync** mode.

Don't sync:

With this feature enabled, the VDA side keyboard layout is used, irrespective of the keyboard layout that is selected in the client device.

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardSyncMode=No
KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
```

Scancode keyboard input mode is the recommended option for the **Don't sync** mode. You must make sure that the client keyboard layout is the same as the VDA side keyboard layout if you configure to Unicode for **Don't Sync** option.

> **Note:**
>
> When you set `KeyboardSyncMode=""` (empty) in the `wfclient.ini` file, the mode reverts to the earlier behavior. In the earlier behavior, the keyboard layout is read from the `$HOME/.ICAClient/wfclient.ini` file. And, send this value to the VDA along with other client information when the session starts.

Keyboard Input Mode Citrix® recommends the following keyboard input mode for the different keyboard layout sync options:

- Scancode mode for **Don't Sync** option.
- Unicode mode for **Allow dynamic sync** and **Sync only once - when session launches** options.

You can change the configuration of `KeyboardEventMode` in the `wfclient.ini` file. However, for best performance, use the Citrix-recommended modes for different scenarios, physical keyboards, and client devices.

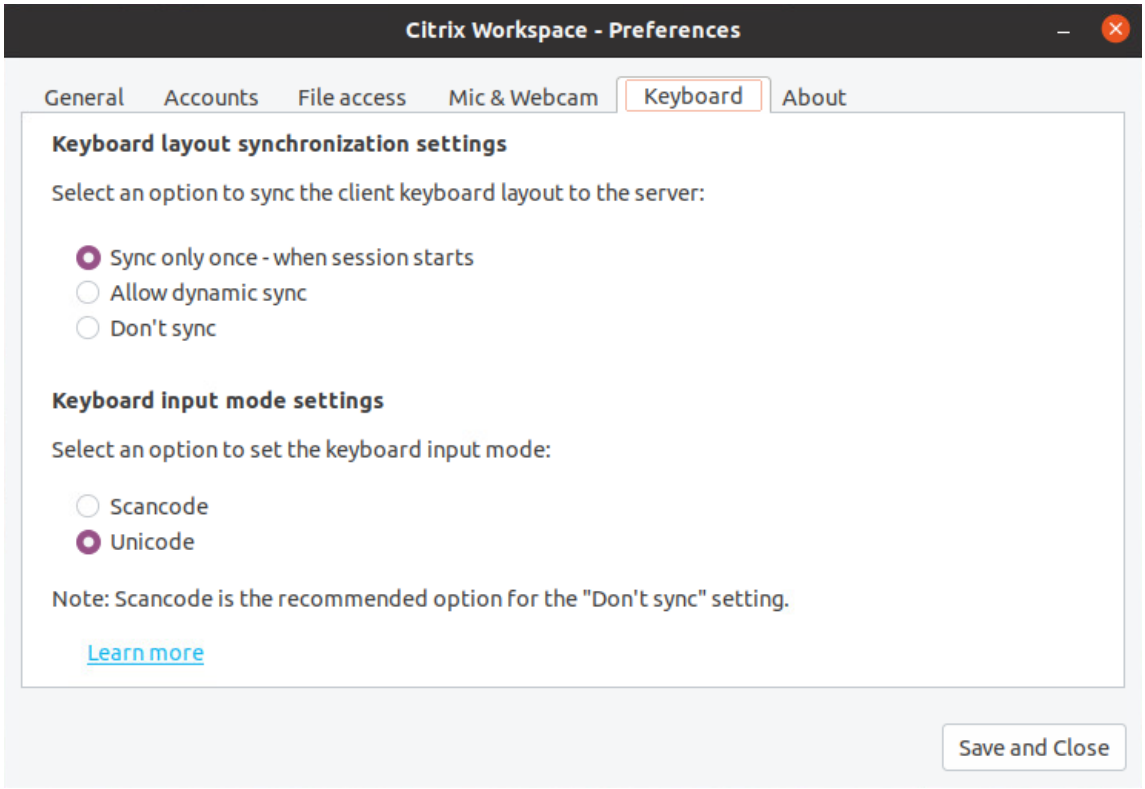
Keyboard input mode enhancements Previously, you were able to enable different keyboard input modes only by updating the value of `KeyboardEventMode` in the configuration file. There was no UI option to select the keyboard input mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with Citrix Workspace app 2309, you can configure different keyboard input modes from the newly introduced **Keyboard input mode settings** section. You can select **Scancode** or **Unicode** as keyboard input mode.

To configure keyboard input mode by using the GUI, do the following:

1. From the Citrix Workspace app icon in the notification area, select **Preferences**.
   The **Citrix Workspace** –**Preferences** dialog box appears.
2. Click Keyboard.
   You can see the **Keyboard input mode settings** section.



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, the Keyboard input mode setting is selected as **Unicode**. For more information on keyboard input mode, see the **Configure keyboard layout** section in the Keyboard layout synchronization documentation.

4. Click **Save and Close**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The keyboard configuration changes take effect once you reconnect to the application. If you change the keyboard input mode in the UI, the parameter value of the `KeyboardEventMode` in the `wfclient.ini` file is also updated automatically.

For example, consider a scenario where you're using a US international keyboard layout and the VDA is using the Russian keyboard layout.

When you choose **Scancode** and type the key next to Caps lock, the scancode `1E` is sent to the VDA. The VDA then uses `1E` to display the character `ф`.

If you choose **Unicode** and type the key next to Caps lock, the character `a` is sent to the VDA. So, even if the VDA uses the Russian keyboard layout, the character `a` appears on the screen.

Support for extended keyboard layouts Starting with Citrix Workspace app for Linux version 2309, the Scancode keyboard input mode supports the following extended keyboard layouts:

- Japanese 106 keyboard
- Portuguese ABNT/ABNT2 keyboards
- Multimedia keyboards

The Scancode keyboard input mode supports the extended keyboard layouts along with all keyboard layout synchronization modes.

This support is enabled by default. However, perform the following extra steps to configure the "Japanese 106 keyboard":

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardType=106 Keyboard (Japanese)
```

Client IME for East Asian languages Client Input Method Editor (IME) feature enhances input and display experience with Chinese, Japanese, and Korean (CJK) language characters in Citrix Workspace app for Linux. You can choose to use the Client IME when you have a favorite IME in Linux Client or IME is not available from the remote server.

To enable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
KeyboardEventMode=Unicode
UseLocalIM=True
```

If your client Linux distribution doesn't have a working iBus, you must set the KeyboardLayout value. You must explicitly set this value according to your IME language in the wfclient.ini configuration file as follows:

- For Chinese IME - KeyboardLayout=Chinese (PRC)
- For Japanese IME - KeyboardLayout=Japanese (JIS)
- For Korean IME - KeyboardLayout=Korean

Enhancement to support keyboard layout synchronization for GNOME 42

Starting with the 2305 version, Citrix Workspace app for Linux supports keyboard layout synchronization for desktops like Ubuntu 22.04 which uses the GNOME 42 desktop environment and later versions.

Keyboard layout support for Windows VDA and Linux VDA

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Swedish (no dead keys)	se	nodeadkeys	→	sv-SE	0000041d	se	-
Arabic	ara	-	→	ar-SA	00000401	ara	-
Arabic (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
German (Austria)	at	-	→	de-AT	00000407	at	-
Belgian (alt. ISO)	be	iso-alternate	→	fr-BE	0000080c	be	iso-alternate
Belgian	be	-	→	nl-BE	00000813	be	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Bulgarian	bg	-	→	bg-BG	00030402	bg	-
Bulgarian (traditional phonetic)	bg	phonetic	→	bg-BG	00040402	bg	phonetic
Bulgarian (new phonetic)	bg	bas_phonetic	→	bg-BG	00020402	bg	bas_phonetic
Portuguese (Brazil)	br	-	→	pt-BR	00000416	br	-
Belarusian	by	-	→	be-BY	00000423	by	-
English (Canada)	ca	eng	→	en-CA	00000409	ca	eng
Canadian Multilingual	ca	multix	→	fr-CA	00011009	ca	multix
French (Canada, legacy)	ca	fr-legacy	→	fr-CA	00000c0c	ca	fr-legacy
French (Canada)	ca	-	→	fr-CA	00001009	ca	-
French (Switzerland)	ch	fr	→	fr-CH	0000100c	ch	fr
German (Switzerland)	ch	-	→	de-CH	00000807	ch	-
Chinese (Simplified)	cn	-	→	en-US	00000409	us	-
Czech	cz	-	→	cs-CZ	00000405	cz	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Czech (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty
German	de	-	→	de-DE	00000407	de	-
German (Macintosh)	de	mac	→	de-DE	00000407	de	mac
Danish	dk	-	→	da-DK	00000406	dk	-
Estonian	ee	-	→	et-EE	00000425	ee	-
Spanish (Latin American)	es	-	→	es-ES	0000040a	es	-
Spanish (Macintosh)	es	mac	→	es-ES	0000040a	es	mac
Finnish	fi	-	→	fi-FI	0000040b	fi	-
French	fr	-	→	fr-FR	0000040c	fr	-
French (Macintosh)	fr	mac	→	fr-FR	0000040c	fr	mac
English (UK)	gb	-	→	en-GB	00000809	gb	-
English (Macintosh)	gb	mac	→	en-GB	00000809	gb	mac
English (UK, extended, with Win keys)	gb	extd	→	en-GB	00000452	gb	extd
Greek	gr	-	→	el-GR	00000408	gr	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Croatian	hr	-	→	hr-HR	0000041a	hr	-
Hungarian	hu	-	→	hu-HU	0000040e	hu	-
Irish	ie	-	→	en-IE	00001809	ie	-
Hebrew	il	-	→	he-IL	0002040d	il	-
English (India, with rupee)	in	eng	→	en-IN	00004009	in	eng
Iraqi	iq	-	→	ar-IQ	00000401	iq	-
Icelandic	is	-	→	is-IS	0000040f	is	-
Italian	it	-	→	it-IT	00000410	it	-
Japanese	jp	-	→	en-US	00000409	us	-
Japanese (Macintosh)	jp	mac	→	en-US	00000409	us	mac
Korean	kr	-	→	en-US	00000409	us	-
Spanish (Latin American)	latam	-	→	es-MX	0000080a	latam	-
Lithuanian	lt	-	→	lt-LT	00010427	lt	-
Lithuanian (IBM LST 1205-92)	lt	ibm	→	lt-LT	00000427	lt	ibm
Lithuanian (Standard)	lt	std	→	lt-LT	00020427	lt	std
Latvian	lv	-	→	lv-LV	00020426	lv	-
Norwegian	no	-	→	nb-NO	00000414	no	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Polish	pl	-	→	pl-PL	00000415	pl	-
Polish (QWERTZ)	pl	qwertz	→	pl-PL	00010415	pl	qwertz
Portuguese	pt	-	→	pt-PT	00000816	pt	-
Portuguese (Macintosh)	pt	mac	→	pt-PT	00000816	pt	mac
Romanian (standard)	ro	std	→	ro-RO	00010418	ro	std
Serbian	rs	-	→	sr-Cyrl-RS	00000c1a	rs	-
Serbian (Latin)	rs	latin	→	sr-Latn-RS	0000081a	rs	latin
Russian	ru	-	→	ru-RU	00000419	ru	-
Russian (typewriter)	ru	typewriter	→	ru-RU	00010419	ru	typewriter
Russian (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
Swedish	se	-	→	sv-SE	0000041d	se	-
Swedish (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
Slovenian	si	-	→	sl-SI	00000424	si	-
Slovak	sk	-	→	sk-SK	0000041b	sk	-
Slovak (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
Thai	th	-	→	th-TH	0000041e	th	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Thai (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
Tajik	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
Turkish	tr	-	→	tr-TR	0000041f	tr	-
Turkish (F)	tr	f	→	tr-TR	0001041f	tr	f
Chinese (Traditional)	tw	-	→	en-US	00000409	us	-
Ukrainian	ua	-	→	uk-UA	00000422	ua	-
English (US)	us	-	→	en-US	00000409	us	-
English (Macintosh)	us	mac	→	en-US	00000409	us	mac
English (Dvorak)	us	dvorak	→	en-US	00010409	us	dvorak
English (Dvorak, left-handed)	us	dvorak-l	→	en-US	00030409	us	dvorak-l
English (Dvorak, right-handed)	us	dvorak-r	→	en-US	00040409	us	dvorak-r
English (US, intl., with dead keys)	us	intl	→	en-US	00020409	us	intl

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Vietnamese	vn	-	→	vi-VN	0000042a	vn	-

VDA keyboard layout

The VDA keyboard layout feature helps you use the VDA keyboard layout regardless of the client's keyboard layout settings. It supports the following types of keyboard: PC/XT 101, 102, 104, 105, 106.

To use the server-side keyboard layout:

1. Launch the wfclient.ini file.
2. Change the value of the `KeyboardLayout` attribute as follows:

   ```
   KeyboardLayout=(Server Default)
   ```

   The default value for the `KeyboardLayout` attribute is (User Profile).
3. Relaunch the session for the changes to take effect.

Synchronize multiple keyboards at session start

Previously, only the active keyboard on the client was synchronized with VDA after the session started in full-screen mode. In this scenario, if you configured **Sync only once - when session launches** on your Citrix Workspace app, and you had to change to a different keyboard, you have to manually install the keyboard on your remote desktop. This feature is used mostly when the client side keyboard input mode is scancode input mode. Users can select a keyboard layout in a remote session as the active keyboard layout which is synchronized from the client keyboard layout list.

Starting with 2402, all available keyboards on the Linux client are synchronized with VDA after the session starts in full-screen mode. You can select the required keyboard from the list of installed keyboards on the VDA, after the session starts in full-screen mode.

Prerequisites:

On Citrix Workspace app for Linux:

Enable **Sync only once - when the session launches** in the keyboard preference setting. For more information, see the Keyboard layout synchronization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On VDA:

Enable the following VDA policies:

- Unicode Keyboard Layout Mapping. For more information, see Enable Unicode keyboard layout mapping or Keyboard and Input Method Editor (IME)
- Client keyboard layout synchronization and IME improvement. For more information, see Keyboard and Input Method Editor (IME)

Configuration on Citrix Workspace app for Linux:

This feature is applicable only on virtual desktops. This feature is disabled by default. To enable this feature, do the following:

1. Navigate to the `/config` folder and open the `All_Regions.ini` file.
2. Go to the `[Virtual Channels\Keyboard]` section and add the following entry:

```
1 SyncKbdLayoutList=TRUE
```

To disable this feature, set the value of `SyncKbdLayoutList` to *False*.

Configuration on VDA:

The feature **Synchronize multiple keyboards at session starts** is enabled by default on VDA. Update the VDA registry setting to disable it when needed:

1. Open the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create the DWORD entry **DisableKbdLayoutList** and set its value to 0. Setting the value to 1, disables the **Synchronize multiple keyboards at session start** feature.
3. Restart the session for the changes to take effect.

Enhanced keyboard and IME diagnostics tool

Starting with version 2411, a new self-service command line tool hosted in Windows Virtual Desktop app is supported by Citrix Workspace app for Linux to diagnose keyboard and Input Method Editor (IME) related issues. This tool meets various user requirements, provides platform versatility, and caters to personalized needs. The keyboard and IME functions depend on different configurations and capabilities in Virtual Delivery Agent and Citrix Workspace app. Incorrect settings in the Virtual Desktop Agent or client side might result in unexpected input behavior.

With this tool, you can easily identify issues that were previously difficult to find. They are:

- **Keyboard layout sync mode inconsistency**: Checks the keyboard layout sync settings and group policies and resolves problems in sync mode configurations within a given environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Client and VDA keyboard layout inconsistency**: Verifies if the client keyboard layout matches the VDA keyboard layout.
- **Transparent key pass-through from client to VDA**: Examines the windowing system, client transparent key pass-through settings, and session full-screen mode to suggest best practices.
- **Keyboard input mode inconsistency**: Reviews the VDA policy and the selected keyboard input mode to confirm if keyboard functions operate correctly.

Prerequisites

- Citrix Workspace app for Linux 2411 or higher.
- Windows VDA 2503 or higher.

This command line tool is hosted in Windows VDA as `CtxKbImeDiagnostics.exe`.

Interface	Description	Note
`CtxKbimeDiagnostics`	Shows diagnostic results for current user's ICA sessions.	If the user has admin privilege, it shows diagnostics for all active ICA sessions. If the user has no admin privilege, it shows diagnostics for the current user's ICA sessions.
`CtxKbimeDiagnostics [-v]`	Shows setting information and diagnostic results for current users ICA sessions.	Admin privilege shows diagnostics for all active ICA sessions.
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	Shows setting information and diagnostic results for this session.	
`CtxKbimeDiagnostics [-s Session_Id]`	Shows diagnostic results for a specific session.	Admin privilege can query other ICA sessions. Normal users can query their own sessions.
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	Shows all setting information and diagnostic results for a specific session.	Admin privilege can query other ICA sessions. Normal users can query their own sessions.
`CtxKbimeDiagnostics [-h]`	Shows supported arguments/parameters and examples.	Help interface.
`CtxKbimeDiagnostics [-V]`	Shows current tool version.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced keyboard settings

Starting with version 2601, Citrix Workspace app for Linux introduces enhanced keyboard settings that provide improved control over system shortcuts and keyboard input modes. These enhancements include UI settings for system shortcut pass-through (transparent key pass-through) and an automatic mode for keyboard input that dynamically selects the best input method based on the VDA type.

System shortcut pass-through settings

To configure system shortcut pass-through:

1. Select the **Keyboard** tab.
2. In the **System shortcut pass-through settings** section, select one of the following options:
    - **Local device** –Shortcuts are sent to the local Linux client.
    - **Fullscreen HDX session only** (Default) –When the VDA session is in full-screen mode, shortcuts are sent to the VDA session. Otherwise, shortcuts are sent to the local Linux client.
    - **Remote session** –Shortcuts are sent to the VDA session.

> **Note:**
>
> Keyboard configuration changes take effect in real time.

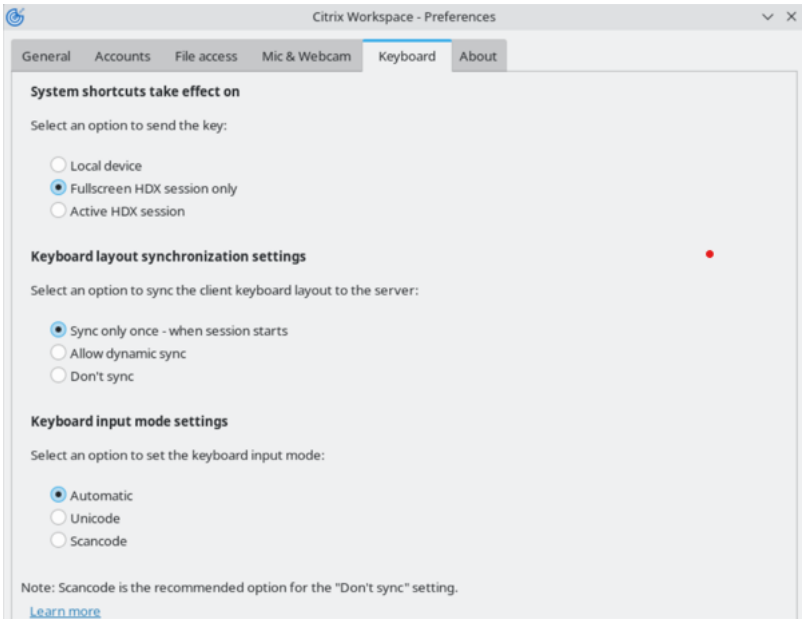
Automatic keyboard input mode

To configure keyboard input mode:

1. Select the **Keyboard** tab.
2. In the **Keyboard input mode settings** section, select one of the following options:
    - **Automatic** (Default) –Dynamically selects the keyboard input mode based on the current session. For Linux VDA sessions, the input mode is Scancode. For Windows VDA or Mac VDA sessions, the input mode is Unicode.
    - **Scancode**
    - **Unicode**

> **Note:**
>
> The keyboard configuration changes take effect when you modify the configuration in the UI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



USB

September 7, 2025

USB support enables users to interact with a wide range of USB devices when connected to a virtual desktop. Users can plug USB devices into their computers and the devices are redirected to their virtual desktop after enabling auto-redirection. You can enable auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default. USB devices available for remoting include the following:

- Flash drives
- Smartphones
- PDAs
- Printers
- Scanners
- MP3 players
- Security devices
- Tablets

USB redirection requires either Citrix Virtual Apps and Desktops 7.6 or later.

The following isochronous features in USB devices are supported in typical low latency or high speed LAN environments:

- Webcams

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microphones
- Speakers
- Headsets

But usually the standard audio or webcam redirection are more suitable.

The following types of devices are supported directly in a virtual apps and desktops session, and so do not use USB support:

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

> **Note:**
>
> Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. For information on configuring policy rules for other specialist USB devices, see CTX119722.

By default, certain types of USB devices aren't supported for remoting through Citrix Virtual Apps and Desktops™ or Citrix DaaS. For example, a user might have a NIC attached to the system board by internal USB. Remoting this NIC isn't appropriate. By default, the following types of USB device aren't supported for use in the virtual apps and desktops:

- Bluetooth dongles
- Integrated NICs
- USB hubs

To update the default list of USB devices available for remoting, edit the `usb.conf` file in the `$ICAROOT/` folder. For more information, see the Update the list of USB devices available for remoting section.

To allow the remoting of USB devices to virtual desktops, enable the USB policy rule. For more information, see the Citrix Virtual Apps and Desktops documentation.

How USB support works

When a user plugs a USB device, it's checked against the USB policy. And, if allowed, redirected to the virtual desktop. If the default policy denies the device, it's available only to the local desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consider a user plugging in a USB device in desktops accessed through desktop appliance mode. In this case, that device is auto-redirected to the virtual desktop after enabling auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default. To configure the auto-redirection of USB devices, do the following:

1. Navigate to the `$Home/.ICAClient/wfclient.ini` configuration file.
2. Add the following entry:

   `DesktopApplianceMode=True`
3. Navigate to `/opt/Citrix/ICAClient/usb.conf` configuration file.
4. Set any of the following device rules:

   ALLOW - Set the **ALLOW** keyword to allow a specific device based on its Vendor ID (vid) and Product ID (pid).

   CONNECT –Set the **CONNECT** keyword to allow a specific device and automatically redirect it based on its Vendor ID (vid) and Product ID (pid).

   Sample device rule:

   ALLOW: vid=046D pid=0002 # Allow a specific device

   CONNECT: vid=046D pid=0002 # Allow and auto-connect a specific device

The session window must have focus when the user plugs in the USB device for redirection to occur, unless desktop appliance mode is in use.

> **Note:**
>
> If you configure the USB policy to a device with the "CONNECT"keyword and set the `DesktopApplianceMode` to True, the USB device redirects to the VDA session automatically. When the `DesktopApplianceMode` mode is set to false, the USB device doesn't redirects to the VDA session automatically.

Known limitation:

- For USB redirection, the policies defined in the `usb.conf` file might not work and the USB devices might not be redirected into session. This issue occurs if you have more than 2000 characters present in the `usb.conf` file. As a workaround, you can remove the existing comments to the policies to reduce the number of characters in the `usb.conf` file.
- Generic USB redirection is supported only when the virtual desktop window is focused.

Mass storage devices

Consider that a user disconnects from a virtual desktop when a USB mass storage device (MSD) is still plugged in to the local desktop. In this case, that device isn't redirected to the virtual desktop when

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the user reconnects. To verify that the MSD is redirected to the virtual desktop, the user must remove and reinsert the device after reconnecting.

> **Note:**
>
> If you insert an MSD into a Linux workstation configured to deny remote support for USB MSDs, Citrix Workspace app doesn't accept the device. And a separate Linux file browser might open. So, Citrix recommends that you pre-configure user devices with the **Browse removable media when inserted** setting cleared by default. On Debian-based devices, do this using the Debian menu bar by selecting **Desktop > Preferences > Removable Drives and Media**. And on the **Storage** tab, under **Removable Storage**, clear the **Browse removable media when inserted** check box.

For the Client USB device redirection, note the following points.

> **Notes:**
>
> Consider that the Client USB device redirection server policy is turned on. In this case, the MSDs are directed as USB devices even if client drive mapping is turned on.

USB classes

The default USB policy rules allow the following classes of USB device:

- Audio (Class 01)

  Includes microphones, speakers, headsets, and MIDI controllers.

- Physical Interface (Class 05)

  These devices are similar to HIDs, but generally provide real-time input or feedback. Also, include force feedback joysticks, motion platforms, and force feedback exoskeletons.

- Still Imaging (Class 06)

  Includes digital cameras and scanners. Digital cameras support the still imaging class that uses the following to transfer images to a computer or other peripheral:

  - Picture Transfer Protocol (PTP)
    or,
  - Media Transfer Protocol (MTP)

  Cameras might also appear as mass storage devices. And it might be possible to configure a camera to use either class, through the setup menus provided by the camera itself.

  If a camera appears as an MSD, client drive mapping is used, and USB support isn't required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Printers (Class 07)

  In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers might have an internal hub or be composite devices. In both cases, the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging.

  Printers normally work appropriately without USB support.

- Mass Storage (Class 08)

  The most common MSDs are USB flash drives. Others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There's a wide variety of devices having internal storage which also presents a mass storage interface. These devices include media players, digital cameras, and mobile phones. Known subclasses include:

- 01 Limited flash devices
- 02 Typically CD/DVD devices (ATAPI/MMC-2)
- 03 Typically tape devices (QIC-157)
- 04 Typically floppy disk drives (UFI)
- 05 Typically floppy disk drives (SFF-8070i)
- 06 Most MSDs use this variant of SCSI

  MSDs can often be accessed through client drive mapping, and so USB support isn't required.

  Important: Some viruses are known to propagate actively using all types of MSDs. Consider carefully whether there's a business requirement to allow the use of MSDs, either through client drive mapping, or USB support. To reduce this risk, the server might be configured to prevent files being run-through client drive mapping.

  > **Note:**
  >
  > If a user requires to redirect a USB 3.0 driver to the Linux VDA using generic USB redirection, plug-in the USB flash drive into a USB 3.0 slot.

- Content Security (Class 0d)

  Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.

- Personal Healthcare (Class 0f)

  These devices include personal healthcare devices such as the following:

  - Blood pressure sensors
  - Heart rate monitors

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Pedometers
    - Pill monitors
    - Spirometers

- Application and Vendor Specific (Classes fe and ff)

  Many devices use vendor-specific protocols or protocols not standardized by the USB consortium, and these devices usually appear as vendor-specific (class ff).

USB device classes

The default USB policy rules deny the following classes of USB devices:

- Communications and CDC Control (Classes 02 and 0a)

  Includes modems, ISDN adapters, network adapters, and some telephones and fax machines.

  The default USB policy does not allow these devices, because one of them might be providing the connection to the virtual desktop itself.

- Human Interface Devices (Class 03)

  Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are the following:

    - Keyboards
    - Mice
    - Pointing devices
    - graphic tablets
    - Sensors
    - Game controllers
    - Buttons
    - Control functions

  Subclass 01 is known as the boot interface class and is used for keyboards and mice.

  The default USB policy does not allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). This setting is because most keyboards and mice are handled appropriately without USB support. And it's normally necessary to use these devices locally as well remotely when connecting to a virtual desktop.

- USB Hubs (Class 09)

  USB Hubs allow extra devices to be connected to the local computer. It isn't necessary to access these devices remotely.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Smart card (Class 0b)

  Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card equivalent chip.

  Smart card readers are accessed using smart card remoting and do not require USB support.

- Video (Class 0e)

  The video class covers devices that are used to manipulate video or video-related material, such as:

  - Webcams
  - Digital camcorders
  - Analog video converters
  - Some television tuners
  - Some digital cameras that support video streaming

  By default, optimum webcam performance is provided by HDX™ RealTime Webcam Video Compression.

- Wireless Controllers (Class e0)

  Includes a wide variety of wireless controllers, such as ultrawide band controllers and Bluetooth.

  Some of these devices might provide critical network access, or connect critical peripherals such as Bluetooth keyboards or mice.

  The default USB policy does not allow these devices. However, there might be particular devices it's appropriate to provide access to using USB support.

List of USB devices

You can update the range of USB devices available for remoting to desktops by editing the list of default rules in the `usb.conf` file on the user device in `$ICAROOT/`.

You can update the list by adding new policy rules to allow or deny USB devices not included in the default range. Rules created by an administrator in this way control which devices are offered to the server. The rules on the server control which of these devices are to be accepted.

The default policy configuration for disallowed devices is:

DENY: class=09 # Hub devices

DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)

DENY: class=0b # Smartcard

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

USB policy rules

Tip: When creating policy rules, see the USB Class Codes, available from the USB website at http://www.usb.org/. Policy rules in the usb.conf file on the user device take the format {ALLOW DENY:} followed by a set of expressions that are based on values for the following tags

Tag	Description
VID	Vendor ID from the device descriptor
REL	Release ID from the device descriptor
PID	Product ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor
SubClass	SubClass from either the device descriptor or an interface descriptor
`Prot`	Protocol from either the device descriptor or an interface descriptor

When creating policy rules, be aware of the following:

- The rules are case-insensitive.
- The rules might have an optional comment at the end, introduced by "#."A delimiter isn't required and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- Whitespace used as a separator is ignored, but can't appear in the middle of a number or identifier. For example, Deny: Class=08 SubClass=05 is a valid rule; Deny: Class=0 8 Sub Class=05 isn't.
- Tags must use the matching operator "=."For example, VID=1230.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example

The following example shows a section of the `usb.conf` file on the user device. For these rules to be implemented, the same set of rules must exist on the server.

```
ALLOW: VID=1230 PID=0007 \\# ANOther Industries, ANOther Flash Drive

DENY: Class=08 SubClass=05 \\# Mass Storage Devices
DENY: Class=0D \\# All Security Devices
```

Start-up modes

Using desktop appliance mode, you can change how a virtual desktop handles previously attached USB devices. In the **WfClient** section of the `$ICAROOT/config/module.ini` file on each user device, set `DesktopApplianceMode=Boolean` as follows.

TRUE	Any USB devices that are already plugged in are available in start-up. The devices are available in start-up only if the devices are not disallowed with a Deny rule in the USB policies. These USB policies are set either on the server (registry entry) or on the user device (policy rules configuration file).
FALSE	No USB devices are available in the start-up.

> **Note:**
>
> Set the "CONNECT"keyword to enable the auto redirect of a device when a session starts. Also, set the "ALLOW"keyword to allow auto-redirect of a device only after a session starts. However, if you set the CONNECT or ALLOW keyword, it auto-redirects the device when unplugged and plugged in during a session.

Configure auto-redirection of USB devices

Earlier, during a session, when a device was unplugged and plugged it automatically redirected. As a result, the device was auto-connected to the VDA. With the Citrix Workspace app 2207 release, you are required to enable auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure the auto-redirection of USB devices (regular and composite devices), do the following:

1. Navigate to the $Home/.ICAClient/wfclient.ini configuration file.
2. Add the following entry:

   DesktopApplianceMode=True
3. Navigate to /opt/Citrix/ICAClient/usb.conf configuration file.
4. Set any of the following device rules:

   - CONNECT –Set the "CONNECT"keyword to enable auto redirect of a device when a session starts.
   - ALLOW –Set the "ALLOW"keyword to allow auto-redirect of a device only after a session starts.

   However, if the CONNECT or ALLOW keyword is set, the device is auto-redirected when it unplugged and plugged in during a session.

Sample device rule:

CONNECT: vid=046D pid=0002 # Allow a specific device by vid/pid'

ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid'

Composite USB device redirection

Starting with the 2207 version, Citrix Workspace app allows splitting of composite USB devices. A composite USB device can perform more than one function. These functions are accomplished by exposing each of those functions using different interfaces. Examples of composite USB devices include HID devices that consist of audio and video input and output.

Currently composite USB device redirection is available in desktop session only. The split devices appear in the Desktop Viewer.

Earlier when a device was unplugged and plugged in during a session, the device was auto-redirected. As a result, the device was auto connected to the VDA. With this release, you are required to enable auto-redirection manually through configuration file settings. Auto-redirection of composite USB devices is disabled by default.

USB 2.1 and later supports the notion of USB composite devices where multiple child devices share a single connection with the same USB bus. Such devices employ a single configuration space and shared bus connection where a unique interface number 00-ff is used to identify each child device. This setting is not the same as a USB hub which provides a new USB bus origin for other independently addressed USB devices for connection.

Composite devices found on the client endpoint can be forwarded to the virtual host as either:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- a single composite USB device, or
- a set of independent child devices (split devices)

When a composite USB device is forwarded, the entire device becomes unavailable to the endpoint. This action blocks the local usage of the device for all applications on the endpoint, including the Citrix Workspace client needed for an optimized HDX remote experience.

Consider a USB headset device with both audio device and HID button for mute and volume control. If the entire device is forwarded using a generic USB channel, the device becomes unavailable for redirection over the optimized HDX audio channel. However, you can achieve the best experience when sending the audio through the optimized HDX audio channel unlike the audio sent using host-side audio drivers through generic USB remoting. It happens because of the noisy nature of the USB audio protocols.

You also notice issues when the system keyboard or pointing device are part of a composite device with other integrated features that are required for the remote session support. When a complete composite device is forwarded, the system keyboard or mouse becomes inoperable at the endpoint, except within the remote desktop session or application.

To resolve these issues, Citrix recommends that you split the composite device and forward only the child interfaces that use a generic USB channel. This setting ensures that the other child devices are available for use by apps on the client endpoint. This client endpoint includes the Citrix Workspace app that provides optimized HDX experiences, while forwarding only the required devices and making them available to the remote session.

Device Rules:

As with regular USB devices, the composite devices for forwarding are selected based on the device rules set in the Citrix Workspace app configuration. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

Each rule consists of the following that match the actual devices at the endpoints USB subsystem:

- an action keyword such as Allow, Connect, or Deny
- a colon (:)
- and zero or more filter parameters

The preceding filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a # character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

To modify the device rules, do the following:

1. Navigate to the /opt/Citrix/ICAClient/usb.conf file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Update the device rules as required.

Sample device rules:

```
ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid

ALLOW: vid=0505 class=03 subclass=01 # Allow any pid for vendor 0505
w/subclass=01

DENY: vid=0850 pid=040C # deny a specific device (including all child
 devices)

DENY: class=03 subclass=01 prot=01 # deny any device that matches all
 filters

CONNECT: vid=0911 pid=0C1C # Allow and auto-connect a specific device


ALLOW: vid=0286 pid=0101 split=01 # Split this device and allow all
interfaces

ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Split and allow only 2
 interfaces

CONNECT: vid=1050 pid=0407 split=01 intf=02 # Split and auto-connect
interface 2

DENY: vid=1050 pid=0407 split=1 intf=03 # Prevent interface 03 from
being remoted
```

You can use any of the following filter parameters to apply rules to the encountered devices:

Filter parameter	Description
vid=xxxx	USB device vendor ID (four-digit hexadecimal code)
pid=xxxx	USB device product ID (four-digit hexadecimal code)
rel=xxxx	USB device release ID (four-digit hexadecimal code)
class=xx	USB device class code (two-digit hexadecimal code)
subclass=xx	USB device subclass code (two-digit hexadecimal code)
prot=xx	USB device protocol code (two-digit hexadecimal code)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter parameter	Description
split=1 (or split=0)	Select a composite device to be split (or non-split)
`intf=xx[,xx,xx,...]`	Selects a specific set of child interfaces of a composite device (comma-separated list of two-digit hexadecimal codes)

The first six parameters select the USB devices for which the rule must be applied. If any parameter is not specified, the rule matches a device with ANY value for that parameter.

The USB Implementors Forum maintains a list of defined class, subclass, and protocol values in Defined Class Codes. USB-IF also maintains a list of registered vendor IDs. You can check the vendor, product, release, and interface IDs of a specific device using a free tool like `lsusb`:

```
 <username@username>-ThinkPad-T470:/var/log$ lsusb

Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW

Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.

Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera

Bus 001 Device 003: ID 8087:0a2b Intel Corp.

Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver

Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver

Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.

Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

```
    | <username@username>-ThinkPad-T470:/var/log$ lsusb -t

    /:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000
       M

    /:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M

    /:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
8
9       |__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage,
            5000M
10
11      /:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M
12
13      |__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M
14
15          |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=
                usbhid, 12M
16
17          |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=
                usbhid, 12M
18
19          |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=
                usbhid, 12M
20
21          |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12
                M
22
23          |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=,
                 12M
24
25          |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12
                M
26
27          |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12
                M
28
29          |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=
                usbhid, 12M
30
31      |__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=
            usbhid, 12M
32
33      |__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
            usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
            usbhid, 12M
36
37      |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39      |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41      |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43      |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45      |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
            |
```

When present, the last two parameters apply only to USB composite devices. The split parameter de-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

termines if a composite device must be forwarded as a split device or as a single composite device.

Split=1 indicates that the selected child interfaces of a composite device must be forwarded as split devices.
Split=0 indicates that the composite device must not be split.

> **Note:**
>
> If the split parameter is omitted, Split=0 is assumed.

The `intf` parameter selects the specific child interfaces of the composite device to which the action must be applied. If omitted, the action applies to all interfaces of the composite device.

Consider a composite USB device (For example, the Bloomberg 4 keyboard) with six interfaces:

- Interface 0 - Bloomberg 4 Keyboard HID
- Interface 1 - Bloomberg 4 Keyboard HID
- Interface 2 - Bloomberg 4 HID
- Interface 3 - Bloomberg 4 Keyboard Audio Channel
- Interface 4 - Bloomberg 4 Keyboard Audio Channel
- Interface 5 - Bloomberg 4 Keyboard Audio Channel
- The suggested rules for this type of device are:

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 # Bloomberg 4 Keyboard
HID

CONNECT: vid=1188 pid=9545 split=01 intf=01 # Bloomberg 4 Keyboard
HID

CONNECT: vid=1188 pid=9545 split=01 intf=02 # Bloomberg 4 HID

DENY: vid=1188 pid=9545 split=01 intf=03 # Bloomberg 4 Keyboard Audio
 Channel

DENY: vid=1188 pid=9545 split=01 intf=04 # Bloomberg 4 Keyboard Audio
 Channel

DENY: vid=1188 pid=9545 split=01 intf=05 # Bloomberg 4 Keyboard Audio
 Channel
```

Composite USB device redirection with Citrix Viewer

To connect the USB devices from the **Devices** section, do the following:

1. In a desktop session, navigate to the Desktop Viewer under **Devices**.
   The split USB devices appear.

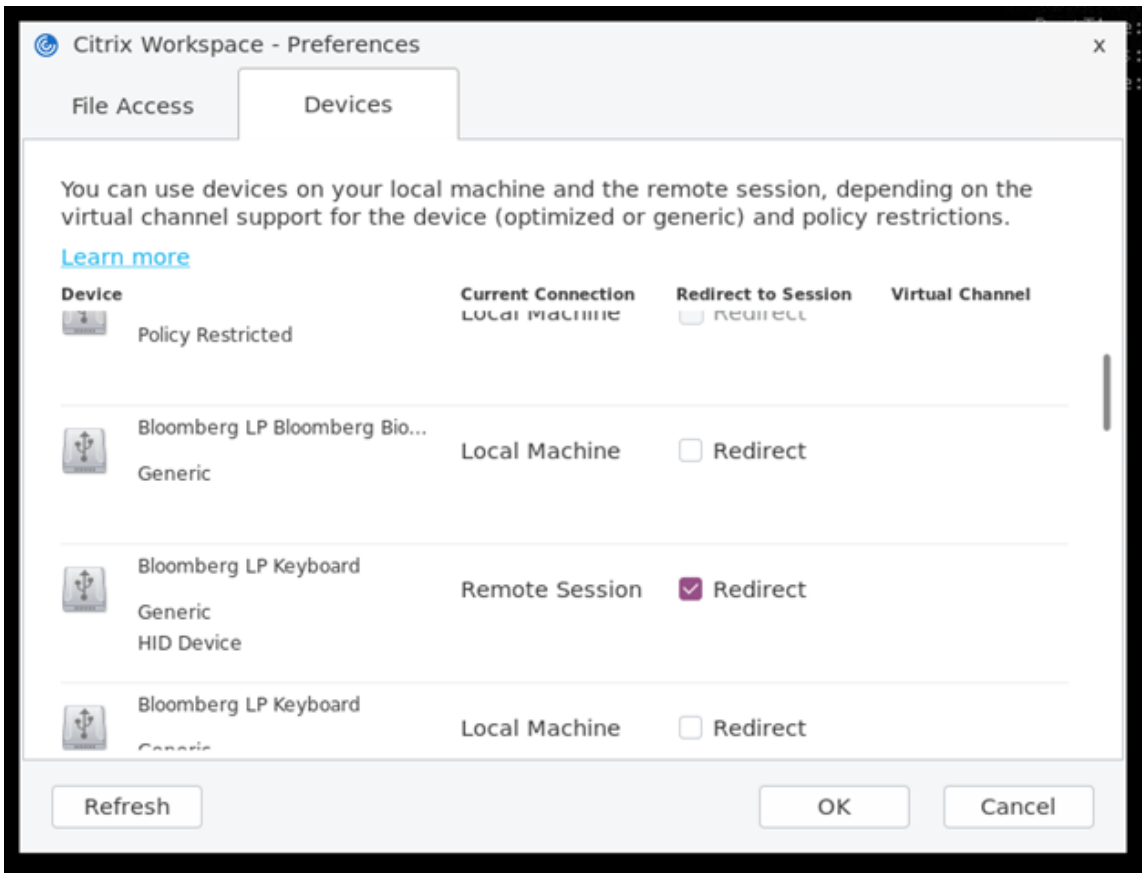
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. To connect a device, select the required menu item.

To connect the USB devices from the **Preferences** section, do the following:

1. Navigate to the **Preferences > Devices** section.
   The split USB devices appear.



2. Select the check boxes next to the devices, as required.
3. Click **OK**.

The selected configuration is applied to the device connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Clear the required menu item or check boxes next to the device to disconnect a device.

Enhancement for composite USB auto-redirection Previously, you had to set **DesktopAppliance-Mode** to *True* in the configuration file to auto-redirect USB devices when a session starts.

With the 2402 release, you are able to manage device connection settings from a UI on the Citrix Workspace app for Linux, without having to depend on configuration files.

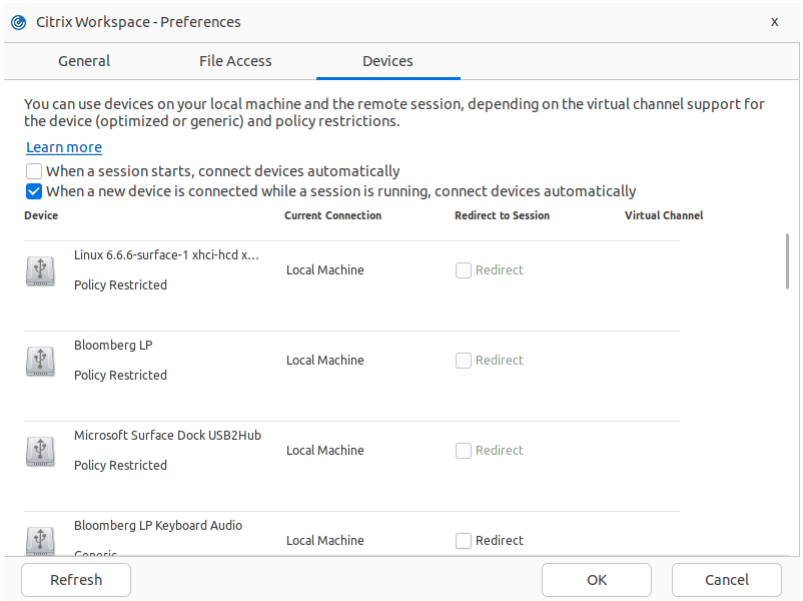
The following two options are added on the **Devices** section in the **Preferences** screen:

- When a session starts, connect devices automatically. By default, this checkbox isn't selected.
- When a new device is connected while a session is running, connect devices automatically. By default, this checkbox is selected.

This feature is enabled by default.

To configure the composite USB redirection by using the GUI, do the following:

1. From the Desktop Viewer toolbar of an HDX session, select **Preferences**. The **Citrix Workspace –Preferences** dialog box appears.
2. Click **Devices**. You can see the **Devices** section.



3. Select one or both of the following options as per your requirement:
    - **When a session starts, connect devices automatically** - When this option is selected, the USB devices are automatically connected to the virtual desktop when a session starts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **When a new device is connected while a session is running, connect devices automatically** - When this option is selected, the USB devices are automatically connected to the virtual desktop while a session is in-progress.

4. Click **OK**.

When one or more HDX sessions are configured for auto-redirection, the behaviors are as follows:

- If there's an HDX session on focus, all USB devices are auto-redirected.
- If there's no HDX session on focus, USB devices are auto-redirected to the last started HDX session.
- After a USB device is redirected, an end user can stop it using the HDX session's toolbar or directly close the HDX session. In this case, the USB device is disconnected and connected back to the client machine. The end user can redirect it again anytime.

Composite USB device redirection using DDC policies

Previously, the composite USB device redirection was managed on the client side. There was no option to manage it on VDA.

Starting with the 2405 release, you can manage the composite USB device redirection on VDA using the DDC policies. The rules set on the VDA take preferences over the rules set on the client. Client can interpret the value set on VDA.

With this release, Citrix Workspace app for Linux supports the following policies which helps you to manage the usage of the composite USB device redirection:

- Client USB device redirection
- Client USB device redirection rules
- Client USB device redirection rules (Version 2)
- Allow existing USB devices to be automatically connected
- Allow newly arrived USB devices to be automatically connected

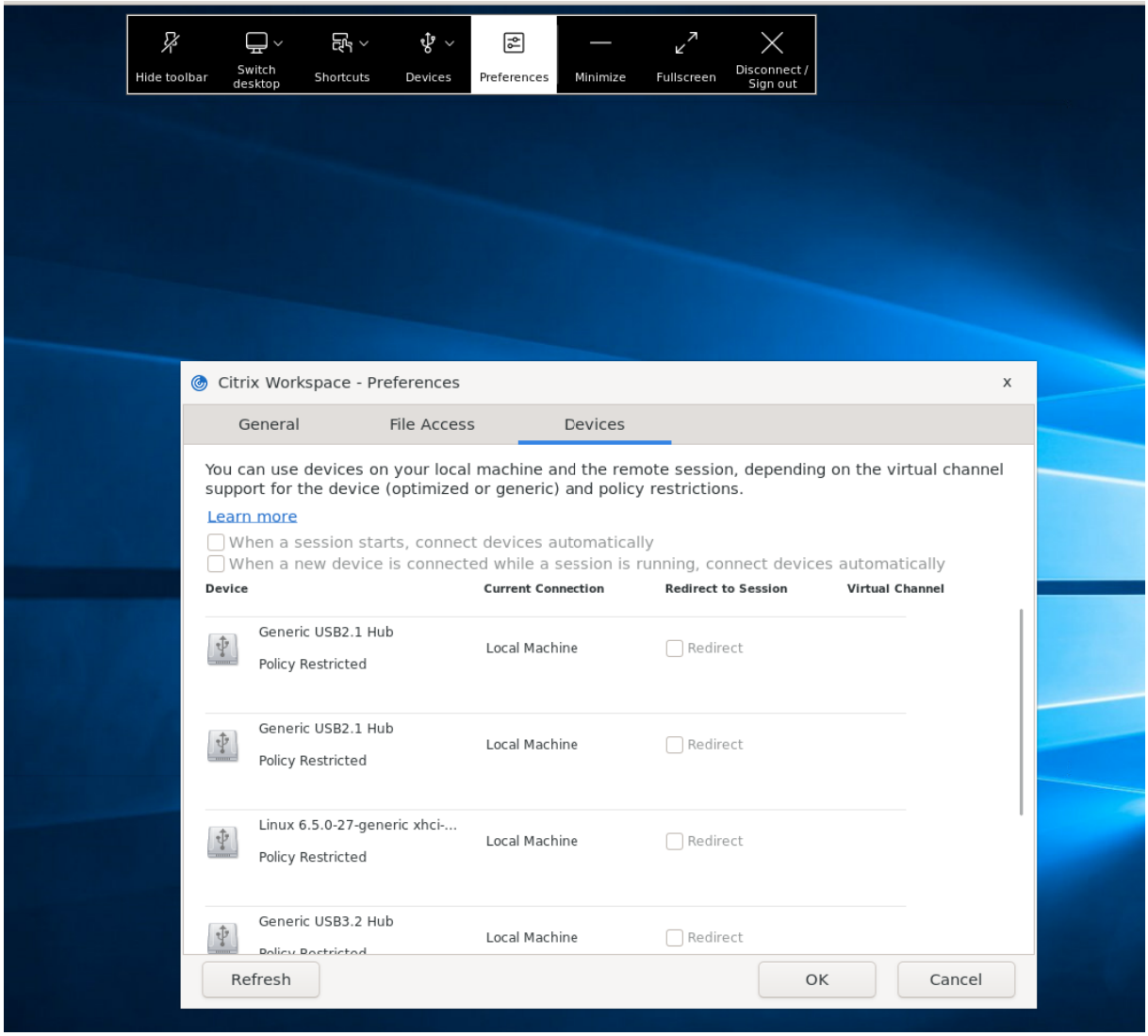
> **Note:**
>
> To configure the preceding polices, users can refer to the documents see Client USB device redirection document.

Desktop Viewer's updates according to the polices

- If the **Client USB device redirection** policy is set to *Prohibited* on DDC, the **Devices** on the toolbar will be set to insensible and the **Devices** option on the **Citrix Workspace app - Preferences** screen won't be visible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Based on the values set for **Allow existing USB devices to be automatically connected** and **Allow newly arrived USB devices to be automatically connected** policies, the following checkboxes might be enabled or disabled on the **Devices** option on the **Citrix Workspace app - Preferences** screen:
  - **When a session starts, connect devices automatically**
  - **When a new device is connected while a session is running, connect devices automatically**



SANE redirection

April 22, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with version 2508, Citrix Workspace app for Linux supports scanner redirection. You can connect a scanning device to the local endpoint and redirect it to a virtual session. This feature lets you access scanned files within the Citrix Workspace app session and upload documents to other apps that are accessible through Citrix Workspace app.

For more information, see SANE redirection.

Requirements

- Citrix Virtual Apps and Desktops 2503 or later

Default behavior

This feature is enabled by default.

Limitations

- If a session is using the scanner and a scan is in progress, attempting to use the scanner from another app in the same session or from a second session causes the first session scan operation to fail abruptly.
- Some third-party scanners can fail to scan in color and grayscale modes. This issue occurs when Citrix Workspace app and the scanner drivers use different versions of the JPEG library.

Configure scanner redirection

To disable this feature:

1. Navigate to `/opt/Citrix/ICAClient/config/module.ini`.
2. Set `VDSCAN=Off`.

Webcams

September 7, 2026

By default, optimum webcam performance is provided by HDX™ RealTime Webcam Video Compression. In some circumstances, however, you might require users to connect webcams using USB support. To connect webcams using USB support, disable HDX RealTime Webcam Video Compression.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Webcam redirection

The following are a few points on webcam redirection:

- Webcam redirection is compatible with and without RTME.
- Webcam redirection works for 32-bit and 64-bit applications. For example, Skype, GoToMeeting. Use a 32-bit browser or 64-bit browser to verify webcam redirection online. For example, `https://webcamtests.com/`.
- Webcam usage is exclusive to applications. For example, when Skype is running with a webcam and you launch GoToMeeting, exit Skype to use the webcam with GoToMeeting.

Webcam redirection for 64-bit apps

Starting with the 2305 release, webcam redirection is supported for 64-bit applications.

System requirements

- `GStreamer` framework version 0.1.x or 1.x depending on the current version installed in the system.
- `ICAClient` version greater than 2106 in case it is using `GStreamer` 1.x
- `Gstreamer` version and plug-ins:
  - `gstreamer1.0-plugins-base`
  - `gstreamer1.0-plugins-bad`
  - `gstreamer1.0-plugins-good`
  - `gstreamer1.0-plugins-ugly`
  - `gstreamer1.0-vaapi plugin` and `libva` library
  - x264 library

> **Note:**
>
> The version of the `GStreamer` plug-in must be consistent with the version of the `GStreamer` framework. For example, if you install the `Gstreamer`1.2.4, the version of all `Gstreamer`1.x plug-ins must be 1.2.4.

Webcam redirection configuration

Do the following steps to activate and configure the webcam redirection feature for 64-bit apps on Citrix Workspace app for Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Verify the `ICAClient` configuration Set the `AllowAudioInput` value to **True** to enable the webcam redirection feature. By default, this value is set to **True** during the installation of `ICAClient`.

If the `AllowAudioInput` value is set to **False**, do the following to enable the webcam redirection feature:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. Set the `AllowAudioInput` value to **True**.

   AllowAudioInput=True

Step 2: Verify the Theora encoder configuration After you have successfully installed the `ICAClient` and the `AllowAudioInput` value is set to **True**, by default the Theora encoder is configured. This encoder is a software-based encoder with acceptable performance. However, this encoder supports only 32-bit apps on a VDA.

Do the following to verify that the Theora encoder supports 32-bit apps:

1. Install Firefox 32-bit on a VDA.
2. Access the webcam test site at `https://webcamtests.com/`

The Theora encoder does not support the webcam redirection feature for 64-bit apps on a VDA. Configure the H264 encoder option to support the webcam redirection feature for 64-bit apps on VDA.

Step 3: Configure H264 encoder H264 encoder supports the webcam redirection feature for 64-bit apps on the VDA. To enable the H264 encoder, you must do the following:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. Set the `HDXH264InputEnabled` value to **True**.

   HDXH264InputEnabled=True

Do the following to verify that the H264 encoder supports 64-bit apps:

1. Install Firefox 64-bit on a VDA.
2. Access the webcam test site at `https://webcamtests.com/`.

Step 4: Verify system dependencies After configuring the H264 encoder, if the webcam redirection feature does not support 64-bit apps on the VDA verify the system dependencies.

The webcam redirection feature for the 64-bit app is based on the `GStreamer` framework. The `ICAClient` uses `GStreamer` framework version 0.1.x or 1.x depending on the current version installed in your system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4.1: Verify `ICAClient` version Verify whether the `ICAClient` version is greater than 2106 in case it is using `GStreamer` 1.x. Previous versions of `ICAClient` might fail.

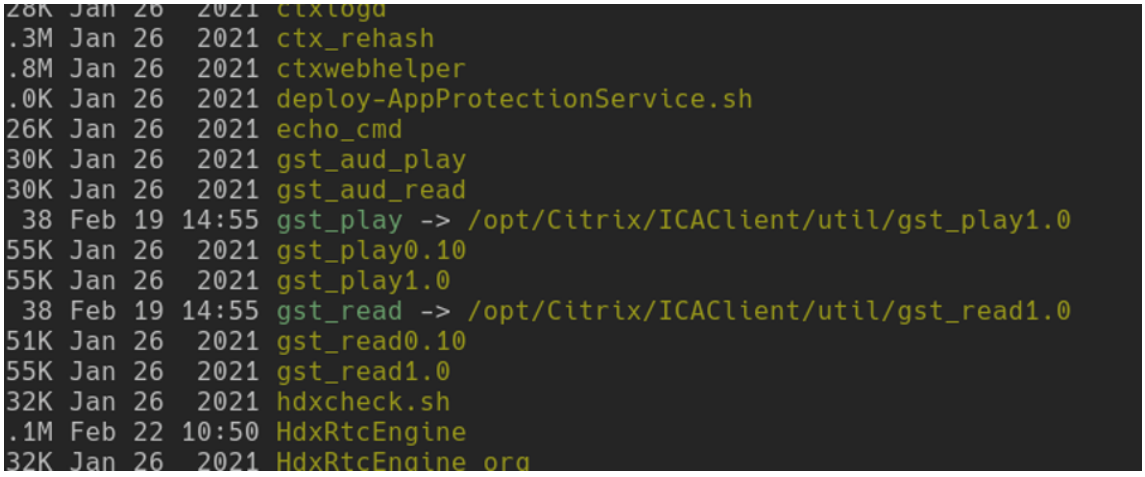
Do the following steps to verify the `ICAClient` version is based on the `GStreamer` framework installed in your system:

1. Enter the following commands in a command-line:

```
cd /opt/Citrix/ICAClient/util
```

```
ls -alh
```

2. Verify whether the `gst_read symlink` is linked to `gst_read1.0` or `gst_read0.1.` as shown in the following image:



You can also run the `workspaceappcheck.sh` script in the `util` directory and verify the output of the section referring to `GStreamer` dependencies.

Citrix recommends using the `ICAClient` version greater than or equal to 2106 and `GStreamer` 1.x.

Step 4.2: Verify `GStreamer` version and plug-ins Apart from the `GStreamer` 1.x framework, you must install the following required plug-ins:

- `Gstreamer1.0-plugins-base`
- `Gstreamer1.0-plugins-bad`
- `Gstreamer1.0-plugins-good`
- `Gstreamer1.0-plugins-ugly`
- `Gstreamer1.0-vaapi plugin`
- `ibva library`
- `x264 library`

For more information to install the preceding `plugins`, see the `GStreamer` installation guide.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The version of the `GStreamer` plug-in must be consistent with the version of the `GStreamer` framework. For example, if you install `Gstreamer1.2.4`, the version of all `Gstreamer1.x` plug-ins must be 1.2.4.

Run the following command to check the current version of the `GStreamer` framework:

```
gst-inspect-1.0 --gst-version
```

For information about troubleshooting, see Webcam in the troubleshooting section.

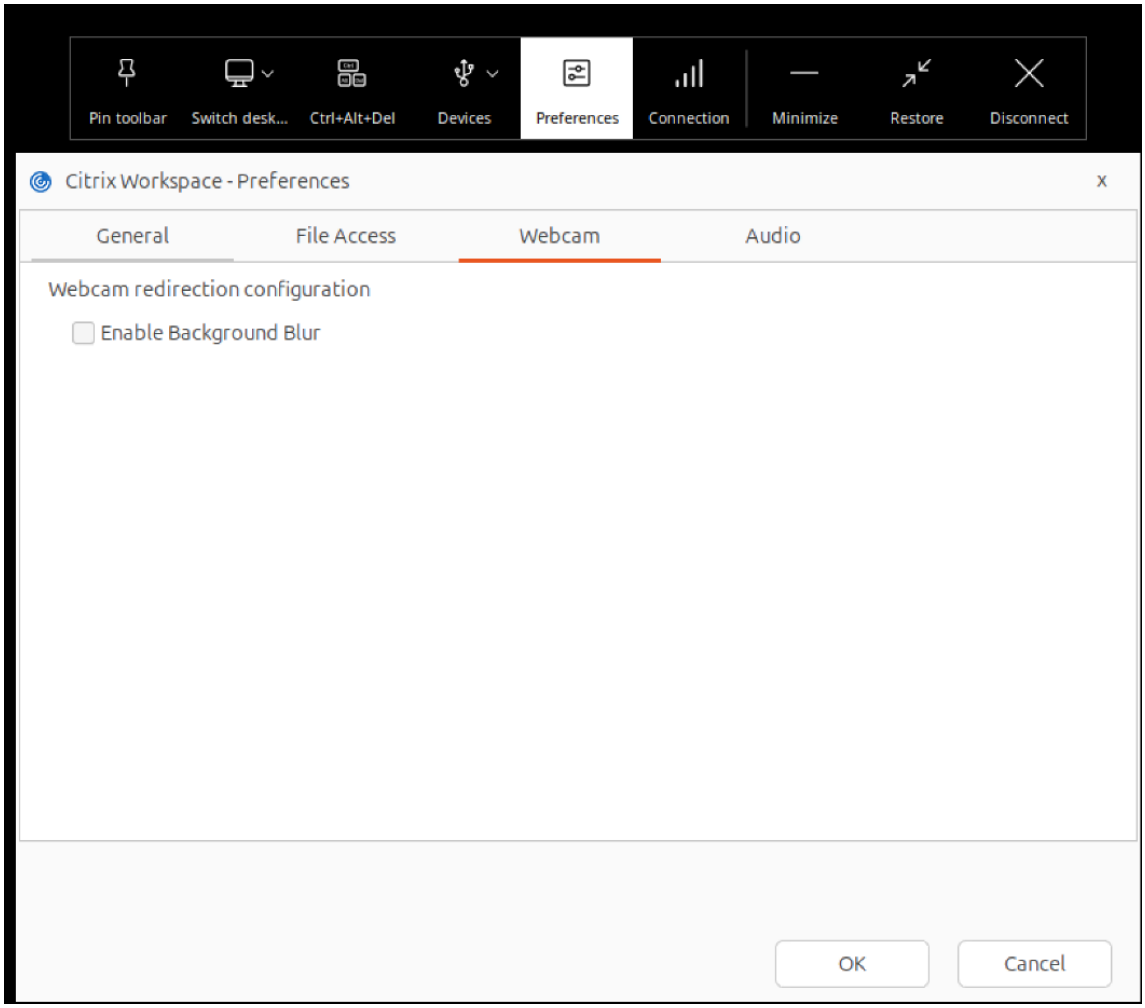
Background blur for webcam redirection using UI

Starting with version 2508, you can enable background blur for webcam redirection using the graphical user interface.

To enable background blur inside the session for webcam redirection, do the following:

1. Click **Preferences** from the Desktop Viewer. The **Citrix Workspace Preferences** dialog box appears.
2. Click the **Webcam** tab. The following dialog box appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select the **Enable Background Blur** check box to enable background blur for webcam redirection.
4. Click **OK**.

> **Note:**
>
> The selected or deselected state of the Enable Background Blur check box is saved on the endpoint for the current VDA session.

Support for MJPEG webcams

Starting with the Citrix Workspace app for Linux 2308 version, MJPEG webcams are supported in the H264 stream. The Webcam performs MJEPG compression internally which provides better image quality and a higher frame rate. This feature is enabled by default. However, if Webcam doesn't support MJPEG, this feature is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multiple webcam resolutions support

Previously, only the VGA resolution was supported for webcam redirection.

Starting with the 2408 release, Citrix Workspace app for Linux supports high-definition webcam streaming for all webcam resolutions that are available on the client side. If media type negotiation fails, HDX now defaults back to the default VGA resolution (640 x 480 pixels). For more information, see High-definition webcam streaming.

This feature is enabled by default. To disable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
2. Go to the [WFClient] section and add the following entry:

```
HDXWebCamEnablePnp=False
```

Known limitations

- Webcam redirection with H.264 encoding is not supported by default in Citrix Workspace app for Linux on Red Hat Enterprise Linux (RHEL).
- RHEL does not ship any `GStreamer` H.264 encoder plug-ins because of H.264 patent licensing restrictions (MPEG-LA). This limitation applies to all RHEL versions. To verify this behavior, run the following command on a default RHEL installation. The command returns no results:

  ```
  gst-inspect-1.0 | grep -i h264 | grep -i enc
  ```

- To enable H.264 webcam encoding, install a compatible `GStreamer` H.264 encoder plug-in. The supported encoders include `vaapih264enc`, `openh264enc`, and `x264enc`. Citrix Workspace app for Linux also supports the Fluendo commercial H.264 encoders (`fluhwvavaapih264enc` and `fluh264enc`) if you license them separately.

Client-drive mapping

September 13, 2025

Client drive mapping allows drive letters on the Citrix Virtual Apps and Desktops™ and Citrix DaaS server to be redirected to directories that exist on the local user device. For example, drive H in a Citrix user session can be mapped to a directory on the local user device running the Workspace app.

Client drive mapping can make any directory mounted on the local user device. The local user device includes a CD-ROM, DVD, or a USB memory stick that are available to the user during a session. Also,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the local user has permission to access the local user device. When a server is configured to allow client drive mapping:

- users can access their locally stored files
- Use the files during their session
- and then save them again either on a local drive or on a drive on the server.

Citrix Workspace app supports client device mapping for connections to Citrix Virtual Apps and Desktops and Citrix DaaS servers. This feature enables a remote application that runs on the server to access devices attached to the local user device. The applications and system resources appear to the user at the user device as if they're running locally. Verify that client device mapping is supported on the server before using these features.

> **Note:**
>
> - The Security-Enhanced Linux (SELinux) security model can affect the operation of the Client Drive Mapping and USB Redirection features. This model is applicable on both Citrix Virtual Apps and Desktops and Citrix DaaS. If you require either or both of these features, disable SELinux before configuring them on the server.
> - Client Drive Mapping requires Portable Operating System Interface (POSIX)-compliant filesystems for full functionality. Network shares mounted using GIO commands (such as gio mount smb://server/share) utilize FUSE (Filesystem in Userspace) or GVFS (GNOME Virtual File System) technology. These technologies provide limited POSIX compliance and are not supported. As a recommendation, use direct kernel CIFS mounts instead to ensure proper Client Drive Mapping operations.

Two types of drive mapping are available:

- Static client drive mapping - Enables administrators to map any part of a user device's file system to a specified drive on the server at logon. For example, it can be used to map all or part of a user's home directory or /tmp. Also, map the mount points of mass storage devices such as CD-ROMs, DVDs, or USB memory sticks.
- Dynamic client drive mapping - Monitors the directories in which mass storage devices are typically mounted on the user device. The mass storage devices include CD-ROMs, DVDs, and USB memory sticks. And any new ones that appear during a session are automatically mapped to the next available drive letter on the server.

When Citrix Workspace app connects to Citrix Virtual Apps and Desktops or Citrix DaaS, client drive mappings are reestablished. This action occurs if client device mapping is enabled. You can use policies to give you more control over how client device mapping is applied. For more information, see the Citrix Virtual Apps and Desktops documentation.

Users can map drives using the **Preferences** dialog box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> By default, enabling static client drive mapping also enables dynamic client drive mapping. To disable the latter but enable the former, set `DynamicCDM` to **False** in `wfclient.ini`.

Starting with version 2101, access to mapped drives comes with an extra security feature.

You can now select the access level for the mapped drive for every store in a session.

To stop the access level dialog from appearing every time, select the **Do not ask me again** option. The setting is applied on that particular store.

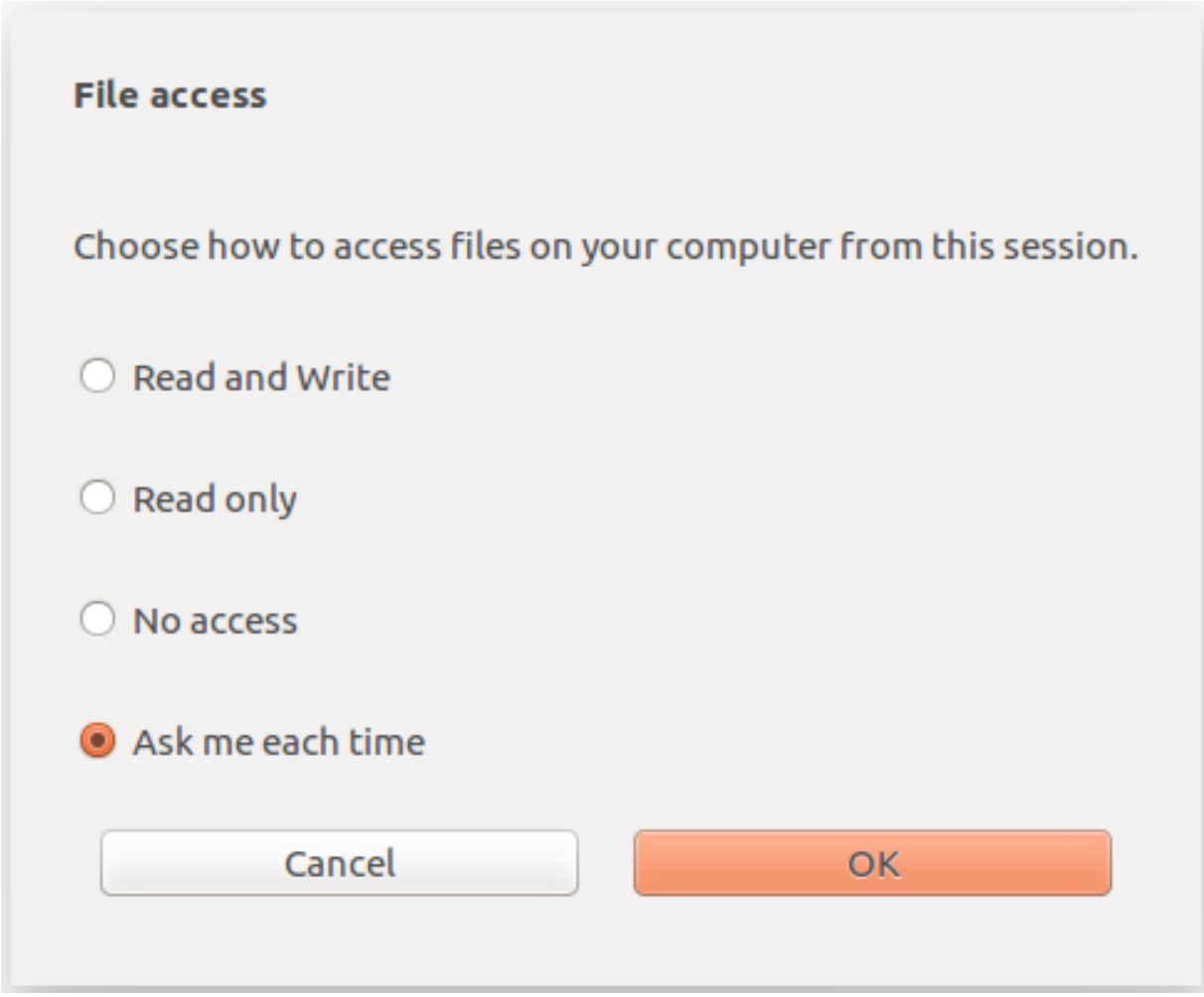
Otherwise, you can set the access levels that appear every time a session is launched.

Previously, your setting for file access through CDM was applied on all configured stores.

Starting with Version 2012, Citrix Workspace app allows you to configure per-store CDM file access.

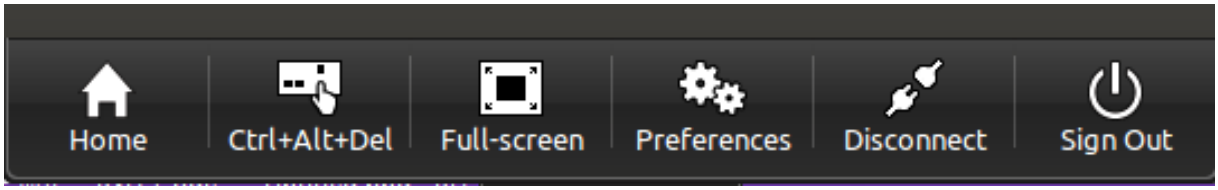
> **Note:**
>
> The file access setting isn't persistent across sessions when using workspace for web. It defaults to the **Ask me each time** option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



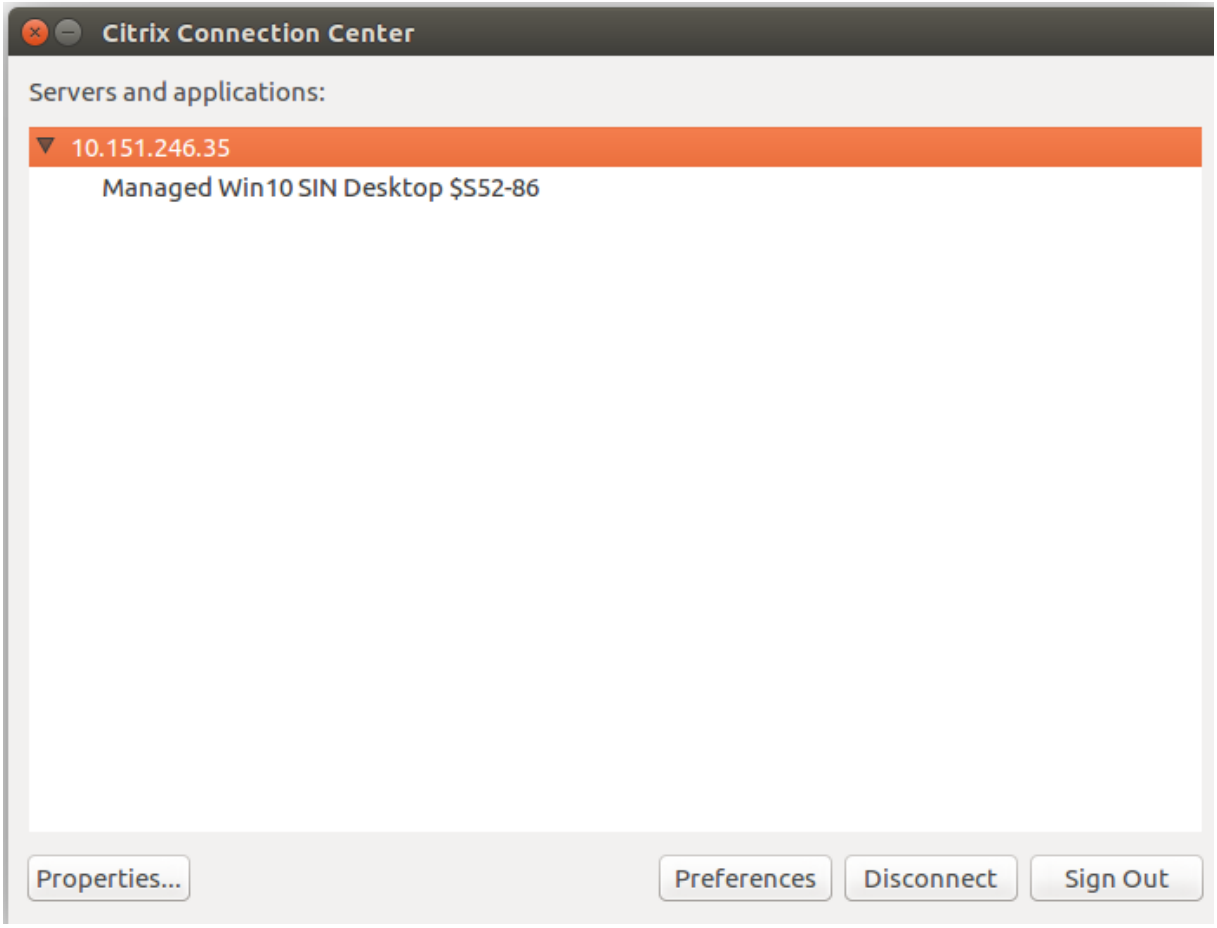
You can use the `wfclient.ini` file to configure the mapped path and file name attributes. Use the GUI to set a file access level as shown in the preceding screen capture.

In a desktop session, you can set a file access level by navigating to the **Preferences** > **File access** dialog from the Desktop Viewer.



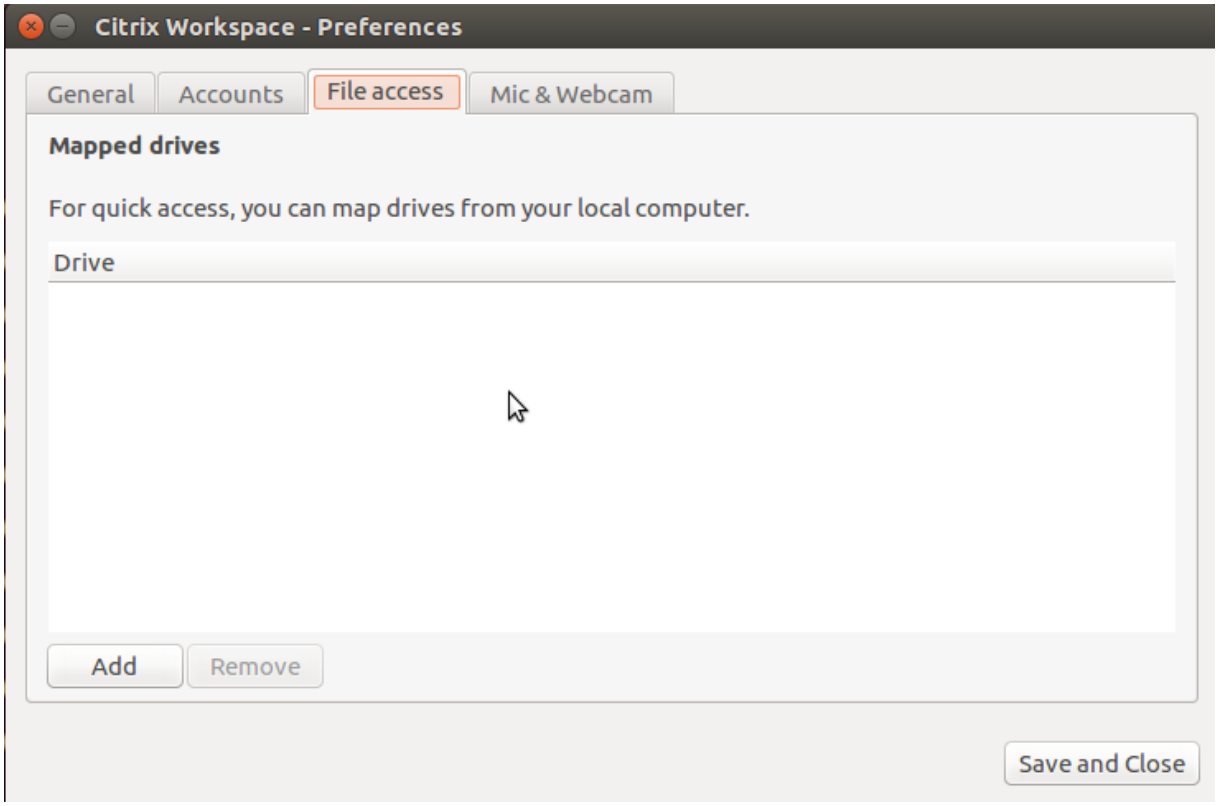
In an app session, you can set a file access level by launching the **File access** dialog from **Citrix Connection Center**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **File access** dialog includes the mapped folder name and its path.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The access level flag isn't supported in the `wfclient.ini` file anymore.

Printer

January 16, 2026

Map client-printers

Citrix Workspace app supports printing to network printers and printers that are attached locally to user devices. By default, unless you create policies to change it, Citrix Virtual Apps and Desktops and Citrix DaaS lets users:

- Print to all printing devices accessible from the user device
- Add printers

These settings, however, might not be perfect in all environments. For example, the default setting that allows users to print to all printers accessible from the user device is the easiest to administer initially. But the default setting might create slower logon times in some environments. In this situation, you might want to limit the list of printers configured on the user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Likewise, your organization's security policies might require that you prevent users from mapping local printing ports. To do so, on the server configure the **ICA® policy Auto connect client COM ports** setting to Disabled.

To limit the list of printers configured on the user device:

1. Open the configuration file, wfclient.ini, in one of the following:
   - `$HOME/.ICAClient` directory to limit the printers for a single user
   - $ICAROOT/config directory to limit the printers for all Workspace app users. All users in this case are those users who first use the self-service program after the change.
2. In the [WFClient] section of the file type:

   ClientPrinterList=printer1:printer2:printer3

   Where printer1, printer2, and so on, are the names of the chosen printers. Separate printer name entries by a colon (:).
3. Save and close the file.

Map a local printer

The Citrix Workspace app for Linux supports the Citrix PS Universal Printer Driver. So, usually no local configuration is required for users to print to network printers or printers that are attached locally to user devices. You might manually map client printers on Citrix Virtual Apps and Desktops or Citrix DaaS for Windows. This manual mapping is required if, for example, the user device's printing software doesn't support the universal printer driver.

To map a local printer on a server:

1. From Citrix Workspace app, start a server connection and log on to a computer running Citrix Virtual Apps and Desktops or Citrix DaaS.
2. On the Start menu, choose **Settings > Printers**.
3. On the File menu, choose **Add Printer**.

   The Add Printer wizard appears.
4. Use the wizard to add a network printer from the Client Network, Client domain. Usually this value is a standard printer name, similar to values created by native Remote Desktop Services, such as "HP LaserJet 4 from client name in session 3."

   For more information about adding printers, see your Windows operating system documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

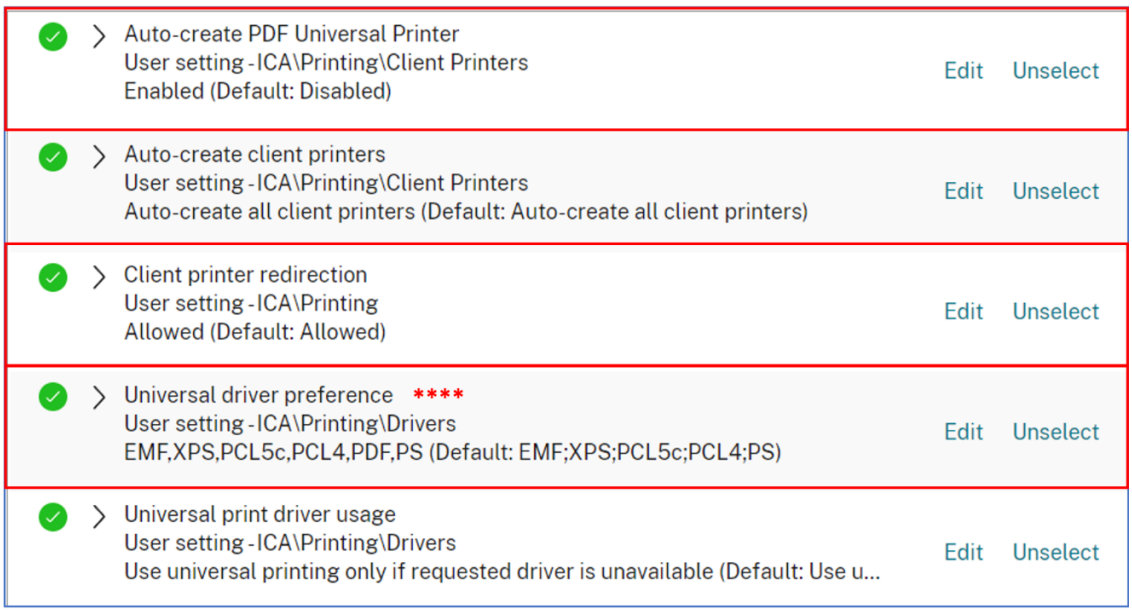
PDF Universal Printing

Starting with the 2405 version, Citrix Workspace app for Linux supprots the PDF universal printing. You can print as PDF once you configure either or both of the following options:

1. Provide a single PDF Universal Printer created in each session.
2. Use the Universal Print Driver (UPD) for regular auto-created printers.

Prerequisites

- Citrix Workspace app for Linux version 2405 or later - Enables consumption of PDF print streams for Citrix Workspace app for Linux.
- Citrix Virtual Apps and Desktops version 2112 or later - Enables PDF universal printing for auto-created client printers.
- Enable the Client printer redirection policy (highlighted in the following image) in the Citrix Studio or web console.



**** "PDF" needs to be added manually if absent from the Universal Driver Preference policy

Provide a single PDF Universal Printer created in each session

To enable creation of the PDF Universal Printer in sessions from a Linux client or any other PDF enabled client endpoint, do the following:

1. Navigate to Citrix Studio or the web console and enable the Auto-Create PDF universal printer policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Set CitrixPDFPrinterAllowed=On in the [WFClient] section in the wfclient.ini file.

Once the preceding steps are completed, the PDF universal printer is created in the session. The printer is called Citrix PDF Printer.

Use this printer in a session to generate a PDF output that delivers to the client. Also, send the PDF output to the default PDF handling application on the endpoint. For the Linux client, this PDF handling application is typically the built-in Preview application, but it could be any registered PDF handling application such as Adobe Acrobat Reader.

Use the UPD for regular auto-created printers

To enable PDF universal printing for all redirected client printers in a session, visit Citrix Studio or a web console from a Linux client. Then, configure the **Universal driver preferences** policy to place the PDF metafile format within the priority list.

After this configuration, the Citrix PDF Universal Driver replaces the HP Color LaserJet 2800 Series PS driver on the host for automatically created printers. The automatically created printers use a universal driver with a Linux client that can print PDFs. When using one of the auto-created printers in a session, PDF is used as the intermediate format of the print job. But the print output flows directly to the selected client-attached printer.

> **Note:**
>
> For printing diagnostics on Linux client endpoints, administrators may enable additional Citrix Workspace app settings in the `config` file. Certain diagnostic-level options can expose **personally identifiable information (PII)**, such as user names, device identifiers, or session details.
>
> Ensure you handle, store, and share configuration files and logs in accordance with your organization's data-protection and privacy policies, and share diagnostic output only through approved channels.

Session experience

June 25, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Boot to Virtual Desktop

Overview

The Boot-to-Virtual-Desktop feature simplifies access to virtual desktops. This feature allows administrators to configure local desktops so that users can directly access their virtual desktops without having to authenticate into any local applications.

The Boot-to-Virtual-Desktop feature is ideal where data protection, compliance, and simplicity are top priorities for organizations. This solution ensures users always work within the virtual desktop, keeping your data secure and reducing risk. It is ideal for kiosk mode and frontline use cases.

Key features

- **Non-domain-joined machine support**: While primarily intended for domain-joined environments, this feature also supports user authentication on non-domain-joined machines. However, manual authentication is required in this scenario.
- **Flexibility**: Direct-boot-to-Virtual-Desktop supports both shared and dedicated local desktops, catering to various use cases like kiosks and frontline users.

Prerequisites

- **Citrix Workspace app prerequisites**: All other system requirements are identical to that of the Citrix Workspace app. For more information, see System requirements.
- **Store configuration**: Before installing the feature, ensure that the store is configured.

Configure Boot-to-Virtual-Desktop using configuration file

This feature is disabled by default. To enable this feature, do the following:

1. **Enable direct boot to Virtual Desktop:**

   - Navigate to the `$ICAROOT/config/AuthManConfig.xml` configuration file.
   - Add the following entries:

   ```
   <key>DesktopLockEnabled</key>
   <value>true</value>
   ```

2. **Provide StoreURL and ResourceName:**

   To use the boot-to-Virtual-Desktop feature, add StoreURL and ResourceName in `$ICAROOT/config/AuthManConfig.xml`:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<StoreURL>test.cloud.com</StoreURL>
<ResourceName>EDaaS Desktop</ResourceName>
```

Configure Boot-to-Virtual-Desktop using script

The script is designed to manage the configuration of the boot-to-Virtual-Desktop feature. To run the script, do the following:

1. Open the terminal on your Linux machine.
2. Navigate to the installation directory of Citrix Workspace™ app.

   > **Note:**
   >
   > `$ICAROOT` is the default installation directory of Citrix Workspace app.

3. Type `cd DesktopLock`.
4. Type `configureDesktopLock.sh` to run the script.

The following command usage information appears:

usage: `./configureDesktopLock.sh <Citrix workspace installation path> <enable|disable>`

To block shortcuts or create an autostart entry, you must provide a separate mechanism to disable shortcuts (if GSettings schema doesn't exist).

To configure boot-to-Virtual-Desktop on endpoints, use the storebrowse command with the following syntax, depending on your Citrix Workspace app version:
to create an autostart entry for boot-to-virtual-desktopp on endpoints, use the storebrowse command with the following syntax, depending on your Citrix Workspace app version:

For Citrix Workspace app version 2503:

```
./desktoplock <storeURL> <resourceName>
```

For Citrix Workspace app version 2505 and later:

```
./desktoplock --storeUrl <storeURL> --resource <resourceName>
```

Battery status indicator

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Starting with the 2111 version, the battery status indicator appears for server VDAs also.

The battery status indicator is enabled by default.

To disable the battery status indicator:

1. Navigate to the <ICAROOT>/config/module.ini folder.
2. Go to the ICA 3.0 section.
3. Set the MobileReceiver=Off.

App indicator icon

The app indicator starts when you launch Citrix Workspace app. It's an icon that is present in the notification area. With the introduction of the app indicator, the Citrix Workspace app for Linux logon performance is improved.

You can observe performance improvement when you:

- First launch of Citrix Workspace app
- Close and relaunch the app
- Quit and relaunch the app

> **Note:**
>
> The libappindicator package is required for the app indicator to appear. Install the libappindicator package suitable for your Linux distribution from the web.

Workspace launcher

Citrix introduces the Workspace launcher (ctx-webhelper) to launch published desktops and applications.

Previously, the browser plug-in provided along with Citrix Workspace app for Linux enabled users to launch published desktops and applications was based on the NPAPI.

As a solution, Citrix is introducing the Workspace launcher (WebHelper). To enable this feature, configure StoreFront to send requests to the Workspace launcher to detect the Citrix Workspace app installation.

Starting with Version 1901, the Citrix Workspace launcher is compatible with direct connections to StoreFront and Citrix Gateway. This feature helps to launch the ICA file automatically and to detect the Citrix Workspace app installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disabling new workspace web UI mode

When you launch the Citrix Workspace app for Linux using the self-service executable file from third-party thin-client vendors, the application can become unresponsive because of 100% CPU utilization.

As a workaround, to switch back to the old UI mode:

1. Remove cached files by using the command:
   `rm -r ~/.ICAClient`
2. Go to `$ICAROOT/config/AuthManconfig.xml` file.
3. Change `CWACapableEnabled` key value to false.
4. Launch Citrix Workspace app for Linux. Observe that the self-service executable file loads the old UI.

Copy and paste files and folders between two virtual desktops

Previously, you can copy only text between two virtual desktops. Starting with Citrix Workspace app for Linux version 2309, you can copy and paste files and folders between two virtual desktops.

This feature is enabled by default.

> **Note:**
>
> - Copy and paste files and folders between two virtual desktops is supported only on the x64 and ARM64 Linux distributions.
> - In the Linux Virtual Delivery Agent, the maximum transfer of data in one single copy-paste operation is 200 MB. For more information, see File copy and paste documentation.

To disable this feature, do the following:

1. Navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file.
2. Edit the value of `VDGDT` to `Off`.

File type association

A Citrix Virtual Apps™ Services might also publish a file, rather than an application or desktop. This process is referred to as publishing content, and allows pnabrowse to open the published file.

There's a limitation to the type of files that the Citrix Workspace app recognizes. Only when a published application is associated with the file type of the published file:

- The system recognizes the file type of the published content

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users can view the file through Citrix Workspace app

For example, to view a published Adobe PDF file using Citrix Workspace app, an application such as Adobe PDF Viewer must be published. Unless a suitable application is published, users can't view the published content.

To enable FTA on the client-side:

1. Verify that the app that you want to associate is a favorite or a subscribed application.
2. To get the list of published applications and the server URL, run the commands:

```
./util/storebrowse -l

./util/storebrowse -S <StoreFront URL>
```

3. Run the ./util/ctx_app_bind command with the following syntax:

   ```
   ./util/ctx_app_bind [-p] example_file|MIME-type published-application
    [server|server-URI]
   ```

   for example,
   ```
   ./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://
   awddc1.bvt.local/citrix/store/discovery
   ```

4. Verify that the file that you're trying to open is client drive mapping (CDM) enabled.
5. Double-click the file to open it using the associated application.

Associating a published application with file types

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

Prerequisite:

Verify that you connect to the Store server where the FTA is configured.

To link a file name extension with a Citrix Workspace app for Linux application:

1. Publish the application.
2. Log on to Citrix Studio.
3. Right-click the application and then select **Properties.**
4. Select **Location.**
5. Add "%**"in the Command-line argument (optional) field to bypass the command-line validation and then click OK.
6. Right-click the application and select **Properties**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Select **File Type Association**.
8. Select all the extensions that you want Citrix Workspace app to associate with the application.
9. Click **Apply** and **Update file types**.
10. Follow the steps mentioned in File type association to enable FTA on the client-side.

> **Note:**
>
> The StoreFront file type association must be ON. By default, file type association is enabled.

Transparent user interface

The Citrix ICA protocol uses the Transparent User Interface Virtual Channel [TUI VC] protocol to transmit data between Citrix Virtual Apps and Desktops™ or Citrix DaaS and host servers. The TUI protocol transmits user interface [UI] component messages for remote connections.

Citrix Workspace app for Linux supports the TUI VC feature. This feature helps the client to receive the TUI packets sent by the server, and the client can access the UI-related components. This functionality helps you to control the display of the default overlay screen. You can toggle the `VDTUI` flag in the `module.ini` file: `VDTUI - On/Off`

Starting with version 1912, the **VDTUI** flag is set to **On** by default. As a result, the "Starting <Application>"dialog box no longer appears when you launch an app. Instead, a "Connecting <Application>" dialog appears with a progress bar. The dialog also displays the progress of the app launch. However, if you set the flag to **Off**, the "Starting <Application>"dialog rendered on top of other application windows, covering the login prompt.

For more information on Virtual Channels, see Citrix ICA virtual channels in the Citrix Virtual Apps and Desktops documentation.

Increase in the number of supported virtual channels

In earlier versions of the client, sessions supported up to 32 virtual channels.

Starting with the 2103 version, you can use up to 64 virtual channels in a session.

Enhanced desktop launch and screen resizing experience

Citrix Workspace app for Linux ensures a smooth transition and prevents black screens and flickers when resizing or stretching your virtual desktop screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The enhanced virtual desktop screen resizing experience and enhanced desktop launch experience features are enabled by default.

Starting with version 2408, the enhanced desktop launch experience feature is enabled by default for single monitor setups only. Starting with version 2411, this feature also supports multiple setups.

To disable the enhanced virtual desktop screen resizing experience feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Go to the [WFClient] section.
3. Add the following entry:

```
EnhancedResizingEnabled=False
```

Starting with version 2411, Citrix Workspace app for Linux ensures an improved desktop launch experience. You'll experience a seamless, flicker-free transition to your desktop without intermediate screens.

To disable the enhanced desktop launch experience feature, do the following:

1. Navigate to the $HOME/.ICAClient/wfclient.ini folder.
2. Go to the [WFClient] section.
3. Add the following entry:

```
DesktopLaunchEnhancement=False
```

Improved loading experience for shared user mode

Starting with the 2408 version, the time taken to load the store is reduced and thus the loading experience for the shared user mode is improved.

> **Note:**
>
> This feature is applicable only on StoreFront™ stores.

This feature is disabled by default. To enable this feature, do the following:

1. Navigate to the `AuthManConfig.xml` configuration file.
2. Set the following entry as True:

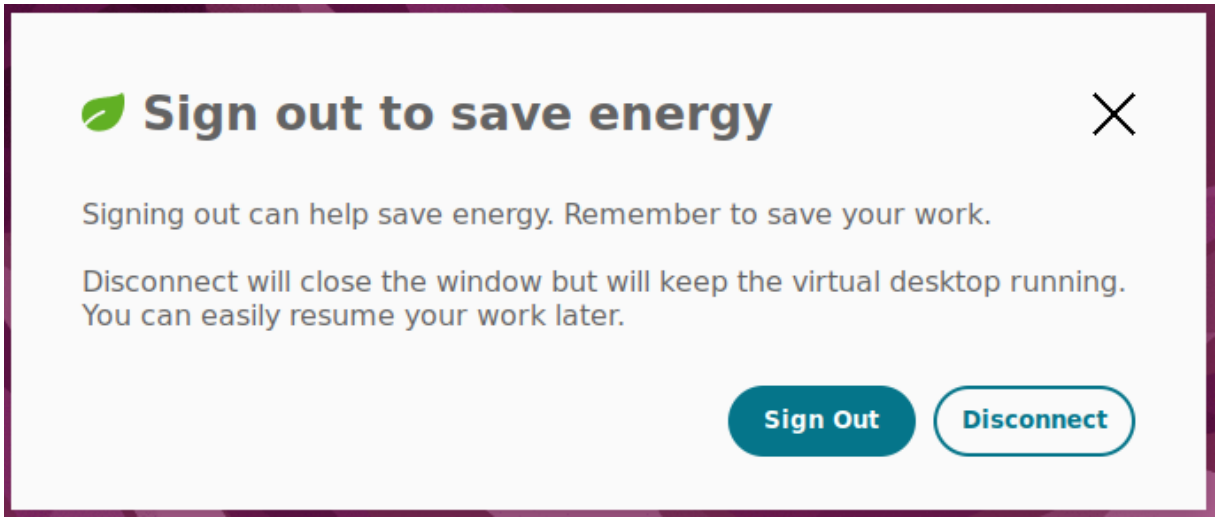
```
<key>KioskSFUIEnhanced</key>
<value>True</value>
```

For more information on shared user mode, see Kiosk mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sustainability initiative from Citrix Workspace app

From the Citrix Workspace app 2402 version onwards, the following prompt might appear when you click disconnect, sign out, or close a virtual desktop.



Users can either **Sign Out** or **Disconnect** from the session.

> **Note:**
>
> By default, this feature is disabled. To enable the dialog box for end users, administrators must configure the feature.

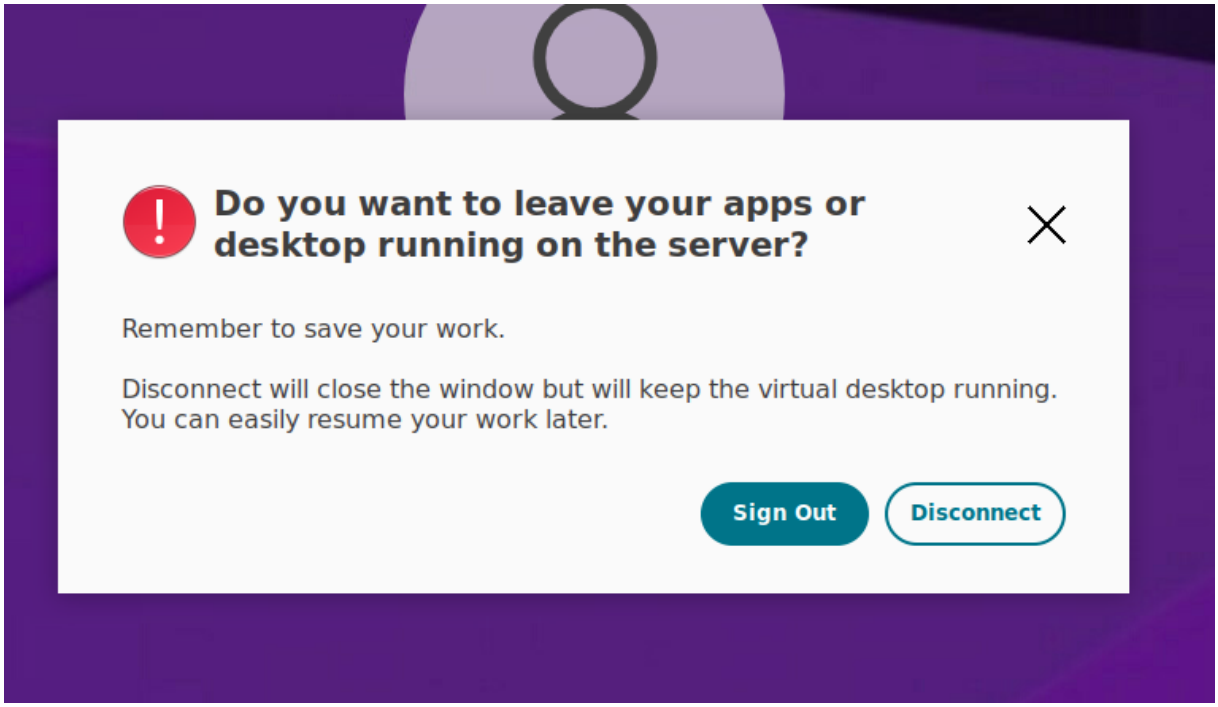
Benefits

This feature allows organizations to encourage users to be more mindful of their energy consumption when using virtual desktops. This feature might help conserve energy by reminding end users to sign out of the unused VMs when not required. This way, organizations can conserve energy by reducing the number of unused VMs left running.

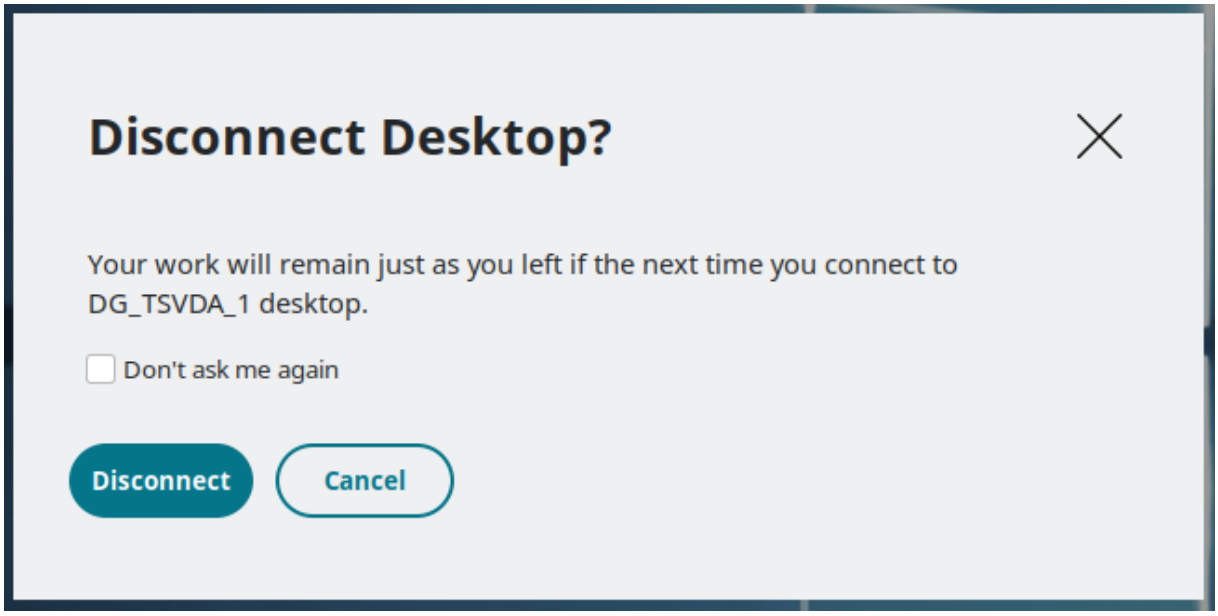
Enable sustainability feature

By default, this feature is disabled. If you don't edit the client-side configuration, the following dialog box appears to the end users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Starting with version 2411, enable the sustainability feature by editing the client-side configuration and adding the line `CloseDialogVersion=1` in `~/.ICAClient/wfclient.ini`. This means the end users don't have an option to **Sign Out**. By default, you can force the end users to click **Disconnect**.



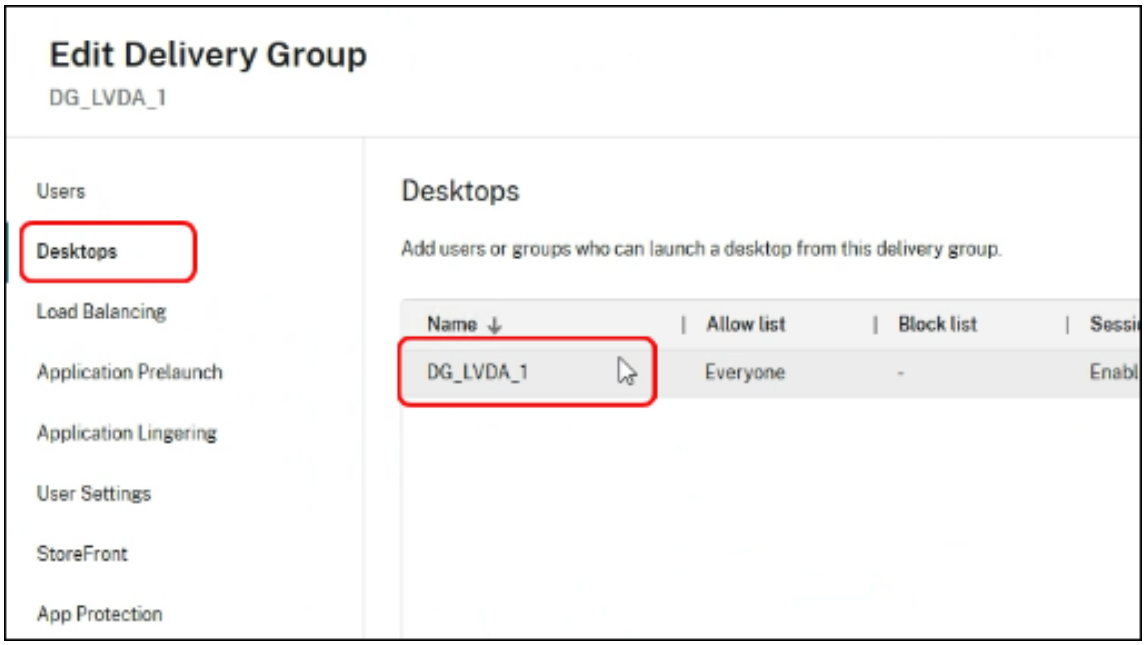
To use the sustainability feature with a custom message, modify the delivery group on DDC 2407 or later as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Save Energy message on TSVDA

To enable this feature on TSVDA, do the following:

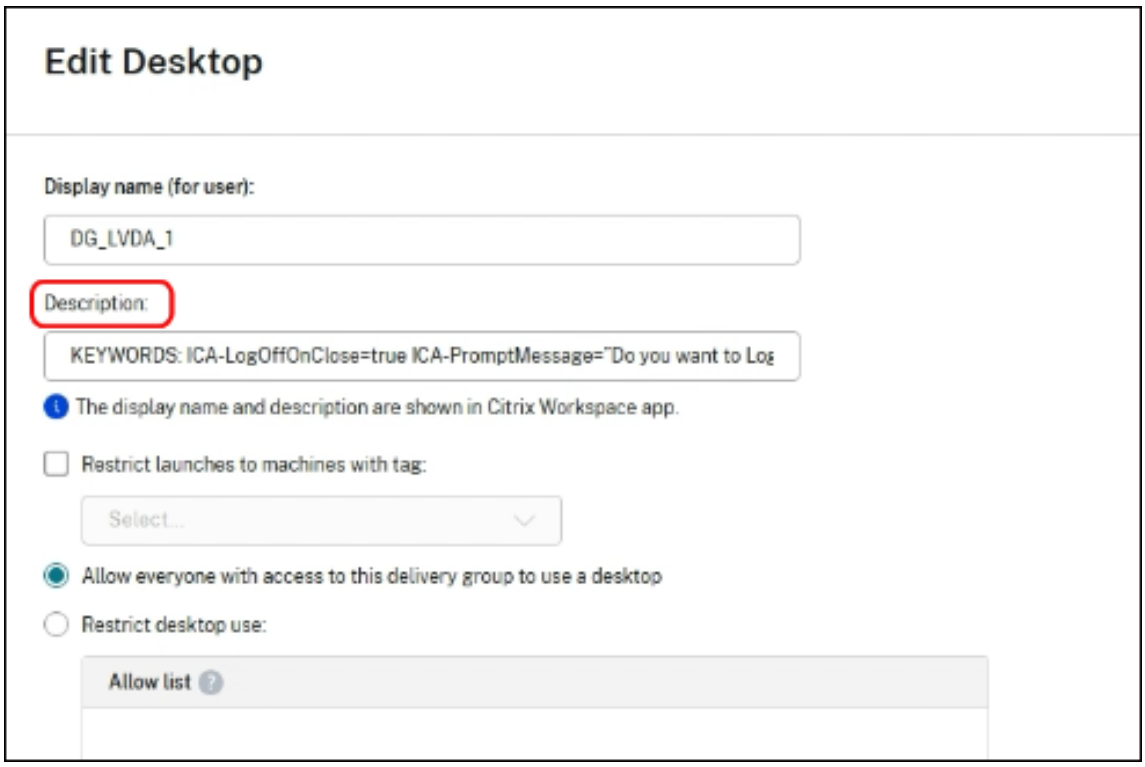
1. Navigate to Citrix Studio.
2. Click **Delivery Groups** from the left navigation pane.
3. Select the required TSVDA from the **Delivery Group** section.
4. Click the **Edit** icon. The **Edit Delivery Group** page appears.
5. Click **Desktops** from the left navigation pane.



6. Select the required VDA where you must add the keywords.
7. Click **Edit**. The **Edit Desktop** page appears.
8. Set the `ICA-LogOffOnClose` keyword to **`true`** in the **Description** field.

   For example, `KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the session?"ICA-Title="Sign out or disconnect"ICA-Icon=true`

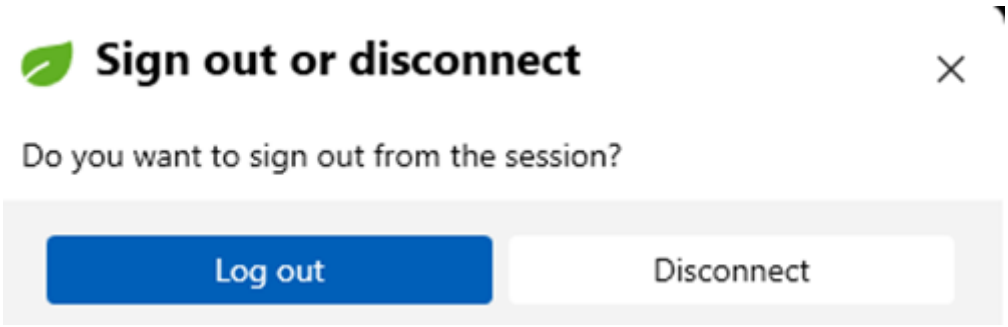
© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Click **OK**, and then click **Save**.

The following dialog box appears when you close the virtual desktop.

> **Note:**
>
> If the configuration is done during an active session, you need to close the current session and restart it for this dialog box to appear.



Configure Save Energy message on WVDA

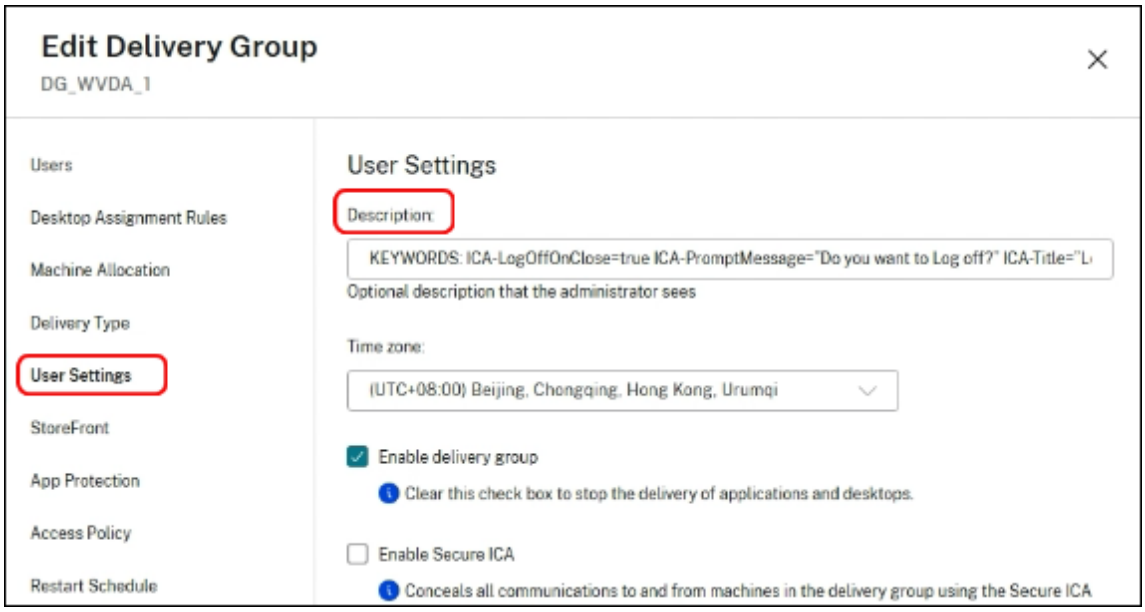
To enable this feature on WVDA, do the following:

1. Navigate to Citrix Studio.
2. Click **Delivery Groups** from the left navigation pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the required WVDA from the **Delivery Group** section.
4. Click the **Edit** icon. The **Edit Delivery Group** page appears.
5. Click **User Settings** from the left navigation pane.
6. Set the `ICA-LogOffOnClose` keyword to **`true`** in the Description field.

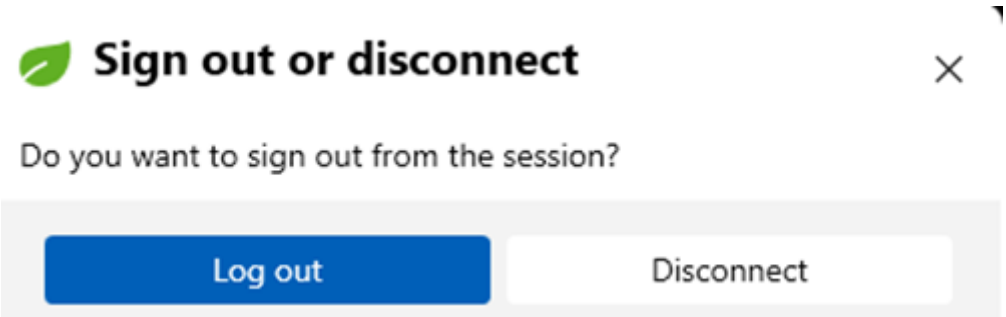
   For example, `KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the session?"ICA-Title="Sign out or disconnect"ICA-Icon=true`



7. Click **Save**.

The following dialog box appears when you close the virtual desktop.

> **Note:**
>
> If the configuration is done during an active session, you need to close the current session and restart it for this dialog box to appear.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customization of Desktop Viewer toolbar

With the 2411 release, you have more control over the **Desktop Viewer** toolbar. You can customize toolbar options using the Global App Configuration service (GACS) or the `.ini` file.

You can customize:

- Show or hide the full Desktop Viewer Toolbar for end users.
- Choose which tabs appear on the Desktop Viewer Toolbar.

Configuration

You can customize the Desktop Viewer toolbar using **GACS Admin UI** or the `.ini` file.

Using GACS To configure the customization of the Desktop Viewer toolbar through the GACS Admin UI, do the following:

1. Sign in to Citrix Cloud with your credentials.

   > **Note:**
   >
   > Refer to the Sign Up for Citrix Cloud article for step-by-step instructions on creating a Citrix Cloud account.

2. Upon authentication, click the menu button on the upper left corner and select **Workspace Configuration**. The Workspace Configuration screen appears.
3. Click **App Configuration** > **Citrix Workspace app**.
4. Select the **Linux** checkbox.
5. You can now update the settings under **Session Experience** > **Toolbar**.

For more information, see Global App Configuration service documentation.

Using .ini file To configure the customization of the Desktop Viewer toolbar through the `.ini` file, follow these steps:

To hide the toolbar:

1. Navigate to the `$HOME/.ICAClient/All_Regions.ini` file.
2. Under the `[Client Engine\GUI]` section, find `ConnectionBar=`.
3. Set `ConnectionBar=0;`

To show the toolbar:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the `$HOME/.ICAClient/All_Regions.ini` file.
2. Under the `[Client Engine\GUI]` section, find `ConnectionBar=`.
3. Set `ConnectionBar=*` or `ConnectionBar=1;`

To configure each button on the toolbar:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
2. Go to the `[WFClient]` section and add the following entry as required.

   For Button "Switch Desktop":

   - To show: Don't set or `SwitchDesktopButtonVisible=True`
   - To hide: `SwitchDesktopButtonVisible=False`

   For Button "Ctrl+Alt+Del":

   - To show: Don't set or `CtrlAltDelButtonVisible=True`
   - To hide: `CtrlAltDelButtonVisible=False`

   For Button "Devices":

   - To show: Don't set or `DevicesButtonVisible=True`
   - To hide: `DevicesButtonVisible=False`

   For Button "Preferences":

   - To show: Don't set or `PreferencesButtonVisible=True`
   - To hide: `PreferencesButtonVisible=False`

   For Button "Connection":

   - To show: Don't set or `ConnectionButtonVisible=True`
   - To hide: `ConnectionButtonVisible=False`

   For Button "Multi-monitor":

   - To show: Don't set or `MultiMonitorButtonVisible=True`
   - To hide: `MultiMonitorButtonVisible=False`

   For Button "Minimize":

   - To show: Don't set or `MinimizeButtonVisible=True`
   - To hide: `MinimizeButtonVisible=False`

   For Button "Fullscreen / Restore":

   - To show: Don't set or `FullscreenButtonVisible=True`
   - To hide: `FullscreenButtonVisible=False`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For Button "Disconnect":

- To show: Don't set or `CloseButtonVisible=True`
- To hide: `CloseButtonVisible=False`

To Customize the Toolbar:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` file.
2. Go to the `[WFClient]` section and add the following entry as required to hide options on the toolbar:

   `DevicesButtonVisible=False`

Connection strength indicator on Desktop Viewer toolbar

Starting with version 2503, Citrix Workspace app for Linux now supports the Connection Strength Indicator (CSI) on the Desktop Viewer toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

> **Note:**
>
> This feature is enabled by default.

Benefits

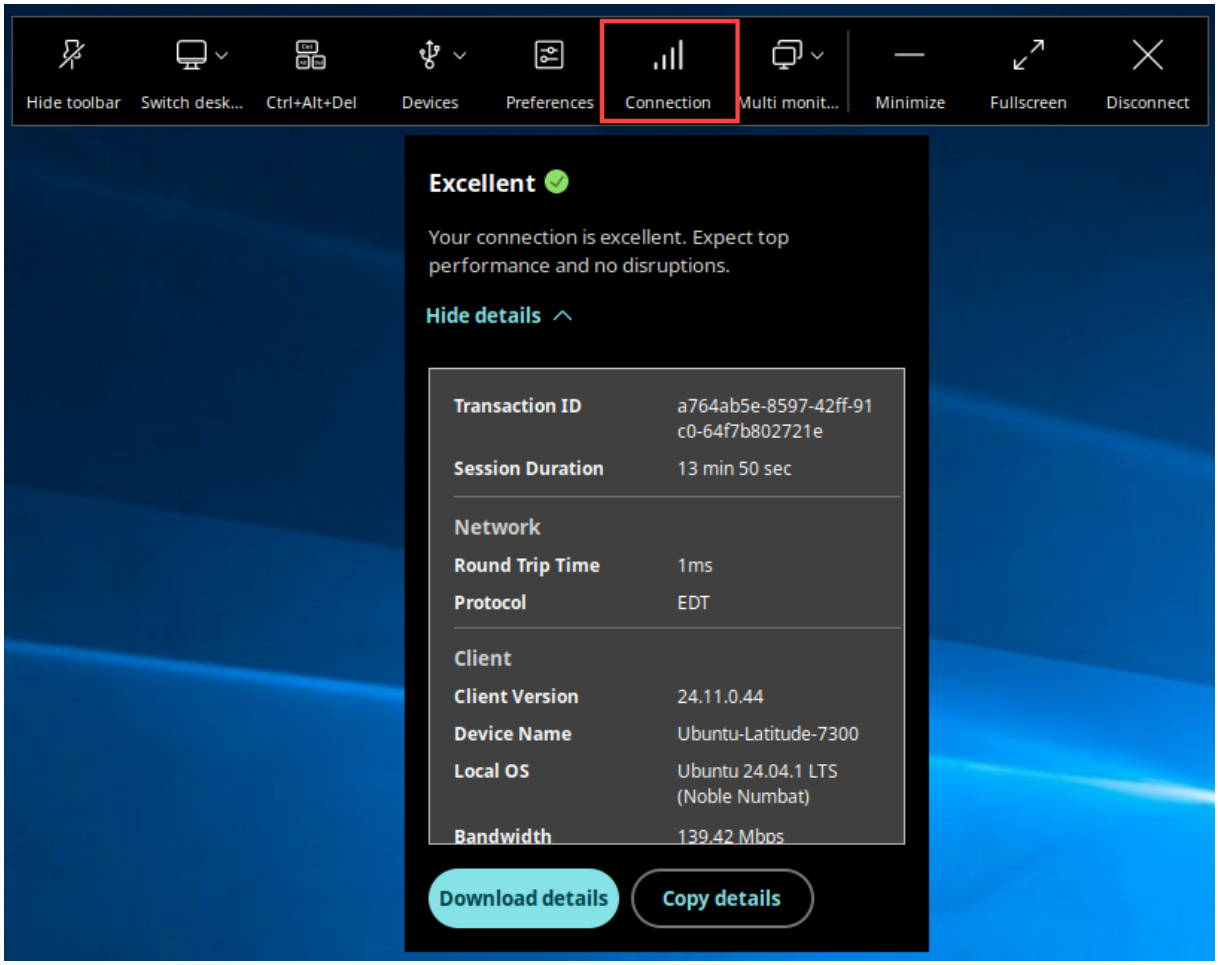
- **Immediate feedback:** The network strength icon provides users with instant alerts when network issues are detected.
- **Enhanced troubleshooting:** Real-time stats and diagnostics help users and IT teams quickly identify and resolve connectivity issues.

Prerequisites

- This feature is only available when a session opened using:
  - VDA 2407 or later
  - VDA 2402 LTSR CU1 or later
- The Supportability Virtual Channel must be enabled on the client side.

When you open the Citrix Workspace app session, you can see the **Connection** icon on the **Desktop Viewer** toolbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> If you are using a lower version of VDA, the Connection icon won't be visible.

The connection strength indicator on the **Desktop Viewer** toolbar provides users with immediate feedback on their network connectivity and offers detailed real-time stats for enhanced troubleshooting. This feature aims to improve user experience and reduce the time spent on resolving connectivity issues.

Enable 'Download details'and 'Copy details'options

> **Note:**
>
> These options are hidden by default.

Download details option: Saves the CSI metrics as a file to your local device.

Copy details option: Copies the CSI metrics directly to your clipboard for quick sharing or reference.

To show these options, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` folder.
2. Navigate to the [WFClient] section.
3. Add the following entry:

   ```
   CsiDownloadButtonVisible=True
   ```

   ```
   CsiCopyButtonVisible=True
   ```

Enhancement to Fullscreen or Extend button behavior

Starting with the 2505 version, the Fullscreen or Extend button adjusts display behavior based on the current configuration:

- When labeled Fullscreen, it maximizes the window to a single display if only one screen is in use. If positioned at a screen border, it extends across multiple displays.
- When labeled Extend, it expands the session to all displays, or a custom layout selected in the Multi-Monitor Selector.
- The button label switches to Extend when the Multi-Monitor Selector is set to "Extend to all displays"or a "Custom Layout"option while in windowed mode.
- Display configurations persist even if monitors are unplugged, as long as a subset of the original configuration remains connected.

This feature is enabled by default.

Enhanced Connection Strength Indicator

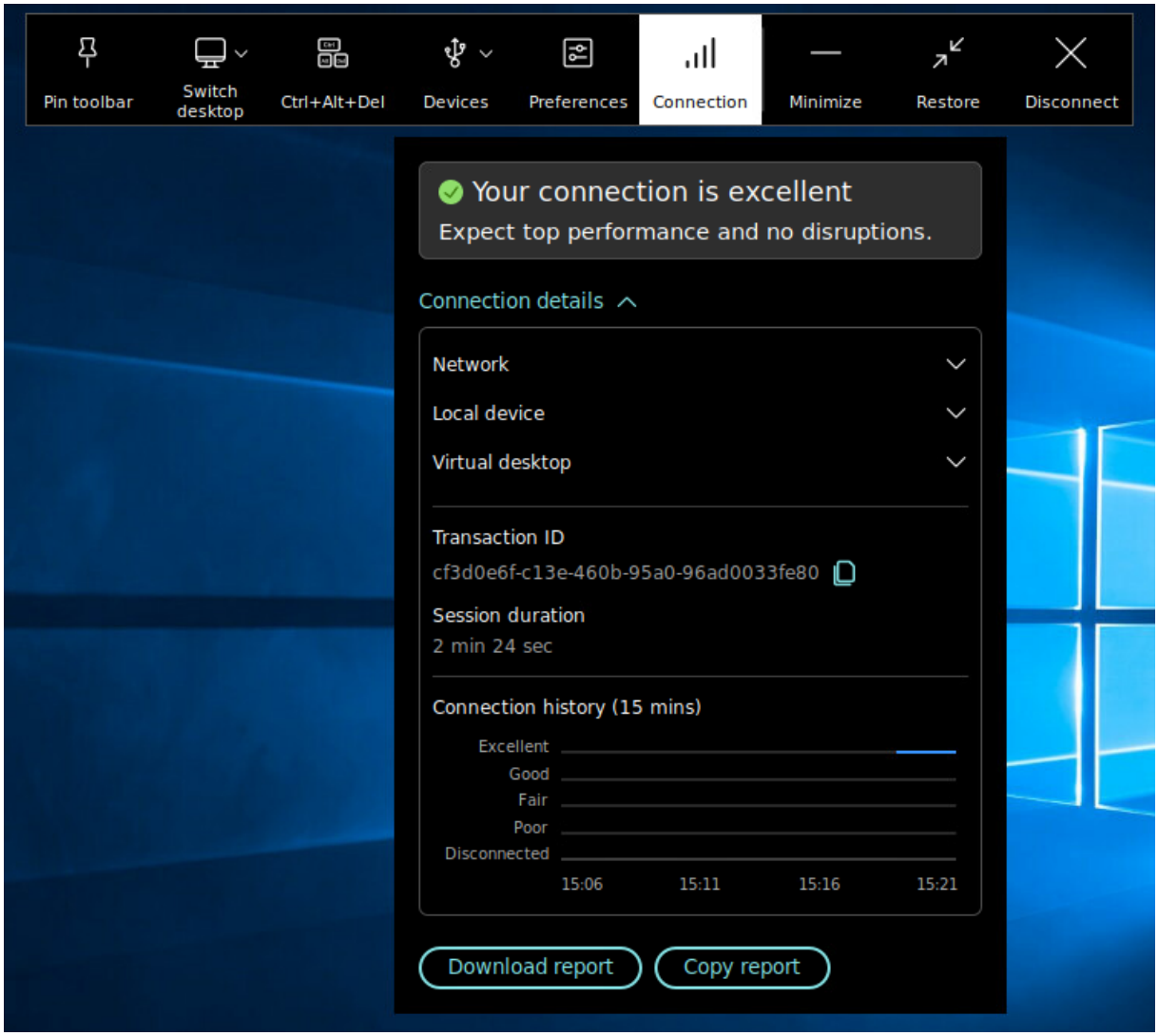
Starting with version 2508, Citrix Workspace app for Linux features an improved Connection Strength Indicator that provides better connectivity insights and user control. The enhanced indicator helps you monitor network performance, identify connectivity problems quickly, and take corrective action before issues impact your work.

The key improvements include the following:

- Real-time Wi-Fi strength: Instantly view your current Wi-Fi signal quality for better connectivity awareness.
- Expanded device details: Access information such as CPU, memory usage directly from the indicator.
- Proactive notifications with snooze options: Receive alerts when your connection strength drops, with the ability to temporarily snooze notifications.
- Actionable recommendations: Get clear suggestions to resolve connectivity issues when your connection strength falls below optimal levels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 15-minute connection history: Review a visual history of your connection strength over the past 15 minutes to assist with troubleshooting and analysis.



Clipboard

Enhanced file transfer capabilities for Linux clients

Previously, you were able to copy and paste files and folders only between two virtual desktops. Starting with the Citrix Workspace app for Linux version 2508, you can copy files and folders from client to VDA.

This feature is enabled by default. To disable this feature, update the following policies on the Domain Delivery Controller™ (DDC):

1. Set the **Restrict session clipboard write** policy to Enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Ensure that the *CFX_FILE* isn't added into the session clipboard write allowed formats policy.

Clipboard Support for HTML-formatted text

Starting with version 2408, Citrix Workspace app for Linux supports copy and paste of the HTML-formatted text between local apps and virtual app or desktop sessions, and also between virtual app or desktop sessions. This feature ensures that the HTML content is accurately retained during the copy-and-paste procedure with no restrictions.

This feature is disabled by default in the clipboard redirection policy.

To enable the HTML format for clipboard, you need to add an entry for CF_HTML (and any other in "Client clipboard write allowed formats"and "Session clipboard write allowed formats") in the **ICA policy** settings. For more information, see Client clipboard redirection.

> **NOTE**
>
> - Client clipboard write allowed formats do not apply if the **Client clipboard redirection policy** is set to **Prohibited** or **Restrict client clipboard write policy** is disabled.
> - Session clipboard write allowed formats do not apply if the **Client clipboard redirection policy** is set to **Prohibited** or **Restrict session clipboard write policy** is disabled.

Improved session reconnection experience

Starting with version 2601, this feature enhances the end-user experience during session timeouts caused by inactivity or network interruptions. Users can reconnect directly from the timeout screen for both desktop and app sessions, and also reconnect after the Auto-Client-Reconnect (ACR) phase. This feature is enabled by default.

Prerequisites:

- Citrix Virtual Apps and Desktops: Version 2511 or later
- Citrix Workspace app: Version 2511 or later

The key features are as follows:

- Displaying specific reasons for session timeouts, such as **Device went to sleep**, or **Network disruption**.
- Allowing seamless reconnection to new or existing sessions based on administrator configuration.
- Supporting scenarios where auto reconnect might fail, such as network switches (for example, Wi-Fi to LAN).
- Supporting direct reconnection after the Auto-Client-Reconnect (ACR) phase.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - The new reconnection feature does not support the hybrid-launched sessions.
> - If a customer experiences a "Failed to reconnect"error immediately after clicking the **Reconnect** button:
>   - Open `.HOME/.ICAClient/All_Region.ini`.
>   - If the following section is not present, add it to the end of the file:
>
> ```
> [Network\Relaunch]
> ResourceName=
> ResourceID=
> StoreURL=
> ```

Automatic Maximum Transmission Unit (MTU) adaptation

Starting with version 2601, Citrix Workspace app for Linux supports dynamic adjustment of the session's Maximum Transmission Unit (MTU). This feature automatically detects and adjusts the MTU during a session if the network path changes. This feature is disabled by default.

To enable this feature:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini`.
2. In the [WFClient] section, add:

```
MtuRediscovery = On
```

For more information, see the EDT MTU Discovery section in the Citrix Virtual Apps and Desktops documentation.

Shortcuts menu for macOS VDA

Starting with Citrix Workspace app 2604 for Linux, users connecting to a macOS VDA can access the **Shortcuts** menu in the session toolbar for quick access to common operating system actions without requiring complex keyboard shortcuts or trackpad gestures.

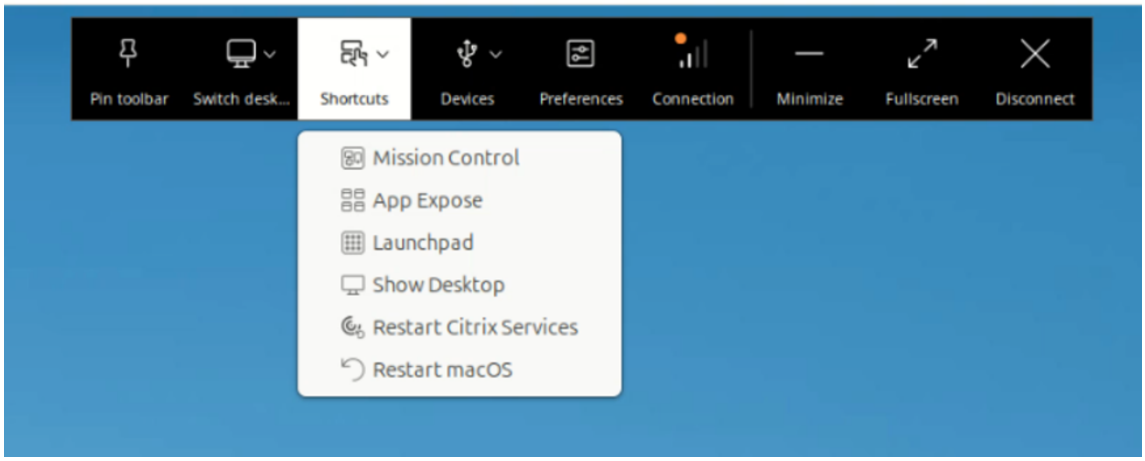
> **Note:**
>
> The **Shortcuts** menu appears only when the endpoint is connected to a macOS VDA.

The **Shortcuts** menu includes the following options:

- Mission Control

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- App Expose
- Launchpad
- Show Desktop
- Restart Citrix Services
- Restart macOS



SDK and API

September 7, 2025

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) supports writing server-side applications and client-side drivers for extra virtual channels using the ICA® protocol.

The server-side virtual channel applications are on Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) servers.

If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- Working source code for several virtual channel sample programs that demonstrate programming techniques.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Linux.

Command-line Reference

For information on command-line reference and parameters, see Citrix Workspace app for Linux Command Reference.

Platform Optimization SDK

As part of the HDX SoC initiative for Citrix Workspace app for Linux, we've introduced the 'Platform optimization SDK'.

This SDK enables an ecosystem of low-cost, low-power, and high-performance devices with innovative form factors.

Developers can use the Platform Optimization SDK to improve the performance of Linux-based devices. This SDK allows developers to create plug-in extensions for the ICA engine component (`wfica`) of Citrix Workspace app. Plug-ins are built as shareable libraries and `wfica` loads these libraries dynamically.

These plug-ins can help you optimize the performance of your Linux devices, enabling the following functions:

- Provide accelerated decoding of JPEG and H.264 data used to draw the session image
- Control the allocation of memory used to draw the session image
- Improve performance by taking control of the low-level drawing of the session image
- Provide graphics output and user input services for OS environments that do not support X11

For information, see Citrix Workspace app for Linux - Platform Optimization SDK.

Availability of Credential Insertion SDK for cloud stores

Previously, using the Credential Insertion SDK, you could authenticate only on on-premises stores. Starting with the Citrix Workspace app for Linux version 2402, you can now authenticate users on the Self-Service plug-in using SSO on cloud stores. To enable this feature, do the following:

1. Navigate to the `/config/AuthManConfig.xml` file.
2. Go to the [AuthManLite] section and update the following entry:

```
<CredentialInsertionEnabled>True</CredentialInsertionEnabled>
<longLivedTokenSupport>false</longLivedTokenSupport>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can use the Credential Insertion SDK only for the basic authentication method (where user name and password are required).

Storebrowse

September 7, 2025

`Storebrowse` is a lightweight command-line utility that interacts between the client and the server. Using the `storebrowse` utility, administrators can automate the following day-to-day operations:

- Add a store.
- List the published apps and desktops from a configured store.
- Subscribe and unsubscribe apps and desktops from a configured store.
- Enable and disable shortcuts for published apps and desktops.
- Launch published applications.
- Reconnect to disconnected sessions.

Generally, the `storebrowse` utility is available in the `/util` folder. You can find it under the installation location. For example, `/opt/Citrix/ICAClient/util`.

Prerequisites

The `storebrowse` utility requires the **libxml2** library package.

Launch published desktops and applications

There are two ways to launch a resource:

- You can use the command line and `storebrowse` commands
- You can use the UI to launch a resource.

This article discusses `storebrowse` commands.

`Storebrowse` enhancement for service continuity

Previously, the Workspace connection lease files were synced with files available on the remote server only if you connected using the Self-Service plug-in. As a result, the service continuity feature wasn't

© 1997–2026 Citrix Systems, Inc. All rights reserved.

supported when you launched apps or desktop session using `storebrowse`. Most third-party thin-client vendors use `storebrowse` to connect to the Workspace platform and the service continuity feature wasn't enabled for them.

Starting with version 2109 for Citrix Workspace app, the Workspace connection lease files sync with files available on the remote server when you connect using `storebrowse` as well. This feature helps the third-party thin-client vendors to access Workspace even when offline.

> **Note:**
>
> - This enhancement is available only when service continuity is enabled in cloud deployments. For more information, see the Configure Service Continuity section in the Citrix Workspace documentation.

Command usage

The following section details the `storebrowse` commands that you can use from the `storebrowse` utility.

Add a store

`-a, --addstore, -as`

Description:

Adds a store with gateway and beacon details along with the ServiceRecord daemon process. This command returns the full URL of the store. An error appears if adding a store fails.

Previously, `-a` command added a store and all linked accounts for the given URL. Starting with the 2408 version, it adds a store for a given URL.

Starting with the 2408 version, the `-as` command adds a store and all linked accounts for the given URL.

Command example of StoreFront:

Command:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Example:

```
./storebrowse -a https://my.firstexamplestore.net
```

> **Note:**
>
> You can add several stores using the `storebrowse` utility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Previously, this command adds a single store and returns the URL of the store. Starting with the 2311 release, along with the existing functionality, this command adds all URLs when multiple accounts are available.

Help

`-?, -h, --help`

Description:

Provides details on the `storebrowse` utility usage.

List store

`-l --liststore`

Description:

Lists the stores that you've added.

Command Example on StoreFront:

`./storebrowse -l`

> **Note:**
>
> Previously, this command was listing only single stores added to an account. Starting with the 2311 release, this command lists multi-stores as well.

List authentication methods

`-lt`

Description: Starting with Citrix Workspace app for Linux version 2402, a new command `-lt` is introduced to list out all types of enabled authentication methods for StoreFront. This command supports using the credential insertion SDK.

Enter the storebrowse command as follows:

```
1  ./storebrowse -lt <full URL>`
```

The output is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enumerate

`-E --enumerate`

Description:

Lists the available resources. By default, the following values appear:

- Resource name
- Display name
- Resource folder

To view more information, append the `-M --details` command to the `-E` command.

> **Note:**
>
> When you run the **-E** command, an authentication window appears if you have not provided your credentials earlier.

Enter the entire store URL as reported by **-liststore**.

Command example of StoreFront:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Subscribed

`-S --subscribed`

Description:

Lists the subscribed resources. By default, the following values appear:

- Resource name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Display name
- Resource folder

To view more information, append the `-M --details` command to the `-E` command.

Command example of StoreFront:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Details

`-M --details`

Description:

This command returns several attributes of the published applications. Generally, this command is used with **-E** and **-S** commands. This command takes an argument that is the sum of the numbers corresponding to the required details:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

> **Notes:**
>
> - To create menu entries for subscribed applications, use the CreateShortcuts(0x100000) argument with the **-S**, **-s**, and **-u** commands.
> - To delete all menu entries, use RemoveShortcuts(0x200000) with the **-S** command.

Command example of StoreFront:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix
/Store/discovery
```

In the preceding command example, 0x264 is the combination of DisplayName(0x200), AppIsDisabled(0x40), AppIsDesktop(0x20), and SoundType(0x4). The output lists the subscribed resources along with the details.

You can use the **-M** command for listing the resources with the required details:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix
/Store/discovery
```

> **Notes:**
>
> - You can express the values in either decimal or in hexadecimal format. For example, 512 for 0x200.
> - When some of the details aren't available through storebrowse, the output value is zero.

Subscribe

```
-s --subscribe
```

Description:

Subscribes the specified resource from a given store.

Command example of StoreFront:

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/
Citrix/Store/discovery
```

Unsubscribe

```
-u --unsubscribe
```

Description:

Unsubscribes the specified resource from a given store.

Command example of StoreFront:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/
Citrix/Store/discovery
```

Launch

```
-L --launch
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Description:

Launches a connection to a published resource. The utility then closes automatically, leaving a successfully connected session.

Command example of StoreFront:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Icons

```
-i --icons
```

Description:

This command fetches desktop and application icons in PNG format. This command is used with the **-E** or the **-S** command.

To fetch icons of required sizes and depths, use the best argument or the size argument method.

Best argument Using the best argument method, you can fetch the best-sized icons available on the server. You can later convert the icons to the required sizes. The best argument method is the most efficient way to store, apply bandwidth, and simplify scripting. The files are saved in the <resource name>.png format.

Size argument To fetch icons of specified sizes and depths, use the size argument method. An error appears if the server is unable to fetch icons of a given size or depth.

The size argument is of the WxB form, where:

- **W** is the width of icons. All icons are square, so only one value is required to specify the size.
- **B** is the color depth. That is, the number of bits per pixel.

> **Note:**
>
> The value **W** is mandatory. The value **B** is optional.

If you leave the values unspecified, icons of all available image depths appear. The files are saved in the <resource name>_WxWxB.png format.

Both the methods save icons in the **.png** format for each resource that the **-E** or the **-S** command returns.

Icons are stored in the **.ICAClient/cache/icons** folder.

Command example of StoreFront:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

Reconnect session

`-W [r|R] --reconnect [r|R]`

Description:

Reconnects the disconnected yet active sessions of the specified store. The [r] option reconnects all the disconnected sessions. The [R] option reconnects all the active and disconnected sessions.

Command example of StoreFront:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

Disconnect session

`-WD --disconnect`

Description:

Disconnects all sessions of the specified store.

Command example of StoreFront:

`./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery`

Terminate session

`-WT --terminate`

Description:

Terminates all sessions of the specified store.

Command example of StoreFront:

`./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Version

```
-v --version
```

Description:

Displays the version of the storebrowse utility.

Command example of StoreFront:

```
./storebrowse -v
```

Root directory

```
-r --icaroot
```

Description:

Specifies the root directory where Citrix Workspace app for Linux is installed. If not specified, the root directory is determined at run time.

Command example of StoreFront:

```
./storebrowse -r /opt/Citrix/ICAClient
```

Username, Password, Domain

```
-U --username, -P --password, -D --domain
```

Description:

Passes the user name, password, and the domain details to the server. This method works only with a PNA store. StoreFront stores ignore this command. The details aren't cached. Enter the details with every command.

Command example of StoreFront:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/
discovery -U user1 -P password -D domain-name
```

Delete store

```
-d --deletestore
```

Description:

Deregisters a store with the ServiceRecord daemon.

Command example of StoreFront:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/
discovery
```

Configure self-service

```
-c --configselfservice
```

Description:

Gets and configures the self-service UI settings that are stored in StoreCache.ctx. Takes an argument of the <entry[=value]> form. If only an entry is present, the setting's current value is printed. However, if a value is present, the value is used to configure the setting.

Command example of StoreFront:

```
./storebrowse -c SharedUserMode=True
```

Add CR file

```
-C --addcr
```

Description:

Reads the provided Citrix Receiver™ (CR) file, and prompts you to add each store. The output is the same as the **-a** command, but has more than one store, separated by new lines.

Command example of StoreFront:

```
./storebrowse -C <path to CR file>
```

Sync connection lease files

```
-o --synclease
```

Description:

Starts to sync Workspace connection lease files with the files available on the remote server for the specified store. This command helps to update the default store and triggers the lease file sync. An error appears if service continuity is disabled.

Command:

```
./storebrowse -o *URL of Store *
```

Command example of StoreFront:

```
./storebrowse –o https://my.firstexamplestore.net
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Close `storebrowse` daemon

`-K --killdaemon`

Description:

Terminates the `storebrowse` daemon. As a result, all credentials and tokens are purged. Starting with the 2311 release, the `-K` command also helps to sign out from the StoreFront™, cloud stores, or NetScaler Gateway.

Command example of StoreFront:

```
./storebrowse -K
```

List error codes

`-e --listerrorcodes`

Description:

Lists the error codes that are registered.

Command example of StoreFront:

```
./storebrowse -e
```

Store gateway

`-g --storegateway`

Description:

Sets the default gateway for a store that is already registered with the ServiceRecord daemon.

Command example of StoreFront:

```
./storebrowse -g “<unique gateway name>” https://my.firstexamplestore
.net/Citrix/Store/discovery
```

> **Note:**
>
> The unique gateway name must be in the list of gateways for the specified store.

Quick launch

`-q, --quicklaunch`

Description:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Launches an application using the direct URL. This command works only for StoreFront stores.

Command example of StoreFront:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Daemonize

```
-n --nosingleshot
```

Description:

Always daemonizes the `storebrowse` process.

Command example of StoreFront:

```
./storebrowse -n
```

File parameters

```
-F --fileparam
```

Description:

Launches a file with the file path and the resource specified.

Command example of StoreFront:

```
./storebrowse -F “<path to file>” -L <Resource Name> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Accept End-User License Agreement (EULA)

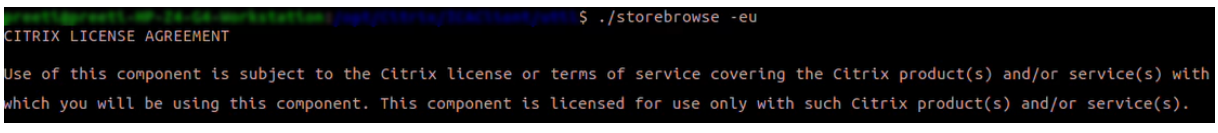
```
-eu --accept-eula
```

Description: This command applies to version 2503 and later. Use this command to accept EULA from the users. This command eliminates the GUI and silently accepts the EULA.

Enter the storebrowse command as follows:

```
./storebrowse -eu
```

The output is as follows:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workflow

This article demonstrates a simple workflow on how to launch an app using the storebrowse commands:

1. `./storebrowse -a https://my.firstexamplestore.net`

   Adds a store and provides the full URL of the store. Make a note of the full URL because it's used in the later commands.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

   Lists all the published apps and desktops. Enter your credentials using the popup that appears for the registered store.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

   Launches the resource. Take the Resource_Name from the output of the previous command.

4. `./storebrowse -K`

   This command purges the credentials entered earlier and closes the `storebrowse` daemon. If you do not mention this command explicitly, the `storebrowse` process exits after an hour.

Troubleshooting

March 5, 2026

This article provides information to help administrators troubleshoot issues with Citrix Workspace app.

Connection

You might come across the following connection issues.

Published resource or desktop session

When establishing a connection to a Windows server, if a dialog box appears with the message "Connecting to server…"but no connection window appears later, you might need to configure the server with a Client Access License (CAL). For more information about licensing, see Licensing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session reconnection

The connection might fail when reconnecting to a session with a higher color depth than that the Citrix Workspace app requires. This failure occurs when running out of available memory on the server.

If the reconnection fails, Citrix Workspace app tries to use the original color depth. Otherwise, the server tries to start a new session with the requested color depth, leaving the original session in a disconnected state. The second connection might also fail if there's still a lack of available memory on the server.

Full Internet name

Citrix® recommends that you configure DNS (Domain Name Server) on your network. This configuration enables you to resolve the names of servers to which you want to connect. If you do not have DNS configured, it might not be possible to resolve the server name to an IP address. Instead, you can specify the server by its IP address, rather than by its name. TLS connections require a fully qualified domain name, not an IP address.

Slow sessions

If a session does not start until you move the mouse, there might be a problem with random number generation in the Linux kernel. As a workaround, run an entropy-generating daemon such as `rngd` (which is hardware-based) or `haveged` (from Magic Software).

Send feedback on Citrix Workspace app

The **Send Feedback** option allows you to inform Cloud Software Group about any issues that you might run into while using Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

This new feature enhances the feedback experience, ensuring a more efficient and informative communication channel between users and support teams.

The **Send Feedback** option includes an integrated log manager, empowering users to capture and include relevant logs for a comprehensive feedback report.

Also, the **Send Feedback** provides seamless communication by enabling users to send feedback emails directly using the default mail client installed on their system.

The supported email clients are the following:

- Thunderbird
- Evolution

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Mutt
- Alpine

To configure email address for send feedback, do the following:

Add the following key in the `Authmanconfig.xml` file:

```
<!-- Configure email address for sendfeedback - - >

<FeedbackEmailAddress>cwa-linux-feedback@cloud.com</
   FeedbackEmailAddress>

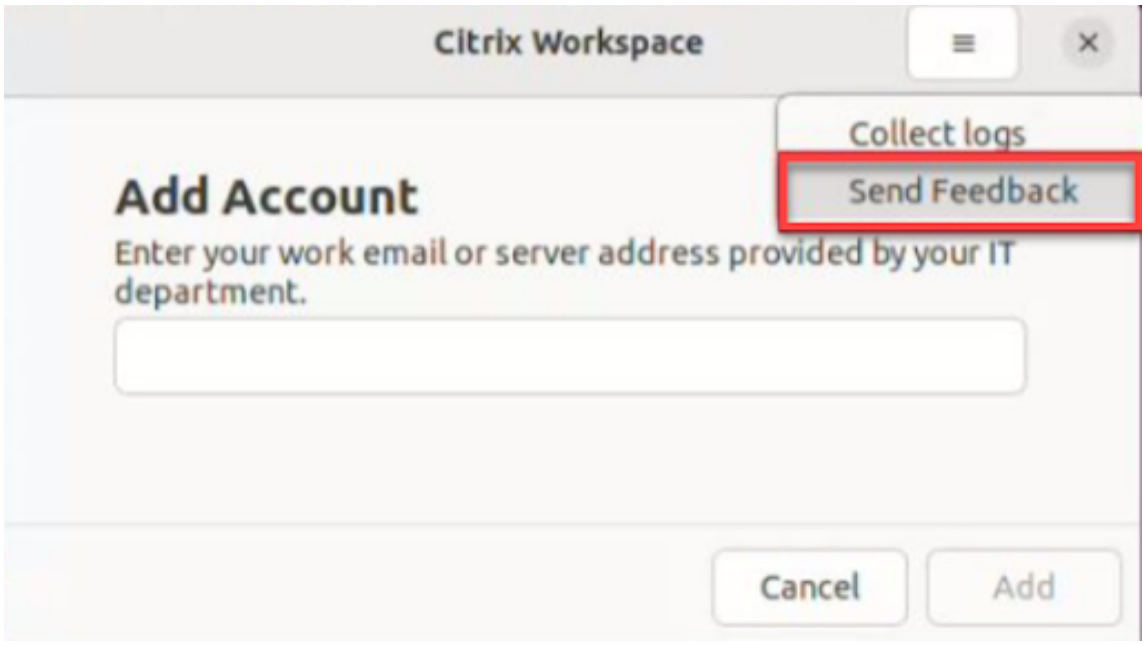
<key>SendFeedbackEnabled</key>

<value>true</value>
```

> **Note:**
>
> By sending your feedback to Cloud Software Group, you agree your participation is in accordance with and subject to the Cloud software Group End User Agreement.

You can send feedback using any one of the following methods:

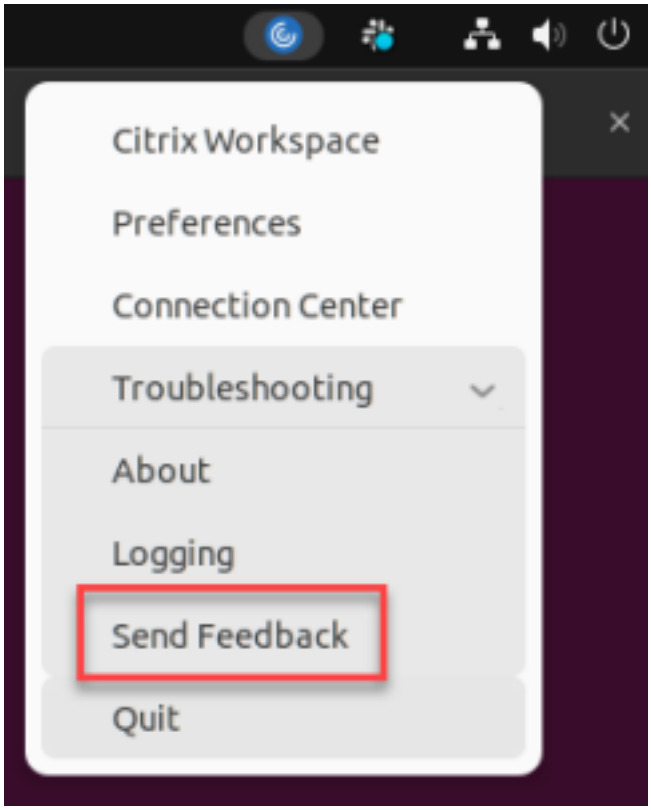
1. Navigate to the **Add Account** screen.
2. Click the hamburger menu.
3. Click **Send Feedback**.



Or,

1. Click **Send Feedback** in the **App indicator** icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



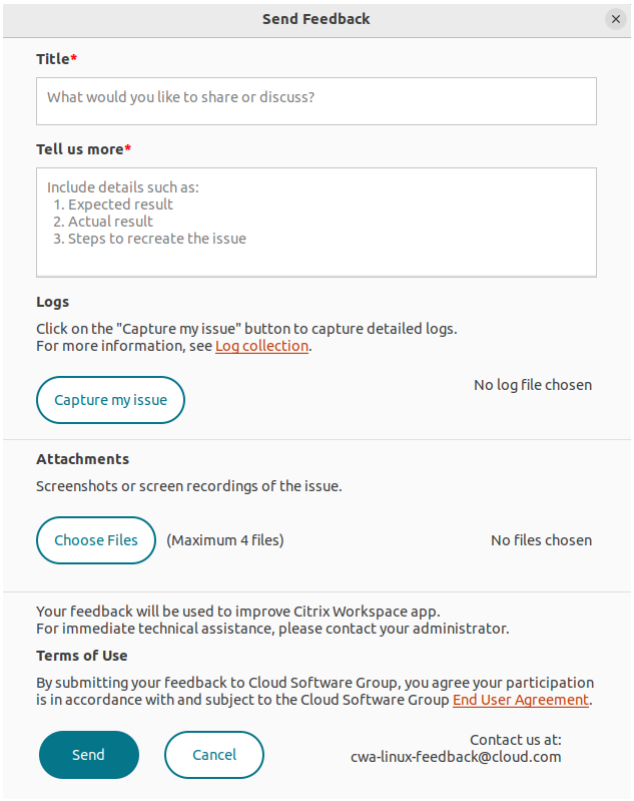
Or,

1. At the command-line, navigate to the `/opt/Citrix/ICAClient/util` path.
2. Run the following command:

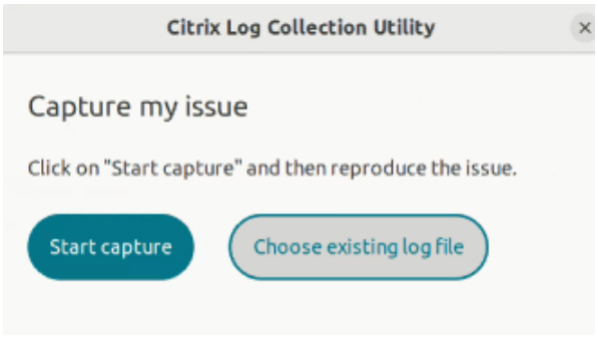
```
./sendfeedback
```

3. The **Send Feedback** screen appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Provide the issue **Title**.
5. Add issue details in the **Tell us more** field.
6. Click **Capture my issue**. The **Citrix Log Collection Utility** screen appears.



Click **Start capture** and then reproduce the issue to collect the latest logs.

Or,

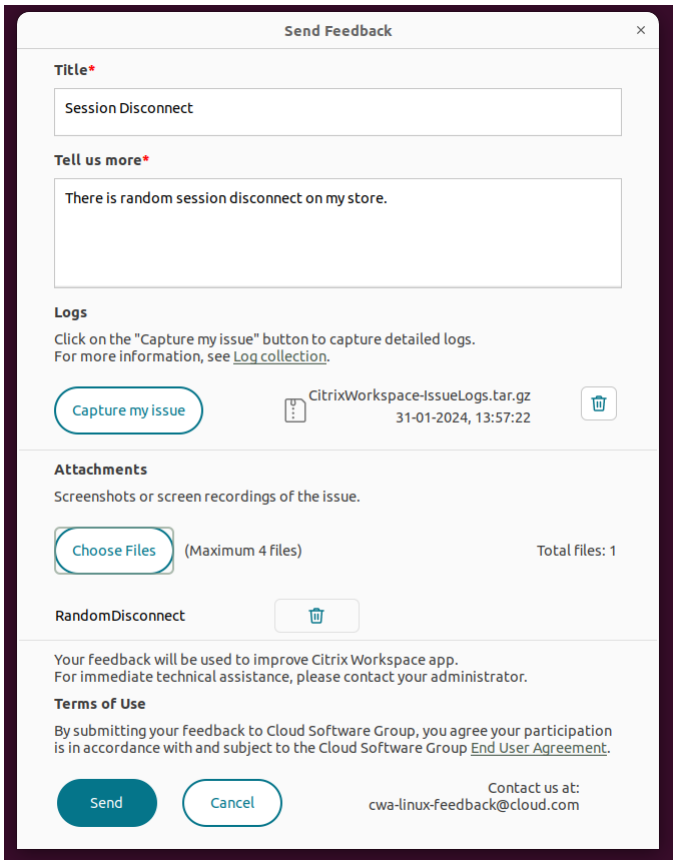
Click **Choose existing logs** if you are not able to reproduce the issue.

> **Note:**
>
> For more information on the Citrix Log Collection Utility, see Log Collection.

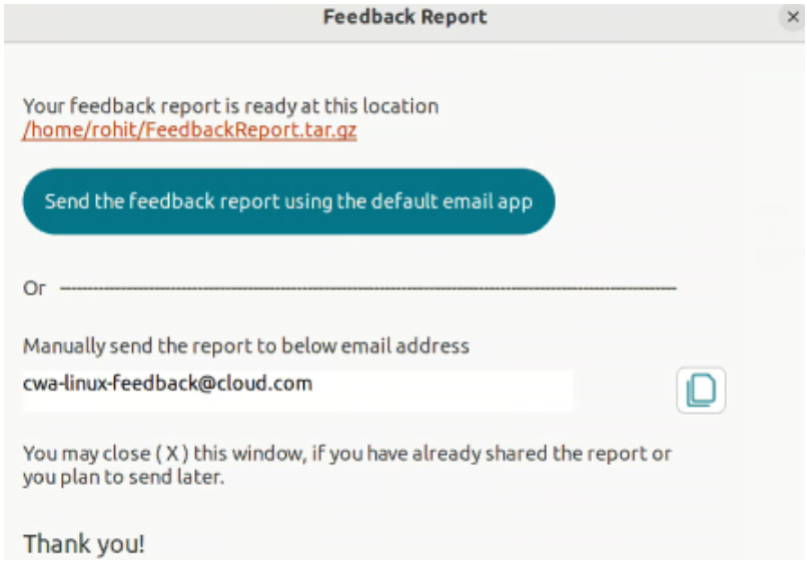
7. Ensure that the log files are displayed next to **Capture my issue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Choose Files** and then add attachments that describe your issues such as screenshots or screen recordings.



9. Click **Send**. The **Feedback report** screen appears.



   The .tar.gz file contains the log files, the issue description as test files, and the attachments.

10. You can send the feedback report to Citrix using the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Send the feedback report using the default email app** to use the default mail app in your system.

Or,

Send the report manually to the provided email ID.

> **Note:**
>
> Ensure that the .zip file is attached in the email.

Cipher suites

If your connection fails with the new cryptographic support:

1. You can use various tools to check the cipher suites that your server support, including:
   - `Ssllabs.com` (requires the server to have Internet access)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. In Linux Client WireShark, find the packet (Client Hello, Server Hello) with the filter (ip.addr == `VDAIPAddress`) to find the SSL section. The result has the cipher suites sent by the client and accepted by the server.

Incorrect Citrix Optimization SDK

The Citrix Optimization SDK package includes an incorrect version of the `UIDialogLibWebKit.so`. As a workaround, do the following:

1. Download Citrix Optimization SDK package version 18.10 from the Downloads page.
   a) Go to the path `CitrixPluginSDK/UIDialogLib/GTK`:

   ```
   cd CitrixPluginSDK/UIDialogLib/GTK
   ```

   b) Delete all the object files:

   ```
   rm -rf *.o
   ```

   c) Go to the WebKit folder:

   ```
   cd ../WebKit
   ```

   d) Remove the existing `UIDialogLibWebKit.so`:

   ```
   rm -rf UIDialogLibWebKit.so
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e) Use the following command in the WebKit directory:

```
make all
```

The new `UIDialogLibWebKit.so` is generated.

f) Copy the new library into the **$ICAROOT/lib** directory.

Weak cipher suites for SSL connections

When making a TLS connection, the Citrix Workspace app offers an advanced and restricted set of cipher suites by default.

If you're connecting to a server that requires an older cipher suite, set the configuration option `SSLCiphers=ALL` in the [WFClient] section of a configuration file.

The following advanced cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

Loss of connection

When using the EDT protocol, you might see the error message: Connection to "…"has been lost. This issue might occur when the connection goes through a router with a Maximum Transmission Unit for EDT that is smaller than the default of 1,500 bytes. Do the following:

- Set `edtMSS=1000` in a configuration file.

Connection errors

Connection errors might produce various different error dialogs. Examples are:

- Error in connection: A protocol error occurred while communicating with the Authentication Service.
- The Authentication Service can't be contacted.
- Your account can't be added using this server address.

Some problems might cause such errors, including:

- An error might occur when the local computer and the remote computer can't negotiate a common TLS protocol. For more information, see TLS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An error might occur when the remote computer requires an older cipher suite for a TLS connection. In this case, you can set the configuration option `SSLCiphers=ALL` in the `\[WFClient\]` section of a configuration file and run `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` before restarting the connection.
- An error might occur when the remote computer requests a client certificate inappropriately. IIS must only **accept** or **require** certificates for Citrix, Authentication, and Certificate.
- Other problems.

Low-bandwidth connections

Citrix recommends you use the latest version of Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) on the server. Also, the use the latest Citrix Workspace app on the user device.

If you're using a low-bandwidth connection, you can change your Citrix Workspace app configuration and the way you use Citrix Workspace app to improve performance.

- **Configure your Citrix Workspace app connection** - Configuring your Citrix Workspace app connections can reduce the bandwidth that ICA requires and improves performance
- **Change how Citrix Workspace app is used** - Changing the way Citrix Workspace app is used can also reduce the bandwidth required for a high-performance connection
- **Enable UDP audio** - This feature can maintain consistent latency on congested networks in Voice-over-IP (VoIP) connections
- **Use the latest versions of Citrix Workspace app for Linux and Citrix Virtual Apps and Desktops or Citrix DaaS** - Citrix continually enhances and improves performance with each release, and many performance features require the latest Citrix Workspace app and server software

Display

Screen tearing

Screen tearing occurs when parts of two (or more) different frames appear on the screen at the same time, in horizontal blocks. This issue is most visible with large areas of fast changing content on screen.

Tearing is avoided when data is captured at the VDA. Tearing isn't introduced when data is passed to the client. However, X11 (the Linux/Unix graphics subsystem) does not provide a consistent way to draw to the screen in a way that prevents tearing.

To prevent screen tearing, Citrix recommends the standard approach which synchronizes application drawing with the drawing of the screen. That is, wait for `vsvnc`, to start the drawing of the next

© 1997–2026 Citrix Systems, Inc. All rights reserved.

frame. Depending on the graphics hardware on the client and the window manager you're using, the following two groups of solutions are available to prevent screen tearing:

- X11 GPU settings
- Use a Composition Manager

X11 GPU Configuration

For Intel HD graphics, create a file in the xorg.conf.d called **20-intel.conf** with the following contents:

```
Section "Device"

 Identifier    "Intel Graphics"
 Driver        "intel"
 Option        "AccelMethod" "sna"
 Option        "TearFree" "true"

 EndSection
```

For NVIDIA graphics, locate the file in the xorg.conf.d folder that includes the "MetaModes"Option for your configuration. For each comma-separated MetaMode used add the following:

{ForceFullCompositionPipeline = On}

For example:

Option "MetaModes""DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"

> **Note:**
>
> Different Linux distributions use different paths to xorg.conf.d, for example, /etc/X11/xorg.conf.d, or, /user/share/X11/xorg.conf.d.

Composition managers

Use the following:

- Compiz (built into Ubuntu Unity). Install the "CompizConfig Settings Manager."

  Run "CompizConfig Settings Manager".

  Under **General** > **Composition** clear **Undirect Fullscreen Windows**.

> **Note:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Use "CompizConfig Settings Manager"with caution because incorrectly changing values can prevent the system from launching.

- Compton (an add-on utility). Refer to the main page/documentation for Compton for full details. For example, run the following command:

  ```
  compton --vsync opengl --vsync -aggressive
  ```

Incorrect keystrokes

If you're using a non-English language keyboard, the screen display might not match the keyboard input. In this case, you must specify the keyboard type and layout that you're using. For more information about specifying keyboards, see Control keyboard behavior.

Excessive redrawing

Some window managers continuously report the new window position when moving seamless windows, which can result in excessive redrawing. To fix this problem, switch the window manager to a mode that draws only window outlines when moving a window.

Icon compatibility

The Citrix Workspace app creates window icons that are compatible with most window managers. However, these icons aren't fully compatible with the X Inter-Client Communication Convention.

Full icon compatibility

To provide full icon compatibility:

1. Open the wfclient.ini configuration file.
2. Edit the following line in the [WFClient] section: UseIconWindow=True
3. Save and close the file.

Cursor color

The cursor can be difficult to see if it's the same or similar in color to the background. You can fix this issue by forcing areas of the cursor to be black or white.

To change the color of the cursor

1. Open the wfclient.ini configuration file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Add one of the following lines to the [WFClient] section:

   CursorStipple=ffff,ffff (to make the cursor black)

   CursorStipple=0,0 (to make the cursor white)

3. Save and close the file.

Color flash

When you move the mouse into or out of a connection window, the colors in the non-focused window start to flash. This issue is a known limitation when using the X Windows System with PseudoColor displays. If possible, use a higher color depth for the affected connection.

Color changes with TrueColor display

You have the option of using 256 colors when connecting to a server. This option assumes that the video hardware has palette support to enable applications to change the palate colors to produce animated displays.

TrueColor displays have no facility to emulate the ability to produce animations by rapidly changing the palette. Software emulation of this facility is expensive for time and network traffic. To reduce this cost, Citrix Workspace app buffers rapid palette changes, and updates the real palette only every few seconds.

Incorrect display

Citrix Workspace app uses EUC-JP or UTF-8 character encoding for Japanese characters, while the server uses SJIS character encoding. Citrix Workspace app does not translate between these character sets. This issue can cause problems displaying:

- files that are saved on the server and viewed locally
- files that are saved locally and viewed on the server

This issue also affects Japanese characters in parameters used in extended parameter passing.

Session span

Full-screen sessions span all monitors by default, but a command-line multi-monitor display control option, -span, is also available. It allows full-screen sessions to span extra monitors.

Desktop Viewer toolbar functionality allows you to switch a session between windowed and full-screen session window, including multi-monitor support for the intersected monitors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Span has no effect on Seamless or normal windowed sessions (including those sessions in maximized windows).

The - span option has the following format:
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]

If `h` is specified, a list of monitors is printed on `stdout`. If `h` is the whole option value, `wfica` exits.

If `o` is specified, the session window has the `override-redirect` attribute.

Caution:

- The use of this option isn't recommended. It's intended as a last option to use with uncooperative window managers.
- The session window isn't visible to the window manager, does not have an icon, and can't be restacked.
- It can be removed only by ending the session.

If `a` is specified, Citrix Workspace app tries to create a session that covers all monitors.

Citrix Workspace app assumes that the rest of the -span option value is a list of monitor numbers:

- A single value selects a specific monitor.
- Two values select monitors at the top-left and bottom-right corners of the required area.
- Four values specify monitors at the top, bottom, left, and right edges of the area.

Assuming `o` wasn't specified, wfica uses the _NET_WM_FULLSCREEN_MONITORS message to request an appropriate window layout from the window manager, if it's supported. Otherwise, it uses size and position hints to request the desired layout.

The following command can be used to test for window manager support:
`xprop -root | grep \\_NET\\_WM\\_FULLSCREEN\\_MONITORS`

If there's no output, there's no support. If there's no support, you might need an override-redirect window. You can set up an override-redirect window using `-span o`.

To make a session that spans extra monitors from the command line:

1. At a command prompt, type:

   `/opt/Citrix/ICAClient/wfica -span h`

   A list of the numbers of the monitors currently connected to the user device is printed to `stdout` and `wfica` exits.

2. Make a note of these monitor numbers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. At a command prompt, type:

   ```
   /opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
   ```

   The w, x, y, and z values are monitor numbers from step 1 of the preceding steps. The single value w, specifies a specific monitor. Two values w and x specify monitors at the top-left and bottom-right corners of the required area.Four values w, x, y, and z specify monitors at the top, bottom, left, and right edges of the area.

   ```
   > **Important:**
   >
   > - Define the WFICA\_OPTS variable before starting self-service through a browser. To defin this variable, edit your profile file, normally found at $HOME/.bash\_profile or $HOME/.profile, adding a line to define the WFICA\_OPTS variable. For example: `export WFICA_OPTS="-span a"`
   > - This change affects both virtual apps and desktops sessions.
   > - If you have started self-service or `storebrowse`, remove processes that are started for the new environment variable to take effect. Remove them with: `killall AuthManagerDaemon ServiceRecord storebrowse`
   ```

Local applications

You might not escape from a full-screen session to use local applications or another session. This issue occurs because the client-side system UI is hidden and the Keyboard Transparency feature disables the usual keyboard command, for example Alt+Tab, sending the command to the server instead.

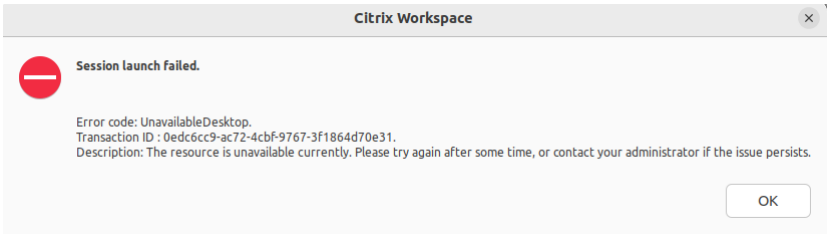
As a workaround, use CTRL+F2 to clear the Keyboard Transparency feature temporarily until the focus next returns to the session window. An alternative workaround is to set TransparentKeyPassthrough to No in $ICAROOT/config/module.ini. This workaround disables the Keyboard Transparency feature. However, you might have to override the **ICA file by adding this** setting in the All_regions.ini file.

Improved error messages

Previously all error messages were having a default error code and a description that isn't specific to the error. Starting with Citrix Workspace app version 2309, the error messages are improved to include the **Error code**, **Transaction ID**, and **Description** fields specific to the error. These error messages appear when a session starts using ICA launch or when a session starts with the Service Continuity feature enabled.

For example, if there's a session launch failure, the following error message is displayed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Webcam

Updating the default webcam

Currently, webcam redirection in Citrix Workspace app for Linux supports only one webcam at a time. The default webcam selected is mapped to the device path `/dev/video0` which is, generally, the built-in webcam in laptops.

To list all devices with video capabilities in the system, you must install v4l tools using the following command:

```
sudo apt-get install v4l-utils
```

List the video devices using the following command:

```
v4l2-ctl --list-devices
```

You might receive an output as follows:

```
user@user-pc:~ $ v4l2-ctl --list-devices
UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
    /dev/video2
    /dev/video3
    /dev/media1
Integrated Camera: Integrated C (usb-0000:00:14.0-8):
    /dev/video0
    /dev/video1
    /dev/media0
```

As per the preceding example, there are two webcams. You can use any of them. Citrix recommends using the first index. There's a known issue with Ubuntu, so that you might see multiple indexes for one webcam. In this example, you can use /dev/video0 and /dev/video2.

To set another capture video as default, do the following:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. In the [WFClient] section, add the following setting.

   `HDXWebCamDevice=<device path>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, add `HDXWebCamDevice=/dev/video2` to set the webcam mapped to `/dev/video2` in a system.

Testing capabilities

On the client, the webcam redirection module can be used in different modes to test isolated components under customer environment conditions.

Production and debug mode This mode compares the video displaying on the VDA side and the actual buffers that the encoder produces on the client side. It allows to test the entire pipeline.

To enable this mode:

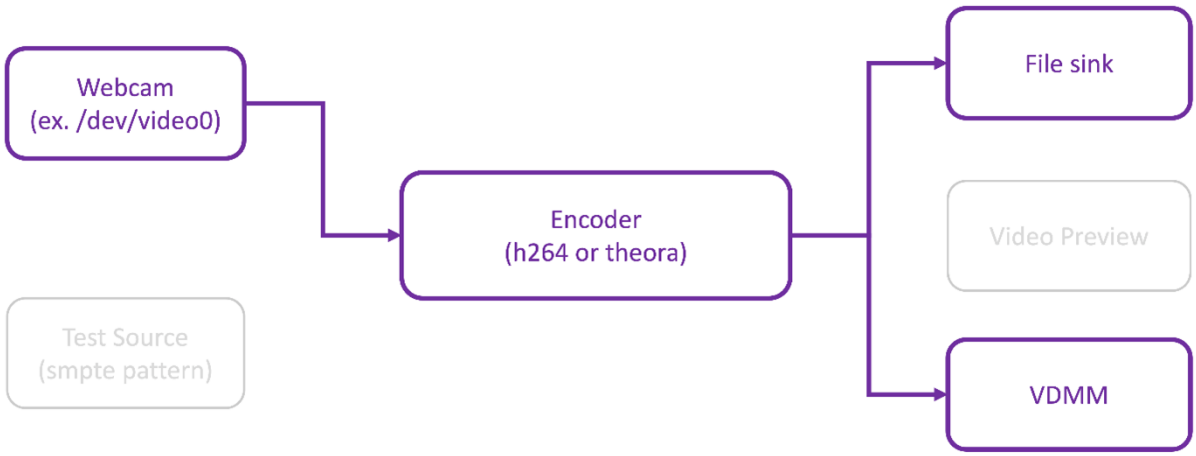
1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. Set the `HDXWebcamDebug` value to **True**.

   HDXWebcamDebug=True

After this mode is enabled, the encoder generates the following files with the buffers, depending on the encoder used:

- For H264 encoder: /tmp/file_mode_buffers.h264
- For Theora encoder: /tmp/file_mode_buffers.theora

The following diagram describes the production and debug modes:



Webcam tester mode This mode allows you to test the webcam isolated from the rest of the pipeline elements.

```
./gst_read --buffers | -b BUFFERS_AMOUNT  [ --input_device | -i
   WEBCAM_DEVICE; default=/dev/video0]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable to webcam tester mode, run the following commands from the command lines:

```
cd /opt/Citrix/ICAClient/util
```

```
`$./gst_read -b 100 /dev/video0
```

After this mode is enabled, a video preview appears and creates the following file with the raw buffers from the webcam:

/tmp/wewbcam_buffers.buff

The only switch required for webcam tester mode is the `--buffers (-b)` options. You can also specify the webcam device to test. For example, see the following:

- ./gst_read -buffers 150
- ./gst_read –buffers 100 –input_device /dev/video2

The following diagram describes the webcam tester mode:



Encoder tester mode This mode allows you to test the encoder isolated from the pipeline.

```
./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT;
    default=10 0 ]  [ --enableH264  | -e ]
```

To enable the encoder tester mode, run the following commands from the command lines:

```
cd /opt/Citrix/ICAClient/util
```

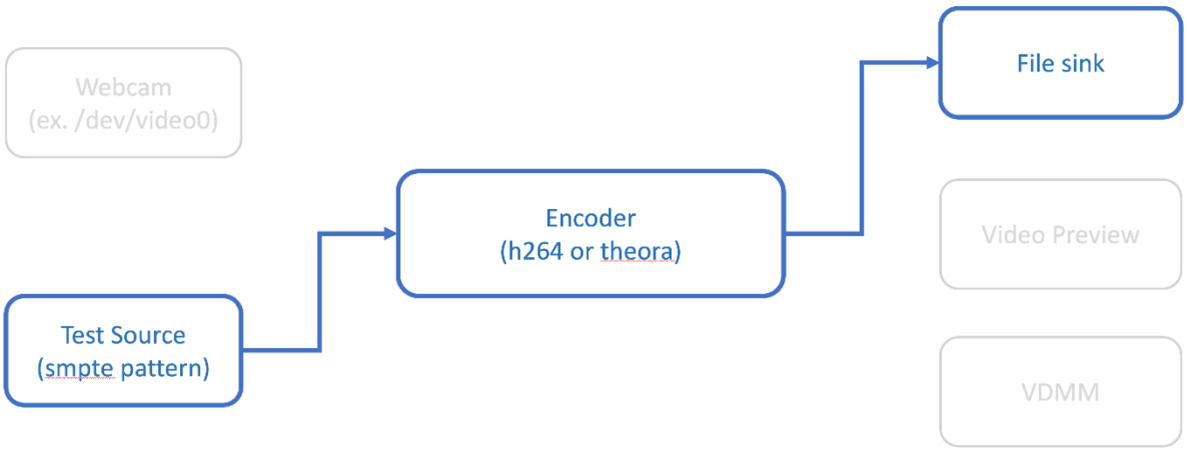
```
./gst_read -o ~/file_buffers.h264 -e
```

The only switch required for this mode is the `--output_file (-o)` options. You can also test Theora or H264 encoders and the amount of buffer to generate. For example, see the following:

- For H264: ./gst_read –output_file ~/file_buffers.h264 –buffers 200 –enableH264
- For Theora: ./gst_read -o ~/file_buffers.theora -b 100

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following diagram describes the encoder tester mode:



H264 software encoder If the software-based H264 encoder does not work correctly, you must verify its dependencies using the following steps:

1. Verify if the x264 `GStreamer` plug-in is in the system as part of `gstreamer-plugins-ugly`. If it's available in the `libgstx264.so` library, run the following command to verify it:

```
1 gst-inspect-1.0 x264
```

```
:/opt/Citrix/ICAClient$ gst-inspect-1.0 x264
Plugin Details:
  Name                     x264
  Description              libx264-based H264 plugins
  Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
  Version                  1.14.5
  License                  GPL
  Source module            gst-plugins-ugly
  Source release date      2019-05-29
  Binary package           GStreamer Ugly Plugins (Ubuntu)
  Origin URL               https://launchpad.net/distros/ubuntu/+source/gst-plugins-ugly1.0

  x264enc: x264enc

  1 features:
  +-- 1 elements
```

2. Run the following command to verify the dependencies of the `libgstx264.so` library:

```
1 ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
:/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
        linux-vdso.so.1 (0x00007ffcf23c5000)
        /usr/local/lib/AppProtection/libAppProtection.so (0x00007fde6482f000)
        libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007fde64596000)
        libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007fde6435e000)
        libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007fde64023000)
        libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007fde63dcf000)
        libx264.so.152 => /usr/lib/x86_64-linux-gnu/libx264.so.152 (0x00007fde63a2a000)
        libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007fde63826000)
        libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007fde6350f000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fde6311e000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007fde62eff000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007fde62cfb000)
        libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007fde629c3000)
        libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007fde6279b000)
        libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007fde62412000)
        libXi.so.6 => /usr/lib/x86_64-linux-gnu/libXi.so.6 (0x00007fde62202000)
        libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007fde61f8d000)
        liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007fde61d11000)
        libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007fde61973000)
        libgstaudio-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstaudio-1.0.so.0 (0x00007fde616fe000)
        libgsttag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgsttag-1.0.so.0 (0x00007fde614c3000)
        librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007fde612bb000)
        libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007fde610b3000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007fde60e41000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fde64c64000)
        libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007fde60c3d000)
        libXdmcp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmcp.so.6 (0x00007fde60a37000)
        libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007fde6081f000)
        libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007fde6060d000)
        libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007fde603f0000)
        libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007fde601db000)
```

If the `libgstx264.so` file isn't present, you must install `GStreamer` plugins ugly using the following command:

```
sudo apt-get install gstreamer1
0-plugins-ugly
```

H264 hardware encoder

1. Verify `vaapi GStreamer` plug-in is in the system as part of `gstreamer1.0-vaapi`. If it's available in the `libgstvaapi.so` library, run the following command to verify it:

   ```
   gst-inspect-1.0 vaapi
   ```

   ```
   :/opt/Citrix/ICAClient$ gst-inspect-1.0 vaapi
   Plugin Details:
     Name                     vaapi
     Description              VA-API based elements
     Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
     Version                  1.14.5
     License                  LGPL
     Source module            gstreamer-vaapi
     Source release date      2019-05-29
     Binary package           gstreamer-vaapi
     Origin URL               http://bugzilla.gnome.org/enter_bug.cgi?product=GStreamer

     0 features:

   :/opt/Citrix/ICAClient$
   ```

2. Run the following command to verify the dependencies of the libgstvaapi.so library:

   ```
   ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
        linux-vdso.so.1 (0x00007ffd635fe000)
        /usr/local/lib/AppProtection/libAppProtection.so (0x00007f5eb1d5e000)
        libgstcodecparsers-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstcodecparsers-1.0.so.0 (0x00007f5eb1b1b000)
        libdrm.so.2 => /usr/lib/x86_64-linux-gnu/libdrm.so.2 (0x00007f5eb190a000)
        libudev.so.1 => /lib/x86_64-linux-gnu/libudev.so.1 (0x00007f5eb16ec000)
        libva-drm.so.2 => /usr/lib/x86_64-linux-gnu/libva-drm.so.2 (0x00007f5eb14e9000)
        libXrandr.so.2 => /usr/lib/x86_64-linux-gnu/libXrandr.so.2 (0x00007f5eb12de000)
        libXrender.so.1 => /usr/lib/x86_64-linux-gnu/libXrender.so.1 (0x00007f5eb10d4000)
        libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007f5eb0d9c000)
        libGL.so.1 => /usr/lib/x86_64-linux-gnu/libGL.so.1 (0x00007f5eb0b10000)
        libva-x11.so.2 => /usr/lib/x86_64-linux-gnu/libva-x11.so.2 (0x00007f5eb090a000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f5eb0706000)
        libEGL.so.1 => /usr/lib/x86_64-linux-gnu/libEGL.so.1 (0x00007f5eb04f2000)
        libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007f5eb02ee000)
        libva-wayland.so.2 => /usr/lib/x86_64-linux-gnu/libva-wayland.so.2 (0x00007f5eb00e9000)
        libva.so.2 => /usr/lib/x86_64-linux-gnu/libva.so.2 (0x00007f5eafec8000)
        libwayland-client.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-client.so.0 (0x00007f5eafcb9000)
        libgstgl-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstgl-1.0.so.0 (0x00007f5eafa53000)
        libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007f5eaf81b000)
        libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007f5eaf582000)
        libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007f5eaf30d000)
        libgstallocators-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstallocators-1.0.so.0 (0x00007f5eaf109000)
        libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007f5eaedce000)
        libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007f5eaeb7a000)
        libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007f5eae863000)
        libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007f5eae4c5000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f5eae2a6000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f5eadeb5000)
        libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007f5eadc8d000)
        libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007f5ead904000)
        libXi.so.6 => /usr/lib/x86_64-linux-gnu/libXi.so.6 (0x00007f5ead6f4000)
        librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007f5ead4ec000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f5eb2261000)
        libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007f5ead2da000)
        libGLX.so.0 => /usr/lib/x86_64-linux-gnu/libGLX.so.0 (0x00007f5ead0a9000)
        libGLdispatch.so.0 => /usr/lib/x86_64-linux-gnu/libGLdispatch.so.0 (0x00007f5eacdf3000)
        libXfixes.so.3 => /usr/lib/x86_64-linux-gnu/libXfixes.so.3 (0x00007f5eacbed000)
        libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007f5eac9e5000)
        libX11-xcb.so.1 => /usr/lib/x86_64-linux-gnu/libX11-xcb.so.1 (0x00007f5eac7e3000)
        libwayland-egl.so.1 => /usr/lib/x86_64-linux-gnu/libwayland-egl.so.1 (0x00007f5eac5e1000)
        libgbm.so.1 => /usr/lib/x86_64-linux-gnu/libgbm.so.1 (0x00007f5eac3d2000)
        libgudev-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgudev-1.0.so.0 (0x00007f5eac1c8000)
        libgstaudio-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstaudio-1.0.so.0 (0x00007f5eabf53000)
        libgsttag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgsttag-1.0.so.0 (0x00007f5eabd18000)
        liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007f5eaba9c000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f5eab82a000)
        libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007f5eab626000)
        libXdmcp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmcp.so.6 (0x00007f5eab420000)
        libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007f5eab208000)
        libwayland-server.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-server.so.0 (0x00007f5eaaff5000)
        libexpat.so.1 => /lib/x86_64-linux-gnu/libexpat.so.1 (0x00007f5eaadc3000)
        libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f5eaaba6000)
        libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007f5eaa991000)
gamilr@ubuntu:/opt/Citrix/ICAClient$
```

3. Resolve any missing dependencies.

To install and configure `vaapi`, follow the `GStreamer vappi` installation guide.

Collect internal `GStreamer` frameworks and gst_read logs

Alternative to regular `ICAClient` logs, you must collect the logs from the `gst_read` module.

Do the following to collect the logs:

1. Open a terminal and run the following commands:

```
export GST_DEBUG=2,gst_read_debug:6
```

```
export GST_DEBUG_FILE=~/gst_read.log
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This variable sets the level of log collection and the file to store them. In this case, we're setting level 2 for the `GStreamer` framework and level 7 for the `gst_read` module. For more information, see the document. It's recommended only to set error and warning levels for the internal `GStreamer` framework and log level for `gst_read`.

2. Download an ICA® file of a valid VDA.
3. On the same terminal, run the following command to start a VDA session:

```
cd /opt/Citrix/ICAClient
```

```
./wfica   <ICA file path>/vda.ica
```

The `gst_read.log` file is generated with the internal `GStreamer` framework and the `gst_read` logs.

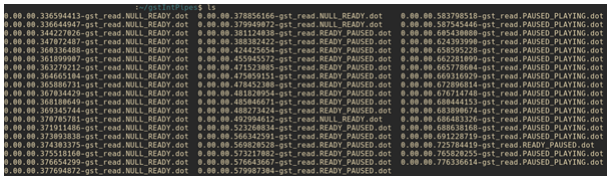
`GStreamer` pipeline inspections To see the actual pipelines that the `GStreamer` framework is creating, do the following:

1. Create a folder to store the dot files, for example: `gstIntPipes`.
2. Open a terminal and export `GST_DEBUG_DUMP_DOT_DIR=<Absolute path>/gstIntPipes`. This variable indicates to the `GStreamer` where to store the dot files.
3. Download an ICA file of a valid VDA.
4. On the same terminal, run the following commands to start a VDA session:

```
cd /opt/Citrix/ICAClient/
```

```
./wfica <ICA file path>/vda.ica
```

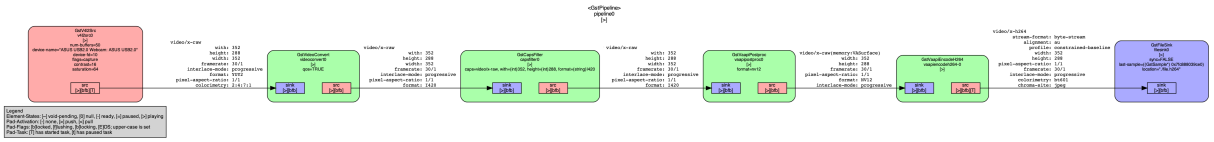
5. The directory `gstIntPipes` includes the dot files. `GStreamer` generates a dot file for every state change in the pipeline. As a result, you can inspect all the processes of the pipeline creation. The following is an example of the set of dot files:



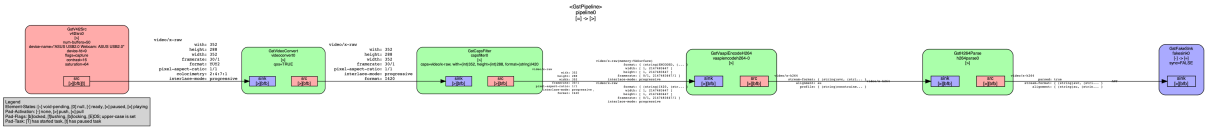
6. Install a dot file utility to see a visual representation of the pipelines. For example, Graphviz. The following images are examples of good and bad creation of the pipeline:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pipeline successfully created:



Pipeline unable to link:



> **Note:**
>
> To enlarge the preceding images or any other images, right-click the image, select **Open image in new tab**, and zoom the browser as required.

As shown in the preceding image, the second pipeline is unable to link the `GstCapsFilter` element and the `GstVaapiEncodeH264` element. The capabilities are never fully negotiated. For more information, see the document.

System diagnostic script for RAVE

We provide a script, `rave_troubleshooting.sh` to verify whether the system configuration and dependencies are suitable to support Remote Audio Video Extensions (RAVE).

> **Note:**
>
> RAVE is an HDX™ feature to support optimized webcam redirection and Windows Media Player redirection for Citrix VDAs.

Do the following to run the script:

1. Click rave_troubleshooting.sh to download the script.
2. Open the terminal in your Linux machine.
3. Type `rave_troubleshooting.sh --help` or `rave_troubleshooting.sh -h` to see the supporting command line arguments.
4. Type one of the following:
   - `rave_troubleshooting.sh -w` or `rave_troubleshooting.sh --webcam` - Use this command to run checks for webcam redirection. This command is the default command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `rave_troubleshooting.sh -r` or `rave_troubleshooting.sh --rave` - Use this command to run checks for RAVE. A pop-up window playing a h264 test video is displayed.

The system configuration and dependencies are displayed.

Generic USB redirection

How to redirect Android phones as generic USB

You can redirect Android phones as generic USB as follows:

1. Connect your Android phone to the system where Citrix Workspace app for Linux is installed using a USB cable.
2. Select USB connection mode (MTP or PTP) on your phone. For most Android phones, the supported mode is PTP.
3. Type the following in the terminal to get your Android phone's vendor ID from the device descriptor (VID) and product ID from the device descriptor (PID):

```
lsusb
```

4. Take a note of the VID and PID your Android phone.
5. Navigate to `usb.conf` file.
6. Add the `CONNECT vid=<vid of your phone> pid=<pid of your phone> split=01 intf=00` line at the end of the `usb.conf` file. For example, add it as follows:

```
CONNECT vid=18d1 pid=4ee2 split=01 intf=00
```

7. Navigate to the **Device** menu in the Desktop Viewer toolbar.
8. Select the Android phone that you want to redirect.

Browser

Local browser

When you click a link in a Windows session, the content appears in a local browser. Server-client content redirection is enabled in wfclient.ini. This redirection causes a local application to run. To disable server-client content redirection, see server-client content redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access published resources

When you access published resources, your browser prompts to save a file. Browsers other than Firefox and Chrome might require configuration before you can connect to a published resource. However, when trying to access a resource by clicking an icon on the page, your browser prompts you to save the ICA file.

Specific browser

If you have problems using a specific web browser, set the environment variable BROWSER to specify the local path and name of the required browser before running `setupwfc`.

Firefox browser

When you launch desktops or applications in Firefox, if a page is unresponsive, try enabling the ICA plug-in.

ICA plug-in in Firefox

When the ICA plug-in is enabled in Firefox, desktop and application sessions might not start. In this case, try disabling the ICA plug-in.

Configuration errors

These errors might occur if you configured a connection entry incorrectly.

E_MISSING_INI_SECTION - Verify the configuration file: "…". The section "…"is missing in the configuration file.

The configuration file was incorrectly edited or is corrupt.

E_MISSING_INI_ENTRY - Verify the configuration file: "…". The section "…"must contain an entry "…".

The configuration file was incorrectly edited or is corrupt.

E_INI_VENDOR_RANGE - Verify the configuration file: "…". The X server vendor range "…"in the configuration file is invalid.

The X Server vendor information in the configuration file is corrupt. Contact Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wfclient.ini configuration errors

These errors might occur if you edited wfclient.ini incorrectly.

`E\\_CANNOT\\_WRITE\\_FILE - Cannot write file: "..."`

There was a problem saving the connection database; for example, no disk space.

`E\\_CANNOT\\_CREATE\\_FILE - Cannot create file: "..."`

There was a problem creating a connection database.

E_PNAGENT_FILE_UNREADABLE - Cannot read Citrix Virtual Apps file "…": No such file or directory.

—Or —

Cannot read Citrix Virtual Apps™ file "…": Permission denied.

You're trying to access a resource through a desktop item or menu, but the Citrix Virtual Apps and Desktops™ or Citrix DaaS file for the resource isn't available. Refresh the list of published resources by selecting Application Refresh on the **View** menu, and try to access the resource again. If the error persists:

- Check the properties of the desktop icon or menu item
- Check the Citrix Virtual Apps and Desktops or Citrix DaaS™ file to which the icon or item refers.

Browser Content Redirection

For information on how to troubleshoot Browser Content Redirection, see the Knowledge Center article CTX230052.

How to import self-signed certificate into nssdb

Run the following command in the terminal to import the self-signed certificate into `nssdb`:

```
1 certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/Downloads/
     badssl.cer
```

The arguments in the commands are:

- `-A` - To add a certificate to the database.
- `-n` - The name of the certificate. This argument is optional and can be used to add the nick name.
- `"badssl.cer"` - The name of the certificate that is exported from the badssl.com site.
- `-t "C,,"` - `-t` is for TRUSTARGS and C is for CA certificate. For more information, see the Google documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `-d ~/.pki/nssdb` - The location of the database.
- `-i` - Denotes the input file. This argument is to add the location and name of the certificate file.

For information about BCR, see the Browser content redirection page in the Citrix Virtual Apps and Desktops documentation.

Others

Connection issues

You might also find the following issues.

Close a session

To know whether the server has instructed Citrix Workspace app to close a session, use the `wfica` program. This program logs when it has received a command to terminate the session from the server.

To record this information through the syslog system, add *SyslogThreshold* with the value 6 to the [WFClient] section of the configuration file. This setting enables the logging of messages that have a priority of LOG_INFO or higher. The default value for *SyslogThreshold* is 4 (=LOG_WARNING).

Similarly, to have `wfica`, send the information to standard error and add *PrintLogThreshold* with the value 6 to the [WFClient] section. The default value for *PrintLogThreshold* is 0 (=LOG_EMERG).

For more information on log collection, see Log collection and for more information on syslog configuration, see syslog configuration.

Configuration file settings

For each entry in wfclient.ini, there must be a corresponding entry in All_Regions.ini for the setting to take effect. Also, for each entry in the [Thinwire3.0], [ClientDrive], and [TCP/IP] sections of wfclient.ini, there must be a corresponding entry in canonicalization.ini for the setting to take effect. See the All_Regions.ini and canonicalization.ini files in the $ICAROOT/config directory for more information.

Published applications

If you have issues running published applications that access a serial port, the application might fail (with or without an error message, depending on the application itself) if the port has been locked by another application. In such circumstances, check that there are no applications that have either temporarily locked the serial port or have locked the serial port and exited without releasing it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To overcome this problem, stop the application that is blocking the serial port. Regarding UUCP-style locks, there might be a lock file left behind after the application exits. The location of these lock files depends on the operating system used.

Starting Citrix Workspace app

If Citrix Workspace app does not start, the error message "Application default file could not be found or is out of date"appears. The reason might be that the environment variable ICAROOT isn't defined correctly. This variable is a requirement if you installed Citrix Workspace app to a non-default location. To overcome this problem, Citrix recommends that you do one of the following:

- Define ICAROOT as the installation directory.

  To check that the ICAROOT environment variable is defined correctly, try starting Citrix Workspace app from a terminal session. If the error message still appears, it's likely that the ICAROOT environment variable isn't correctly defined.

- Reinstall Citrix Workspace app to the default location. For more information about installing Citrix Workspace app, see Install and set up.

  If Citrix Workspace app was previously installed in the default location, remove the `/opt/Citrix/ICAClient` or `$HOME/ICAClient/platform` directory before reinstalling.

Citrix CryptoKit (formerly SSLSDK)

To find the Citrix CryptoKit (formerly SSLSDK) or OpenSSL version number that you're running, you can use the following command:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

You can also run this command on AuthManagerDaemon or PrimaryAuthManager

Keyboard shortcuts

If your window manager uses the same key combinations to provide native functionality, your key combinations might not function correctly. For example, the KDE window manager uses the combinations from CTRL+SHIFT+F1 to CTRL+SHIFT+F4 to switch between desktops 13 to 16. If you experience this problem, try the following solutions:

- Translated mode on the keyboard maps a set of local key combinations to server-side key combinations. For example, by default in Translated mode, CTRL+SHIFT+F1 maps to the server-side key combination ALT+F1. To reconfigure this mapping to an alternative local key combination, update the following entry in the [WFClient] section of $HOME/.ICAClient/wfclient.ini. This setting maps the local key combination Alt+Ctrl+F1 to Alt+F1:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Change Hotkey1Shift=Ctrl+Shift to Hotkey1Shift=Alt+Ctrl.

- Direct mode on the keyboard sends all key combinations directly to the server. They aren't processed locally. To configure Direct mode, in the [WFClient] section of $HOME/.ICAClient/wfclient.ini, set TransparentKeyPassthrough to Remote.
- Reconfigure the window manager so that it suppresses default keyboard combinations.

Remote Croatian keyboard

This procedure ensures that ASCII characters are correctly sent to remote virtual desktops with Croatian keyboard layouts.

1. In the WFClient section of the appropriate configuration file, set UseEUKSforASCII to True.
2. Set UseEUKS to 2.

Japanese keyboard

To configure the use of a Japanese keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Japanese (JIS)

ABNT2 keyboard

To configure the use of an ABNT2 keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Brazilian (ABNT2)

Local keyboard

If some keys on the local keyboard do not behave as expected, choose the best-matching server layout from the list in $ICAROOT/config/module.ini.

Windows Media Player

Citrix Workspace app might not have `GStreamer` plugins to handle a requested format. This issue normally causes the server to request a different format. Sometimes the initial check for a suitable plug-in incorrectly indicates that one is present. This issue is normally detected and causes an error dialog to appear on the server that indicates the Windows Media Player found a problem while playing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the file. Retrying the file within the session typically works because Citrix Workspace app rejects the format. And as a result, the server either requests another format or provides the media itself.

In a few situations, there's no suitable plug-in is detected and the file isn't played correctly, despite the progress indicator moving as expected in the Windows Media Player.

To avoid this error dialog or failure to play in future sessions:

1. Temporarily add the configuration option "SpeedScreenMMAVerbose=On"to the [WFClient] section of $Home/.ICAClient/wfclient.ini, for example.
2. Restart `wfica` from a self-service that has been started from a terminal.
3. Play a video that generates this error.
4. Note (in the tracing output) the mime type associated with the missing plug-in trace, or the mime type that must be supported but does not play (for example, "video/x-h264..").
5. Edit $ICAROOT/config/MediaStreamingConfig.tbl. On the line with the noted mime type, insert a '?'between the ':'and the mime type. This setting disables the format.
6. Repeat steps 2–5 (preceding) for other media formats that produce this error condition.
7. Distribute this modified MediaStreamingConfig.tbl to other machines with the same set of `GStreamer` plugins.

> **Note:**
>
> Alternately, after identifying the mime type it might be possible to install a `GStreamer` plugin to decode it.

Script to verify system requirements for Windows Media Player redirection With the 2307 release, a new bash script is introduced to verify the configuration required for the Windows Media Player redirection feature in the Citrix Workspace app for Linux. This feature helps to reduce troubleshooting time for the Windows Media Player redirection feature. To verify the configuration, you can use the same rave_troubleshooting.sh available at System diagnostic script for RAVE.

Serial port setting

To configure a single serial port, add the following entries in the $ICAROOT/config/module.ini configuration file:

LastComPortNum=1

ComPort1=device

To configure two or more serial ports, add the following entries in the $ICAROOT/config/module.ini configuration file:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Errors

This topic includes a list of other common error messages that you might see when using Citrix Workspace app.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

When running Citrix Workspace app from the command line, this error usually means the description given on the command line wasn't found in the appsrv.ini file.

E_BAD_OPTION - The option "…"is invalid.

Missing argument for option "…".

E_BAD_ARG - The option "…"has an invalid argument: "…".

Invalid argument specified for option "…".

E_INI_KEY_SYNTAX - The key "…"in the configuration file "…"is invalid.

The X Server vendor information in the configuration file is corrupt. Create a configuration file.

E_INI_VALUE_SYNTAX - The value "…"in the configuration file "…"is invalid.

The X Server vendor information in the configuration file is corrupt. Create a configuration file.

E_SERVER_NAMELOOKUP_FAILURE - Cannot connect to server "…".

The server name can't be resolved.

Cannot write to one or more files: "…". Correct any disk full issues or permissions problems and try again.

Check for disk-full issues, or permissions problems. If a problem is found and corrected, retry the operation that prompted the error message.

Server connection lost. Reconnect and try again. These files might be missing data: "…".

Reconnect and retry the operation that prompted the error.

Diagnostic information

If you are experiencing problems using Citrix Workspace app, you might be asked to provide Technical Support with diagnostic information. This information assists this team in trying to diagnose the problem and offer assistance to rectify it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To obtain diagnostic information about Citrix Workspace app:

1. In the installation directory, type util/lurdump. It's recommended that you do this modification while a session is open and if possible, while the issue is occurring.

   A file is generated that provides detailed diagnostic information, which includes version details, the contents of Citrix Workspace app's configuration files, and the values of various system variables.

2. Check the file for confidential information before sending it to Technical Support.

Troubleshoot connections to resources

Users can manage their active connections using the Connection Center. This feature is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. With Connection Center, users can manage connections by:

- Closing an application.
- Logging off a session. This step ends the session and closes any open applications.
- Disconnecting from a session. This step cuts the selected connection to the server without closing any open applications (unless the server is configured to close applications on disconnection).
- Viewing connection transport statistics.

Log collection

In earlier versions, the `debug.ini` and `module.ini` files were used to configure logging.

As of version 2009, you can configure the log collection using one of the following methods:

- Command-line interface
- GUI

Also as of Version 2009, the `debug.ini` configuration file is removed from the Citrix Workspace app installer package.

Logs capture the Citrix Workspace app deployment details, configuration changes, and administrative activities to a log collection database. A third-party developer can apply this log collection mechanism by using the log collection SDK, which is bundled as part of the Citrix Workspace app Platform Optimization SDK.

You can use the log information to:

- Diagnose and troubleshoot issues that occur after any changes. The log provides a breadcrumb trail.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assist change management and track configurations.
- Report administration activities.

If Citrix Workspace app is installed with root user privileges, the logs are stored in the `/var/log/citrix/ICAClient.log`. Otherwise, the logs are stored in `${ HOME } /.ICAClient/logs/ICAClient.log`.

When Citrix Workspace app is installed, a user called `citrixlog` is created to handle the logging functionality.

Command-line interface

1. At the command prompt, navigate to the `/opt/Citrix/ICAClient/util` path.
2. Run the following command to set the log preferences.

   ```
   ./setlog help
   ```

All the available commands are displayed.

The following table lists various modules and their corresponding trace class values. Use the following table for a specific command-line log value set:

Module	Log class
Assertions	LOG_ASSERT
Audio Monitor	TC_CM
BCR with CEF	TC_CEFBCR
Client Audio Mapping	TC_CAM
Connection Center	TC_CONNCENTER
Client Communication Port	TC_CCM
Client Drive Mapping	TC_CDM
Clip	TC_CLIP
Client Printer Mapping	TC_CPM
Client Printer Mapping	TC_CPM
Font	TC_FONT
Frame	TC_FRAME
Graphics Abstraction	TC_GA
Input Method Editor	TC_IME

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Module	Log class
IPC	TC_IPC
Keyboard Mapping	TC_KEY
Licensing Driver	TC_VDLIC
Multimedia	TC_MMVD‘
Mouse Mapping	TC_MOU
MS Teams	TC_MTOP
Other Libraries	TC_LIB
Protocol Driver	TC_PD
PNA Store	TC_PN
Standard Event Logs	LOG_CLASS
SRCC	TC_SRCC
SSPI Login	TC_CSM
Smart Card	TC_SCARDVD
Selfservice	TC_SS
Selfservice Extension	TC_SSEXT
StorefrontLib	TC_STF
Transport Driver	TC_TD
Thinwire	TC_TW
Transparent Window Interface	TC_TUI
Virtual Channel	TC_VD
PAL	TC_VP
UI	TC_UI
UIDialogLibWebKit3	TC_UIDW3
‘UIDialogLibWebKit3_ext	TC_UIDW3E
USB Daemon	TC_CTXUSB
Video Frame Driver	TC_VFM
Web kit	TC_WEBKIT
WinStation Driver	TC_WD
Wfica	TC_NCS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Module	Log class
`Wfica` Engine	TC_WENG
`Wfica` Shell	TC_WFSHELL
Web helper	TC_WH
Zero Latency	TC_ZLC

GUI

Go to **Menu** > **Preferences**. The **Citrix Workspace-Preferences** dialog appears.

At increasing levels of tracing detail, the following values are available:

- Disabled
- Only Error
- Normal
- Verbose

By default, the **Logging** option is set to **Only Error**.

Due to the large amount of data that can be generated, tracing might significantly impact the performance of Citrix Workspace app. The **Verbose** level is recommended only if necessary for troubleshooting.

Click **Save and Close** after you select the desired log collection level. The changes are applied in the session dynamically.

Click the settings icon next to the **Logging** option drop-down menu. The **Citrix Log Preferences** dialog appears.

> **Note:**
>
> If you delete the `ICAClient.log` file, you must restart the log collection service `ctxcwalogd` .
>
> For example, if you are on a `systemd-capable` setup, run the following command:
>
> `systemctl restart ctxcwalogd`.

Enabling log collection on Version 2006 and earlier:

If you are on Version 2006 and earlier, enable log collection using the following procedure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Download and install Citrix Workspace app on your Linux machine.
2. Set the ICAROOT environment variable to the installation location.

   For example, /opt/Citrix/ICAClient.

   By default, the TC_ALL trace class is enabled to provide all the traces.
3. To collect logs for a particular module, open the debug.ini file at $ICAROOT and add the required trace parameters to the [wfica] section.

   Add the trace classes with a "+"symbol. For example, +TC_LIB.

   You can add different classes separated by the pipe symbol.
   For example, +TC_LIB | +TC_MMVD.

The following table lists the wfica modules and their corresponding trace class values:

Module	TraceClasses value
Graphics	TC_TW
EUEM	TC_EUEM
WFICA (Session Launch)	TC_NCS
Printing	TC_CPM
Connection Sequence - WD	TC_WD
Connection Sequence - PD	TC_PD
Connection Sequence - TD	TC_TD
Proxy related files	TC_PROXY
Multimedia Virtual Driver / Webcam	TC_MMVD
Virtual Drivers	TC_VD
Client Drive Mapping	TC_CDM
Audio	TC_CAM
COM (Communication Port)	TC_CCM
Seamless	TC_TWI
Smart Card	TC_SCARDVD

The following table lists the connection center module and their corresponding trace class value:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Module	TraceClasses value
Connection center	TC_CSM

The following table lists the trace class value for setWebHelper:

TraceClasses value
Set logSwitch to 1 (to enable) or 0 (to disable) Example: logSwitch = 1

Troubleshooting:

If `ctxcwalogd` turns unresponsive, the logs are traced in the syslog.

For information about getting new and refreshed logs in subsequent launches, see Syslog configuration.

Syslog configuration

By default, all syslog logs are saved at `/var/log/syslog`. To configure the path and the name of the log file, edit the following line under the [RULES] section in the `/etc/rsyslog.conf` file. For example,

```
1 user.* -/var/log/logfile_name.log
```

Save your changes and then restart the syslog service using the command:

```
sudo service rsyslog restart
```

Points to remember:

- To verify that a new syslog is available, delete the syslog and run the command: `sudo service rsyslog restart`.
- To avoid duplicate messages, add **$RepeatedMsgReduction on** at the beginning of the `rsyslog.conf` file.
- To receive logs, ensure that the **$ModLoad imuxsock.so** line is uncommented at the beginning of the `rsyslog.conf` file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remote log collection

To enable remote log collection on:

- **Server-side configuration:** uncomment the following lines in the `rsyslog.conf` file of the syslog server:

  ```
  $ModLoad imtcp

  $InputTCPServerRun 10514
  ```

- **Client-side configuration:** add the following line in the `rsyslog.conf` file by replacing the localhost with the IP address of the remote server:

  ```
  *.* @@localhost:10514
  ```

Collecting log files

Previously, there was no tool available to collect the log files in Citrix Workspace app. Log files were present in different folders. You had to manually collect log files from different folders.

Starting with the 2109 version, Citrix Workspace app introduces a collectlog.py tool to collect log files from different folders. You can run the tool using the command-line. The log files are generated as a compressed log file. You can download it from the local server.

Prerequisites

- Python 3
- Requires extra space to save the logs

Starting with Version 2109, two new files are added to collect log files using the collectlog.py tool:

- `logcollector.ini` file –Saves the name and path of the log file.
- `collectlog.py` file –Collects the log files and saves them as `cwalog_{ timestamp } .tar.gz` compressed file.

By default, the `[hdxteams]` component is added in the `logcollector.ini` file to collect log files for Microsoft Teams. However, you can add other components also in the `logcollector.ini` file using the following procedure:

1. Navigate to the `${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini` file.
2. Add the component that you require to collect log files as per the following example:

[component_name]

log_name1 = “log_path1”

© 1997–2026 Citrix Systems, Inc. All rights reserved.

log_name2 = “log_path2”

If you are on Version 2109, collect log files using the following procedure:

1. Download and install Citrix Workspace app on your Linux machine.
2. At the command-line, navigate to the `/opt/Citrix/ICAClient/util` path.
3. Run the following command:
   `./collctlog.py -h`

   The following command usage information appears:

   ```
   usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE]optional arguments
   : -h, --help show this help message and exit -c CONFIG, --config
    CONFIG The logcollector.ini path & file -a ARCHIVE, --archive
   ARCHIVE The archive path & file
   ```

4. Run the following commands as required:

   - `./collectlog.py` –Collects log files using the configuration file from the default path and saves them as a compressed log files at the default path.
   - `./collectlog.py -c /user_specified_path/logcollector.ini` –Collects log files using the configuration file from a user-specified path and saves them as a compressed log files at the default path.
   - `./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_specified_path/` –Collects log files using the configuration file from a user-specified path and saves them as a compressed log files at the user-defined path.

   > **Note:**
   >
   > The default path of the `logcollector.ini` configuration file is `/opt/Citrix/ICAClient/config/logcollector.ini`. The default path of the compressed log file is `/tmp`.

5. Navigate to the `/tmp` folder and collect the `cwalog_{ timestamp } .tar.gz` compressed file.

> **Note:**
>
> The log files are saved in the `/tmp` folder with the file name `cwalog_{ timestamp } .tar.gz`.

Enhancement to log collection

Starting with Citrix Workspace app version 2309, the following enhancements are available:

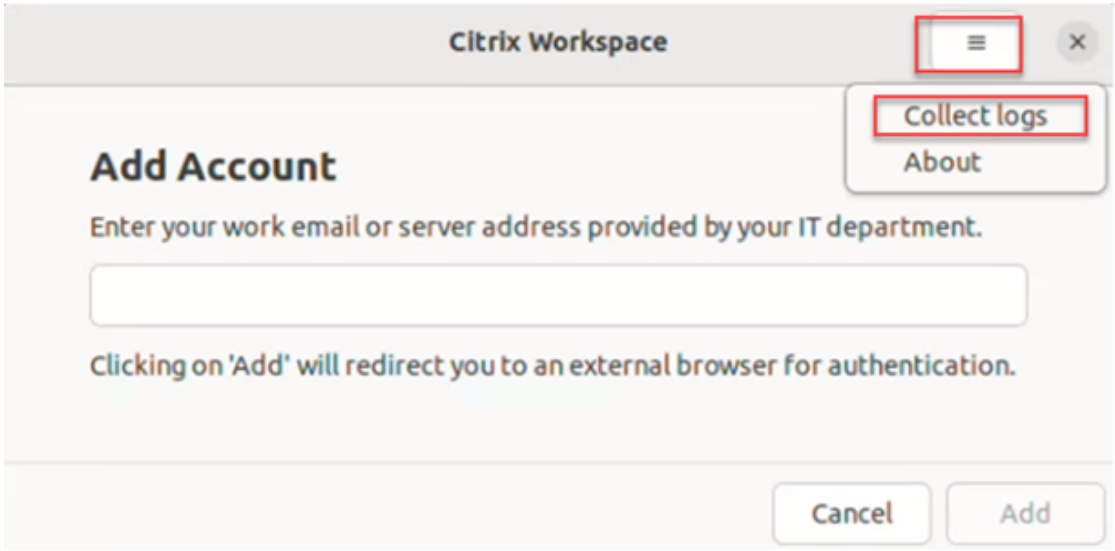
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Log Collection Utility
- Disable DS logs

Citrix Log Collection Utility The Citrix Log Collection Utility helps you collect both new and existing logs. This utility specifically collects verbose logs and saves all logs in a tar.gz file.

You can open the Citrix Log Collection Utility by using any one of the following methods:

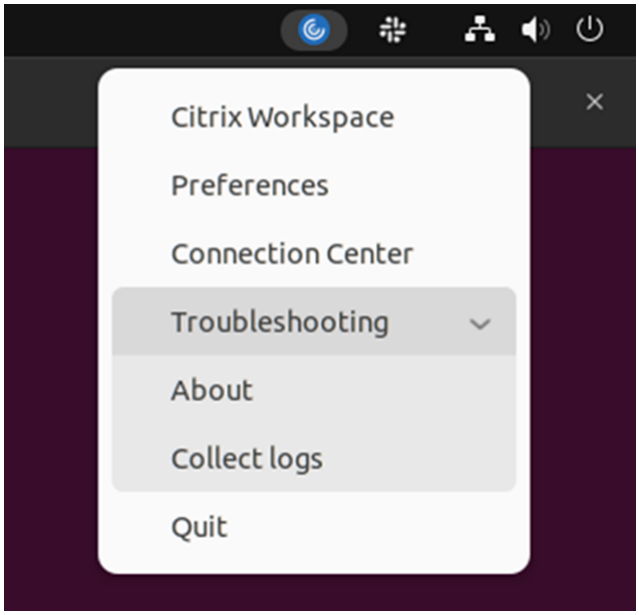
1. Navigate to the **Add Account** screen.
2. Click the hamburger menu.
3. Select **Collect logs**



Or,

Click **Troubleshooting** > **Collect logs** in the **App indicator** icon.

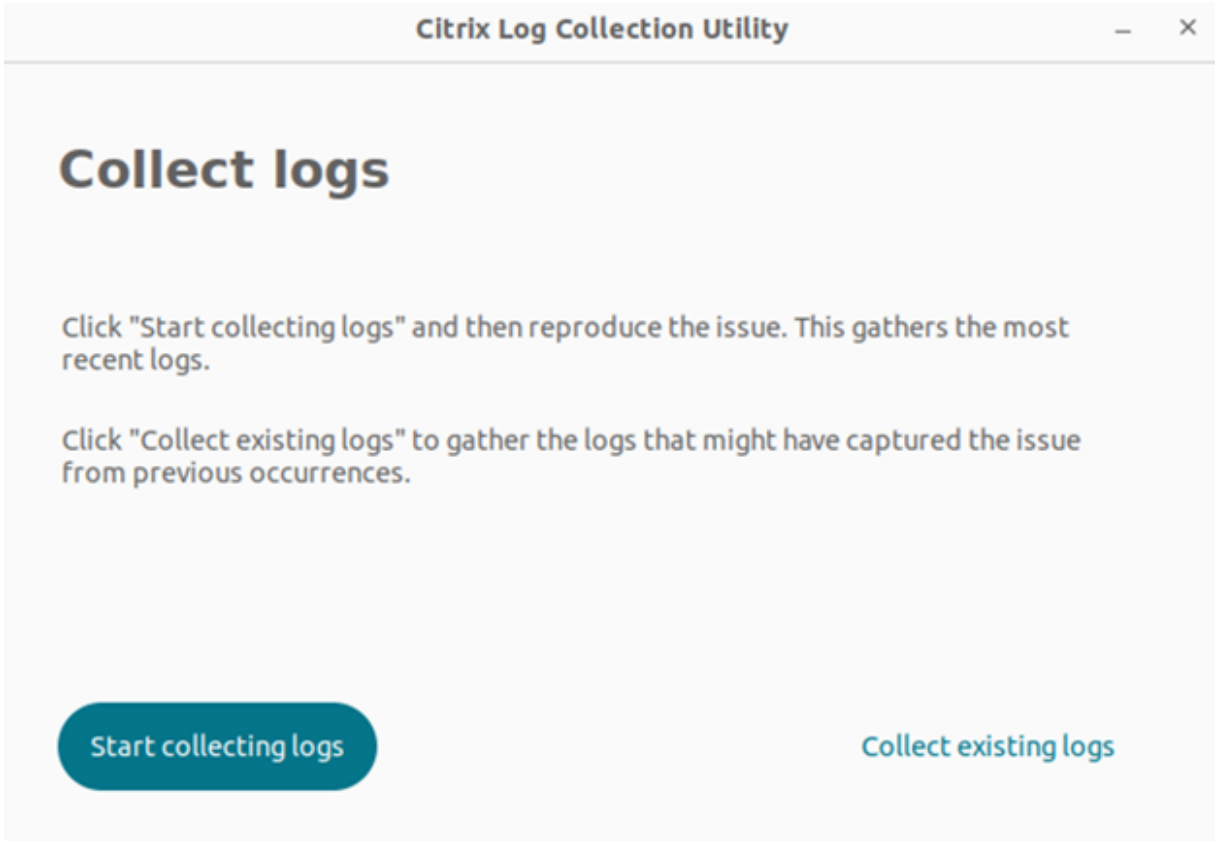
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Or,

1. At the command-line, navigate to the `/opt/Citrix/ICAClient/util` path.
2. Run the following command: ./logmgr

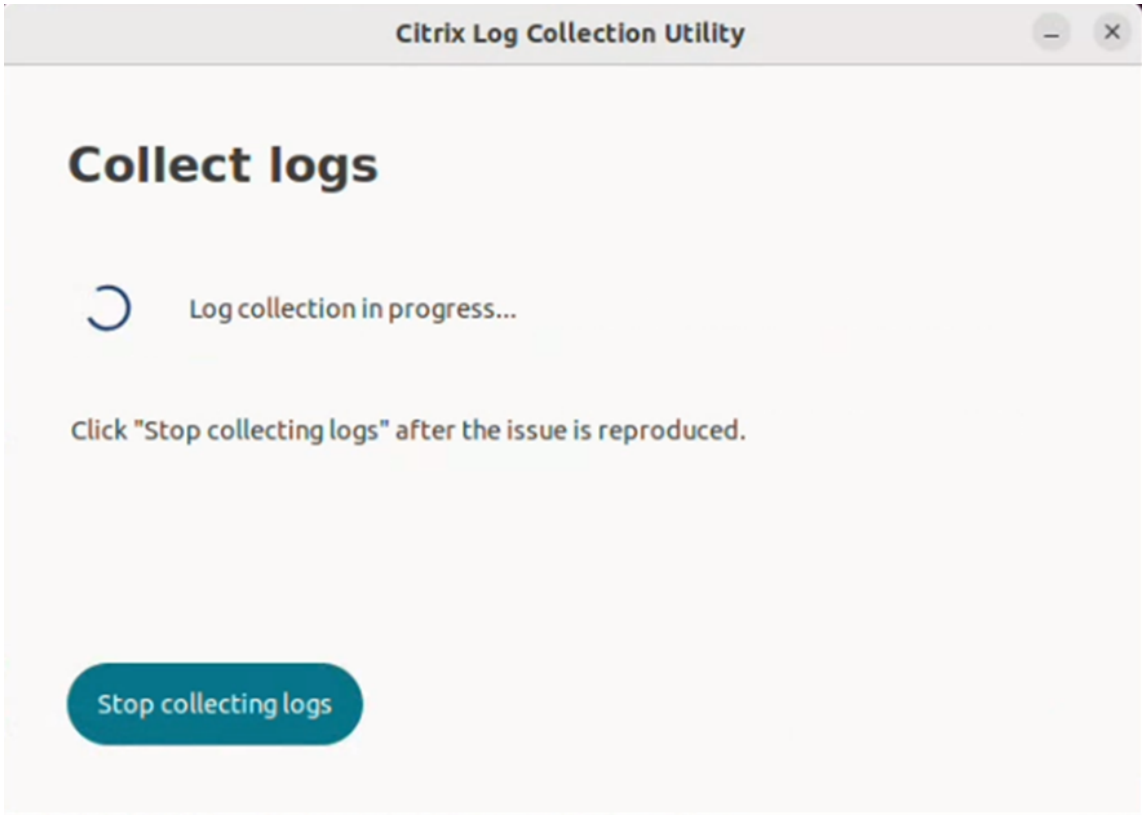
The **Citrix Log Collection utility** screen appears.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

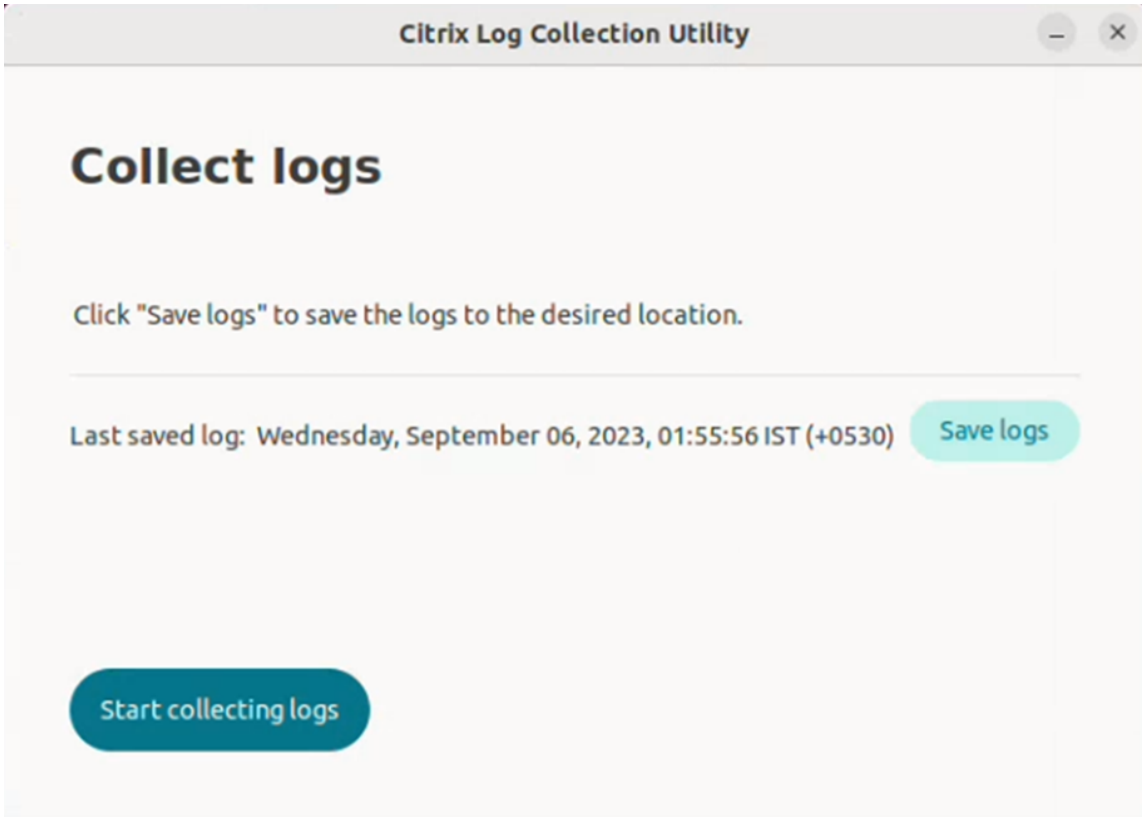
Collect fresh logs

1. Navigate to Citrix Log Collection Utility and click **Start collecting logs**. The following screen appears:

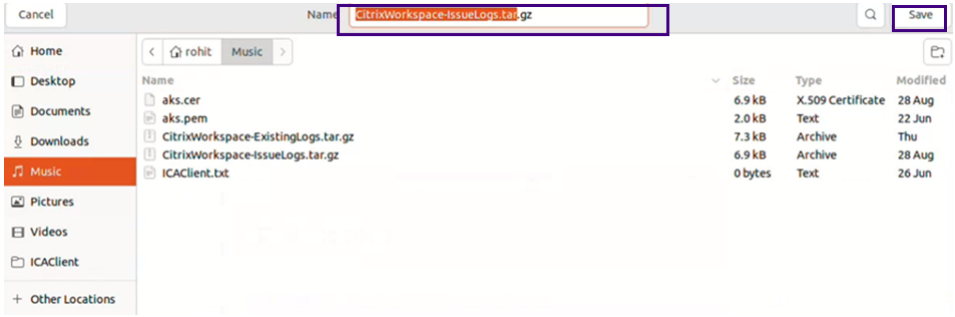


2. Reproduce the issue scenario.
3. Click **Stop collecting logs** after the issue is reproduced. The following screen appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

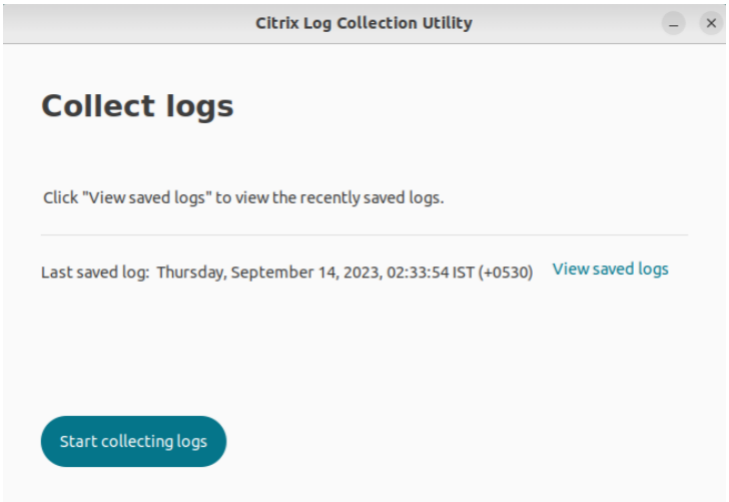


4. Click **Save logs** to save the logs. The file explorer window to save logs is opened.

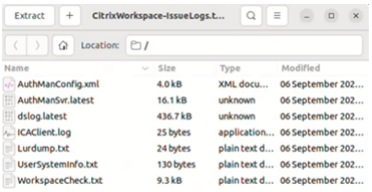


5. Click **Save**. The log file is saved. The following screen appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

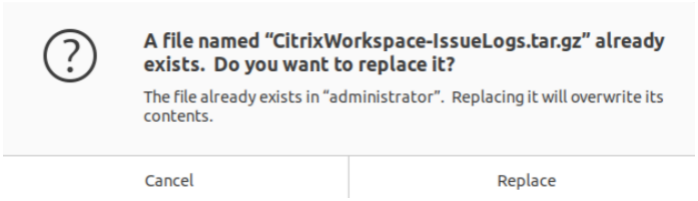


6. Click **View Saved logs** to view the saved logs. The saved log files are displayed in the following screen:



Note:

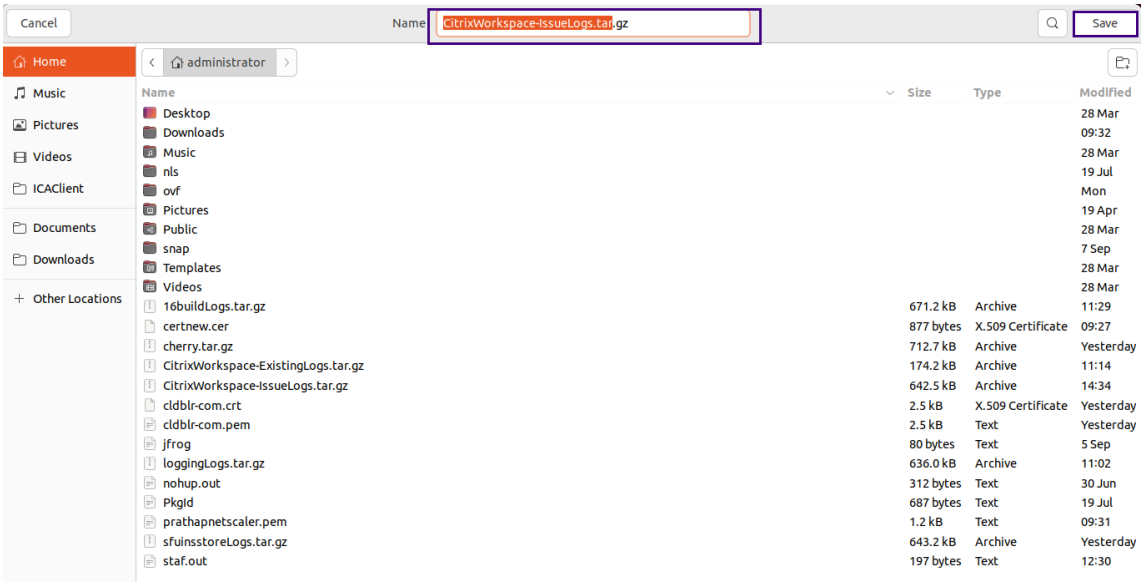
If you click **Start collecting logs** for the second time, you get a warning message to overwrite the existing logs:



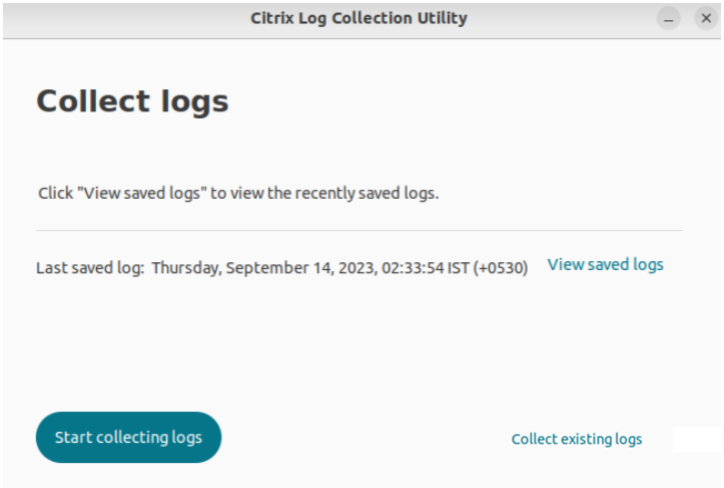
Collect existing logs

1. Open the Citrix Log Collection Utility.
2. Click **Collect existing logs** to collect the logs that might have captured the issue from previous occurrences. The file explorer window is opened to save the existing logs.

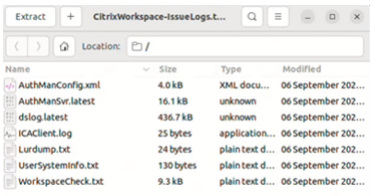
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Save** to save the existing logs to a different folder, from where you can access the log files later. The following screen appears:



4. Click **View saved logs** to view the logs.



Collecting user activity logs Starting with the 2311 version, you can collect the user activity logs. Activities related to most of the `Storebrowse` commands are saved in the log file. You can find the log files within the following location:

```
${ HOME } /.ICAClient/logs/userActivitylog/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the user activity logs are enabled. To disable it, add the following key in the Authmanconfig.xml file:

```
<key>UserActivityLogsDisabled</key>
<value>true</value>
```

Disable collecting DS logs DS logs collects all logs. If you don't require the `dslogs`, you can disable it by adding the following key in the `Authmanconfig.xml` file:

```
<key>DsLogsDisabled</key>
<value>true</value>
```

Enhanced system logs for browser content redirection

Starting with the 2405 version, browser content redirection now allows admins to monitor the feature status as part of the enhancements to the system logs. For more information, see Browser content redirection.

Extended logging support

Starting with version 2601, Citrix Workspace app for Linux adds a configuration option to enable extended logging for easier diagnostics.

To enable extended logging:

1. Edit the `AuthManConfig.xml` file at `/opt/Citrix/ICAClient/config/AuthManConfig.xml`.
2. Set `ExtendedLoggingEnabled` to **`true`**.

Example:

```
<!-- ExtendedLoggingEnabled - true, false (Collects verbose, service
    record, and dslogs) -->
<key>ExtendedLoggingEnabled</key>
<value>false</value>

<!-- To enable extended logging -->
<key>ExtendedLoggingEnabled</key>
<value>true</value>
```

When enabled, extended logs are collected for ServiceRecord and dslogs in Citrix Workspace app for Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deprecation

May 26, 2026

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 announced in	Removed in / To be removed in	Alternative
GCC 8 support	-	2604	-
Citrix Enterprise Browser (CEB)	2601	2604	Chromium, Firefox, and Microsoft Edge.
Legacy Desktop Viewer Toolbar	2508	2601	New Desktop Viewer toolbar.
Raspberry Pi OS Bullseye support	-	2503	Not applicable
XenApp Services (also known as PNAgent)	2405	-	Within Citrix workspace™ app, connect to stores using the store URL rather than the XenApp Services URL.
Fedora Linux	2405	2408	Not applicable
SUSE Linux Enterprise Server	2405	2408	Not applicable
SoftwareMouse	2402	2405	Not applicable
invert-cursor	2402	2405	32-bit cursor and gray cursor
Support for WebRTC SDP format (Plan B)	2309		Upgrade Citrix Workspace app to a supported version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Item	Deprecation announced in	Removed in / To be removed in	Alternative
Support for Single Window mode in Microsoft Teams Optimization	2309		Upgrade Citrix Workspace app to a version that supports MultiWindow mode. For more information, see Feature matrix and version support.
Citrix Workspace app for Linux (x86)	2305	2311	Not applicable
`minica`	2305	2311	Not applicable
ctxh264.so	2303	2408	There will be a new interface for H.264.
Raspberry Pi 3/3B support	2405	2408	Not applicable
GDI	2311	2405	Not applicable
ARMHF	2303	2405	ARM64
GTK2	2209	2405	GTK3
VDSCARD.DLL	2209	2405	VDSCARDV2.DLL
`GStreamer 0.1`	2205	2311	`GStreamer 1.0`
Web Packages	2010	2101	Full Packages
SUSE 11 SP3 Full Package (Self-Service Support) RPM package	1908	1910	Not applicable
`pacexec` binary	1912	1912	Not applicable
pnabrowse	-	2103	`Storebrowse`
Flash Redirection	2006	2006	Use Browser Content Redirection (BCR)

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.