Citrix Workspace app for Linux

Contents

About this release

February 2, 2021

What's new in 2101

Client drive mapping (CDM) enhancement

With this release, access to mapped drives comes with an additional 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 every time a session is launched.

App protection support on Debian package experimental feature

App protection is now 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 no"
sudo debconf-show icaclient
* app_protection/install_app_protection: no
sudo apt install -f ./icaclient_<version>._amd64.deb
```

Microsoft Teams enhancements

- The Citrix Workspace app installer is now packaged with the Microsoft Teams ringtones.
- Support for Dual-Tone Multifrequency (DTMF) signaling interaction with telephony systems (for example, PSTN) and conference calls in Microsoft Teams. This feature is enabled by default.
- Audio output switches automatically to newly plugged-in audio devices, and an appropriate audio volume is set.
- HTTP proxy support for anonymous authentication.

What's new in 2012

Client drive mapping (CDM) enhancement

Previously, your setting for file access through CDM was applied on all configured stores.

Starting with this release, Citrix Workspace app allows you to configure per-store CDM file access.

> **Note:**
>
> The file access setting isnt' persistent across sessions when using workspace for web. It defaults to the **Ask me each time** option.

For more information, see Client-drive mapping.

App protection experimental feature

> **Note:**
>
> - This feature is supported only when Citrix Workspace app is installed by using the tarball package. Also, x64 and armhf are the only two supported packages.
> - This feature is supported only on on-premises deployments of Citrix Virtual Apps and Desktops.

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 by keylogging and screen capturing malware. App protection prevents exfiltration of confidential information such as user credentials and sensitive information displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

For information about how to configure app protection on Citrix Virtual Apps and Desktops, see the App protection section in the Citrix Virtual Apps and Desktops documentation.

For more information about app protection in Citrix Workspace app, see App protection.

Authentication enhancement experimental feature

We now present the authentication dialog inside Citrix Workspace app and show store details on the logon screen for a better user experience. We encrypt and store authentication tokens 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.
> - This authentication enhancement is not available on armhf platform.

Prerequisite:

You must install the libsecret library.

This feature is disabled by default.

For more information, see Authenticate.

Audio configuration enhancement

Starting with this release, the default value of the `VdcamVersion4Support` attribute in the `module.ini` file is set to `True`.

For more information, see Audio.

What's new in 2010

Enhanced audio redirection

Previously, only the default audio device was mapped in a session even when many devices were available on the machine. The mapped device commonly appeared as **Citrix HDX Audio**.

With this release, Citrix Workspace app for Linux displays all local audio devices that are available in a session. Instead of **Citrix HDX Audio**, they now appear with their respective device names. You can switch to any of the available devices dynamically in a session. Unlike in earlier releases, now you don't need to select the default audio device before launching the session. Sessions update dynamically when you plug in or remove audio devices.

For more information, see Audio.

Additionally, this release addresses issues to improve the Multi-Stream ICA feature.

What's new in 2009

Enhancement to logging

Previously, the `debug.ini` and `module.ini` files were used to configure logging.

As of Version 2009, you can configure logging using one of the following methods:

- Command-line interface
- GUI (GUI)

Also as of Version 2009, the `debug.ini` configuration file is removed from the Citrix Workspace app installer.

Logging captures the deployment details, configuration changes, and administrative activities of Citrix Workspace app to a logging database. A third-party developer can use the logging 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.
- Assist change management and track configurations.
- Report administration activities.

> **Note:**
>
> This logging mechanism is applicable only on Retail build.

For more information about logging, see Logging.

What's new in 2006

Optimization for Microsoft Teams

Optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops 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.

Citrix Workspace app for Linux supports audio, video, and screen sharing features with Microsoft Teams optimization.

> **Note:**
>
> Microsoft Teams optimization is supported only on x64 Linux distributions.

For information on how to enable logging, follow the steps mentioned under Logging for Microsoft Teams.

For information on system requirements, see Microsoft Teams Optimization.

For more information, see Optimization for Microsoft Teams and Microsoft Teams redirection.

Support for NetScaler App Experience(NSAP) virtual channel

Previously available as an experimental feature, the NetScaler App Experience (NSAP) virtual channel feature is now fully functional. The NSAP virtual channel helps in sourcing HDX Insight data, which improves scalability and performance. The NSAP virtual channel is enabled by default. To disable it, toggle the NSAP 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.

Update to Citrix Analytics Service

Citrix Workspace app is instrumented to transmit data to 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 for Performance and Self-service search for Virtual Apps and Desktops.

TLS version update

Previously, the minimum TLS version supported was 1.0, and the maximum TLS version supported was 1.2.

Starting with this release, the minimum and maximum TLS version supported is 1.2. To configure a different value for `MinimumTLS`, see TLS.

CryptoKit update

CryptoKit Version 14.2 is integrated with the OpenSSL 1.1.1d version.

What's new in 2004

Language support

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

Improved logon and enumeration performance

With this release, cloud user accounts notice shorter logon and app enumeration time.

Audio optimization for Microsoft Teams experimental feature

As an experimental feature, Citrix Workspace app provides audio optimization for Microsoft Teams running within a Citrix Virtual Desktop session.

> **Note:**
>
> Microsoft Teams audio optimization is supported only on the x64 Linux distributions.

For more information, see the Optimization for Microsoft Teams and Microsoft Teams redirection sections in the Citrix Virtual Apps and Desktops documentation.

Support for NetScaler App Experience (NSAP) virtual channel experimental feature

As an experimental feature, HDX Insight data is sourced from the NSAP virtual channel and sent uncompressed, which improves scalability and performance. The NSAP virtual channel is enabled by default. To disable it, toggle the NSAP 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.

What's new in 1912

Transparent user interface enhancement

Version 1910 introduced the transparent user interface (TUI) feature, including the **VDTUI** flag. The feature helps the client system to receive the TUI packets sent by the server, and the client can access the UI-related components. However, with the flag set to **Off**, the "Starting <Application>" dialog rendered on top of other application windows, covering the login prompt.

Now, the **VDTUI** flag, located in the `module.ini` file, 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 progress of the app launch.

GStreamer 1.x support **experimental feature**

In earlier releases, GStreamer 0.10 was the default version supported for multimedia redirection. Starting with this release, you can configure GStreamer 1.x as the default version.

Limitations:

- When you play a video, the forward and the backward option might not work as expected.
- When you launch the Citrix Workspace app on ARMHF devices, GStreamer 1.x might not work as expected.

For more information, see Enabling GStreamer 1.x.

Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR) **experimental feature**

The BCR feature redirects contents of a web browser to a client device. The feature creates a corresponding browser that embeds within the Citrix Workspace app.

Previously, BCR used a `WebkitGTK+` based overlay to render the content. Starting with this release, BCR uses a CEF-based overlay for better user experience. It helps offload network usage, page processing, and graphics rendering to the endpoint.

For more information, see Enabling CEF-based BCR.

For information about BCR, see Browser content redirection in the Citrix Virtual Apps and Desktops documentation.

> **Notes:**
>
> - The **pacexec** binary is removed from the x86 version of Citrix Workspace app.
> - Citrix Files might not be compatible with the Workspace with Intelligence feature.

What's new in 1910

Language support

Citrix Workspace app for Linux is now available in the Brazilian Portuguese language.

App indicator icon

The app indicator starts when you launch Citrix Workspace app. It is 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.

Transparent user interface

The Citrix ICA protocol uses Transparent User Interface Virtual Channel [TUI VC] protocol to transmits data between Citrix Virtual Apps and Desktop and host servers. The TUI protocol transmits user interface [UI] component messages for remote connections.

Previously, Citrix Workspace app for Linux did not support the TUI VC feature. As a result, the client system could not handle UI component data from the server efficiently. So, when attempted to launch an app, the "Starting <Application>" dialog rendered on top of other applications.

Now, 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`

For more information on Virtual Channels, see Citrix ICA virtual channels in Citrix Virtual Apps and Desktops documentation.

What's new in 1908

This release addresses a number of issues that help to improve overall performance and stability. Also, the Platform Optimization SDK includes UI Dialog libraries using libwebkit2gtk (2.16.6). The newly added libraries are UIDialogLibWebKit3.so and UIDialogLibWebKit3_ext.so. For instructions on getting started with the UI Dialog library, see the Readme in the UIDialogLib3 directory.

What's new in 1906

Improved UI experience with latest webkit support

In earlier releases, the self-service UI required `libwebkitgtk` Version 1.0. Due to Version 1.0 deprecation, most Linux distributions no longer support it. Going forward, Citrix Workspace app for Linux requires libwebkit2gtk (2.16.6+).

libwebkit2gtk has the following advantages:

- 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 it takes to sign in.
- The app works better with newer Linux distributions and provides with the latest webkit security fixes.

> **Note:**
>
> webkit2gtk is not available on some Linux distributions. As a workaround, consider the following options:
>
> - Build webkit2gtk from the source before installing Citrix Workspace app 1906.
> - Download the web package from the Downloads page. Only web launches are supported in this package.
> - Move to a later Linux distribution that supports webkit2gtk 2.16.6 or later.

Language support

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

VDA keyboard layout

The VDA keyboard layout feature lets 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 feature, modify the `KeyboardLayout=(Server Default)` section of the `wfclient.ini` file and relaunch the session.

Secure SaaS with Citrix Embedded Browser experimental feature

Secure access to SaaS applications provides a unified user experience that delivers published SaaS applications to the users. SaaS apps are available with single sign-on. Administrators can now protect the organization's network and end-user devices from malware and data leaks by filtering access to specific websites and website categories.

Citrix Workspace app for Linux support the use of SaaS apps using the Access Control Service. The service enables administrators to provide a cohesive experience, integrating single sign-on, and content inspection.

Prerequisite:

Ensure that `libgtkglext1` package is available.

Delivering SaaS apps from the cloud has the following benefits:

- Simple configuration – Easy to operate, update, and consume.
- Single sign-on – Hassle-free log on with single sign-on.
- Standard template for different apps – Template-based configuration of popular apps.

> **Note:**
>
> SaaS with Citrix Browser Engine is supported only on x64 and x86 platforms and not on ArmHardFloatPort (armhf) hardware.

For information on how to configure SaaS apps using Access Control Services, see the Access Control documentation.

For more information about SaaS apps with Citrix Workspace app, see Workspace configuration in Citrix Workspace app for Windows documentation.

What's new in 1903

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. These cipher suites were deprecated in Citrix Receiver version 13.10 with an option for backward compatibility.

In this release, the TLS_RSA_ cipher suites have been removed entirely. Instead, this release supports the advanced TLS_ECDHE_RSA_ cipher suites. If your environment is not configured with the TLS_ECDHE_RSA_ cipher suites, client launches are not supported due to weak ciphers. This release supports 1536-bit RSA keys for client authentication.

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)

For more information see, cipher suites.

> **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

Bloomberg audio redirection

This feature allows the use of Bloomberg v4 audio interfaces across multiple sessions. The audio from the sessions now goes through the optimized channel to the Bloomberg interface. The fingerprint interface is redirected to a single session as before.

> **Note:**
>
> By default, this feature is disabled for the x86, x64, and for ARMHF platforms.

For more information on how to configure Bloomberg audio redirection, follow the steps mentioned under selective redirection.

Sign-on page

This release introduces a new sign-on page in the self-service user interface.

Disconnect time

This release addresses issues that help to significantly improve the disconnect time.

What's new in 1901

Support for Citrix Analytics

Citrix Workspace app for Linux is instrumented to securely transmit logs to Citrix Analytics when certain events are triggered by the app. The logs are analyzed and stored on Citrix Analytics servers when enabled. For more information about Citrix Analytics, see Citrix Analytics.

Workspace launcher with Citrix Gateway

Citrix introduced the Workspace launcher (WebHelper) in version 1809. In version 1901, Citrix Workspace launcher works 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.

Logging enhancements II

Logging enhancements II is an extension of the Logging enhancements and better logging features. The feature introduces support for logging for many modules and simplifies the process of collecting logs. It helps users troubleshoot, and, in cases of complicated issues, facilitates support by providing detailed logs.

For information about enabling logging, see Logging.

Keyboard layout synchronization between client and VDA

Previously, the keyboard layouts on the Windows or Linux VDA and on the client device were synchronized manually. For example, when the keyboard layout changed from English to French on the client device but not on the VDA, key mapping issues can occur and persist until the keyboard layout on the VDA was changed to French too.

Starting with this release, Citrix is addressing the issue by automatically synchronizing the keyboard layout of the VDA with that of the client device. Anytime the keyboard layout on the client device changes, the layout on the VDA follows automatically.

> **Note:**
>
> This feature requires version 7.16 or later of the VDA.

For more information, see Keyboard layout synchronization.

What's new in 1810

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

What's new in 1809

Connecting this version of Citrix Workspace app for Linux to Citrix Workspace services is an experimental feature.

Introducing workspace launcher

Previously, the browser plug-in provided along with Citrix Workspace app for Linux enabled users to launch published desktops and applications. This plug-in was based on the Netscape Plugin Application Programming Interface (NPAPI).

Mozilla Corporation has announced that NPAPI support is deprecated as of version 52 of the Firefox browser. Other browsers, too, have deprecated support for NPAPI.

As a solution, Citrix is introducing Workspace launcher (WebHelper). To enable this feature, configure StoreFront to send requests to Workspace launcher to detect the Citrix Workspace app installation.

For information about configuring StoreFront, see **Solution – 2** > **a) Administrator configuration** in Knowledge Center article CTX237727.

> **Note:**
>
> Citrix Workspace launcher currently works only with direct connections to StoreFront. It is not supported in other cases such as connections through Citrix Gateway.

Disabling new workspace web UI mode

When you launch the Citrix Workspace app for Linux using self-service executable file from third-party thin-client vendors, the application can become unresponsive due to 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.

What's new in 1808

Citrix Workspace app

Citrix Receiver is now Citrix Workspace app.
Citrix Workspace app extends the user experience you have enjoyed with Citrix Receiver, making it easier for you to stay productive. Citrix Workspace app incorporates the full capabilities of Citrix Receiver and lays the groundwork for new capabilities for future Citrix Virtual Apps and Desktops releases and the comprehensive Citrix Workspace.

Citrix Workspace app has simplified versioning based on the YYMM format, which makes this release of Citrix Workspace app 1808. The previous release had file version number 13.10.0.20.

Existing users or endpoints of Citrix Receiver for Linux can seamlessly transition to this new version of Citrix Workspace app for Linux by doing an in-place upgrade.

Upgrading to Citrix Workspace app:

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

Citrix Workspace app has a new icon set in a blue theme. It replaces the earlier Citrix Receiver icon that had a black theme.

The **Citrix Workspace** screen overlay appears on the first launch of the app or when you upgrade and when you uninstall and reinstall the app, to inform you about the transition. You can either click **Got it** to continue using the Workspace app, or click **Learn more** for more details.

Connecting this version of Citrix Workspace app for Linux to Citrix Workspace services is an experimental feature.

Bloomberg v4 keyboard selective redirection support

This feature allows the use of the Bloomberg v4 keyboard 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.

> **Note:**
>
> By default, this feature is enabled for x86 and x64 architectures and is disabled for ARMHF architecture.

For more details, see selective redirection.

Fixed issues

Fixed issues in 2101

- When using a custom proxy, an extra authentication prompt might appear. The issue is caused by the Chromium Embedded Framework (CEF) used by browser content redirection. As a workaround, configure your agent to bypass the extra prompt. [CVADHELP-14804]
- When you attempt to reconnect to a session, the session might become unresponsive. The issue occurs with sessions that are smart card enabled. As a workaround, reinsert the smart card. [CVADHELP-15028]
- With Microsoft Teams in **Optimized** mode, video playback might become unresponsive during conference calls. The issue occurs when a participant switches between a built-in and a USB camera. [CVADHELP-16400]
- With Microsoft Teams in **Optimized** mode, the `HdxRtcEngine.exe` process might exit unexpectedly. [CVADHELP-16504]

Fixed issues in earlier releases

Fixed issues in 2012

- When you attempt to launch a webpage redirected using browser content redirection, the webpage might become unresponsive. The issue occurs when you click a link that opens in a new window or new tab. [RFLNX-5306]

- While using CEF-based BCR, microphones and cameras are not redirected. To enable redirection, set the `CefEnableMediaDevices` attribute to `True` in the `All_Regions.ini`.[RFLNX-5337]
- When you press ALT+Ctrl keys, the keys might remain stuck. The issue occurs when the Keyboard Layout option is set to Server Default. [RFLNX-5444]
- Attempts to select the USB options, Picture Transfer Protocol (PTP) and Media Transfer Protocol (MTP) on an Android phone might fail. To fix this issue with the Windows and Linux VDAs, add the following allow rule in the usb.conf file:

  ALLOW: VID = (vid of the device) disableselectconfig=1

  [CVADHELP-15304]
- Citrix Director might incorrectly report the version number of Citrix Workspace app as 2009 instead of 2010. [RFLNX-5743]
- You can launch Citrix Workspace app for Linux successfully at your first attempt, but later attempts might fail. [RFLNX-5971]
- When you attempt to add an unauthenticated (anonymous) store, two error messages might appear. The issue occurs with Citrix Workspace app 2010 for Linux. [RFLNX-5980]

Fixed issues in 2010

- When you are running a video call or sharing the screen in Microsoft Teams, the screen might flicker. [RFLNX-4778]
- Attempts to customize the webrpc.log and webrtc.log files fail. [RFLNX-5221]
- Resources are enumerated for the store even after deleting the store using the storebrowse utility. [RFLNX-5499]
- When German or French locale is installed on the machine, the Microsoft Teams Optimization might not work. [RFLNX-5599]
- When you launch a session from Citrix Workspace app for Linux, the session might flicker. The issue occurs because the session disconnects and reconnects. The issue occurs mainly with Microsoft applications. [CVADHELP-14194]
- When you perform clipboard operations such as copying and pasting content between different sessions, the operations might fail intermittently. [CVADHELP-15228]
- When you start a slideshow presentation with Microsoft PowerPoint launched through Citrix Workspace app for Linux version 1906 or later, the presentation might not open in full-screen mode. [CVADHELP-15648]
- Citrix Workspace app for Linux might not display an authentication dialog for stores that use HTML5 local storage. The issue occurs when you use the self-service user interface. [CVADHELP-15720]

Fixed issues in 2009

- Occasionally, the Meeting view doesn't restore during multitasking in Microsoft Teams. The issue occurs when a local window overlays the remote window. As a result, the remote window does not receive the mouse events. As a workaround, on the minimized screen, hover over the digital clock and double-click on the caller's name. [RFLNX-4937]
- In a session running on UDP connections, the performance might be slow. [RFLNX-5135]
- When you drag the window of a seamless third-party published application across your screen, the window might automatically minimize. [CVADHELP-13677]
- A single USB device redirected to a session running on a device might be unexpectedly redirected to an incoming session running on the same device. [CVADHELP-13684]
- In a multi-monitor environment, when you attempt to relaunch a full-screen session on a monitor, the connection bar stays on a different monitor. The issue occurs even when the mouse cursor remains on the same monitor. [CVADHELP-14642]
- When you attempt to reconnect to a session, the session might disconnect immediately after the desktop appears. The issue occurs with sessions that require smart card authentication. [CVADHELP-15036]

Fixed issues in 2006

- Session launch might fail on Red Hat 8.2, CentOS 8.x, Fedora 29, 30, and 31 distributions. [RFLNX-3114] [RFLNX-4438] [RFLNX-4296]
- With the `wfica_for_plugins` binaries added back to the Platform Optimization SDK, an unnecessary dependency that was introduced on LIBS_GTK is now removed. [RFLNX-4604]
- Server fetch and client render for CEF-based BCR fails. As a result, browser content redirection fails. [RFLNX-4459]
- After you click a published application in Citrix StoreFront, a connection dialog appears and remains there. The issue occurs in non-seamless mode. [CVADHELP-13896]
- After you select the **Activate** option to activate Citrix Workspace app on your desktop, the **receiverconfig.cr** file is downloaded. Attempts to add the store to Citrix Workspace app by launching that file might fail. [CVADHELP-14389]
- Attempts to map Citrix Workspace app for Linux to a COM serial port might fail, indicating that the port cannot be reached. The issue occurs when the previous COM entries are not populated [CVADHELP-14391]
- Citrix Workspace app for Linux might fail to identify certain smart cards. As a result, attempts to launch a session with those cards fail. [CVADHELP-14878]

Fixed issues in 2004

- If you remove the **Preferences** section from the **All_Regions.ini** file, the wfica process fails. As a result, sessions fail to connect. [RFLNX-3965]

- The **Preferences** > **Accounts** submenu does not appear on the self-service window after you add a cloud store for the first time. [RFLNX-3605]
- The Linux Platform Optimization SDK does not work for Citrix Workspace app Versions 1908, 1910, and 1912. The issue occurs when the `wfica_for_plugins` binaries are removed from the Citrix Workspace app installer package. [RFLNX-4298]
- When you add a store using the **storebrowse** command, the store does not appear on the **Preferences** > **Accounts** tab. The issue occurs when the self-service user interface is running on the back end. [RFLNX-3683]
- In a session, wfica can exit unexpectedly on a website with Browser Content Redirection (BCR) enabled. The issue occurs if you set the value of **AllowMultiStream** to **True**. [CVADHELP-13168]
- In a dual-monitor setup, attempts to change the display of the published desktop to full-screen mode might fail when the monitors have different resolutions. [CVADHELP-13990]
- You might experience display issues in seamless sessions. The issue occurs when you resize a seamless window or switch between seamless windows. [CVADHELP-13458]
- After you launch a desktop session from a PNA store, the progress bar window might remain there unless you close it manually. [CVADHELP-14405]

Fixed issues in 1912

- On Ubuntu16.04x64, the Citrix Workspace app icon might appear incorrectly on the taskbar. [RFLNX-3582]
- After you change the symbolic link [symlink] of gst-play with gst-play1.0, .mp4 video files might render with a black screen in the background and without audio. [RFLNX-2429]
- When you switch from screensaver mode to fullscreen ICA session mode, the keyboard might lose focus. The issue occurs on ArmHardFloat (armhf) devices that run on the Raspberry Pi OS. [RFLNX-3553]
- When you use the self-service user interface, the **Preferences** window options might not work as expected. The issue occurs when the libwebkit1 package is unavailable as is the case with Debian 10 buster clients. [RFLNX-3596]
- When any other system user (not the first user) attempts to launch Citrix Workspace app, the self-service user interface might fail to open, and the following error message appears:

  “Bind Error - address already in use.”

  [RFLNX-3601]
- On Ubuntu 18.04 and later, when you use the self-service user interface to launch applications, the launched application is named “wfica_seamless” - and not after the application. The issue occurs because the default desktop environment is GNOME. [RFLNX-3650]

- When you sign out and then back in with a different user account, the Home > Favorites page displays an incorrect list of Favorite Apps. [RFLNX-3458]
- After you close the self-service user interface, the following error message appears:

  "free(): double free detected in tcache 2 Aborted."

  The issue occurs with ArmHardFloat (armhf) devices that run on the Raspbian Buster OS. [RFLNX-3578]
- With the Unified Experience policy disabled, disabled applications might still enumerate in Citrix Workspace app for Linux. [CVADHELP-13742]
- A removable USB drive cannot be mapped to a VDA on the CentOS 7.7 client. [CVADHELP-13422]

Fixed issues in 1910

- Citrix Workspace app for Linux depended on libcurl3 for installation. With this fix, the dependency has been removed for easier installation. [RFLNX-3487]
- Rendering H.264 encoded data with Video Decode and the Presentation API for Unix (VDPAU) Optimization Pack might not work as expected. [RFLNX-2892]
- When using Citrix Workspace app for Linux versions 1906 or 1908, the sign-in page might not appear when shared users sign out of their workspace. Instead, the following sign-in prompt appears: Sign in to access your Workspace. [RFLNX-3519]
- When a desktop session spans multiple monitors, the toolbar might disappear. [RFLNX-3248]

Fixed issues in 1908

- In a multi-monitor setup, you cannot save the multi-monitor layout if you set another monitor as the primary monitor. [RFLNX-2918]
- When you switch between **Window** and **Full-screen** modes, special keys on the English keyboard might not map to the VDA. [RFLNX-2796]
- USB mass storage devices might disconnect from user sessions when you copy files to the USB devices. The issue occurs when you use Citrix Workspace app for Linux with generic USB redirection and the size of the files is greater than 1 GB. [LC9699]
- With the Browser Content Redirection policy enabled, pages might return a 413 error message when you play a video on YouTube. The issue occurs after you access multiple video links. [LD1761]
- When you set the Use Video Codec for Compression policy to For the entire screen for VDA version 1903, the VDA session might disconnect. [LD1842]
- In browser content redirection, certain websites (for example, SAP Fiori Launchpad) might fail to load contents properly and errors might occur when you log on to the server on the Linux client devices. [LD1843]
- USB redirection might fail when there is USB traffic on endpoints. [LD1636]

Fixed issues in 1906

- This fix addresses double authentication prompts when the internal beacons are not configured properly. [RFLNX-2573]
- When using storebrowse in a Citrix Workspace app, the app enumeration fails. [RFLNX-2712]
- Applications using the webcam inside a session becomes unresponsive if the webcam is also in use by the native application running on the endpoint. [RFLNX-2870]
- When you move any office 365 apps from **Windowed mode** to **Full screen mode**, the app turns unresponsive. [RFLNX–2904]
- When using Citrix Workspace app for Linux, you might be asked to authenticate twice. The issue occurs when you connect using Citrix Gateway. [LD1440]
- Incorrect DNS polling for CAS data collection might occur for a direct ICA launch and for CAS disabled stores. [LD1418]
- The clipboard redirection might not work correctly when you attempt to copy and paste text from a published to a local application. [LD0809]
- Citrix Workspace app for Linux might not show all the resources in the **Favorites** tab even after you refresh the app enumeration. [LD1261]
- When you attempt to reset the password in Citrix Receiver for Linux or Citrix Workspace app for Linux, the password reset option might not appear. An incorrect error message appears. [LD0613]
- Session reliability might not work with NetScaler High Availability failover for on-prem stores. [LD1213]
- When you attempt to reconnect to a seamless application session on an Ubuntu client, an extra gray window might appear. [LD1578]
- A protocol error might occur when attempting to communicate with the Authentication Service while adding the gateway address from an external network. [LD0258]
- Attempts to use the **storebrowse –K** command in Citrix Receiver for Linux or Citrix Workspace app for Linux might fail. [LD1705]
- When using client drive mapping, you cannot delete the folders on the USB flash drive. [LD1778]
- Session Reliability might fail on the Cloud Connector due to a SIGPIPE error. This error terminates the wfica process and disconnects the session. [LD1824]
- The list of recently launched SaaS and Web apps might not appear under the **Recent** tab. [RFLNX-3200]
- On a HTTP-configured StoreFront set up, the Storebrowse utility might exit unexpectedly when communicating with Citrix Gateway. [RFLNX-3144]

- The Citrix Workspace app becomes unresponsive after you right-click and select **Quit** on the system tray window. [RFLNX-2898]
- When you expand the Chrome embedded PowerPoint application to full screen mode from **Windowed mode**, the screen might freeze. This issue occurs when the vertical scaling is incorrect. [RFLNX-2904]
- The authentication dialog box appears repeatedly after you click **Cancel** on the **Log On** page. This issue occurs when you launch self-service, add an account, log on, and then log off from the account. [RFLNX-3111]
- When using more than one smart card certificate (for example, Logon, Signature, Encipherment and so on), the logon certificate fails to appear. [RFLNX-2917]
- When using storebrowse with PNA url and an expired password, the **Change Expired Password** screen does not appear. [LC9129]
- When using Fedora 29 and later, the Citrix Workspace app for Linux exits unexpectedly with an error message "SIGSEGV". This issue occurs because Fedora Version 29 and later are not currently supported due to incompatibility in the `libidn` package provided by the operating system. [LD0705]
- The Citrix Optimization SDK package contains in incorrect version of the UIDialogLibWebKit.so. As a workaround, do the follow the steps:

  1. Download Citrix Optimization SDK package version 18.10 from the Downloads page.
  2. Go to the path CitrixPluginSDK/UIDialogLib/GTK:

     ```
     cd CitrixPluginSDK/UIDialogLib/GTK
     ```

  3. Delete all the object files:

     ```
     rm -rf *.o
     ```

  4. Go to WebKit folder:

     ```
     cd ../WebKit
     ```

  5. Remove the existing UIDialogLibWebKit.so:

     ```
     rm -rf UIDialogLibWebKit.so
     ```

  6. Use the following command in the WebKit directory:

     ```
     make all
     ```

     The new UIDialogLibWebKit.so is generated.

  7. Copy the new library into the **$ICAROOT/lib** directory.

> **Note:**
>
> Before launching the self-service, kill the AuthManagerDaemon and ServiceRecord processes. [RFLNX-2822]

Fixed issues in 1903

- When a Microsoft Office 365 PowerPoint presentation running in a seamless published Chrome browser completes, the display might not refresh. There can be a duplication of elements on the screen and mouse clicks do not work as expected. [LD0777]
- Several unwanted windows that do not correspond to any process or application might appear on the taskbar. [LD1176]
- Citrix Workspace app for Linux might fail with connection error 0.0.0.2. [LD1122]

  For more information, see Cryptographic update.

Fixed issues in 1901

- USB devices that are attached to an endpoint and mapped into a VDA session can fail to redirect into the session. The issue occurs if you rename a USB device within the session and then detach and reattach it. [LD0111]
- Certain third-party applications might not function correctly when you launch them from Citrix Workspace app for Linux. The issue occurs when the applications do not pass the checks for the main application window, and then taskbar icons are not created for those applications. [LD0545]
- Client-to-server File Type Association (FTA) works only once per user and login. To open a local file with the associated published application, see Associating a published application with file types and File Type Association. [RFLNX-1363]

Fixed issues in 1810

- For certain time zones, an incorrect time for calendar appointments might be shown when using Versions 1808 or 1809 of Citrix Workspace app for Linux. [LD0467]
- Attempts to send data from Citrix Receiver for Linux over a custom virtual channel might fail. [RFLNX-2288]

Fixed issues in 1809

- When you attempt to start published applications, the wfica.exe process might exit unexpectedly. The issue occurs when multiple users share the Linux host where Citrix Receiver for Linux 13.10 is installed. [LD0176]

Fixed issues in 1808

- When full-screen H264 encoding is enabled, the text carets on some applications such as the command prompt and text editors disappear. To mitigate this issue (until it is resolved in the Citrix Workspace app), small frames support - a feature of HDX "DeepCompressionV2" codec - is disabled on the VDA. [RFLNX-2172]
- The **udtMSS** flag is enabled by default in the All_Regions.ini file to allow the Citrix Workspace app to honor the value set in StoreFront's default.ica file. [RFLNX-2228]
- The authentication dialog box is hidden behind the full-screen session window when you click anywhere within the session without entering your credentials.
- The Desktop Viewer that disappeared randomly on certain monitors appears fine now.
- When you save a session on specific monitors, upon relaunch, the session spreads across all monitors.
- When you purge user subscription details, the session fails to launch successfully.
- When you click **Save Layout**, the session becomes unresponsive. This issue occurs when you launch multiple sessions from different instances of StoreFront that are configured with or without Save Layout support.

Known issues

Known issues in 2101

- When playing lengthy videos, the audio stops but the video continues to play seamlessly. The issue occurs when you set the `VdcamVersion4Support` to `True`. As a workaround, disable the multi-audio option by setting `VdcamVersion4Support` to `False`. [RFLNX-6472]
- During a Microsoft Teams meeting, audio might be choppy when on mute. The issue occurs on thin-clients. [RFLNX-6537]
- Sometimes, Citrix Workspace app might not be able to render the incoming videos in Microsoft Teams. [RFLNX-6662]
- When you use the `cefenablemediadevices` flag with Microsoft Teams, the microphone does not work as intended. The issue occurs when using CEF-based BCR feature with Microsoft Teams. [RFLNX-6689]

Known issues in earlier releases

Known issues in 2012

- When a session gets terminated or disconnected abruptly, the `HdxRtcEngine.exe` process might exit unexpectedly. [RFLNX-5885]

- 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. For a workaround, see the Knowledge Centre article CTX272423 and CTX131504. [CVADHELP-16170]
- When you establish HDX Optimization for a Microsoft Teams video call, the video might become unresponsive and the audio stops playing. The issue occurs when you disconnect or reconnect a headset during the call. [CVADHELP-16186]

Known issues in 2010

- Unable to view files in the **Files** tab. The issue occurs in cloud deployments. [RFLNX-5596]
- In Microsoft Teams, you must select the audio device manually. The audio device is not set as default automatically. [RFLNX-5652]
- Attempts to use drop-down menu in a session with full-screen mode might fail. The issue occurs when browser content redirection is enabled. [CVADHELP-13884]
- The TCP fallback option might not work even when `HDXoverUDP` is set to `Preferred`. The issue occurs when you connect using Citrix Gateway. [CVADHELP-15526]

Known issues in 2009

- The Multi-Stream ICA feature might not work correctly. [RFLNX-4286]
- When you are running a video call or sharing the screen in Microsoft Teams, the screen might flicker. [RFLNX-4778]
- Attempts to switch between desktop sessions might fail. [CVADHELP-15229]

Known issues in 2006

- Occasionally, the **Meeting** view doesn't restore during multitasking in Microsoft Teams. The issue occurs when a local window overlays the remote window. As a result, the remote window does not receive the mouse events. As a workaround, on the minimized screen, hover over the digital clock and double-click on the caller's name. [RFLNX-4937]
- Sometimes, session reconnection fails. The issue occurs when you configure the Multi-Stream ICA (MSI) protocol with a single port over TCP with SD-WAN. [RFLNX-4782]

Known issues in 2004

- Citrix Workspace app for Linux might fail to identify certain smart cards. As a result, attempts to launch a session with the card fail.
- When you launch a session after enabling the Multi-Stream ICA (MSI) protocol in Workspace app and on SD-WAN, the session exits unexpectedly. The following error message appears:

  "The connection to VDA was lost…"

The issue occurs because single-port MSI is not supported. [RFLNX-4219]

- Session launch might fail on CentOS 8.x, Fedora 29, 30, and 31 distributions. For a workaround, see Knowledge Center article CTX270926. [RFLNX-3114]

Known issues in 1912

- While using CEF-based BCR, the keyboard focus does not point back to the main window if you redirect a URL. As a workaround, create a browser tab and toggle to access the main tab. [RFLNX-3871]
- While using CEF-based BCR, you might observe a notification that the webcontainer process has stopped. The issue occurs when you close the browser instance. [RFLNX-3872]
- When you use the self-service user interface, the **Preferences** window options might not work as expected, and the Workspace application becomes temporarily unresponsive. The issue occurs on the Ubuntu 19.10 distribution. [RFLNX-3720]
- Workspace intelligence feeds are not supported on Citrix Workspace app Version 1912.
- Webcam redirection does not work with Microsoft Teams. This is a limitation because Citrix does not support Microsoft Teams Optimization [MTOP] in Citrix Workspace app for Linux. [RFLNX-3674]

Known issues in 1910

- When you use the self-service user interface, the **Preferences** window options might not work as expected. The issue occurs when the libwebkit1 package is unavailable as is the case with Debian 10 buster clients. As a workaround, remove the **UIDialogLibWebKit.so** library located inside the `install/path/lib` directory. [RFLNX-3596]
- Due to architectural changes, you can no longer connect to the cloud store [cloud setup]. Citrix recommends that you use the latest Version of Citrix Workspace app.

Known issues in 1908

- Due to architectural changes, you can no longer connect to the cloud store [cloud setup]. Citrix recommends that you use the latest Version of Citrix Workspace app.

Known issues in 1906

- After disconnecting the ICA session, the wfica process may exit after a couple of minutes. This is because, the wifca process tries to contact the network during exit. [RFLNX-3025]
- When you connect to a PNAgent store, not all the subscribed resources appear when you use the command `./util/storebrowse -S`. [RFLNX-2944]

- When using Skype, occasionally a webcam might not establish video when you log on consecutive times. As a workaround, close and restart the Skype session. [RFLNX-2897]
- The DynamicCDM feature might not work on CentOS 7.6, and the USB flash disk is not mapped to the desktop session. [RFLNX-3117]
- The first launch of a session on an ArmHardFloatPort (armhf) device that is based on Raspbian GNU/Linux 8.0 (jessie) might fail. The subsequent launches succeed. [RFLNX-3211]
- Citrix Workspace app for Linux does not support 32-bit cursors. If a 32-bit cursor is used on the VDA, it appears as black. This issue has been observed in earlier releases too. [RFLNX-1296]
- ICA launch might fail on Fedora 29/30. As a workaround, follow the steps:

    1. Install openssl10 by using the command

```
sudo yum install compat-openssl10.x86_64
```

    1. Set the environment variable in ~/.bashrc to load for every session. This action points to the older libcrypto library.

```
export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o
```

> **Note:**
>
> The app works fine in X.Org server as compared to the Wayland compositor. For distributions that have Wayland as the default graphics protocol, uncomment either of the following:
>
> `WylandEnable=false in /etc/gdm/custom.conf` or `/et/gdm3/custome.conf`. Log off and log on to point to the X.Org server. [RFLNX-3114]

- Due to architectural changes, you can no longer connect to the cloud store [cloud setup]. Citrix recommends that you use the latest Version of Citrix Workspace app.

Known issues in 1903

- When using Fedora 29 and later, the Citrix Workspace app for Linux exits unexpectedly with an error message “SIGSEGV”. This issue occurs because Fedora Version 29 and later are not currently supported due to incompatibility in the `libidn` package provided by the operating system. [LD0705]
- The Citrix Optimization SDK package contains in incorrect version of the UIDialogLibWebKit.so. As a workaround, perform the follow the steps:

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 WebKit folder:

```
cd ../WebKit
```

d) Remove the existing UIDialogLibWebKit.so:

```
rm -rf UIDialogLibWebKit.so
```

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.

> **Note:**
>
> Before launching the self-service, kill the AuthManagerDaemon and ServiceRecord processes. [RFLNX-2822]

Known issues in 1901

- No new issues have been observed in this release.

Known issues in 1810

- Sessions might fail to connect to StoreFront through the Citrix Gateway. The issue occurs when client authentication is mandatory. As a workaround, set client authentication to **Optional** or disable it. [RFLNX-2431]

Known issues in 1809

- “Automatically move pointer to the default button in a dialog box” does not work randomly. [LD0843]

Known issues in 1808

- When using storebrowse with PNA url and an expired password, the **Change Expired Password** screen does not appear. [LC9129]

Known Limitations

- When using Microsoft Teams, the “Test Call” option does not appear. [RFLNX-4234]

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

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 may or may not act on feedback based on its severity, criticality, and importance. Citrix is not committing to productizing experimental features and might withdraw them for any reason at any time.

Prerequisites to install Citrix Workspace app

January 28, 2021

System requirements and compatibility

See the following list for system requirements:

Hardware	Requirements
Linux kernel	- Version 2.6.29 or later
Disk Space	- A minimum of 55 MB - Additional 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 higher

Libraries and Codec	Requirements
Libraries	- glibcxx 3.4.15 or later - glibc 2.11.3 or later - gtk 2.20.1 or later - libcap1 or libcap2 - libjson-c (for instrumentation) - GCC 4.8 for x64 * - GCC 4.9 for Armhf * - X11 or X.Org - udev support
Self-service user interface	- webkit2gtk 2.16.6 or later - libxml2 2.7.8 - libxerces-c 3.1
Codec libraries	- Advanced Linux Sound Architecture (ALSA) libasound2 - Speex - Vorbis codec libraries

Network	Requirements
Network protocol	- TCP/IP

Components	Requirements
H.264	For x86 devices: - A minimum processor speed of 1.6 GHz - Single-monitor sessions - Display resolutions for example, 1280 x 1024 pixels
	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 **Note:** Performance improves after using faster processor clock speeds.
HDX MediaStream Flash Redirection	For all HDX MediaStream Flash Redirection requirements, see Knowledge Center article http://support.citrix.com/article/CTX134786. Citrix recommends testing with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.
Customer Experience Improvement Program (CEIP) integration	- zlib 1.2.3.3 - libtar 1.2 and later - libjson 7.6.1 or later

Components	Requirements
HDX RealTime Webcam Video Compression	- 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	- 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 **Note:** If GStreamer is not included in your Linux distribution, you can download it from https://gstreamer.freedesktop.org/download/. Use of certain codes (for example, those in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help.

Components	Requirements
Browser content redirection	- webkit2gtk version 2.16.6 - glibcxx 3.4.20 or later
Philips SpeechMike	- Visit the Philips web site to install the relevant drivers
Microsoft Teams Optimization	- Software o GStreamer 1.0 or later and Cairo 2 o libc++-9.0 or later o libgdk 3.22 or later o OpenSSL 1.1.1d o x64 Linux distribution - Hardware o Minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call. o 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

* Following the 1910 release, Citrix Workspace app for Linux might not work as expected unless 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

Compatibility matrix

Citrix Workspace app for Linux 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
  - 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 to access Citrix resources using Citrix Workspace app.

> **Note:**
>
> If the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the local key store), an untrusted certificate warning appears. If a user chooses to continue through the warning, the apps are displayed but cannot be launched. The root certificate must be installed in the client's certificate store.

Root certificates

For domain-joined machines, you can use Group Policy Object administrative template to distribute and trust CA certificates.

For non-domain joined machines, the organization can 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
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 for Linux supports wildcard certificates, however they should only be used in accordance with your organization's security policy. In practice, alternatives to wildcard certificates, such as a certificate containing the list of server names within the Subject Alternative Name (SAN) extension, could be considered. Such certificates can be issued by both private and public certificate authorities.

Intermediate certificates and the 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 Citrix Gateway documentation.

If your StoreFront server is not able to provide the intermediate certificates that match the certificate it

is using, or you install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store:

1. Obtain one or more intermediate certificates separately in PEM format.

   > **Tip:**
   >
   > If you cannot 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 install 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
   ```

Joint Server Certificate Validation Policy

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

> **Important:**
>
> Before installing Citrix Workspace app for Linux, confirm that the certificates at the server or gateway are correctly configured as described here. Connections may 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 for Linux now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Workspace app for Linux releases, it then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app for Linux's connection to fail.

Suppose that a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Workspace app for Linux:

- "Example Server Certificate"

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

Then, Citrix Workspace app for Linux checks that all these certificates are valid. Citrix Workspace app for Linux also checks that it already trusts “Example Root Certificate.” If Citrix Workspace app for Linux does not trust “Example Root Certificate,” the connection fails.

> **Important:**
>
> - Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there are currently two certificates (“DigiCert”/”GTE CyberTrust Global Root,” and “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”) that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available (“DigiCert Baltimore Root”/”Baltimore CyberTrust Root”). If you configure “GTE CyberTrust Global Root” at the gateway, Citrix Workspace app for Linux connections on those user devices will fail. Consult the certificate authority’s documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.
> - Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

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

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

Then, Citrix Workspace app for Linux uses these two certificates. It then searches for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as “Example Root Certificate”), the connection succeeds. Otherwise, the connection fails. This configuration supplies the intermediate certificate that Citrix Workspace app for Linux needs, but also allows Citrix Workspace app for Linux to choose any valid, trusted, root certificate.

Now suppose that a gateway is configured with these certificates:

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

A web browser may ignore the wrong root certificate. However, Citrix Workspace app for Linux will not ignore the wrong root certificate, and the connection will fail.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- “Example Server Certificate”
- “Example Intermediate Certificate 1”
- “Example Intermediate Certificate 2”

> **Important:**
>
> - Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and an earlier root certificate is still in use at the same time as a later root certificate. In this case, there will be at least two intermediate certificates. For example, the earlier root certificate “Class 3 Public Primary Certification Authority” has the corresponding cross-signed intermediate certificate “VeriSign Class 3 Public Primary Certification Authority - G5.” However, a corresponding later root certificate “VeriSign Class 3 Public Primary Certification Authority - G5” is also available, which replaces “Class 3 Public Primary Certification Authority.” The later root certificate does not use a cross-signed intermediate certificate.
> - The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To). But the cross-signed intermediate certificate has a different Issuer name (Issued By). This distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such “Example Intermediate Certificate 2”).

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

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

Avoid configuring the gateway to use the cross-signed intermediate certificate, as it selects the earlier root certificate:

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

It is not recommended to configure the gateway with only the server certificate:

- “Example Server Certificate”

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

Hdxcheck

Citrix provides a script, hdxcheck.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 for Linux. The script is located in the `Utilities` directory of the installation package.

To run the hdxcheck.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 `./hdxcheck.sh` to run the script.

Install, Uninstall, and Upgrade

December 3, 2020

You can install the Citrix Workspace app using any of the following methods:

- Download the Citrix Workspace app from Citrix Downloads.
- Deploy Citrix Workspace app using workspace for web (configured with StoreFront).

Manual install

Download the following packages from the Citrix Downloads page.

Debian packages

Install one of the `Icaclient` packages, or one of the `IcaclientWeb` packages based on your OS architecture.

To use generic USB redirection, install one of the `ctxusb` packages based on your OS architecture.

Package name	Contents
Debian packages (Ubuntu, Debian, Linux Mint etc.)	
icaclient_20.06.0.15_amd64.deb	Self-service support, 64-bit x86_64
icaclient_20.06.0.15_i386.deb	Self-service support, 32-bit x86
icaclient_20.06.0.15_armhf.deb	Self-service support, ARM HF
icaclientWeb_20.06.0.15_amd64.deb	Web Receiver only, 64-bit x86_64
icaclientWeb_20.06.0.15_i386.deb	Web Receiver only, 32-bit x86

Package name	Contents
icaclientWeb_20.06.0.15_armhf.deb	Web Receiver only, ARM HF
ctxusb_20.06.0.15_amd64.deb	USB package, 64-bit x86_64
ctxusb_20.06.0.15_i386.deb	USB package, 32-bit x86
ctxusb_20.06.0.15_armhf.deb	USB package, ARM HF

Install using a Debian package

When installing Citrix Workspace app from 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 are trying to install.

This procedure uses a command line and the native package manager for Ubuntu/Debian/Mint. You can also install the package by double-clicking the downloaded .deb package in a file browser. This 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.

> **Prerequisites:**
>
> You must install the `icaclient` package or the `icaclientWeb` package.

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 for the following three packages by typing `gdebi packagename.deb`. For example:
   - `gdebi icaclient\\_19.0.6.6\\_amd64.deb`
   - `gdebi icaclientWeb\\_19.0.6.6\\_i386.deb`
   - `gdebi ctxusb\\_2.7.6\\_amd64.deb`

   To use `dpkg` in the above examples, replace `gdebi` with `dpkg -i`.

   If using `dpkg`, install any missing dependencies by typing `sudo apt-get -f install`.

   > **Note:**
   >
   > The `ctxusb` package is optional to support the generic USB redirection feature.
4. Accept the EULA.

Red Hat packages

Install one of the `ICAClient` packages, or one of the `ICAClientWeb` packages based on your OS architecture.

To use generic USB redirection, install one of the `ctxusb` packages based on your OS architecture.

Package name	Contents
Redhat packages (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-20.06.0.15-0.x86_64.rpm	Self-service support, Red Hat (including Linux VDA) based, 64-bit x86_64
ICAClient-rhel-20.06.0.15-0.i386.rpm	Self-service support, Red Hat based, 32-bit x86
ICAClientWeb-rhel-20.06.0.15-0.x86_64.rpm	Web Receiver only, Red Hat based, 64-bit x86_64
ICAClientWeb-rhel-20.06.0.15-0.i386.rpm	Web Receiver only, Red Hat based, 32-bit x86
ICAClient-suse-20.06.0.15-0.x86_64.rpm	Self-service support, SUSE based, 64-bit x86_64
ICAClient-suse-20.06.0.15-0.i386.rpm	Self-service support, SUSE based, 32-bit x86
ICAClientWeb-suse-20.06.0.15-0.x86_64.rpm	Web Receiver only, SUSE based, 64-bit x86_64
ICAClientWeb-suse-20.06.0.15-0.i386.rpm	Web Receiver only, SUSE based, 32-bit x86
ctxusb-20.06.0.15-1.x86_64.rpm	USB package, 64-bit x86_64
ctxusb-20.06.0.15-1.i386.rpm	USB package, 32-bit x86

> **Note:**
>
> The *SuSE 11 SP3 Full Package (Self-Service Support)* RPM package is deprecated.

Install using an RPM package

If you are 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.

To set up the EPEL repository on Red Hat

Download the appropriate source RPM package from:
https://fedoraproject.org/wiki/EPEL#Extra_Packages_for_Enterprise_Linux_.28EPEL.29.

For information on how to use it, see https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F

For example, on Red Hat Enterprise 7.x, you can install the EPEL repository by using following command:

```
`yum localinstall epel-release-latest-7.noarch.rpm`
```

> **Tip:**
>
> RPM Package Manager does not install any missing required software. To download and install the software, we recommend using **zypper install <file name>** at a command line on OpenSUSE or **yum localinstall <filename>** on Fedora/Red Hat.

To install from the RPM package

> **Prerequisites:**
>
> You must install the `icaclient` package or the `icaclientWeb` package.

1. Set up the EPEL repository.
2. Log on as a privileged (root) user.
3. Run the installation for the following three packages by typing zypper in .

   > **Note:**
   >
   > The `ctxusb` package is an optional package. Install the package to support Generic USB Redirection.

4. Open a terminal window.

   For SUSE installations:

   - `zypper in ICAClient-suse-19.12.0.19-0.x86_64.rpm`
   - `zypper in ICAClient-suse-19.12.0.19-0.i386.rpm`
   - `zypper in ctxusb-2.7.19-1.x86\\_64.rpm`

   For Red Hat installations:

   - `yum localinstall ICAClient-rhel-19.12.0.19-0.i386.rpm`
   - `yum localinstall ICAClientWeb-rhel-19.12.0.19-0.i386.rpm`
   - `yum localinstall ctxusb-2.7.19-1.i386.rpm`

5. Accept the EULA.

To install a missing package

On a Red Hat based distribution (RHEL, CentOS, Fedora, and so on), if the following error message appears:

```
1  "… requires libwebkitgtk-1.0.so.0"
```

add an EPEL repository (details can be found at https://fedoraproject.org/wiki/EPEL).

Tarball packages

Install one of the following packages based on your OS architecture.

Package name	Contents
Tarballs (Script install for any distribution)	
linuxx64-20.06.0.15.tar.gz	64-bit Intel
linuxx86-20.06.0.15.tar.gz	32-bit Intel
linuxarmhf-20.06.0.15.tar.gz	ARM HF

The difference between packages that offer support for Web Workspace app and those packages that support self-service is that the latter packages include dependencies required for self-service in addition to those needed for the Web Workspace app. Dependencies for self-service are a superset of those required for Web Workspace app, but the files installed are identical.

- If you require only workspace app for web, or your distribution does not have the necessary packages to support self-service, install only the workspace app for web package.
- Otherwise, install Citrix Workspace app from the Debian package or the RPM package. These files are easier to use because they automatically install any required packages.
- If you want to customize the installation location, install Citrix Workspace app from the tarball package.

> **Note:**
>
> - 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 perform dependency checks nor 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).

   > **Note:**
   >
   > If you specify a non-default location, set it in $ICAROOT in `$HOME/.profile` or `$HOME/.bash\\_profile`.

6. When prompted to proceed, 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 thus, 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 published VDI applications. Type `y` at the prompt to install USB support.

> **Note:**
>
> If you are not logged on as a privileged user (root), the following warning appears:
>
> "USB support cannot 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

This procedure has been tested with the tarball package. Remove the RPM and Debian packages using your operating system's standard tools.

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`.

> **Note:**
>
> To uninstall Citrix Workspace app, you must be logged in as the same user who performed the installation.

To uninstall the tarball package

1. Run setup by typing `$ICAROOT/setupwfc` and press Enter.
2. To remove the client, type `2` and press **Enter**.

Upgrade

To upgrade from Citrix Receiver to Citrix Workspace app, download and install the latest Citrix Workspace app from Citrix Downloads.

The **Citrix Workspace** screen overlay appears on the first launch of the app, when you upgrade, and when you uninstall and reinstall the app. Click **Got it** to continue using Citrix Workspace app, or click **Learn more** to find out more details.

Get started

October 29, 2020

Set up

You can download the installation package, customize the configuration and then isntall the Citrix Workspace app. You can modify the contents of Citrix Workspace app package and then repackage the files.

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, linuxx86.13.2.0.nnnnnn.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 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 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 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.

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 but where the requirements for self-service have not been met.

Terminal prompt

To start the Citrix Workspace app at the terminal prompt, type:
`/opt/Citrix/ICAClient/selfservice`

And press Enter (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Workspace app).

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 located in different menus depending on your Linux distribution.

Preferences

To set preferences, click **Preferences** from the Citrix Workspace app menu. You can control how desktops are displayed, connect to different applications and desktops, and manage file and device access.

Manage an account

To access desktops and applications, you need an account with XenDesktop or Citrix Virtual Apps. 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 adminstrator 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. Authenticate to the server when asked.

Desktop display

> **Note:**
>
> This feature is not available with Citrix Virtual Apps for UNIX sessions.

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 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 work with more than one desktop using multiple Citrix Virtual Apps and Desktops 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.

Automatic session reconnect

Citrix Workspace app can reconnect to desktops and applications that are disconnected.For example, a network infrastructure issue.

- 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 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 needs to 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:

- U**se 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.

Flash player

You can choose how flash content is displayed. This content is normally displayed in **Flash Player** and includes video, animation, and applications:

On the **Flash** page of the **Preferences** dialog box, select one of the following options:

- **Optimize content** - Improves playback quality at the risk of reducing security.
- **Don’t optimize content** - Provides basic playback quality without reducing security.
- **Ask me each time** - Prompts each time a flash content is displayed.

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 by Citrix Virtual Apps and Desktops 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 are added. For PNAgent, the store URL is displayed and uniquely identifies the store.

After connecting to a store, 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 servers. You can also change those settings for individual connections, if necessary.

Although the tasks and responsibilities of administrators and users can overlap, the term “user” is employed to distinguish typical user tasks from those typically performed by administrators.

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. In addition, 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. Obtain the unique ID of the desktop or application that you want to connect to. This is the first quoted string on a line acquired in one of the following commands:
   - List all of the desktops and applications on the server:

     ```
     ./util/storebrowse -E <store URL>
     ```

   - List the desktops and applications that you have 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 cannot connect to a server, your administrator might need to change the server location or SOCKS proxy details. 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 so that .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 are 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."

   ```
   setenv 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 need to configure Firefox on its Preferences/Applications setting page.

   For "Citrix ICA settings file content," select:

   - "Citrix Workspace app Engine (default)" in the drop-down menu 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 Connection Center:

1. On the Citrix Workspace app menu, click **Connection Center**.

   The servers that are used appears and, the each 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.

Configure

February 3, 2021

When using Citrix Workspace app for Linux, the following configuration steps allow users to access their hosted applications and desktops.

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:**
>
> Add an entry to `All\\_Regions.ini` only if you want to allow other configuration files to override the value in `module.ini`. The values in 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.

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. `$HOME/.ICAClient/All\\_Regsions.ini` can match or reduce the possible values set by `$ICAROOT/config/All\\_Regions.ini`, it cannot 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 is not assigned a value, the default is automatically applied. For example, if `InitialProgram` is followed by an equal sign (=) but no value, the default (not to run a program after logging in) is applied.

Precedence

`All\\_Regions.ini` specifies parameters that can be set by other files. 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` - Values in this file override those in:
   - The connections .ICA file
   - `wfclient.ini`
2. `module.ini` - Values in this file are used if they have not been set in `All\\_Regions.ini`, the connections .ICA file, or `wfclient.ini` but they are not restricted by entries in `All\\_Regions.ini`.

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.

App protection experimental feature

> **Note:**
>
> - This feature is supported only when Citrix Workspace app is installed by using the tarball package. Also, x64 and armhf are the only two supported packages.
> - This feature is supported only on on-premises deployments of Citrix Virtual Apps and Desktops.

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 by keylogging and screen capturing malware. App protection prevents exfiltration of confidential information such as user credentials and sensitive information displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

Prerequisite:

- Ubuntu 18.04 or later.

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 cannot 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.

By default, the app protection component is not installed.

Restart your machine for the changes to take effect. App protection might not work as expected unless you restart your machine.

Known issues:

- When you minimize a protected screen, app protection continues to run in the back end.

Customer Experience Improvement Program (CEIP)

Data collected	Description	What we use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app 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 will handle your data in accordance with the terms of your contract with Citrix, and protect 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. Please review how Google handles data collected for Google Analytics.

You can turn off sending CEIP data to Citrix and Google Analytics (except for the two data elements collected for Google Analytics indicated by an * in the second table below) by:

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`.

> **Note:**
>
> Once you set the `EnableCeip` key to `Disable`, if you would like to disable sending the final two CEIP data elements collected by Google Analytics (that is, Operating System version & Workspace app version) navigate to the following section and set the value as suggested:

Location: `<ICAROOT>/config/module.ini`

Section: `GoogleAnalytics`

Entry: `DisableHeartBeat`

Value: `True`

The specific CEIP data elements collected by Google Analytics are:

Operating system version*	Workspace app version*	App name	Client ID
Session launch method	Compiler version	Hardware platform	

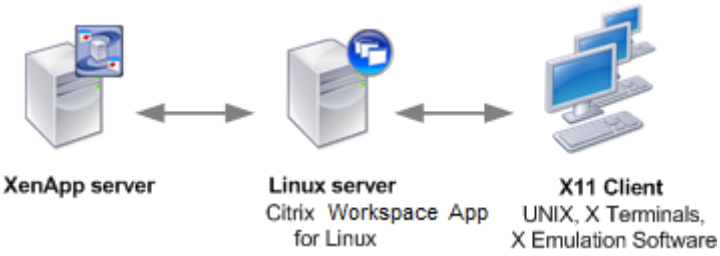
ICA-to-X proxy

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 to deliver Microsoft Windows applications to X terminals or to UNIX workstations for which Citrix Workspace app is not available.

> **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 multiple copies of Citrix Workspace app simultaneously on one system with each sending 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 is not available, you need an extra server to act as the proxy. This 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 is not a problem if you are using X terminals (which usually do not have local drives). If you are 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 are not passed to the final device:

- USB redirection
- Smart card redirection
- COM port redirection
- Audio is not delivered to the X11 device, even if the server acting as a proxy supports audio.
- Client printers are not passed through to the X11 device. You access the UNIX printer from the server manually using LPD printing, or use a network printer.
- Redirection of multimedia input is not expected to work because it requires a webcam on the machine running Citrix Workspace app, which is the server acting as a proxy. However, redirection of multimedia output works with 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. If Citrix Workspace app is not installed in the default installation directory, ensure 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 &`.

Server-client content redirection

Server-client content redirection enables administrators to specify that URLs in a published application are opened using 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 allocate Citrix resources more efficiently, thereby providing users with better performance.

The following types of URL can be redirected:

- HTTP
- HTTPS
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Older Real Players)

If Citrix Workspace app for Linux does not have an appropriate application or cannot directly access the content, the URL is opened using the server application.

Server-client content redirection is configured on the server and enabled by default in Citrix Workspace app if the path includes RealPlayer and at least one of Firefox, Mozilla, or Netscape.

To enable server-client content redirection if RealPlayer and a browser are not in the path

1. Open the configuration file `wfclient.ini`.
2. In the [Browser] section, modify the following settings:

   Path=path

   Command=command

   where path is the directory where the browser executable is located and 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
```

1. In the [Player] section, modify the following settings:

   Path=path

   Command=command

   where path is the directory where the RealPlayer executable is located and command is the name of the executable used to handle the redirected multimedia URLs, appended with the URL sent by the server.

2. Save and close the file.

> **Note:**
>
> For both Path settings, you need only specify the directory where the browser and RealPlayer executables reside. You do not need to specify the full path to the executables. For example, in the [Browser] section, Path might be set to /usr/X11R6/bin rather than /usr/X11R6/bin/netscape. In addition, you can specify multiple directory names as a colon-separated list. If these settings are not specified, the user's current $PATH is used.

To turn off server-client content redirection from Citrix Workspace:

1. Open the configuration file module.ini.
2. Change the CREnabled setting to Off.
3. Save and close the file.

Connection

Configure connections

On devices with limited processing power or where limited bandwidth is available, there is 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** - SpeedScreen Latency Reduction improves performance over high latency connections by providing instant feedback to the user in response to typed data or mouse clicks. Use SpeedScreen Latency Reduction Manager to enable this feature on the server. By default, in Citrix Workspace app, this is disabled for keyboard and only enabled for the mouse on high latency connections. 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 requires more processor resources to compress and decompress the data, but it can increase performance over low-bandwidth connections. Use 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 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.

Font

ClearType font smoothing

ClearType font smoothing (also known as subpixel font rendering) improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing. You can turn this feature on or off. Or you specify the type of smoothing by editing the following setting in [WFClient] section of the appropriate configuration file:

FontSmoothingType = number

Where number can take one of the following values:

Value	Behavior
0	The local preference on the device is used. This value is defined by the FontSmoothingTypePref setting.
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 takes precedence over the value set in [WFClient].

If the server sets the value to 0, the local preference is determined by another setting in the [WFClient]: FontSmoothingTypePref = number

Where 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)

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 so that these 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:

A two-part procedure is as follows. First, you enable special folder redirection by making an entry in module.ini; then you specify the folder locations in the [WFClient] section, as described here:

1. Add the following text to module.ini (for example, $ICAROOT/config/module.ini):

   [ClientDrive]

   SFRAllowed = True

2. Add the following text to the [WFClient] section (for example, $HOME/.ICAClient/wfclient.ini):

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.

Client-drive mapping

Client drive mapping allows drive letters on the Citrix Virtual Apps or Citrix Virtual Desktops 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 Workspace app.

Client drive mapping can make any directory mounted on the local user device, including a CD-ROM, DVD, or a USB memory stick, available to the user during a session, provided the local user has permission to access it. When a server is configured to allow client drive mapping, users can access their locally stored files, work with them 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 servers. Client device mapping enables a remote application running 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 are running locally. Ensure 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 (on both Citrix Virtual Apps and Desktops). If you require either or both of these features, disable SELinux before configuring them on the server.

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 letter on the server at logon. For example, it can be used to map all or part of a user's home directory or /tmp, and the mount points of hardware devices such as CD-ROMs, DVDs, or USB memory sticks.

- Dynamic client drive mapping monitors the directories in which hardware devices such as CD-ROMs, DVDs, and USB memory sticks are typically mounted on the user device. 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 or Citrix Virtual Desktops, client drive mappings are reestablished unless client device mapping is disabled. 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.

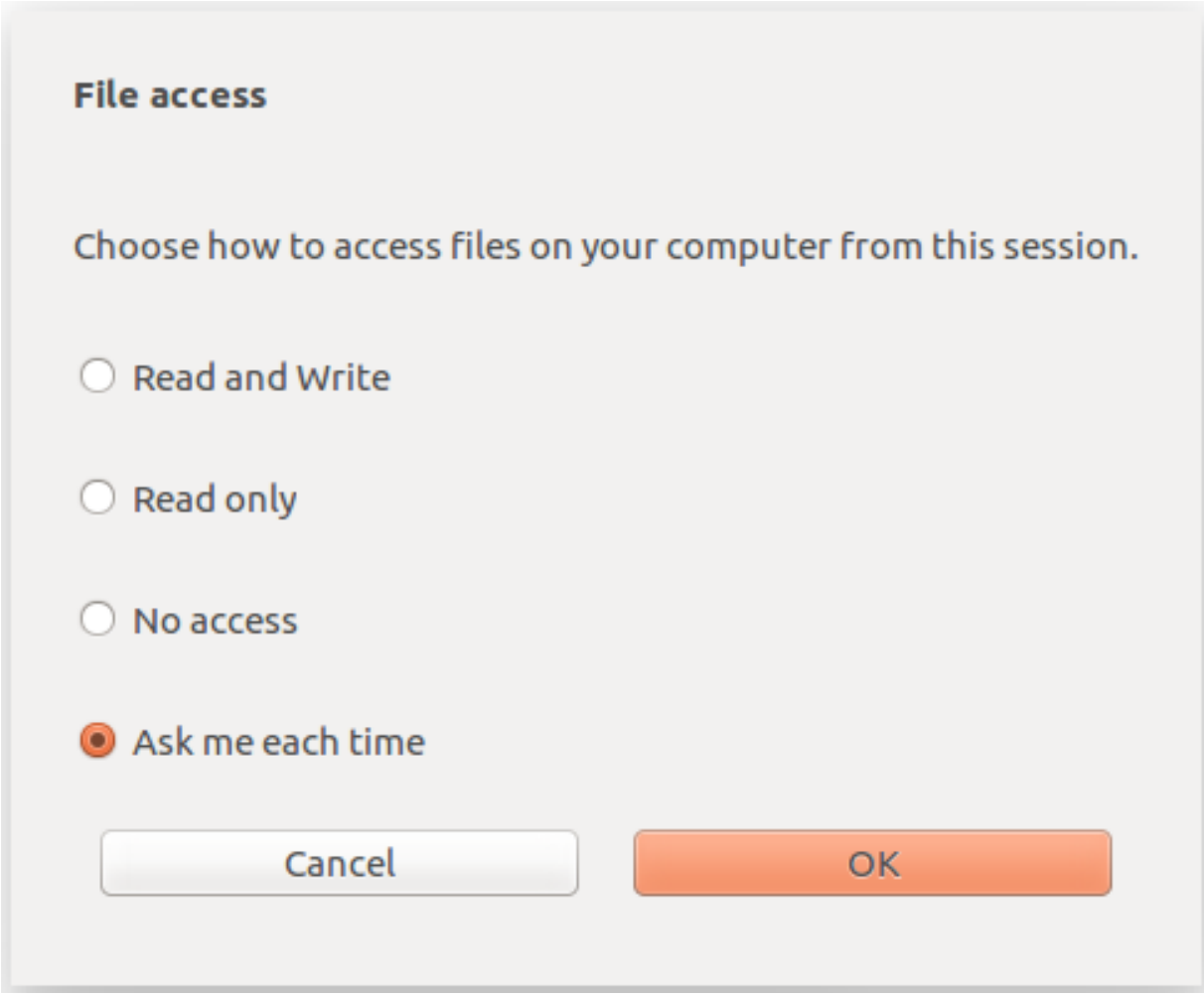
Users can map drives using the Preferences dialog box.

> **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`.

Previously, your setting for file access through CDM was applied on all configured stores.

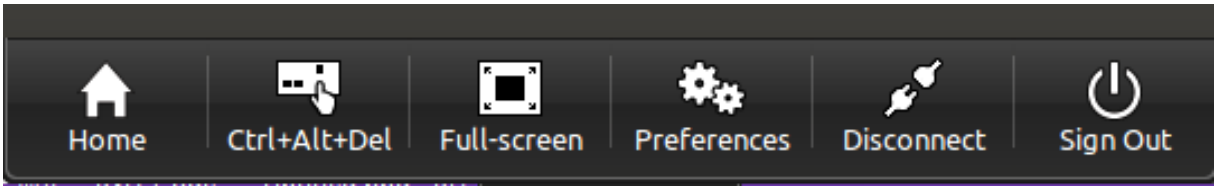
Starting with Version 2012, Citrix Workspace app allows you to configure per-store CDM file access.

> **Note:**
>
> The file access setting isnt' persistent across sessions when using workspace for web. It defaults to the **Ask me each time** option.

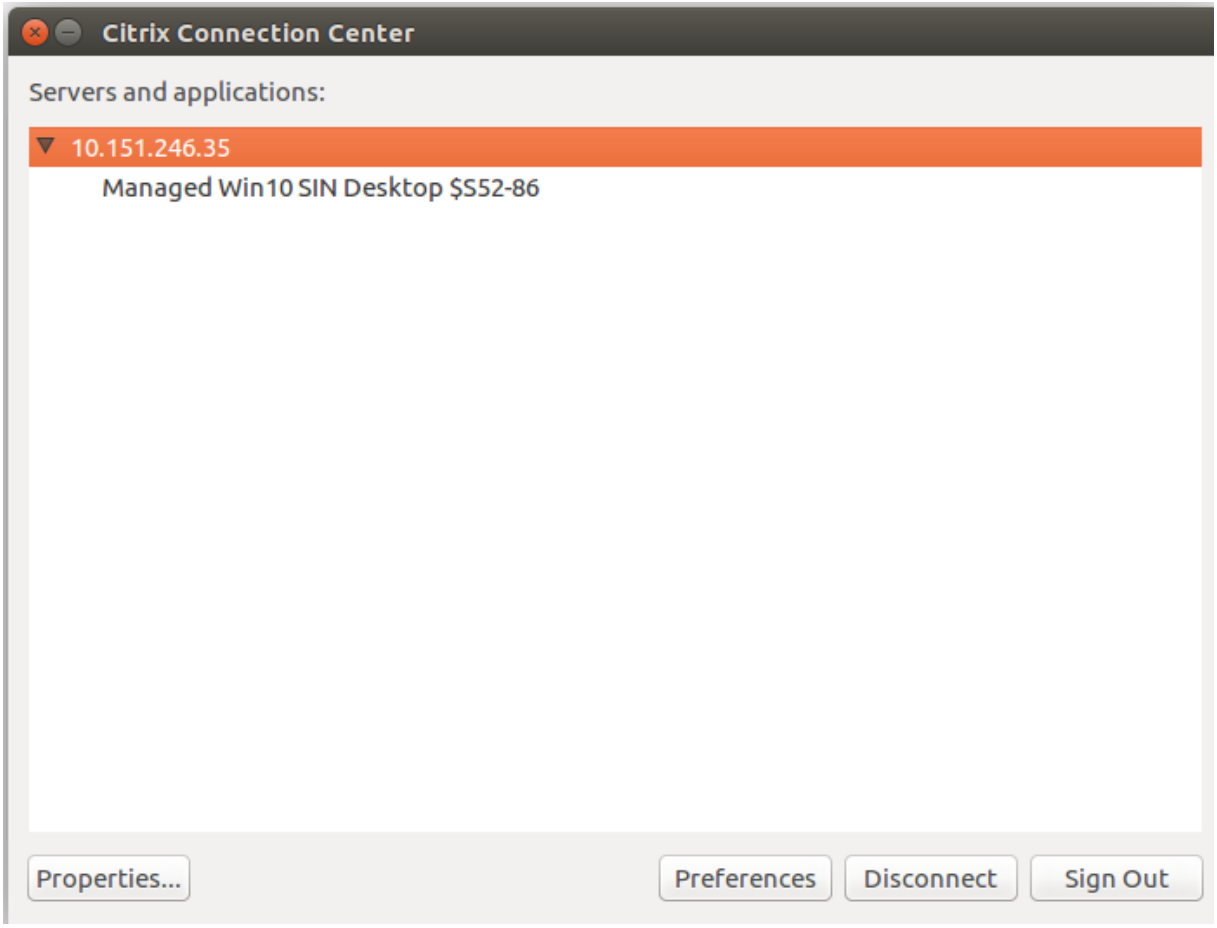


You can use the `wfclient.ini` file to configure the mapped path and file name attributes. Use the GUI to set a file access level as shown in the preceding screen capture.

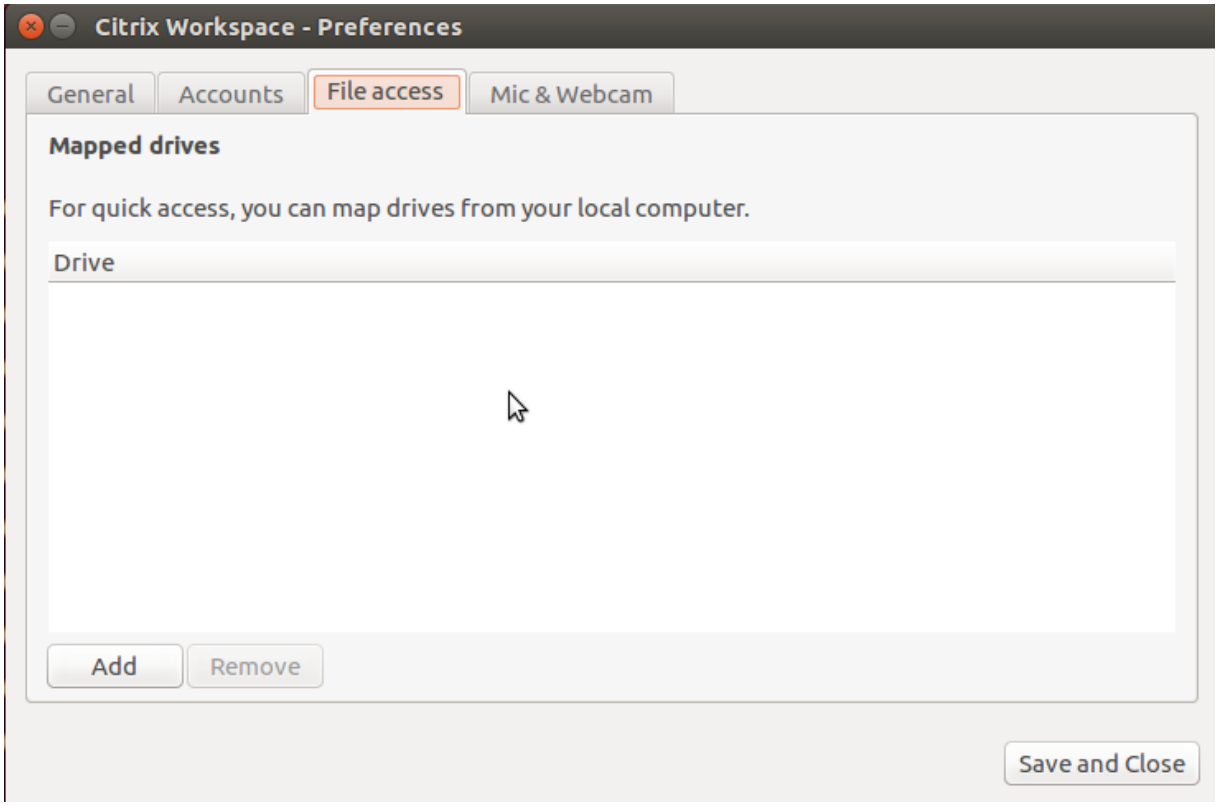
In a desktop session, you can set a file access level by navigating to **Preferences** > **File access** dialog from the Desktop Viewer.



In an app session, you can set a file access level by launching the **File access** dialog from **Citrix Connection Center**.



The **File access** dialog includes the mapped folder name and its path.



The access level flag is not supported in the `wfclient.ini` file anymore.

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 lets users:

- Print to all printing devices accessible from the user device
- Add printers

These settings, however, might not be the optimum 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.

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 client printers on UNIX

In a UNIX environment, printer drivers defined by Citrix Workspace app are ignored. The printing system on the user device must be able to handle the print format generated by the application.

Before users can print to a client printer from Citrix Virtual Apps for UNIX, printing must be enabled by the administrator. For more information, see the Citrix Virtual Apps for UNIX section in the Citrix Virtual Apps and Desktops documentation.

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, however, manually map client printers on Citrix Virtual Apps for Windows if, for example, the user device's printing software does not 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.
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 is a standard printer name, similar to those 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.

Audio

Previously, only the default audio device was mapped in a session even when many devices were available on the machine. The mapped device commonly appeared as **Citrix HDX Audio**.

Starting with Version 2010, Citrix Workspace app for Linux displays all local audio devices that are available in a session. Instead of **Citrix HDX Audio**, they now appear with their respective device names. You can switch to any of the available devices dynamically in a session. Unlike in earlier releases, now you don't need to select the default audio input or output before launching the session. Sessions update dynamically when you plug in or remove audio devices.

Starting from Version 2012, the enhanced audio redirection feature is enabled by default.

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 add the following entry:

   VdcamVersion4Support=False

> **Note:**
>
> - When the enhanced audio redirection feature is disabled, only the default audio device with the name **Citrix HDX Audio** appears in the session.
> - The **Mic and Webcam** option in the **Preferences** dialog remains disabled by default. For information on how to enable mic and webcam, see Preferences.

Known limitations:

- On a VDA running on Windows Server 2016, you can't change the audio device selection in a session. The selection is set to the default audio input and output only.
- Audio device redirection is not supported with Bluetooth audio devices.
- You can change the default audio device only on Windows 10 , Windows 7 and Windows 8 operating system. On Windows server operating systems, such as Windows Server 2012, 2016, 2019, you cannot change the default audio device due to a limitation in Microsoft Remote Desktops Session.

The default audio device is typically the default ALSA device configured for your system. Use the following procedure to specify a different device:

1. Choose and open a configuration file according to which users you want your changes to affect. See default settings for information about how updates to particular configuration files affect different users.
2. Add the following option, creating the section if necessary:


```
[ClientAudio]

AudioDevice = \<device\>
```

Where device information is located in the ALSA configuration file on your operating system.

> **Note:**
>
> The location of this information is not standard across all Linux operating systems. Citrix recommends consulting your operating system documentation for more details about locating this information.

Map client audio

Client audio mapping enables applications executing on the Citrix Virtual Apps server or Citrix Virtual Desktops to play sounds through a sound device installed on the user device. You can set audio quality on a per-connection basis on the server and users can set it on the user device. If the user device and server audio quality settings are different, the lower setting is used.

Client audio mapping can cause excessive load on servers and the network. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process.

You configure client audio mapping using policies. For more information, see the Citrix Virtual Apps and Desktops documentation.

> **Note:**
>
> Client audio mapping is not supported when connecting to Citrix Virtual Apps for UNIX.

Enabling UDP audio

UDP audio can improve the quality of phone calls made over the Internet. It uses User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP).

Limitations:

- UDP audio is not available in encrypted sessions (that is, those using TLS or ICA Encryption). In such sessions, audio transmission uses TCP.
- The ICA channel priority can affect UDP audio.

1. Set the following options in the ClientAudio section of module.ini:
   - Set EnableUDPAudio to True. By default, this 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.

2. Set client and server audio settings as follows so that the resultant audio is of a medium quality (that is, not high or low).

		Audio quality on client	Audio quality on client	Audio quality on client
		High	Medium	Low
Audio quality on server	High	High	Medium	Low
Audio quality on server	Medium	Medium	Medium	Low
Audio quality on server	Low	Low	Low	Low

UDP on the client

In `$ICAROOT/config/module.ini` file, add the following:

Under the [ClientAudio] section:

EnableUDPAudio=True
UDPAudioPortLow=int
UDPAudioPortHigh=int

In $HOME/.ICAClient/wfclient.ini file, add the following:

Under the [WFClient] section:

AllowAudioInput=True
EnableAudioInput=true
AudioBandWidthLimit=1

> **Note:**
>
> If the .ICAClient folder is not found (occurs only in case of first-time installation and launching) launch the Citrix Workspace app and close. This action creates the .ICAClient folder.

Add the following under wfclient.ini.* Set policy on DDC:

Set “Windows Media redirection” to “Prohibited”
Set “Audio over UDP” to “Allowed”
Set “Audio over UDP real time transport” to “enabled
Set “Audio quality” to “Medium”

Changing how Citrix Workspace app is used

ICA technology is highly optimized and typically does not have high CPU and bandwidth requirements. However, if you are using a very low-bandwidth connection, consider the following to preserve performance:

- **Avoid accessing large files using client drive mapping**. When you access a large file with client drive mapping, the file is transferred over the server connection. On slow connections, this might take a long time.
- **Avoid printing large documents on local printers**. When you print a document on a local printer, the print file is transferred over the server connection. On slow connections, this might take a long time.
- **Avoid playing multimedia content**. Playing multimedia content uses many bandwidths and can cause reduced performance.

USB

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. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets.

USB redirection requires either Citrix Virtual Apps 7.6 (or later) or Citrix Virtual Desktops. Citrix Virtual Apps does not support USB redirection of mass storage devices and requires special configuration to support audio devices. See Citrix Virtual Apps 7.6 documentation for details.

Isochronous features in USB devices such as webcams, microphones, speakers, and headsets are supported in typical low latency/high speed LAN environments. But usually the standard audio or webcam redirection are more suitable.

The following types of device are supported directly in a Citrix 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 are not supported for remoting through Citrix Virtual Apps and Desktops. For example, a user might have a NIC attached to the system board by internal USB. Remoting this would not be appropriate. The following types of USB device are not supported by default for use in a Citrix Virtual Apps and Desktops session:

- Bluetooth dongles
- Integrated NICs
- USB hubs

To update the default list of USB devices available for remoting, edit the usb.conf file, located in $ICAROOT/. 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 in a USB device, it is checked against the USB policy, and, if allowed, redirected to the virtual desktop. If the device is denied by the default policy, it is available only to the local desktop.

For desktops accessed through desktop appliance mode, when a user plugs in a USB device, that device is automatically redirected to the virtual desktop. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.

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.

Mass storage devices

If a user disconnects from a virtual desktop when a USB mass storage device is still plugged in to the local desktop, that device is not redirected to the virtual desktop when the user reconnects. To ensure that the mass storage device is redirected to the virtual desktop, the user must remove and reinsert the device after reconnecting.

> **Note:**
>
> If you insert a mass storage device into a Linux workstation that has been configured to deny remote support for USB mass storage devices, the device will not be accepted by the Workspace app software. And a separate Linux file browser might open. Therefore, 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 point.

> **Note:**
>
> - If the Client USB device redirection server policy is turned on, mass storage devices are always directed as USB devices even if client drive mapping is turned on.
> - The app does not support composite device redirection for USB devices.

USB classes

The following classes of USB device are allowed by the default USB policy rules:

- 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 and include force feedback joysticks, motion platforms, and force feedback exoskeletons.

- Still Imaging (Class 06)

  Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras might also appear as mass storage devices. And it might be possible to configure a camera to use either class, through setup menus provided by the camera itself.

  If a camera appears as a mass storage device, client drive mapping is used, and USB support is not required.

- 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 mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There is a wide variety of devices having internal storage which also presents a mass storage interface; these 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 mass storage devices use this variant of SCSI

  Mass storage devices can often be accessed through client drive mapping, and so USB support is not required.

  Important: Some viruses are known to propagate actively using all types of mass storage. Consider carefully whether there is a business need to permit the use of mass storage devices, either through client drive mapping, or USB support. To reduce this risk, the server might be configured to prevent files being executed through client drive mapping.

- 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 blood pressure sensors, heart rate monitors, pedometers, pill monitors, and 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 usually appear as vendor-specific (class ff).

USB device classes

The following classes of USB device are denied by the default USB policy rules:

- 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 keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and 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 is because most keyboards and mice are handled appropriately without USB support. And it is 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 is not necessary to access these devices remotely.

- 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, and 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 ultra wide band controllers and Bluetooth.

  Some of these devices might be providing critical network access, or connecting critical peripherals such as Bluetooth keyboards or mice.

  The default USB policy does not allow these devices. However, there might be particular devices it is 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 contained in the usb.conf file on the user device in $ICAROOT/.

You 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 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

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 usb.conf on the user device take the format {ALLOW:|DENY:} followed by a set of expressions 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:

- Rules are case-insensitive.
- Rules might have an optional comment at the end, introduced by "#." A delimiter is not required and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- Whitespace used as a separator is ignored, but cannot 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 is not.

- Tags must use the matching operator "=." For example, VID=1230.

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 in the file $ICAROOT/config/module.ini on each user device, set DesktopApplianceMode = Boolean as follows.

TRUE	Any USB devices that are already plugged in start-up provided the device is not disallowed with a Deny rule in the USB policies on either the server (registry entry) or the user device (policy rules configuration file).
FALSE	No USB devices start up.

Webcams

By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression. In some circumstances, however, you may require users to connect webcams using USB support. To do this, you must disable HDX RealTime Webcam Video Compression.

Webcam redirection

Following are a few points on webcam redirection:

- Webcam redirection works with and without RTME.
- Webcam redirection works for 32-bit applications. For example, Skype, GoToMeeting. Use a 32-bit browser to verify webcam redirection online. For example, www.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.

Xcapture

The Citrix Workspace app package includes a helper application, xcapture, to assist with the exchange of graphical data between the server clipboard and non-ICCCM-compliant X Windows 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

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 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.

Mouse

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 or Citrix Virtual Desktops 7.8 (or later). It is 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.

> **Tip:**
>
> Refer to the section Alternative Relative Mouse values for additional information about enabling relative mouse features.

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 are not 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 relative mouse for first-person gaming-style application interfaces.

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 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.

Keyboard

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 accordingly:
    - 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.

Bloomberg keyboard redirection

> **Note:**
>
> Bloomberg audio redirection follows similar configuration steps.

You can achieve Bloomberg keyboard redirection as follows:

- through generic USB redirection
- through generic USB redirection and with selective redirection support

Generic redirection

Configuring the Bloomberg v4 keyboard through Generic USB Redirection on the client side:

As a prerequisite, the policy should be enabled in 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.

Selective redirection

This feature allows the use of the Bloomberg v4 keyboard 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.

> **Note:**
>
> By default, this feature is enabled for x86 and x64 platforms and is disabled for ARMHF platforms.

To enable the feature:

1. Edit the BloombergRedirection section as follows in the config/All_Regions.ini file.

   ```
   BloombergRedirection=true
   ```
2. Perform all the steps mentioned in Generic redirection.

To disable the feature:

1. Edit the BloombergRedirection section in the config/All_Regions.ini file.
2. Set the BloombergRedirection value to false.

   ```
   BloombergRedirection=false
   ```
3. Perform 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.

Browser content redirection

Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR) [Experimental]

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.

Enabling CEF-based BCR

To enable CEF-based BCR:

1. Edit the file located at:
   `$ICAROOT/config/All_Regions.ini`
   where, $ICAROOT is the default installation directory of Citrix Workspace app.
2. Add the following entry in the [Client Engine\WebPageRedirection] section:

   UseCefBrowser=true

For information about BCR, see Browser content redirection in the Citrix Virtual Apps and Desktops documentation.

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, 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 both on the Server and Client, as well as 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 entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During the downtime, all of the user's data, key presses, and other interactions are stored, and the application appears frozen. When the connection is re-established, these interactions are replayed into the application.

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 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, Common Gateway Protocol, is enabled (using policy settings) on the server. Disabling Common Gateway Protocol also disables HDX Broadcast session reliability.

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 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 support

> **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, thereby reducing 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 depending on the media file types supported by GStreamer on a user device.

With client-side fetching, you can also allow the user device to stream media directly from URLs of the form http://, <mms://>, or <rtsp://> rather than streaming the media through a Citrix server. 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 are using the tarball script (this 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, which continues to use playbin2, using the SpeedScreenMMAEnablePlaybin2 option in the Multimedia section of All-Regions.ini.
- 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.
- If you want to use GStreamer 1.0, follow the instructions below:

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 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 1912 release, you can configure GStreamer 1.x as the default version.

Limitations:

- When you play a video, forward and backward seek 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

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 - is the installation path of Citrix Workspace app for Linux.
- GST_PLUGINS_PATH - is GStreamer's plug-in path. For example, on a 64-bit debian machine it is */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

HDX MediaStream Flash Redirection

HDX MediaStream Flash Redirection enables Adobe Flash content to play locally on user devices, providing users with high definition audio and video playback, without increasing bandwidth requirements.

1. Ensure that your user device meets the feature requirements. For more information, see System requirements.
2. Add the following parameters to the [WFClient] section of wfclient.ini (for all connections made by a specific user) or 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 is set to **Never** and 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 is set to **Disabled**.

    - **HDXFlashUseServerHttpCookie=Disabled**; **Enabled**

      Enables or disables HTTP cookie redirection. By default, this is set to **Disabled**.

    - **HDXFlashEnableClientSideCaching=Disabled**; **Enabled**

      Enables or disables client-side caching for web content fetched by Citrix Workspace app. By default, this is set to **Enabled**.

    - **HDXFlashClientCacheSize= [25-250]**

Defines the size of the client-side cache, in MB. This 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 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 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, ensuring users experience optimal performance when using applications such as GoToMeeting with HD Faces, Skype for Business.

1. Ensure that your user device meets the feature requirements.
2. Ensure that the `Multimedia` virtual channel is enabled. To do this, open the module.ini configuration file, located in the $ICAROOT/config directory, and check that `MultiMedia` in the [ICA3.0] section is set to "On."
3. Enable audio input by clicking 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, 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:

   HDXWebCamEnabled=Off

   For more information, see default settings.

2. Open the usb.conf file, typically located 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 are served by Citrix Virtual Apps and Desktops 7. 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.

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 helps to reduce CPU costs while processing graphics that include complex images but relatively small amounts of text or non-critical text.

> **Important:**
>
> To configure this feature, do not use any lossless setting in the Citrix Virtual Apps and Desktops 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 wfclient.ini, set **H264Enabled** to False. This also disables text tracking.

To disable text tracking only

With deep compression codec support enabled, in wfclient.ini set **TextTrackingEnabled** to False.

Screen tiles

You can improve the way that JPEG-encoded screen tiles are processed using the direct-to-screen bitmap decoding, batch tile decoding, and deferred XSync features.

1. Ensure that your JPEG library supports these features.
2. In the Thinwire3.0 section of wfclient.ini, set DirectDecode and BatchDecode to True.

   Note: Enabling batch tile decoding also enables deferred XSync.

Logging

In earlier releases, the `debug.ini` and `module.ini` files were used to configure logging.

As of Version 2009, you can configure logging using one of the following methods:

- Command-line interface
- Graphical user interface (GUI)

Also as of Version 2009, the `debug.ini` configuration file is removed from the Citrix Workspace app installer package.

Logging captures the Citrix Workspace app deployment details, configuration changes, and administrative activities to a logging database. A third-party developer can leverage this logging mechanism by using the logging 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.
- 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/ICAClient.log`. Otherwise, the logs are stored in `${ HOME } /.ICAClient/logs/ICAClient.log`.

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

Module	Log class
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
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

Module	Log class
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
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 errors
- Normal
- Verbose

By default, the **Logging** option is set to **Normal**.

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 not recommended unless required for troubleshooting.

Click **Save and Close** after you select the desired logging 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 logging service `ctxlogd`.
>
> For example, if you are on a systemd-capable setup, run the following command:

`systemctl restart ctxlogd`.

Enabling logging on Version 2006 and earlier:

If you are on Version 2006 and earlier, enable the logging using the procedure below:

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 multiple classes separated by the pipe symbol.
   For example, `+TC_LIB|+TC_MMVD`.

The following table lists various modules and their corresponding trace class values:

Troubleshooting:

If `ctxlogd` turns unresponsive, the logs are traced in 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. You can configure the path and the name of the log file by editing 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 ensure that a new syslog is available, delete 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.

Remote logging

To enable remote logging 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 rsyslog.conf file by replacing localhost with the IP address of the remote server:

  ```
  *.* @@localhost:10514
  ```

Optimization for Microsoft Teams

Optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops 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 necessary components for Microsoft Teams optimization into the VDA and the 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 x64 Linux distributions.

For information on how to enable logging, follow the steps mentioned under Logging for Microsoft Teams.

For information on system requirements, see Microsoft Teams Optimization.

For more information, see Optimization for Microsoft Teams and Microsoft Teams redirection.

Logging for Microsoft Teams

To enable logging for Microsoft Teams:

1. Navigate to the `/opt/Citrix/ICAClient/debug.ini` file.
2. Modify the [HDXTeams] section as follows:

```
[HDXTeams]
; Retail logging for HDXTeams 0/1 = disabled/enabled
HDXTeamsLogSwitch = 1
; Debug logging; , It is in decreasing order
; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
   LS_VERBOSE = 0
WebrtcLogLevel = 0
; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
WebrpcLogLevel = 0
```

Support for NetScaler App Experience (NSAP) virtual channel

Previously available as an experimental feature, the NetScaler App Experience (NSAP) virtual channel feature is now fully supported. All HDX Insight data is sourced from the NSAP virtual channel exclusively and sent uncompressed. This approach improves scalability and performance of sessions. The NSAP virtual channel is enabled by default. To disable it, toggle the VDNSAP flag `VDNSAP=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.

Multi-monitor layout persistence

This feature retains the session monitor layout information across endpoints. The session appears at the same monitors 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 All_Regions.ini file

  or

To retain AllRegions.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, 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.

> **Note:**
>
> The layout is overwritten with every save, and the layout is saved only on the active StoreFront.
>
> If you launch multiple desktop sessions from the same StoreFront on different monitors, saving the layout in one session saves the layout information of all the sessions.

Save layout

To enable the save layout feature:

1. Install the StoreFront 3.15 or later version (equal or greater than v3.15.0.12) on a compatible Delivery Controller (DDC).
2. Download the build of Citrix Workspace app 1808 or later for Linux from the Downloads page and then install it on your Linux machine.
3. Set the ICAROOT environment variable to the install location.
4. Check whether the **All_Regions.ini** file is present in the **.ICAClient** folder. If so, delete it.
5. In the **$ICAROOT/config/All_Regions.ini** file, look for the field – **SaveMultiMonitorPref**. By default, the value of this field is “true” (meaning this feature is turned on). To toggle off this

feature, set this field to false.

If you make any changes to the value of **SaveMultiMonitorPref**, you must delete the **All_Regions.ini** file present in the **.ICAClient** folder to prevent value mismatches and a possible profile lockdown. Set or unset the **SaveMultiMonitorPref** flag before launching sessions.

6. Launch a new desktop session.
7. Click **Save Layout** on the Desktop Viewer toolbar to save the current session layout. A notification appears at the bottom right of the screen, indicating success.

   When you click Save layout, the icon grays out. This indicates that saving is in progress. When the layout is saved the icon appears normal.

   However, if the icon is grayed out for a long time, see Knowledge Center article CTX235895 for troubleshooting information.
8. Disconnect or log off from the session.

   Relaunch the session. The session appears in the same mode, on the same monitor, and in the same position.

Limitations and unsupported scenarios:

- Saving a layout for windowed mode session spanning across multiple monitors is not supported due to limitations with the Linux Display manager.
- Saving session information across monitors with varied resolution is not supported in this release and might result in unpredictable behavior.
- Customers deployments with multiple StoreFront

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. Ensure 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.

Workspace launcher

Citrix introduces Workspace launcher (WebHelper) to launch published desktops and applications. Mozilla Corporation has announced that Netscape Plugin Application Programming Interface (NPAPI) support is deprecated as of version 52 of the Firefox browser. Other browsers, too, have deprecated support for NPAPI.

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.

Citrix Workspace launcher currently works not only with direct connections to StoreFront, but also through Citrix Gateway.

Keyboard layout synchronization

Keyboard layout synchronization between client and VDA enables you to switch among preferred keyboard layouts on the client device when using a Windows or a Linux VDA. This feature is disabled by default.

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 is dependent on XKB lib, which allows automatic keyboard layout synchronization between the VDA and the client device.
- When using a Windows Server 2016 or Windows Server 2019, navigate to the following path in the Registry Editor `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` and add a new DWORD value with key name `DisableKeyboardSync` and set the value to `0`.

To enable this feature, add the following lines to the module.ini file:

```
[ICA 3.0]

KeyboardSync=On

[KeyboardSync]

DriverName = VDIME.DLL
```

When you set **KeyboardSync=On** in the module.ini file and set **KeyboardLayout=(User Profile)** in the **wfclient.ini** file, the vdime virtual driver detects the active keyboard layout on the client and sends the information to VDA. When the keyboard layout changes in a client session, the vdime is aware and sends the new layout to VDA immediately.

To disable this feature, set **KeyboardSync=Off** in the module.ini file to revert to the earlier behavior. In the earlier behavior, the keyboard layout is read from the **$HOME/.ICAClient/wfclient.ini** file and sent to the VDA along with other client information when the session starts.

Usage

With this feature enabled, when the keyboard layout changes on the client device during a session, the keyboard layout of the session changes accordingly.

Keyboard layout support for Windows VDA and Linux VDA

> **Note:**
>
> The Linux keyboard locale for all the references in the following table is a hyphen.

Linux Keyboard Layout	Linux Keyboard / Linux VDA layout	Windows Locale	Windows Keyboard ID	Linux VDA Layout
ara	-	ar-SA	00000401	ara
ara	azerty	ar-DZ	00020401	ara
at	-	de-AT	00000407	at
be	iso-alternate	fr-BE	0000080c	be
be	-	nl-BE	00000813	be
bg	-	bg-BG	00030402	bg
bg	phonetic	bg-BG	00040402	bg
bg	bas_phonetic	bg-BG	00020402	bg
br	-	pt-BR	00000416	br
by	-	be-BY	00000423	by
ca	eng	en-CA	00000409	ca
ca	multix	fr-CA	00011009	ca
ca	fr-legacy	fr-CA	00000c0c	ca
ca	-	fr-CA	00001009	ca
ch	fr	fr-CH	0000100c	ch
ch	-	de-CH	00000807	ch
cn	-	en-US	00000409	us
cz	-	cs-CZ	00000405	cz
cz	qwerty	cs-CZ	00010405	cz
de	-	de-DE	00000407	de
de	mac	de-DE	00000407	de

Linux Keyboard Layout	Linux Keyboard / Linux VDA layout	Windows Locale	Windows Keyboard ID	Linux VDA Layout
dk	-	da-DK	00000406	dk
ee	-	et-EE	00000425	ee
es	-	es-ES	0000040a	es
es	mac	es-ES	0000040a	es
fi	-	fi-FI	0000040b	fi
fr	-	fr-FR	0000040c	fr
fr	mac	fr-FR	0000040c	fr
gb	-	en-GB	00000809	gb
gb	mac	en-GB	00000809	gb
gb	extd	en-GB	00000452	gb
gr	-	el-GR	00000408	gr
hr	-	hr-HR	0000041a	hr
hu	-	hu-HU	0000040e	hu
ie	-	en-IE	00001809	ie
il	-	he-IL	0002040d	il
in	eng	en-IN	00004009	in
iq	-	ar-IQ	00000401	iq
is	-	is-IS	0000040f	is
it	-	it-IT	00000410	it
jp	-	en-US	00000409	us
jp	mac	en-US	00000409	us
kr	-	en-US	00000409	us
latam	-	es-MX	0000080a	latam
lt	-	lt-LT	00010427	lt
lt	ibm	lt-LT	00000427	lt
lt	std	lt-LT	00020427	lt
lv	-	lv-LV	00020426	lv
no	-	nb-NO	00000414	no

Linux Keyboard Layout	Linux Keyboard / Linux VDA layout	Windows Locale	Windows Keyboard ID	Linux VDA Layout
pl	-	pl-PL	00000415	pl
pl	qwertz	pl-PL	00010415	pl
pt	-	pt-PT	00000816	pt
pt	mac	pt-PT	00000816	pt
ro	std	ro-RO	00010418	ro
rs	-	sr-Cyrl-RS	00000c1a	rs
rs	latin	sr-Latn-RS	0000081a	rs
ru	-	ru-RU	00000419	ru
ru	typewriter	ru-RU	00010419	ru
ru	mac	ru-RU	00000419	ru
se	-	sv-SE	0000041d	se
se	mac	sv-SE	0000041d	se
si	-	sl-SI	00000424	si
sk	-	sk-SK	0000041b	sk
sk	qwerty	sk-SK	0001041b	sk
th	-	th-TH	0000041e	th
th	pat	th-TH	0001041e	th
tj	-	tg-Cyrl-TJ	00000428	tj
tr	-	tr-TR	0000041f	tr
tr	f	tr-TR	0001041f	tr
tw	-	en-US	00000409	us
ua	-	uk-UA	00000422	ua
us	-	en-US	00000409	us
us	mac	en-US	00000409	us
us	dvorak	en-US	00010409	us
us	dvorak-l	en-US	00030409	us
us	dvorak-r	en-US	00040409	us
us	intl	nl-NL	00020409	us

Linux Keyboard Layout	Linux Keyboard / Linux VDA layout	Windows Locale	Windows Keyboard ID	Linux VDA Layout
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 below:

   `KeyboardLayout=(Server Default)`

   The default value for `KeyboardLayout` attribute is (User Profile).
3. Relaunch the session for the changes to take effect.

File type association

A Citrix Virtual Apps Services may 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 is a limitation to the type of files that are recognized by Citrix Workspace app for Linux. For the system to recognize the file type of the published content and for users to view it through Citrix Workspace app, a published application must be associated with the file type of the published file. 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 cannot view the published content.

To enable FTA on the client-side:

1. Ensure 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. Ensure that the file you are attempting 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

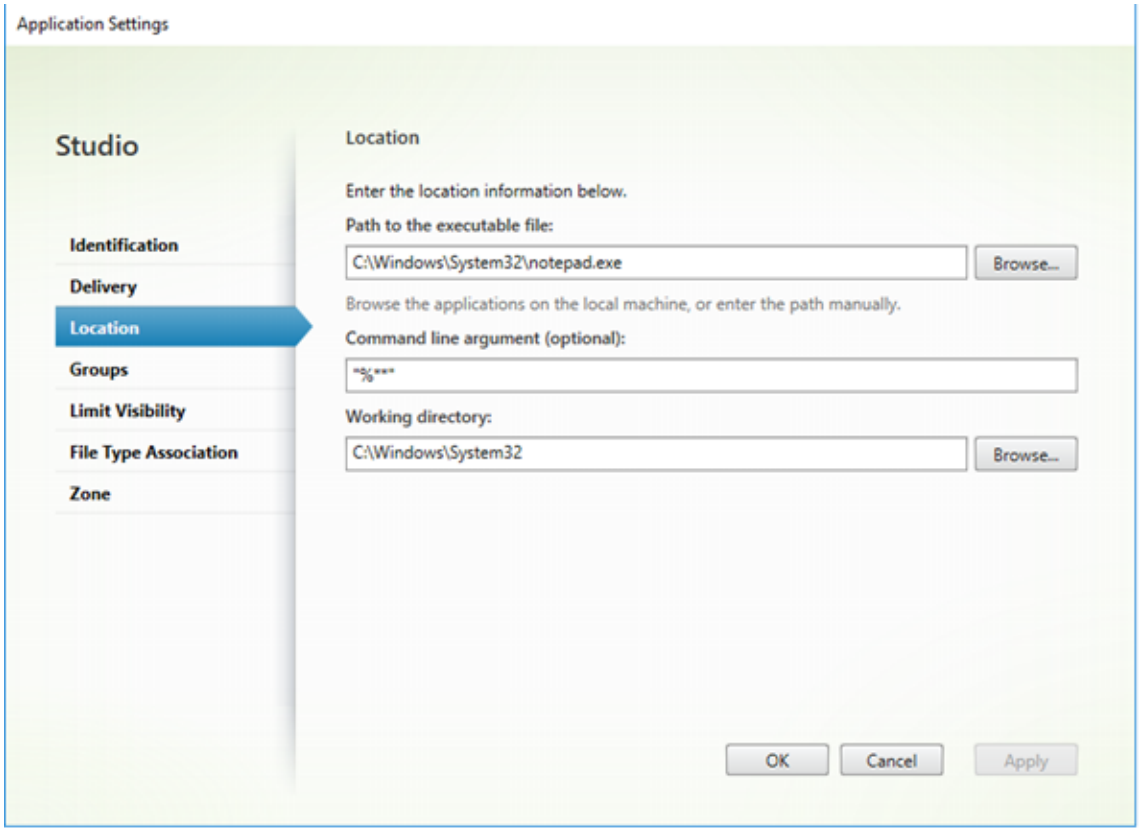
Citrix Workspace app reads and applies the settings configured by administrators in Citrix Studio.

Prerequisite:

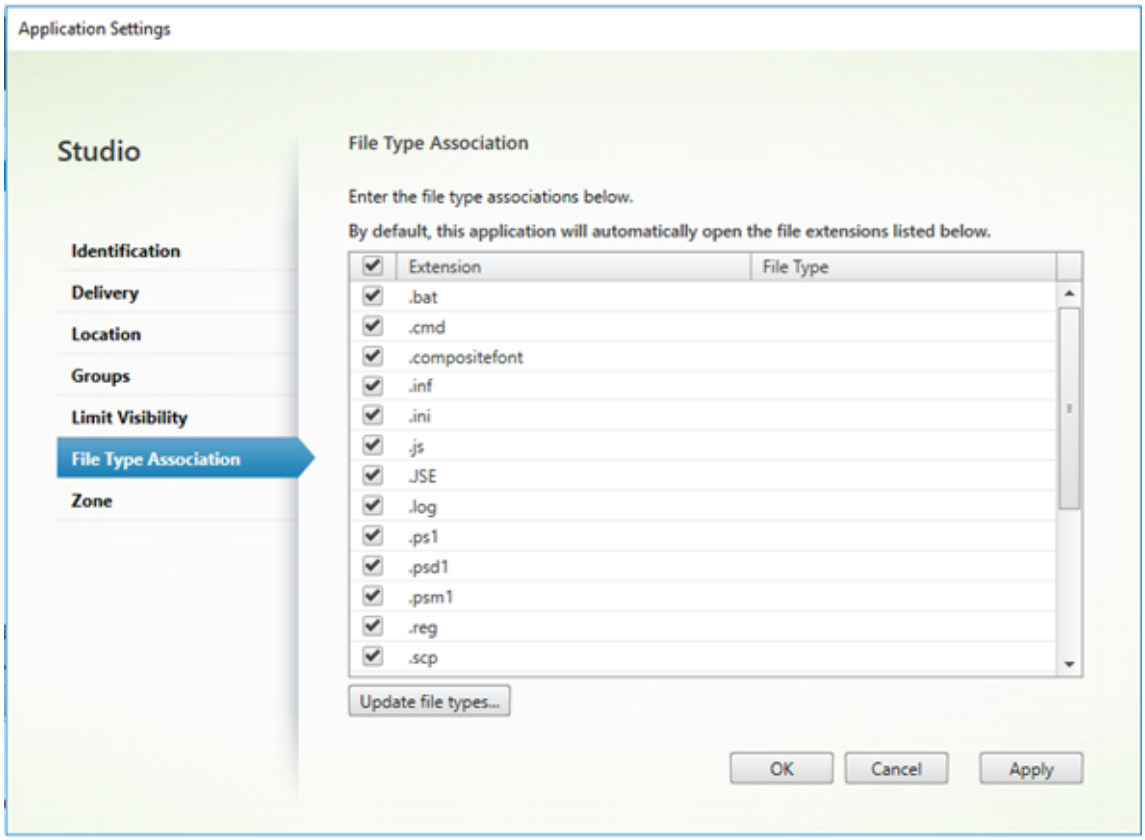
Ensure that you connect to the Store server where the FTA is configured.

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 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**.
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:**
>
> Ensure StoreFront file type association is ON. By default, file type association is enabled.

Authenticate

December 3, 2020

To provide a better experience, starting with Citrix Workspace app 2012, we present the authentication dialog inside Citrix Workspace app and show store details on the logon screen. We encrypt and store authentication tokens 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:

You must install the libsecret library.

This feature is disabled by default.

To enable this enhancement:

1. Locate the configuration file: `$ICAROOT/config/AuthManConfig.xml`.
2. Set the value of `AuthManLiteEnabled` to **`true`**.

Smart card

To configure smart card support in Citrix Workspace app for Linux, you must configure 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.

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 procedure below:

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. Alternatively, you can use an absolute path beginning with "/."

After you remove a smart card, configure the behavior of Citrix Workspace app by updating the `SmartCardRemovalAction` in the configuration file 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.

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 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 “libpscslite1” package must be present.

> **Important:**
>
> If you are using the SunRay terminal with SunRay server software Version 2.0 or later, install the PC/SC SRCOM bypass package, available for download from

http://www.sun.com/.

For more information about configuring smart card support on servers, see Smart cards in the Citrix Virtual Apps and Desktops documentation.

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide multiple proofs of identify 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 logon support already implemented for StoreFront. The web logon pages for Citrix Gateway and Traffic Manager virtual servers also consume this protocol.

For more information, see SAML authentication and Multi-Factor (nFactor) authentication in the Citrix ADC documentation.

Secure

January 28, 2021

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.

> **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 are 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 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 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 deployments only: Citrix Secure Web Gateway or SSL Relay solutions with Transport Layer Security (TLS) protocols. TLS versions 1.0 through 1.2 are supported.

Citrix Gateway

Citrix Gateway (formerly Access Gateway) secures connections to StoreFront stores, and 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. You can do this in one of these ways:
   - The first time you use the self-service user interface, you are 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 are 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 are 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 deployment. Citrix Workspace app supports the SOCKS protocol, along with the Citrix Secure Web Gateway and Citrix SSL Relay, the secure proxy protocol, and Windows NT Challenge/Response (NTLM) authentication.

The list of supported proxy types is restricted by the contents of Trusted_Regions.ini and Untrusted_Regions.ini to the Auto, None, and Wpad types. If you use the SOCKS, Secure or Script types, edit those files to add the additional types to the permitted list.

> **Note:**
>
> To ensure a secure connection, enable TLS.

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 is detected and used at run time without any additional configuration.

> **Important:**
>
> NTLM support requires the OpenSSL 1.1.1d and libcrypto.so libraries. Install the libraries on the user device. These libraries are often included in Linux distributions. You can also download 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 may 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 either Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app and the server. No configuration of Citrix Workspace app is required if you are using the Citrix Secure Web Gateway in Normal mode.

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. For more information, see the Citrix Virtual Apps (Citrix Secure Web Gateway) documentation.

If you are 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. Relay mode is not supported by Citrix Secure Web Gateway Version 2.0.

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.

SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the Citrix Virtual Apps 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

You can control the versions of the TLS protocol that can be negotiated by adding the following configuration options in the [WFClient] section:

- MinimumTLS=1.2
- MaximumTLS=1.2

These values are the default values, which are implemented in code. Adjust them as you require.

> **Note:**
>
> - 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.

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.

> **Note:**
>
> As with the TLS version configuration, if you change this after starting self-service or storebrowse you must type:
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

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. These cipher suites were deprecated in Citrix Receiver version 13.10 with an option for backward compatibility.

The TLS_RSA_ cipher suites have been removed entirely. Instead, it supports the advanced TLS_ECDHE_RSA_ cipher suites. If your environment is not configured with the TLS_ECDHE_RSA_ cipher suites, client launches are not supported due to 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

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 generally deprecated by the industry. However, to support backward compatibility with older versions of Citrix Virtual Apps and Desktops, Citrix Workspace app for Linux has an option to enable these cipher suites.

For better security, set the flag `Enable\\_TLS\\_RSA\\_` to `False`.

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 are insecure. 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 are using version 1901 and earlier, perform the following steps:

If .ICAClient is already present in the home directory of the current user:

- Delete `All\\_Regions.ini` file

Or

- To retain `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 is not present in the home folder of the current user, then it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the features is retained.

The following table lists the cipher suites in each set:
Table 1 – Cipher suite support matrix

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open		FIPS				SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

> **Note:**
>
> All cipher suites above 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.

Storebrowse

June 30, 2020

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.

Command usage

The following section details the storebrowse commands that you can use from the storebrowse utility.

-a, –addstore

Description:

Adds a new 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.

Command example on 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.

-?, -h, –help

Description:

Provides details on the storebrowse utility usage.

-l –liststore

Description:

Lists the stores that you have added.

Command Example on StoreFront:

```
./storebrowse -l
```

-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 on StoreFront:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-S –subscribed

Description:

Lists the subscribed 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.

Command example on StoreFront:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-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 on StoreFront:

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

where, 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 are not available through storebrowse, the output value is zero.

-s –subscribe

Description:

Subscribes the specified resource from a given store.

Command example on StoreFront:

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```


-u –unsubscribe

Description:

Unsubscribes the specified resource from a given store.

Command example on StoreFront:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

-L –launch

Description:

Launches a connection to a published resource. The utility then terminates automatically, leaving a successfully connected session.

Command example on StoreFront:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

-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 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 needed 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 on StoreFront:

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

-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 on StoreFront:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

-WD –disconnect

Description:

Disconnects all sessions of the specified store.

Command example on StoreFront:

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

-WT –logoff

Description:

Terminates all sessions of the specified store.

Command example on StoreFront:

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

-v –version

Description:

Displays the version of the storebrowse utility.

Command example on StoreFront:

```
./storebrowse -v
```

-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 on StoreFront:

```
./storebrowse -r /opt/Citrix/ICAClient
```

-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 are not cached. You must enter the details with every command.

Command example on StoreFront:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
user1 -P password -D domain-name
```

-d –deletestore

Description:

Deregisters a store with the ServiceRecord daemon.

Command example on StoreFront:

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```


-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 on StoreFront:

```
./storebrowse -c SharedUserMode=True
```

-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 on StoreFront:

```
./storebrowse -C <path to CR file>
```

-K –killdaemon

Description:

Terminates the storebrowse daemon. As a result, all credentials and tokens are purged.

Command example on StoreFront:

```
./storebrowse -K
```

-e –listerrorcodes

Description:

Lists the error codes that are registered.

Command example on StoreFront:

```
./storebrowse -e
```

-g –storegateway

Description:

Sets the default gateway for a store that is already registered with the ServiceRecord daemon.

Command example on 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.

-q, –quicklaunch

Description:

Launches an application using the direct URL. This command works only for StoreFront stores.

Command example on StoreFront:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```

-n –nosingleshot

Description:

Always daemonizes the storebrowse process.

Command example on StoreFront:

```
./storebrowse -n
```

-F –fileparam

Description:

Launches a file with the file path and the resource specified.

Command example on StoreFront:

```
./storebrowse -F "<path to file>" -L <Resource Name> <https://my.firstexamplestore
.net/Citrix/Store/discovery>
```

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 is 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 kills the storebrowse daemon. If you do not mention this command explicitly, the storebrowse process exits after an hour.

Troubleshoot

January 28, 2021

This article contains information to help administrators troubleshoot issues with Citrix Workspace app for Linux.

Connection

You might come across the following connection issues.

Published resource or desktop session

If, when establishing a connection to a Windows server, a dialog box appears with the message “Connecting to server…” but no subsequent connection window appears, you might need to configure the server with a Client Access License (CAL). For more information about licensing, see Licensing.

Session reconnection

Sometimes reconnecting to a session with a higher color depth than that requested by Citrix Workspace app causes the connection to fail. This failure is due to a lack 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. However, the second connection might also fail if there is still a lack of available memory on the server.

Full Internet name

Citrix recommends that you configure DNS (Domain Name Server) on your network to enable you to resolve the names of servers to which you want to connect. If you do not have DNS configured, it may not be possible to resolve the server name to an IP address. Alternatively, 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.

Proxy detection failure

If your connection is configured to use automatic proxy detection and you see a "Proxy detection failure: Javascript error" error message when trying to connect, copy the `wpad.dat` file into `$ICAROOT/util`. Run the following command, where host name is the hostname of the server to which you are trying to connect:

```
cat wpad.dat | ./pacexec pac.js FindProxyForURL <http://hostname>
hostname 2\>&1 | grep "undeclared variable"
```

If you get no output, there is a serious issue with the `wpad.dat` file on the server that you need to investigate. However, if you see output such as "assignment to undeclared variable …" you can fix the problem. Open `pac.js` and for each variable listed in the output, add a line at the top of the file in the following format, where "…" is the variable name.

```
var ...;
```

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).

Cipher suites

If your connection fails with the new cryptographic support:

1. You can use various tools to check what cipher suites your server supports, including:
   - `Ssllabs.com` (requires the server to have Internet access)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. In Linux Client WireShark find packet (Client Hello, Server Hello) with filter (ip.addr == VDAIPAddress) to find the SSL section. The result has the cipher suites sent by the client and accepted by the server.

Weak cipher-suites for SSL connections

When making a TLS connection, the Citrix Workspace app for Linux offers a more modern and restricted set of cipher suites by default. If you are 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 UDT protocol, you might see the error message: Connection to "…" has been lost. This issue can occur when the connection goes through a router with a Maximum Transmission Unit for UDT 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 cannot be contacted
- Your account cannot be added using this server address

Some problems might cause such errors, including:

- When the local computer and the remote computer cannot negotiate a common TLS protocol. For more information, see TLS.
- 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.
- When the remote computer requests a client certificate inappropriately. IIS should only **accept** or **require** certificates for Citrix, Authentication, and Certificate.
- Other problems.

Low-bandwidth connections

Citrix recommends that you use the latest version of Citrix Virtual Apps and Desktops on the server and Citrix Workspace app on the user device.

If you are 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 Virtual Apps and Citrix Workspace app for Linux** - 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. Although the data is captured at the VDA in a way that avoids tearing, and the data is passed to the client in a way that doesn't introduce tearing, 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 initiate the drawing of the next frame. There are some options when using Linux, depending on the graphics hardware you have on the client and what window manager you are using. These options are divided into two groups of solutions:

- 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"

```
1  Identifier    "Intel Graphics"
2  Driver        "intel"
3  Option        "AccelMethod" "sna"
```



```
4   Option        "TearFree" "true"
```

EndSection

For NVIDIA graphics, locate the file in the xorg.conf.d folder that contains 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:**
>
> Use "CompizConfig Settings Manager" with caution because incorrectly changing values can prevent the system from launching.

- Compton (an add-on utility). Refer to the man page/documentation for Compton for full details. For example, run the following command:

  ```
  compton --vsync opengl --vsync -aggressive
  ```

Incorrect keystrokes

If you are using a non-English language keyboard, the screen display may not match the keyboard input. In this case, you should specify the keyboard type and layout that you are 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 for linux creates window icons that are compatible with most window managers, but are not 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 is 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.
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

Users 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, or 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 multiple 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.

> **Important:**
>
> Span has no effect on Seamless or normal windowed sessions (including those 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 value is not recommended. It is intended as a last resort, for use with uncooperative window managers. The session window is not visible to the window manager, does not have an icon, and cannot 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 specify monitors at the top, bottom, left, and right edges of the area.

Assuming `o` was not specified, wfica uses the _NET_WM_FULLSCREEN_MONITORS message to request an appropriate window layout from the window manager, if it is 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 is no output, there is no support. If there is no support, you may need an override-redirect window. You can set up an override-redirect window using `-span o`.

To make a session that spans multiple 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.

3. At a command prompt, type:

   ```
   /opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
   ```

   where w, x, y, and z are monitor numbers obtained in step 1 above and 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, and 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 do this, 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 Citrix Virtual Apps and Desktops sessions.

   If you have started self-service or storebrowse, remove processes they started in order 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, 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 turn off 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 disables the Keyboard Transparency feature. However you might have to override the ICA file by adding this setting in the All_regions.ini file.

Browser

Local browser

When you click on a link in a Windows session, the content appears in a local browser. Server-client content redirection is enabled in wfclient.ini. This causes a local application to run. To disable server-client content redirection, see server-client content redirection.

Access published resources

When you access published resources, your browser prompts to save a file. Browsers other than Firefox and Chrome may 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 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.

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 are trying to access a resource through a desktop item or menu, but the Citrix Virtual Apps file for the resource is not 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, and the Citrix Virtual Apps file to which the icon or item refers.

PAC file errors

These errors might occur if your deployment uses proxy auto-configuration (PAC) files to specify proxy configurations.

Proxy detection failure: Improper auto-configuration URL.

An address in the browser was specified with an invalid URL type. Valid types are http:// and https://, and other types are not supported. Change the address to a valid URL type and try again.

Proxy detection failure: .PAC script HTTP download failed: Connect failed.

Check if an incorrect name or address was entered. If so, fix the address and retry. If not, the server could be down. Retry later.

Proxy detection failure: .PAC script HTTP download failed: Path not found.

The requested PAC file is not on the server. Either change this on the server, or reconfigure the browser.

Proxy detection failure: .PAC script HTTP download failed.

The connection failed while downloading the PAC file. Reconnect and try again.

Proxy detection failure: Empty auto-configuration script.

The PAC file is empty. Either change this on the server, or reconfigure the browser.

Proxy detection failure: No JavaScript support.

The PAC executable or the pac.js text file is missing. Reinstall Citrix Workspace app.

Proxy detection failure: JavaScript error.

The PAC file contains invalid JavaScript. Fix the PAC file on the server. Also see Connection.

Proxy detection failure: Improper result from proxy auto-configuration script.

A badly formed response was received from the server. Either fix this on the server, or reconfigure the browser.

Certificates

When you use a store with SAML authentication (using AUTHv3 protocol), the following error message appears: "Unacceptable TLS Certificate."

The issue occurs when you use Citrix Workspace app for Linux 1906 and later. For troubleshooting instructions, see Knowledge Center article CTX260336.

If your StoreFront server is unable to provide the intermediate certificates that match the certificate it is using, or you install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store:

1. Obtain one or more intermediate certificates separately in PEM format.

   > **Tip:**
   >
   > If you cannot 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 install 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 was issued by a certificate authority and is not yet trusted by the user device, follow these instructions before adding a StoreFront store:

1. Obtain the root certificate in PEM format.
   Tip: If you cannot 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`

Others

Connection issues

You might also encounter the following issues.

Close a session

If you want to know whether the server has instructed Citrix Workspace app to close a session, you can use the *wfica* program to log 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 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 logging, see Logging 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. In addition, 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. Under 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.

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 is not defined correctly. This 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 is likely that the ICAROOT environment variable is not 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 are 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 maps the local key combination Alt+Ctrl+F1 to Alt+F1:
  - Change Hotkey1Shift=Ctrl+Shift to Hotkey1Shift=Alt+Ctrl.
- Direct mode on the keyboard sends all key combinations directly to the server. They are not 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 use of a Japanese keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Japanese (JIS)

ABNT2 keyboard

To configure 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 normally causes the server to request a different format. Sometimes the initial check for a suitable plugin incorrectly indicates that one is present. This is normally detected and causes an error dialog to appear on the server indicating that Windows Media Player encountered a problem while playing the file. Retrying the file within the session typically works because the format is rejected by Citrix Workspace app. And as a result, the server either requests another format or renders the media itself.

In a few situations, the fact that there is no suitable plugin is not detected and the file is not played correctly, despite the progress indicator moving as expected in 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 plugin trace, or the mime-type that should 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 disables the format.
6. Repeat steps 2 - 5 (above) 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 may be possible to install a GStreamer plugin to decode it.

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:

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Errors

This topic contains a list of other common error messages you may 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 usually means the description given on the command line was not 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 cannot 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 may 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.

To obtain diagnostic information about Citrix Workspace app

1. In the installation directory, type util/lurdump. It is recommended that you do this while a session is open and, if possible, while the issue is occurring.

   A file is generated that contains detailed diagnostic information, including 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.

SDK and API

June 30, 2020

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) provides support for writing server-side applications and client-side drivers for additional virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers. 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.
- 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 have come up with the 'Platform optimization SDK' for enabling an ecosystem of low cost, low power, high performance devices with innovative form factors.

The Platform Optimization SDK can be used by developers looking to improve the performance of Linux-based devices by allowing them to create plug-in extensions for the ICA engine component

(wfica) of Citrix Workspace app for Linux. Plugins are built as shareable libraries that are dynamically loaded by wfica. These plugins 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.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States