Citrix Workspace app for Linux

Contents

About this release 3

Features in Technical Preview 32

System requirements and compatibility 44

Install, Uninstall, and Update 55

Get started 65

Configure 77

Authenticate 177

Secure communications 182

Storebrowse 191

Troubleshoot 202

SDK and API 226

ICA Settings Reference 227

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

About this release

September 20, 2023

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

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

What's new in 2308

HTTPS protocol support for proxy server

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

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

Support for MJPEG webcams

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

Supports system certificate paths for SSL connection

With this release, Citrix Workspace app supports system certificate paths for SSL connection. This feature simplifies the certificate management process on the client side and improves the user experience. With this feature, Citrix Workspace can create a TLS connection with the certificate in the system certificate path. This feature is enabled by default.

Enhanced virtual channel SDK

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

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

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

- Virtual driver viewport functions
- Programming reference

Support for keyboard shortcut to switch between Full-screen and Window mode

Previously, you could use either the **Window** or **Full-screen** button on the Desktop Viewer to toggle between **Full-screen** and **Window** mode.

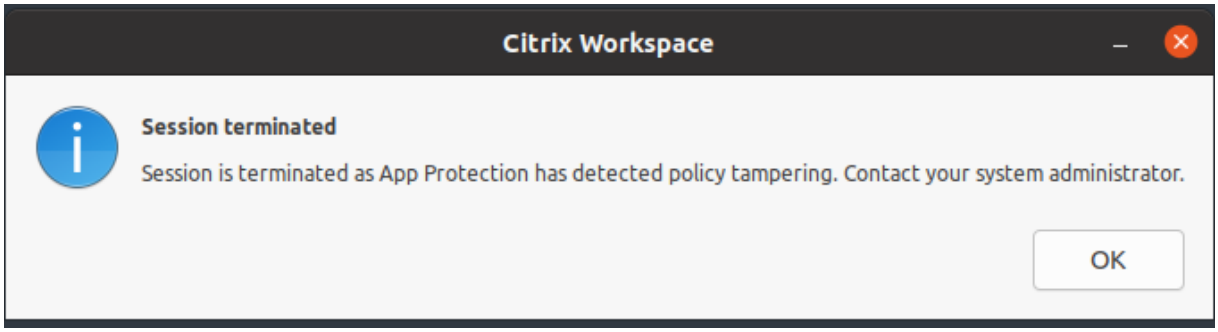
Starting with this release, you can use a keyboard shortcut Ctrl+F2 to switch between **Full-screen** and **Window** mode. For example, when the desktop session is in **Full-screen** mode, if you press "Ctrl+F2", the desktop session exits from the **Full-screen** mode.

This feature is disabled by default.

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

Policy tampering detection

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



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

Technical Preview

- Webcam redirection and service continuity support for ARM64 devices
- Enable Packet Loss Concealment to improve audio performance
- Multi-touch support

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

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

Fixed issues in 2308

- In a second hop scenario, you might be disconnected from the application that uses the Topaz USB Signature Pad or any other USB devices. This issue occurs when using the generic USB redirection feature in both hops. [CVADHELP-23053]
- After you upgrade Citrix Workspace app for Linux to 2206 or later versions, you might fail to sign in to Citrix Workspace app. This issue occurs only in the shared user mode when you sign in for the second or subsequent times. [CVADHELP-22775]
- When the Browser Content Redirection (BCR) feature is enabled, you might face disk space issues on thin clients. This issue occurs because the local cache of the redirected webpage is saved locally. [CVADHELP-21764]
- You might notice false HDMI audio devices detected inside the session. [CVADHELP-18849]
- When you install the 64-bit rpm package of Citrix Workspace app for Linux, you might get another requirements to install library package that are required for 32-bit. [CVADHELP-23347]
- You might not be able to enter text in the search box of redirected browser content on YouTube website when accessing in Full screen mode. This issue occurs with Citrix Workspace app for Linux 2106 or later. [CVADHELP-20399]
- You might need to authenticate twice when connecting to a PNA store by using Storebrowse -E or -S command. This issue occurs with Citrix Workspace app of Linux 2205 or later. [CVADHELP-22917]
- When you use the shortcut key "Ctrl + Alt + Enter", the keyboard might stop responding on pressing the "Enter" key. This issue occurs only in Linux VDA desktop session started from Citrix Workspace app for Linux. [CVADHELP-22930]
- The white cursor isn't clearly displayed on a dark blue or black background. This issue occurs in Citrix Workspace app for Linux version 2307. [HDX-52458]
- You might fail to use the sessions in **Full-screen** mode on both monitors, when the secondary monitor is plugged in after a session is started. [HDX-52816]
- You might not be able to redirect a USB storage device to an app or desktop in a double hop session. [HDX-52155]
- You might see a blank page for the content redirected using the Browser Content redirection feature on Chrome. This issue occurs when you access an allowed site with Citrix Workspace app for Linux 2305. [HDX-50561]

Known issues in 2308

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

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

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

Earlier releases

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

2307

What's new

Script to verify system requirements for Windows Media Player redirection

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

Added support for playing short tones in optimized Microsoft Teams

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

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

Prerequisites:

Update to the latest version of Microsoft Teams.

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

Technical Preview

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

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

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

Fixed issues

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

2305

What's new

Enhancement to support keyboard layout synchronization for GNOME 42

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

For more information, see Keyboard layout synchronization section.

Client IME for East Asian languages

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

- you have a favorite IME in Linux Client or,
- IME is not available from the remote server.

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

Addition of client-side jitter buffer mechanism

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

Webcam redirection for 64-bit

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

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

Support for more than 200 groups in Azure AD

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

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

Support for App Protection on Ubuntu 22.04

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

Enhancement to sleep mode for optimized Microsoft Teams call

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

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

Improved experience for optimized Microsoft Teams video conference calls

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

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

Technical Preview

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

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

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

Fixed issues

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

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

2303

What's new

Persistent login

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

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

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

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

For more information, see Persistent login.

Support for authentication using FIDO2 in HDX session

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

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

By default, FIDO2 authentication is disabled.

For more information, see Support for authentication using FIDO2.

Improved audio echo cancellation support

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

For more information, see Improved audio echo cancellation support

Inactivity Timeout for Citrix Workspace app

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

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

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

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

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

Background blurring for webcam redirection

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

For more information, see Background blurring for webcam redirection.

Configure path for Browser Content Redirection overlay Browser temp data storage

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

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

Support for new PIV cards

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

- IDEMIA next-generation smartcard
- DELL TicTok Smartcard

Performance optimization for smartcard driver

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

Microsoft Teams enhancements

Configuring a preferred network interface

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

For more information, see Configuring a preferred network interface.

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

Fixed issues

- When you access Hyperspace over Citrix Virtual Apps, the sign-in page that is specific to Hyperspace might appear on top of the apps that are already started. [CVADHELP-20368]
- When you access a second application, the current session might close and the session might restart. The data from the previous session might not be present and the data is updated as if the session started at the time the second application was started. This issue doesn't occur when you start the initial application in a session. [CVADHELP-21914]
- You might not be able to update the 24-hour time format under the **Selfservice** > **Profile** > **Account Setting** > **Regional Setting** > **Time format** section. This issue occurs only in a cloud store. [CVADHELP-20866]
- The session might close abruptly after you unplug the USB device while you drag multiple files from the VDA session to the USB device. This issue occurs only on Ubuntu. [HDX-30219]
- You might experience performance issues when signing in to the Citrix Workspace app using a smart card with the VDSCARDV2.DLL driver version. This issue occurs on eLux distributions only. [HDX-44314]

2302

What's new

Inactivity Timeout for Citrix Workspace app [Technical Preview]

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

The inactivity timeout value can be set starting from 10 minutes to 1440 minutes. The interval to change this timeout value must be in multiples of 5. For example: 10, 15, 20, or 25 minutes. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module.

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

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

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not ac-

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

> cept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Support for Korean language

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

Performance optimization for Citrix Workspace app

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

Technical Preview

- Screen pinning in custom web stores

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

Fixed issues

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

2212

What's new

Addition of client-side jitter buffer mechanism [Technical Preview]

This feature ensures smooth audio even when the network latency fluctuates. By default, this feature is disabled.

To enable this feature, do the following:

1. Navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file and edit it.
2. Disable audio latency control as follows:

```
`AudioLatencyControlEnabled = FALSE`
```

3. Enable jitter buffer as follows:

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

```
`JitterBufferEnabled = TRUE`
```

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Support for multiple audio devices

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

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

Support for audio recording

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

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

Technical Preview

- Support for 32-bit cursor
- Background blurring and replacement for Citrix Optimized Microsoft Teams

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

Fixed issues

- You might not find a valid smartcard certificate after you remove the smartcard and insert again. [CVADHELP-20787]
- You might fail to sign in to Citrix Workspace app using the TicTok smartcard. [CVADHELP-20578]
- You might fail to sign in to Citrix Workspace app using the smartcard from IDEMIA. [CVADHELP-20652]
- The Citrix Workspace app might stop responding when audio redirection is using the Speex codec with multiple audio devices enabled. [CVADHELP-21212]

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

- When you sign out from the Citrix Workspace app and sign in again, the Citrix Workspace app starts without entering the sign-in credentials. This issue occurs only in cloud deployments and if the `longLivedTokenSupport` parameter value is set to *True*. [RFLNX-9160]
- Transaction ID error messages might appear when you start a session. For example: "The option "-transactionid" is invalid". [HDX-45618]
- When you install Citrix Workspace app and start the session with root privileges, the session might exit. [HDX-46967]
- When you install and start Citrix Workspace app, the following error message might appear:

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

2211

What's new

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

Fixed issues

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

2209

What's new

Support for authentication using FIDO2 [Technical Preview]

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

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

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

By default, FIDO2 authentication is disabled. To enable FIDO2 authentication, do the following:

1. Navigate to the `<ICAROOT>/config/module.ini` file.
2. Go to the ICA 3.0 section.
3. Set `FIDO2= On`.

This feature currently supports roaming authenticators (USB only) with PIN code and touch capabilities. You can configure FIDO2 Security Keys based authentication. For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.

When you access an app or a website that supports FIDO2, a prompt appears, requesting access to the security key. If you've previously registered your security key with a PIN (a minimum of 4 and a maximum of 64 characters), you must enter the PIN while signing in.

If you've registered your security key previously without a PIN, simply touch the security key to sign in.

Limitation:

You might fail to register the second device to a same account using FIDO2 authentication.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Microsoft Teams enhancements

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

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

- **WebRTC SDK upgrade:** The version of the WebRTC SDK that is used for the optimized Microsoft Teams is upgraded to version M98.

Upgraded version of compatibility libraries

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

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

App Protection update

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

Technical Preview

- Keyboard input mode enhancements
- Support for extended keyboard layouts

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

Fixed issues

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

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

2207

What's new

Enhancement to improve audio quality

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

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

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

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

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

Composite USB device redirection

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

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

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

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

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

Improved audio echo cancellation support [Technical Preview]

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

By default, the echo cancellation feature is disabled. During real-time user cases, it's recommended to turn on the echo cancellation if the speaker is used instead of the headset.

Limitation:

By design, the echo cancellation feature is disabled for high quality audio.

For more information, see the **Improved audio echo cancellation support** section in the Audio documentation.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

Support for secondary ringer

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

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

Technical Preview

- Support for DPI matching

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

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

Fixed issues

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

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

uration differs between the protocols, and the client cannot connect via one protocol. [RFLNX-8747]

- When you try to connect remotely to a machine that has Citrix Workspace app with App Protection installed, the x11vnc server crashes and the connection fail. As a result, you might not be able to connect remotely to the machine through the x11vnc server. [RFLNX-8933]
- When you add a store with default settings, the Storebrowse enumeration might fail. This issue occurs only in the Debian 32-bit OS. [RFLNX-8743]
- You might get an error message when you install the Citrix Workspace app with App Protection feature enabled on 32-bit Linux machines. [RFLNX-8809]
- When you add a store using the `storebrowse -a` command and enumerate using the `storebrowse -E` command, the Storebrowse enumeration might fail. This issue occurs only in the Raspberry Pi OS. [RFLNX-8803]

2205

What's new

Authentication enhancement for Storebrowse

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

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

The authentication enhancement supports storebrowse for the following operations:

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

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

> **Note:**
>
> - You can continue to use the remaining storebrowse commands as used earlier (using AuthMangerDaemon).
> - The authentication enhancement is applicable for cloud deployments only.
> - With this enhancement, the persistent login feature is supported.

For more information, see the Authentication enhancement.

Persistent login [Technical Preview]

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

With this functionality, the SSO to Citrix DaaS sessions is extended up to a period of 365 days. This extension is based on the lifetime of Long-Lived Tokens. Your credentials are cached by default for 4 days or Lifetime whichever is lower. And, then extended when you become active within these 4 days by connecting to the Citrix Workspace app.

> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds aren't deployed in production environments.

For more information, see Persistent login.

Email-based auto-discovery of store

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

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

Fixed issues

- The DNS server in a customer environment with limited internet access might not resolve the URL, `clientstream.launchdarkly.com`. As a result, Citrix Workspace app sends many DNS queries (>1000 within three seconds per day) to the URL. [CVADHELP-19559]

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

- When the App Protection feature is enabled, the anti-keylogging functionality might not work for the Authentication Manager interface that uses the `UIDialogLibWebKit3.so` library. This issue is resolved in the GNOME and KDE desktop environment. [RFLNX-8027]
- Attempting to print from a VDA session running on Raspberry Pi ARMHF client version 3 or 4 might make the session unresponsive. [CVADHELP-18506]
- When you launch the self-service user interface with the default settings, the following error message might appear:

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

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

2203

What's new

Support for EDT IPv6

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

Support for TLS protocol version 1.3

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

Custom web stores

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

> **Note:**
>
> The Pinning multi-monitor screen layout feature is not supported in the custom web store.

For more information, see Custom web stores.

Authentication enhancement experimental feature

Starting with this release, authentication enhancement supports storebrowse for the following operations:

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

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

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

For more information, see Authentication enhancement for Storebrowse.

Keyboard layout synchronization enhancement

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

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

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

For more information, see Keyboard layout synchronization.

Multi-window chat and meetings for Microsoft Teams

You can use multiple windows for chat and meetings in Microsoft Teams, when optimized by HDX in Citrix Virtual Apps and Desktops 2112 or higher. You can pop out the conversations or meetings in various ways. For details about the pop-out window feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings.

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

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

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

Enhancement to auto-redirection of USB devices

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

Fixed issues

- When you add a store and authenticate it to the Citrix Workspace app, the authentication window is loaded for the second time, even after successful authentication. This issue occurs when you first sign into the Citrix Workspace app after setting the `AuthManLiteEnabled` to **True**. [RFLNX-8694]
- After you install the Citrix Workspace app with App Protection feature enabled on the OS that uses `glibc 2.34` or later, the OS boot might fail on restarting the system. [RFLNX-8358]
- When you are using Microsoft Teams to make a P2P call or to attend a meeting, and wait for some time, the load for one CPU core might increase to 100% due to socket error. [HDX-38974]
- Citrix Workspace app does not support the new version of Raspberry Pi OS based on the Debian bullseye. [HDX-37000]
- When you launch a session with the ICA file and sign off from the session, the expected return value that you receive from the `wfica` command line is 0. However, instead of the expected value, the value that you receive is 2. This issue occurs in Citrix Workspace app version 2106 or later. [HDX-38916]
- In Citrix Workspace app, you might experience intermittent failures when answering or making a Microsoft Teams call. The following error message appears:

  “Call could not be established.”

  [HDX-38819]

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

Known issues

Known issues in 2307

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

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

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

Known issues in 2305

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

Known issues in 2303

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

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

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

Known issues in 2211

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

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

- When you install and start Citrix Workspace app, the following error message might appear:

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

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

  As a workaround, navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file and replace `IgnoreErrors=9,15` with `IgnoreErrors=9,15,32`. [HDX-44416]

- When you sign out from the Citrix Workspace app and sign in again, the Citrix Workspace app starts without entering the sign-in credentials. This issue occurs only in cloud deployments and if the `longLivedTokenSupport` parameter value is set to *True*. As a workaround, do the following:

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

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

  [RFLNX-9160]

Known issues in 2209

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

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

  [HDX-39764]

- Attempts to start a server VDA session using smart card authentication might fail for a smart card with multiple users. As a workaround, reinsert the card. [HDX-44255]

- The VDA might crash after redirecting the interface of the device. This issue occurs when you enable the "Client USB device redirection" policy on DDC and attach composite USB devices to the endpoint, such as the USB Headset. Also, add the input value in the usb.conf file as `vid=** pid=** split=01 and intf=00,01`. After that you start the session from Citrix Workspace app and set redirect the interface of a device. [HDX-44117]

- The session launch might fail on the Raspberry Pi ARMHF OS based on Debian 11. Citrix recommends you to use Raspberry Pi ARM64 OS based on Debian 11 or older Raspberry Pi ARMHF OS based on Debian 10. [HDX-41729]

- When you remove a primary account, the sign-in credentials might not be deleted from the selfservice cache. As a result, you might be able to sign-in to the store without providing credentials. As a workaround, quit the selfservice to delete the credentials. [RFLNX-9051]

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

- After you provide the sign-in credentials and start selfservice, a white screen might appear. As a workaround, quit the selfservice and restart it. [RFLNX–8951]
- In OpenSUSE SLES 15, you might get a spinning wheel when you connect to a cloud store. [RFLNX–9109]
- You might fail to start Selfservice on RHEL9 and Fedora 36. As a workaround, ensure that the value of `AuthManLiteEnabled` is set to *False* in the `$ICAROOT/config/AuthManConfig.xml` file. [RFLNX-9128]

Known issues in 2207

- The DNS polling for CAS data collection might occur for direct ICA launch and for CAS disabled stores. [CVADHELP-20018]
- When using storebrowse commands, if you add and enumerate a second store, you might fail to launch the apps or desktops from the first store. As a workaround, you must enumerate the specific store again before launching any apps or desktops. [RFLNX-8953]
- In a desktop session, when you play a video using Windows Media Player, the mouse cursor might disappear on the rave video. This issue occurs only if you have set the following policies in DDC as follows:
  - "Use video codec for compression" as "For actively changing regions"
  - "Windows Media redirection" as "Allowed" (Default setting)
  - "Browser Content Redirection" as "Allowed" (Default setting)
  - "InvertCursorEnabled" as "BOTH" and the following values are added in the ~/.ICAClient/wfclient.ini file:
    - InvertCursorEnabled=True
    - InvertCursorRefreshRate=60
    - InvertCursorMode=1

[HDX-37259]

Known issues in 2205

- You might experience the session disconnection issues when connected through the Citrix Workspace app for Linux 2205 version endpoints. This issue occurs if you configure the lock screen using the **Force a specific default lock screen image** policy setting with certain types of JPEG file type and apply to the Citrix VDA 2203. As a workaround, upgrade to the Citrix Workspace app version 2207 or later. [CVADHELP-21572]
- When an SSL error occurs on one protocol during a TCP and EDT/UDP connection attempt, both connections might fail because of the race condition. This SSL error can occur if the TLS con-

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

figuration differs between the protocols, and the client cannot connect via one protocol. As a workaround, set the HDXoverUDP attribute to On or Off in the ICA file. [RFLNX-8747]

- HDX RealTime Webcam video compression does not support camera with MJPEG video format in Citrix Workspace app. [HDX-40352]
- The video or an image in Citrix Workspace app might not render correctly. This issue occurs when Citrix Workspace app is used along with VDA version 2109 or later. As a workaround, do the following.

  1. Sign into Citrix Studio.
  2. Edit the Use video codec for compression policy settings.
  3. Select the **For the entire screen** option from the **Value** drop-down list. [HDX-40287]

- When you add a store using the `storebrowse -a` command and enumerate using the `storebrowse -E` command, the Storebrowse enumeration might fail. This issue occurs only in the Raspberry Pi OS. As a workaround, do the following:

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

```
<StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
<!--NeedCopy-->
```

  [RFLNX-8803]

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

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

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

  [RFLNX-8743]

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

Known issues in 2203

- When launching a published Remote Desktop Protocol (RDP) application with multiple monitors in an Ubuntu endpoint, only one monitor displays content even though the client machine

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

has multiple monitors. The “Use all my monitors for the remote session” checkbox in the display option of RDP application is selected before connecting to a remote desktop through RDP. The issue occurs in the seamless mode and multi-monitor setup. [CVADHELP-16768]

- Citrix Workspace app does not pass the `Clientname` and `clientaddress` parameters to DDC during resource enumeration. As a result, `Set-BrokerAccessPolicyRule` filtered with client name or client IP might not work properly. [CVADHELP-17667]
- When you preview a video using the webcam in the Skype, the preview might show a black screen. [HDX-37860]

Known issues in 2112

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

Known issues in 2111

- When you log on to a cloud store, the screen might appear in white. [RFLNX-8337]
- When you try to launch Citrix Workspace app, the self-service user interface might fail to open, and the following error message appears:

  “User-defined signal 2”

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

Known issues in 2109

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

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

Known issues in 2108

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

Known issues in 2106

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

Known issue in 2103

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

Known issues in 2101

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

Legacy documentation

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

Third-party notices

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

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

Experimental features

On occasion, Citrix releases experimental features as a mechanism for seeking customer feedback on the potential desirability of new technologies or features. Citrix does not accept support cases for experimental features but welcomes feedback for improving them. Citrix might or might not act on

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

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.

Features in Technical Preview

September 18, 2023

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

Webcam redirection and service continuity support for ARM64 devices

This feature is in technical preview from 2308 release.

The following features are supported on ARM64 architecture-based endpoint devices running Citrix Workspace app for Linux:

- Webcam redirection
- Service continuity

For more information, see Support for ARM64 architecture.

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

Enable Packet Loss Concealment to improve audio performance

This feature is in technical preview from 2308 release.

The jitter buffer mechanism is improved, and the Packet Loss Concealment (PLC) is added for both Speex and Opus codec. The enhanced jitter buffer mechanism can detect the out-of-order data packers and reorder them correctly. PLC helps to reconstruct the lost data packets. This enhancement helps to improve the packet loss tolerance and jitter tolerance and thus increases audio performance for UDP audio. By default, this enhancement is disabled.

To enable this enhancement, do the following:

1. Navigate to the /opt/Citrix/ICAClient/config/module.ini configuration file and edit it.
2. Enable jitter buffer as follows:

```
JitterBufferEnabled = TRUE
<!--NeedCopy-->
```

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

3. Enable PLC as follows:

```
PacketLossConcealmentEnabled=TRUE
<!--NeedCopy-->
```

4. Enable UDP audio feature.

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

Multi-touch support

This feature is in technical preview from 2308 release.

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

- **Select an item**: Tap on the touchpad.
- **Scroll**: Place two fingers on the touchpad and slide horizontally or vertically.
- **Zoom in or out**: Place two fingers on the touchpad and pinch in or stretch out.
- **Show more commands (similar to right-clicking)**: Tap the touchpad with two fingers, or press in the lower-right corner.

Known limitation:

- Doesn't support session reliability, which means no touch event cache is stored.
- Doesn't support on Linux VDA

Known issues:

- Multi-touch isn't supported on multi-monitors for which the display mode is set as **Join Displays** (extended mode). [HDX-52394]
- You might not be able to press a finger on the screen and hold it on the ASUS touch screen. [HDX-52521]

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

Support for authentication using FIDO2 when connecting to on-premises stores

This feature is in technical preview from 2308 release.

Users can authenticate using passwordless FIDO2 security keys when signing in to on-premises stores through Citrix Workspace app for Linux. The security keys support different types of security inputs

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

such as security pins, biometrics, card swipe, smart card, Public Key Certificates, and so on. For more information about FIDO2 see FIDO2 Authentication.

Citrix Workspace app uses the Citrix Enterprise Browser as the default browser for FIDO2 authentication. Administrators can configure the type of browser to authenticate to Citrix Workspace app.

To enable the feature, navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
    <key>FIDO2Enabled</key>
    <value>true</value>
<!--NeedCopy-->
```

To modify the default browser, navigate to `$ICAROOT/config/AuthManConfig.xml` and modify the browser settings as required. The possible values are `CEB`, `chromium`, `firefox`, and `chromium-browser`.

```
    <FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>
<!--NeedCopy-->
```

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

Support for IPv6 UDT with DTLS

This feature is in technical preview from 2307 release.

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

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

This feature is enabled by default.

No additional configuration is required when you use IPv6 DTLS direct connection with VDA on Citrix Workspace app for Linux.

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

App Protection support for ARM64 devices

This feature is in technical preview from 2307 release.

App Protection is supported on ARM64 architecture-based devices running Citrix Workspace app for Linux. For more information, see Support for ARM64 architecture.

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

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

Support for IPv6 TCP with TLS

This feature is in technical preview from 2305 release.

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

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

This feature is enabled by default.

No additional configuration is required when you use IPv6 TLS direct connection with VDA on Citrix Workspace app for Linux.

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

Enhancement on 32-bit cursor support

This feature is in technical preview from 2305 release.

Starting with Citrix Workspace app for Linux version 2212, support for the 32-bit cursor was enabled by default.

Starting with 2305 release, you can disable the support for the 32-bit cursor. For this enhancement, a new parameter named `Cursor32bitSupport` is added in the `wfclient.ini` file.

To disable support for the 32-bit cursor, see Support for 32-bit cursor documentation.

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

Support for authentication using FIDO2 when connecting to on-premises stores

This feature is in technical preview from 2305 release.

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

Citrix Workspace app uses the Citrix Enterprise Browser as the default browser for FIDO2 authentication. Administrators can configure the type of browser to authenticate to Citrix Workspace app.

To enable the feature, navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

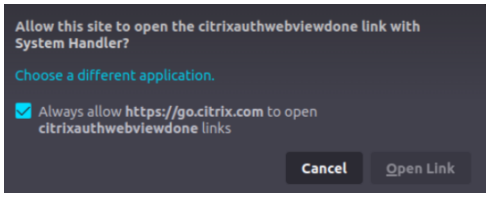
```
1 ```
2 <key>FIDO2Enabled</key>
3 <value>true</value>
4 <!--NeedCopy--> ```
```

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

To modify the default browser, navigate to `$ICAROOT/config/AuthManConfig.xml` and modify the browser settings as required. The possible values are `CEB`, `chromium`, `firefox`, and `chromium-browser`.

```
1 ```
2 <FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>
3 <!--NeedCopy--> ```
```

For user permissions, when you open the browser for the first time after the FIDO2 authentication, the following dialog box appears:



> **Note:**
>
> The preceding dialog box appears only if you select a browser other than Citrix Enterprise Browser.

Select the **Always allow https://go.citrix.com to open citrixauthwebviewdone links** checkbox and click **Open Link**.

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

Copy and paste files and folders between two virtual desktops

This feature is in technical preview from 2305 release.

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

This feature is enabled by default.

> **Note:**
>
> Copy and paste files and folders between two virtual desktops is supported only on the x64 Linux distribution and on the ARM64 architectured-based devices running Citrix Workspace app for Linux.

To disable this feature, do the following:

1. Navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file.
2. Edit the value of `VDGDT` to `Off`.

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

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

Support for ARM64 architecture

This feature is in technical preview from 2305 release.

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

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

Hardware acceleration support for optimized Microsoft Teams

This feature is in technical preview from 2305 release.

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

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

Prerequisite:

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

```
1 ```
2 sudo apt install va-driver-all
3 <!--NeedCopy--> ```
```

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

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

```
1 ```
2 {
3   "VideoHwEncode": 1,  }
4
5 <!--NeedCopy--> ```
```

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

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

Screen pinning in custom web stores

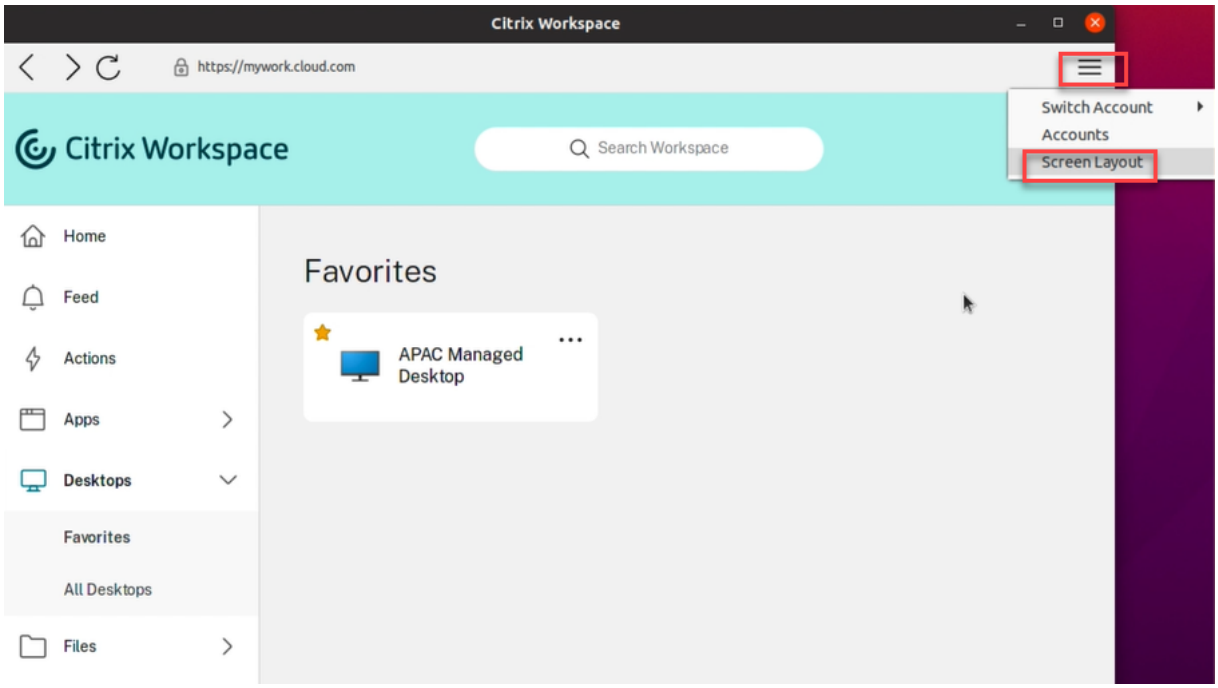
This feature is in technical preview from 2302 release.

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

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

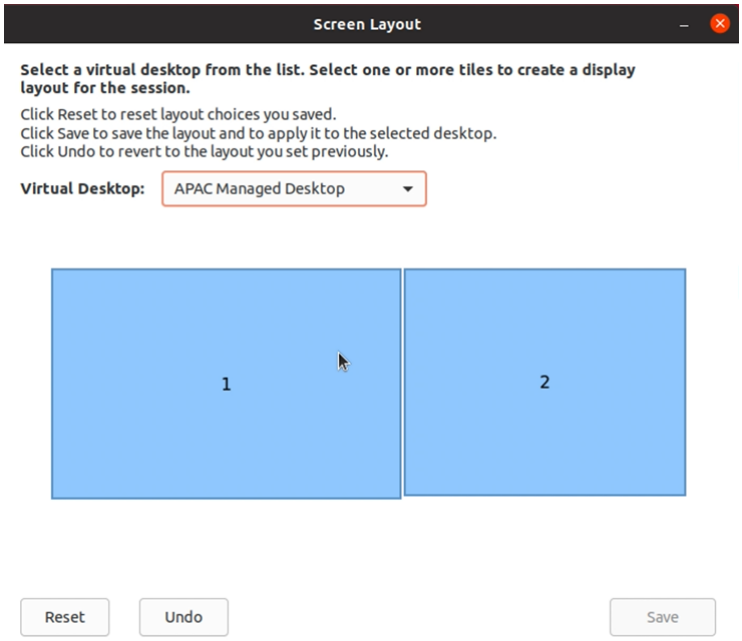
```
<key>ScreenPinEnabled</key>
<value> true </value>
<!--NeedCopy-->
```

Only after adding the preceding key, you can see the **Screen Layout** option in the Citrix Workspace app menu.



To select the screen layout, select **Screen Layout** in the Citrix Workspace app menu. The **Screen Layout** dialog box appears.

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



Select a virtual desktop from the drop-down menu. The layout selection is applied only to the desktop that you select.

Select one or more tiles to form a rectangular selection for the layout. The session then appears as per the layout selection.

Limitations:

- Enabling screen pinning disables the save layout feature in a session.
- This feature is applicable only on desktops that are marked as favorite.

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

Support for 32-bit cursor

This feature is in technical preview from 2212 release.

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

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

Starting with the 2305 version, you can disable the support for the 32-bit cursor. For this enhancement, a new parameter named `Cursor32bitSupport` is added in the `wfclient.ini` file.

To disable support for the 32-bit cursor, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Go to the [Thinwire3.0] section and set the following entry:

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

```
Cursor32bitSupport = False
<!--NeedCopy-->
```

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

Background blurring and replacement for Citrix Optimized Microsoft Teams

This feature is in technical preview from 2212 release.

Prerequisite:

Ensure that you have installed wget.

Starting with version 2212 for Citrix Workspace app, Citrix Optimized Microsoft Teams in Citrix Workspace app for Linux now supports background blurring and background replacement. You can use this feature by selecting **More** > **Apply Background Effects** when you are in a meeting or in a P2P call.

Keyboard input mode enhancements

This feature is in technical preview from 2209 release.

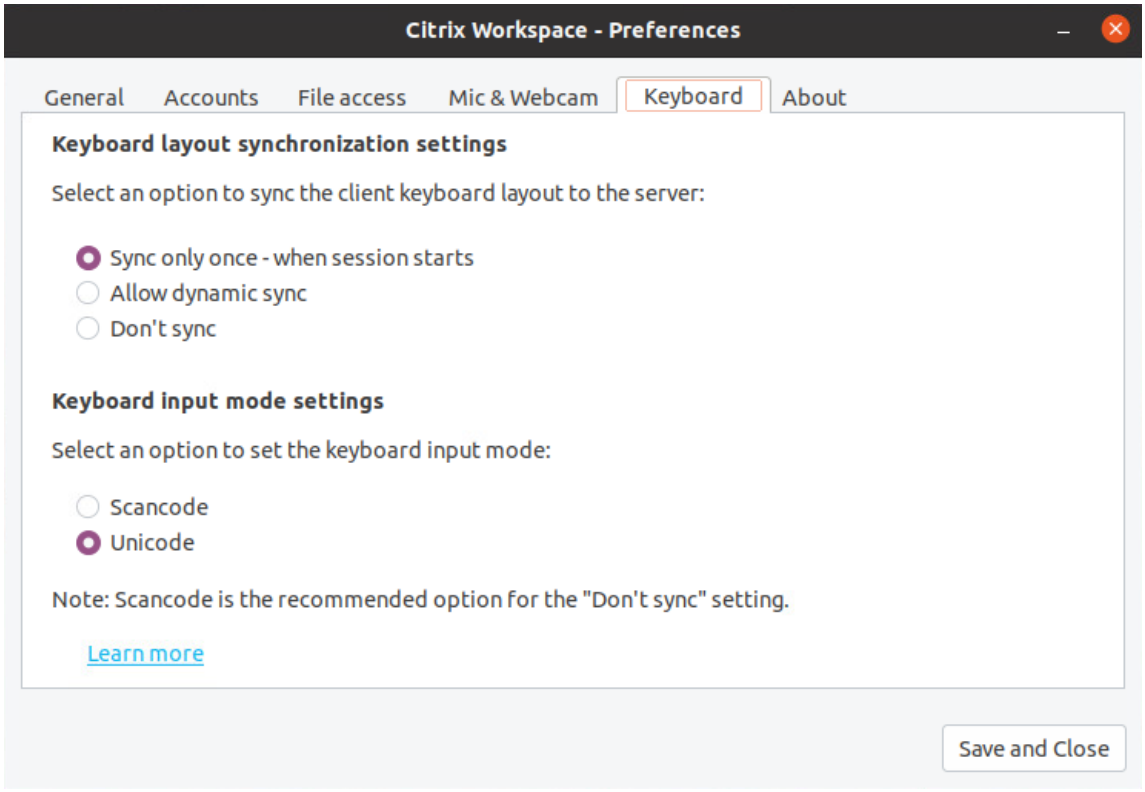
Previously, you were able to enable different keyboard input modes only by updating the value of `KeyboardEventMode` in the configuration file. There was no UI option to select the keyboard input mode.

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

To configure keyboard input mode by using the GUI, do the following:

1. From the Citrix Workspace app icon in the notification area, select **Preferences**.
   The **Citrix Workspace – Preferences** dialog box appears.
2. Click Keyboard.
   You can see the **Keyboard input mode settings** section.

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



3. Select one of the following options:

   - **Scancode** – Sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
   - **Unicode** - Sends the key from the client-side keyboard to VDA and VDA generates the same character in VDA. Applies client-side keyboard layout.

   By default, the Keyboard input mode setting is selected as **Unicode**. For more information on keyboard input mode, see the **Configure keyboard layout** section in the Keyboard layout synchronization documentation.

4. Click **Save and Close**.

> **Note:**
>
> The keyboard configuration changes take effect once you reconnect to the application. If you change the keyboard input mode in the UI, the parameter value of the `KeyboardEventMode` in the `wfclient.ini` file is also updated automatically.

For example, consider a scenario where you're using a US international keyboard layout and the VDA is using the Russian keyboard layout.

When you choose **Scancode** and type the key next to Caps lock, the scancode `1E` is sent to the VDA. The VDA then uses `1E` to display the character ф.

If you choose **Unicode** and type the key next to Caps lock, the character `a` is sent to the VDA. So, even

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

if the VDA uses the Russian keyboard layout, the character a appears on the screen.

Support for extended keyboard layouts

This feature is in technical preview from 2209 release.

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

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

The Scancode keyboard input mode supports the extended keyboard layouts along with all keyboard layout synchronization modes.

This support is enabled by default. However, perform the following extra steps to configure the "Japanese 106 keyboard":

1. Navigate to the $HOME/.ICAClient/wfclient.ini configuration file.
2. Add the following entries:

```
KeyboardType = 106 Keyboard (Japanese)
<!--NeedCopy-->
```

Support for DPI matching

This feature is in technical preview from 2207 release.

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

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

- Applications
- Text
- Images
- Other graphical elements

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

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

1. Navigate to the $HOME/.ICAClient/wfclient.ini configuration file.

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

2. Go to [WFClient] section and set the following entry:

   DPIMatchingEnabled=TRUE

Limitation:

Currently, the DPI matching feature does not support the fractional scaling on the client side.
If the DPI scale value is high, the Microsoft Teams optimization might not support as expected.

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

This feature is in technical preview from 2109 release.

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

Global App Config Service

This feature is in technical preview from 2109 release.

The new Global App Configuration Service for Citrix Workspace allows a Citrix administrator to deliver Workspace service URLs through a centrally managed service.

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
1       <key>AppConfigEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

For more information on Workspace service URLs settings, see Global App Configuration Service documentation.

> **Note:**
>
> - Citrix Workspace app for Linux uses the Global App Configuration Service only to deliver Workspace service URLs.

Technical Preview to General Availability (GA)

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

Service or feature	General availability version
HTTPS protocol support for proxy server	2308

System requirements and compatibility

August 26, 2023

Requirements

Hardware requirements

Linux kernel:

- Version 2.6.29 or later

Disk space:

- A minimum of 55 MB
- An extra 110 MB if you expand/extract the installation package on the disk
- A minimum of 1 GB RAM for system-on-a-chip (SoC) devices that use HDX MediaStream Flash Redirection

Color video display:

- 256 color video display or greater

Libraries and codec

Libraries:

- `glibcxx` 3.4.25 or later
- `glibc` 2.27 or later
- gtk 2 (2.20.1 or later)
- libcap1 or libcap2
- `libjson-c` (for instrumentation)
- X11 or X.Org (Wayland isn't supported)
- `udev` support
- Advanced Linux Sound Architecture (ALSA) libasound2
- PulseAudio

Self-service user interface:

- webkit2gtk 2.16.6 or later

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

- libxml2 2.7.8
- `libxerces-c` 3.1

Codec libraries:

- Speex
- Vorbis codec libraries

Red Hat Package Manager (RPM) based distribution requirements:

- `chkconfig`

Network requirements

Network protocol:

- TCP/IP

H.264 requirements

For x86 devices:

- A minimum processor speed of 1.6 GHz

For the HDX 3D Pro feature:

- A minimum processor speed of 2 GHz
- A native hardware with accelerated graphics driver

For ARM devices:

- A hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro

HDX MediaStream Flash Redirection

For all HDX MediaStream Flash Redirection requirements, see Knowledge Center article CTX134786.

We recommend that you test the article with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.

Authentication requirements

cURL 7.68 or later with OpenSSL for cloud authentication.

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

Customer Experience Improvement Program (CEIP) integration requirements

- `zlib` 1.2.3.3
- `libtar` 1.2 or later
- `libjson` 7.6.1 or later

HDX RealTime webcam video compression requirements

- A Video4Linux compatible webcam
- `GStreamer` 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package

  Or,

- `GStreamer` 1.0 (or a later 1.x version), including the distribution's "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly", and "gstreamer-libav" packages

HDX MediaStream Windows Media redirection requirements

- `GStreamer` 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection

  Or,

- `GStreamer` 1.0 (or a later 1.x version), including the distribution's "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly", and "gstreamer-libav" packages

> **Notes:**
>
> - If `GStreamer` isn't included in your Linux distribution, you can download it from the GStreamer page.
> - Use of certain codes (for example, as in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help.

Browser content redirection requirements

- webkit2gtk version 2.16.6

Philips SpeechMike requirements

- Visit the Philips website to install the relevant drivers

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

App Protection requirements

App Protection works best with the following Operating Systems along with the Gnome Display Manager:

- 64-bit Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- 64-bit Debian 9 and Debian 10
- 64-bit CentOS 7
- 64-bit RHEL 7
- ARMHF 32-bit Raspberry Pi OS (Based on Debian 10 (buster))
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

> **Note:**
>
> - If you are using Citrix Workspace app earlier than version 2204, the App Protection feature does not support the operating systems that use `glibc` 2.34 or later.
> - On Ubuntu 20.04.5 or later, when you double-click the `.deb` package file, the Snap Store installer opens. This installer doesn't support user prompts. So, you must install the Citrix Workspace app using the command line in a terminal or using other software installers like `gnome-software`, `gdebi`, and `synaptics`.

Microsoft Teams optimization requirements

Minimum version:

- Citrix Workspace app 2006

Software:

- `GStreamer` 1.0 or later and Cairo 2
- libc++-9.0 or later
- `libgdk` 3.22 or later
- OpenSSL 1.1.1d
- x64 Linux distribution

Hardware:

- A minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call
- Dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz

Authentication enhancement:

- `Libsecret` library
- libunwind-12 library

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

Service continuity requirements

Starting with Version 2106, you can install Service Continuity on the Debian version of Citrix Workspace app.

Run the following commands from the terminal before installing Citrix Workspace app:

```
sudo apt-get update -y
```

Mandatory preinstalled libraries:

- libwebkit2gtk-4.0-37 version 2.30.1 or later
  - If you are using Debian, run the following command:

    ```
    1 sudo apt-get install libwebkit2gtk-4.0-37
    2 <!--NeedCopy-->
    ```

  - If you are using RPM, run the following command:

    ```
    1 sudo yum install libwebkit2gtk-4*
    2 <!--NeedCopy-->
    ```

  - For Ubuntu, RHEL, SUSE, Fedora, or Debian, Citrix recommends you to install the latest libwebkit2gtk-4.0-37 version 2.30.1 or later.
  - For the Raspberry Pi with Buster OS, Citrix recommends you to install the libwebkit2gtk-4.0-37 version 2.30.1.
- gnome-keyring version 3.18.3 or later
  - If you are using Debian, run the following command:

    ```
    1 sudo apt-get install gnome-keyring
    2 <!--NeedCopy-->
    ```

  - If you are using RPM, run the following command:

    ```
    1 sudo yum install gnome-keyring
    2 <!--NeedCopy-->
    ```

- Libsecret
  - If you are using Debian, run the following command:

    ```
    1 sudo apt-get install libsecret-1-0
    2 <!--NeedCopy-->
    ```

  - If you are using RPM, run the following command:

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

```
sudo yum install libsecret-1*
<!--NeedCopy-->
```

> **Notes:**
>
> Following the 1910 version, Citrix Workspace app works as expected only if the operating system meets the following GCC version criteria:
>
> - GCC version for x64 architecture: 4.8 or later
> - GCC version for ARMHF architecture: 4.9 or later
>
> Following the 2101 version, Citrix Workspace app works as expected only if the operating system meets the following requirements:
>
> - GCC version 4.9 or later
> - `glibcxx` 3.4.20 or later
>
> Following the 2209 version, Citrix Workspace app works as expected only if the operating system meets the following requirement:
>
> `glibcxx` 3.4.25 or later

Compatibility matrix

Citrix Workspace app is compatible with all currently supported versions of the Citrix products.

For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the Citrix Product Lifecycle Matrix.

Server requirements

StoreFront

- You can use all currently supported versions of Citrix Workspace app to access StoreFront stores from both internal network connections and through Citrix Gateway:
  - StoreFront 1811 and later.
  - StoreFront 3.12.
- You can use StoreFront configured with the workspace for web. The workspace for web provides access to StoreFront stores from a web browser. For the limitations of this deployment, see Important considerations in the StoreFront documentation.

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

Connections and certificates

Connections

Citrix Workspace app for Linux supports HTTPS and ICA-over-TLS connections through any one of the following configurations.

- For LAN connections:
  - StoreFront using StoreFront services or workspace for web
- For secure remote or local connections:
  - Citrix Gateway 12.0 and later
  - NetScaler Gateway 10.1 and later
  - NetScaler Access Gateway Enterprise Edition 10
  - Netscaler Access Gateway Enterprise Edition 9.x
  - Netscaler Access Gateway VPX

  For information about the Citrix Gateway versions supported by StoreFront, see System requirements of StoreFront.

Certificates

To ensure secure transactions between server and client, use the following certificates:

Private (self-signed) certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the user device. This installation helps to access Citrix resources using Citrix Workspace app.

> **Note:**
>
> An untrusted certificate warning appears, if the remote gateway's certificate can't be verified upon connection. This verification might fail since the root certificate isn't included in the local key store. If you choose to continue through the warning, the apps are displayed but can't be launched. The root certificate must be installed in the client's certificate store.

Root certificates

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

For non-domain joined machines, create a custom install package to distribute and install the CA certificate. Contact your system administrator for assistance.

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

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 supports wildcard certificates, however they must only be used in accordance with your organization's security policy.

Alternatives to wildcard certificates, such as a certificate that includes the list of server names within the Subject Alternative Name (SAN) extension, can be considered. Both private and public certificate authorities issue such certificates.

Append intermediate certificate to Citrix Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway server certificate. For information, see Configuring Intermediate Certificates in the Citrix Gateway documentation.

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

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

   > **Tip:**
   >
   > If you can't find a certificate in the .pem file extension, use the `openssl` utility to convert

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

> a certificate to the .pem file extension.

2. When you install the package (usually root):
   a) Copy one or more files to $ICAROOT/keystore/intcerts.
   b) Run the following command after you installed the package:

      ```
      $ICAROOT/util/ctx_rehash
      ```

Joint server certificate validation policy

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

> **Important:**
>
> Before installing Citrix Workspace app, confirm that the certificates on the server or gateway are correctly configured as described here. Connections might fail if:
>
> - the server or gateway configuration includes a wrong root certificate
> - the server or gateway configuration does not include all intermediate certificates
> - the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
> - the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Workspace app uses all the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Workspace app versions, it verifies that the certificates are trusted. If any certificate is untrusted, the connection fails.

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

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

If a gateway is configured with these valid certificates, use the following configuration for stricter validation. This configuration determines exactly which root certificate the Citrix Workspace app uses:

- Example Server Certificate
- Example Intermediate Certificate
- Example Root Certificate

Citrix Workspace app verifies all these certificates are valid. Citrix Workspace app also verifies that it already trusts the Example Root Certificate. If Citrix Workspace app does not trust the Example Root Certificate, the connection fails.

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

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

If a gateway is configured with these valid certificates, we can use the following configuration, leaving out the root certificate:

- Example Server Certificate
- Example Intermediate Certificate

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

If a gateway is configured with these certificates:

- Example Server Certificate
- Example Intermediate Certificate
- Wrong Root Certificate

A web browser might ignore the wrong root certificate. However, Citrix Workspace app does not ignore the wrong root certificate, and the connection fails.

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

- Example Server Certificate
- Example Intermediate Certificate 1
- Example Intermediate Certificate 2

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

> **Important:**
>
> - Some certificate authorities use a cross-signed intermediate certificate. This certificate is used where there's more than one root certificate, and an earlier root certificate is still in use as a later root certificate. In this case, there are at least two intermediate certificates. For example, the earlier root certificate *Class 3 Public Primary Certification Authority* has the corresponding cross-signed intermediate certificate *Verisign Class 3 Public Primary Certification Authority - G5*. However, a corresponding later root certificate *Verisign Class 3 Public Primary Certification Authority - G5* is also available, which replaces *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 difference distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such as Example Intermediate Certificate 2).

This configuration, leaving out the root certificate and the cross-signed intermediate certificate, is recommended:

- Example Server Certificate
- Example Intermediate Certificate

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

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

It isn't recommended to configure the gateway with only the server certificate:

- Example Server Certificate

In this case, if Citrix Workspace app can't locate all the intermediate certificates, the connection fails.

Supports system certificate paths for SSL connection

Citrix Workspace app version 2308 supports system certificate paths for SSL connection. This feature simplifies the certificate management process on the client side and improves the user experience. With this feature, Citrix Workspace can create a TLS connection with the certificate in the system certificate path. This feature is enabled by default.

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

Workspacecheck

We provide a script, workspacecheck.sh, as part of the Citrix Workspace app installation package. The script checks whether your device meets all the system requirements in support of the functionalities of Citrix Workspace app. The script is in the `Utilities` directory of the installation package.

To run the workspacecheck.sh script

1. Open the terminal in your Linux machine.
2. Type `cd $ICAROOT/util` and press **Enter** to navigate to the `Utilities` directory of the installation package.
3. Type `./workspacecheck.sh` to run the script.

Out-of-support applications and operating systems

Citrix does not offer support in the context of applications and operating systems that are no longer supported by their vendors.

While attempting to address and resolve a reported issue, Citrix assesses whether the issue directly relates to an out-of-support application or operating system. To help in making that determination, Citrix might ask you to attempt to reproduce an issue using the supported version of the application or operating system. If the issue seems to be related to the out-of-support application or operating system, Citrix will not investigate the issue further.

Install, Uninstall, and Update

August 26, 2023

You can install the Citrix Workspace app by downloading the file from the Citrix website at Downloads.

Verify the version of the Citrix Workspace app

Perform the following steps to verify the current version of the Citrix Workspace app installed on your system:

1. Open a terminal window.
2. Run the following command:

   For Debian packages:

```
dpkg --list | grep -i icaclient
<!--NeedCopy-->
```

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

OR

```
cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
<!--NeedCopy-->
```

For Red Hat packages:

```
rpm -qa | grep -i icaclient

<!--NeedCopy-->
```

OR

```
cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
<!--NeedCopy-->
```

For Tarball packages:

```
cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
<!--NeedCopy-->
```

Manual install

Download the following packages from the Citrix Downloads page.

Debian packages

Install the `Icaclient` package based on your OS architecture.

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

> **Note:**
>
> To avoid the compatibility issue, ensure that you install the same version of `Icaclient` and `ctxusb` packages.

Package name	Contents
Debian packages (Ubuntu, Debian, Linux Mint etc.)	
`icaclient_<version>_amd64.deb`	Self-service support, 64-bit x86_64
`icaclient_<version>_i386.deb`	Self-service support, 32-bit x86
`icaclient_<version>_armhf.deb`	Self-service support, ARM HF

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

Package name	Contents
ctxusb_<version>_amd64.deb	USB package, 64-bit x86_64
ctxusb_<version>_i386.deb	USB package, 32-bit x86
ctxusb_<version>_armhf.deb	USB package, ARM HF

Install using a Debian package

> **Prerequisites:**
>
> Verify that you have installed all the required system requirements, as mentioned at System requirements section.

When installing Citrix Workspace app from the Debian package on Ubuntu, open the packages in the Ubuntu Software Center.

In the following instructions, replace
packagename with the name of the package that you're trying to install.

This procedure uses a command line and the native package manager for Ubuntu, Debian, or Mint. You can also install the package by double-clicking the downloaded .deb package in a file browser. This action typically starts a package manager that downloads any missing required software. If no package manager is available, Citrix recommends you to use the **gdebi**, a command-line tool.

> **Note:**
>
> On Ubuntu 20.04.5 or later, when you double-click the `.deb` package file, the Snap Store installer opens. This installer doesn't support user prompts. So, you must install the Citrix Workspace app using the command line in a terminal or using other software installers like `gnome-software`, `gdebi`, and `synaptics`.

To install the package using the command line:

1. Log on as a privileged (root) user.
2. Open a terminal window.
3. Run the installation using one of the following commands:
   - `apt` – Use the following command to install the Citrix Workspace app with dependency:

     ```
     sudo apt install -f ./icaclient_<version>._amd64.deb
     <!--NeedCopy-->
     ```

     To install the USB package, run the following command:

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

```
sudo apt install -f ctxusb_<version>._amd64.deb
<!--NeedCopy-->
```

- `dpkg -i` – Use the following command to install the Citrix Workspace app:

```
sudo dpkg -i icaclient_<version>_amd64.deb
sudo apt-get -f install
<!--NeedCopy-->
```

To install the USB package, run the following command:

```
sudo dpkg -i ctxusb_<version>_amd64.deb
sudo apt-get -f install
<!--NeedCopy-->
```

- `gdebi` – Use the following command to install the Citrix Workspace app:

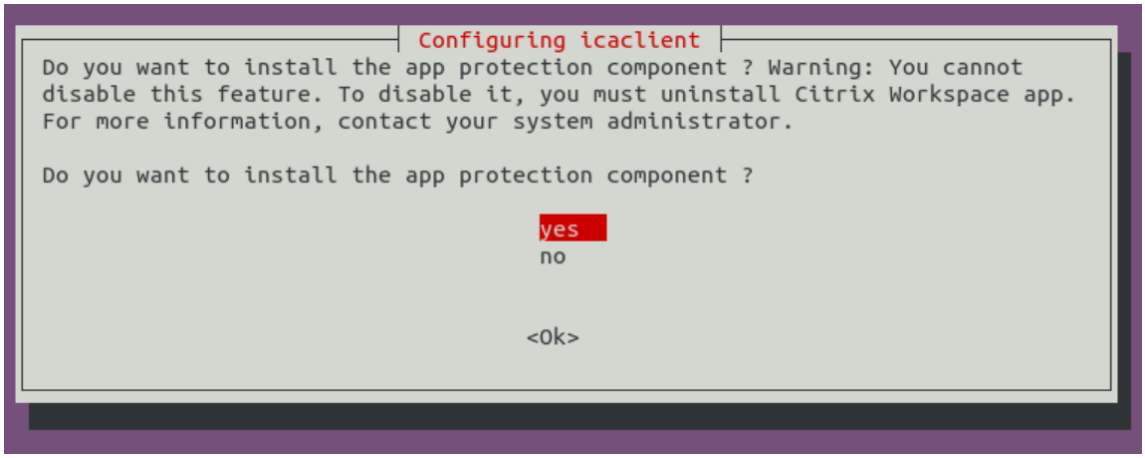
```
gdebi icaclient_<version>_amd64.deb
<!--NeedCopy-->
```

To install the USB package, run the following command:

```
gdebi ctxusb_<version>_amd64.deb
<!--NeedCopy-->
```

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

4. Starting with Version 2101, the following interactive prompt appears asking you to install App Protection:



5. Select **Yes** to proceed with the installation with the App Protection component.

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

Silent installation of the App Protection component on Debian packages

Starting with Version 2102, App Protection is supported on the Debian version of Citrix Workspace app.

For silent installation of the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

```
export DEBIAN_FRONTEND="noninteractive"
<!--NeedCopy-->
```

```
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
<!--NeedCopy-->
```

```
sudo debconf-show icaclient
<!--NeedCopy-->
```

```
sudo apt install -f ./icaclient_<version>._amd64.deb`

<!--NeedCopy-->
```

Red Hat packages

Install the `ICAClient` package based on your OS architecture.

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

> **Note:**
>
> To avoid the compatibility issue, ensure that you install the same version of `Icaclient` and `ctxusb` packages.

Package name	Contents
Redhat packages (Redhat, SUSE, Fedora etc.)	
`ICAClient-rhel-<version>.x86_64.rpm`	Self-service support, Red Hat (including Linux VDA) based, 64-bit x86_64
`ICAClient-rhel-<version>.i386.rpm`	Self-service support, Red Hat based, 32-bit x86
`ICAClient-suse-<version>.x86_64.rpm`	Self-service support, SUSE based, 64-bit x86_64

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

Package name	Contents
ICAClient-suse-<version>.i386.rpm	Self-service support, SUSE based, 32-bit x86
ctxusb-<version>.x86_64.rpm	USB package, 64-bit x86_64
ctxusb-<version>.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.

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

To install from the RPM package

> **Prerequisites:**
>
> Verify that you have installed all the required system requirements, as mentioned at System requirements section.

1. Set up the EPEL repository.

   > **Note:**
   >
   > For RHEL and CentOS, install the EPEL repository before you can install the Linux VDA successfully. For information on how to install EPEL, see the instructions.

2. Log on as a privileged (root) user.
3. Open a terminal window.
4. Run the installation for the following three packages by typing Zypper in .

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

> **Note:**
>
> - `ctxusb` is an optional package. Install the package to support Generic USB Redirection.
> - `ctxappprotection` is an optional package. Install the package only if you want to install the App Protection component.

For SUSE installations:

- `zypper in ICAClient-suse-<version>.x86_64.rpm`
- `zypper in ctxusb-<version>.x86_64.rpm`
- `zypper in ctxappprotection-<version>.x86_64.rpm`

For Red Hat installations:

- `yum localinstall ICAClient-rhel-<version>.x86_64.rpm`
- `yum localinstall ctxusb-<version>.x86_64.rpm`
- `yum localinstall ctxappprotection-<version>.x86_64.rpm`

To install a missing package

On a Red Hat based distribution (RHEL, CentOS, Fedora, and so on), add an EPEL repository (details can be found at https://docs.fedoraproject.org/en-US/epel/), if the following error message appears:

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

Tarball packages

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

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

> **Note:**
>
> - If you want to customize the installation location, install Citrix Workspace app from the

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

> tarball package. If you want to install any required packages automatically, install Citrix Workspace app from the Debian package or the RPM package.
>
> - Do not use two different installation methods on the same machine. If you do, you might see error messages and unwanted behavior.

Install using a tarball package

> **Note:**
>
> The tarball package does not do dependency checks or install dependencies. All system dependencies must be resolved separately.

1. Open a terminal window.
2. Extract the contents of the `.tar.gz` file into an empty directory. For example, type: `tar xvfz packagename.tar.gz`.
3. Type `./setupwfc` and then press Enter to run the setup program.
4. Accept the default of `1` (to install Citrix Workspace app) and press **Enter**.
5. Type the path and name of the required installation directory and then press Enter. Or, press Enter to install Citrix Workspace app in the default location.

   The default directory for privileged (root) user installations is `/opt/Citrix/ICAClient`.

   The default directory for non-privileged user installations is `$HOME/ICAClient/platform`. Platform is a system-generated identifier for the installed operating system, for example, `$HOME/ICAClient/linuxx86` for the Linux/x86 platform).

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

6. When prompted to continue, type `y` and then press Enter.
7. You can choose whether to integrate Citrix Workspace app into your desktop environment. The installation creates a menu option from which users can start Citrix Workspace app. Type `y` at the prompt to enable the integration.
8. If you have previously installed `GStreamer`, you can choose whether to integrate `GStreamer` with Citrix Workspace app, and support HDX MediaStream Multimedia Acceleration. To integrate Citrix Workspace app with `GStreamer`, type `y` at the prompt.

   > **Note:**
   >
   > On some platforms, installing the client from a tarball package can cause the system to

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

> become unresponsive after prompting you to integrate with KDE and GNOME. This issue occurs with the first-time initialization of gstreamer-0.10. If you encounter this issue, terminate the installation process (using the keys ctrl+c) and run the command `gst-inspect-0.10 -- gst-disable-registry-fork --version`. After running the command, you can rerun the tarball package without experiencing the issue.

9. If you log on as a privileged user (root), choose to install USB support for Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) published VDI applications. Type `y` at the prompt to install USB support.

   > **Note:**
   >
   > If you 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

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`.

> **Notes:**
>
> - To uninstall Citrix Workspace app, you must be logged in as the same user who does the installation.
> - When you uninstall the Citrix Workspace app, out of date cache files at `$HOME/.local/share/webkitgtk` might not be removed automatically. As a workaround, manually remove the cache files.

To uninstall Citrix Workspace app on the tarball package

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

To uninstall Citrix Workspace app on Debian/Ubuntu Operating systems

1. Open a terminal window.

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

2. Run the installation using one of the following commands:

```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt autoremove -y
<!--NeedCopy-->
```

OR,

```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt purge icaclient -y
<!--NeedCopy-->
```

> **Note:**
>
> You can also remove the Debian package using your operating system's standard tools.

To uninstall Citrix Workspace app on Fedora/RHEL/CentOS Operating systems

1. Open a terminal window.
2. Run the installation using the following command:

```
yum remove icaclient -y
<!--NeedCopy-->
```

> **Note:**
>
> You can also remove the RPM package using your operating system's standard tools.

Verify whether the uninstallation of the Citrix Workspace app is successful. For more information see, Verify the version of the Citrix Workspace app section.

Update

Before updating Citrix Workspace app, verify the current version of the Citrix Workspace app installed in your system. For more information see, Verify the version of the Citrix Workspace app section.

To update to a newer version of the Citrix Workspace app, download and install the latest Citrix Workspace app from Citrix Downloads. For installation procedure, you can follow the steps mentioned at the following installation section:

- Debian packages

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

- Red Hat packages
- Tarball packages

If you have the Citrix Workspace app installed in your system, the system detects the existing app, and updates to a newer version. However, for Tarball packages, consider a scenario where you have installed the earlier version of the app in one folder and you have installed the newer version of the app in a different folder. In this scenario, both versions of the app might exist in your system.

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

Get started

August 26, 2023

This article is a reference document to help you get started with Citrix Workspace app for Linux.

Verify the current version of the Citrix Workspace app installed in your system. For more information see, Verify the version of the Citrix Workspace app](/en-us/citrix-workspace-app-for-linux/install.html#verify-the-version-of-the-citrix-workspace-app) section.

Store

A **store** aggregates available applications and desktops for a user into a single place. A user can have multiple stores and switch across stores as needed. An admin delivers the store URL that has preconfigured resources and settings. You can access these stores through the Citrix Workspace app.

For more information on store, see the StoreFront documentation.

Types of stores

You can add the following store types in the Citrix Workspace app:

- Workspace
- StoreFront
- Citrix Gateway Store
- Custom web store

Workspace

Citrix Workspace is a cloud-based enterprise app store that provides secure and unified access to apps, desktops, and content (resources) from anywhere, on any device. These resources can be Citrix DaaS,

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

content apps, local and mobile apps, SaaS and Web apps, and browser apps. For more information, see Citrix Workspace Overview.

StoreFront

StoreFront is an on-premises enterprise app store that aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single easy-to-use store for users.

For more information, see StoreFront documentation.

Citrix Gateway Store

Configure Citrix Gateway to enable users to connect from outside the internal network. For example, users who connect from the Internet or from remote locations.

Custom web stores

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

To use this feature, if Global App Configuration Service is available:

The administrator must add the domain or the custom web store to the list of allowed URLs in the Global App Configuration Service. After you have added the domain or the custom web store, provide the custom web store URL or email address in the **Add Account** screen in the Citrix Workspace app. The custom web store opens in the native Workspace app window.

For more information about configuring web store URLs for end-users, see Global App Configuration Service.

> **Note:**
>
> The Pinning multi-monitor screen layout feature is not supported in the custom web store.

To remove the custom web store, go to **Accounts** > **Add or Remove accounts**, select the custom web store URL, and click **Remove**.

As a prerequisite, you must enable the custom web store in the `AuthManConfig.xml` file. To enable it:

1. Navigate to the `$ICAROOT/config/AuthManConfig.xml` configuration file.
2. Add the following entries:

```
<key>AppConfigEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

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

To use this feature, if Global App Configuration Service isn't available:

Perform the following configuration changes:

1. Navigate to the `$ICAROOT/config/AuthManConfig.xml` configuration file.
2. Add the following entries:

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

3. Add the list of URLs that must be considered for the custom web store in the following way.

```
<AllowedWebStoreCache>
<value><URL1></value>
<value><URL2></value>
..
<value>....</value>
</AllowedWebStoreCache>
<!--NeedCopy-->
```

> **Note:**
>
> You can only use the URLs listed in the `AuthManConfig.xml` file for the custom web store. You can add extra URLs in the`AuthManConfig.xml` file that you want to be considered for the custom web store.

Adding store URL to Citrix Workspace app

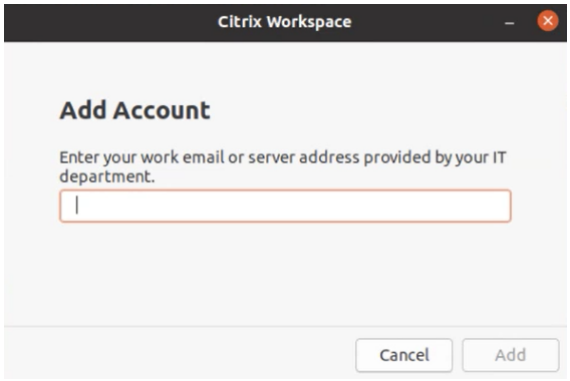
You can provide users with the account information that they need to access virtual desktops and applications using the following:

- Providing users with account information to enter manually
- Configuring email-based auto-discovery
- Adding store through CLI

Provide users with account information to enter manually

After installing the Citrix Workspace app successfully and when you launch the app for the first time, the following screen appears. Users are required to enter an email or server address to access the apps and desktops. When a user enters the details for a new account, Citrix Workspace app tries to verify the connection. If successful, Citrix Workspace app prompts the user to log on to the account.

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



To enable users to set up accounts manually, be sure to distribute the information required to connect to their virtual desktops and applications.

- To connect to a Workspace store, provide the Workspace URL.
- To connect to a StoreFront store, provide the URL for that server. For example:`https://servername.company.com`.
- To connect through Citrix Gateway, provide users with the Citrix Gateway fully qualified domain name.

Email-based auto-discovery of store

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

To disable this feature, do the following:

1. Navigate to `$ICAROOT/config/AuthManConfig.xml` file.
2. Set the following entry to false.

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

Adding store through CLI

Install Citrix Workspace app for Linux as an administrator using the command-line interface.

For more information, see Storebrowse section.

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

Set up

You can download the installation package, customize the configuration, and then install the Citrix Workspace app.

You can modify the contents of the Citrix Workspace app package and then repackage the files.

Customize installation

1. Expand the Citrix Workspace app package file into an empty directory. The package file is called platform.major.minor.release.build.tar.gz (for example, `linuxx86-<version>.tar.gz` for the Linux/x86 platform).
2. Make the required changes to the Citrix Workspace app package. For example, you can add a TLS root certificate to use a certificate from the Certificate Authority that is not a part of the standard Citrix Workspace app installation.
3. Open the `PkgID` file.
4. Add the following line to indicate that the package was modified:

   MODIFIED=traceinfo

   where, `traceinfo` is information indicating who made the change and when.
5. Save and close the file.
6. Open the package file list, platform/platform.psf (for example, linuxx86/linuxx86.psf for the Linux/x86 platform).
7. Update the package file list to reflect the changes you made to the package. Not updating might cause an error when installing the new package. Changes can include updating the size of any files you modified, or adding new lines for any files you added to the package. The columns in the package file list are:
   - File type
   - Relative path
   - Subpackage (always set to `cor`)
   - Permissions
   - Owner
   - Group
   - Size
8. Save and close the file.
9. Use the tar command to rebuild the Citrix Workspace app package file. For example, `tar czf ../newpackage.tar.gz *`, where `newpackagez` is the name of the new Citrix Workspace app package file.

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

Latest webkit support

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 that 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.
> - Move to a later Linux distribution that supports webkit2gtk 2.16.6 or later.

Launch

You can start Citrix Workspace app either at a terminal prompt or from one of the supported desktop environments.

Ensure that the environment variable `ICAROOT` is set to point to the actual installation directory.

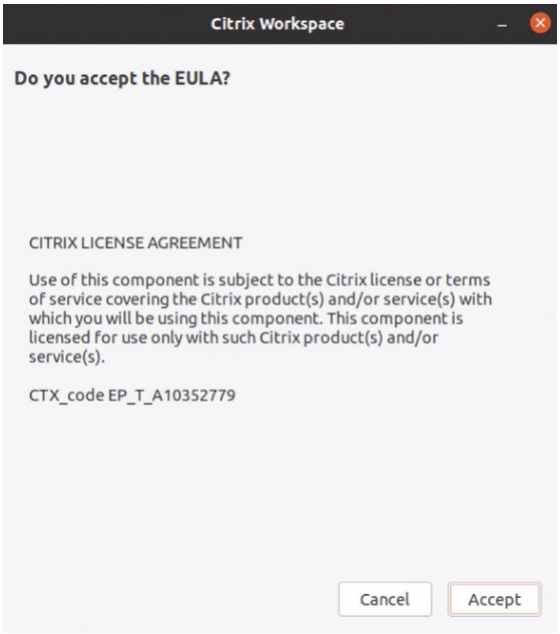
> **Tip:**
>
> The following instruction does not apply to installations made from the Web packages, and where the tarball is used. This instruction is applicable when the requirements for self-service have not been met.

Terminal prompt

To start the Citrix Workspace app at the terminal prompt:

1. Type `/opt/Citrix/ICAClient/selfservice`
2. Press Enter (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Workspace app).
   The **Do you accept the EULA?** dialog box appears.

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



3. Click **Accept** to proceed with adding store.

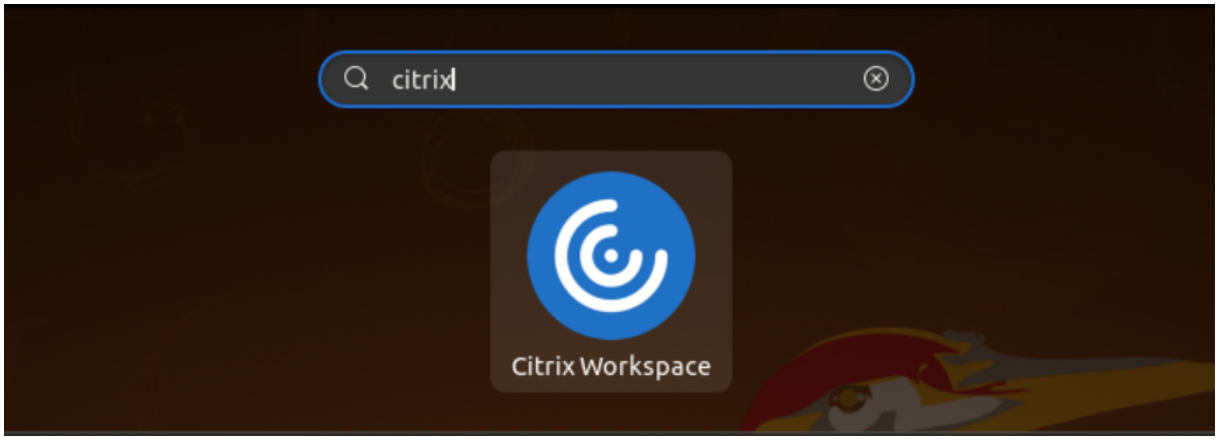
> **Note:**
>
> The **Do you accept the EULA?** dialog box appears only if you access the Citrix Workspace app for Linux first time after the installation.

Linux desktop

You can start the Citrix Workspace app from a desktop environment using a file manager.

On some desktops, you can also start Citrix Workspace app from a menu. Citrix Workspace app is available in different menus depending on your Linux distribution.

On Ubuntu, the Citrix Workspace app icon appears as follows:



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

Preferences

To set preferences, click **Preferences** from the Citrix Workspace app menu. You can control the following:

- How desktops are displayed
- Connect to different applications and desktops
- Manage file and device access

Manage an account

To access desktops and applications, you need an account with Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Your IT help desk might ask you to add an account to Citrix Workspace for this purpose. Or they might ask you to use a different Citrix Gateway or Access Gateway server for an existing account. You can also remove accounts from Citrix Workspace.

1. On the **Accounts** page of the **Preferences** dialog, do one of the following:
    - To add an account, click **Add**. Contact your system administrator for more information.
    - To change details of a store that the account uses, such as the default gateway, click **Edit**.
    - To remove an account, click **Remove**.
2. Follow the on-screen prompts. When prompted, authenticate to the server.

Desktop display

You can display desktops across the entire screen on your user device (full screen mode), which is the default, or in a separate window (windowed mode).

- On the **General** page of the **Preferences** dialog box, select a mode using the **Display desktop in** option.

Use the **You can enable Desktop Viewer** toolbar functionality to dynamically modify the window configuration of your remote session.

Desktop Viewer

Your requirements for the way users access virtual desktops can vary from user to user and might vary as your corporate needs evolve.

Use the Desktop Viewer when users interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the **Desktop Viewer** toolbar functionality allows the user to switch a session between windowed and full-screen session window, including multi-monitor support for the intersected monitors. Users can switch between desktop sessions and use more than one desktop using multiple Citrix Virtual Apps

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

and Desktops or Citrix DaaS connections on the same user device. Buttons to minimize all desktop sessions, send the Ctrl+Alt+Del sequence, disconnect, and log off from the session are provided to manage a user's session conveniently.

Pressing **Ctrl+Alt+Break** displays the **Desktop Viewer** toolbar buttons in a pop-up window.

Automatic session reconnects

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 access happens.

1. On the **File Access** page of the **Preferences** dialog box, select a mapped drive and then one of the following options:
   - **Read and write** - Allow the desktop or application to read and write to local files.
   - **Read only** - Allow the desktop or application to read but not write to local files.
   - **No access** - Do not allow the desktop or application to access local files.
   - **Ask me each time** - Display a prompt each time the desktop or application access local files.
2. Click **Add**, specify the location, and select a drive to map to it.

Microphone and Webcam

To set up a microphone or a webcam, you can change the way a virtual desktop or application accesses your local microphone or webcam:

On the **Mic & Webcam** page of the **Preferences** dialog box, select one of the following options:

- **Use my microphone and webcam** - Allow the microphone and webcam to be used by the desktop or application.
- **Don't use my microphone or webcam** - Do not allow the microphone or webcam to be used by the desktop or application.

Flash player

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

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

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 or Citrix DaaS administrators. Using the **Preferences** > **Accounts** page, you can configure the URL of a StoreFront server or, if email-based account discovery is configured, by entering the email address.

> **Tip:**
>
> If you use the same name for multiple stores on the StoreFront server, you avoid duplications by adding numbers. The names for such stores depend on the order in which they are added. For Citrix Workspace app, the store URL is displayed and uniquely identifies the store.

After connecting to a store, the self-service shows the tabs: **FAVORITES**, **DESKTOPS**, and **APPS**. To launch a session, click the appropriate icon. To add an icon to **FAVORITES**, click the **Details** link next to the icon and select A**dd To Favorites**.

Configure connection settings

You can configure some default settings for connections between Citrix Workspace app and Citrix Virtual Apps and Desktops or Citrix DaaS servers. You can also change these settings for individual connections, if necessary.

Although the tasks and responsibilities of administrators and users can overlap, the term “user” is used to distinguish user tasks from those tasks that an administrator performs.

Connect to resources from a command line or browser

You create connections to servers when you click a desktop or application icon on the Citrix Workspace app home page. Also, you can open connections from a command line or from a web browser.

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

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\>
<!--NeedCopy--> ```
```

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

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

   - List the desktops and applications that you've subscribed to:

     ```
     ./util/storebrowse -S <store URL>
     <!--NeedCopy-->
     ```

2. Run the following command to start the desktop or application:

   ```
   ./util/storebrowse - L <desktop or application ID> <store URL>
   <!--NeedCopy-->
   ```

If you can't connect to a server, you might need to check your administrator for issues like server location or SOCKS proxy. For more information, see
proxy server.

To create a connection from a web browser

Configuration for starting sessions from a web browser is typically carried out automatically during installation. Because of the wide variety of browsers and operating systems, some manual configuration can be required.

If you set up `.mailcap` and `MIME` files for Firefox, Mozilla, or Chrome manually, use the following file modifications. Using these modifications, the `.ICA` files start up the Citrix Workspace app executable, `wfica`. To use other browsers, modify the browser configuration accordingly.

1. Run the following commands for non-administrator installation of Citrix Workspace app. The settings of ICAROOT might be changed if they are installed to a non-default location. You can test the result with the command

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

`xdg-mime query default application/x-ica`, which must return “wfica.desktop.”

```
export ICAROOT=/opt/Citrix/ICAClient
```

```
xdg-icon-resource install --size 64 $ICAROOT/icons/000_Receiver_64.png
Citrix Workspace app
```

```
xdg-mime default wfica.desktop application/x-ica
```

```
xdg-mime default new_store.desktop application/vnd.citrix.receiver.
configure
```

2. Create or extend the file /etc/xdg/mimeapps.list (for administrator installation) or `$HOME/.local/share/applications/mimeapps.list` (`mimeapps.list`). The file must start with [Default Applications], and follow by:

   ```
   application/x-ica=wfica.desktop;
   ```

   ```
   application/vnd.citrix.receiver.configure=new_store.desktop;
   ```

   You might require to configure Firefox on its Preferences/Applications setting page.

   For “Citrix ICA settings file content,” select:

   - “Citrix Workspace app Engine (default)” in the drop-down menu

     or

   - “Use other …” and then select the file /usr/share/applications/wfica.desktop (for an administrator installation of Citrix Workspace app)

     or

   - $HOME/.local/share/applications/wfica.desktop (for a non-administrator installation).

Connection Center

Users can manage their active connections using the Connection Center. This feature is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. With Connection Center, users can manage connections by:

- Closing an application.
- Logging off a session. This step ends the session and closes any open applications.
- Disconnecting from a session. This step cuts the selected connection to the server without closing any open applications (unless the server is configured to close applications on disconnection).
- Viewing connection transport statistics.

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

Manage a connection

To manage a connection using the **Connection Center**:

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

   The servers that are used appear and active sessions are listed.

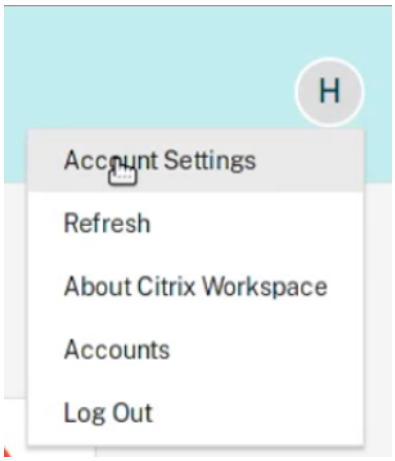
2. Do one of the following:

   - Select a server, disconnect or log off, or view its properties.
   - Select an application, close the window.

User Interface enhancement

Previously, the settings menu was available from the **Preferences** option in the Desktop Viewer.

Starting with version 2106, the settings menu appears in line with the Self-Service plug-in. The menu options are now improved to align with the look and feel of the native Citrix Workspace. This enhancement results in a seamless and a better user experience.



> **Note:**
>
> This enhancement is available by default in Citrix Workspace app Version 2106 in cloud deployments.

To switch to the native and old style appearance, do the following:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and set the value of `WebUISettings` to **False**.

Configure

September 20, 2023

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

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:**
>
> If an entry in `All\\_Regions.ini` is set to a specific value, the value for that entry in `module.ini` isn't used. The values in `All\\_Regions.ini` take precedence over the value in `module.ini`.

Template file

If the `$HOME/.ICAClient/wfclient.ini` file does not exist, `wfica` creates it by copying `$ICAROOT/config/wfclient.template`. When you change this template file, the changes are applied to all the Citrix Workspace app users.

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`.

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

If you specify only one value, that value is used. The `$HOME/.ICAClient/All\\_Regions.ini` file can match or reduce the possible values set in the `$ICAROOT/config/All\\_Regions.ini`file, it can't take away restrictions.

> **Note:**
>
> The value set in `wfclient.ini` takes precedence over the value in `module.ini`.

Parameters

The parameters listed in each file are grouped into sections. Each section begins with a name in brackets that indicates parameters that belong together; for example, `\[ClientDrive\]` for parameters related to client drive mapping (CDM).

Defaults are automatically supplied for any missing parameters except where indicated. If a parameter is present but not assigned a value then the default value is automatically applied. For example, consider the `InitialProgram` parameter is followed by an equal sign (=) and no value is provided. In this example, the default value (not to run a program after logging in) is applied.

Precedence

The `All\\_Regions.ini` file specifies parameters that the other files can set. It can restrict the values of parameters or set them exactly.

For any given connection, the files are checked in the following order:

1. `All\\_Regions.ini` - The values in this file override those values in:
   - The connections `.ICA` file
   - `wfclient.ini`
2. `module.ini` - The values in this file are used if they have not been set in `All\\_Regions.ini`, the connections `.ICA` file, or `wfclient.ini`. However, these values aren't restricted with the entries in `All\\_Regions.ini`.

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.

Inactivity Timeout for Citrix Workspace app

The inactivity timeout feature signs you out of the Citrix Workspace app based on a value that the admin sets. Starting with the 2303 version, admins can specify the amount of idle time that is allowed before a user is automatically signed out of the Citrix Workspace app. You're automatically signed out

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

when no activity from the mouse, keyboard, or touch occurs for the specified interval of time, within the Citrix Workspace app window. The inactivity timeout does not affect the already running Citrix Virtual Apps and Desktops and Citrix DaaS sessions or the StoreFront stores.

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

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

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

```
<key>ITOEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module.

Steps to configure InactivityTimeoutInMinutes in the client machine:

1. Download the Configuring Citrix Workspace using PowerShell module.
2. To use the module, you must generate an API Client ID and Secret. For more information about obtaining credentials and getting started with the Citrix Cloud APIs, see Get started with Citrix Cloud APIs.
3. To import this module, pass the path to the Citrix.Workspace.StoreConfigs directory to the Import-Module cmdlet, that is, from the directory containing this file, run `Import-Module ./Citrix.Workspace.StoreConfigs`.
4. After the module has been imported, run `Get-Help -Full` to obtain help for a specific cmdlet. For example: `Get-Help Set-WorkspaceCustomConfigurations -Full`
5. Run the following command to set `inactivityTimeoutInMinutes` to 1 hour, for example:

   ```
   Set-WorkspaceCustomConfigurations -WorkspaceUrl -ClientId -
       ClientSecret -InactivityTimeoutInMinutes "60"
   <!--NeedCopy-->
   ```

   You don't need to run the preceding command on all clients; must run only once and test.

The end-user experience is as follows:

- A notification appears three minutes before you're signed out, with an option to stay signed in, or sign out.

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

- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click **Sign out** to end the session for the current store.

> **Note:**
>
> The inactivity timeout feature doesn't support distributions that have Wayland as the default graphics protocol. For distributions that have Wayland, uncomment either of the following: `WaylandEnable=false` in `/etc/gdm/custom.conf` or in `/etc/gdm3/custom.conf`.

Persistent login

Starting with the 2303 version, the persistent login feature enables you to stay logged in for up to the duration (2–365 days) configured by your admin. When this feature is enabled, you need not provide login credentials for the Citrix Workspace app during the configured period.

With this functionality, the SSO to Citrix DaaS sessions is extended up to a period of 365 days. This extension is based on the lifetime of Long-Lived Tokens. Your credentials are cached by default for 4 days or Lifetime whichever is lower. And then extended when you become active within these 4 days by connecting to the Citrix Workspace app.

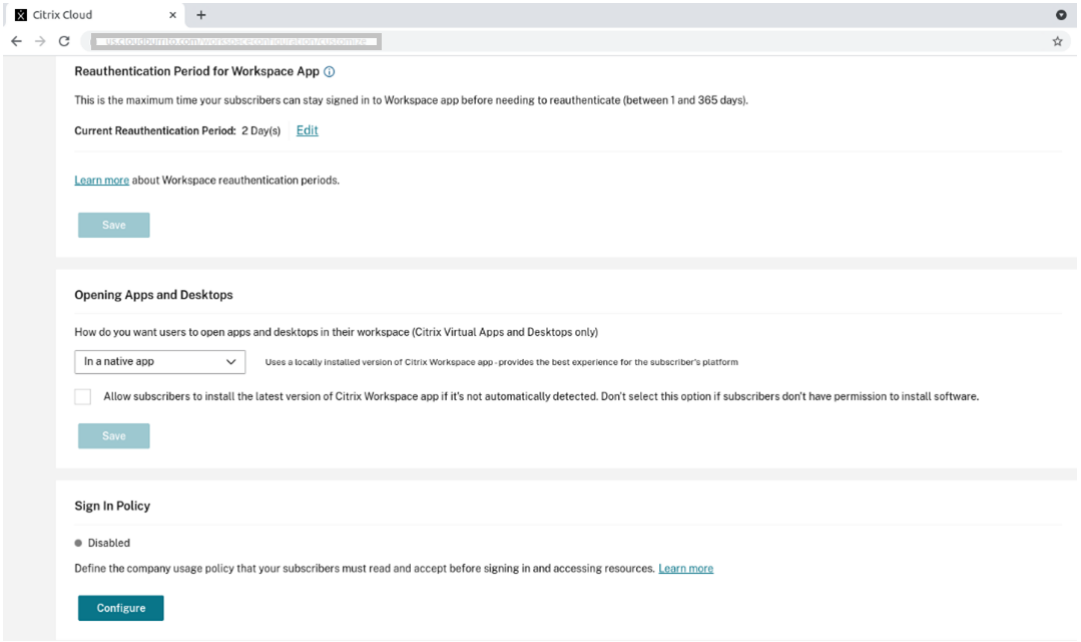
Configure the persistent login feature

An admin needs to configure the persistent login on the Workspace environment using the following procedure:

1. Sign in to Citrix Cloud.
2. In the Citrix Cloud console, click the menu in the upper left corner of the screen.
3. Select the **Workspace Configuration** option > **Customize** > **Preferences**.
4. Scroll down to **Reauthentication Period for Workspace App**.
5. Click **Edit** next to the **Current Reauthentication Period** field.
6. Enter the required days in the **Current Reauthentication Period** field.
7. You must enter two days or more in the **Current Reauthentication Period** field.

For more information, see the instructions in the **Reauthentication Period for Workspace App section** in the following image:

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

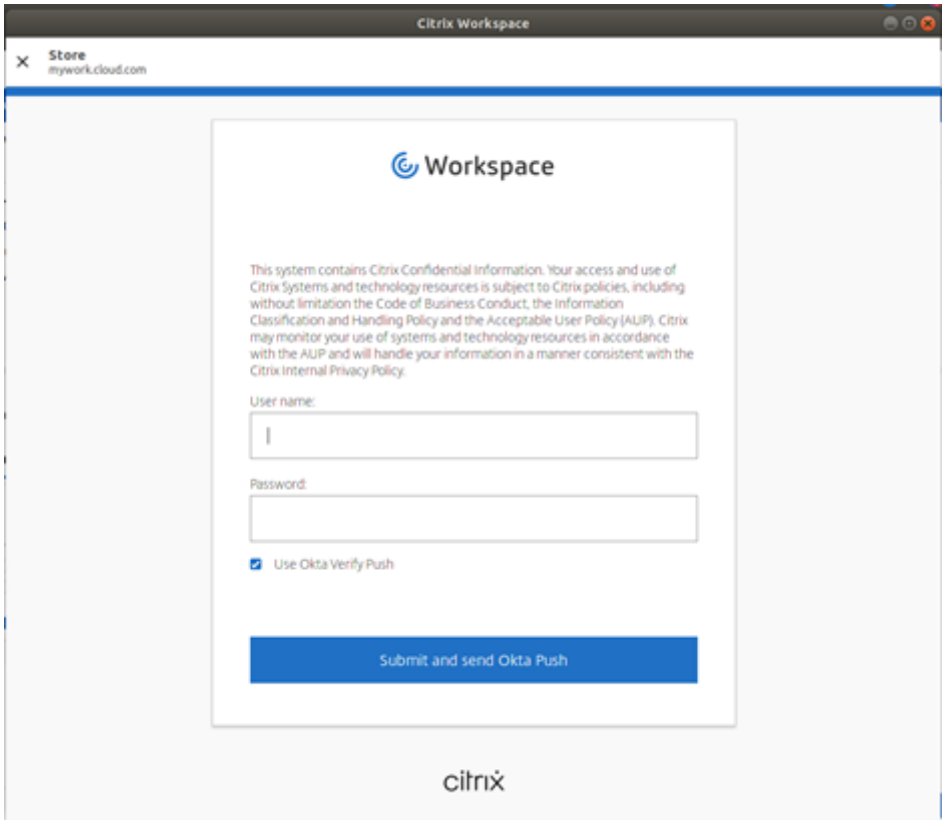


Experience with enhanced authentication

The persistent login window is embedded within the self-service window.

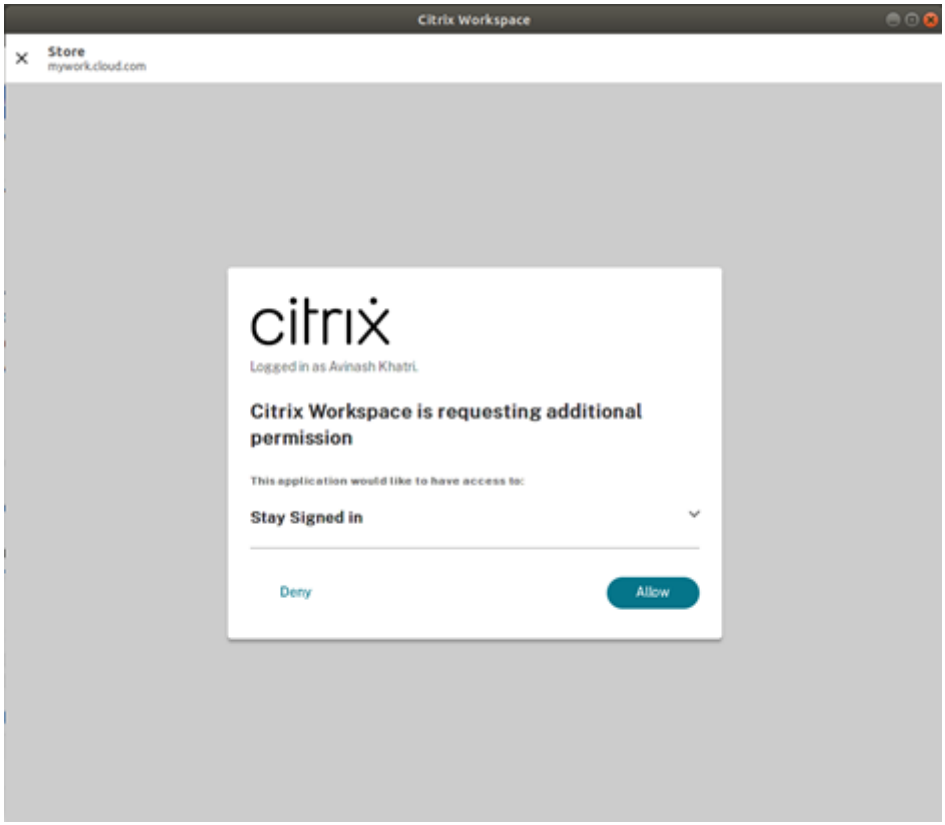
1. Access the Citrix Workspace app.
   The authentication window appears.

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



2. Sign in with your credentials.
   You are redirected to the Permission prompt to accept.

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



3. Click **Allow**.

> **Note:**
>
> If you select **Deny** for consent, you would see a second login prompt and you need to sign in to Citrix Workspace app for every 24 hours.

Disable the persistent login feature

An admin can disable the persistent login feature in the Citrix Cloud UI or in the `AuthManConfig.xml` file. However, the value set in the `AuthManConfig.xml` file overrides the value set in the Citrix Cloud UI.

Using Citrix Cloud UI

1. Sign in to Citrix Cloud.
2. In the Citrix Cloud console, click the menu in the upper left corner of the screen.
3. Select the **Workspace Configuration** option > **Customize** > **Preferences**.
4. Scroll down to **Reauthentication Period for Workspace App**.
5. Click **Edit** next to the **Current Reauthentication Period** field.
6. Enter one day in the **Current Reauthentication Period** field.

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

Using the AuthManConfig.xml file

To disable the persistent login feature, do the following

1. Navigate to <ICAROOT>/config/AuthManConfig.xml file.
2. Set the values as follows:

```
<AuthManLite>
    <primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>
    <secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>
    <longLivedTokenSupport>true</longLivedTokenSupport>
    <nativeLoggingEnabled>true</nativeLoggingEnabled>
    <platform>linux</platform>
    <saveTokens>true</saveTokens>
    <compressedGroupsEnabled>true</compressedGroupsEnabled>
</AuthManLite>
<!--NeedCopy-->
```

Creating custom user-agent strings in network request

Starting with the 2109 version, Citrix Workspace app introduces an option to append the User-Agent strings in the network request and identify the source of a network request. Based on this User-Agent strings request, you can decide how to manage your network request. This feature allows you to accept network requests only from trusted devices.

> **Note:**
>
> - This feature is supported on cloud deployments of Citrix Workspace app. Also, x86, x64, and ARMHF are the supported packages.

To customize the User-Agent strings, do the followings:

1. Locate the $ICAROOT/config/AuthManConfig.xml configuration file.
2. Add a value to the following entry:

```
<UserAgentSuffix> </UserAgentSuffix>
```

Example that includes App and Version in the customized text:

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

If you're adding App and AppVersion, separate them by a forward slash ("/").

- If the network request is from the UI-based Citrix Workspace app, the following User-Agent appears in the network requests:

  ```
  CWAWEBVIEW/CWAVersion App/AppVersion
  ```

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

- If the network request isn't from the UI-based Citrix Workspace app, the following User-Agent appears in the network requests:

  `CWA/CWAVersion App/AppVersion`

> **Notes:**
>
> - If you aren't adding AppVersion at the end of the UserAgentSuffix string, the Citrix Workspace app version is appended in the network requests.
> - Restart `AuthManagerDaemon` and `ServiceRecord` for the changes to take effect.

Service continuity

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) regardless of the health status of the cloud services.

For information on requirements that support service continuity on Citrix Workspace app, see System Requirements.

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

Pinning multi-monitor screen layout

Starting with Version 2103, you can save the selection for multi-monitor screen layout. The layout is how a desktop session is displayed. Pinning helps to relaunch a session with the selected layout, resulting in an optimized user experience.

As a prerequisite, you must enable this feature in the `AuthManConfig.xml` file. Navigate to `$ICAROOT/config/AuthManConfig.xml` and add the following entries:

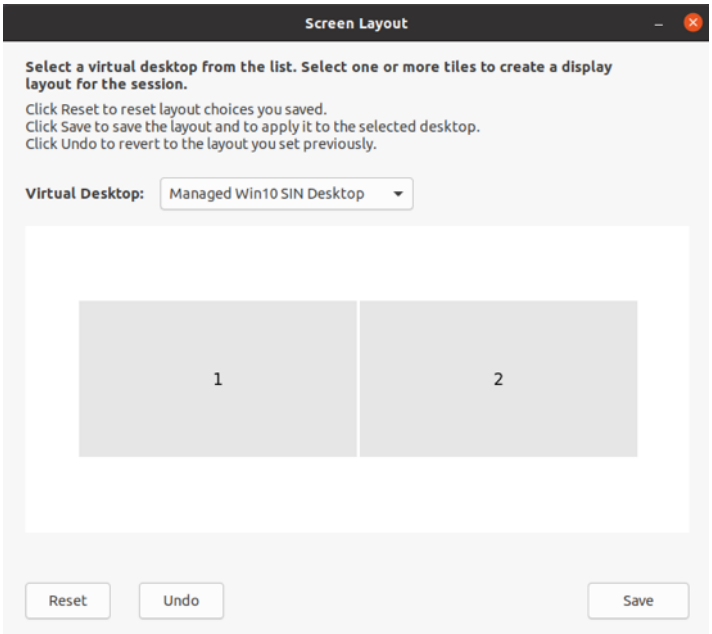
```
1       <key>ScreenPinEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Only after adding the preceding key, you can see the **Screen Layout** option in the **App indicator** icon. For more information about the app indicator icon, see App indicator icon.

To select the screen layout, click the app indicator icon in the taskbar, and select **Screen Layout**. The **Screen Layout** dialog appears.

Alternately, you can launch the **Screen Layout** dialog by pressing **Ctrl+m** keys when on the self-service window.

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



Select a virtual desktop from the drop-down menu. The layout selection is applied only to the desktop that you select.

Select one or more tiles to form a rectangular selection for the layout. The session then appears as per the layout selection.

Limitations:

- Enabling screen pinning disables the save layout feature in a session.
- This feature is applicable only on desktops that are marked as favorite.

Application Categories

Application Categories allow users to manage collections of applications in Citrix Workspace app. You can create application groups for the following:

- Applications shared across different delivery groups
- Applications used by a subset of users within delivery groups

For more information, see Create an application group in the Citrix Virtual Apps and Desktops documentation.

App Protection

> **DISCLAIMER**
>
> App Protection policies work by filtering access to required functions of the underlying operating system. Specific API calls are required to capture screen or keyboard presses. This feature

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

> means that App Protection policies can provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys can emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.

App Protection is an add-on feature that provides enhanced security when you use Citrix Virtual Apps and Desktops. The feature restricts the ability of clients to be compromised with keylogging and screen-capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information that are displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

> **Notes:**
>
> - This feature is supported when Citrix Workspace app is installed by using the tarball, Debian, and Red Hat Package Manager (RPM) packages. Also, x64 and ARMHF are the only supported architectures.
> - This feature is supported in on-premises deployments of Citrix Virtual Apps and Desktops. Also, in deployments using the Citrix Virtual Apps and Desktops Service with StoreFront.

App Protection requires that you install an add-on license on your License Server. A Citrix Virtual Desktops license must also be present. For information on Licensing, see the **Configure** section in the Citrix Virtual Apps and Desktops.

Starting with version 2108, the App Protection feature is now fully functional. The App Protection feature supports apps and desktop sessions and is enabled by default. However, you must configure the App Protection feature in the `AuthManConfig.xml` file to enable it for the authentication manager and the Self-Service plug-in interfaces.

Starting with this version, you can launch protected resources from Citrix Workspace app while Mozilla Firefox is running.

Starting with version 2012, the App Protection feature is an experimental feature.

Prerequisite:

App Protection works best with the following operating systems along with the Gnome Display Manager:

- 64-bit Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- 64-bit Debian 9 and Debian 10
- 64-bit CentOS 7
- 64-bit RHEL 7
- ARMHF 32-bit Raspberry Pi OS (Based on Debian 10 (buster))
- ARM64 Raspberry Pi OS (Based on Debian 11 (bullseye))

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

> **Note:**
>
> If you are using Citrix Workspace app earlier than version 2204, the App Protection feature does not support the operating systems that use `glibc` 2.34 or later.
>
> If you install the Citrix Workspace app with App Protection feature enabled on OS that uses `glibc` 2.34 or later, the OS boot might fail on restarting the system. To recover from the OS boot failure, do any of the following:
>
> - Reinstall the OS. However, we do not support the App Protection feature on the OS that uses `glibc` 2.34 or later.
> - Go to Recovery mode of the OS and uninstall the Citrix Workspace app using a terminal.
> - Boot through the live OS and remove the `rm -rf /etc/ld.so.preload` file from the existing OS.

Installing the App Protection component:

When you install the Citrix Workspace app using the tarball package, the following message appears.

"Do you want to install the App Protection component? Warning: You can't disable this feature. To disable it, you must uninstall Citrix Workspace app. For more information, contact your system administrator. [default $INSTALLER_N]:"

Enter **Y** to install the App Protection component.

By default, the App Protection component isn't installed.

Restart your machine for the changes to take effect. App Protection work as expected only after you restart your machine.

Installing the App Protection component on RPM packages:

Starting with Version 2104, App Protection is supported on the RPM version of Citrix Workspace app.

To install App Protection, do the following:

1. Install Citrix Workspace app.
2. Install the App Protection `ctxappprotection<version>.rpm` package from the Citrix Workspace app installer.
3. Restart the system for the changes to take effect.

Installing the App Protection component on Debian packages:

Starting with Version 2101, App Protection is supported on the Debian version of Citrix Workspace app.

For silent installation of the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

```
1 export DEBIAN_FRONTEND="noninteractive"
```

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

```
sudo debconf-set-selections <<< "icaclient app_protection/
    install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

Starting with Version 2106, Citrix Workspace app introduces an option to configure the anti-keylogging and anti-screen-capturing functionalities separately for both the authentication manager and Self-Service plug-in interfaces.

Configuring App Protection for authentication manager:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    authmananti -A 1
     <key>AuthManAntiScreenCaptureEnabled</key>
     <value>true</value>
     <key>AuthManAntiKeyLoggingEnabled</key>
     <value>true </value>

<!--NeedCopy-->
```

Configuring App Protection for the Self-Service plug-in interface:

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    protection -A 4
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>

<!--NeedCopy-->
```

Known issues:

- When you minimize a protected screen, App Protection continues to run in the background.

Limitation:

- Sometimes, you can't launch protected resources when an application that is installed from the

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

Snap Store is running. As a workaround, identify the application that causes the issue from the Citrix Workspace app log file. Also, close the application.

- When you're trying to take a screenshot of a protected window, the entire screen, including the non-protected apps in the background, are grayed out.

Battery status indicator

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

> **Note:**
>
> Starting with the 2111 version, the battery status indicator appears for server VDAs also.

The battery status indicator is enabled by default.

To disable the battery status indicator:

1. Navigate to the `<ICAROOT>/config/module.ini` folder.
2. Go to the `ICA 3.0` section.
3. Set the `MobileReceiver= Off`.

Customer Experience Improvement Program (CEIP)

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

Additional information

Citrix handles your data following the terms of your contract with Citrix. Also, protects it as specified in the Citrix Services Security Exhibit available on the Citrix Trust Center.

Citrix also uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. You might review how Google handles data collected for Google Analytics.

Clear sending CEIP data to Citrix and Google Analytics. For this activity, there is an exception for the data collected for Google Analytics indicated by * in the second table in the following section. Do the

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

following to clear sending CEIP data to Citrix and Google Analytics:

1. Navigate to the <ICAROOT>/config/module.ini folder and go to the CEIP section.
2. Select the entry EnableCeip and set it to Disable.

> **Note:**
>
> After you set the EnableCeip key to Disable, you can disable sending the final two CEIP data elements collected by Google Analytics. These data elements are Operating System version and Workspace app version. For this action, navigate to the following section and set the value as suggested:

Location: <ICAROOT>/config/module.ini

Section: GoogleAnalytics

Entry: DisableHeartBeat

Value: True

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

The specific CEIP data elements collected by Google Analytics are:

Operating system version*	Workspace app version*	App name	Workspace app language
Session launch method	Compiler version	Hardware platform	Store configuration
Citrix Virtual Apps and Desktops Session Launch Status	Authentication configuration	Connection protocol	Browser Content Redirection feature usage
Connection Lease Details	App Protection configuration		

App indicator icon

The app indicator starts when you launch Citrix Workspace app. It's an icon that is present in the notification area. With the introduction of the app indicator, the Citrix Workspace app for Linux logon performance is improved.

You can observe performance improvement when you:

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

- 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.

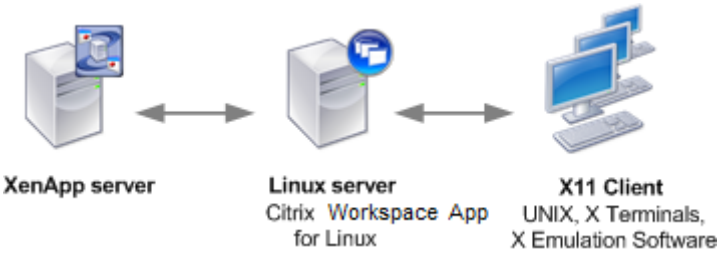
ICA-to-X proxy

You can use a workstation running Citrix Workspace app as a server and redirect the output to another X11-capable device. You might want to do this task to deliver Microsoft Windows applications to X terminals or to UNIX workstations for which Citrix Workspace app isn't available.

> **Note:**
>
> Citrix Workspace app software is available for many X devices, and installing the software on these devices is the preferred solution in these cases. Running Citrix Workspace app in this way, as an ICA-to-X proxy, is also referred to as server-side ICA.

When you run Citrix Workspace app, you can think of it as an ICA-to-X11 converter that directs the X11 output to your local Linux desktop. However, you can redirect the output to another X11 display. You can run extra copies of Citrix Workspace app simultaneously on one system. In this case, each Citrix Workspace app sends its output to a different device.

This graphic shows a system with Citrix Workspace app for Linux set up as an ICA-to-X proxy:



To set up this type of system, you need a Linux server to act as the ICA-to-X11 proxy:

- If you have X terminals already, you can run Citrix Workspace app on the Linux server that usually supplies the X applications to the X terminals.
- If you want to deploy UNIX workstations for which Citrix Workspace app isn't available, you need an extra server to act as the proxy. This server can be a PC running Linux.

Applications are supplied to the final device using X11, using the capabilities of the ICA protocol. By default, you can use drive mapping only to access the drives on the proxy. This setting isn't a problem if you're using X terminals (which usually do not have local drives). If you're delivering applications to other UNIX workstations, you can either:

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

- NFS mounts the local UNIX workstation on the workstation acting as the proxy, then point a client drive map at the NFS mount point on the proxy.
- Use an NFS-to-SMB proxy such as SAMBA, or an NFS client on the server such as Microsoft Services for UNIX.

Some features aren't passed to the final device:

- USB redirection
- Smart card redirection
- COM port redirection
- Audio isn't delivered to the X11 device, even if the server acting as a proxy supports audio.
- Client printers aren't passed through to the X11 device. You access the UNIX printer from the server manually using LPD printing, or use a network printer.
- Redirection of multimedia input isn't supported. Because, it requires a webcam on the machine that runs Citrix Workspace app, where the server acts as a proxy. However, redirection of multimedia output supports when `GStreamer` installed on the server acting as a proxy (untested).

To start Citrix Workspace app with server-side ICA from an X terminal or a UNIX workstation:

1. Use ssh or telnet to connect to the device acting as the proxy.
2. In a shell on the proxy device, set the **DISPLAY** environment variable to the local device. For example, in a C shell, type:

   ```
   setenv DISPLAY <local:0>
   ```

   > **Note:**
   >
   > If you use the command `ssh -X` to connect to the device acting as the proxy, you do not need to set the **DISPLAY** environment variable.

3. At a command prompt on the local device, type xhost <proxy server name>
4. Verify whether Citrix Workspace app is installed in the default installation directory. If not installed, verify that the environment variable ICAROOT is set to point to the actual installation directory.
5. Locate the directory where Citrix Workspace app is installed. At a command prompt, type `selfservice &`.

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 give Citrix resources more efficiently, by that provides better performance to the users. The following types of URL can be redirected:

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

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

The URL is opened using the server application when:

- Citrix Workspace app does not have an appropriate application
- Citrix Workspace app can't directly access the content

Server-client content redirection is configured on the server. This feature is enabled by default in Citrix Workspace app if the path includes the following:

- RealPlayer
- One of Firefox, Mozilla, or Netscape.

To enable server-client content redirection if RealPlayer and a browser aren't in the path:

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

   Path=path

   Command=command

   The path is the directory where the browser executable is located. The command is the name of the executable used to handle redirected browser URLs, appended with the URL sent by the server. For example:

   `$ICAROOT/nslaunch` Netscape, Firefox, Mozilla

   This setting specifies the following:

   - The `nslaunch` utility is run to push the URL into an existing browser window
   - Each browser in the list is tried in turn until content can be displayed successfully
3. In the [Player] section, modify the following settings:

   Path=path

   Command=command

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

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

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

To clear server-client content redirection from Citrix Workspace:

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

Connection

Configure connections

On devices with limited processing power or where limited bandwidth is available, there's a trade-off between performance and functionality. Users and administrators can choose an acceptable mixture of rich functionality and interactive performance. Making one or more of these changes, often on the server not the user device, can reduce the bandwidth that a connection requires and can improve performance:

- **Enable SpeedScreen Latency Reduction** - The SpeedScreen Latency Reduction improves performance over high latency connections. For this improvement, an instant feedback is provided to the user in response to typed data or mouse clicks. Use the SpeedScreen Latency Reduction Manager to enable this feature on the server. By default, in Citrix Workspace app, this feature is disabled for a keyboard. This feature is only enabled for the mouse on high latency connections. For more information, see the Citrix Workspace app for Linux OEM's reference guide.
- **Enable data compression** - Data compression reduces the amount of data transferred across the connection. This configuration requires more processor resources to compress and decompress the data, but it can increase performance over low-bandwidth connections. Use the **Citrix Audio Quality and Image Compression** policy settings to enable this feature.
- **Reduce the window size** - Change the window size to the minimum that is comfortable. On the farm set the Session Options.
- **Reduce the number of colors** - Reduce the number of colors to 256. On the Citrix Virtual Apps and Desktops or Citrix DaaS site, set the Session Options.
- **Reduce sound quality** - If audio mapping is enabled, reduce the sound quality to the minimum setting using the Citrix Audio quality policy setting.

For information about troubleshooting, see Connections in the troubleshooting section.

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

Font

ClearType font smoothing

ClearType font smoothing improves the quality of displayed fonts beyond the available quality through:

- traditional font smoothing or,
- anti-aliasing.

ClearType font smoothing is also known as subpixel font rendering. You can turn this feature on or off.

You can also specify the type of smoothing by doing the following:

1. Navigate to the [WFClient] section of the appropriate configuration file.
2. Edit the following setting:

   FontSmoothingType = number

   Where the number can take one of the following values:

Value	Behavior
0	The local preference on the device is used. The **FontSmoothingTypePref** setting defines this value.
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing

Both standard smoothing and ClearType smoothing can increase Citrix Workspace app's bandwidth requirements.

> **Important:**
>
> The server can configure `FontSmoothingType` through the `ICA` file. This value takes precedence over the value set in [WFClient].

If the server sets the value to 0, the following setting in the [WFClient] determines the local preference: FontSmoothingTypePref = number

Where a number can take one of the following values:

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

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. As a result, these folders remain fixed across different server types and server farm configurations. It is important if, for example, a mobile user logs on to servers in different server farms. For static, desk-based workstations, where the user can log on to servers that reside in a single-server farm, special folder redirection is rarely necessary.

To configure special folder redirection:

Enable special folder redirection by making an entry in the module.ini file and specify the folder locations as follows:

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

   [ClientDrive]

   SFRAllowed = True

   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.

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

- 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 and Desktops and Citrix DaaS server to be redirected to directories that exist on the local user device. For example, drive H in a Citrix user session can be mapped to a directory on the local user device running the Workspace app.

Client drive mapping can make any directory mount on the local user device. The local user device includes a CD-ROM, DVD, or a USB memory stick, that are available to the user during a session. Also, the local user has permission to access the local user device. When a server is configured to allow client drive mapping:

- users can access their locally stored files
- Use the files during their session
- and then save them again either on a local drive or on a drive on the server.

Citrix Workspace app supports client device mapping for connections to Citrix Virtual Apps and Desktops and Citrix DaaS servers. This feature enables a remote application that runs on the server to access devices attached to the local user device. The applications and system resources appear to the user at the user device as if they're running locally. Verify that client device mapping is supported on the server before using these features.

> **Note:**
>
> The Security-Enhanced Linux (SELinux) security model can affect the operation of the Client Drive Mapping and USB Redirection features. This model is applicable on both Citrix Virtual Apps and Desktops and Citrix DaaS. If you require either or both of these features, disable SELinux before configuring them on the server.

Two types of drive mapping are available:

- Static client drive mapping - Enables administrators to map any part of a user device's file system to a specified drive on the server at logon. For example, it can be used to map all or part of a user's home directory or /tmp. Also, map the mount points of mass storage devices such as CD-ROMs, DVDs, or USB memory sticks.
- Dynamic client drive mapping - Monitors the directories in which mass storage devices 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 and Desktops or Citrix DaaS, client drive mappings are reestablished unless client device mapping is disabled. You can use policies to give you

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

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`.

Starting with version 2101, access to mapped drives comes with an extra security feature.

You can now select the access level for the mapped drive for every store in a session.

To stop the access level dialog from appearing every time, select the **Do not ask me again** option. The setting is applied on that particular store.

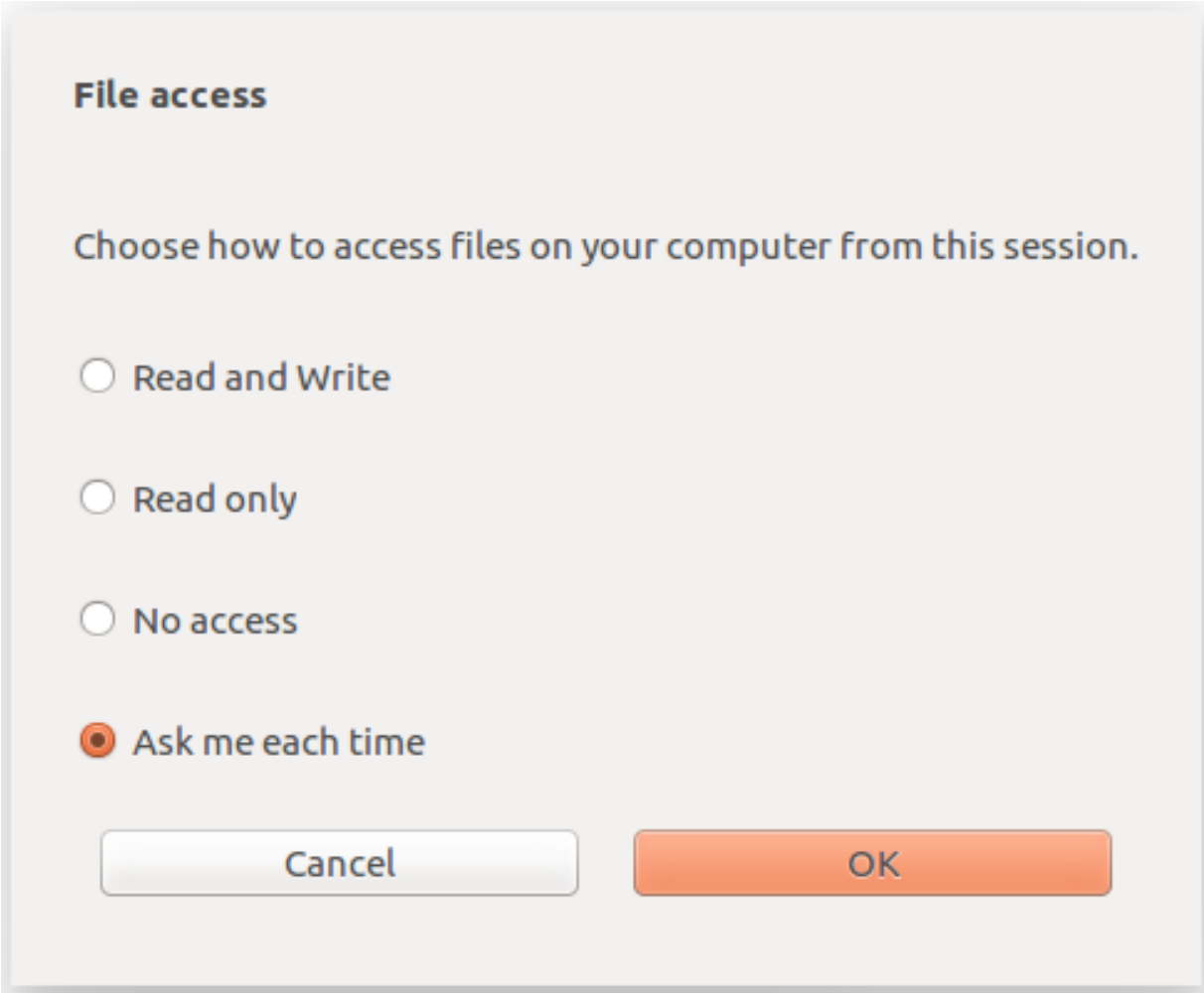
Otherwise, you can set the access levels that appear every time a session is launched.

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

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

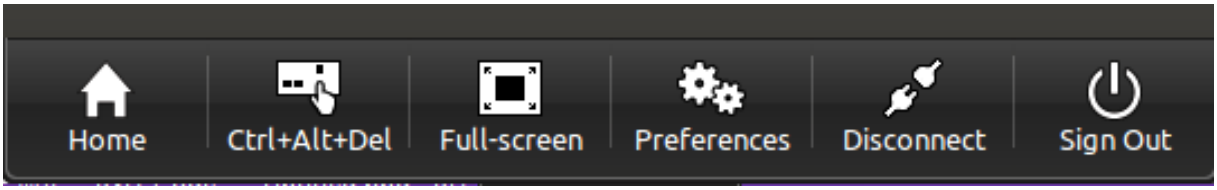
> **Note:**
>
> The file access setting isn't persistent across sessions when using workspace for web. It defaults to the **Ask me each time** option.

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



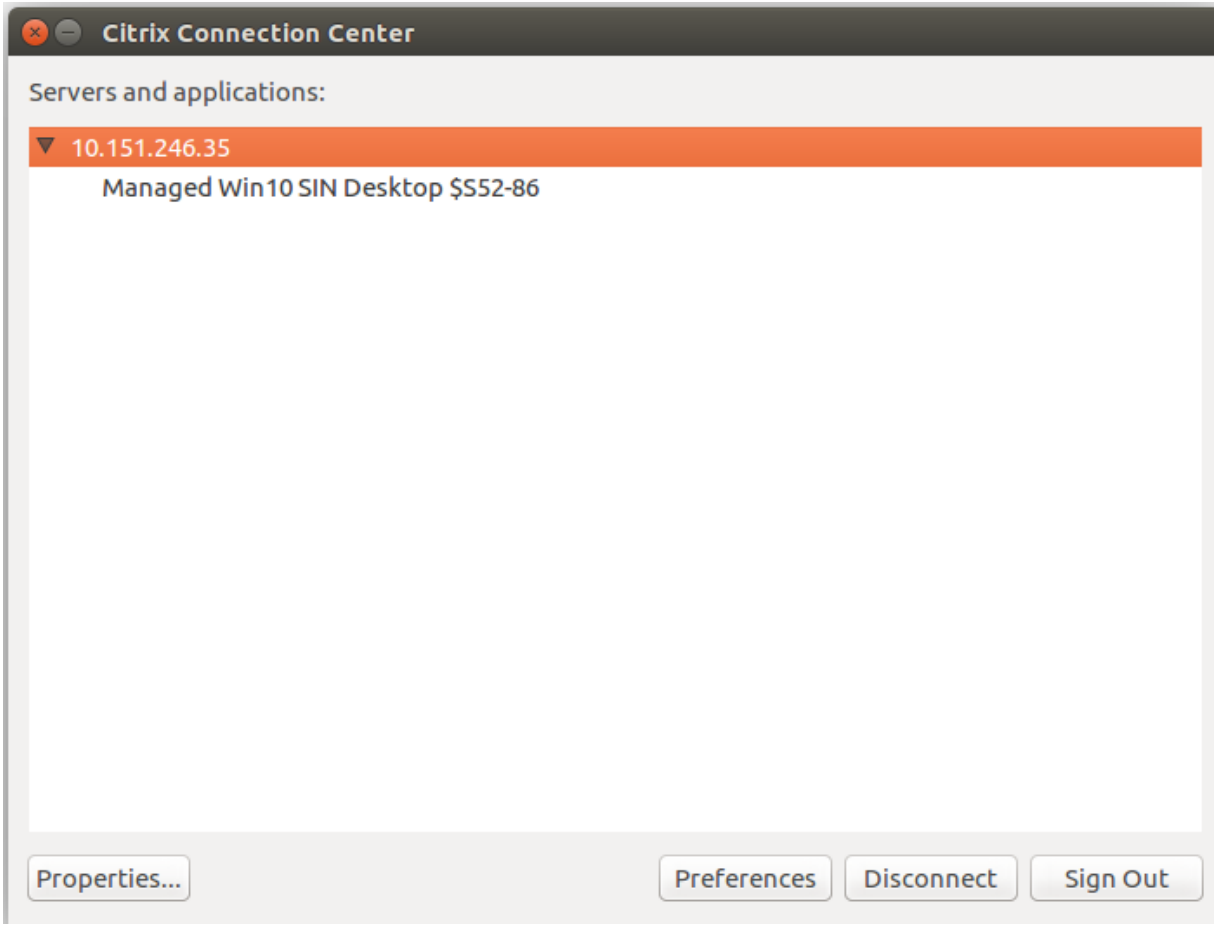
You can use the `wfclient.ini` file to configure the mapped path and file name attributes. Use the GUI to set a file access level as shown in the preceding screen capture.

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



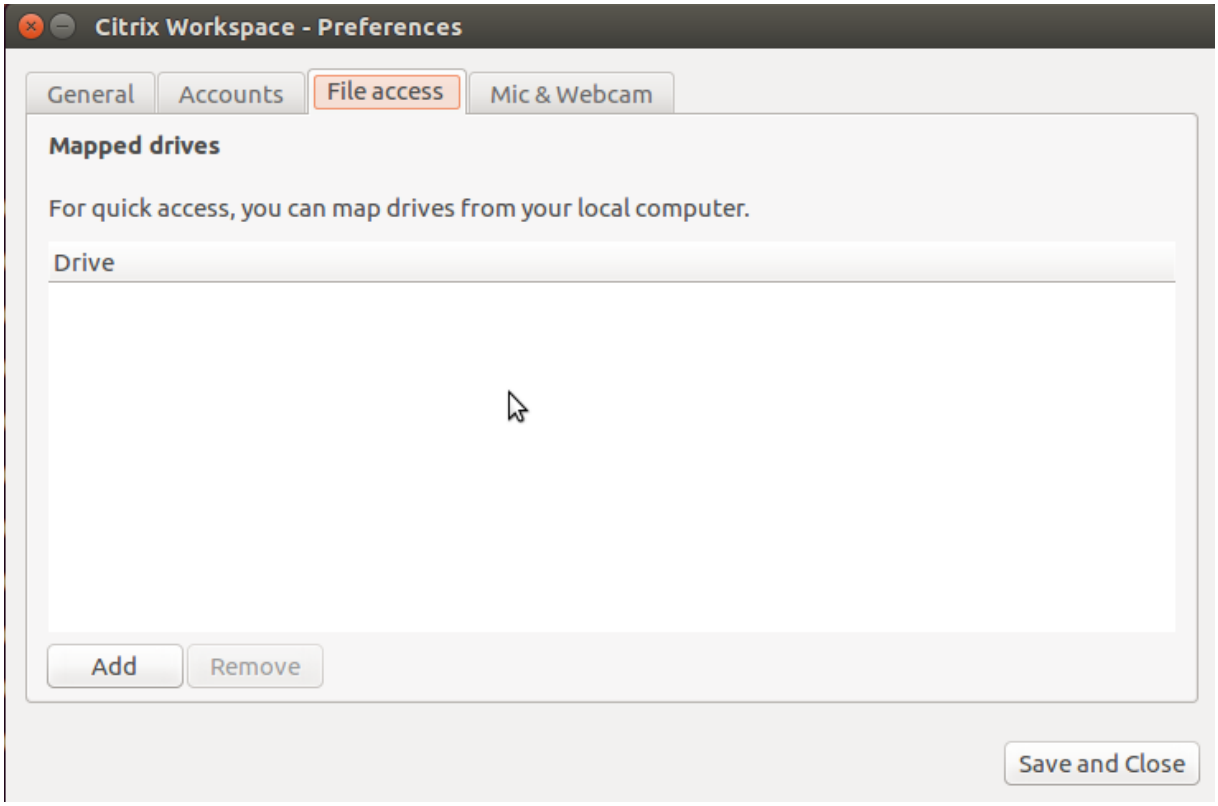
In an app session, you can set a file access level by launching the **File access** dialog from **Citrix Connection Center**.

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



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

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



The access level flag isn't 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 and Desktops and Citrix DaaS lets users:

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

These settings, however, might not be perfect in all environments. For example, the default setting that allows users to print to all printers accessible from the user device is the easiest to administer initially. But the default setting might create slower logon times in some environments. In this situation, you might want to limit the list of printers configured on the user device.

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

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

- $ICAROOT/config directory to limit the printers for all Workspace app users. All users in this case are those users who first use the self-service program after the change.

2. In the [WFClient] section of the file type:

   ClientPrinterList=printer1:printer2:printer3

   Where printer1, printer2, and so on, are the names of the chosen printers. Separate printer name entries by a colon (:).

3. Save and close the file.

Map a local printer

The Citrix Workspace app for Linux supports the Citrix PS Universal Printer Driver. So, usually no local configuration is required for users to print to network printers or printers that are attached locally to user devices. You might manually map client printers on Citrix Virtual Apps and Desktops or Citrix DaaS for Windows 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 and Desktops or Citrix DaaS.
2. On the Start menu, choose **Settings > Printers**.
3. On the File menu, choose **Add Printer**.

   The Add Printer wizard appears.

4. Use the wizard to add a network printer from the Client Network, Client domain. Usually this value is a standard printer name, similar to values created by native Remote Desktop Services, such as "HP LaserJet 4 from client name in session 3."

   For more information about adding printers, see your Windows operating system documentation.

Audio

Client audio mapping enables applications that run on the Citrix Virtual Apps and Desktops or Citrix DaaS server to play sounds and record audio through a sound device installed on the user device. You can configure client audio mapping using policies. For more information, see the Citrix Virtual Apps and Desktops documentation.

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

Support for audio recording

Starting with version 2212, the audio recording feature is enabled by default. The devices to record audio appear when a session starts.

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

> **Note:**
>
> - The **Mic and Webcam** option in the **Preferences** dialog is disabled by default. For information on how to enable the mic and webcam, see Preferences.

Support for multiple audio devices

Starting with Version 2112, the `VdcamVersion4Support` attribute in the `module.ini` file is renamed to `AudioRedirectionV4`. Starting with version 2212, the default value for `AudioRedirectionV4` is set to **True**. As a result:

- the PulseAudio library is used to access the audio devices and extra devices are supported.
- more than one app can use the audio devices at a time.
- Citrix Workspace app displays all local audio devices that are available in a session. Instead of Citrix HDX Audio, the audio devices appear with their respective device names. You can select an audio device in an app in a session or use the default audio device during a session which is also the default audio device of the client machine. If necessary, you can change the default audio device from the system settings of the client machine. After the default audio device of the client machine is updated, the new device appears as the default audio device in the session.
- sessions update dynamically when you plug in or remove audio devices.

If you set the value of `AudioRedirectionV4` to **False**:

- the ALSA library is used to access the audio devices and only single device is supported.
- In a session, there is only one speaker and one microphone with the name “Citrix HDX Audio”, which corresponds to the default device on the client side.
- only one app can use the Citrix HDX Audio device at a time.

To set the `AudioRedirectionV4` to **False**, 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:

   AudioRedirectionV4=False
3. Restart the session for the changes to take effect.

Known limitations:

By default, the `AudioRedirectionV4` value is set to **True**. The following known limitation is present when the value of `AudioRedirectionV4` is set to **True**:

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

- If you launch a session from the command-line interface with root privilege, the PulseAudio server might refuse the connection when trying to connect to it. In this case, the audio devices might start using the ALSA library which supports single devices only.

If you set the `AudioRedirectionV4` value to **False**, the following known limitations are present:

- You can't change the audio device selection in a session. The selection is set to the default audio input and output only. This limitation is resolved when you set the `AudioRedirectionV4` value to **True**.
- Audio device redirection isn't supported with Bluetooth and HDMI audio devices. This limitation is resolved when you set the `AudioRedirectionV4` value to **True**.

When the `AudioRedirectionV4` value is **False**, 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\>
<!--NeedCopy-->
```

In this section, the device information is present in the ALSA configuration file on your operating system.

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

Enhancement to improve audio quality

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

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

Starting with version 2207, you can select the appropriate playback threshold and pulse audio prebuffer to improve the audio quality. For this enhancement, the following parameters are added in the

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

[ClientAudio] section of the `module.ini` file:

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

Improved audio echo cancellation support

Starting with the 2303 version, Citrix Workspace app supports echo cancellation. This feature is designed for real-time user cases, and it improves the user experience. The echo cancellation feature supports low quality, medium quality, and adaptive audio. Citrix recommends using adaptive audio for better performance.

By default, the echo cancellation feature is disabled. During real-time user cases, it is recommended to turn on the echo cancellation if the speaker is used instead of the headset.

To enable this feature, do the following:

1. Navigate to the `<ICAROOT>/config` folder and open the `module.ini` file.
2. Go to the [ClientAudio] section and update the value of the `EnableEchoCancellation` parameter as follows:

   ```
   EnableEchoCancellation =TRUE
   ```

Limitation:

By design, the echo cancellation feature is disabled for high quality audio. For more information on high quality audio, see the Citrix Virtual Apps and Desktops documentation.

Addition of client-side jitter buffer mechanism

Starting with version 2305, Citrix Workspace app ensures clear audio even when the network latency fluctuates. By default, this feature is enabled.

To disable this feature, navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file and edit `JitterBufferEnabled=FALSE`.

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

Adaptive audio

Starting with version 2109, Citrix Workspace app supports adaptive audio. With adaptive audio, you don't need to manually configure the audio quality policies on the VDA. Adaptive audio optimizes settings for your environment and replaces obsolete audio compression formats to provide an excellent user experience. Adaptive audio is enabled by default. For more information, see Adaptive audio.

Starting with version 2112, adaptive audio works when using User Datagram Protocol (UDP) audio delivery.

Known limitation:

- Adaptive audio requires CPU processors that support Streaming SIMD Extensions (SSE) 4.x. Citrix Workspace app might be closed when adaptive audio is used with the CPU processor that doesn't support SSE 4.x.

Enabling UDP audio

UDP audio can improve the quality of phone calls made over the Internet. It uses UDP instead of TCP.

Starting with Version 2112, adaptive audio works when using UDP audio delivery. Also, from this version, Citrix Workspace app supports the Datagram Transport Layer Security (DTLS) protocol for UDP audio. As a result, you can access the UDP audio through Citrix Gateway. By default, this feature is disabled.

Starting with version 2202, Citrix Workspace app supports UDP audio through Citrix Gateway.

To enable UDP audio:

1. Navigate to the `<ICAROOT>/config` folder and open the module.ini file.
2. Set the following options in the [ClientAudio] section of module.ini:
    - Set `EnableUDPAudio` to **True**. By default, this value is set to **False**, which disables UDP audio.
    - Specify the minimum and maximum port numbers for UDP audio traffic using `UDPAudioPortLow` and `UDPAudioPortHigh` respectively. By default, ports 16500–16509 are used.
3. Set the following policies on the Domain Delivery Controller (DDC):
    - Set **Audio over UDP** to **Allowed**.
    - Set **Audio over UDP real-time transport** to **Enabled**.
4. By default, adaptive audio is enabled on the VDA and supports UDP audio. If you have disabled adaptive audio, set the following policy on the Domain Delivery Controller (DDC):
    - Set **Audio quality** to **Medium**.

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

As a result, the resultant audio is of a medium quality, and it can support UDP audio.

To enable UDP audio through Citrix Gateway:

1. Navigate to the <ICAROOT>/config folder and open the module.ini file.
2. Go to the [WFClient] section and set the following entry:

   EnableUDPThroughGateway=True

3. Go to the [ClientAudio] section and set the following entry:

   EnableUDPAudio=True

4. Set the following policies on the Domain Delivery Controller (DDC):

   - Set **Audio over UDP** to **Allowed**.
   - Set **Audio over UDP real-time transport** to **Enabled**.

5. By default, adaptive audio is enabled on the VDA and supports UDP audio. If you have disabled adaptive audio, set the following policy on the Domain Delivery Controller (DDC):

   - Set **Audio quality** to **Medium**.

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 after enabling auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default. USB devices available for remoting include the following:

- Flash drives
- Smartphones
- PDAs
- Printers
- Scanners
- MP3 players
- Security devices
- Tablets

USB redirection requires either Citrix Virtual Apps and Desktops 7.6 or later.

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

The following types of devices are supported directly in a virtual apps and desktops session, and so do not use USB support:

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

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

> **Note:**
>
> Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. For information on configuring policy rules for other specialist USB devices, see CTX119722.

By default, certain types of USB devices aren't supported for remoting through Citrix Virtual Apps and Desktops or Citrix DaaS. For example, a user might have a NIC attached to the system board by internal USB. Remoting this NIC wouldn't be appropriate. By default, the following types of USB device aren't supported for use in the virtual apps and desktops:

- Bluetooth dongles
- Integrated NICs
- USB hubs

To update the default list of USB devices available for remoting, edit the `usb.conf` file in the `$ICAROOT/` folder. For more information, see the Update the list of USB devices available for remoting section.

To allow the remoting of USB devices to virtual desktops, enable the USB policy rule. For more information, see the Citrix Virtual Apps and Desktops documentation.

How USB support works

When a user plugs a USB device, it's checked against the USB policy. And, if allowed, redirected to the virtual desktop. If the default policy denies the device, it's available only to the local desktop.

Consider a user plug in a USB device in desktops accessed through desktop appliance mode. In this case, that device is auto-redirected to the virtual desktop after enabling auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default. To configure the auto-redirection of USB devices, do the following:

1. Navigate to the `$Home/.ICAClient/wfclient.ini` configuration file.
2. Add the following entry:

   DesktopApplianceMode=True
3. Navigate to `/opt/Citrix/ICAClient/usb.conf` configuration file.
4. Set any of the following device rules:

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

- CONNECT – Set the “CONNECT” keyword to enable auto redirect of a device when a session starts.
- ALLOW – Set the “ALLOW” keyword to allow auto-redirect of a device only after a session starts.
  However, if the “CONNECT” or “ALLOW” keyword is set, the device is auto-redirected when it is unplugged and plugged in during a session.

Sample device rule:
CONNECT: vid=046D pid=0002 # Allow a specific device by vid/pid
ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid

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.

Known limitation:

For USB redirection, the policies defined in the `usb.conf` file might not work and the USB devices might not be redirected into session. This issue occurs if you have more than 2000 characters present in the `usb.conf` file. As a workaround, you can remove the existing comments to the policies to reduce the number of characters in the `usb.conf` file.

Mass storage devices

Consider that a user disconnects from a virtual desktop when a USB mass storage device is still plugged in to the local desktop. In this case, that device isn’t redirected to the virtual desktop when the user reconnects. To verify 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, Citrix Workspace app doesn’t accept the device. And a separate Linux file browser might open. So, Citrix recommends that you pre-configure user devices with the **Browse removable media when inserted** setting cleared by default. On Debian-based devices, do this using the Debian menu bar by selecting **Desktop > Preferences > Removable Drives and Media**. And on the **Storage** tab, under **Removable Storage**, clear the **Browse removable media when inserted** check box.

For the Client USB device redirection, note the following points.

> **Notes:**
>
> Consider that the Client USB device redirection server policy is turned on. In this case, the mass storage devices are directed as USB devices even if client drive mapping is turned on.

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

USB classes

The default USB policy rules allow the following classes of USB device:

- Audio (Class 01)

  Includes microphones, speakers, headsets, and MIDI controllers.

- Physical Interface (Class 05)

  These devices are similar to HIDs, but generally provide real-time input or feedback. Also, include force feedback joysticks, motion platforms, and force feedback exoskeletons.

- Still Imaging (Class 06)

  Includes digital cameras and scanners. Digital cameras support the still imaging class that uses the 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 the setup menus provided by the camera itself.

  If a camera appears as a mass storage device, client drive mapping is used, and USB support isn't 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's a wide variety of devices having internal storage which also presents a mass storage interface. These devices include media players, digital cameras, and mobile phones. Known subclasses include:

- 01 Limited flash devices
- 02 Typically CD/DVD devices (ATAPI/MMC-2)
- 03 Typically tape devices (QIC-157)
- 04 Typically floppy disk drives (UFI)
- 05 Typically floppy disk drives (SFF-8070i)
- 06 Most mass storage devices use this variant of SCSI

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

Mass storage devices can often be accessed through client drive mapping, and so USB support isn't required.

Important: Some viruses are known to propagate actively using all types of mass storage. Consider carefully whether there's a business requirement to allow 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 run-through client drive mapping.

> **Note:**
>
> Currently, if user requires to redirect a USB 3.0 driver to the Linux VDA using generic USB redirection, plug-in the USB flash drive into a USB 3.0 slot.

- Content Security (Class 0d)

  Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.

- Personal Healthcare (Class 0f)

  These devices include personal healthcare devices such as the following:

  - Blood pressure sensors
  - Heart rate monitors
  - Pedometers
  - Pill monitors
  - Spirometers

- Application and Vendor Specific (Classes fe and ff)

  Many devices use vendor-specific protocols or protocols not standardized by the USB consortium, and these devices usually appear as vendor-specific (class ff).

USB device classes

The default USB policy rules deny the following classes of USB devices:

- Communications and CDC Control (Classes 02 and 0a)

  Includes modems, ISDN adapters, network adapters, and some telephones and fax machines.

  The default USB policy does not allow these devices, because one of them might be providing the connection to the virtual desktop itself.

- Human Interface Devices (Class 03)

  Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are the following:

  - Keyboards

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

  - Mice
  - Pointing devices
  - graphic tablets
  - Sensors
  - Game controllers
  - Buttons
  - Control functions

  Subclass 01 is known as the boot interface class and is used for keyboards and mice.

  The default USB policy does not allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). This setting is because most keyboards and mice are handled appropriately without USB support. And it's normally necessary to use these devices locally as well remotely when connecting to a virtual desktop.

- USB Hubs (Class 09)

  USB Hubs allow extra devices to be connected to the local computer. It isn't necessary to access these devices remotely.

- Smart card (Class 0b)

  Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card equivalent chip.

  Smart card readers are accessed using smart card remoting and do not require USB support.

- Video (Class 0e)

  The video class covers devices that are used to manipulate video or video-related material, such as:

  - Webcams
  - Digital camcorders
  - Analog video converters
  - Some television tuners
  - Some digital cameras that support video streaming

  By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression.

- Wireless Controllers (Class e0)

  Includes a wide variety of wireless controllers, such as ultrawide band controllers and Bluetooth.

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

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

The default USB policy does not allow these devices. However, there might be particular devices it's appropriate to provide access to using USB support.

List of USB devices

You can update the range of USB devices available for remoting to desktops. To update the range, edit the list of default rules in the `usb.conf` file on the user device in `$ICAROOT/`.

You can update the list by adding new policy rules to allow or deny USB devices not included in the default range. Rules created by an administrator in this way control which devices are offered to the server. The rules on the server control which of these devices are to be accepted.

The default policy configuration for disallowed devices is:

DENY: class=09 # Hub devices

DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

USB policy rules

Tip: When creating policy rules, see the USB Class Codes, available from the USB website at http://www.usb.org/. Policy rules in the `usb.conf` file on the user device take the format {ALLOW:|DENY:} followed by a set of expressions 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

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

Tag	Description
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 isn't required and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- Whitespace used as a separator is ignored, but can't appear in the middle of a number or identifier. For example, Deny: Class=08 SubClass=05 is a valid rule; Deny: Class=0 8 Sub Class=05 isn't.
- Tags must use the matching operator "=." For example, VID=1230.

Example

The following example shows a section of the `usb.conf` file on the user device. For these rules to be implemented, the same set of rules must exist on the server.

```
ALLOW: VID=1230 PID=0007 \## ANOther Industries, ANOther Flash Drive

DENY: Class=08 SubClass=05 \## Mass Storage Devices

DENY: Class=0D \## All Security Devices
```

Start-up modes

Using desktop appliance mode, you can change how a virtual desktop handles previously attached USB devices. In the **WfClient** section of the `$ICAROOT/config/module.ini` file on each user device, set `DesktopApplianceMode = Boolean` as follows.

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

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

> **Note:**
>
> Set the “CONNECT” keyword to enable the auto redirect of a device when a session starts. Also, set the “ALLOW” keyword to allow auto-redirect of a device only after a session starts. However, if the CONNECT or ALLOW keyword is set, the device is auto-redirected when it is unplugged and plugged in during a session.

Configure auto-redirection of USB devices

Earlier when a device was unplugged and plugged in during a session, the device was redirected automatically. As a result, the device was auto-connected to the VDA. With the Citrix Workspace app 2207 release, you are required to enable auto-redirection manually through configuration file settings. Auto-redirection of USB devices is disabled by default.

To configure the auto-redirection of USB devices (regular and composite devices), do the following:

1. Navigate to the $Home/.ICAClient/wfclient.ini configuration file.
2. Add the following entry:

   DesktopApplianceMode=True
3. Navigate to /opt/Citrix/ICAClient/usb.conf configuration file.
4. Set any of the following device rules:
   - CONNECT – Set the “CONNECT” keyword to enable auto redirect of a device when a session starts.
   - ALLOW – Set the “ALLOW” keyword to allow auto-redirect of a device only after a session starts.

   However, if the CONNECT or ALLOW keyword is set, the device is auto-redirected when it unplugged and plugged in during a session.

Sample device rule:

CONNECT: vid=046D pid=0002 # Allow a specific device by vid/pid‘

ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid‘

Composite USB device redirection

Starting with the 2207 version, Citrix Workspace app allows splitting of composite USB devices. A composite USB device can perform more than one function. These functions are accomplished by exposing each of those functions using different interfaces. Examples of composite USB devices include HID devices that consist of audio and video input and output.

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

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

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

USB 2.1 and later supports the notion of USB composite devices where multiple child devices share a single connection with the same USB bus. Such devices employ a single configuration space and shared bus connection where a unique interface number 00-ff is used to identify each child device. This setting is not the same as a USB hub which provides a new USB bus origin for other independently addressed USB devices for connection.

Composite devices found on the client endpoint can be forwarded to the virtual host as either:

- a single composite USB device, or
- a set of independent child devices (split devices)

When a composite USB device is forwarded, the entire device becomes unavailable to the endpoint. This action blocks the local usage of the device for all applications on the endpoint, including the Citrix Workspace client needed for an optimized HDX remote experience.

Consider a USB headset device with both audio device and HID button for mute and volume control. If the entire device is forwarded using a generic USB channel, the device becomes unavailable for redirection over the optimized HDX audio channel. However, you can achieve the best experience when the audio is sent through the optimized HDX audio channel unlike the audio sent using host-side audio drivers through generic USB remoting. This is because of the noisy nature of the USB audio protocols.

You also notice issues when the system keyboard or pointing device are part of a composite device with other integrated features required for the remote session support. When a complete composite device is forwarded, the system keyboard or mouse becomes inoperable at the endpoint, except within the remote desktop session or application.

To resolve these issues, Citrix recommends that you split the composite device and forward only the child interfaces that use a generic USB channel. This setting ensures that the other child devices are available for use by applications on the client endpoint, including the Citrix Workspace app that provides optimized HDX experiences, while allowing only the required devices to be forwarded and available to the remote session.

Device Rules:

As with regular USB devices, the composite devices for forwarding are selected based on the device rules set in the Citrix Workspace app configuration. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

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

Each rule consists of an action keyword (Allow, Connect, or Deny), a colon (:), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a # character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

To modify the device rules, do the following:

1. Navigate to the /opt/Citrix/ICAClient/usb.conf file.
2. Update the device rules as required.

Sample device rules:

```
ALLOW: vid=046D pid=0102 ## Allow a specific device by vid/pid

ALLOW: vid=0505 class=03 subclass=01 ## Allow any pid for vendor 0505 w/
subclass=01

DENY: vid=0850 pid=040C ## deny a specific device (including all child
devices)

DENY: class=03 subclass=01 prot=01 ## deny any device that matches all
filters

CONNECT: vid=0911 pid=0C1C ## Allow and auto-connect a specific device

ALLOW: vid=0286 pid=0101 split=01 ## Split this device and allow all
interfaces

ALLOW: vid=1050 pid=0407 split=01 intf=00,01 ## Split and allow only 2
interfaces

CONNECT: vid=1050 pid=0407 split=01 intf=02 ## Split and auto-connect
interface 2

DENY: vid=1050 pid=0407 split=1 intf=03 ## Prevent interface 03 from being
remoted
```

You can use any of the following filter parameters to apply rules to the encountered devices:

Filter parameter	Description
vid=xxxx	USB device vendor ID (four-digit hexadecimal code)
pid=xxxx	USB device product ID (four-digit hexadecimal code)

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

Filter parameter	Description
rel=xxxx	USB device release ID (four-digit hexadecimal code)
class=xx	USB device class code (two-digit hexadecimal code)
subclass=xx	USB device subclass code (two-digit hexadecimal code)
prot=xx	USB device protocol code (two-digit hexadecimal code)
split=1 (or split=0)	Select a composite device to be split (or non-split)
intf=xx[,xx,xx,…]	Selects a specific set of child interfaces of a composite device (comma-separated list of two-digit hexadecimal codes)

The first six parameters select the USB devices for which the rule must be applied. If any parameter is not specified, the rule matches a device with ANY value for that parameter.

The USB Implementors Forum maintains a list of defined class, subclass, and protocol values in Defined Class Codes. USB-IF also maintains a list of registered vendor IDs. You can check the vendor, product, release, and interface IDs of a specific device using a free tool like lsusb:

```
 <username@username>-ThinkPad-T470:/var/log$ lsusb

Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW

Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.

Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera

Bus 001 Device 003: ID 8087:0a2b Intel Corp.

Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver

```

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

```
Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver

Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.

Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

<!--NeedCopy-->
```

```
    | <username@username>-ThinkPad-T470:/var/log$ lsusb -t

    /:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000
       M

    /:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M

    /:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M

    |__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage,
       5000M

    /:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M

    |__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M

        |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=
           usbhid, 12M

        |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=
           usbhid, 12M

        |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=
           usbhid, 12M

        |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12
           M

        |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=,
            12M

        |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12
           M
```

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

```
27          |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12
               M
28
29          |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=
               usbhid, 12M
30
31      |__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=
           usbhid, 12M
32
33      |__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
           usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
           usbhid, 12M
36
37      |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39      |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41      |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43      |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45      |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
           |
46
47  <!--NeedCopy-->
```

When present, the last two parameters apply only to USB composite devices. The split parameter determines if a composite device must be forwarded as split devices or as a single composite device.

Split=1 indicates that the selected child interfaces of a composite device must be forwarded as split devices.
Split=0 indicates that the composite device must not be split.

> **Note:**
>
> If the split parameter is omitted, Split=0 is assumed.

The intf parameter selects the specific child interfaces of the composite device to which the action must be applied. If omitted, the action applies to all interfaces of the composite device.

Consider a composite USB device (For example, the Bloomberg 4 keyboard) with six interfaces:

- Interface 0 - Bloomberg 4 Keyboard HID
- Interface 1 - Bloomberg 4 Keyboard HID
- Interface 2 - Bloomberg 4 HID

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

- Interface 3 - Bloomberg 4 Keyboard Audio Channel
- Interface 4 - Bloomberg 4 Keyboard Audio Channel
- Interface 5 - Bloomberg 4 Keyboard Audio Channel
- The suggested rules for this type of device are:

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=01 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=02 ## Bloomberg 4 HID

DENY: vid=1188 pid=9545 split=01 intf=03 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=04 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=05 ## Bloomberg 4 Keyboard Audio
Channel
```

Composite USB device redirection with Citrix Viewer

To connect the USB devices from the **Devices** section, do the following:

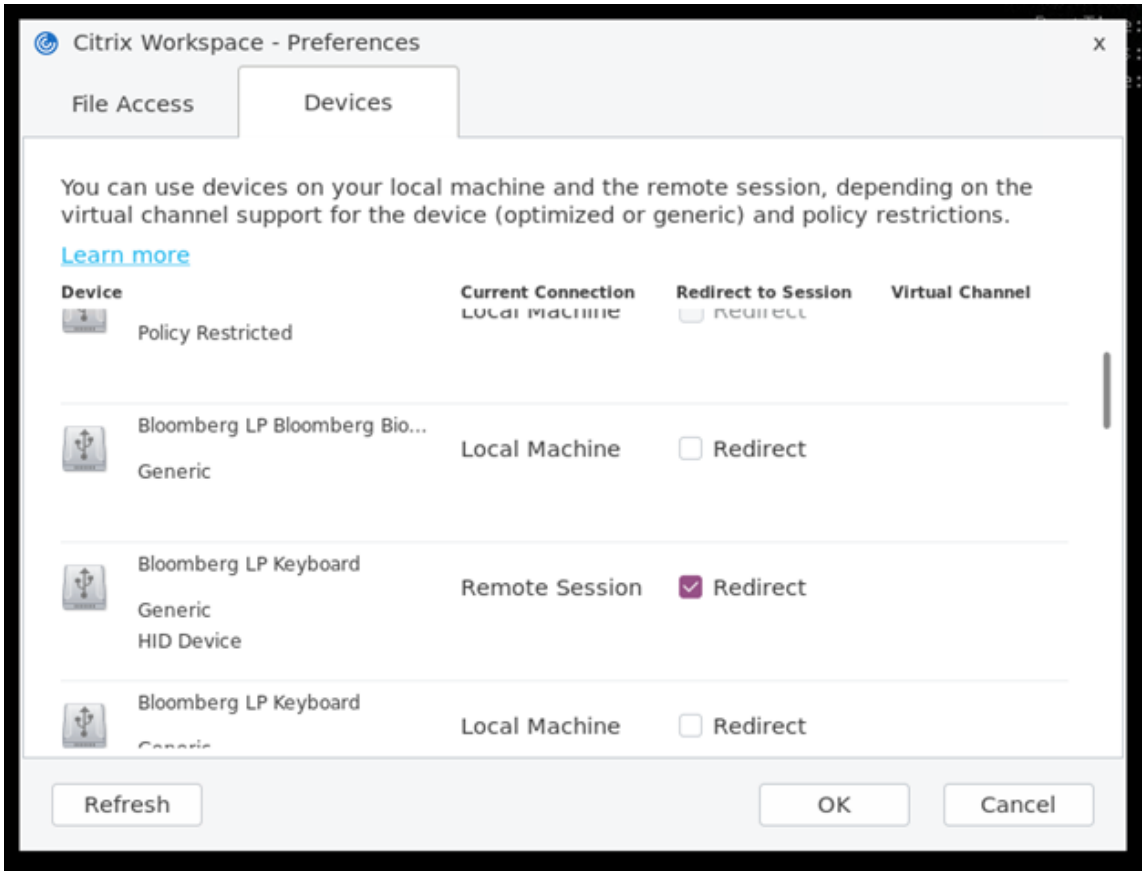
1. In a desktop session, navigate to the Desktop Viewer under **Devices**.
   The split USB devices appear.

2. To connect a device, select the required menu item.

To connect the USB devices from the **Preferences** section, do the following:

1. Navigate to the **Preferences > Devices** section.
   The split USB devices appear.

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



2. Select the check boxes next to the devices, as required.
3. Click **OK**.

The selected configuration is applied to the device connection.

> **Note:**
>
> Clear the required menu item or check boxes next to the device to disconnect a device.

Webcams

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

Webcam redirection

The following are a few points on webcam redirection:

- Webcam redirection is compatible with and without RTME.

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

- Webcam redirection works for 32-bit and 64-bit applications. For example, Skype, GoToMeeting. Use a 32-bit browser or 64-bit browser to verify webcam redirection online. For example, `https://webcamtests.com/`.
- Webcam usage is exclusive to applications. For example, when Skype is running with a webcam and you launch GoToMeeting, exit Skype to use the webcam with GoToMeeting.

Webcam redirection for 64-bit apps

Starting with the 2305 release, webcam redirection is supported for 64-bit applications.

System requirements

- `GStreamer` framework version 0.1.x or 1.x depending on the current version installed in the system.
- `ICAClient` version greater than 2106 in case it is using `GStreamer` 1.x
- `Gstreamer` version and plug-ins:
  - `gstreamer1.0-plugins-base`
  - `gstreamer1.0-plugins-bad`
  - `gstreamer1.0-plugins-good`
  - `gstreamer1.0-plugins-ugly`
  - `gstreamer1.0-vaapi plugin` and `libva` library
  - x264 library

> **Note:**
>
> The version of the `GStreamer` plug-in must be consistent with the version of the `GStreamer` framework. For example, if you install the `Gstreamer`1.2.4, the version of all `Gstreamer`1.x plug-ins must be 1.2.4.

Webcam redirection configuration

Do the following steps to activate and configure the webcam redirection feature for 64-bit apps on Citrix Workspace app for Linux.

Step 1: Verify the ICAClient configuration

Set the `AllowAudioInput` value to **True** to enable the webcam redirection feature. By default, this value is set to **True** during the installation of `ICAClient`.

If the `AllowAudioInput` value is set to **False**, do the following to enable the webcam redirection feature:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.

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

2. Set the `AllowAudioInput` value to **True**.

   AllowAudioInput=True

Step 2: Verify the Theora encoder configuration

After you have successfully installed the `ICAClient` and the `AllowAudioInput` value is set to **True**, by default the Theora encoder is configured. This encoder is a software-based encoder with acceptable performance. However, this encoder supports only 32-bit apps on a VDA.

Do the following to verify that the Theora encoder supports 32-bit apps:

1. Install Firefox 32-bit on a VDA.
2. Access the webcam test site at `https://webcamtests.com/`

The Theora encoder does not support the webcam redirection feature for 64-bit apps on a VDA. Configure the H264 encoder option to support the webcam redirection feature for 64-bit apps on VDA.

Step 3: Configure H264 encoder

H264 encoder supports the webcam redirection feature for 64-bit apps on the VDA. To enable the H264 encoder, you must do the following:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. Set the `HDXH264InputEnabled` value to **True**.

   HDXH264InputEnabled=True

Do the following to verify that the H264 encoder supports 64-bit apps:

1. Install Firefox 64-bit on a VDA.
2. Access the webcam test site at `https://webcamtests.com/`.

Step 4: Verify system dependencies

After configuring the H264 encoder, if the webcam redirection feature does not support 64-bit apps on the VDA verify the system dependencies.

The webcam redirection feature for the 64-bit app is based on the `GStreamer` framework. The `ICAClient` uses `GStreamer` framework version 0.1.x or 1.x depending on the current version installed in your system.

Step 4.1: Verify ICAClient version

Verify whether the `ICAClient` version is greater than 2106 in case it is using `GStreamer` 1.x. Previous versions of `ICAClient` might fail.

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

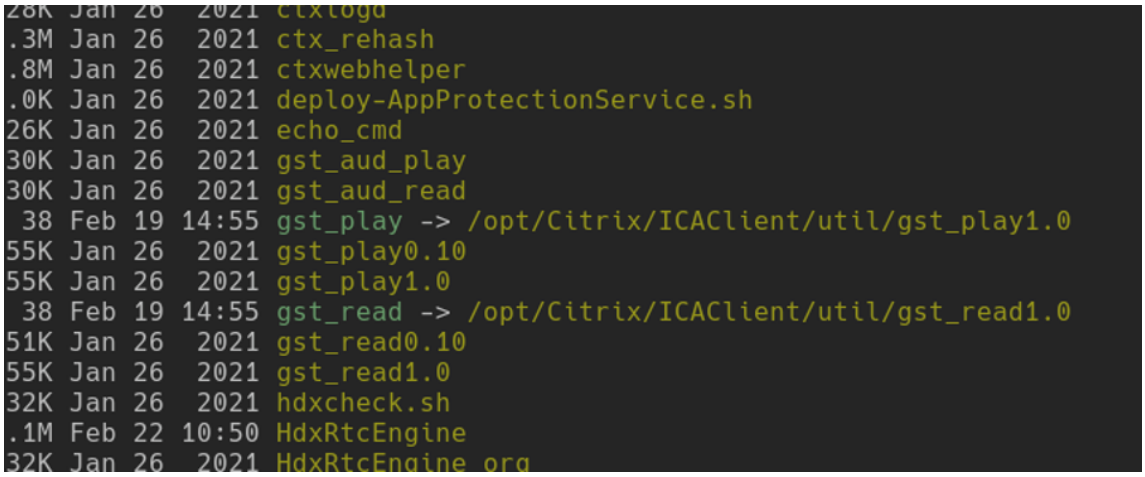
Do the following steps to verify the ICAClient version is based on the GStreamer framework installed in your system:

1. Enter the following commands in a command-line:

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
ls -alh
<!--NeedCopy-->
```

2. Verify whether the gst_read symlink is linked to gst_read1.0 or gst_read0.1. as shown in the following image:



You can also run the workspaceappcheck.sh script in the util directory and verify the output of the section referring to GStreamer dependencies.

Citrix recommends using the ICAClient version greater than or equal to 2106 and GStreamer 1.x.

Step 4.2: Verify Gstreamer version and plug-ins

Apart from the GStreamer 1.x framework, you must install the following required plug-ins:

- Gstreamer1.0-plugins-base
- Gstreamer1.0-plugins-bad
- Gstreamer1.0-plugins-good
- Gstreamer1.0-plugins-ugly
- Gstreamer1.0-vaapi plugin
- ibva library
- x264 library

For more information to install the preceding plugins, see the GStreamer installation guide.

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

> **Note:**
>
> The version of the GStreamer plug-in must be consistent with the version of the GStreamer framework. For example, if you install Gstreamer1.2.4, the version of all Gstreamer1.x plug-ins must be 1.2.4.

Run the following command to check the current version of the GStreamer framework:

```
gst-inspect-1.0 --gst-version
<!--NeedCopy-->
```

For information about troubleshooting, see Webcam in the troubleshooting section.

Background blurring for webcam redirection

Starting with the 2303 version, Citrix Workspace app for Linux supports background blurring for webcam redirection. To enable this feature, do the following:

1. Navigate to the ~/.ICAClient/wfclient.ini configuration file.
2. Add the following entry in the wfclient.ini file:

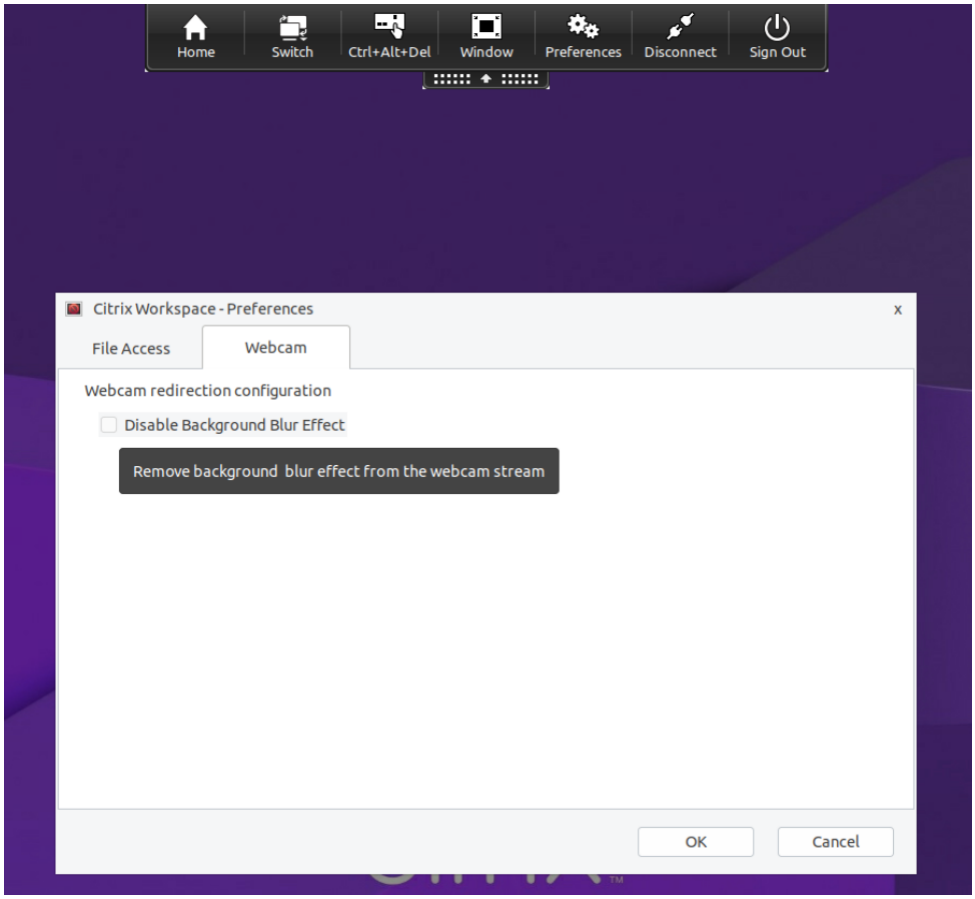
```
HDXWebCamEnableBackgndEffect=True
<!--NeedCopy-->
```

> **Note:**
>
> The configuration setting enables the background blurring for webcam redirection feature for UI and UI-less clients.

To disable background blurring inside the session for webcam redirection using the graphical user interface:

1. Click **Preferences** from the **Desktop Viewer**. The **Citrix Workspace – Preferences** dialog box appears.
2. Click the **Webcam** tab. The following dialog box appears.

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



3. Select the **Disable Background Blur Effect** check box to disable background blurring for webcam redirection.
4. Click **OK**.

Support for MJPEG webcams

Starting with 2308 version, MJPEG webcams are supported in the H264 stream. The Webcam performs MJEPG compression internally which provides better image quality and higher frame rate. This feature is enabled by default. However, if Webcam doesn't support MJPEG, this feature is disabled.

Xcapture

The Citrix Workspace app package includes a helper application, xcapture. This application assists the exchange of graphical data between the server clipboard and non-ICCCM-compliant X Window applications on the X desktop. Users can use xcapture to:

- Capture dialog boxes or screen areas and copy them between the user device desktop (including non-ICCCM-compliant applications) and an application running in a connection window
- Copy graphics between a connection window and X graphics manipulation utilities xmag or xv

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

To start xcapture from the command-line:

At the command prompt, type `/opt/Citrix/ICAClient/util/xcapture` and press ENTER (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Workspace app).

To copy from the user device desktop:

1. From the xcapture dialog box, click **From Screen**. The cursor changes to a crosshair.
2. Choose from the following tasks:
   - Select a window. Move the cursor over the window that you want to copy and click the middle mouse button.
   - Select a region. Hold down the left mouse button and drag the cursor to select the area you want to copy.
   - Cancel the selection. Click the right mouse button. While dragging, you can cancel the selection by clicking the right button before releasing the middle or left mouse button.
3. From the xcapture dialog box, click **To ICA**. The xcapture button changes color to show that it is processing the information.
4. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from xv to an application in a connection window:

1. From xv, copy the information.
2. From the xcapture dialog box, click From XV and then click To ICA. The xcapture button changes color to show that it is processing the information.
3. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from an application in the connection window to xv:

1. From the application in a connection window, copy the information.
2. From the xcapture dialog box, click From ICA and then click To XV. The xcapture button changes color to show that it is processing the information.
3. When the transfer is complete, paste the information into xv.

Cursor

Support for cursor color inverting

Previously, the Citrix Workspace app displayed a dotted cursor that appeared the same in color to the black and white background of a text. As a result, it was difficult to locate the position of the cursor.

Starting with Version 2112, the cursor color inverts based on the background color of a text. As a result, you can easily locate the position of the cursor in the text. By default, this feature is disabled.

Prerequisites:

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

- If `.ICAClient` is already present in the home folder of the current user:

  Delete `All_Regions.ini` file

  Or,

  To retain the `All_Regions.ini` file, add the following lines at the end of the [Virtual Channels\Thinwire Graphics] section:

  InvertCursorEnabled=

  InvertCursorRefreshRate=

  InvertCursorMode=

If the `.ICAClient` folder is not present then it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the feature is retained.

To enable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Go to [Thinwire3.0] section and set the following entry:

   InvertCursorEnabled=True

> **Note:**
>
> The cursor does not invert when the value for the **Use video codec for compression** policy in Citrix Studio is set to `Do not use video codec`.

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 and Desktops 7.8 (or later) or Citrix DaaS. It's disabled by default.

To enable the feature:

In the file `$HOME/.ICAClient/wfclient.ini`, in the section [WFClient], add the entry RelativeMouse=1.

This step enables the feature but keeps it inactive until you activate it. For more information on enabling relative mouse features, see Alternative Relative Mouse values section.

To activate the feature:

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

Type Ctrl/F12.

After the feature is enabled, type Ctrl/F12 again to synchronize the server pointer position with the client. The server and client pointer positions aren't synchronized when using Relative Mouse.

To deactivate the feature:

Type Ctrl-Shift/F12.

The feature is also switched off when a session window loses focus.

Alternative Relative Mouse values

Alternatively, consider using the following values for RelativeMouse:

- RelativeMouse=2 Enables the feature and activates it whenever a session window gains focus.
- RelativeMouse=3 Enables, activates, and keeps the feature activated always.
- RelativeMouse=4 Enables or disables the feature when the client-side mouse pointer is hidden or shown. This mode is suitable for automatically enabling or disabling the relative mouse for first-person gaming-style application interfaces.

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:
    - 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.

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

Generic redirection

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

As a prerequisite, the policy must be enabled in the Domain Delivery Controller (DDC).

1. Find the vid and pid of the Bloomberg keyboard. For example, in Debian and Ubuntu run the following command:

   ```
   lsusb
   ```

2. Go to $ICAROOT and edit the usb.conf file.
3. Add the following entry in the usb.conf file to allow the Bloomberg keyboard for USB redirection, and then save the file.

   ALLOW: vid=1188 pid=9545

4. Restart the `ctxusbd` daemon on the client. For example, in Debian and Ubuntu run the following command:

   ```
   systemctl restart ctxusbd
   ```

5. Launch a client session. Make sure that the session has focus while plugging in the Bloomberg v4 keyboard for redirection.

> **Note:**
>
> You can add the following configuration to disable the `selectconfiguration` command:
>
> `ALLOW: vid=1100 pid=0101 disableselectconfig=1`.
>
> The `selectconfiguration` is a command used in VDA to configure USB devices.

Selective redirection

This feature allows the use of the Bloomberg keyboard v4 and v5 interface across multiple sessions. This functionality provides flexibility to use the keyboard in all remote sessions except the fingerprint and audio interfaces. The fingerprint and audio interfaces are redirected to single sessions as before.

To enable the feature:

1. Edit the BloombergRedirection section as follows in the `$HOME/.ICAClient/wfclient.ini` file.

   ```
   1 BloombergRedirection=true
   2 <!--NeedCopy-->
   ```

2. Do all the steps mentioned in Generic redirection.

To disable the feature:

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

1. Edit the BloombergRedirection section as follows in the `$HOME/.ICAClient/wfclient.ini` file.

```
BloombergRedirection=false
<!--NeedCopy-->
```

2. Do all the steps mentioned in Generic redirection.

> **Note:**
>
> Setting the value to false reverts the functionality to the behavior present in earlier versions of the client, where all the interfaces are redirected to a single session.

Support for keyboard shortcut to switch between Full-screen and Window mode

Previously, you could use either the **Window** or **Full-screen** button on the Desktop Viewer to toggle between **Full-screen** and **Window** mode.

Starting with Citrix Workspace app 2308 release, you can use a keyboard shortcut Ctrl+F2 to switch between **Full-screen** and **Window** mode. For example, when the desktop session is in **Full-screen** mode, if you press "Ctrl+F2", the desktop session exits from the **Full-screen** mode.

This feature is disabled by default.

To enable this feature:

1. If `.ICAClient` is already present in the home folder of the current user when the new Citrix Workspace app for Linux version is installed:

   Delete the All_Regions.ini file.
   Or
   Retain the All_Regions.ini file and add the following lines at the end of the [Client Engine\Application Launching] section:

```
    FullScreenShortcutSupport=*
<!--NeedCopy-->
```

2. Navigate to the /opt/Citrix/ICAClient/config/All_Regions.ini file and modify the value of FullScreenShortcutSupport as follows:

```
 FullScreenShortcutSupport=true
<!--NeedCopy-->
```

   By default, the keyboard shortcut is Ctrl+F2.

You can also customize the shortcut key. The shortcuts are composed of two different parts such as **KeyPassthroughEscapeShift** and **KeyPassthroughEscapeChar** in the `All_Regions.ini` file.

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

The two keys that you're using must be from the following list:

Name	Section	Value
KeyPassthroughEscapeShift	[Virtual Channels\Keyboard] in All_Regions.ini	[Alt, Ctrl, Shift, Alt+Ctrl, Alt+Shift, Ctrl+Shift, Alt+Ctrl+Shift], Default value: Ctrl
KeyPassthroughEscapeChar	[Virtual Channels\Keyboard] in All_Regions.ini	[F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Minus, Plus, Tab, Pause], Default value: F2, Note: Minus and Plus are the keys on the numeric pad.

For example, if you want to use "Ctrl+Shift+F3" as the keyboard shortcut, the configuration items must be as follows:

- KeyPassthroughEscapeShift=Ctrl+Shift
- KeyPassthroughEscapeChar=F3

Limitation:

- If you use a keyboard combination that conflicts with the client OS shortcuts or contains a system shortcut, the **Full-screen** toggle might not work because the client OS takes precedence on using this shortcut. For example, if you use "Ctrl + F3" as a Linux OS system shortcut, you can't use "Ctrl + F3" or "Shift + Ctrl + F3" as the Citrix Workspace app **Full-screen** toggle.
- Ctrl+Alt+F'*' or Alt+Ctrl+F"* (F'*' refers to F1-F12) are keyboard shortcuts used to switch between Virtual Terminals in Linux. These shortcuts must not be used for **Full-screen** toggle.
- Alt+Ctrl+Plus or Alt+Ctrl+Minus (Plus and Minus are the key on the numerical keyboard) are mapped to the symbols XF86Next_VMode/XF86Prev_VMode in the Linux system and not available for shortcuts. So, these combinations must not be used for **Full-screen** toggle.

Browser content redirection

Chromium Embedded Framework (CEF) for Browser Content Redirection

In releases earlier to Version 1912, BCR used a WebkitGTK+ based overlay to render the content. However, on thin clients, there were performance issues. Starting with Version 1912, BCR uses a CEF-based overlay. This functionality enriches the user experience for BCR. It helps offload network usage, page processing, and graphics rendering to the endpoint.

Starting with Version 2106, CEF-based browser content redirection is fully functional. The feature is enabled by default.

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

If needed, you can replace the `libffmpeg.so` file provided in the Workspace app package with a suitable `libffmpeg.so` file that has the required codecs, in the `$ICAROOT/bcr/libffmpeg.so` path.

> **Note:**
>
> This feature isn't supported on the ARMHF platform.

Enabling CEF-based BCR

To enable CEF-based BCR:

1. Navigate to the `$ICAROOT/config/All_Regions.ini` file where, $ICAROOT is the default installation directory of Citrix Workspace app.
2. Go to the `[Client Engine\WebPageRedirection]` section and set the following entry:

   UseCefBrowser=True

Limitation:

- Web apps that use pop-ups might not work when BCR is used.

Known issues:

- When you set the `UseCefBrowser` option to **True** in the `~/.ICAClient/All_Regions.ini`, the Japanese, Chinese (Simplified), and Korean IME might not work in the input fields. Citrix Workspace app for Linux does not support the Japanese, Chinese (Simplified), and Korean IME when using Secure SaaS with Citrix Embedded Browser.
- When you attempt to launch a webpage redirection using CEF-based BCR, you might receive an unknown certificate error. The issue occurs on Citrix Workspace app version 2106 and later.
  As a workaround, run the following command in the terminal to import the self-signed certificate into `nssdb`:

  ```
  1  certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/
        Downloads/badssl.cer
  2  <!--NeedCopy-->
  ```

  The arguments in the commands are:

  - `-A` - To add a certificate to the database.
  - `-n` - The name of the certificate. This argument is optional and can be used to add the nick name.
  - `"badssl.cer"` - The name of the certificate that is exported from the badssl.com site.
  - `-t "C,,"` - `-t` is for TRUSTARGS and C is for CA certificate. For more information, see the Google documentation.
  - `-d ~/.pki/nssdb` - The location of the database.

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

- `-i` - Denotes the input file. This argument is to add the location and name of the certificate file.

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

Configure path for Browser Content Redirection overlay Browser temp data storage

Starting with the Citrix Workspace app 2303 version, you are requested to configure temp data storage path for the CEF based browser. To configure the path, do the following:

1. Navigate to the `$ICAROOT/config/All_Regions.ini` file where, `$ICAROOT` is the default installation directory of Citrix Workspace app.
2. Go to the `[Client Engline\WebPageRedirection]` section and add the following entry:

```
CefCachePath = <folder for CEF based BCR tmp files>
<!--NeedCopy-->
```

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 on the server, client, and configured on the AccessGateway.

For instructions on configuring HDX Broadcast auto-client reconnection, see your Citrix Virtual Apps and Desktops documentation.

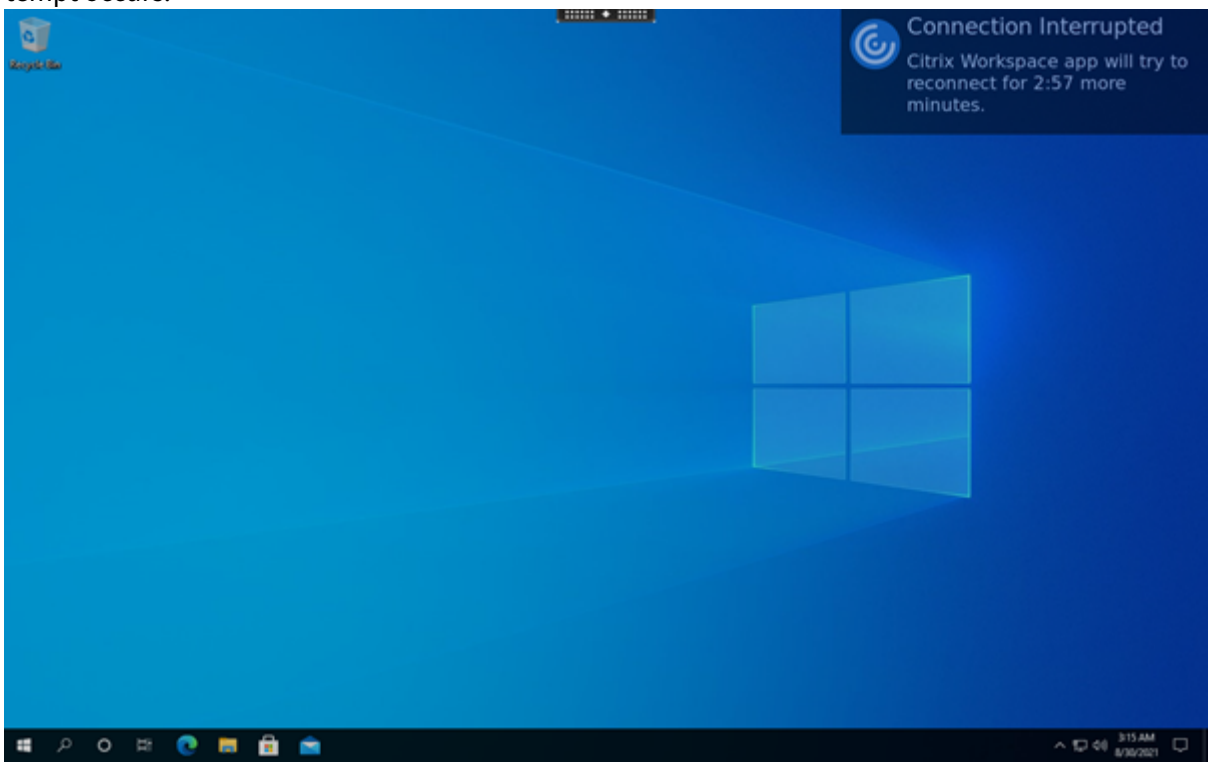
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Session reliability

This topic describes the HDX Broadcast session reliability feature, which is enabled by default.

With HDX Broadcast session reliability, users continue to see a published application's window if the connection to the application experiences an interruption. For example, wireless users enter in a tunnel might lose their connection when they enter the tunnel and regain 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.

You can now see screen changes when the session reliability begins. With this enhancement, the session window is grayed out and a countdown timer displays the time until the next reconnection attempt occurs.



> **Tip**
>
> You can alter the grayscale brightness used for an inactive session using the **Reconnection UI transparency level** policy. By default, this value is set to 80. The maximum value can't exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

When a session successfully reconnects, the countdown notification message disappears. You can interact with the desktop as usual.

Starting with the 2109 version, the session reliability notification is enabled by default.

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

To disable this enhancement:

1. Navigate to the `/opt/Citrix/ICAClient/config/module.ini` configuration file.
2. In the [WFClient] section, modify the following setting:

```
SRNotification=False
```

> **Note:**
>
> This feature is supported only for Citrix Virtual Desktops.

When auto-client reconnection and session reliability are configured, session reliability takes precedence if there is a connection problem. Session reliability attempts to re-establish a connection to the existing session. It might take up to 25 seconds to detect a connection problem. And then takes a configurable period (the default is 180 seconds) to attempt the reconnection. If session reliability fails to reconnect, then auto-client reconnect attempts to reconnect.

If HDX Broadcast session reliability is enabled, the default port used for session communication switches from 1494 to 2598.

Citrix Workspace users cannot override the server settings.

> **Important:**
>
> HDX Broadcast session reliability requires that another feature, the Common Gateway Protocol, is enabled (using policy settings) on the server. Disabling the Common Gateway Protocol also disables HDX Broadcast session reliability.

Using session reliability policies

The session reliability connections policy setting enables session reliability.

The session reliability timeout policy setting has a default of 180 seconds, or three minutes. If needed, you can extend the time session reliability to keep a session open. It does not prompt you for reauthentication.

> **Tip**
>
> As you extend the amount of time a session is kept open, you might get distracted and walk away from your device. This situation potentially leaves the session accessible to unauthorized users.

Incoming session reliability connections use port 2598, unless you change the port number defined in the session reliability port number policy setting.

For information on configuring session reliability policies, see Session reliability policy settings.

> **Note:**
>
> Session reliability is enabled by default at the server. To disable this feature, configure the policy

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

> managed by the server.

Multimedia performance

The Citrix Workspace app includes a broad set of technologies that provide a high-definition user experience for today's media-rich user environments. These technologies improve the user experience when connecting to hosted applications and desktops, as follows:

- HDX MediaStream Windows Media Redirection
- HDX MediaStream Flash Redirection
- HDX RealTime Webcam Video Compression
- H.264

> **Note:**
>
> Citrix supports RTOP coexistence with Citrix Workspace app for Linux Version 1901 and later with `GStreamer` 0.1.

HDX MediaStream Windows Media Redirection

HDX MediaStream Windows Media Redirection overcomes the need for the high bandwidths required to provide multimedia capture and playback on virtual Windows desktops accessed from Linux user devices. Windows Media Redirection provides a mechanism for playing the media run-time files on the user device rather than on the server. As a result, reduces the bandwidth requirements for playing multimedia files.

Windows Media Redirection improves the performance of Windows Media Player and compatible players running on virtual Windows desktops. A wide range of file formats are supported, including:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAV sound files

Citrix Workspace app includes a text-based translation table, MediaStreamingConfig.tbl, for translating Windows-specific media format GUIDs into MIME types `GStreamer` can use. You can update the translation table to do the following:

- Add previously unknown or unsupported media filters/file formats to the translation table
- Block problematic GUIDs to force fall-back to server-side rendering.
- Add more parameters to existing MIME strings to allow for troubleshooting of problematic formats by changing a stream's `GStreamer` parameters
- Manage and deploy custom configurations that depend on the media file types supported by `GStreamer` on a user device.

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

With client-side fetching, you can also allow the user device to stream media directly from the 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're using the tarball script (this step is done automatically for the .deb and .rpm packages).

Note about the client-side fetching feature:

- By default, this feature is enabled. You can disable it using the SpeedScreenMMACSFEnabled option in the Multimedia section of All-Regions.ini. With this option set to False, Windows Media Redirection is used for media processing.
- By default, all MediaStream features use the GStreamer playbin2 protocol. You can revert to the earlier playbin protocol for all MediaStream features except Client-Side Fetching. The Client-Side Fetching feature continues to use playbin2, using the SpeedScreenMMAEnablePlaybin2 option in the Multimedia section of the All-Regions.ini file.
- Citrix Workspace app does not recognize playlist files or stream configuration information files such as .asx or .nsc files. If possible, users must specify a standard URL that does not reference these file types. Use gst-launch to verify that a given URL is valid.

Note about GStreamer 1.0:

- By default, GStreamer 0.10 is used for HDX MediaStream Windows Media redirection. GStreamer 1.0 is used only when GStreamer 0.10 is not available.
- If you want to use GStreamer 1.0, use the following instructions:

1. Find the install directory of the GStreamer plug-ins. Depending on your distribution, the OS architecture, and the way you install GStreamer, the installation location of the plug-ins

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

varies. The typical installation path is /usr/lib/x86_64-linux-gnu/gstreamer-1.0 or $HOME/.local/share/gstreamer-1.0.

2. Find the install directory of Citrix Workspace app for Linux. The default directory for privileged (root) user installations is /opt/Citrix/ICAClient. The default directory for non-privileged user installations is $HOME/ICAClient/platform (where the platform can be linuxx64, for example). For more information, see Install and set up.
3. Install libgstflatstm1.0.so by making a symbolic link in the GStreamer plug-ins directory: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so. This step might require elevated permissions, with sudo, for example.
4. Use gst_play1.0 as the player: ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play. This step might require elevated permissions, with sudo, for example.

- If you want to use GStreamer 1.0 in HDX RealTime Webcam Video Compression, use gst_read1.0 as the reader: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Enabling GStreamer 1.x

In releases earlier to 1912, GStreamer 0.10 was the default version supported for multimedia redirection. Starting with the 1912 release, you can configure GStreamer 1.x as the default version.

Limitations:

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

To install GStreamer 1.x

Install the GStreamer 1.x framework and the following plug-ins from https://gstreamer.freedesktop.org/documentation/installing/on-linux.html:

- Gstreamer-plugins-base
- Gstreamer-plugins-bad
- Gstreamer-plugins-good
- Gstreamer-plugins-ugly
- Gstreamer-libav

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/.

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

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
<!--NeedCopy-->
```

By default, the generated binaries are available at */usr/local/lib/gstreamer-1.0/*.

For information about troubleshooting, see Knowledge Center article CTX224988.

To configure GStreamer 1.x

To configure `GStreamer` 1.x for use with Citrix Workspace app, apply the following configuration using the shell prompt:

- $ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.
- $ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play

Where,

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

Limitations:

- In releases earlier to Version 2106, the webcam redirection might fail and the session might get disconnected when using `GStreamer` version 1.15.1 or later.

HDX MediaStream Flash Redirection

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

1. Verify that your user device meets the feature requirements. For more information, see System requirements.
2. Add the following parameters to the [WFClient] section of `wfclient.ini` (for all connections made by a specific user) or to the [Client Engine\Application Launching] section of `All\\_Regions.ini` (for all users of your environment):

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

- **HDXFlashUseFlashRemoting=Ask**: **Never**; **Always**

  Enables HDX MediaStream for Flash on the user device. By default, this value is set to **Never**. Also, users are presented with a dialog box asking them if they want to optimize Flash content when connecting to webpages containing that content.

- **HDXFlashEnableServerSideContentFetching=Disabled**; **Enabled**

  Enables or disables server-side content fetching for Citrix Workspace app. By default this value is set to **Disabled**.

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

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

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

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

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

  Defines the size of the client-side cache, in MB. This value can be any size between 25 MB and 250 MB. When the size limit is reached, existing content in the cache is deleted to allow storage of new content. By default, this value is set to **100**.

- **HDXFlashServerSideContentCacheType=Persistent**: **Temporary**; **NoCaching**

  Defines the type of caching used by Citrix Workspace app for content fetched using server-side content fetching. By default, this value is set to **Persistent**.

  Note: This parameter is required only if **HDXFlashEnableServerSideContentFetching** is set to **Enabled**.

3. Flash redirection is disabled by default. In /config/module.ini change FlashV2=Off to FlashV2=On to enable the feature.

HDX RealTime webcam video compression

HDX RealTime provides a webcam video compression option to improve bandwidth efficiency during video conferencing. This option ensures users experience optimal performance when using applications such as GoToMeeting with HDFaces, Skype for Business.

1. Verify that your user device meets the feature requirements.
2. Verify that the `Multimedia` virtual channel is enabled. To enable it, open the `$ICAROOT/config/module.ini` file, and check that `MultiMedia` in the [ICA3.0] section is set to `On`.

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

3. Enable audio input by clicking the **Use my microphone and webcam on the Mic & Webcam** page of the **Preferences** dialog.

Disable HDX RealTime webcam video compression

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

- Disable HDX RealTime Webcam Video Compression
- Enable USB support for webcams

1. Add the following parameter to the [WFClient] section of the appropriate .ini file:

   AllowAudioInput=False

   For more information, see default settings.

2. Open the `usb.conf` file, typically available at `$ICAROOT/usb.conf`.
3. Remove or comment out the following line:

   > DENY: class=0e # UVC (default via HDX RealTime Webcam Video Compression)

4. Save and close the file.

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. For this protection, you can filter 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:

Verify that the `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.

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

> **Note:**
>
> SaaS with Citrix Browser Engine is supported only on x64 and x86 platforms and not on ArmHard-FloatPort (ARMHF)) hardware.

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

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

H.264

Citrix Workspace app supports the display of H.264 graphics, including HDX 3D Pro graphics, that the Citrix Virtual Apps and Desktops 7 serves. This support uses the deep compression codec feature, which is enabled by default. The feature provides better performance of rich and professional graphics applications on WAN networks compared with the existing JPEG codec.

> **Note:**
>
> In H.264, the Citrix Workspace app for Linux supports YUV 420 format only and it doesn't support YUV 444 format.

Follow the instructions in this topic to disable the feature (and process graphics using the JPEG codec instead). You can also disable text tracking while still enabling deep compression codec support. This setting helps to reduce CPU costs while processing graphics that include complex images but relatively small amounts of text or non-critical text.

> **Important:**
>
> To configure this feature, do not use any lossless setting in the Citrix Virtual Apps and Desktops or Citrix DaaS Visual quality policy. If you do, H.264 encoding is disabled on the server and does not work in Citrix Workspace app.

To disable deep compression codec support:

In the `wfclient.ini` file, set **H264Enabled** to **False**. This setting also disables text tracking.

To disable text tracking only:

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

Logging

In earlier versions, 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:

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

- Command-line 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 apply 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/citrix/ICAClient.log`. Otherwise, the logs are stored in `${ HOME } /.ICAClient/logs/ICAClient.log`.

When Citrix Workspace app is installed, a user called `citrixlog` is created to handle the logging functionality.

Command-line interface

1. At the command prompt, navigate to the `/opt/Citrix/ICAClient/util` path.
2. Run the following command to set the log preferences.

   ```
   ./setlog help
   ```

All the available commands are displayed.

The following table lists various modules and their corresponding trace class values. Use the following table for a specific command-line log value set:

Module	Log class
Assertions	LOG_ASSERT
Audio Monitor	TC_CM
BCR with CEF	TC_CEFBCR
Client Audio Mapping	TC_CAM
Connection Center	TC_CONNCENTER

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

Module	Log class
Client Communication Port	TC_CCM
Client Drive Mapping	TC_CDM
Clip	TC_CLIP
Client Printer Mapping	TC_CPM
Client Printer Mapping	TC_CPM
Font	TC_FONT
Frame	TC_FRAME
Graphics Abstraction	TC_GA
Input Method Editor	TC_IME
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

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

Module	Log class
PAL	TC_VP
UI	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
USB Daemon	TC_CTXUSB
Video Frame Driver	TC_VFM
Web kit	TC_WEBKIT
WinStation Driver	TC_WD
`Wfica`	TC_NCS
`Wfica` Engine	TC_WENG
`Wfica` Shell	TC_WFSHELL
Web helper	TC_WH
Zero Latency	TC_ZLC

GUI

Go to **Menu** > **Preferences**. The **Citrix Workspace-Preferences** dialog appears.

At increasing levels of tracing detail, the following values are available:

- Disabled
- Only Error
- Normal
- Verbose

By default, the **Logging** option is set to **Only Error**.

Due to the large amount of data that can be generated, tracing might significantly impact the performance of Citrix Workspace app. The **Verbose** level is recommended only if necessary for troubleshooting.

Click **Save and Close** after you select the desired 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.

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

> **Note:**
>
> If you delete the `ICAClient.log` file, you must restart the logging service `ctxcwalogd`.
>
> For example, if you are on a systemd-capable setup, run the following command:
>
> `systemctl restart ctxcwalogd`.

Enabling logging on Version 2006 and earlier:

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

1. Download and install Citrix Workspace app on your Linux machine.
2. Set the `ICAROOT` environment variable to the installation location.

   For example, `/opt/Citrix/ICAClient`.

   By default, the `TC_ALL` trace class is enabled to provide all the traces.
3. To collect logs for a particular module, open the `debug.ini` file at `$ICAROOT` and add the required trace parameters to the `[wfica]` section.

   Add the trace classes with a “+” symbol. For example, `+TC_LIB`.

   You can add different classes separated by the pipe symbol.
   For example, `+TC_LIB|+TC_MMVD`.

The following table lists the `wfica` modules and their corresponding trace class values:

Module	TraceClasses value
Graphics	TC_TW
EUEM	TC_EUEM
WFICA (Session Launch)	TC_NCS
Printing	TC_CPM
Connection Sequence - WD	TC_WD
Connection Sequence - PD	TC_PD
Connection Sequence - TD	TC_TD
Proxy related files	TC_PROXY
Multimedia Virtual Driver / Webcam	TC_MMVD
Virtual Drivers	TC_VD
Client Drive Mapping	TC_CDM
Audio	TC_CAM

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

Module	TraceClasses value
COM (Communication Port)	TC_CCM
Seamless	TC_TWI
Smart Card	TC_SCARDVD

The following table lists the connection center module and their corresponding trace class value:

Module	TraceClasses value
Connection center	TC_CSM

The following table lists the trace class value for setWebHelper:

TraceClasses value
Set logSwitch to 1 (to enable) or 0 (to disable)
Example: logSwitch = 1

Troubleshooting:

If `ctxlogd` turns unresponsive, the logs are traced in the syslog.

For information about getting new and refreshed logs in subsequent launches, see Syslog configuration.

Syslog configuration

By default, all syslog logs are saved at /var/log/syslog. To configure the path and the name of the log file, edit the following line under the [RULES] section in the `/etc/rsyslog.conf` file. For example,

```
1 user.* -/var/log/logfile_name.log
```

Save your changes and then restart the syslog service using the command:

```
sudo service rsyslog restart
```

Points to remember:

- To verify that a new syslog is available, delete the syslog and run the command: `sudo service rsyslog restart`.

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

- 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 the `rsyslog.conf` file by replacing the localhost with the IP address of the remote server:

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

Collecting log files

Previously, there was no tool available to collect the log files in Citrix Workspace app. Log files were present in different folders. You had to manually collect log files from different folders.

Starting with the 2109 version, Citrix Workspace app introduces a collectlog.py tool to collect log files from different folders. You can run the tool using the command-line. The log files are generated as a compressed log file. You can download it from the local server.

Prerequisites

- Python 3
- Requires extra space to save the logs

Starting with Version 2109, two new files are added to collect log files using the collectlog.py tool:

- `logcollector.ini` file – Saves the name and path of the log file.
- `collectlog.py` file – Collects the log files and saves them as `cwalog_{ timestamp } .tar .gz` compressed file.

By default, the `[hdxteams]` component is added in the `logcollector.ini` file to collect log files for Microsoft Teams. However, you can add other components also in the `logcollector.ini` file using the following procedure:

1. Navigate to the `${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini` file.

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

2. Add the component that you require to collect log files as per the following example:

[component_name]

log_name1 = “log_path1”

log_name2 = “log_path2”

If you are on Version 2109, collect log files using the following procedure:

1. Download and install Citrix Workspace app on your Linux machine.
2. At the command-line, navigate to the `/opt/Citrix/ICAClient/util` path.
3. Run the following command:
   `./collctlog.py -h`

   The following command usage information appears:

   ```
   usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE]optional arguments: -h,
    --help show this help message and exit -c CONFIG, --config CONFIG The
   logcollector.ini path & file -a ARCHIVE, --archive ARCHIVE The archive
   path & file
   ```

4. Run the following commands as required:
   - `./collectlog.py` – Collects log files using the configuration file from the default path and saves them as a compressed log files at the default path.
   - `./collectlog.py -c /user_specified_path/logcollector.ini` – Collects log files using the configuration file from a user-specified path and saves them as a compressed log files at the default path.
   - `./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_spec/` – Collects log files using the configuration file from a user-specified path and saves them as a compressed log files at the user-defined path.

   > **Note:**
   >
   > The default path of the `logcollector.ini` configuration file is `/opt/Citrix/ICAClient/config/logcollector.ini`. The default path of the compressed log file is `/tmp`.

5. Navigate to the `/tmp` folder and collect the `cwalog_{ timestamp } .tar.gz` compressed file.

> **Note:**
>
> The log files are saved in the `/tmp` folder with the file name `cwalog_{ timestamp } .tar.gz`.

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

Optimization for Microsoft Teams

Optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops or Citrix DaaS and Citrix Workspace app. Optimization for Microsoft Teams is similar to HDX RealTime Optimization for Microsoft Skype for Business. The difference is that we bundle all the necessary components for Microsoft Teams optimization into the VDA and the 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.
> - Microsoft optimization is supported in both Citrix Virtual Apps and Desktops and Citrix DaaS.
> - For Thin Clients that use Dell Wyse, use the **Citrix Configuration Editor** to edit any parameter in the `/var/.config/citrix/hdx_rtc_engine/config.json` file. For more information see the Dell documentation.

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

For information on system requirements, see Microsoft Teams optimization requirements.

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

Enhancement to audio configuration

If Microsoft Teams configures auto gain control and noise suppression options, Citrix-redirected Microsoft Teams honors the values as configured. Otherwise, these options are enabled by default. However, starting from Citrix Workspace app 2104, the echo cancellation option is disabled by default. Starting from Citrix Workspace app 2112, admins can change the default settings to troubleshoot Audio issues (like robotic voice, high CPU causing choppy audio, and so on) by doing the following:

1. Navigate to the /var/.config/citrix/hdx_rtc_engine/config.json file.
2. Set the following options:
   - `EnableAEC` value to 1 to enable and 0 to disable echo cancellation
   - `EnableAGC` value to 1 to enable and 0 to disable auto gain control
   - `EnableNS` value to 1 to enable and 0 to disable noise suppression

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

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

{

```

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

```
7
8       "EnableAEC":1,"EnableAGC":1,"EnableNS":1
9
10   }
11
12 <!--NeedCopy-->
```

After the call is established, monitor the `webrpc` log (`/tmp/webrpc/<current date>/`) for the following entries to verify that the changes took effect:

```
1 /tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
     14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
     constraints, aec=1, agc=1, ns=1
2 <!--NeedCopy-->
```

Encoder performance estimator for Microsoft Teams

The `HdxRtcEngine` is the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection. The `HdxRtcEngine.exe` can estimate the best outgoing video (encoding) resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 720p, and 1080p.

The performance estimation process uses macroblock code to determine the best resolution that can be achieved with the particular endpoint. The Codec negotiation during a call setup includes the highest possible resolution. The Codec negotiation can be between the peers, or between the peer and the conference server.

The following table lists the four performance categories for endpoints that have its own **maximum** available resolution:

Endpoint performance	Maximum resolution	Registry key value
Fast	1080p (1920x1080 16:9 @ 30 fps)	3
Medium	720p (1280x720 16:9 @ 30 fps)	2
Slow	360p (either 640x360 16:9 @ 30 fps, or 640x480 4:3 @ 30 fps)	1
Very slow	240p (either 320x180 16:9 @ 30 fps, or 320x240 4:3 @ 30 fps)	0

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

To set the outgoing video (encoding) resolution value, for example to 360p, run the following command from the terminal:

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

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

{


    "OverridePerformance":1

 }

<!--NeedCopy-->
```

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

<!--NeedCopy-->
```

Logging can also be enabled by adding the following line to the config.json file:

```
{

"WebrpcLogLevel": 0,"WebrtcLogLevel": 0
 }

<!--NeedCopy-->
```

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

Adding the libunwind-12 library dependency for llvm-12

Starting with the 2111 release, a new dependency called the libunwind-12 library is added for llvm-12. However, by default, it does not exist in the original repository. Install the libunwind-12 library manually in the repository using the following steps:

1. Open the terminal.
2. Enter the following line to install the `llvm` repository key file:

```
1  wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key|sudo apt-key
       add
2 <!--NeedCopy-->
```

3. Enter the following line to configure the `llvm` repository source list:

```
1  sudo vim /etc/apt/sources.list
2 <!--NeedCopy-->
```

4. Add the following line:

```
1 deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
2 deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
3 <!--NeedCopy-->
```

5. Run the following command to install the libunwind-12 library:

```
1 sudo apt-get update -y
2 sudo apt-get install libunwind-12
3 <!--NeedCopy-->
```

Configuring a preferred network interface

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

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

```
1        mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3         vim /var/.config/citrix/hdx_rtc_engine/config.json
4
```

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

```
5         {
6
7
8              " NetworkPreference" :1
9
10           }
11
12 <!--NeedCopy-->
```

3. Update the “NetworkPreference:” value with one of the following values as required:
   - 1: Ethernet
   - 2: Wi-Fi
   - 3: Cellular
   - 4: VPN
   - 5: Loopback
   - 6: Any

By default and if no value is set, the WebRTC media engine chooses the best available route.

Enhancements to Microsoft Teams optimization

- Starting with version 2101 for Citrix Workspace app:
  - The Citrix Workspace app installer is packaged with the Microsoft Teams ringtones.
  - Audio output switches automatically to newly plugged-in audio devices, and an appropriate audio volume is set.
  - HTTP proxy support for anonymous authentication.
- Starting with version 2103 for Citrix Workspace app, the VP9 video codec is disabled by default.
- Starting with version 2104 for Citrix Workspace app, the echo cancellation feature is disabled by default. We recommend that you do not use your built-in speakers and microphone for calls. Use headphones instead. This fix aims to address choppy audio issues noticed on thin clients
- Starting with version 2106 for Citrix Workspace app:
  - Previously, when you clicked **Screen sharing**, preview of a default or main monitor was only available for screen sharing.

    With this version, a preview of all screens is displayed on the screen picker menu. You can select any screen for screen sharing in the VDA environment. A red square appears on the selected monitor and a small picture of the selected screen content appears on the screen picker menu.

    In seamless mode, you can select one from all screens to share. When the Desktop Viewer changes the window mode (maximized, restore, or minimize), the screen share stops.

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

- Starting with version 2112 for Citrix Workspace app:

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

  - **Request control in Microsoft Teams**

    With this release, you can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other modifications to the shared screen.

    To take control when a screen is being shared, click **Request control** at the top of the Microsoft Teams screen. The meeting participant who's sharing the screen can either allow or deny your request.

    While you have control, you can make selections, edits, and other modifications to the shared screen. When you're done, click **Release control**.

    Limitations:

    * Users on a Linux client cannot *Give* control to other users. In other words, after the user on the Linux client starts sharing content, the option **Give control** is not present in the sharing toolbar. This is a Microsoft limitation.
    * The **Request Control** option is not available during the peer-to-peer call between an optimized user and a user on the native Microsoft Teams desktop client that is running on the endpoint. As a workaround, users can join a meeting to get the **Request Control** option.

  - **Support for dynamic e911**

    With this release, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it provides the capability to:

    * configure and route emergency calls
    * notify security personnel

    The notification is provided based on the current location of the Citrix Workspace app running on the endpoint, instead of the Microsoft Teams client running on the VDA.
    Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112 for Linux, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law. To support this feature, the LLDP library must be included in the Operating System distribution of the Thin Client.

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

- Starting with version 2203 for Citrix Workspace app:

  Multi-window chat and meetings for Microsoft Teams

  With this release, you can use multiple windows for chat and meetings in Microsoft Teams, when optimized by HDX in Citrix Virtual Apps and Desktops 2112 or higher. You can pop out the conversations or meetings in various ways. For details about the pop-out window feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings.

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

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

- Starting with version 2207 for Citrix Workspace app:
  - **App sharing enabled:** Starting with Citrix Workspace app 2209 for Linux and Citrix Virtual Apps and Desktops 2109, you can share an app using the Screen sharing feature in Microsoft Teams.
  - **Enhancements to high DPI support:** When the high DPI feature is enabled and you're using 4K monitors, Microsoft Teams video overlays are in the desired position and of the correct size. Irrespective of your display settings such as single or multi-monitor arrangements, overlays always appear correctly and aren't scaled up or appear in an undesired position. To enable this enhancement, ensure that the `DPIMatchingEnabled` parameter in the `wfclient.ini` configuration file is set to **True**. For more information, see Support for DPI matching.
  - **WebRTC SDK upgrade:** The version of the WebRTC SDK that is used for the optimized Microsoft Teams is upgraded to version M98.

- Starting with version 2305 for Citrix Workspace app:
  - **Enhancement to sleep mode for optimized Microsoft Teams call**

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

  Starting with the 2305 release, Citrix Workspace app or the optimized Microsoft Teams screen doesn't go into sleep mode even if there is no mouse or keyboard interaction during an optimized Microsoft Teams meeting.

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

- **Improved experience for optimized Microsoft Teams video conference calls**

  Starting with the 2305 release, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved by adapting to the proper resolution for the best call experience for all callers.

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

- **Added support for playing short tones in optimized Microsoft Teams**

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

  Starting with the 2307 release, Citrix Workspace app supports playing the short tones as desired. This support also enables the secondary ringtone feature.

  Prerequisites:

  Update to the latest version of Microsoft Teams.

Support for NetScaler App Experience (NSAP) virtual channel

Previously available as an experimental feature, the NSAP virtual channel feature is fully supported starting with version 2006. All HDX Insight data is sourced from the NSAP virtual channel exclusively and sent uncompressed. This approach improves the scalability and the performance of sessions. The NSAP virtual channel is enabled by default. To disable it, toggle the VDNSAP flag `NSAP=Off` in the module.ini file.

For more information, see HDX Insight in the Linux Virtual Delivery Agent documentation, and HDX Insight in the Citrix Application Delivery Management service documentation.

Multi-monitor layout persistence

This feature retains the session monitor layout information across endpoints. The sessions appear on the same monitors as configured.

Prerequisite:

This feature requires the following:

- StoreFront v3.15 or later.

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

- If `.ICAClient` is already present in the home folder of the current user:

  Delete the All_Regions.ini file

  or

  To retain the `All_Regions.ini` file, add the following lines at the end of the [Client Engine\Application Launching] section:

  SubscriptionUrl=

  PreferredWindowsBounds=

  PreferredMonitors=

  PreferredWindowState=

  SaveMultiMonitorPref=

If the `.ICAClient` folder is not present then it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the feature is retained.

Use cases

- Launch a session on any monitor in windowed mode and save the setting.
  When you relaunch the session, it appears in the same mode, on the same monitor, and in the same position.
- Launch a session on any monitor in full-screen mode and save the setting.
  When you relaunch the session, it appears in full-screen mode on the same monitor.
- Stretch and span a session in windowed mode across multiple monitors and then switch to full-screen mode. The session continues in full-screen across all monitors. When you relaunch the session, it appears in full-screen mode, spanning across all monitors.

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

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).

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

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 update 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 color change indicates that saving is in progress. When the layout is saved the icon appears normal.
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 extra 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. Verify that about half the screen is present in each monitor.
4. From the Citrix Virtual Desktop toolbar, select **Full-screen**.

   The screen extends to both the monitors.

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

Workspace launcher

Citrix introduces the Workspace launcher (ctx-webhelper) to launch published desktops and applications.

Previously, the browser plug-in provided along with Citrix Workspace app for Linux enabled users to launch published desktops and applications was based on the NPAPI.

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

Starting with Version 1901, the Citrix Workspace launcher is compatible with direct connections to StoreFront and Citrix Gateway. This feature helps to launch the ICA file automatically and to detect the Citrix Workspace app installation.

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 isn't 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 the self-service executable file from third-party thin-client vendors, the application can become unresponsive because of 100% CPU utilization.

As a workaround, to switch back to the old UI mode:

1. Remove cached files by using the command:
   `rm -r ~/.ICAClient`
2. Go to `$ICAROOT/config/AuthManconfig.xml` file.
3. Change `CWACapableEnabled` key value to false.
4. Launch Citrix Workspace app for Linux. Observe that the self-service executable file loads the old UI.

Keyboard layout synchronization

Keyboard layout synchronization enables you to switch among preferred keyboard layouts on the client device. This feature is disabled by default. After you enable this feature, the client keyboard layout automatically synchronizes to the virtual apps and desktops.

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

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

- **Sync only once - when session launches** – Based on the `KeyboardLayout` value in the wfclient.ini file, the client keyboard layout is synchronized to the server when the session launches. If the `KeyboardLayout` value is set to `0`, the system keyboard is synchronized to VDA. If the `KeyboardLayout` value is set to a specific language, the language-specific keyboard is synchronized to VDA. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, sign out and sign in to the app. Also, the changes take effect if you sign in again or reconnect to the VDA session. The **Sync only once - when session launches** mode is the default keyboard layout selected for the Citrix Workspace app.
- **Allow dynamic sync** - This option synchronizes the client keyboard layout to the server when you change the client keyboard layout.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

Prerequisite:

- Enable the Unicode Keyboard Layout Mapping feature on the Windows VDA. For more information, see Knowledge Center article CTX226335.
- Enable the Dynamic Keyboard layout sync feature on the Linux VDA. For more information, see Dynamic keyboard layout synchronization
- Keyboard layout synchronization depends on XKB lib.
- When using a Windows Server 2016 or Windows Server 2019, navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` registry path and add a DWORD value with key name `DisableKeyboardSync` and set the value to `0`.
- If `.ICAClient` is already present in the home folder of the current user:

  Delete the All_Regions.ini file

  or

  To retain the `All_Regions.ini` file, add the following lines at the end of the[Virtual Channels\Keyboard] section:

  KeyboardSyncMode=

  KeyboardEventMode=

Configure keyboard layout

Citrix Workspace app provides both UI and configuration settings to enable the three different keyboard layout synchronization modes.

To configure keyboard layout synchronization using the graphical user interface:

1. From the Citrix Workspace app icon in the notification area, select **Preferences**.

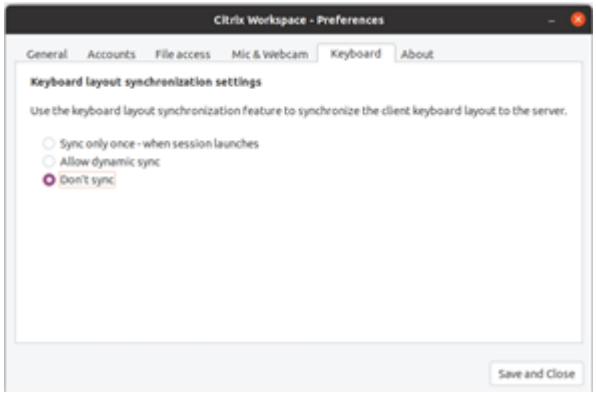
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Or,

Open the terminal, navigate to the installation path, and run the following command:

`util/configmgr`

The **Citrix Workspace – Preferences** dialog appears.



2. Click **Keyboard** tab.

   The **Keyboard layout synchronization settings** page appears.

3. Select from one of the following options:

   - **Sync only once - when session launches** - Indicates that the keyboard layout is synced to the VDA only once at the session launch. Unicode keyboard input mode is the recommended option for the **Sync only once – when session launches** mode.
   - **Allow dynamic sync** - Indicates that the keyboard layout is synced dynamically to the VDA when the client keyboard is changed in a session. Unicode keyboard input mode is the recommended option for the **Allow dynamic sync** mode.
   - **Don't sync** - Indicates that the client uses the keyboard layout present on the server, irrespective of the keyboard layout that is selected in the client. Scancode keyboard input mode is the recommended option for the **Don't sync** mode. You must make sure that the client keyboard layout is the same as the keyboard layout on the VDA if you select Unicode for the **Don't Sync** option.

4. Click **Save and Close**.

To configure keyboard layout synchronization using configuration file settings:

Modify the `wfclient.ini` configuration file to enable the required keyboard layout.

Sync only once – when session launches:

With this feature enabled, when launching a session, the active keyboard layout on the client device is synchronized to VDA. Based on the `KeyboardLayout` value in the `wfclient.ini` file, the client keyboard layout is synchronized to the server when the session launches. If the `KeyboardLayout`

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

value is set to `0`, the system keyboard is synchronized to VDA. If the `KeyboardLayout` value is set to a specific language, the language-specific keyboard is synchronized to VDA.

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardSyncMode=Once
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
<!--NeedCopy-->
```

Unicode keyboard input mode is the recommended option for the **Sync only once – when session launches** mode.

Allow dynamic sync:

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

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardSyncMode=Dynamic
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
<!--NeedCopy-->
```

Unicode keyboard input mode is the recommended option for the **Allow dynamic sync** mode.

Don’t sync:

With this feature enabled, the VDA side keyboard layout is used, irrespective of the keyboard layout that is selected in the client device.

To select this mode, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardSyncMode=No
KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
<!--NeedCopy-->
```

Scancode keyboard input mode is the recommended option for the **Don’t sync** mode. You must make sure that the client keyboard layout is the same as the VDA side keyboard layout if you configure to Unicode for **Don’t Sync** option.

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

> **Note:**
>
> When you set `KeyboardSyncMode=""` (empty) in the `wfclient.ini` file, the mode reverts to the earlier behavior. In the earlier behavior, the keyboard layout is read from the `$HOME/.ICAClient/wfclient.ini` file and sent to the VDA along with other client information when the session starts.

Keyboard Input Mode

Citrix recommends the following keyboard input mode for the different keyboard layout sync options:

- Scancode mode for **Don't Sync** option.
- Unicode mode for **Allow dynamic sync** and **Sync only once - when session launches** options.

You can change the configuration of `KeyboardEventMode` in the `wfclient.ini` file. However, for best performance, use the Citrix-recommended modes for different scenarios, physical keyboards, and client devices.

Client IME for East Asian languages

Client Input Method Editor (IME) feature enhances input and display experience with Chinese, Japanese, and Korean (CJK) language characters in Citrix Workspace app for Linux. You can choose to use the Client IME when you have a favorite IME in Linux Client or IME is not available from the remote server.

To enable this feature, do the following:

1. Navigate to the `$HOME/.ICAClient/wfclient.ini` configuration file.
2. Add the following entries:

```
KeyboardEventMode = Unicode
UseLocalIM = True
<!--NeedCopy-->
```

If your client Linux distribution doesn't have a working iBus, you must set the `KeyboardLayout` value explicitly according to your IME language in the wfclient.ini configuration file as follows:

- For Chinese IME - `KeyboardLayout = Chinese (PRC)`
- For Japanese IME - `KeyboardLayout = Japanese (JIS)`
- For Korean IME - `KeyboardLayout = Korean`

Enhancement to support keyboard layout synchronization for GNOME 42

Starting with the 2305 version, Citrix Workspace app for Linux supports keyboard layout synchronization for desktops like Ubuntu 22.04 which uses GNOME 42 desktop environment and later versions.

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

Keyboard layout support for Windows VDA and Linux VDA

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Arabic	ara	-	→	ar-SA	00000401	ara	-
Arabic (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
German (Austria)	at	-	→	de-AT	00000407	at	-
Belgian (alt. ISO)	be	iso-alternate	→	fr-BE	0000080c	be	iso-alternate
Belgian	be	-	→	nl-BE	00000813	be	-
Bulgarian	bg	-	→	bg-BG	00030402	bg	-
Bulgarian (traditional phonetic)	bg	phonetic	→	bg-BG	00040402	bg	phonetic
Bulgarian (new phonetic)	bg	bas_phonetic	→	bg-BG	00020402	bg	bas_phonetic
Portuguese (Brazil)	br	-	→	pt-BR	00000416	br	-
Belarusian	by	-	→	be-BY	00000423	by	-
English (Canada)	ca	eng	→	en-CA	00000409	ca	eng
Canadian Multilingual	ca	multix	→	fr-CA	00011009	ca	multix
French (Canada, legacy)	ca	fr-legacy	→	fr-CA	00000c0c	ca	fr-legacy

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

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
French (Canada)	ca	-	→	fr-CA	00001009	ca	-
French (Switzerland)	ch	fr	→	fr-CH	0000100c	ch	fr
German (Switzerland)	ch	-	→	de-CH	00000807	ch	-
Chinese (Simplified)	cn	-	→	en-US	00000409	us	-
Czech	cz	-	→	cs-CZ	00000405	cz	-
Czech (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty
German	de	-	→	de-DE	00000407	de	-
German (Macintosh)	de	mac	→	de-DE	00000407	de	mac
Danish	dk	-	→	da-DK	00000406	dk	-
Estonian	ee	-	→	et-EE	00000425	ee	-
Spanish (Latin American)	es	-	→	es-ES	0000040a	es	-
Spanish (Macintosh)	es	mac	→	es-ES	0000040a	es	mac
Finnish	fi	-	→	fi-FI	0000040b	fi	-
French	fr	-	→	fr-FR	0000040c	fr	-

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

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
French (Macintosh)	fr	mac	→	fr-FR	0000040c	fr	mac
English (UK)	gb	-	→	en-GB	00000809	gb	-
English (Macintosh)	gb	mac	→	en-GB	00000809	gb	mac
English (UK, extended, with Win keys)	gb	extd	→	en-GB	00000452	gb	extd
Greek	gr	-	→	el-GR	00000408	gr	-
Croatian	hr	-	→	hr-HR	0000041a	hr	-
Hungarian	hu	-	→	hu-HU	0000040e	hu	-
Irish	ie	-	→	en-IE	00001809	ie	-
Hebrew	il	-	→	he-IL	0002040d	il	-
English (India, with rupee)	in	eng	→	en-IN	00004009	in	eng
Iraqi	iq	-	→	ar-IQ	00000401	iq	-
Icelandic	is	-	→	is-IS	0000040f	is	-
Italian	it	-	→	it-IT	00000410	it	-
Japanese	jp	-	→	en-US	00000409	us	-
Japanese (Macintosh)	jp	mac	→	en-US	00000409	us	mac

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

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Korean	kr	-	→	en-US	00000409	us	-
Spanish (Latin American)	latam	-	→	es-MX	0000080a	latam	-
Lithuanian	lt	-	→	lt-LT	00010427	lt	-
Lithuanian (IBM LST 1205-92)	lt	ibm	→	lt-LT	00000427	lt	ibm
Lithuanian (Standard)	lt	std	→	lt-LT	00020427	lt	std
Latvian	lv	-	→	lv-LV	00020426	lv	-
Norwegian	no	-	→	nb-NO	00000414	no	-
Polish	pl	-	→	pl-PL	00000415	pl	-
Polish (QWERTZ)	pl	qwertz	→	pl-PL	00010415	pl	qwertz
Portuguese	pt	-	→	pt-PT	00000816	pt	-
Portuguese (Macintosh)	pt	mac	→	pt-PT	00000816	pt	mac
Romanian (standard)	ro	std	→	ro-RO	00010418	ro	std
Serbian	rs	-	→	sr-Cyrl-RS	00000c1a	rs	-
Serbian (Latin)	rs	latin	→	sr-Latn-RS	0000081a	rs	latin
Russian	ru	-	→	ru-RU	00000419	ru	-

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

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
Russian (typewriter)	ru	typewriter	→	ru-RU	00010419	ru	typewriter
Russian (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
Swedish	se	-	→	sv-SE	0000041d	se	-
Swedish (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
Slovenian	si	-	→	sl-SI	00000424	si	-
Slovak	sk	-	→	sk-SK	0000041b	sk	-
Slovak (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
Thai	th	-	→	th-TH	0000041e	th	-
Thai (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
Tajik	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
Turkish	tr	-	→	tr-TR	0000041f	tr	-
Turkish (F)	tr	f	→	tr-TR	0001041f	tr	f
Chinese (Traditional)	tw	-	→	en-US	00000409	us	-
Ukrainian	ua	-	→	uk-UA	00000422	ua	-
English (US)	us	-	→	en-US	00000409	us	-

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

Linux Client Keyboard Description	Linux Client Keyboard Layout	Linux Client Keyboard Variant	Syncs to	Windows Locale ID	Windows VDA Keyboard Layout (ID)	Linux VDA Keyboard Layout	Linux VDA Keyboard Variant
English (Macintosh)	us	mac	→	en-US	00000409	us	mac
English (Dvorak)	us	dvorak	→	en-US	00010409	us	dvorak
English (Dvorak, left-handed)	us	dvorak-l	→	en-US	00030409	us	dvorak-l
English (Dvorak, right-handed)	us	dvorak-r	→	en-US	00040409	us	dvorak-r
English (US, intl., with dead keys)	us	intl	→	nl-NL	00020409	us	intl
Vietnamese	vn	-	→	vi-VN	0000042a	vn	-

VDA keyboard layout

The VDA keyboard layout feature helps you use the VDA keyboard layout regardless of the client's keyboard layout settings. It supports the following types of keyboard: PC/XT 101, 102, 104, 105, 106.

To use the server-side keyboard layout:

1. Launch the wfclient.ini file.
2. Change the value of the `KeyboardLayout` attribute as follows:

   `KeyboardLayout=(Server Default)`

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

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

File type association

A Citrix Virtual Apps Services might also publish a file, rather than an application or desktop. This process is referred to as publishing content, and allows pnabrowse to open the published file.

There's a limitation to the type of files that the Citrix Workspace app recognizes. Only when a published application is associated with the file type of the published file:

- The system recognizes the file type of the published content
- Users can view the file through Citrix Workspace app

For example, to view a published Adobe PDF file using Citrix Workspace app, an application such as Adobe PDF Viewer must be published. Unless a suitable application is published, users can't view the published content.

To enable FTA on the client-side:

1. Verify that the app that you want to associate is a favorite or a subscribed application.
2. To get the list of published applications and the server URL, run the commands:

```
./util/storebrowse -l

./util/storebrowse -S <StoreFront URL>
<!--NeedCopy-->
```

3. Run the ./util/ctx_app_bind command with the following syntax:

   ```
   ./util/ctx_app_bind [-p] example_file|MIME-type published-application [
   server|server-URI]
   ```

   for example,
   ```
   ./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.
   bvt.local/citrix/store/discovery
   ```

4. Verify that the file that you're trying to open is client drive mapping (CDM) enabled.
5. Double-click the file to open it using the associated application.

Associating a published application with file types

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

Prerequisite:

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

To link a file name extension with a Citrix Workspace app for Linux application:

1. Publish the application.

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

2. Log on to Citrix Studio.
3. Right-click the application and then select **Properties.**
4. Select **Location.**
5. Add "%**" in the Command-line argument (optional) field to bypass the command-line validation and then click OK.
6. Right-click the application and select **Properties**.
7. Select **File Type Association**.
8. Select all the extensions that you want Citrix Workspace app to associate with the application.
9. Click **Apply** and **Update file types**.
10. Follow the steps mentioned in File type association to enable FTA on the client-side.

> **Note:**
>
> The StoreFront file type association must be ON. By default, file type association is enabled.

Support for Citrix Analytics

Starting with the version 2006, Citrix Workspace app is updated to transmit data to the Citrix Analytics Service from ICA sessions that you launch from a browser.

For more information on how Citrix Analytics uses this information, see Self-Service Search for Performance and Self-service search for Virtual Apps and Desktops.

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

Transparent user interface

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

Citrix Workspace app for Linux supports the TUI VC feature. This feature helps the client to receive the TUI packets sent by the server, and the client can access the UI-related components. This functionality helps you to control the display of the default overlay screen. You can toggle the `VDTUI` flag in the `module.ini` file: `VDTUI - On/Off`

Starting with version 1912, the **VDTUI** flag is set to **On** by default. As a result, the "Starting <Application>" dialog box no longer appears when you launch an app. Instead, a "Connecting

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

<Application>" dialog appears with a progress bar. The dialog also displays the progress of the app launch. However, if you set the flag to **Off**, the "Starting <Application>" dialog rendered on top of other application windows, covering the login prompt.

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

Increase in the number of supported virtual channels

In earlier versions of the client, sessions supported up to 32 virtual channels.

Starting with the 2103 version, you can use up to 64 virtual channels in a session.

Authenticate

September 18, 2023

Starting from Citrix Workspace app 2012, you can view the authentication dialog inside Citrix Workspace app and store details on the sign-in screen. This provides better experiences.

Authentication tokens are encrypted and stored so that you don't need to reenter credentials when your system or session restarts.

> **Note:**
>
> This authentication enhancement is available only in cloud deployments.

Prerequisite:

Install the `libsecret` library.

This feature is enabled by default.

Authentication enhancement for Storebrowse

Starting with version 2205, the authentication dialog is present inside Citrix Workspace app and the store details are displayed on the logon screen for a better user experience. The authentication tokens are encrypted and stored so that you don't need to reenter credentials when your system or session restarts.

The authentication enhancement supports storebrowse for the following operations:

- `Storebrowse -E`: Lists the available resources.
- `Storebrowse -L`: Launches a connection to a published resource.
- `Storebrowse -S`: Lists the subscribed resources.

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

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

> **Note:**
>
> - You can continue to use the remaining storebrowse commands as used earlier (using AuthMangerDaemon).
> - The authentication enhancement is applicable for cloud deployments only.
> - With this enhancement, the persistent login feature is supported.

Support for more than 200 groups in Azure AD

Starting with the 2305 release, an Azure AD user who is part of more than 200 groups can view apps and desktops assigned to the user. Previously, the same user wasn't able to view these apps and desktops.

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

Authentication enhancement for Storebrowse configuration

By default, the authentication enhancement feature is disabled.

If the gnome-keyring isn't available, the token is stored in the selfservice process memory.

To enforce storage of the token in memory, disable gnome-keyring, using the following steps:

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

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

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

Smart card

To configure smart card support in Citrix Workspace app for Linux, you must configure the StoreFront server through the StoreFront console.

Citrix Workspace app supports smart card readers that are compatible with PCSC-Lite and PKCS#11 drivers appropriately. By default, Citrix Workspace app now locates `opensc-pkcs11.so` in one of the standard locations.

Citrix Workspace app can find `opensc-pkcs11.so` in a non-standard location or another `PKCS\##11` driver. You can store the respective location using the following procedure:

1. Locate the configuration file: `$ICAROOT/config/AuthManConfig.xml`.
2. Locate the line <key>PKCS11module</key> and add the driver location to the <value> element immediately following the line.

   > **Note:**
   >
   > If you enter a file name for the driver location, Citrix Workspace app navigates to that file in the `$ICAROOT/PKCS\ ##11` directory. You can also use an absolute path beginning with "/".

After you remove a smart card, configure the behavior of Citrix Workspace app by updating the `SmartCardRemovalAction` using the following steps:

1. Locate the configuration file: `$ICAROOT/config/AuthManConfig.xml`
2. Locate the line <key>SmartCardRemovalAction</key> and add `noaction` or `forcelogoff` to the <value> element immediately following the line.

The default behavior is `noaction`. No action is taken to clear stored credentials and generated tokens on removal of the smart card.

The `forcelogoff` action clears all credentials and tokens within StoreFront on removal of the smart card.

Enabling smart card support

Citrix Workspace app supports various smart card readers if smart card is enabled on both server and Citrix Workspace app.

You can use smart cards for the following purposes:

- Smart card logon authentication - Authenticates you to Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) servers.
- Smart card application support - Enables smart card-aware published applications to access the local smart card devices.

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

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.

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

Enhancement on smart card support

Starting with Version 2112, Citrix Workspace app supports the Plug and Play functionality for the smart card reader.

When you insert a smart card, the smart card reader detects the smart card in the server and client.

You can plug-and-play different cards at the same time, and all of these cards are detected.

Prerequisites:

Install the `libpcscd` library on the Linux client.

> **Note:**
>
> This library might be installed by default in the recent versions of most Linux distributions. However, you might need to install the `libpcscd` library in earlier versions of some Linux distributions, such as Ubuntu 1604.

To disable this enhancement:

1. Navigate to the `<ICAROOT>/config/module.ini` folder.
2. Go to the `SmartCard` section.
3. Set the `DriverName=VDSCARD.DLL`.

Support for new PIV cards

Starting with version 2303, Citrix Workspace app supports the following new Personal Identification Verification (PIV) cards:

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

- IDEMIA next-generation smartcard
- DELL TicTok Smartcard

Performance optimization for smartcard driver

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

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide extra 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 sign in support already implemented for StoreFront. The web sign-in 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.

Support for authentication using FIDO2 in HDX session

Starting with the 2303 version, you can authenticate within an HDX session using password-less FIDO2 security keys. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. For more information about FIDO2, see FIDO2 Authentication.

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

By default, FIDO2 authentication is disabled. To enable FIDO2 authentication, do the following:

1. Navigate to the `<ICAROOT>/config/module.ini` file.
2. Go to the `ICA 3.0` section.
3. Set `FIDO2= On`.

This feature currently supports roaming authenticators (USB only) with PIN code and touch capabilities. You can configure FIDO2 Security Keys based authentication. For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.

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

When you access an app or a website that supports FIDO2, a prompt appears, requesting access to the security key. If you've previously registered your security key with a PIN (a minimum of 4 and a maximum of 64 characters), then you must enter the PIN while signing in.

If you've registered your security key previously without a PIN, simply touch the security key to sign in.

Limitation:

You might fail to register the second device to a same account using FIDO2 authentication.

Customized authentication

The following table provides a reference to the available customized authentication for Citrix Workspace app:

Utility	SDK	Authentication type	Libraries used	Binaries	Authentication type detection
Fast Connect	Credential insertion SDK	Username/pass passthrough	libCredInject.sc	cis	Parameters- Used by third party authenticator integrations
Custom Dialog	Platform Optimization SDK	Username/password/domain/token	UIDialogLib.so and UIDialogLib-WebKit3.so	No	Auto detection - Used by thin clients partners
Storebrowse	Citrix Workspace app	Username/pass	No	Storebrowse	Parameters

Secure communications

August 26, 2023

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.

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

> **Note:**
>
> Citrix recommends using Citrix Gateway between StoreFront servers and user devices.

- A firewall: Network firewalls can allow or block packets based on the destination address and port. If you're using Citrix Workspace app through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.
- Trusted server.
- For Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments only (not applicable to XenDesktop 7): A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or Transport Layer Security (TLS) tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace app and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.
- For Citrix Virtual Apps and Desktops or Citrix DaaS deployments only: Citrix Secure Web Gateway or SSL Relay solutions with TLS protocols. TLS versions 1.0 through 1.2 are supported.

Citrix Gateway

Citrix Gateway (formerly Access Gateway) secures connections to StoreFront stores. Also, lets administrators control, in a detailed way, user access to desktops and applications.

To connect to desktops and applications through Citrix Gateway:

1. Specify the Citrix Gateway URL that your administrator provides using one of the following ways:
   - The first time you use the self-service user interface, you 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're establishing a connection with the storebrowse command, enter the URL at the command line

   The URL specifies the gateway and, optionally, a specific store:

   - To connect to the first store that Citrix Workspace app finds, use a URL of the form, for example: https://gateway.company.com.
   - To connect to a specific store, use a URL of the form, for example: https://gateway.company.com?<storename>. This dynamic URL is in a non-standard form; do not include = (the equals sign character) in the URL. If you're establishing a connection to a specific store with storebrowse, you might need quotation marks around the URL in the storebrowse command.

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

2. When prompted, connect to the store (through the gateway) using your user name, password, and security token. For more information on this step, see the Citrix Gateway documentation.

   When authentication is complete, your desktops and applications are displayed.

Proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app and your Citrix Virtual Apps and Desktops or Citrix DaaS deployment.

Citrix Workspace app supports the SOCKS and HTTPS protocol (Technical Preview), along with the following:

- Citrix Secure Web Gateway and Citrix SSL Relay, the secure proxy protocol
- Windows NT Challenge/Response (NTLM) authentication.

To configure a proxy to launch a desktop using the SOCKS protocol, do the following:

1. Navigate to the `~/.ICAClient/All_Regions.ini` configuration file.
2. Update the following attributes:
   a) Update `ProxyType`. You can use `SocksV5` as `ProxyType`.
   b) Update `ProxyHost`. You can add `ProxyHost` in the following format:

      `<IP>:<PORT>`. For example “10.122.122.122:1080”.

> **Note:**
>
> - To use proxy, disable EDT. To disable EDT, set the `HDXoverUDP` attribute to *off* in the `[Network\UDT]` section of the `~/.ICAClient/All_Regions.ini` configuration file.
> - To ensure a secure connection, enable TLS.

HTTPS protocol support for proxy server

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

To open a desktop using an HTTPS protocol, do the following:

1. Navigate to the ~/.ICAClient/All_Regions.ini configuration file.
2. Go to [Network\UDT] section.
3. Set the following:

```
HDXoverUDP=Off
<!--NeedCopy-->
```

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

4. Go to [Network\Proxy] section.
5. Update the following attributes:
    - Update ProxyType. You can use Secure as ProxyType.
    - Update ProxyHost. You can add ProxyHost in the following format:

<IP>:<PORT>. For example “192.168.101.37:6153”.

Secure proxy server

Configuring connections to use the secure proxy protocol also enables support for Windows NT Challenge/Response (NTLM) authentication. If this protocol is available, it 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 might also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Secure Web Gateway

You can use the Citrix Secure Web Gateway in Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app and the server. If you are using the Secure Web Gateway in **Normal** mode, Citrix Workspace app doesn’t require any configuration.

If the Citrix Secure Web Gateway Proxy is installed on a server in the secure network, you can use the Citrix Secure Web Gateway Proxy in Relay mode. If you’re using Relay mode, the Citrix Secure Web Gateway server functions as a proxy and you must configure Citrix Workspace app to use:

- The fully qualified domain name (FQDN) of the Citrix Secure Web Gateway server.

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

- The port number of the Citrix Secure Web Gateway server.

> **Note:**
>
> Citrix Secure Web Gateway Version 2.0 doesn't support Relay mode.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example: my_computer.my_company.com is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (my_company), and a top-level domain (com). The combination of intermediate and top-level domain (my_company.com) is referred to as the domain name.

SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the Citrix Virtual Apps and Desktops or Citrix DaaS server for TLS-secured communication. When the SSL Relay receives a TLS connection, it decrypts the data before redirecting it to the server.

If you configure SSL Relay to listen on a port other than 443, you must specify the non-standard listening port number to Citrix Workspace app.

You can use Citrix SSL Relay to secure communications:

- Between a TLS-enabled user device and a server

For information about configuring and using SSL Relay to secure your installation, see the Citrix Virtual Apps documentation.

TLS

Previously, the minimum TLS version supported was 1.0, and the maximum TLS version supported was 1.2. Starting with version 2203, the maximum TLS version supported is 1.3.

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

- MinimumTLS=1.1
- MaximumTLS=1.3

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

> **Notes:**
>
> - These values are read whenever programs start. If you change them after starting self-service or storebrowse, type: **killall AuthManagerDaemon ServiceRecord selfservice**

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

> **storebrowse**.
>
> - Citrix Workspace app for Linux does not allow the use of the SSLv3 protocol.
> - TLS 1.0/1.1 works only with the older VDI or Citrix Gateway which support them.

To select the cipher suite set, add the following configuration option in the [WFClient] section:

- SSLCiphers=GOV

This value is the default value. Other recognized values are COM and ALL.

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

CryptoKit update

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

Cryptographic update

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

The TLS_RSA_ cipher suites have been removed entirely. Instead, it supports the advanced TLS_ECDHE_RSA_ cipher suites.

If your environment isn't configured with the TLS_ECDHE_RSA_ cipher suites, client launches aren't supported because of weak ciphers. For client authentication, 1536-bit RSA keys are supported.

The following advanced cipher suites are supported:

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

DTLS v1.0 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS v1.2 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

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

- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

TLS v1.3 supports the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_AES_256_GCM_SHA384 (0x1302)

> **Note:**
>
> From version 1903 and later, DTLS is supported from Citrix Gateway 12.1 and later. For information on DTLS supported cipher suites for Citrix Gateway, see Support for DTLS protocol

Cipher suites

To enable different cipher suites, change the parameter `SSLCiphers` value to `ALL`, `COM`, or `GOV`. By default, the option is set to `ALL` in the `All_Regions.ini` file in the `$ICAROOT/config` directory.

The following sets of cipher suites are provided by ALL, GOV, and COM, respectively:

- ALL
  - all 3 ciphers are supported.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

For troubleshooting information, see Cipher suites.

Cipher suites with the prefix TLS_RSA_ do not offer forward secrecy. These cipher suites are now deprecated in the industry. However, to support backward compatibility with older versions of Citrix Virtual Apps and Desktops or Citrix DaaS, Citrix Workspace app includes an option to enable these cipher suites.

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

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

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

> **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're using version 1901 and earlier, do the following steps:

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

- Delete `All\\_Regions.ini` file

Or

- To retain the `AllRegions.ini` file, add the following lines at the end of the [Network\SSL] section:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

If the `.ICAClient` folder isn't present in the home folder of the current user, it indicates a fresh install of the Citrix Workspace app. In that case, the default setting for the features is retained.

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

> **Note:**
>
> All the preceding cipher suites are FIPS- and SP800-52- compliant. The first two are allowed only for (D)TLS1.2 connections. See **Table 1 – Cipher suite support matrix** for a comprehensive representation of cipher suite supportability.

Certificates

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

The issue occurs when you use Citrix Workspace app 1906 and later. For troubleshooting instructions, see the following Knowledge Center articles:

- CTX260336
- CTX231524
- CTX203362

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

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

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

   > **Tip:**
   >
   > If you can't find a certificate in PEM format, use the `openssl` utility to convert a certificate in CRT format to a .pem file.

2. As the user installs the package (usually root):

   a) Copy one or more files to $ICAROOT/keystore/intcerts.

   b) Run the following command as the user who installed the package:

   ```
   $ICAROOT/util/ctx_rehash
   ```

If you authenticate a server certificate that a certificate authority issued and not trusted in the user devices, follow these instructions before adding a StoreFront store:

1. Get the root certificate in PEM format.
   Tip: If you can't find a certificate in this format, use the `openssl` utility to convert a certificate in CRT format to a .pem file.
2. As the user who installed the package (usually root):
   a) Copy the file to $ICAROOT/keystore/cacerts.
   b) Run the following command:
   ```
   $ICAROOT/util/ctx_rehash
   ```

Enhancement to HDX Enlightened Data Transport Protocol (EDT)

In earlier releases, when `HDXoverUDP` is set to `Preferred`, data transport over EDT is used as primary with fallback to TCP.

Starting with Citrix Workspace app version 2103, when session reliability is enabled, EDT, and TCP are attempted in parallel during the following:

- Initial connection
- Session reliability reconnection
- Auto client reconnect

This enhancement reduces connection time when EDT is preferred. However, the required underlying UDP transport is unavailable and TCP must be used.

By default, after fallback to TCP, adaptive transport continues to seek EDT every five minutes.

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

Enlightened Data Transport (EDT) MTU discovery

Citrix Workspace app version 2109 supports Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT). It increases the reliability and compatibility of the EDT protocol and provides an improved user experience.

For more information see, the EDT MTU Discovery section in the Citrix Virtual Apps and Desktops documentation.

Support for EDT IPv6

Starting with Citrix Workspace app version 2203, EDT IPv6 is supported.

> **Note:**
>
> IPv6 is supported in both TCP and EDT. However, IPv6 is not supported in TCP over TLS and in EDT over DTLS.

Storebrowse

August 26, 2023

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:

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

- You can use the command line and storebrowse commands
- You can use the UI to launch a resource.

This article discusses storebrowse commands.

Storebrowse enhancement for service continuity

Previously, the Workspace connection lease files were synced with files available on the remote server only if you connected using the Self-Service plug-in. As a result, the service continuity feature was not supported when you launched apps or desktop session using storebrowse. Most third-party thin-client vendors use storebrowse to connect to the Workspace platform and the service continuity feature was not enabled for them.

Starting with version 2109 for Citrix Workspace app, the Workspace connection lease files sync with files available on the remote server when you connect using storebrowse as well. This feature helps the third-party thin-client vendors to access Workspace even when offline.

> **Note:**
>
> - This enhancement is available only when service continuity is enabled in cloud deployments. For more information, see the Configure Service Continuity section in the Citrix Workspace documentation.

Command usage

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

Add a store

`-a, --addstore`

Description:

Adds a store with gateway and beacon details along with the ServiceRecord daemon process. This command returns the full URL of the store. An error appears if adding a store fails.

Command example of StoreFront:

Command:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Example:

```
./storebrowse -a https://my.firstexamplestore.net
```

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

> **Note:**
>
> You can add several stores using the storebrowse utility.

Help

`-?, -h, --help`

Description:

Provides details on the storebrowse utility usage.

List store

`-l --liststore`

Description:

Lists the stores that you've added.

Command Example on StoreFront:

`./storebrowse -l`

Enumerate

`-E --enumerate`

Description:

Lists the available resources. By default, the following values appear:

- Resource name
- Display name
- Resource folder

To view more information, append the `-M --details` command to the `-E` command.

> **Note:**
>
> When you run the **-E** command, an authentication window appears if you have not provided your credentials earlier.

Enter the entire store URL as reported by **-liststore**.

Command example of StoreFront:

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

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

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

Subscribed

`-S --subscribed`

Description:

Lists the subscribed resources. By default, the following values appear:

- Resource name
- Display name
- Resource folder

To view more information, append the `-M --details` command to the `-E` command.

Command example of StoreFront:

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

Details

`-M --details`

Description:

This command returns several attributes of the published applications. Generally, this command is used with **-E** and **-S** commands. This command takes an argument that is the sum of the numbers corresponding to the required details:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)

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

- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

> **Notes:**
>
> - To create menu entries for subscribed applications, use the CreateShortcuts(0x100000) argument with the **-S**, **-s**, and **-u** commands.
> - To delete all menu entries, use RemoveShortcuts(0x200000) with the **-S** command.

Command example of StoreFront:

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

In the preceding command example, 0x264 is the combination of DisplayName(0x200), AppIsDisabled(0x40), AppIsDesktop(0x20), and SoundType(0x4). The output lists the subscribed resources along with the details.

You can use the **-M** command for listing the resources with the required details:

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

> **Notes:**
>
> - You can express the values in either decimal or in hexadecimal format. For example, 512 for 0x200.
> - When some of the details aren't available through storebrowse, the output value is zero.

Subscribe

```
-s --subscribe
```

Description:

Subscribes the specified resource from a given store.

Command example of StoreFront:

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

Unsubscribe

```
-u --unsubscribe
```

Description:

Unsubscribes the specified resource from a given store.

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

Command example of StoreFront:

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

Launch

```
-L --launch
```

Description:

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

Command example of StoreFront:

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

Icons

```
-i --icons
```

Description:

This command fetches desktop and application icons in PNG format. This command is used with the **-E** or the **-S** command.

To fetch icons of required sizes and depths, use the best argument or the size argument method.

Best argument

Using the best argument method, you can fetch the best-sized icons available on the server. You can later convert the icons to the required sizes. The best argument method is the most efficient way to store, apply bandwidth, and simplify scripting. The files are saved in the <resource name>.png format.

Size argument

To fetch icons of specified sizes and depths, use the size argument method. An error appears if the server is unable to fetch icons of a given size or depth.

The size argument is of the WxB form, where:

- **W** is the width of icons. All icons are square, so only one value is required to specify the size.
- **B** is the color depth. That is, the number of bits per pixel.

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

> **Note:**
>
> The value **W** is mandatory. The value **B** is optional.

If you leave the values unspecified, icons of all available image depths appear. The files are saved in the <resource name>_WxWxB.png format.

Both the methods save icons in the **.png** format, for each resource that the **-E** or the **-S** command returns.

Icons are stored in the **.ICAClient/cache/icons** folder.

Command example of StoreFront:

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

Reconnect session

`-W [r|R] --reconnect [r|R]`

Description:

Reconnects the disconnected yet active sessions of the specified store. The [r] option reconnects all the disconnected sessions. The [R] option reconnects all the active and disconnected sessions.

Command example of StoreFront:

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

Disconnect session

`-WD --disconnect`

Description:

Disconnects all sessions of the specified store.

Command example of StoreFront:

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

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

Terminate session

```
-WT --terminate
```

Description:

Terminates all sessions of the specified store.

Command example of StoreFront:

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

Version

```
-v --version
```

Description:

Displays the version of the storebrowse utility.

Command example of StoreFront:

```
./storebrowse -v
```

Root directory

```
-r --icaroot
```

Description:

Specifies the root directory where Citrix Workspace app for Linux is installed. If not specified, the root directory is determined at run time.

Command example of StoreFront:

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

Username, Password, Domain

```
-U --username, -P --password, -D --domain
```

Description:

Passes the user name, password, and the domain details to the server. This method works only with a PNA store. StoreFront stores ignore this command. The details aren't cached. Enter the details with every command.

Command example of StoreFront:

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

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

Delete store

```
-d --deletestore
```

Description:

Deregisters a store with the ServiceRecord daemon.

Command example of StoreFront:

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

Configure self-service

```
-c --configselfservice
```

Description:

Gets and configures the self-service UI settings that are stored in StoreCache.ctx. Takes an argument of the <entry[=value]> form. If only an entry is present, the setting's current value is printed. However, if a value is present, the value is used to configure the setting.

Command example of StoreFront:

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

Add CR file

```
-C --addcr
```

Description:

Reads the provided Citrix Receiver (CR) file, and prompts you to add each store. The output is the same as the **-a** command, but has more than one store, separated by new lines.

Command example of StoreFront:

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

Sync connection lease files

```
-o --synclease
```

Description:

Starts to sync Workspace connection lease files with the files available on the remote server for the specified store. This command helps to update the default store and triggers the lease file sync. An error appears if service continuity is disabled.

Command:

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

```
./storebrowse -o *URL of Store *
```

Command example of StoreFront:

```
./storebrowse -o https://my.firstexamplestore.net
```

Close storebrowse daemon

```
-K --killdaemon
```

Description:

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

Command example of StoreFront:

```
./storebrowse -K
```

List error codes

```
-e --listerrorcodes
```

Description:

Lists the error codes that are registered.

Command example of StoreFront:

```
./storebrowse -e
```

Store gateway

```
-g --storegateway
```

Description:

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

Command example of StoreFront:

```
./storebrowse -g “<unique gateway name>” https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Note:**
>
> The unique gateway name must be in the list of gateways for the specified store.

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

Quick launch

`-q, --quicklaunch`

Description:

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

Command example of StoreFront:

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

Daemonize

`-n --nosingleshot`

Description:

Always daemonizes the storebrowse process.

Command example of StoreFront:

```
./storebrowse -n
```

File parameters

`-F --fileparam`

Description:

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

Command example of StoreFront:

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

Workflow

This article demonstrates a simple workflow on how to launch an app using the storebrowse commands:

1. `./storebrowse -a https://my.firstexamplestore.net`

   Adds a store and provides the full URL of the store. Make a note of the full URL because it's used in the later commands.

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

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

   Lists all the published apps and desktops. Enter your credentials using the popup that appears for the registered store.

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

   Launches the resource. Take the Resource_Name from the output of the previous command.

4. `./storebrowse -K`

   This command purges the credentials entered earlier and closes the storebrowse daemon. If you do not mention this command explicitly, the storebrowse process exits after an hour.

Troubleshoot

September 18, 2023

This article provides information to help administrators troubleshoot issues with Citrix Workspace app.

Connection

You might come across the following connection issues.

ICA launch Fedora 29/30

ICA launch might fail on Fedora 29/30. As a workaround, follow the steps:

1. Install `compat-openssl10` by using the command.

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

2. 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:**
>
> Citrix Workspace app works fine in the X.Org server as compared to the Wayland compositor. For distributions that have Wayland as the default graphics protocol, uncomment either of the following:

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

> `WaylandEnable=false` in `/etc/gdm/custom.conf` or in `/etc/gdm3/custom.conf`
>
> Sign out and sign in to point to the X.Org server.

Published resource or desktop session

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

Session reconnection

The connection might fail when reconnecting to a session with a higher color depth than that the Citrix Workspace app requires. This failure occurs when running out of available memory on the server.

If the reconnection fails, Citrix Workspace app tries to use the original color depth. Otherwise, the server tries to start a new session with the requested color depth, leaving the original session in a disconnected state. The second connection might also fail if there's still a lack of available memory on the server.

Full Internet name

Citrix recommends that you configure DNS (Domain Name Server) on your network. This configuration enables you to resolve the names of servers to which you want to connect. If you do not have DNS configured, it might not be possible to resolve the server name to an IP address. Instead, you can specify the server by its IP address, rather than by its name. TLS connections require a fully qualified domain name, not an IP address.

Slow sessions

If a session does not start until you move the mouse, there might be a problem with random number generation in the Linux kernel. As a workaround, run an entropy-generating daemon such as `rngd` (which is hardware-based) or `haveged` (from Magic Software).

Cipher suites

If your connection fails with the new cryptographic support:

1. You can use various tools to check the cipher suites that your server support, including:
   - `Ssllabs.com` (requires the server to have Internet access)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)

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

2. In Linux Client WireShark, find the packet (Client Hello, Server Hello) with the filter (ip.addr == `VDAIPAddress`) to find the SSL section. The result has the cipher suites sent by the client and accepted by the server.

Incorrect Citrix Optimization SDK

The Citrix Optimization SDK package includes an incorrect version of the `UIDialogLibWebKit.so`. As a workaround, do the following:

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

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

    b) Delete all the object files:

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

    c) Go to 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.

Weak cipher suites for SSL connections

When making a TLS connection, the Citrix Workspace app offers an advanced and restricted set of cipher suites by default.

If you're connecting to a server that requires an older cipher suite, set the configuration option `SSLCiphers=ALL` in the [WFClient] section of a configuration file.

The following advanced cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

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

Loss of connection

When using the EDT protocol, you might see the error message: Connection to "…" has been lost. This issue might occur when the connection goes through a router with a Maximum Transmission Unit for EDT that is smaller than the default of 1,500 bytes. Do the following:

- Set `edtMSS=1000` in a configuration file.

Connection errors

Connection errors might produce various different error dialogs. Examples are:

- Error in connection: A protocol error occurred while communicating with the Authentication Service
- The Authentication Service 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 can't 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 must only **accept** or **require** certificates for Citrix, Authentication, and Certificate.
- Other problems.

Low-bandwidth connections

Citrix recommends you use the latest version of Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) on the server. Also, the use the latest Citrix Workspace app on the user device.

If you're using a low-bandwidth connection, you can change your Citrix Workspace app configuration and the way you use Citrix Workspace app to improve performance.

- **Configure your Citrix Workspace app connection** - Configuring your Citrix Workspace app connections can reduce the bandwidth that ICA requires and improves performance
- **Change how Citrix Workspace app is used** - Changing the way Citrix Workspace app is used can also reduce the bandwidth required for a high-performance connection
- **Enable UDP audio** - This feature can maintain consistent latency on congested networks in Voice-over-IP (VoIP) connections

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

- **Use the latest versions of Citrix Workspace app for Linux and Citrix Virtual Apps and Desktops or Citrix DaaS** - Citrix continually enhances and improves performance with each release, and many performance features require the latest Citrix Workspace app and server software

Display

Screen tearing

Screen tearing occurs when parts of two (or more) different frames appear on the screen at the same time, in horizontal blocks. This issue is most visible with large areas of fast changing content on screen.

Tearing is avoided when data is captured at the VDA. Tearing isn't introduced when data is passed to the client. However, X11 (the Linux/Unix graphics subsystem) does not provide a consistent way to draw to the screen in a way that prevents tearing.

To prevent screen tearing, Citrix recommends the standard approach which synchronizes application drawing with the drawing of the screen. That is, wait for `vsvnc`, to start the drawing of the next frame. Depending on the graphics hardware on the client and the window manager you're using, the following two groups of solutions are available to prevent screen tearing:

- X11 GPU settings
- Use a Composition Manager

X11 GPU Configuration

For Intel HD graphics, create a file in the xorg.conf.d called **20-intel.conf** with the following contents:

```
Section "Device"

 Identifier    "Intel Graphics"
 Driver        "intel"
 Option        "AccelMethod" "sna"
 Option        "TearFree" "true"

 EndSection
```

For NVIDIA graphics, locate the file in the xorg.conf.d folder that includes the "MetaModes" Option for your configuration. For each comma-separated MetaMode used add the following:

{ForceFullCompositionPipeline = On}

For example:

Option "MetaModes" "DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"

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

> **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 main page/documentation for Compton for full details. For example, run the following command:

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

Incorrect keystrokes

If you're using a non-English language keyboard, the screen display might not match the keyboard input. In this case, you must specify the keyboard type and layout that you're using. For more information about specifying keyboards, see Control keyboard behavior.

Excessive redrawing

Some window managers continuously report the new window position when moving seamless windows, which can result in excessive redrawing. To fix this problem, switch the window manager to a mode that draws only window outlines when moving a window.

Icon compatibility

The Citrix Workspace app creates window icons that are compatible with most window managers. However, these icons aren't fully compatible with the X Inter-Client Communication Convention.

Full icon compatibility

To provide full icon compatibility:

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

1. Open the wfclient.ini configuration file.
2. Edit the following line in the [WFClient] section: UseIconWindow=True
3. Save and close the file.

Cursor color

The cursor can be difficult to see if it's the same or similar in color to the background. You can fix this issue by forcing areas of the cursor to be black or white.

To change the color of the cursor

1. Open the wfclient.ini configuration file.
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

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

- files that are saved locally and viewed on the server

This issue also affects Japanese characters in parameters used in extended parameter passing.

Session span

Full-screen sessions span all monitors by default, but a command-line multi-monitor display control option, -span, is also available. It allows full-screen sessions to span extra monitors.

Desktop Viewer toolbar functionality allows you to switch a session between windowed and full screen session window, including multi-monitor support for the intersected monitors.

> **Important:**
>
> Span has no effect on Seamless or normal windowed sessions (including those sessions in maximized windows).

The - span option has the following format:
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]

If `h` is specified, a list of monitors is printed on `stdout`. If `h` is the whole option value, wfica exits.

If `o` is specified, the session window has the `override-redirect` attribute.

> **Caution:**
>
> - The use of this option isn't recommended. It's intended as a last option to use with uncooperative window managers.
> - The session window isn't visible to the window manager, does not have an icon, and 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 values specify monitors at the top, bottom, left, and right edges of the area.

Assuming `o` wasn't specified, wfica uses the _NET_WM_FULLSCREEN_MONITORS message to request an appropriate window layout from the window manager, if it 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 might need an override-redirect window. You can set up an override-redirect window using `-span o`.

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

To make a session that spans extra monitors from the command line:

1. At a command prompt, type:

   ```
   /opt/Citrix/ICAClient/wfica -span h
   ```

   A list of the numbers of the monitors currently connected to the user device is printed to stdout and wfica exits.

2. Make a note of these monitor numbers.

3. At a command prompt, type:

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

   The w, x, y, and z values are monitor numbers from step 1 of the preceding steps. The single value w, specifies a specific monitor. Two values w and x specify monitors at the top-left and bottom-right corners of the required area.Four values w, x, y, and z specify monitors at the top, bottom, left, and right edges of the area.

   > **Important:**
   >
   > - Define the WFICA_OPTS variable before starting self-service through a browser. To defin this variable, edit your profile file, normally found at $HOME/.bash_profile or $HOME/.profile, adding a line to define the WFICA_OPTS variable. For example:
   >
   >   ```
   >   export WFICA_OPTS="-span a"
   >   ```
   >
   > - This change affects both virtual apps and desktops sessions.
   > - If you have started self-service or storebrowse, remove processes that are started for the new environment variable to take effect. Remove them with:
   >
   > ```
   > killall AuthManagerDaemon ServiceRecord storebrowse
   > ```

Local applications

You might not escape from a full-screen session to use local applications or another session. This issue occurs because the client-side system UI is hidden and the Keyboard Transparency feature disables the usual keyboard command, for example Alt+Tab, sending the command to the server instead.

As a workaround, use CTRL+F2 to clear the Keyboard Transparency feature temporarily until the focus next returns to the session window. An alternative workaround is to set TransparentKeyPassthrough to No in $ICAROOT/config/module.ini. This workaround disables the Keyboard Transparency feature. However, you might have to override the **ICA file by adding this** setting in the All_regions.ini file.

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

Webcam

Updating the default webcam

Currently, webcam redirection in Citrix Workspace app for Linux supports only one webcam at a time. The default webcam selected is mapped to the device path `/dev/video0` which is, generally, the built-in webcam in laptops.

To list all devices with video capabilities in the system, you must install v4l tools using the following command:

```
sudo apt-get install v4l-util
<!--NeedCopy-->
```

List the video devices using the following command:

```
v4l2-ctl --list-devices
<!--NeedCopy-->
```

You might receive an output as follows:

```
user@user-pc:~ $ v4l2-ctl --list-devices
UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
    /dev/video2
    /dev/video3
    /dev/media1
Integrated Camera: Integrated C (usb-0000:00:14.0-8):
    /dev/video0
    /dev/video1
    /dev/media0
<!--NeedCopy-->
```

As per the preceding example, there are two webcams. You can use any of them. Citrix recommends using the first index. There is a known issue with Ubuntu, so that you might see multiple indexes for one webcam. In this example, you can use /dev/video0 and /dev/video2.

To set another capture video as default, do the following:

1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. In the [WFClient] section, add the following setting.

   `HDXWebCamDevice=<device path>`

For example, add `HDXWebCamDevice=/dev/video2` to set the webcam mapped to `/dev/video2` in a system.

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

Testing capabilities

On the client, the webcam redirection module can be used in different modes to test isolated components under customer environment conditions.

Production and debug mode

This mode compares the video displaying on the VDA side and the actual buffers that the encoder produces on the client side. It allows to test the entire pipeline.

To enable this mode:

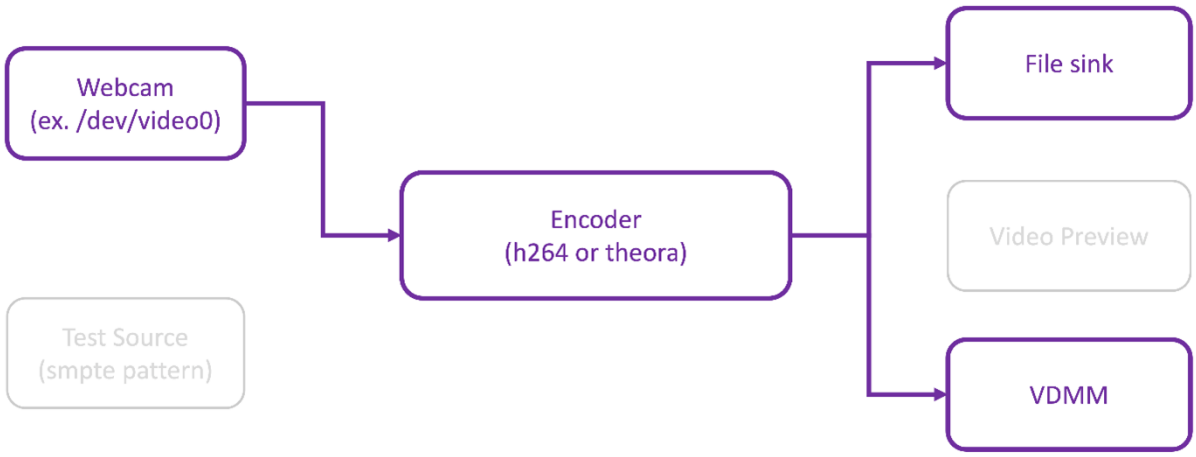
1. Navigate to the `~/.ICAClient/wfclient.ini` configuration file and edit it.
2. Set the `HDXWebcamDebug` value to **True**.

   HDXWebcamDebug = True

After this mode is enabled, the encoder generates the following files with the buffers, depending on the encoder used:

- For H264 encoder: /tmp/file_mode_buffers.h264
- For Theora encoder: /tmp/file_mode_buffers.theora

The following diagram describes the production and debug mode:



Webcam tester mode

This mode allows you to test the webcam isolated from the rest of the pipeline elements.

```
./gst_read --buffers | -b BUFFERS_AMOUNT  [ --input_device | -i
   WEBCAM_DEVICE; default=/dev/video0]
<!--NeedCopy-->
```

To enable to webcam tester mode, run the following commands from the command lines:

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

```
    cd /opt/Citrix/ICAClient/util
    <!--NeedCopy-->
```

```
    `$./gst_read -b 100 /dev/video0
    <!--NeedCopy-->
```

After this mode is enabled, a video preview appears and creates the following file with the raw buffers from the webcam:

/tmp/wewbcam_buffers.buff

The only switch required for webcam tester mode is the `--buffers (-b)` options. You can also specify the webcam device to test. For example, see the following:

- ./gst_read -buffers 150
- ./gst_read –buffers 100 –input_device /dev/video2

The following diagram describes the webcam tester mode:

Encoder tester mode

This mode allows you to test the encoder isolated from the pipeline.

```
./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT;
    default=10 0 ]  [ --enableH264  | -e ]
<!--NeedCopy-->
```

To enable the encoder tester mode, run the following commands from the command lines:

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

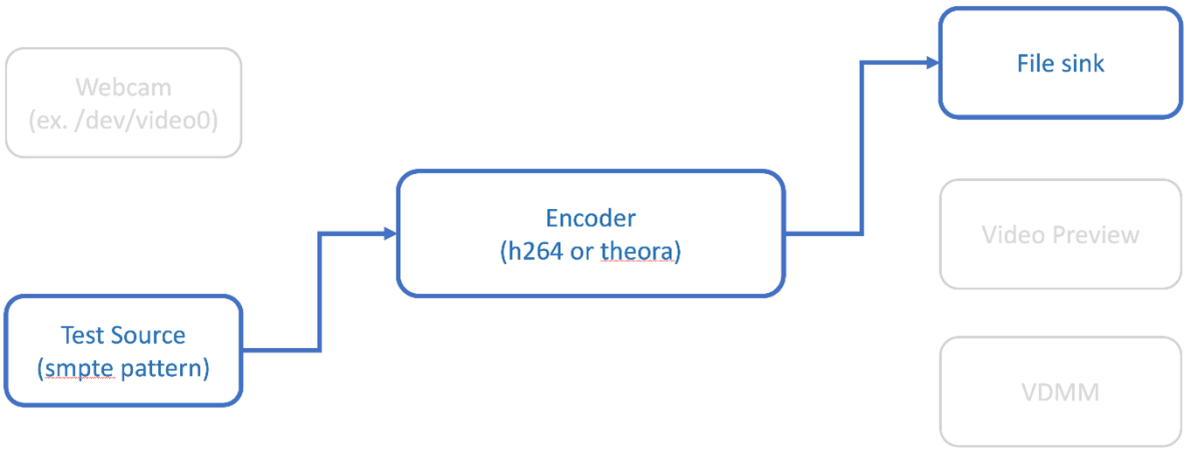
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
./gst_read -o ~/file_buffers.h264 -e
 <!--NeedCopy-->
```

The only switch required for this mode is the `--output_file (-o)` options. You can also test Theora or H264 encoders and the amount of buffer to generate. For example, see the following:

- For H264: ./gst_read –output_file ~/file_buffers.h264 –buffers 200 –enableH264
- For Theora: ./gst_read -o ~/file_buffers.theora -b 100

The following diagram describes the encoder tester mode:



H264 software encoder

If the software-based H264 encoder does not work correctly, you must verify its dependencies using the following steps:

1. Verify if the x264 `GStreamer` plug-in is in the system as part of `gstreamer-plugins-ugly`. If it is available in the `libgstx264.so` library, run the following command to verify it:

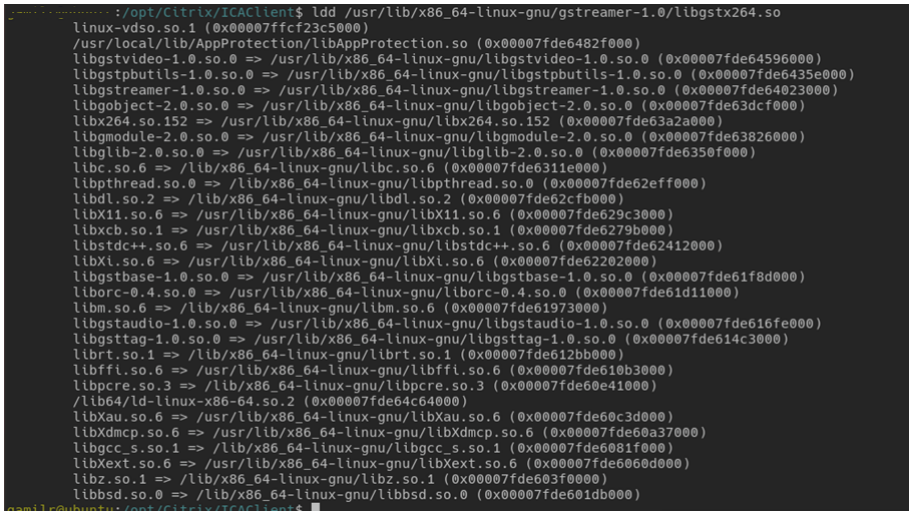
   ```
   gst-inspect-1.0 x264
   <!--NeedCopy-->
   ```

   ```
   :/opt/Citrix/ICAClient$ gst-inspect-1.0 x264
   Plugin Details:
     Name                     x264
     Description              libx264-based H264 plugins
     Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
     Version                  1.14.5
     License                  GPL
     Source module            gst-plugins-ugly
     Source release date      2019-05-29
     Binary package           GStreamer Ugly Plugins (Ubuntu)
     Origin URL               https://launchpad.net/distros/ubuntu/+source/gst-plugins-ugly1.0

     x264enc: x264enc

     1 features:
     +-- 1 elements
   ```

2. Run the following command to verify the dependencies of the `libgstx264.so` library:

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

```
ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
<!--NeedCopy-->
```



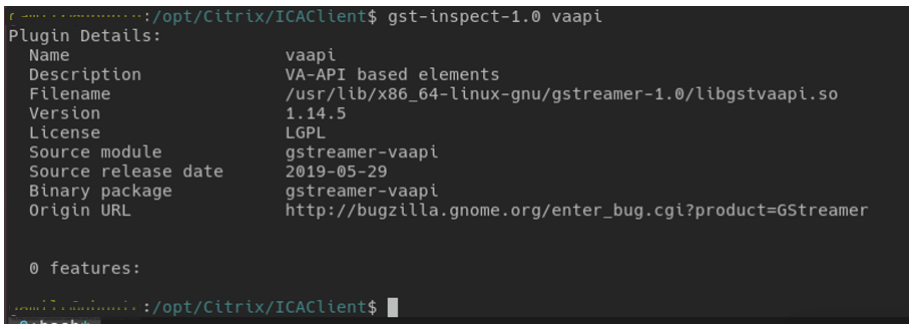
If the `libgstx264.so` file is not present, you must install GStreamer plugins ugly using the following command:

```
sudo apt-get install gstreamer1
0-plugins-ugly
<!--NeedCopy-->
```

H264 hardware encoder

1. Verify `vaapi GStreamer` plug-in is in the system as part of `gstreamer1.0-vaapi`. If it is available in the `libgstvaapi.so` library, run the following command to verify it:

   ```
   gst-inspect-1.0 vaapi
   <!--NeedCopy-->
   ```

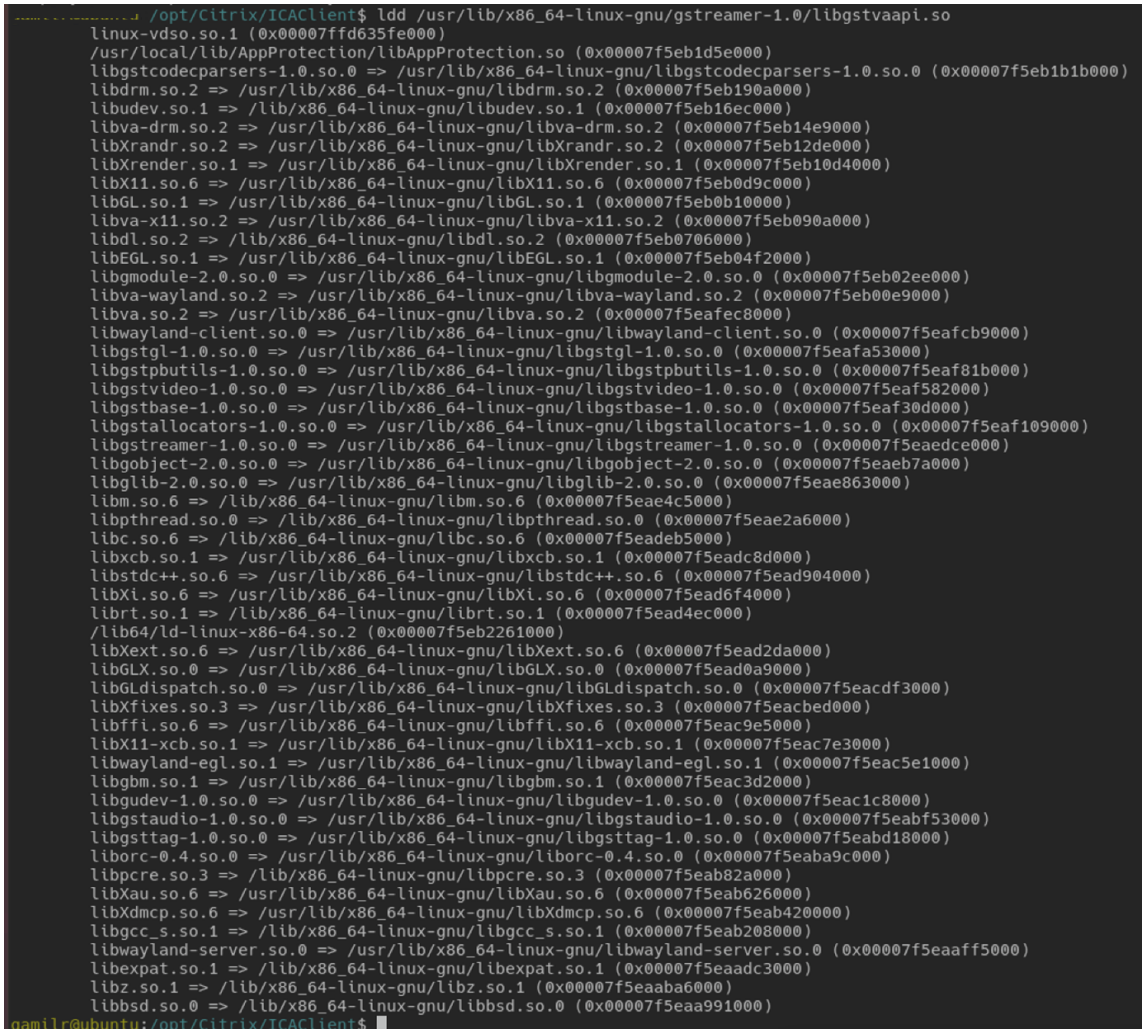
   

2. Run the following command to verify the dependencies of the libgstvaapi.so library:

   ```
   ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
   ```

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

```
<!--NeedCopy-->
```



3. Resolve any missing dependencies.

To install and configure `vaapi`, follow the `GStreamer vappi` installation guide.

Collect internal GStreamer frameworks and gst_read logs

Alternative to regular `ICAClient` logs, you must collect the logs from the `gst_read` module.

Do the following to collect the logs:

1. Open a terminal and run the following commands:

```
export GST_DEBUG=2, gst_read_debug:6
<!--NeedCopy-->
```

```
export GST_DEBUG_FILE=~/gst_read.log
```

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

```
<!--NeedCopy-->
```

> **Note:**
>
> This variable sets the level of logging and the file to store them. In this case, we are setting level 2 for the GStreamer framework and level 7 for the gst_read module. For more information, see the document. It is recommended only to set error and warning levels for the internal GStreamer framework and log level for gst_read.

2. Download an ICA file of a valid VDA.
3. On the same terminal, run the following command to start a VDA session:

```
cd /opt/Citrix/ICAClient
<!--NeedCopy-->
```

```
./wfica   <ICA file path>/vda.ica
<!--NeedCopy-->
```

The gst_read.log file is generated with the internal GStreamer framework and the gst_read logs.

GStreamer pipeline inspections

To see the actual pipelines that the GStreamer framework is creating, do the following:

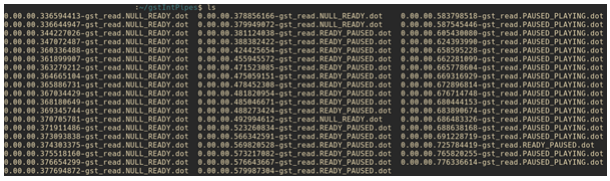
1. Create a folder to store the dot files, for example: gstIntPipes.
2. Open a terminal and export GST_DEBUG_DUMP_DOT_DIR=<Absolute path>/gstIntPipes. This variable indicates to the GStreamer where to store the dot files.
3. Download an ICA file of a valid VDA.
4. On the same terminal, run the following commands to start a VDA session:

```
cd /opt/Citrix/ICAClient/
<!--NeedCopy-->
```

```
./wfica <ICA file path>/vda.ica
<!--NeedCopy-->
```

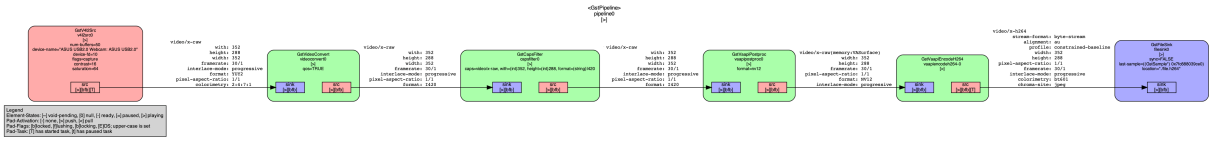
5. The directory gstIntPipes includes the dot files. GStreamer generates a dot file for every state change in the pipeline. As a result, you can inspect all the processes of the pipeline creation. The following is an example of the set of dot files:

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

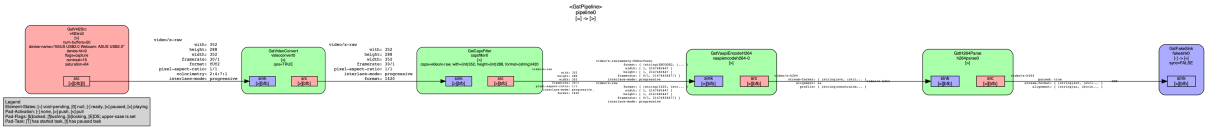


6. Install a dot file utility to see a visual representation of the pipelines. For example, Graphviz. The following images are examples of good and bad creation of the pipeline:

Pipeline successfully created:



Pipeline unable to link:



> **Note:**
>
> To enlarge the preceding images or any other images, right-click the image, select **Open image in new tab**, and zoom the browser as required.

As shown in the preceding image, the second pipeline is unable to link the `GstCapsFilter` element and the `GstVaapiEncodeH264` element. The capabilities are never fully negotiated. For more information, see the document.

System diagnostic script for RAVE

We provide a script, `rave_troubleshooting.sh` to verify whether the system configuration and dependencies are suitable to support Remote Audio Video Extensions (RAVE).

> **Note:**
>
> RAVE is an HDX feature to support optimized webcam redirection and Windows Media Player redirection for Citrix VDAs.

Do the following to run the script:

1. Click rave_troubleshooting.sh to download the script.
2. Open the terminal in your Linux machine.
3. Type `rave_troubleshooting.sh --help` or `rave_troubleshooting.sh -h` to see the supporting command line arguments.
4. Type one of the following:

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

- `rave_troubleshooting.sh -w` or `rave_troubleshooting.sh --webcam` - Use this command to run checks for webcam redirection. This is the default command.
- `rave_troubleshooting.sh -r` or `rave_troubleshooting.sh --rave` - Use this command to run checks for RAVE. A pop-up window playing a h264 test video is displayed.

The system configuration and dependencies are displayed.

Browser

Local browser

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

Access published resources

When you access published resources, your browser prompts to save a file. Browsers other than Firefox and Chrome might require configuration before you can connect to a published resource. However, when trying to access a resource by clicking an icon on the page, your browser prompts you to save the ICA file.

Specific browser

If you have problems using a specific web browser, set the environment variable BROWSER to specify the local path and name of the required browser before running `setupwfc`.

Firefox browser

When you launch desktops or applications in Firefox, if a page is unresponsive, try enabling the ICA plug-in.

ICA plug-in in Firefox

When the ICA plug-in is enabled in Firefox, desktop and application sessions might not start. In this case, try disabling the ICA plug-in.

Configuration errors

These errors might occur if you configured a connection entry incorrectly.

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

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're trying to access a resource through a desktop item or menu, but the Citrix Virtual Apps and Desktops or Citrix DaaS file for the resource isn't available. Refresh the list of published resources by selecting Application Refresh on the **View** menu, and try to access the resource again. If the error persists:

- Check the properties of the desktop icon or menu item
- Check the Citrix Virtual Apps and Desktops or Citrix DaaS file to which the icon or item refers.

Others

Connection issues

You might also find the following issues.

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

Close a session

To know whether the server has instructed Citrix Workspace app to close a session, use the *wfica* program. This program logs when it has received a command to terminate the session from the server.

To record this information through the syslog system, add *SyslogThreshold* with the value 6 to the [WFClient] section of the configuration file. This setting enables the logging of messages that have a priority of LOG_INFO or higher. The default value for *SyslogThreshold* is 4 (=LOG_WARNING).

Similarly, to have *wfica,* send the information to standard error and add *PrintLogThreshold* with the value 6 to the [WFClient] section. The default value for *PrintLogThreshold* is 0 (=LOG_EMERG).

For more information on 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. Also, for each entry in the [Thinwire3.0], [ClientDrive], and [TCP/IP] sections of wfclient.ini, there must be a corresponding entry in canonicalization.ini for the setting to take effect. See the All_Regions.ini and canonicalization.ini files in the $ICAROOT/config directory for more information.

Published applications

If you have issues running published applications that access a serial port, the application might fail (with or without an error message, depending on the application itself) if the port has been locked by another application. In such circumstances, check that there are no applications that have either temporarily locked the serial port or have locked the serial port and exited without releasing it.

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 variable is a requirement if you installed Citrix Workspace app to a non-default location. To overcome this problem, Citrix recommends that you do one of the following:

- Define ICAROOT as the installation directory.

  To check that the ICAROOT environment variable is defined correctly, try starting Citrix Workspace app from a terminal session. If the error message still appears, it is likely that the ICAROOT environment variable is not correctly defined.

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

- Reinstall Citrix Workspace app to the default location. For more information about installing Citrix Workspace app, see Install and set up.

  If Citrix Workspace app was previously installed in the default location, remove the `/opt/Citrix/ICAClient` or `$HOME/ICAClient/platform` directory before reinstalling.

Citrix CryptoKit (formerly SSLSDK)

To find the Citrix CryptoKit (formerly SSLSDK) or OpenSSL version number that you're running, you can use the following command:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

You can also run this command on AuthManagerDaemon or PrimaryAuthManager

Keyboard shortcuts

If your window manager uses the same key combinations to provide native functionality, your key combinations might not function correctly. For example, the KDE window manager uses the combinations from CTRL+SHIFT+F1 to CTRL+SHIFT+F4 to switch between desktops 13 to 16. If you experience this problem, try the following solutions:

- Translated mode on the keyboard maps a set of local key combinations to server-side key combinations. For example, by default in Translated mode, CTRL+SHIFT+F1 maps to the server-side key combination ALT+F1. To reconfigure this mapping to an alternative local key combination, update the following entry in the [WFClient] section of $HOME/.ICAClient/wfclient.ini. This setting maps the local key combination Alt+Ctrl+F1 to Alt+F1:
  - Change Hotkey1Shift=Ctrl+Shift to Hotkey1Shift=Alt+Ctrl.
- Direct mode on the keyboard sends all key combinations directly to the server. They aren't processed locally. To configure Direct mode, in the [WFClient] section of $HOME/.ICAClient/wfclient.ini, set TransparentKeyPassthrough to Remote.
- Reconfigure the window manager so that it suppresses default keyboard combinations.

Remote Croatian keyboard

This procedure ensures that ASCII characters are correctly sent to remote virtual desktops with Croatian keyboard layouts.

1. In the WFClient section of the appropriate configuration file, set UseEUKSforASCII to True.
2. Set UseEUKS to 2.

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

Japanese keyboard

To configure the use of a Japanese keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Japanese (JIS)

ABNT2 keyboard

To configure the use of an ABNT2 keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Brazilian (ABNT2)

Local keyboard

If some keys on the local keyboard do not behave as expected, choose the best-matching server layout from the list in $ICAROOT/config/module.ini.

Windows Media Player

Citrix Workspace app might not have GStreamer plugins to handle a requested format. This issue normally causes the server to request a different format. Sometimes the initial check for a suitable plug-in incorrectly indicates that one is present. This issue is normally detected and causes an error dialog to appear on the server that indicates the Windows Media Player found a problem while playing the file. Retrying the file within the session typically works because Citrix Workspace app rejects the format. And as a result, the server either requests another format or provides the media itself.

In a few situations, there's no suitable plug-in is detected and the file isn't played correctly, despite the progress indicator moving as expected in the Windows Media Player.

To avoid this error dialog or failure to play in future sessions:

1. Temporarily add the configuration option "SpeedScreenMMAVerbose=On" to the [WFClient] section of $Home/.ICAClient/wfclient.ini, for example.
2. Restart wfica from a self-service that has been started from a terminal.
3. Play a video that generates this error.
4. Note (in the tracing output) the mime type associated with the missing plug-in trace, or the mime type that must be supported but does not play (for example, "video/x-h264..").
5. Edit $ICAROOT/config/MediaStreamingConfig.tbl. On the line with the noted mime type, insert a '?' between the ':' and the mime type. This setting disables the format.
6. Repeat steps 2–5 (preceding) for other media formats that produce this error condition.

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

7. Distribute this modified MediaStreamingConfig.tbl to other machines with the same set of GStreamer plugins.

> **Note:**
>
> Alternately, after identifying the mime type it might be possible to install a GStreamer plugin to decode it.

Script to verify system requirements for Windows Media Player redirection

With the 2307 release, a new bash script is introduced to verify the configuration required for the Windows Media Player redirection feature in the Citrix Workspace app for Linux. This feature helps to reduce troubleshooting time for the Windows Media Player redirection feature. To verify the configuration, you can use the same rave_troubleshooting.sh available at System diagnostic script for RAVE.

Serial port setting

To configure a single serial port, add the following entries in the $ICAROOT/config/module.ini configuration file:

LastComPortNum=1

ComPort1=device

To configure two or more serial ports, add the following entries in the $ICAROOT/config/module.ini configuration file:

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Errors

This topic includes a list of other common error messages that you might see when using Citrix Workspace app.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

When running Citrix Workspace app from the command line, this error usually means the description given on the command line wasn't found in the appsrv.ini file.

E_BAD_OPTION - The option "..." is invalid.

Missing argument for option "...".

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

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 might be asked to provide Technical Support with diagnostic information. This information assists this team in trying to diagnose the problem and offer assistance to rectify it.

To obtain diagnostic information about Citrix Workspace app:

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

   A file is generated that provides detailed diagnostic information, which includes version details, the contents of Citrix Workspace app's configuration files, and the values of various system variables.

2. Check the file for confidential information before sending it to Technical Support.

Troubleshoot connections to resources

Users can manage their active connections using the Connection Center. This feature is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. With Connection Center, users can manage connections by:

- Closing an application.

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

- 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

August 21, 2023

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) supports writing server-side applications and client-side drivers for extra virtual channels using the ICA protocol.

The server-side virtual channel applications are on Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) servers.

If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- Working source code for several virtual channel sample programs that demonstrate programming techniques.
- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Linux.

Command-line Reference

For information on command-line reference and parameters, see Citrix Workspace app for Linux Command Reference.

Platform Optimization SDK

As part of the HDX SoC initiative for Citrix Workspace app for Linux, we've introduced the 'Platform optimization SDK'.

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

This SDK enables an ecosystem of low cost, low power, and high performance devices with innovative form factors.

Developers can use the Platform Optimization SDK to improve the performance of Linux-based devices. This SDK allows developers to create plug-in extensions for the ICA engine component (`wfica`) of Citrix Workspace app. Plug-ins are built as shareable libraries and `wfica` loads these libraries dynamically.

These plug-ins can help you optimize the performance of your Linux devices, enabling the following functions:

- Provide accelerated decoding of JPEG and H.264 data used to draw the session image
- Control the allocation of memory used to draw the session image
- Improve performance by taking control of the low-level drawing of the session image
- Provide graphics output and user input services for OS environments that do not support X11

For information, see Citrix Workspace app for Linux - Platform Optimization SDK.

ICA Settings Reference

August 21, 2023

The ICA Settings Reference file provides registry settings and ICA file settings lists, allowing administrators to customize the behavior of the Citrix Workspace app. You can also use the ICA Settings Reference to troubleshoot an unexpected Citrix Workspace app behavior.

ICA Settings Reference (PDF download)

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

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).