Citrix Workspace app for ChromeOS

Contents

Citrix Workspace app for ChromeOS 3

About this release 4

Features in Technical Preview 28

Citrix Workspace app for ChromeOS - Preview 38

Prerequisites for installing 38

Install 40

Get started 46

Configure 52

Customer Experience Improvement Program (CEIP) 58

Clipboard 62

File handling 64

File type association 73

Graphics 74

Keyboard 81

Licensing 92

Multimedia 94

Microsoft Teams optimization 100

Support for Zoom optimization 110

Multi-monitor 114

Peripherals 119

Power settings 137

Printing 138

Seamless experience 141

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session experience 147

Store experience 161

Touch and mobility support 172

URL redirection 174

Virtual channels 177

Troubleshoot 180

Configuration utility tool 188

Authenticate 196

Single sign-on for Citrix Workspace app using Okta as the IdP 200

Single sign-on for Citrix Workspace app using Microsoft Azure as the IdP 206

SDK and API 212

Deprecation 216

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace app for ChromeOS

June 14, 2024

Citrix Workspace app for ChromeOS is a native Chrome packaged app that lets you access Citrix hosted workspace applications and virtual desktops from Chrome devices. It's available from the Chrome Web Store.

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

With the Citrix Workspace app for ChromeOS app installed, you can access desktops and applications within your web browsers. No additional configuration or deployment options are required on StoreFront.

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

For information about deprecated items, see the Deprecation page.

Language support

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

ChromeOS LTS compatibility

Google has the Long-term Support (LTS) version on ChromeOS if you prefer fewer updates. At any point in time, one or more versions of the Citrix Workspace app are compatible with the latest version of ChromeOS LTS.

If you're looking for a version of Citrix Workspace app with latest bug fixes and newer features, we recommend:

- use the latest version of Citrix Workspace app
- use the latest Google ChromeOS version on the stable channel.

For more information on backward compatibility, exclusions, and common questions see the ChromeOS LTS compatibility section in the Install page.

Reference articles

- Global App Configuration service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Optimization for Microsoft Teams
- Microsoft Teams optimization in Citrix Virtual Apps and Desktops environments
- Tech Brief: Workspace Single Sign-On
- Tech Paper: Citrix Workspace app quick start guide
- Tech Brief: Citrix Workspace
- Developer documentation - Citrix Workspace app for Chrome HDX SDK
- Developer documentation - Citrix Virtual Channel SDK
- Citrix Workspace app release timelines

What's new in related products

- Citrix DaaS
- Citrix Workspace
- StoreFront
- Citrix Workspace app for Windows
- Citrix Workspace app for HTML5
- Workspace user interface (UI)

Legacy documentation

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

About this release

June 10, 2024

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

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

What's new in 2405

This release is compatible with ChromeOS version 125. This release addresses areas that improve overall performance and stability.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Technical Preview

- Improved in-session toolbar.

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

Fixed issues in 2405

- In a multi-monitor setup, when you open a published app, a blank screen appears instead of the app screen. The issue occurs when you use full-screen H.264 mode. For more information, see Limitations. [CVADHELP-24883]
- On unmanaged devices, when you start an app or desktop session, the client name sent from Citrix Workspace app for ChromeOS is HTML5-X-X. After the fix, the client name now appears as CrOS-X-X. [RFHTMCRM-12155]
- When you enable the service continuity feature, and start a session offline, the lease files fail to download intermittently, after you sign out from the Citrix Workspace and sign in again. [RFHTMCRM-12492]
- When you start a desktop session, and open an app to enter text, when you start entering, the text disappears and reappears. You can observe that the text flickers. The issue occurs when you use full-screen H.264 mode. For more information, see Limitations. [CVADHELP-24883]

Known issues in 2405

There are no new known issues.

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

Earlier releases

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

2402.1

What's new

This release is compatible with ChromeOS version 121. This release addresses areas that improve overall performance and stability.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Support for Zoom optimization Starting with the 2402.1 version, Citrix Workspace app for ChromeOS supports integration with Zoom virtual desktop infrastructure (VDI) solution for optimized audio and video conferencing experience from within sessions.

After addressing the third-party dependencies related to this feature, it can now be configured and used immediately. Users can take advantage of optimized audio and video, as well as see a decrease in the VDA resource consumption during Zoom meetings within the Citrix session.

For more information about the feature, see Support for Zoom optimization.

Service continuity Starting from the 2402.1 version, the service continuity feature is disabled.

> **Note:**
>
> If you previously enabled the service continuity feature and are using an older version of Citrix Workspace app for ChromeOS, you might be unable to use service continuity. To enable this feature, it is recommended that you update the Citrix Workspace app to the latest version, which is 2402.1 or later and follow the instructions in the Knowledge Center article CTX632723.
>
> For more information on configuration, see the Service continuity documentation.

Config utility tool This release addresses areas that improve overall stability of config utility tool. The configuration setting **allowEditStoreName** is included in the tool.

How to access the tool Previously, the config utility tool was available on the Knowledge Center page.

Starting from the 2402 version, you can download the config utility tool from the Citrix downloads page.

Virtual Channel SDK Starting with the 2402 release, Citrix Virtual Channel SDK (VCSDK) for ChromeOS has capabilities and functionalities that facilitate compatibility of Citrix Workspace app for ChromeOS with third-party plug-ins. Third-party plug-ins must be integrated with VCSDK. This capability handling ensures seamless backward and forward compatibility across all versions and combinations. For more information about these functionalities, see the developer documentation page.

In addition, APIs to support multi-monitor scenarios are added.

HTTP proxy setting on Chromebook In case you have set up the HTTP proxy setting on your Chromebook, it's possible that your sessions might not start.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For more information on how to resolve the issue, see the HTTP proxy setting on Chromebook article.

Short name for store URL Previously, you were able to see the store URLs, but there was no provision to add or modify a short name for the store URLs. This arrangement made it difficult for the administrators and users to remember the store URLs.

Starting with the 2402 release, for managed users, administrators can push a custom store name along with the store URL from the Google Admin Console. This feature makes it easier for users to identify the different stores.

For more information about this feature, see Short name for store URL.

Fixed issues

- If you have virtual desktops with the delivery group name that contains multi-byte characters, you can't start a virtual desktop session. [CVADHELP-24846]
- If you're on an optimized Microsoft Teams call and decide to stop sharing your screen, you might observe a blank rectangle in place of the video section. [RFHTMCRM-11689]
- In kiosk mode, sessions might not start automatically even when the **Auto launch desktop** setting is enabled in StoreFront. [CVADHELP-23698] [RFHTMCRM-11815]
- When you enable the service continuity feature, and click **Reconnect to Workspace**, on the sign-in screen **Use Workspace offline** banner doesn't appear. [RFHTMCRM-11720]
- Citrix Workspace app icon appears on the Chrome shelf instead of the actual desktop session's icons. The issue occurs when you enable the service continuity feature and the cloud deployment outage occurs. [RFHTMCRM-11647]
- When you copy and paste files that are larger than 4 KB using Client Drive Mapping functionality from your local device to the VDA, data might get corrupted. [RFHTMCRM-12156]
- In a session, the mouse click might become unresponsive. [RFHTMCRM-11841] [CVADHELP-24210]
- When a user signs out of a store page (intentionally or due to inactivity) and signs in back to the same store page, the store page might go blank or an infinite spinner might appear. The issue occurs on service continuity-enabled cloud deployments.RFHTMCRM -12212]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2312

What's new

This release is compatible with ChromeOS version 119. This release addresses areas that improve overall performance and stability.

Support for secondary ringer You can use the secondary ringer feature to select a secondary device on which you want to receive the incoming call notification when Microsoft Teams is optimized.

For example, consider that you have set a speaker as the Secondary ringer, and your endpoint is connected to the headphones. In this case, Microsoft Teams sends the incoming call ringer to both the headphones and the speaker. You can't set a secondary ringer in the following cases:

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

> **Note**
>
> By default, this feature is disabled.

Known limitations in the feature

- When you enable this feature, you might hear the secondary ringer play two times with a slight lag. This issue is a bug in Microsoft Teams, and they plan to fix it in the upcoming Microsoft Teams release.

For more information about configuration, see Support for secondary ringer.

Simulcast implementation for optimized Microsoft Teams video conference calls Starting with the 2312 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. It is done 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 depending on several factors including endpoint capability, network conditions, and so on. For example, 720p, 360p, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle therefore giving all users the optimum video experience.

Store URL without HTTPS Starting from the 2312 release, you can enter the store URL directly without mentioning `https://` in the URL explicitly.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> If you're still using a `http` store, we strongly recommend that you migrate to the `https` store. In the meantime, you can access your `http` store by explicitly adding `http` at the beginning of the store URL.

Fixed issues

- A session might fail to start when a cloud deployment outage occurs. For more information on how to configure service continuity, see Service continuity. [RFHTMCRM-11539]
- In a session, when you open the Microsoft Excel app and use the key combination **Ctrl + space-bar**, the key combination might not work as expected. [RFHTMCRM-11718]

2311

What's new in 2311

This release is compatible with ChromeOS version 119. This release addresses areas that improve overall performance and stability.

Technical Preview

- Adaptive Transport

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

Fixed issues in 2311

- USB redirection might not be successful when the DDC V1 policy set on the Citrix Studio in the DDC machine doesn't take effect. The issue occurs when the DDC V1 policy isn't set as a higher priority than the VDA registry setting with the key `\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB`. [RFHTMCRM-11072]
- When you start a desktop session and check the Citrix Director console, the ICARTT value might appear zero. The ICARTT value might have a positive value when you immediately check after you start the session. However, after some time, it might later appear as zero. [CVADHELP-23905]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2310

What's new

This release is compatible with ChromeOS version 118. This release addresses areas that improve overall performance and stability.

Fixed issues in 2310

- When you start a Citrix Workspace app for ChromeOS session on a Chromebook, the Google Drive files might not open. [RFHTMCRM-10540]
- When you open Citrix Workspace app for ChromeOS and navigate to **Settings** > **General** and select the **High DPI Scaling** option, you might see a duplicate cursor when you start the desktop session. [RFHTMCRM-10839]
- When you use Microsoft Teams in a desktop session, the participant's video might not appear correctly when you set the display resolution to the **Device Pixel Ratio Scaling** option. [RFHTMCRM-5271]
- In a session, the audio devices including both speakers and microphones might not appear. The issue occurs if the local machine has no microphone devices, or if the user disables all the microphone devices. [RFHTMCRM-10900]

2309.5

What's new

This release is compatible with ChromeOS version 117. This release addresses areas that improve overall performance and stability.

Fixed issues

This release addresses Window Management API related issues with the Virtual Channel SDK.

2309

What's new

This release is compatible with ChromeOS version 117. This release addresses areas that improve overall performance and stability.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scan code input mode Citrix Workspace app allows you to use external physical keyboards to collaborate with the server-side keyboard layout on the VDA. When administrators enable Scan code mode, the end user might find themselves using the keyboard layout of the server instead of the client.

This feature enhances the user experience particularly when using an East-Asian language physical keyboard.

> **Notes:**
>
> - By default, this feature policy is disabled.
> - On touch devices, when Scan code is enabled, the on-screen software keyboard doesn't work from the Citrix Workspace app.

For more information about configuration, see Scan code input mode.

Custom keyboard mapping Starting with the 2309 version, end users can use Windows-specific shortcuts and key combinations when the VDA is a Windows OS machine, and the native input device is a ChromeOS keyboard. You can now map **Ctrl** and **Alt** keys using custom mapping. The user can select the right or left Control (Ctrl) key to act as an Alt key.

> **Notes:**
>
> - The mapping is possible in full screen mode only.
> - After you save the setting, the mapping affects all sessions.
> - The feature is enabled by default.

For more information about configuration, see Custom keyboard mapping.

For more information on how to use the feature, see the Help documentation.

System shortcuts to VDA in full screen mode Starting with the 2309 version, Citrix Workspace app on ChromeOS devices support passing system shortcuts to the VDA (remote desktop session) in full screen mode. However, it doesn't take effect on the client OS.

Previously, these combinations worked locally. Now, when the feature is enabled and in full screen mode, these combinations are sent to the VDA and yet doesn't take effect locally. For example, the **Refresh** key is a system key on the Chromebook, and a combination of **Ctrl+Shift+Refresh** is a system shortcut on ChromeOS to rotate screen. However, the Windows VDA takes no action because there's no such shortcut in the Windows OS.

Another example, `Alt`+[is used to dock a ChromeOS window on the left, but the same shortcut doesn't take any effect on the Windows VDA. Some applications might use such shortcuts for a specific function for example, `Alt`+[is used by some Barcode Scanner as a prefix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - This feature is enabled by default.

For more information about configuration, see System shortcuts to VDA in full screen mode.

Fixed issues in 2309

- In kiosk mode with a multimonitor setup, both screens might go black when you connect your second monitor and start the session [RFHTMCRM-10905].

  If you are on version 2308, we recommend you upgrade to 2309.

  However, if you want to continue working on 2308, add the following JSON data in from the Google Admin Console:

```
{

"settings": {

        "Value": {

                "settings_version": "1.0",
                "engine_settings": {

                        "features": {

                                    "graphics": {

                                    "graphicsWebWorker": {

                                                "enabled":
                                                   false
                                        }
,
                                  "graphicsWasmRender": false
                                        }

                                     }

                             }

                    }

          }

 }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2308

What's new in 2308

This release is compatible with ChromeOS version 115. This release improves performance related to graphics.

Fixed issues in 2308

- When you start a session in the Managed guest session mode, the USB auto redirection might not work as expected. [RFHTMCRM-10625]
- The Service continuity feature doesn't work. In other words, you can't connect to the DaaS apps and desktops during outages. [RFHTMCRM-9261]

2307

What's new

This release is compatible with ChromeOS version 114. In addition, this release addresses a few issues that help to improve overall performance and stability.

Microsoft Teams enhancements Microsoft Teams optimization supports real-time transcription of what the speaker is saying when Live Captions is enabled in Microsoft Teams.

Auto redirection of USB devices To redirect USB devices automatically, you must follow the USB device rules.
You can configure USB device rules through:

- Google Admin Policy
- Device rules
- Client USB device redirection rules (Version 2)

Enhancement to HDX session experience With an enhanced compression technique, Citrix Workspace app for ChromeOS consumes low network resources and improves session responsiveness.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enhancements to Composite USB redirection through DDC policies Starting with the 2307 version, you can determine if a particular composite USB interface or class can redirect to VDA by default or not. If you have a composite USB connected to the ChromeOS device, then the configuration **enableDefaultAllowPolicy** helps you decide whether, by default, you can allow USB redirection through DDC policies. VDA versions 2212 and later support this feature.

For more information, see the Enhancements to Composite USB redirection through DDC policies documentation.

Client Drive Mapping Starting with the 2307 version, the Client Drive Mapping (CDM) feature supports folder mapping on the local ChromeOS device so they're accessible from within a session. You can map any folder from the ChromeOS device. For example, folders from Downloads, Google Drive, and USB drives, if the folder doesn't contain system files.

The end user can do the following operations:

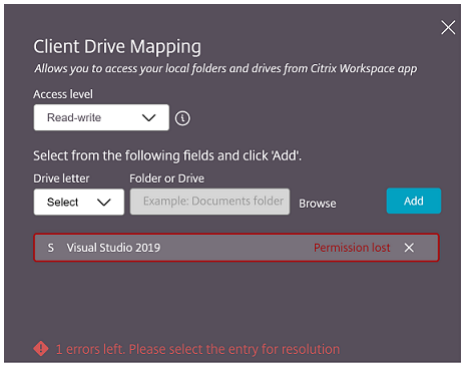
- Copy files and folders to the mapped drive from the session and conversely.
- View the list of files and folders in the mapped drive.
- Open, read, and modify the file contents in the mapped drive.
- View the file properties (modified time and file size only) in the mapped drive.

This feature provides the advantage of accessing both virtual desktop drives and local machine drives together in the file explorer within the HDX session.

Known limitations

- You can't rename files and folders inside the mapped drive.
- Mappings have the name of the folder and not the full path.
- If your local folder has hidden files, and you mapped the same folder, the hidden files are visible inside the session in the mapped drive.
- You can't change the file property to read-only access in the mapped drive.
- CDM isn't supported when sessions are opened in Embed mode using HDX SDK.
- When you map a folder from a removable device and if you remove the device during an active session, you can't use the mapped drive inside the session. To remove the mappings manually, click **X** mark against the particular mapping.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



For more information, see Client Drive Mapping documentation.

Technical Preview

- Accessibility and TalkBack

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

Fixed issues

- When the end user opens a published app and refreshes Citrix Workspace app, a duplicate instance of the published app appears. To apply the configuration settings, see the Refresh store section. [CVADHELP-22229]
- In the multi-monitor mode, when you open a published app on the secondary monitor, mouse clicks might not behave as expected. [CVADHELP-21916]
- The session launch progress notification window that appears at the lower right of the screen might not close even after the session starts. The issue occurs when the VDA version is 7.15. [RFHTMCRM-10161]

2306

This release is compatible with ChromeOS version 114, which Google has chosen as a Long Term Support (LTS) version. As such, Citrix continues to support this release to the end of the LTS lifecycle. Do refer to the Citrix Compatibility Statement for details and exclusions.

What's new

Configure Composite USB Redirection through DDC policies Previously, administrators used Google Admin policies to configure the client-side USB redirection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

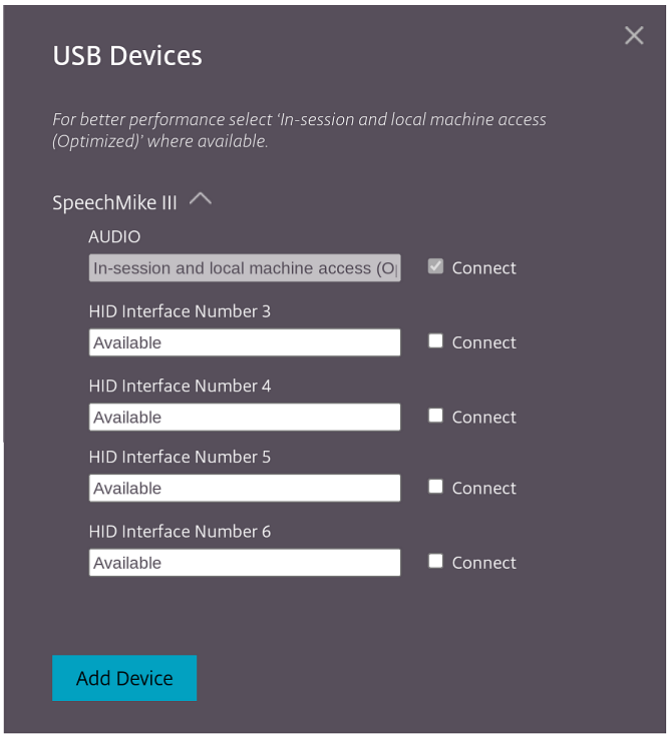
Starting with the 2306 release, you can configure USB redirection through the DDC policies as well. Configurations through DDC policies allow administrators to have a unified and centralized way of defining policies and behavior. These policies are applicable for on-premises and cloud deployments on managed devices and users. This feature is supported on VDA versions 2212 and later.

For information on how to configure, see the Configure Composite USB Redirection through DDC policies documentation.

Enhancements to Composite USB device UI Starting with the 2306 release, when the configuration of a Composite USB device is set to "split": true, the **USB Devices** UI displays the components based on interface numbers instead of interface classes.

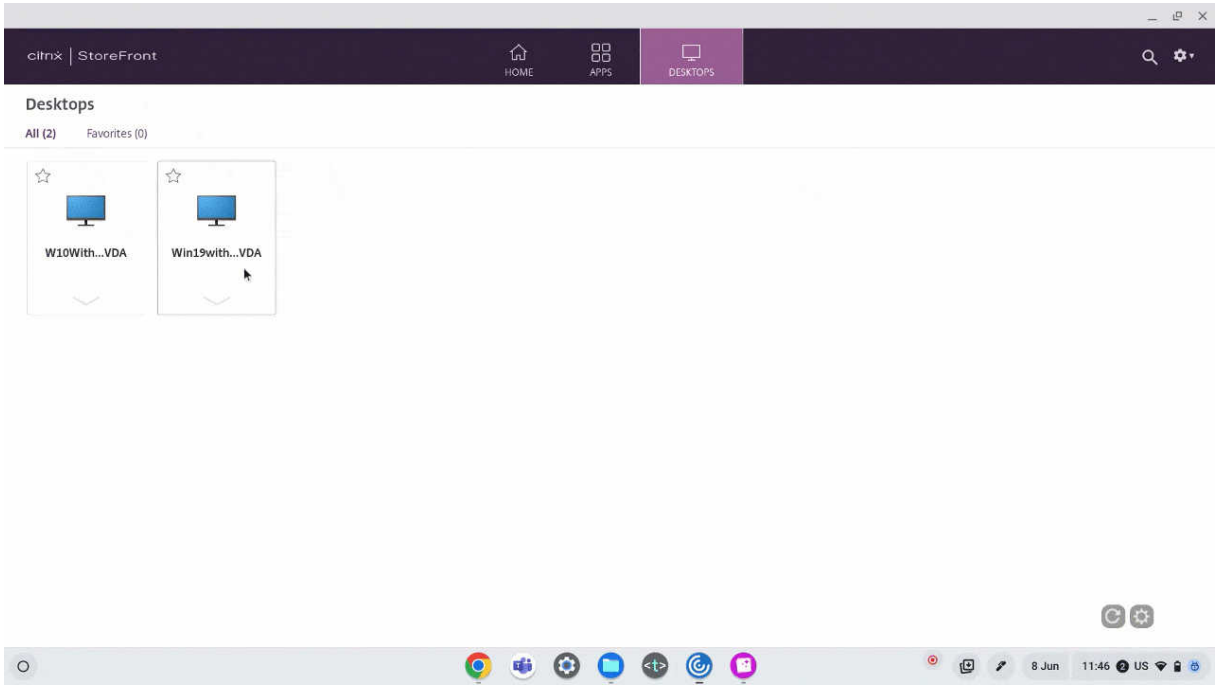
For more information, see the Composite USB redirection article.

User interface The following is an example:



Improved virtual apps and desktops launch experience Starting with the 2306 release, the improved app and desktop launch experience provides timely and relevant information about the launch status.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Fixed issues

- When you unplug and plug the USB device that is already in a session, redirecting the device again fails. A loading spinner UI appears until you restart the Citrix Workspace app. [RFHTMCRM-9715]
- When you are in an optimized Microsoft Teams meeting, the camera streaming fails. The video appears blurry and sometimes the video can become unresponsive. The issue occurs when the screen sharing feature is disabled, and the end user enables the camera in a Microsoft Teams meeting. [RFHTMCRM-9968]
- On a Chromebook, when the session is in the Tablet mode, you might have to tap the app icon, example notepad icon, multiple times from the Chrome shelf to bring the seamless application to focus. [RFHTMCRM-9803]
- When sessions are in the Tablet mode, a Chromebook's stylus pen might not function. [RFHTMCRM-9951]
- In a session, an end user might observe intermittent audio issues. The issue occurs after you upgrade to Citrix Workspace app for ChromeOS 2304 and later versions. [CVADHELP-22784]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2305

What's new

Support for network printers Previously, the Citrix PDF Printer option was used to print from the virtual desktop session. The print driver converted the file to PDF and transferred the PDF to the local device. The PDF was then opened in a new window for viewing and printing.

Starting with the 2305 release, Citrix Workspace app for ChromeOS supports network printing. End users can view the list of printers that are connected to their Chromebook inside the session. Users can select a printer directly without generating intermediate PDF files on the local device. This feature is supported on:

- VDA versions 2112 and later.
- ChromeOS version 112 and later.

> **Note:**
>
> - By default, this feature is enabled, and only the PDF format of metafile printing is supported.

For information on how to configure, see Support for network printers documentation.

Support for multiple stores Starting with the 2305 release, IT administrators can assign multiple stores to end users. Now, it's easy for end users to switch between multiple stores without needing to remember the exact store URL. This feature improves the user experience when accessing multiple stores.

For information on how to configure, see Support for multiple stores documentation.

Enhancements to URL redirection Previously, when [host-to-client redirection] (/en-us/citrix-workspace-app-for-chrome/configure.html#host-to-client-redirection) was enabled, URLs were intercepted on the server VDA and sent to the user's device. Citrix Workspace app for ChromeOS displayed a dialog box asking the user to select whether to open the URL within the session or on the local device. The dialog box appeared for every URL.

Starting with 2305, administrators can configure the URL redirection to open the links in the local device without extra dialog boxes. This enhancement improves the user experience.

> **Note:**
>
> - By default, this feature is disabled.

For information on how to configure, see the Enhancements to URL redirection documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Manifest V3 support for SDK scenarios Starting with the 2305 release, Citrix Workspace app for ChromeOS supports the HDX SDK with Chrome extensions having manifest version 3.

For more information, see Citrix Workspace app for ChromeOS HDX SDK in the developer guides documentation.

Enhancements to Virtual Channel SDK Starting with the 2305 release, Citrix Workspace app for ChromeOS supports Window Management APIs in the Virtual Channel SDK. Web APIs enable IT administrators to create interactive applications and customize them for their end users.

Fixed issues

- When you attempt to disconnect a virtual app or desktop session through an HDX SDK for ChromeOS, the session remains active in DDC. However, the session status changes to inactive after a couple of minutes. [RFHTMCRM-9181]
- In a session, when two participants are in the optimized Microsoft Teams meeting, the screen sharing and audio might fail. The issue occurs when you enable and disable the camera several times during the call. [CVADHELP-22251]
- When you upgrade your device to ChromeOS version 108, text on the published desktop might appear blurred. The issue occurs on devices where the graphical processing unit (GPU) doesn't support medium precision. [CVADHELP-22362]

  > **Note:**
  >
  > - Some devices'display settings don't support high precision, and the text on the published desktop might appear correctly. However, the display might appear abnormal because of this fix. To correct it, administrators can set the **webglHighPrecision** attribute to **false** through the Google Admin Policy.
  >   The following is an example of JSON data:

```
1 ```
2         "hardware" : {
3
4             "webglHighPrecision" : false
5          }
6 ,
7 <!--NeedCopy--> ```
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2304

What's new

Gesture enhancements on touch devices Starting with the 2304 release, Citrix Workspace app enhances end user experience related to gestures, multi-touch, and soft keyboard functionality (Tablet mode). In your Citrix Workspace app sessions, you can use all the familiar multi-touch gestures, including the tap, swipe, and drag.

The following is the gesture guide:

To do this:	On Citrix Workspace app, do this:
Single click	One-finger tap
Right-click	Touch-hold-release
Open the on-screen keyboard	Three-finger tap (or from the toolbar, tap **Keyboard** icon)
Drag	Touch, hold, and slide
Enable cursor	Two-finger tap

Fixed issues in 2304

- There are no fixed issues in this release.

2303

What's new

This release is compatible with ChromeOS version 111. In addition, this release addresses a few issues that help to improve overall performance and stability.

Plug and Play audio device support Previously, only a single audio playback and recording device was supported and displayed as **Citrix HDX Audio** irrespective of the real device name.

Starting With the 2303 release, you can connect multiple audio devices and redirect them to VDA. When you redirect USB audio devices, you can now view the real name of the audio device under the **Sound** settings > **Playback** and **Sound** settings > **Recording** on the VDA. The list of devices on the VDA dynamically update whenever an audio device is plugged in or removed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> By default, this feature is enabled.

For more information, see Plug and Play audio device support.

Background blurring and effects in Microsoft Teams optimization Starting with the 2303 release, Citrix Workspace app for ChromeOS supports background blurring and effects in Microsoft Teams optimization for video calls. You can either blur or replace the background effects provided by Microsoft Teams to avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). This feature can be used with P2P and conference calls.

> **Notes:**
>
> - By default, this feature is disabled.
> - This feature is now integrated with the Microsoft Teams UI. Multi-window support is a prerequisite that needs a VDA update to 2112 or higher. For more information, see Multi-window meetings and chat.

For more information, see Background blurring and effects in Microsoft Teams optimization.

Fixed issues in 2303

- In a session, when two participants are in the optimized Microsoft Teams meeting, the screen turns black when the camera is disabled. In addition, when you click the icons like Screen Sharing, Chat, People, the icons are clickable. However, the options under it get hidden under the black screen and don't appear as expected. [CVADHELP-22173]

2301.1

What's new

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

Fixed issues

- When you copy or paste text in the session, the session becomes unresponsive. The issue occurs when you use Citrix Workspace app for ChromeOS version 2301. [CVADHELP-21951]
- The audio device redirection to the Citrix Virtual Apps and Desktops session isn't working. A red 'X' mark appears on the volume toggle icon in the system tray. The issue occurs after you update the Citrix Workspace app for ChromeOS with the 2301 version. [RFHTMCRM-8799]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2301

What's new

This release is compatible with ChromeOS version 109. In addition, this release addresses a few issues that help to improve overall performance and stability.

Service continuity Service continuity removes or reduces the dependency on the availability of components that are involved in the connection process. You can launch the Citrix Virtual Apps and Desktops and Citrix DaaS regardless of the health status of the cloud services. In other words, service continuity allows you to connect to the DaaS apps and desktops during outages. As a prerequisite, your device must maintain a network connection to a resource location.

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

Plug and Play audio device support Previously, only a single audio playback and recording device was supported and displayed as **Citrix HDX Audio** irrespective of the real device name.

Starting with the 2301 version, we support multiple audio devices and redirect them to VDA. Now, when you redirect audio devices, you can view the real name of the audio device under the **Sound** settings > **Playback** and **Sound** settings > **Recording** on the VDA. The list of devices on the VDA is dynamically updated whenever an audio device is plugged in or removed.

Known Limitations

- On the VDA, the name of the built-in audio device is in English only. The issue occurs when you use ChromeOS-based devices. [RFHTMCRM-8667]

For more information, see the Plug and Play audio device support documentation.

Multi-window chat and meetings for Microsoft Teams Starting with the 2301 version, you can use multiple windows for chat and meetings in Microsoft Teams. You can pop out the conversations or meetings in various ways.

For details about the pop-out window feature, see Pop out a chat in Microsoft Teams.

For troubleshooting see, CTX253754.

Microsoft will deprecate the single-window support in the future. If you're running an older version of Citrix Workspace app or Virtual Delivery Agent (VDA), you can upgrade to:

- Citrix Workspace app 2301 or later
  and
- VDA 2203 or later

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Browser Content Redirection Browser Content Redirection (BCR) redirects the remote browser's content to the user's computer desktop. BCR is a frameless-borderless web browser that runs within the remote desktop window and covers (overlays) the remote (VDA) browser's content area.

BCR redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint. Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA.

In other words, BCR provides the ability of rendering webpages in the allow list on the client side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

> **Note:**
>
> - BCR is compatible with Citrix Virtual Apps and Desktops versions 2212 and later.

For more information on how to set up the allow list see:

- Browser content redirection Chrome extension.
- Browser content redirection policy settings.

Known issues in the feature

- During BCR, when you open a website link in a new tab, it opens in the client browser instead of the session browser. [HDX-43206]

Known limitations in the feature

- This feature doesn't support:
  - Server fetch and client render scenario.
  - Integrated Windows Authentication (IWA) webserver.
  - Multimonitor feature.
- When you upload or download a file to some of the BCR-redirected websites, the ChromeOS file picker appears instead of a VDA session file picker. [HDX-43207]
- Printing isn't supported from BCR-redirected pages.

Double hop Starting with the 2301 version, Citrix Workspace app supports double-hop scenarios. This feature is an enhancement to USB redirection.

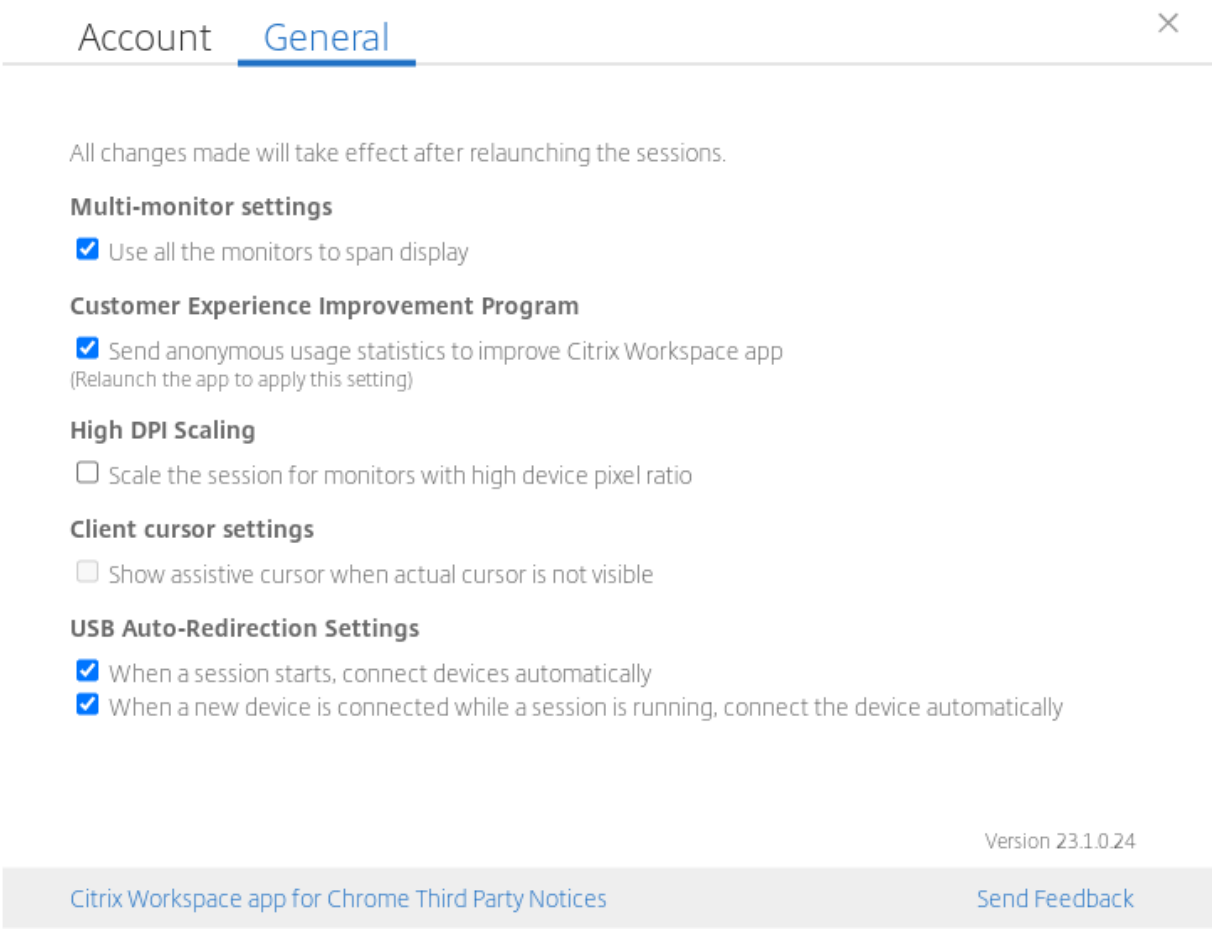
For more information, see Double hop in the Citrix Virtual Apps and Desktops documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB auto redirection settings Previously, there was no option related to USB auto-redirection settings to set the end user preferences. As administrators control these policies, the end user has to manually redirect required USB devices on every session launch.

Starting with the 2301 version, the end user can select a preference for auto-redirection for any USB device within a Virtual Desktop session. Citrix Workspace app now provides app-level settings, where the end user can control the USB auto-redirection. The end user can set preferences and can save the settings across session launches.

There are two options: one at the session launch and the other while the session is ongoing.



Note:

- This feature supports on-premises and cloud deployments and is available only for managed Chrome users.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fixed issues in 2301

- In cloud deployments, the enhanced PDF printing feature does not work as expected. The print preview opens in a new window instead of opening in the same window. [RFHTMCRM-8672]
- Webcam redirection isn't working when you use Citrix Virtual Apps and Desktops version 2206 and later. With the latest fix, the webcam redirection is successful from the Citrix Workspace app for ChromeOS version 2301 and later. [RFHTMCRM-8580]
- When you use Citrix Virtual Apps and Desktops version 2203 and later you might observe that the VDA session appears distorted. [RFHTMCRM-8657]
- When you use a Chromebook and attempt to call from optimized Microsoft Teams, the call doesn't work as expected. The following error message appears:

  "Sorry, it wasn't possible to connect". [CVADHELP-21670] [CVADHELP-21500]

Known issues

Known issues in 2402.1

- The service continuity feature might not work for custom domain URLs. [RFHTMCRM-12363]
- If you attempt to download files or modify files inside the mapped drive from VDA using apps that rely on temporary files, data might get corrupted. For example, browsers, Microsoft office apps such as Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]
- In a session, you might observe poor audio quality. The pitch of the audio stream might change automatically.

  As a workaround, set the attribute **AudioRedirectionV4** to **false**. For detailed steps on how to disable **AudioRedirectionV4**, see the Plug and play audio device support section. [CVADHELP-24722]

Known issues in 2402

- If you attempt to download files or modify files inside the mapped drive from VDA using apps that rely on temporary files, data might get corrupted. For example, browsers, Microsoft office apps such as Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]
- When a user signs out of a store page (intentionally or due to inactivity) and signs in back to the same store page, the store page might go blank or an infinite spinner might appear. The issue occurs on service continuity-enabled cloud deployments.

  As a workaround, click the **Reload** icon on the store page. [RFHTMCRM-12212]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- In a session, you might observe poor audio quality. The pitch of the audio stream might change automatically.

  As a workaround, set the attribute **AudioRedirectionV4** to **false**. For detailed steps on how to disable **AudioRedirectionV4**, see the Plug and play audio device support section. [CVADHELP-24722]

Known issues in 2312

- When you enable the service continuity feature, and when the cloud deployment outage occurs, the Citrix Workspace app icon appears on the Chrome shelf instead of the actual desktop or app session's icons. [RFHTMCRM-11647]

Known issues in 2310

- When you start a desktop session using Citrix Workspace app, green blocks are visible on the display screen that blocks the UI. The issue might occur when you move an application window inside the launched desktop. [CVADHELP-23377]
- In kiosk mode, sessions might not start automatically. [CVADHELP-23698]

Known issues in 2309

- On Chromebook devices, Citrix Workspace app doesn't fall back to IPv4 from IPv6 on a dual-stack Wi-Fi network. [CVADHELP-22537]

Known issues in 2203

- Webcam redirection might not work in some Citrix Virtual Apps and Desktops or XenDesktop. [HDX-39396]

Limitations

- Citrix Workspace app for ChromeOS does not support full-screen H.264 graphics mode for multiple monitors.
- During screen sharing using Microsoft Teams optimization, the red border around the shared window does not appear.
- When **Use Hardware Encoding for Video Codec** is set to **Enabled** in Citrix Studio, your screen might appear green during a session through an Intel vGPU VDA. [RFHTMCRM-5521]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- In multi-monitor sessions through a Microsoft Windows 7 VDA, extended monitors might appear black. Also, the mouse cursor might not render correctly. We recommend selecting a combined display resolution of less than 4800 pixels in width and in height. [RFHTMCRM-5539]
- The server falls back to YUV420 even when configured to Graphics-Thinwire YUV444 setting. The graphics-rich applications are limited to the YUV420 range. [RFHTMCRM-5520]
- Single sign-on (SSO) with Google IdP (Identity provider) isn't supported.
- When you try to sign in to Citrix Workspace app, you can observe issues during the sign-in process. The following error message appears: ERR_TOO_MANY_REDIRECTS.

  The issue occurs when you use Google IdP. [CVADHELP-19362]
- In the optimized Microsoft Teams video call, when you add the third participant, the video goes blank for one of the first two participants. The issue occurs when the first two participants use ChromeOS, and the third participant uses a different OS. [RFHTMCRM-7408]
- When you connect multiple audio devices in a session, you can hear audio from one device only. You might be unable to switch to the other audio device. [HDX-49312]
- In a session, you might not hear the audio from some applications when you disconnect and reconnect to your previous session through the toolbar. [HDX-49313]
- When the end users sign in to the store that is configured through Imprivata as an identity provider (IdP), the client detection screen appears. However, when users click **Detect Citrix Workspace app**, the following error appears:

  "receiver links are blocked."

  As a workaround, reload the Citrix Workspace app for ChromeOS. [CVADHELP-22026]
- When you switch networks and one of the Wi-Fi connections lacks internet connectivity, the session reliability feature doesn't function properly. [RFHTMCRM-12349]
- The lease file sync timer resets every time you click the Citrix Workspace app reload button. This action impacts the delivery of the service continuity feature to the end user. [RFHTMCRM-12499]
- Lease files fail to download after signing off and signing back into the Citrix Workspace app for ChromeOS. [RFHTMCRM-12492]
- The service continuity feature is not supported in Kiosk mode. [RFHTMCRM-12518]

Deprecation

For information about deprecated items, see the Deprecation page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Legacy documentation

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

Technical preview

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.

Features in Technical Preview

June 10, 2024

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

List of features in Technical Preview

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

Title	Available from version	Enablement form (Click the icon)	Feedback form (Click the icon)
Improved in-session toolbar	2405	You can configure the feature	
Adaptive Transport	2311		
Accessibility and TalkBack	2307	Enablement not required	

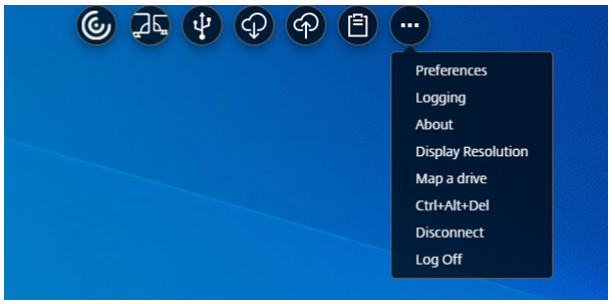
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Improved in-session toolbar

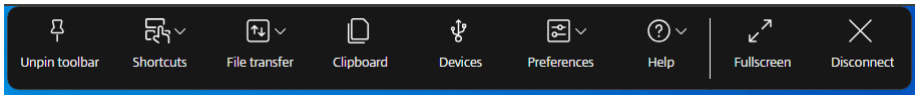
This feature is in technical preview from 2405 release.

Starting with the 2405 version, an enhanced toolbar UI appears when you start a desktop session. The look and feel of the in-session toolbar UI has changed. The toolbar UI is specifically designed to enhance the end user experience by organizing the options in a user-friendly manner.

Old toolbar UI



New toolbar UI



> **Note:**
>
> This feature is disabled by default. To enable the feature, follow the configuration steps. To provide feedback about this feature, click the Podio form.

Configuration

You can enable the new toolbar UI by using the Google Admin Policy.

Google Admin Policy For managed devices and users, administrators can enable the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> You can apply this configuration on the following as well:
>
> - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
> - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
> - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

The following is an example of JSON data:

```
{

    "engine_settings": {

        "ui": {

            "toolbar":
                {
  "switchToNewToolbar": true
                }

             }

        }

 }

<!--NeedCopy-->
```

4. Save the changes.

Icons and actions

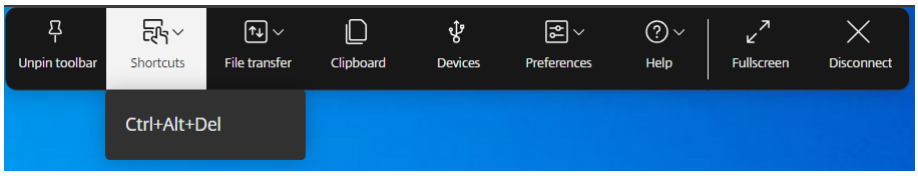
End users can perform the following actions:

> **Note:**
>
> The icons are visible to the end users only if their organization's admin has enabled the specific feature.

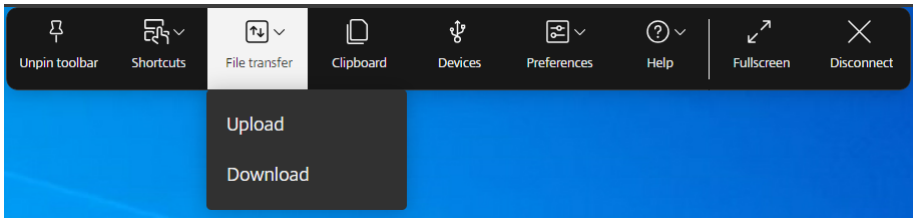
- **Toolbar notch** –when you start an app or a desktop session, the toolbar notch appears at the top the screen. When you click the notch, the toolbar appears in the unpinned state. Drag and reposition the toolbar notch onto any side of the screen. After you release the mouse, the notch will automatically align itself with the nearest edge.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Pin** –when you pin it, you can drag and reposition the toolbar onto any side of the screen. After you release the mouse, the notch will automatically align itself with the nearest edge. The advantage of pinning the toolbar is that it doesn't minimize into a notch after you complete an action that involves toolbar icons.
- **Unpin** –when you unpin the toolbar, it minimizes into a notch after you complete an action that involves toolbar icons.
- **Shortcut keys** –you can perform the **Ctrl+Alt+Del** function with the click of a button. This option facilitates users to sign out, switch users, lock the system, or access the Task Manager.



- **File transfer** –you can upload or download a file between a user device and a session. For more information, see File handling.

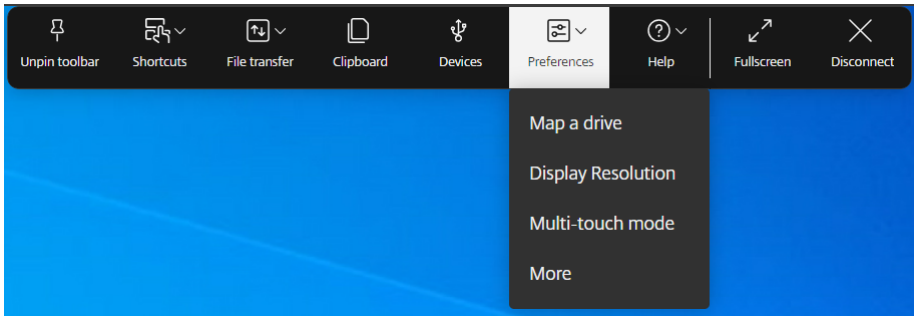


- **Clipboard** –you can use the clipboard option to copy and paste plain text and HTML data from the VDA to the local device and back. For more information, see Clipboard.
- **Devices** –click to open the **USB Devices** dialog box. Click **Add** to view the USB devices connected to the local device. The dialog box lists the devices that can be redirected to the session. To redirect the USB devices, select an appropriate device and click **Connect**. For more information, see USB device redirection.

  > **Note:**
  >
  > You can view the **Devices** icon only if your IT administrator provides access to connect USB devices through policy settings.

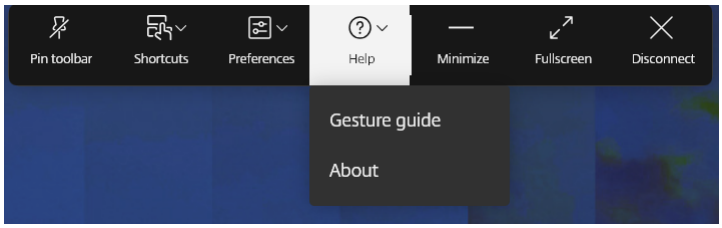
- **Preference** –You can set your preference as follows. The following four options appear:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



  - **Map a drive** –the Client Drive Mapping (CDM) feature allows you to access your local folders and drives from Citrix Workspace app. For more information, see File handling.
  - **Display Resolution** –select the size of the resolution for the session display. By default, the screen resolution is set to Auto-fit screen.
  - **Multi-touch mode** –click to use the multi-touch mode. You can toggle between Panning and Multi-touch mode. This option is applicable to touch screen devices. For more information, see Touch and mobility support.
  - **More** –displays preferences about the soft keyboard button and Citrix Customer Experience Improvement Program (CEIP).

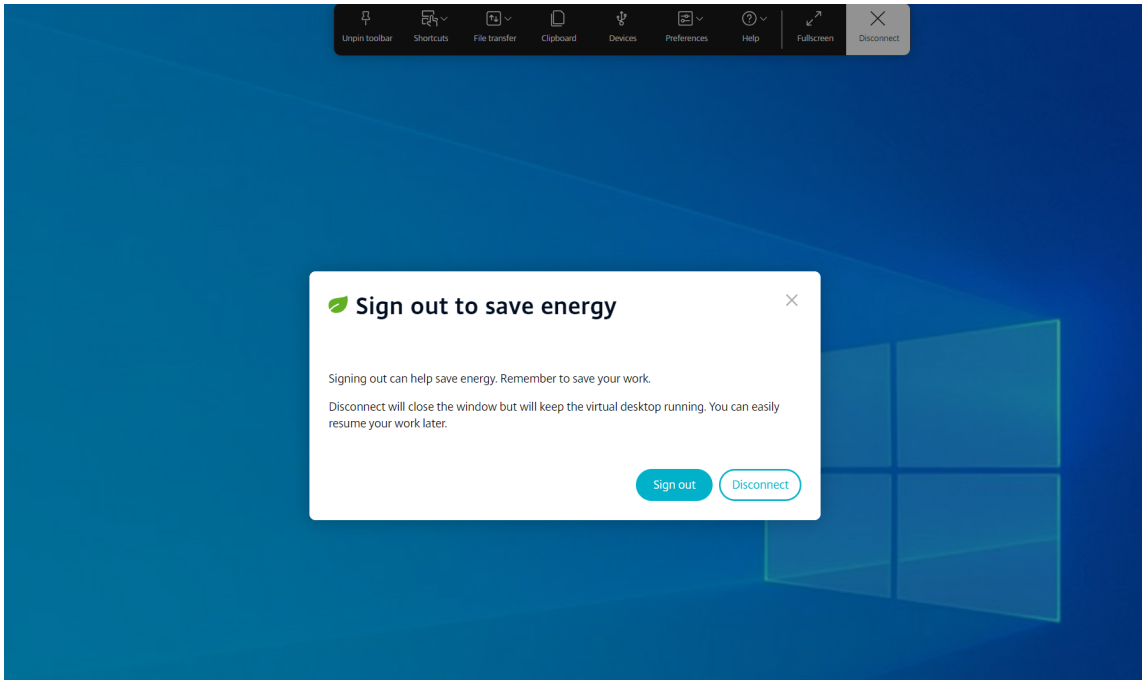
- **Help** - the following three options appear:



  - **Gesture Guide** –a gesture guide appears with details on how to use finger taps. This option is applicable to touch screen devices.
  - **About** –displays the current version of the Citrix Workspace app that you are using.

- **Minimize** –you can minimize the session window.
- **Fullscreen** –you can switch your screen from windowed to fullscreen. If you have a multi-monitor set-up, the fullscreen button will extend the screen across the set-up and also function as a multi-monitor button.
- **Disconnect** –the disconnect action will keep the virtual desktop running. Sign out to save energy. For more information, see Sustainability initiative from Citrix Workspace app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Adaptive Transport

This feature is in technical preview from 2311 release.

Starting from the 2311 version, Citrix Workspace app for ChromeOS supports the Adaptive Transport feature.

Adaptive Transport delivers a superior user experience on challenging long-haul connections while maintaining server scalability. This feature delivers a high-quality HDX experience on web-based platforms.

For more information, see the Adaptive transport section in the Citrix Virtual Apps and Desktops documentation.

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

System requirements

The following are the requirements for using Adaptive Transport and EDT:

- Control plane

  Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Virtual Apps and Desktops 1912 or later

- Virtual Delivery Agent
  - Version 1912 or later (2203 or later recommended)
  - Version 2012 is the minimum required for using EDT with the Citrix Gateway Service

- StoreFront
  - Version 3.12.x
  - Version 1912.0.x

- Citrix Gateway (ADC)
  - 13.1.17.42 or later (recommended)
  - 13.0.52.24 or later
  - 12.1.56.22 or later

- Firewall (from VDA perspective)
  - UDP 1494 inbound –if session reliability is disabled
  - UDP 2598 inbound –if session reliability is enabled
  - UDP 443 inbound –if you enable VDA SSL for ICA encryption (DTLS)
  - UDP 443 outbound –if using Citrix Gateway Service. For more information, see the Citrix Gateway service documentation.

Administrator configurations

- To configure the **HDX Adaptive Transport** setting in the Citrix policy, see the Configuration section in the Citrix Virtual Apps and Desktops documentation.
- You can configure the Adaptive Transport feature in the following way:

  Google Admin Policy

  For managed devices and users, administrators can enable the feature using the Google Admin Policy as follows:

  1. Sign in to the Google Admin Policy.
  2. You can apply this configuration to the following:
     - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
     - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

The following is an example of JSON data:

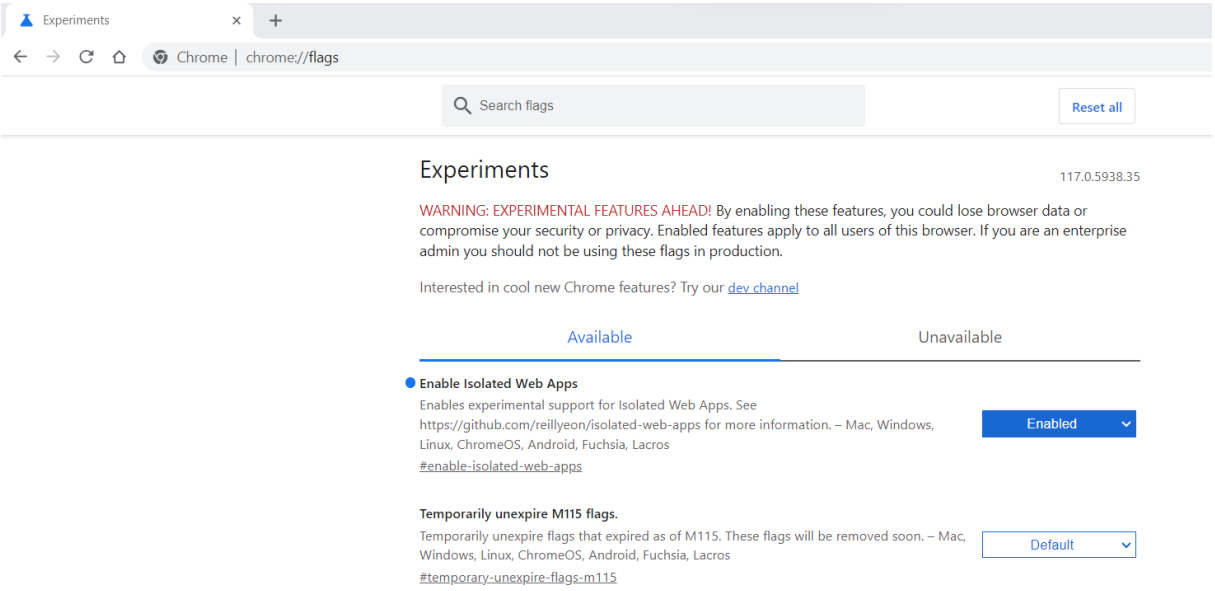
```
{

"settings": {

"Value": {

    "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "edt": {

                        "enabled": true
                             }

                         }

                     }

                 }

             }

 }

<!--NeedCopy-->
```

3. Save the changes.

End user configuration

To enable the adaptive transport feature, enter `chrome://flags` in the Google Chrome browser address bar. Enable the option **Enable Isolated Web Apps** as shown in the following screenshot:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Accessibility and TalkBack

This feature is in technical preview from 2307 release.

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

To use the ChromeOS narrator (ChromeVox), end users must use the keyboard shortcut Ctrl+Alt+Z to turn the narrator on. Use the same key combination to turn the narrator off.

> **Note:**
>
> - By default, this feature is disabled.

Configuration

You can configure the Accessibility feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js To enable the accessibility feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

2. Edit the **configuration.js** file and add the **accessibility** attribute. Set the **enable** attribute to **true**.

   The following is an example of JSON data:

```
'features' :
{

    'accessibility': {

          'enable': true
         }
 ,
 }


<!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy For managed devices and users, administrators can enable the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management > Chrome Management > User Settings**.
3. Add the following strings to the policy.txt file under the engine_settings key.
   Following is an example of JSON data:

```
'features' :
{

    'accessibility': {

          'enable': true
         }
 ,
 }


<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Save the changes.

Citrix Workspace app for ChromeOS - Preview

June 12, 2024

Citrix Workspace app for ChromeOS 2408 - Preview is coming soon. Look forward to the new features and resolved issues in the upcoming 2408 release.

The generally available version of Citrix Workspace app for ChromeOS is 2405. For more information on the current release, see About this release.

Prerequisites for installing

April 24, 2024

System requirements and compatibility

Requirements

All devices must meet the minimum hardware requirements for the installed operating system.

Users devices require the latest Google Chrome operating system (OS) to access desktops and apps using Citrix Workspace app. Citrix recommends you use the latest Citrix Workspace app from the Google ChromeOS Stable channel.

Citrix Workspace app for ChromeOS is supported only on ChromeOS. Citrix Workspace app supports the ChromeOS Flex operating system too.

Add and open Chrome apps Citrix Workspace app for ChromeOS is supported only on ChromeOS. On your Chromebook, you can add and open apps from the Chrome Web Store. For more information, see the Google support article.

> **Notes:**
>
> - Chrome Apps in the Chrome Web Store are only supported on Chromebooks and won't work on Windows, Mac, or Linux after December 2022.
> - End Of Life (EOL) Chromebook devices do not update to more recent versions of the Google ChromeOS. The EOL devices do not support all the Citrix Workspace app for ChromeOS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> updates. We recommend and support the latest versions of the Google Chrome operating system.

Supportability matrix

Citrix Workspace app for ChromeOS supports access to desktops and applications through the following versions of StoreFront. Stores must be accessed through Citrix Receiver for Web sites. Citrix Workspace app for ChromeOS does not support direct access to StoreFront stores, either using the store URL or the XenApp Services URL.

- StoreFront 2.5 and later

Citrix Workspace app for ChromeOS can be used to access desktops and applications delivered by the following product versions:

- XenApp and XenDesktop 7.6 and later

Secure user connections

In a production environment, Citrix recommends securing communications between Citrix Workspace for Web sites and users'devices with Citrix Gateway and HTTPS. Citrix recommends using SSL certificates with a key size of at least 1024 bits throughout the environment in which Citrix Workspace app for ChromeOS is deployed. Citrix Workspace app for ChromeOS enables user access to desktops and applications from public networks with the following versions of Citrix Gateway.

- NetScaler Gateway 10.5 and later

Citrix Workspace app for ChromeOS supports CloudBridge disabling compression and printer compression in addition to using HDX Insight analytics to display in CloudBridge Insight Center.

- CloudBridge 7.4 and later

> **Note:**
>
> If you're unable to connect to the SSL-enabled VDA with Citrix Workspace app for ChromeOS, see TLS settings on VDAs. Configure the cipher suite that suits you.

Microsoft Teams optimization requirements

Minimum version:

- Microsoft Teams optimization for audio calls, video calls, and screen sharing is generally available from release 2105.5 and later.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

We recommend that you use the latest version of Citrix Workspace app for ChromeOS. By default, screen sharing is disabled. To enable screen sharing, see settings.

- VDA version 1906 or later.

Hardware:

For a peer-to-peer video conference call or screen sharing, the minimum requirement is:

- an Intel® Core™ i3 processor with a 2.4 GHz quad core CPU that supports 720p HD resolution.

Install

April 12, 2024

Both end users and IT administrators can install Citrix Workspace app for ChromeOS.

Install from Chrome Web Store

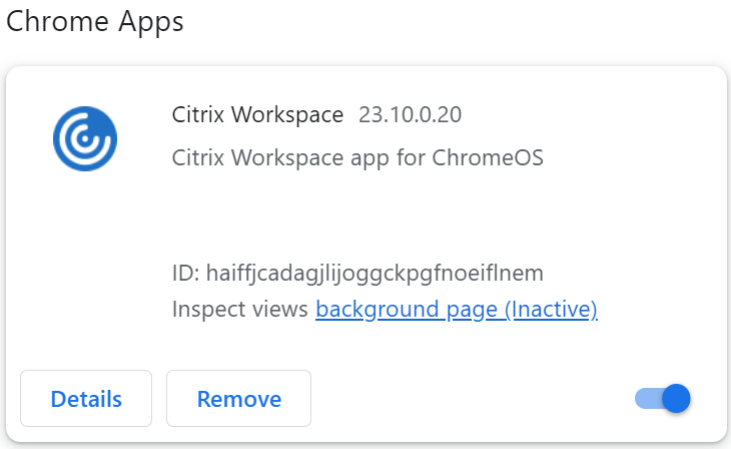
The end user can install Citrix Workspace app for ChromeOS from the Chrome Web Store as follows:

1. Click the link https://chromewebstore.google.com/detail/citrix-workspace/haiffjcadagjlijoggckpgfnoeiflnem.

   The Citrix Workspace app for ChromeOS web store page appears.

2. Click **Add to Chrome**.

   The app is installed. Navigate to `chrome://extensions` in your Chrome browser to view the Chrome Apps.

3. Search for *Citrix Workspace app* in the ChromeOS Launcher to use it.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> To start using the app, end users can enter either a valid store URL or an email address. Usually, an IT administrator gives you the store URL address or configures your email address with the associated store URLs. Adhere to your organization's guidelines.

Install manually

There are several options for deploying Citrix Workspace app for ChromeOS.

- You can use the Google App management console to configure Citrix Workspace using Google policy. For more information on ChromeOS configuration, see Knowledge Center article CTX141844.
- You can repackage Citrix Workspace app for ChromeOS to include a Citrix Workspace configuration (.cr) file you've generated. The **.cr** file contains the connection details for Citrix Gateway and the Citrix Receiver for Web site that provides users' desktops and apps. Users browse to chrome://extensions and then drag the repackaged app (.crx) file onto the Chrome window to install Citrix Workspace app for ChromeOS. Because the app is pre-configured, users can start working with Citrix Workspace app when they install it, without a need to do extra configuration steps.

Admins can deliver your custom Citrix Workspace app for ChromeOS application to end users in the following ways:

- Publish the repackaged application for users through Google Apps for Business using the Google Admin Console.
- Provide the .crx file to users through other means, such as through email.
- Users can install Citrix Workspace app for ChromeOS from the Chrome Web Store. For more information, see Install from Chrome Web Store.

After your install, Citrix Workspace app must be configured with connection details for Citrix Gateway and the Citrix Receiver for Web site that provides users' desktops and apps. This capability can be achieved in two ways:

- Generate a **.cr** file containing the appropriate connection details and distribute this file to users. To configure Citrix Workspace app for ChromeOS, users double-click the **.cr** file and click Add when prompted. For more information about generating.cr files from StoreFront, see Export store provisioning files for users.
- Provide users with the URL that they must enter manually when they first start Citrix Workspace app for ChromeOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Repackage

To simplify the deployment process for users, you can repackage Citrix Workspace app for ChromeOS with a new **.cr** file to preconfigure Citrix Workspace app for ChromeOS with the appropriate connection details for your environment. Users can start working with Citrix Workspace app for ChromeOS when they've installed it without the need to do any additional configuration steps.

1. Download the unpackaged version of Citrix Workspace app for ChromeOS to a suitable location.
2. Download the sample configuration file and customize it as appropriate for your environment.
3. Rename the modified configuration file to default.cr and copy it to the Citrix Workspace app for ChromeOS root directory.

   Configuration files with different names or in other locations aren't included when Citrix Workspace app for ChromeOS is repackaged.
4. By default, the in-session toolbar is enabled. If you want to disable the in-session toolbar do the following steps.

   Note: We recommend that you back up the configuration.js file before you modify it.

   a) Use a text editor to open the configuration.js file in the Citrix Workspace app for ChromeApp root directory.

   b) Locate the following section in the file.

   ```
   pre codeblock 'appPrefs':{ 'chromeApp':{ 'ui': { 'toolbar': {
    'menubar':true, 'clipboard': false <!--NeedCopy-->
   ```

   c) Change the setting for the menubar attribute to **false**.

   Note: To override any previous configuration, we recommend that you use the Google Admin console to push the policy.
5. By default, Citrix Workspace app for ChromeOS can open any file extension using the Files App in a Chromebook. You can use the Chromebook that is intended for opening files in Google Drive using the FileAccess component in the VDA.

   If an administrator wants to disable this option to download the unpackaged version of Citrix Workspace app and edit the "file handlers"section in manifest.json to resemble the following:

```
"file handlers" : {

        "text" :
            "extensions" :  \[
                 "ica",
                  "cr"
              \]
           }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 9
10      }
11
12  <!--NeedCopy-->
```

6. In Chrome, browse to chrome://extensions, select the **Developer mode** checkbox in the top right corner of the page and then click the **Pack extension** button.

   For security reasons, StoreFront only accepts connections from known Citrix Workspace app for ChromeOS instances. You must add your repackaged application to allow list to enable users to connect to a Citrix Receiver for Web site.

7. On the StoreFront server, use a text editor to open the web.config file for the Citrix Receiver for Web site, which is in the **C:\inetpub\wwwroot\Citrix\storename** Web directory. The *storename* is the name, which is specified for the store when it was created.

8. Locate the following elements in the file.

   ```
   pre codeblock <html5 ... chromeAppOrigins="chrome-extension://
   haiffjcadagjlijoggckpgfnoeiflnem"... /> <!--NeedCopy-->
   ```

9. Change the value of the **chromeAppOrigins** attribute to chrome-extension:*//packageid*, where **packageid** is the ID generated for your repackaged application.

Backup and early access release builds

There is an option to use the backup and early access release builds for Citrix Workspace app for ChromeOS. The backup build option provides business continuity if there are any ongoing issues in the production build. Before you proceed, familiarize with the following build IDs:

- `haiffjcadagjlijoggckpgfnoeiflnem`: is the ID for the published version of Citrix Workspace app for ChromeOS on the Chrome Web store.
- `lbfgjakkeeccemhonnolnmglmfmccaag`: is the ID for the Early Access Release (EAR) version of Citrix Workspace app for ChromeOS.
- `anjihnbmjbbpofafpmklejenkgnjfcdi` is the ID for the backup build of Citrix Workspace app for ChromeOS. The backup build has the contents of the release before the current production release with a different version ID.

To access the backup build

To access the backup build, do the following:

1. Click the link https://chrome.google.com/webstore/detail/citrix-workspace-backup/anjihnbmjbbpofafpmklejenkgnjfcdi.

   The Citrix Workspace app Backup extension page appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Click **Add to Chrome**.

   The app is installed. Navigate to `chrome://extensions` in your Chrome browser to view the extension.

3. Search for Citrix Workspace app in the ChromeOS Launcher to use it.

To access the EAR build

To access the EAR build, do the following:

1. Click the link https://chrome.google.com/webstore/detail/citrix-workspace-backup/lbfgjakkeeccemhonnolnmglmfmccaag.

   The Citrix Workspace app for ChromeOS extension page appears.

2. Click **Add to Chrome**.

   The app is installed. Navigate to `chrome://extensions` in your Chrome browser to view the extension.

3. Search for Citrix Workspace app in the ChromeOS Launcher to use it.

ChromeOS LTS compatibility

Google has the Long-term Support (LTS) version on ChromeOS if you prefer fewer updates. At any point in time, one or more versions of the Citrix Workspace app are compatible with the latest version of ChromeOS LTS.

If you're looking for a version of Citrix Workspace app with the latest bug fixes and newer features, we recommend:

- use the latest version of Citrix Workspace app
- use the latest Google ChromeOS version on the stable channel.

Backward compatibility

Bug fixes on ChromeOS or Citrix Workspace app might not be backward compatible with ChromeOS LTS version. To access backward compatibility, you might need to switch to the ChromeOS stable channel.

New features that are provided by Citrix or Google might depend on newer software versions. To access new features, use the stable channel for ChromeOS and the latest version of Citrix Workspace app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exclusions

The following features aren't eligible for compatibility with ChromeOS LTS:

- Microsoft Teams Optimization
- Browser Content Redirection

Updates to the excluded features are available on the latest version of ChromeOS on the stable channel along with the latest version of the Citrix Workspace app.

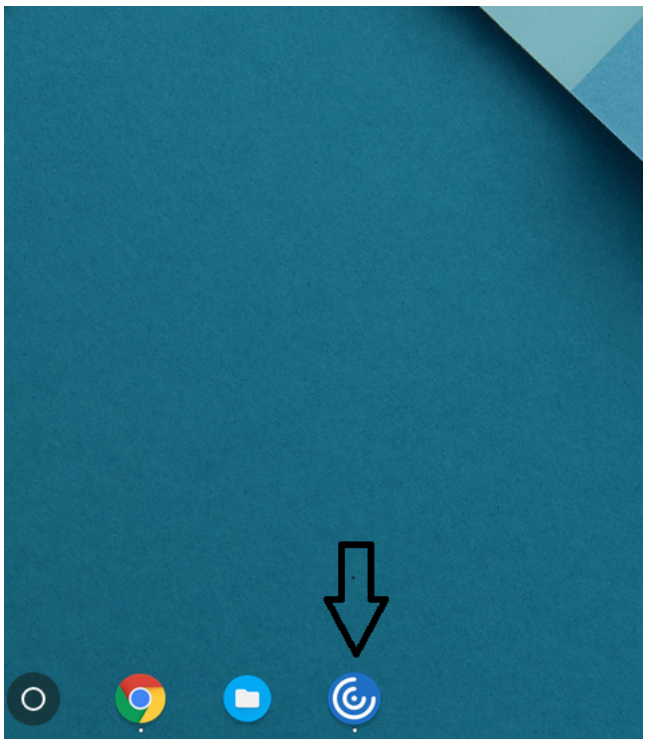
Common questions

- How do I know which version of the Citrix Workspace app is compatible with the latest ChromeOS LTS release?
  - You can find the latest version on the About this release page.
  - You can find the installable file for the latest version on the Citrix Downloads page.
- As an administrator, how do I test on the ChromeOS LTS channel?
  - For information, see Long-term support releases in the Google ChromeOS education page.
- As an administrator, what do I must do if I encounter an issue while on ChromeOS LTS with Citrix Workspace app?
  - Verify if you observe the same issue with the latest version of ChromeOS on the stable channel along with the latest version of the Citrix Workspace app. If yes, report the issue through your usual support channels. If not, update to the version where you didn't find the issue.

Uninstall

After installing and configuring Citrix Workspace app, select the Citrix Workspace icon in the Chrome apps list. Citrix Workspace app for ChromeOS starts as shown in the following image. To remove Citrix Workspace app for ChromeOS from their devices, right-click the Citrix Workspace icon in the Chrome apps list and select **Uninstall**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Upgrade

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

- Download the Citrix Workspace app from the Citrix download page and install the app to upgrade from Citrix Receiver to Citrix Workspace app.
- Upgrade your Citrix Workspace app using your OS app store.
- On Windows and macOS, auto-update to Citrix Workspace app from Citrix Receiver using Citrix Receiver Updates.

For the documentation of Citrix Receiver for Chrome, see Citrix Receiver.

Get started

April 23, 2024

Set up

Desktops and applications appear after logging in. You can search for resources and click an icon to start a desktop or application in a new window.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When you start an extra application, Citrix Workspace app for ChromeOS checks if the application can be launched in an existing session before creating a session. This capability enables you to access many applications in a single session.

You can configure the features and functionalities of Citrix Workspace app for ChromeOS using any of the following methods:

- Google Admin Policy
- Web.config in StoreFront
- default.ica
- configuration.js

> **Note:**
>
> With version 1901, the splash screen is no longer visible to users. The schema "**splashScreen" : false"** will no longer be supported in future releases. You must remove the schema, if present, from the Google Admin policy or the configuration.js file.

Using Google Admin policy

> **Note:**
>
> Citrix recommends using this method only when Citrix Workspace app for ChromeOS is repackaged for users.

Before Version 2.1, only store or beacon related configurations can be pushed through the Google Admin Policy. For additional information about this policy, see Knowledge Center articles CTX141844 and CTX229141.

With Citrix Workspace app for ChromeOS Version 2.1, other Chrome configurations can also be pushed through the Google Admin Policy.

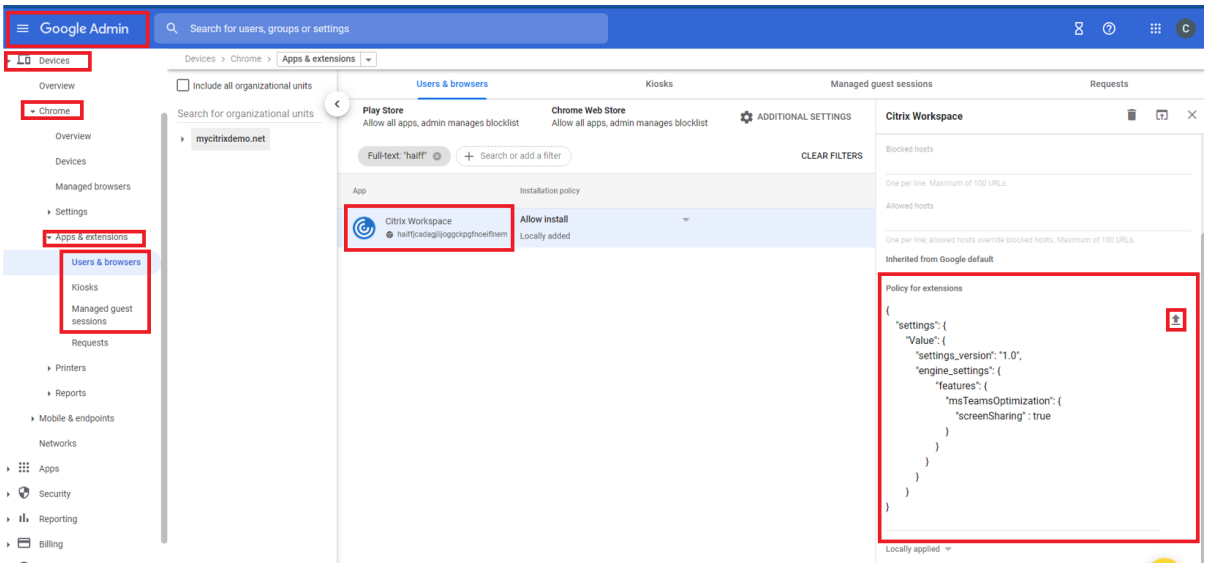
How to push policies through the Google Admin console

To push any policy through the Google admin console, follow these steps:

1. In the **Google Admin** console, select **Devices > Chrome > Apps & extensions > Users & browsers**.
2. Search for Citrix Workspace app (enter the web store app id, for example, `haiffjcadagjlijoggckpgfnc`).
3. Click the Citrix Workspace app icon.
4. The policy for extensions appears. Copy and paste the policy or upload the policy.txt file with the relevant JSON.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Click **Save**.
6. Repeat the steps for **Kiosk** and **Managed guest sessions** as required.



For more information, see Google support.

Verifying the configuration of policies

To verify that policies are pushed correctly, do the following:

1. Navigate to `chrome://policy/`.
2. Click `Reload policies`.
3. Search for the Citrix Workspace app for ChromeOS Web Store ID, which is `haiffjcadagjlijoggckpgfnc`
   .
   - If policies are pushed successfully from the Google Admin Console, they appear under the Web Store ID: `haiffjcadagjlijoggckpgfnoeiflnem`. If not, verify that the policies are configured correctly. To create or edit the policy, make sure to use the `Configuration Utility Tool`.
   - If the policies appear under the Web Store ID but do not take effect in the session, contact Citrix Technical support.

Using webconfig

> **Note:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Citrix recommends that you use the **web.config** file method for configuration purposes only when a store version of Citrix Workspace app for ChromeOS is being used.

To change the configuration using the Web.config file method (only for those using on-premises Store-Front):

1. Open the **web.config** file for the Citrix Receiver for Web site. This file is in **C:\inetpub\wwwroot\Citrix\<store** where *storename* is the name specified for the store when it was created.
2. Locate the **chromeAppPreferences** field and set its value with the configuration as a JSON string.

For example:

```
chromeAppPreferences = {

    "ui": {

        "toolbar": {

            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

Another sample example is as follows,

```
web.config | default.ica
    <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
  </serverSettings>
  <clientSettings>
    <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
      changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
      loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
      webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
    <storeProxy keepAliveURL="Home/KeepAlive">
      <resourcesProxy listURL="Resources/List" resourceDetails="default" />
      <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
        logoffURL="Sessions/Logoff" />
      <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
        getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
    </storeProxy>
    <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
      <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
      <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
        minimumSupportedOSVersion="10.6" />
      <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9]|\d\d).*Safari;MSIE \d\d;Tri
        launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
        singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflne
        chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}' />
      <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*((Firefox/((5[2-9]|[6789][0
        skipDoubleHopCheckWhenDisabled="false" />
    </pluginAssistant>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Using the default.ica file

> **Note:**
>
> Citrix recommends that you use the **default.ica** file method for configuration purposes only for Web Interface users.

Citrix Workspace app for ChromeOS allows Custom.ica files without any initial program value.

To change the configuration using the **default.ica** file:

1. Open the default.ica file from **C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica** for Web interface customers, where **sitename** is the name specified for the site when it was created. For StoreFront customers, the **default.ica** file is at **C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\d** where **storename** is the name specified for the store when it was created.
2. Add a key at the end of the file, **chromeAppPreferences** with its value set to configuration as the JSON object.

For example:

```
chromeAppPreferences={

    "ui":{

        "toolbar": {

            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

A sample **default.ica** file looks as follows:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

web.config default.ica

```
19
20  [Application]
21  TransportDriver=TCP/IP
22  DoNotUseDefaultCSL=On
23  BrowserProtocol=HTTPonTCP
24  LocHttpBrowserAddress=!
25  WinStationDriver=ICA 3.0
26  ProxyTimeout=30000
27  AutologonAllowed=ON
28  TWIMode=Off
29  FontSmoothingType=0
30
31  [EncRC5-0]
32  DriverNameWin16=pdc0w.dll
33  DriverNameWin32=pdc0n.dll
34
35  [EncRC5-40]
36  DriverNameWin16=pdc40w.dll
37  DriverNameWin32=pdc40n.dll
38
39  [EncRC5-56]
40  DriverNameWin16=pdc56w.dll
41  DriverNameWin32=pdc56n.dll
42
43  [EncRC5-128]
44  DriverNameWin16=pdc128w.dll
45  DriverNameWin32=pdc128n.dll
46
47  [Compress]
48  DriverNameWin16=pdcompw.dll
49  DriverNameWin32=pdcompn.dll
50
51  chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'
```

Using the configuration.js file

The **configuration.js** file is in the **ChromeApp root** folder. Access this file directly to modify Citrix Workspace app for ChromeOS.

> **Note:**
>
> - Citrix recommends that you back up the configuration.js file before you modify.
> - Administrator-level credentials are required to edit the configuration.js file; after editing the file, repackage the app to make other modifications to toolbar elements.
> - In kiosk mode, the toolbar is hidden by default. When editing the configuration.js file to enable the toolbar, verify that kiosk mode is disabled. Citrix recommends that you use one of the alternative methods (for example, the default.ica file) to enable the toolbar.

Custom branding of logo and icon

You can customize the Citrix Workspace app logo and icons for apps and desktops as you want. You can customize them as follows:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Install the Citrix Workspace app for ChromeOS build from the chrome web store.
2. Navigate to the folder **/chromeAppUI/resources/images**.
3. Replace the following images with the images that you want but with the same dimensions:
    - icon_16x16.png
    - icon_32x32.png
    - icon_48x48.png
    - icon_128x128.png
    - icon_256x256.png
4. Navigate to the **ChromeApp root** folder and open the **manifest.json** file.
5. Replace the value for the name and description with the required text.
6. Save the changes.
7. Reload the app from the extensions page.

Configure

April 12, 2024

Feature flag management

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

How to configure

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

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

Enable traffic to the following URLs

- events.launchdarkly.com
- app.launchdarkly.com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

On the cloud setup, administrators can disable the LaunchDarkly service by setting the **enableLaunchDarkly** attribute to **False** in the Global App Configuration service.

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

On the on-premises deployment, administrators can disable the LaunchDarkly service using the Google Admin Policy as follows:

1. Sign in to the Google Admin Console.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.

```
"thirdPartyServices": {


  "enableLaunchDarkly": false

 }
 ,

<!--NeedCopy-->
```

4. Click **Save**.

> **Note:**
>
> - By default, the LaunchDarkly service is enabled if the **enableLaunchDarkly** attribute isn't present.

On the on-premises deployment, administrators can disable the LaunchDarkly service using the configuration.js file as follows:

> **Note:**
>
> - Administrator-level credentials are required to edit the configuration.js file; after editing the file, repackage the app for the changes to take effect.

1. Open the **configuration.js** file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Add the **enableLaunchDarkly** attribute and set the attribute to **false**.

```
"thirdPartyServices": {


    "enableLaunchDarkly": false

      }
 ,
<!--NeedCopy-->
```

3. Click **Save**.

> **Note:**
>
> - By default, the LaunchDarkly service is enabled if the **enableLaunchDarkly** attribute isn't present.

Note on Configuration JSON

With the version 2202.1 (22.2.1.8), Citrix Workspace app honors only valid JSON for pushing the configuration. Do the following to validate the JSON file:

1. Verify the JSON data. Use the link https://jsonlint.com/ to verify.
2. Follow the steps mentioned in the Get started page to update:

    - Google Policy
    - web.config
    - default.ica
    - configuration.js

    We recommend using the Configuration utility tool to generate valid JSON settings to customize Citrix Workspace app for ChromeOS using:

    - configuration.js
    - web.config
    - default.ica
    - Google Policy

> **Note**:
>
> You might experience session launch issues when the configuration JSON is invalid.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HTTP proxy setting on Chromebook

In case you have set up the HTTP proxy setting on your Chromebook, it's possible that your sessions might not start.

To resolve the issue, you can disable the **nativeSocket** setting on the Google Admin Console and make sure that you've enabled the **WebSockets connections** policy in DDC. For more information, see the WebSocket article.

The following is an example of JSON data:

```
{

        "settings": {

        "Value": {

              "settings_version": "1.0",
              "engine_settings": {

                          "transport":
                                 {
  "nativeSocket": false
                                     }

                               }

                      }

           }

 }

<!--NeedCopy-->
```

> **Warning:**
>
> Disabling the **nativeSocket** attribute enables WebSocket connection, which might affect performance in comparison to using a native socket.

Kiosk mode

Citrix Workspace app for ChromeOS kiosk mode helps you to run all apps in the same window. Using this feature, you can run Citrix Workspace apps in kiosk mode, and then launch any Windows app or desktop using the same mode. In addition, kiosk mode allows you to publish remote apps or desktops as a dedicated Chrome package using a persistent URL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

How to configure

You can control this feature by adjusting the kiosk settings in the Chrome admin panel. This setting applies for managed Chrome devices only.

See the Google support site for instructions on enabling the Citrix Workspace app to run in kiosk mode on managed and non-managed Chrome devices.

If you're deploying a Citrix Workspace app, you must publish using the visibility options set to `Public /unlisted` to verify interoperability with kiosk mode. Go to the Chrome Web Store Developer Dashboard

The store URL is read-only when kiosk mode is active and can't be edited using the **Account** settings screen. However, you can change this setting by either:

- repackaging the app with the `.cr` file, or
- using the Google Admin Console. Use Google Policy Management to access Google Admin Console.

```
    <Services version="1.0">
    <Service>
    <rfWeb>http://your_RfWebURL_or_persistenturl</rfWeb>
    <Name>Mystore</Name>
    <Gateways>
    <Gateway>
    <Location>https://yourcompany.gateway.com</Location>
    </Gateway>
    </Gateways>
    <Beacons>
    <Internal>
    <Beacon>http://yourcompany.internalwebsite.net</Beacon>
    </Internal>
    <External>
    <Beacon>http://www.yourcompany.externalwebsite.com</Beacon>
    </External>
    </Beacons>
    </Service>
    </Services>

<!--NeedCopy-->
```

If you're using the Google Admin Console, edit the **policy.txt** file containing the Citrix Workspace configuration. Replace the value of "url"under "rf_web"with a persistent URL.

```
    {

    "settings": {

    "Value": {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    "settings_version": "1.0",
    "store_settings": {

    "beacons": {

    "external": [
    {

    "url": "http://www.yourcompany.externalwebsite.com"
     }

    ],
    "internal": [
    {

    "url": "http://yourcompany.internalwebsite.net"
     }

    ]
     }
,
    "gateways": [
    {

    "is_default": true,
    "url": "https://yourcompany.gateway.com"
     }

    ],
    "name": "mystore",
    "rf_web": {

    "url": " http://your_RfWebURL_or_persistenturl "
     }

     }

     }

     }

     }

<!--NeedCopy-->
```

Global App Configuration service

From this release, as an administrator, you can use the Global App Configuration service to:

- centrally manage and configure app settings and set defaults.
- apply the settings for both managed and unmanaged (BYOD) devices

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- apply the settings for both cloud users (domain claimed) and on-premises users (URL claimed).

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

> **Notes:**
>
> This feature is available for workspace and HTTPS-based stores only.
> For the Global App Configuration service to work, verify if your users can access the URL `https://discovery.cem.cloud.us`, `https://gacs-discovery.cloud.com`, and `https://gacs-config.cloud.com`.

Customer Experience Improvement Program (CEIP)

June 20, 2024

How to configure

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

Additional Information

Citrix handles your data in line with the terms in your contract. Citrix protects your data as specified in the Citrix Services Security Exhibit available on the Citrix Trust Center.

Citrix uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. You can either disable or block CEIP data. Review how Google handles data collected for Google Analytics.

> **Note:**
>
> No data is collected for the users in the European Union (EU), European Economic Area (EEA),

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Switzerland, and the United Kingdom (UK).

CEIP data to Citrix and Google Analytics

Starting from the 2203 version, end users can:

- decide whether to send the usage data to Citrix and Google Analytics or not
- block CEIP through GUI

Disabling CEIP

You can disable sending CEIP data to Citrix and Google Analytics. To do that, use one of the following methods:

- Disable CEIP using Google Admin Policy
- Disable CEIP using `configuration.js` file

> **Note:**
>
> When you disable CEIP for version 2203 and later, minimal information about the Citrix Workspace app version that is installed is uploaded. This minimal information is valuable to Citrix because it provides the distribution of different versions used by customers.

To disable CEIP using Google Admin Policy

> **Note:**
>
> Administrator-level credentials are required to do this procedure.

1. Log on to the Google Admin Console.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the code snippet shown after Step 4 to the `policy.txt` file under the **engine_settings** key.
4. Click **Save**.

For more information on google policy, see Knowledge Center article CTX141844.

For Version 1907 and earlier, set the enabled attribute under **ceip** to **false**.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For Version 1908 and later, set the enabled attribute under **analytics** to **false**. However, the **analytics** key is backward compatible with the **ceip** key.

```
"analytics":{

    "enabled":false,
 }

<!--NeedCopy-->
```

To disable CEIP using configuration.js

The `configuration.js` file is in the **ChromeApp root** folder. Edit this file to configure Citrix Workspace app for ChromeOS.

> **Notes:**
>
> - Citrix recommends that you back up the `configuration.js` file before making changes.
> - Citrix recommends editing the `configuration.js` file, only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the `configuration.js` file.

For Version 1907 and earlier, set the enabled attribute under **ceip** to **false** in the `configuration.js` file.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

For Version 1908 and later, set the enabled attribute under **analytics** to **false** in the `configuration.js` file.

```
"analytics":{

    "enabled":false,
 }


<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Blocking CEIP

For Version 2007 and later, administrators are allowed to block CEIP through the `configuration.js` file and Google Admin Policy.

For Version 2203 and later, end users are allowed to block CEIP through the GUI.

The blocking CEIP configuration takes precedence over the configuration made through the GUI and Google Admin Policy, and CEIP data isn't sent to Citrix.

To block CEIP using Google Admin Policy

> **Note:**
>
> Administrator-level credentials are required to do this procedure.

1. Log on to the Google Admin Console.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the code snippet shown after Step 4 to the `policy.txt` file under the **engine_settings** key.
4. Click **Save**.

```
"analytics":{

    "connectionEnabled":false,
                }

<!--NeedCopy-->
```

To block CEIP using configuration.js

1. Open the `configuration.js` file.
2. Add the **connectionEnabled** attribute, and set the attribute to **false**:

```
"analytics":{

"connectionEnabled":false,
             }


<!--NeedCopy-->
```

To block CEIP using GUI

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Only the end user can modify the CEIP settings using the GUI.

1. Open Citrix Workspace app for ChromeOS.
2. Select **Settings** > **General**.
3. Clear **Help improve Citrix Workspace by sending anonymous usage statistics** option.

   Relaunch Citrix Workspace app for the changes to take effect.

Specific CEIP data

The specific CEIP data elements collected by Google Analytics are:

Citrix Workspace app version	Session mode (Kiosk, Public/General)	Session type (desktop/application)	XenDesktop information (Delivery Controller and VDA versions)
Launch type (SDK/I-CAFile/FTA/Store and so on)	Time zone of the session	Language of the session	Client keyboard layout
Network socket type (HTTPS/HTTP)	Feature usage (clipboard, file transfer, app switcher, printing, USB, smart card, and so on)	Device pixel ratio	Secure ICA (used / not used)
Asset ID of enrolled enterprise Chromebooks	Reconnection timeout (if!= 180)	Multi-Monitor	Global App Configuration Service

Clipboard

April 12, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Support for copying image clips

Using the standard keyboard shortcuts, you can copy and paste image clips between your local device and your virtual desktop and app sessions. You can use the standard keyboard shortcuts for copying and pasting. As an example, you can use apps such as Microsoft Word, Microsoft Paint, and Adobe Photoshop. Previously, this functionality was available only for text.

> **Note:**
>
> - Due to network bandwidth constraints, sessions might become unresponsive when you try to copy and paste an image clip larger than 2 MB.
> - You can select and press Ctrl + C and Ctrl + V to copy and paste. The right-click functionality to copy or paste is also supported.
> - We've tested this feature with BMP, PNG, JPEG, and GIF formats.

Configuring the clipboard

You can copy HTML content and retain formatting when copying a link in Chrome. An <img> tag is added in HTML format, which allows you to copy images and text. This feature is richer than plain text.

To enable this feature, add the following registry entry to the VDA:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\Additional Formats\HTML Format
"**Name"="HTML Format**"

> **Warning**
>
> Using the Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix can't guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

The clipboard feature has resolved many issues. For additional information, see Knowledge Center article CTX086028.

Support for HTML data format

Starting with the version 2207, you can use HTML format for clipboard operations between the virtual desktop and the endpoint device. When you copy and paste the HTML data, the source content format is copied. When you paste the data, the destination content carries the formatting as well. In addition, HTML format provides a better look and feel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For more information on how to set the policies, see Client clipboard write allowed formats in the Citrix Virtual Apps and Desktops documentation.

Clipboard supports HTML format

You can use HTML format for clipboard operations between the virtual desktop and the endpoint device. When you copy the HTML data, the source content format is copied, and when you paste the data, the destination content carries the formatting. In addition, HTML format provides a better look and feel.

For more information on how to set the policies, see Client clipboard write allowed formats in the Citrix Virtual Apps and Desktops documentation.

File handling

April 12, 2024

File transfer

Citrix Workspace app for ChromeOS provides secure file transfer between a user device and a session. The session can be of the type Citrix Virtual Apps and Desktops and Citrix DaaS session. This feature uses a file transfer virtual channel instead of client drive mapping.

By default, users can:

- Upload files from a local download folder or attached peripheral
- Seamlessly access data from their Citrix Virtual Apps and Desktops and Citrix DaaS sessions.
- Download files from their Citrix Virtual Apps and Desktops and Citrix DaaS sessions.
- You can download files to a local folder or a peripheral on their user device.

Administrators can configure file transfer, uploads, and downloads using policies in Citrix Studio.

> **Prerequisites**

- XenApp or XenDesktop 7.6 or later, with:
  - Hotfix ICATS760WX64022.msp on server OS VDAs (Windows 2008 R2 or Windows 2012 R2)
  - Hotfix ICAWS760WX86022.msp or ICAWS760WX64022.msp on client OS VDAs (Windows 7 or Windows 8.1)
- To change file transfer policies: Group Policy Management (GPM) hotfix GPMx240WX64002.msi or GPMx240WX86002.msi on machines running Citrix Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feature limitations:

- A user can upload or download a maximum of 10 files at a time.
- Maximum file size:
  - For uploads: 2147483647 bytes (2 GB)
  - For downloads: 262144000 bytes (250 MB)
- If either the **Upload file to Desktop** or the **Download file from Desktop** policy is set to **Disabled**, the toolbar still displays both the Upload and the Download icons. However, the functionality is based on the policy setting. If both policies are set to **Disabled**, the Upload and Download icons aren't displayed in the toolbar.

Configure file transfer policies

To configure file transfer using a Citrix Studio policy

By default, file transfer is enabled.

Use Citrix Studio to change the following policies, located under **User Setting**> **ICA** > **File Redirection**.

Citrix Studio policy	Description
Allow file transfer between desktop and client	To enable or disable the file transfer feature
Upload file to Desktop	To enable or disable file upload in the session. Requires the "allow file transfer between desktop and client"policy to be set to true.
Download file from Desktop	To enable or disable file download from the session. Requires the "allow file transfer between desktop and client"policy to be set to true.

To configure file transfer using configuration.js file

The **configuration.js** file is in the **ChromeApp root** folder. Edit this file directly to modify Citrix Workspace app to suit your requirement.

Notes:

- Citrix recommends that you back up the **configuration.js** file before making changes.
- Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Administrator-level credentials are required to edit the **configuration.js** file. After editing the file, repackage the app to make more modifications to the toolbar elements.

To change the file transfer configuration using the configuration.js file

Open the **configuration.js** file and configure the settings as follows:

File Transfer Client Settings	Description
AllowUpload	To enable or disable upload from client-side. By default set to true (enabled).
AllowDownload	To enable or disable download from the client-side. By default set to true (enabled).
MaxUploadSize	To set the maximum size of the file that can be uploaded in bytes. By default set to 2147483648 bytes (2 GB)
MaxDownloadSize	To set the maximum size of the file that can be downloaded in bytes. By default set to 2147483648 bytes (2 GB).

Following are the behavior cases when the policies set in Citrix Studio and the client are different.

Citrix Studio Policy Upload / Download	Client- side setting Upload / Download	Resulting Behavior
DISABLED	ENABLED	DISABLED
DISABLED	DISABLED	DISABLED
ENABLED	DISABLED	DISABLED
ENABLED	ENABLED	ENABLED

Note:

When there's a conflicting value set for **Maximum File Size upload or download** in the registry and in the client-side settings, the minimum size value among the two is applied.

To configure file transfer using the Google admin policy

By default, the file transfer feature is enabled.

To disable it, set the enabled attribute to false.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "features": {

                           "filetransfer" : {

                                   "allowupload": true,
                                   "allowdownload": true,
                                   "maxuploadsize": 2147483647,
                                   "maxdownloadsize": 2147483647
                               }

                        }

                    }

                }

         }

     }

 }


<!--NeedCopy-->
```

List of file transfer options with their descriptions:

- `allowupload`: Allows you to upload files from device to remote session.
- `allowdownload`: Allows you to download files from device to remote session.
- `maxuploadsize`: It is the maximum file size, in bytes that can be uploaded. By default, it is set to 2,147,483,648 bytes (2 GB).
- `maxdownloadsize`: It is the maximum file size, in bytes that can be downloaded. By default, it is set to 2,147,483,648 bytes (2 GB).

Client Drive Mapping

Starting with the 2307 version, the Client Drive Mapping (CDM) feature supports folder mapping on the local ChromeOS device so they're accessible from within a session. You can map any folder from the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ChromeOS device, for example, folders from Downloads, Google Drive, and USB drives, if the folder doesn't contain system files.

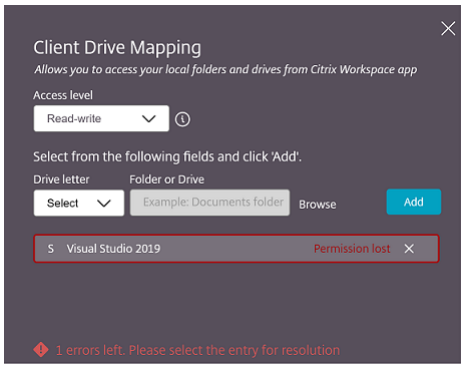
The end user can do the following operations:

- Copy files and folders to the mapped drive from the session and the other way around.
- View the list of files and folders in the mapped drive.
- Open, read, and modify the file contents in the mapped drive.
- View the file properties (modified time and file size only) in the mapped drive.

This feature provides the advantage of accessing both virtual desktop drives and local machine drives together in the file explorer within the HDX session.

Known limitations

- You can't rename files and folders inside the mapped drive.
- Mappings have the name of the folder and not the full path.
- If your local folder has hidden files, and you mapped the same folder, the hidden files are visible inside the session in the mapped drive.
- You can't change the file property to read-only access in the mapped drive.
- CDM isn't supported when sessions are opened in Embed mode using HDX SDK.
- When you map a folder from a removable device and remove the device during an active session, you can't use that mapped drive inside the session. To remove the mappings manually, click **X** mark against the particular mapping.



Configure CDM

You can configure the CDM feature in one of the following ways:

- Configuration.js
- Google Admin Policy

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - As a prerequisite, an administrator must enable the **Client drive redirection** policy on the Delivery Controller (DDC). For more information, see Client Drive Redirection in the Citrix Virtual Apps and Desktops documentation.

Configuration.js

To disable CDM support using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit the file to configure the CDM feature.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set the value of **clientDriveMapping** to **false**.

   The following is an example of JSON data:

```
'features': {

    'clientDriveMapping': {

       'enabled': false,
       'availableAccessLevels': ["Read-write","Read-only,No-access
          "],
       'accessLevel': "Read-write"
     }

 }

<!--NeedCopy-->
```

4. Save the changes.

Google admin policy

For managed devices and users, administrators can disable the CDM feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings**.

> **Note:**
>
> You can apply this configuration on the following as well:
>
> - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
> - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

The following is an example of JSON data:

```
{

"settings": {

    "Value": {

        "settings_version": "2.0",
        "engine_settings": {

            "features": {

                "clientDriveMapping": {

                "availableAccessLevels": ["Read-write", "Read-only
                   ","No-access"],
                "accessLevel": "Read-write"
                                }

                        }

                    }

                }

            }

 }

<!--NeedCopy-->
```

4. Save the changes.

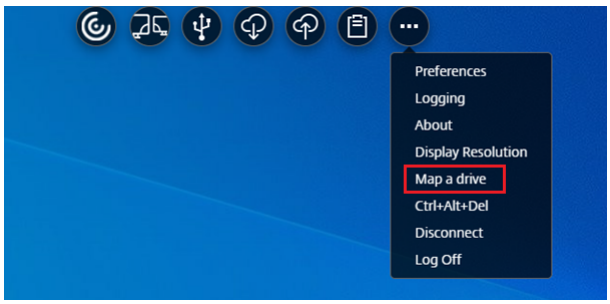
Access level You can set the folder or drive access levels when the feature is enabled. For example, if an administrator sets **availableAccessLevels** as [**"No-Access", "Read-only"**], the end user can view the **Read-Only Access** and **No-Access** options in the drop-down list.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

How to use the CDM feature

On desktop sessions:

1. Navigate to the **Toolbar** > **more (...)** > **Map a drive**.

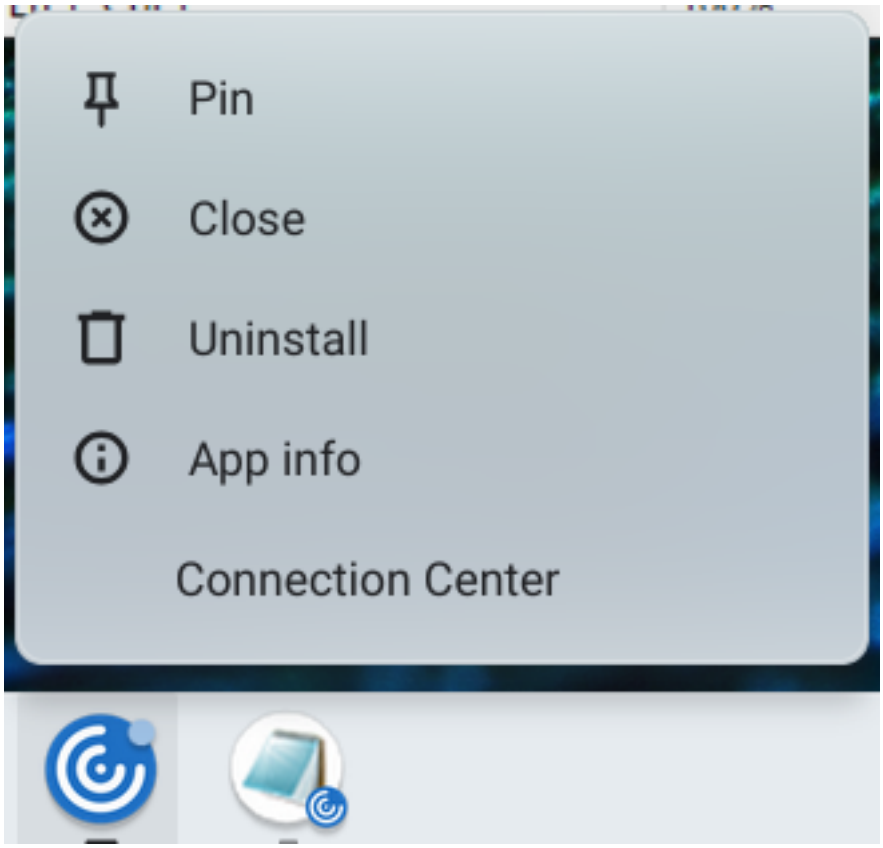


   The CDM dialog appears.

2. See How to use CDM UI section for the next steps.

On app and desktop sessions:

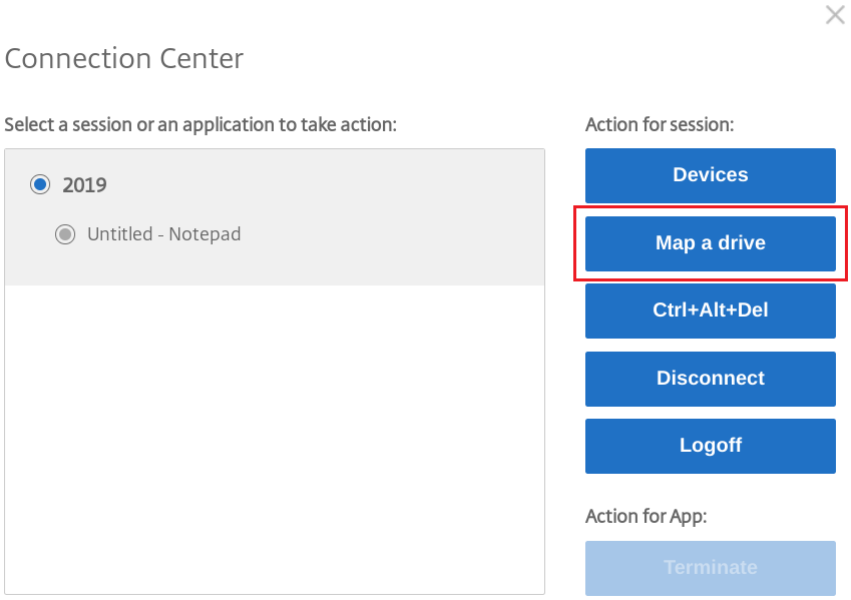
1. From the Chrome shelf, right-click the Citrix Workspace app icon and select **Connection Center**



   The **Connection Center** screen appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Select the session and the app. Click **Map a drive**.

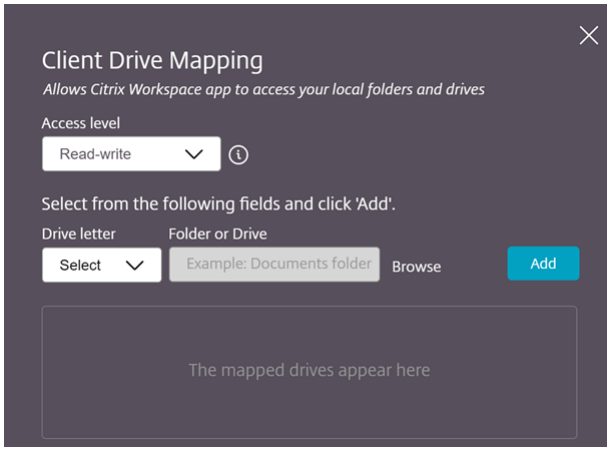


The CDM dialog appears.

3. See How to use CDM UI section for the next steps.

How to use CDM UI

1. Select the **Access level** for the folder or the drive. The drop-down list option that you see depends on the access level set by your organization's IT administrator for your profile.



2. Select a **Drive letter** and click **Browse** to navigate to your folder or drive in your Chromebook.
3. Click **Add**.
4. Disconnect and reconnect the session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The session displays the drive letter that is mapped inside the session.

File type association

April 23, 2024

Google Drive access

With Google drive support, users can open, edit, and save Windows file types from a Chrome device that runs Citrix Workspace. While running a Google Chrome device, users can seamlessly use existing Windows-based applications (for example, Microsoft Word) and access the files residing on Google Drive.

If a user opens a file in Google Drive, edits it, and saves it Drive, the same file can be accessed through the Citrix Virtual Apps hosted application. For example, a `.docx` file attachment downloaded from Gmail. The file can be viewed, edited, and saved to Google Drive.

How to configure

Prerequisites

To enable Google Drive access, you must install the Citrix File Access component (FileAccess.exe) on your VDA and enable file type associations in Citrix Studio. You can download Citrix File Access from the Citrix downloads page.

To enable Google Drive access from Citrix Workspace

1. Install `FileAccess.exe` on each Citrix Virtual Apps or Citrix Virtual Apps and Desktops and Citrix DaaS VDA.
2. Configure the appropriate FTAs for the published applications in Citrix Studio.
3. Enable cookies and trust the sites `https://accounts.google.com` and <`https://ssl.gstatic.com`>. You can do it on the Citrix Virtual Apps or Citrix Virtual Apps and Desktops and Citrix DaaS VDA.

Only files from Google Drive can be opened using Citrix Workspace. To open a file from Google Drive, right-click and open the file using Citrix Workspace.

Citrix recommends that you associate one file type with only one published application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Proxy connection support

The Citrix Workspace app for ChromeOS supports opening documents from a Google drive using published applications through the unauthenticated proxy servers.

How to configure:

To enable the proxy connection, configure the proxy setting in the internet options.

To disable Google Drive access from Citrix Workspace

In the manifest.json file, replace:

```
"file_handlers" : {

      "all-file-types" : {

         "extensions" : [
            "*"
         ]
       }

    }
 ,
<!--NeedCopy-->
```

with:

```
    "file_handlers" : {

          "cr-file-type" : {

             "extensions" : [
                "cr",
               "ica"
             ]
           }

        }
 ,
<!--NeedCopy-->
```

Graphics

May 14, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Graphics and H.264

How to configure

To configure graphics and H.264 protocol support, use the Google admin policy by including the following. By default, H.264 protocol support is enabled. To disable it, set the enabled attribute to false.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                       "features": {

                           "graphics": {

                               "jpegSupport": true,
                               "h264Support" : {

                                    "enabled": true,
                                    "losslessOverlays": true,
                                    "dirtyRegions": true,
                                    "yuv444Support": false
                                }

                            }

                        }

                    }

                }

         }

    }

 }


<!--NeedCopy-->
```

List of graphics options with their descriptions:

- “jpegSupport”: JPEG capability in Graphics (Thinwire).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- “h264Support”: H.264 protocol support.
- “enabled”: H.264 support capability in Thinwire.
- “losslessOverlays”: Loss-less overlay capability in Thinwire.
- “dirtyRegions”: Dirty regions capability in Thinwire.
- “yuv444Support”: Yuv444 support capability in Thinwire.

> **Note:**
>
> We recommend setting the **Legacy Graphics Mode** to **Disabled**.

Feature limitations

- Citrix Workspace app for ChromeOS does not support full-screen H.264 graphics mode for multiple monitors.
- When you start a desktop session, and open an app to enter text, when you start entering the text disappears and reappears. You can observe that the text flickers. The issue occurs when you use full-screen H.264 mode.
- In a multi-monitor setup, when you open a published app, a blank screen appears instead of the app screen. The issue occurs when you use full-screen H.264 mode.

Selective H.264

How to configure

Configuring Selective H.264 in StoreFront using the web.config file To change the Selective H.264 configuration using the web.config file:

1. Open the web.config file for Citrix Receiver for Web site.
   This file is in the C:\inetpub\wwwroot\Citrix\<Storename> Web folder, where *Storename* is the name that is specified for the store when it was created.
2. Locate the **chromeAppPreferences** field and set its value with the configuration as a JSON string; for example:
   chromeAppPreferences='{“graphics”:{“selectiveH264”:false}}

Configuring Selective H.264 using the configuration.js file The **configuration.js** file is in the **ChromeApp root** folder. Edit this file to modify Citrix Workspace app according to your requirement.

By default, selective H.264 is set to true.

To disable the Selective H.264 configuration using the configuration.js file:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Open the configuration.js file and set the selectiveH264 attribute to **false**.

```
'graphics': {
        'selectiveH264': false
}
```

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

Other (H.264)

How to configure

To configure H.264, use the Google admin policy by including the following. By default, the option under the **other** section is disabled. To enable it, set the disabled attribute h264nonworker to true.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "other": {

                        "h264nonworker" : false
                         }

                 }

          }

     }

 }


<!--NeedCopy-->
```

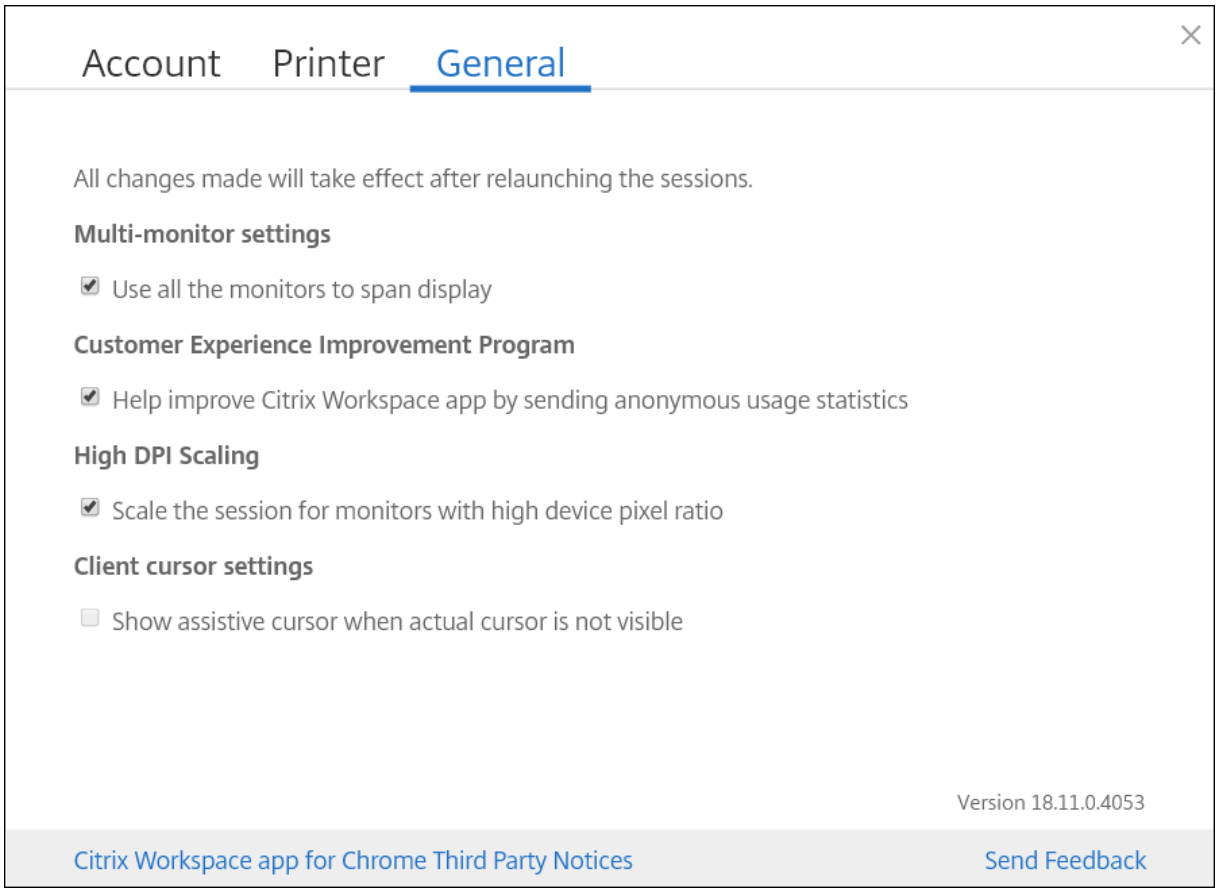
List of options with their descriptions:

- “h264nonworker”: Enable the option to decode an H.264 frame in the main thread.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Assistive cursor

When a cursor isn't visible inside a desktop session, you can enable an assistive cursor. Requires a session restart.



How to configure

The assistive cursor feature is disabled by default. To enable the assistive cursor feature, use the Google admin policy by including the following.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "ui": {

                    "assistiveCursor": true
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                        }

                    }

                }

            }

 }


<!--NeedCopy-->
```

Note:

- If an administrator enables the assistive cursor as described earlier, the corresponding checkbox on the client-side setting is selected by default. To disable the feature, clear the checkbox.
- If an administrator disables the assistive cursor as described earlier, the checkbox is cleared and the feature is disabled.

DPI scaling

About this feature

Citrix Workspace app for ChromeOS allows the operating system to control the resolution of app and desktop sessions and supports DPI client scaling for app sessions on a single monitor.

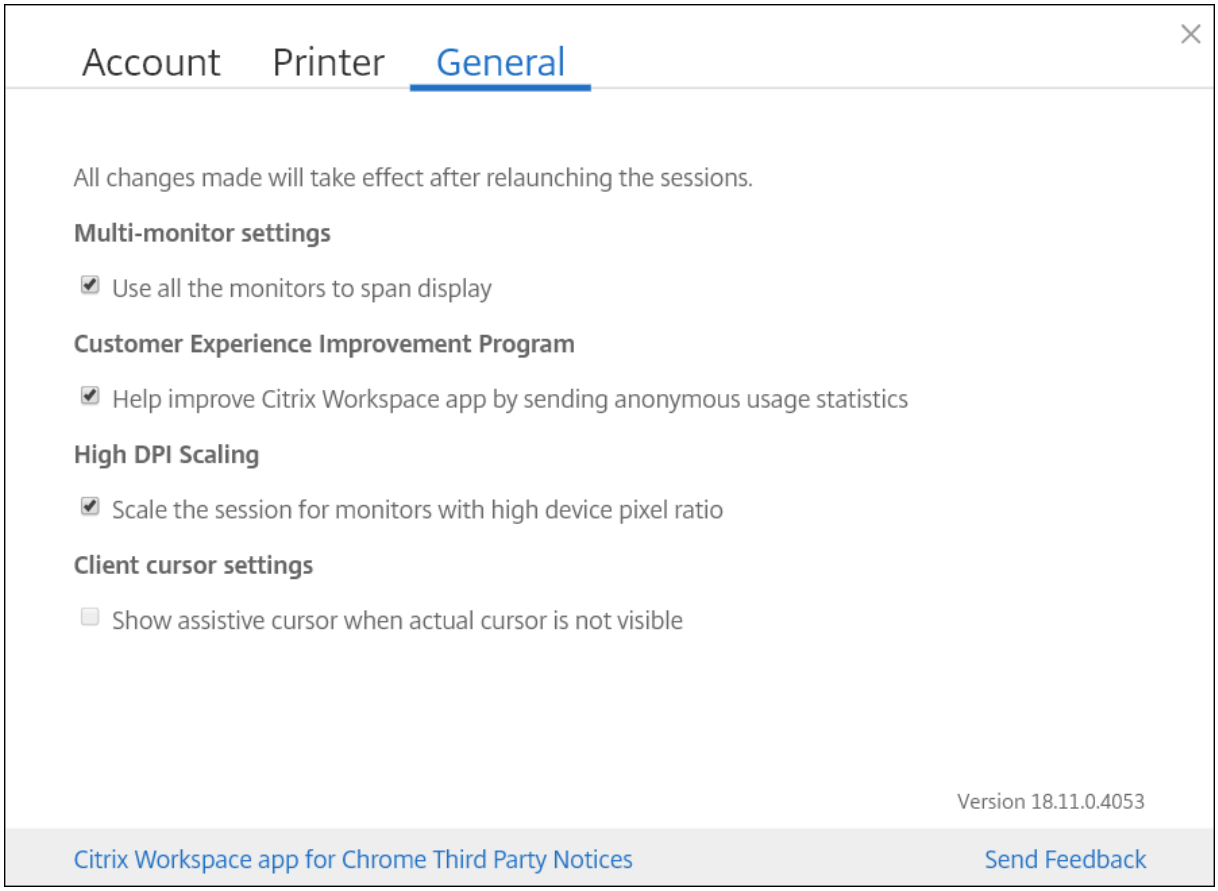
Citrix Workspace app for ChromeOS supports DPI scaling by allowing you to set the VDA resolution on monitors that have a high pixel ratio.

The **High DPI Scaling** feature is disabled by default for app and desktop sessions. For better resolution on high DPI enabled devices, go to **Settings** and select the **High DPI Scaling** checkbox.

How to configure

You can configure the **High DPI Scaling** setting using the Google Admin policy only.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The DPI scaling feature **Scale the session for monitors with high device pixel ratio** is enabled by default.

To set the resolution for desktop sessions, go to the session toolbar. Select **Preferences** > **Display Resolution** > **Use device pixel ratio** for the correct resolution to be set on the VDA. When the resolution is set properly on the VDA, blurry text becomes crisper.

To enable or disable the feature, edit the **Google Admin Console** policy and set the value of **scaleToDPI** to **true** or **false**.

For example, to disable the feature, set the **scaleToDPI** property to **false**.

```
{

    "settings": {

                "Value": {

                        "settings_version": "1.0",
                              "engine_settings": {

       "features" : {

       "graphics" : {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
13
14                  "dpiSetting": {
15
16                                    "scaleToDPI": false
17                                     }
18
19                                  }
20
21                              }
22
23                          }
24
25                      }
26
27                  }
28
29              }
30
31
32
33  <!--NeedCopy-->
```

Keyboard

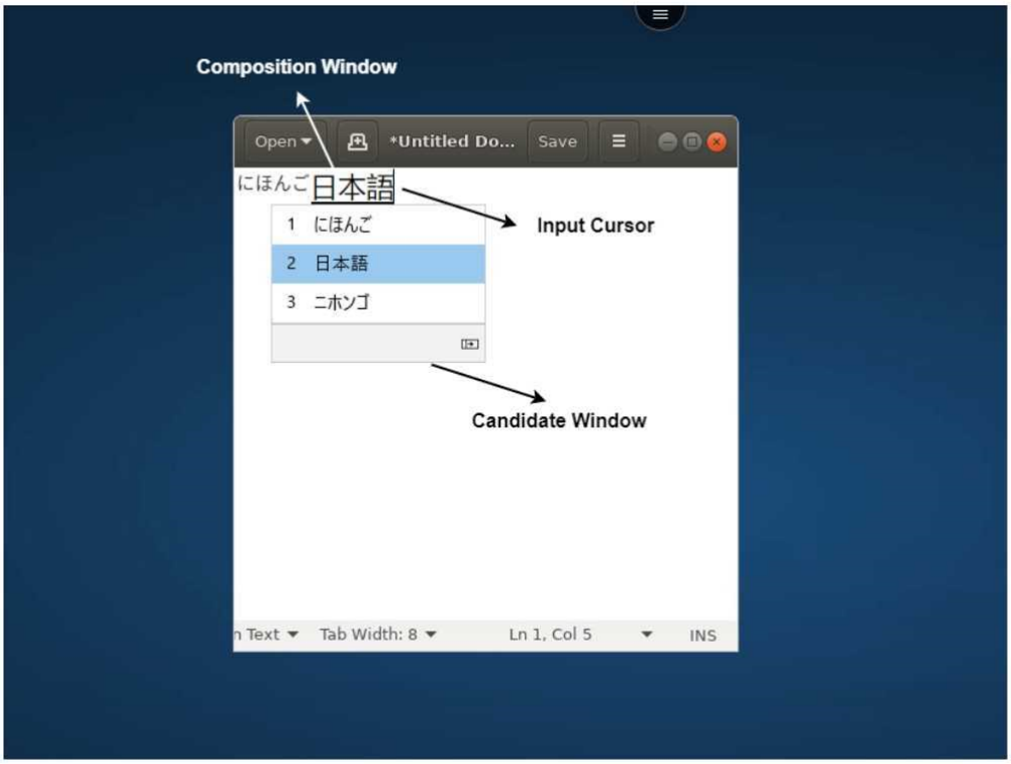
April 23, 2024

Generic client IME for East Asian languages

The Generic Client Input Method Editor (IME) feature enhances the input and display experience with Chinese, Japanese, and Korean (CJK) language characters. This feature allows you to compose CJK characters at the cursor position when you are in a session. The feature is available for the Windows VDA and Linux VDA environments.

Generally, IME displays user interface (UI) components such as a candidate window and a composition window. The composition window includes the composition characters and composition UI elements. For example, underline and background color. The candidate window displays the candidate list.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The composition window enables you to choose between the confirmed characters and the composing characters. The composition window and the candidate window move with the input cursor. As a result, the feature gives an enhanced input of characters at the cursor location in the composition window. In addition, it gives an improved display in the composition and the candidate window.

Prerequisites:

- For Linux VDA, enable **Client keyboard layout sync and IME improvement** policy.
- For Windows VDA, enable **Unicode Keyboard Layout Mapping**, **Client Keyboard Layout Sync**, and **IME Improvement policies**.
- Use Citrix Linux VDA version 2012 and later. For Citrix Windows VDA, all the currently available Windows VDA versions support the generic client IME feature.
- The browser language must be Japanese, Chinese (Simplified), Chinese (Traditional), or Korean.
- Use Google Chrome or Mozilla Firefox.

Feature limitations:

- Character composition is unsuccessful within the Microsoft Excel cell. The issue happens when the cell is selected using a mouse click. [RFHTMCRM-6086]
- Generic client IME is now supported when you use an extended screen. However, for multi-monitor sessions that are not yet supported, you can use **Server IME** instead.

  To enable the **Server IME**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Change the VDA or the server keyboard language to Chinese, Japanese or Korean (CJK) as wished.
2. Change the Chromebook keyboard language to English.

Known Issue in the feature:

- When Citrix IME isn't added to the VDA desktop session, you might be unable to type the IME characters. The issue happens intermittently on VDA versions 2202 and earlier. [HDX-36748]

Configuration:

Starting with version 2209, the Generic Client IME feature is enabled by default.

As an administrator, you can disable the feature using the **configuration.js** file on the StoreFront server usually at ProgramFiles%\Citrix\Receiver StoreFront\HTML5Client. To disable the feature, navigate to **appPrefs** > **chromeApp** > **feature** > **ime** > set **genericIME** to **false**.

For example,

```
    "appPrefs":{

        "chromeApp":{

            "features" : {

                    "ime" : {

                    "genericIME": false
                }

       }

     }

     }
<!--NeedCopy-->
```

- As an administrator, you can disable the feature using the Google Admin Policy console by setting **genericIME** to **false**.
  For example,

```
    {

    "settings": {

    "Value": {

      "settings_version": "1.0",
      "engine_settings": {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        "features": {

          "ime": {

            "genericIME": false
           }

         }

       }

      }

 }

<!--NeedCopy-->
```

Shortcuts

You can use standard Windows shortcuts to copy data that includes text tables, and images, between hosted applications. The hosted applications can be:

- within the same session
- within different sessions

Only Unicode plain text can be copied and pasted between hosted applications and the local clipboard on the device.

Users can use standard Windows keyboard shortcuts with Citrix Workspace app for ChromeOS because these shortcuts are passed from ChromeOS to hosted applications. Similarly, shortcuts specific to particular applications can also be used, provided they do not conflict with any ChromeOS shortcuts.

However, the **Windows** key must also be pressed for function keys to be recognized. So, an external keyboard is required. For more information about using Windows keyboards with ChromeOS, see https://support.google.com/chromebook/answer/1047364. Citrix-specific shortcuts, such as those for switching between sessions and windows, can't be used with Citrix Workspace app for ChromeOS.

Excel shortcuts

How to configure

Keyboard shortcuts are configured with the **sendAllKeys** attribute.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For all Excel shortcuts to work, configure as follows: **HTML5_CONFIG > features > sendAllKeys**

The **sendAllKeys** attribute defaults to **true.** To change the default, open the **configuration.js** file, add the **sendAllKeys** attribute, and set the attribute to **false.**

For more information, see How to push policies through the Google Admin console.

Support for Microsoft Windows logo key and shortcut keys

> **Note:**
>
> - In Chromebooks, use the Search key to map the Microsoft Windows logo key.

Starting with the version 2108 release, we're supporting the Microsoft Windows logo key and shortcut keys on your Citrix Workspace app for ChromeOS sessions.

We've added support for the following key combinations:

- Windows + R
- Windows + D
- Windows + E
- Windows + M
- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + Number
- Windows + X
- Windows + K

Automatic display of virtual keyboard

Starting with the 2211 version, a virtual keyboard automatically appears when you place the cursor on an editable field. This feature enhances the user experience on touchscreen devices, unlike the previous behavior where you had to click the keyboard icon to view the virtual keyboard.

Scan code input mode

Citrix Workspace app allows you to use external physical keyboards to collaborate with the server-side keyboard layout on the VDA. When administrators enable Scan code mode, the end user might find themselves using the keyboard layout of the server instead of the client.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This feature enhances the user experience particularly when using an East-Asian language physical keyboard.

> **Notes:**
>
> - By default, this feature policy is disabled.
> - On touch devices, when Scan code is enabled, the on-screen software keyboard doesn't work from the Citrix Workspace app.

Configuration

You can configure the Scancode input method in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To enable the Scan code support feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.
2. Edit the file and set the value **scancode** to **true**.

   The following is an example of JSON data:

```
"features" : {

        "ime": {

           "scancode": true,
         }

 }

<!--NeedCopy-->
```

3. Save the changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Google Admin Policy For managed devices and users, administrators can enable the Scan code support feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key.

   > **Note:**
   >
   > You can apply this configuration on the following as well:
   >
   > - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   > - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

   ```
   "features" :
   {

       "ime": {

                       "scancode": true
                   }

    }

   <!--NeedCopy-->
   ```

4. Save the changes.

Custom keyboard mapping

Starting with the 2309 version, end users can use Windows-specific shortcuts and key combinations when the VDA is a Windows OS machine, and the native input device is a ChromeOS keyboard. You can now map **Ctrl** and **Alt** keys using custom mapping. The user can select the right or left Control (Ctrl) key to act as an Alt key.

> **Notes:**
>
> - The mapping is possible in full screen mode only.
> - After you save the setting, the mapping affects all sessions.
> - The feature is enabled by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration

You can configure the custom keyboard mapping in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.
2. Edit the file and set the value **CustomKeyboardMapping** to **false**.

   The following is an example of JSON data:

```
"features" : {

        "ime": {

           "CustomKeyboardMapping": false,
         }

 }

<!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy For managed devices and users, administrators can enable the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key.

   > **Notes:**
   >
   > You can apply this configuration on the following as well:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
> - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

The following is an example of JSON data:

```
"features" :
{

    "ime": {

                "CustomKeyboardMapping": false
            }

 }

<!--NeedCopy-->
```

4. Save the changes.

For more information on how to use the feature, see the Help documentation article.

System shortcuts to VDA in full screen mode

Starting with the 2309 version, Citrix Workspace app on ChromeOS devices support passing system shortcuts to the VDA (remote desktop session) in full screen mode. However, it doesn't take effect on the client OS.

Previously, these combinations worked locally. Now, when the feature is enabled and in full screen mode, these combinations are sent to the VDA and yet doesn't take effect locally. For example, a **Refresh** key is a system key on the Chromebook, and the combination of **Ctrl+Shift+Refresh** is a system shortcut on ChromeOS to rotate screen. However, the Windows VDA takes no action because there's no such shortcut in the Windows OS.

Another example, `Alt`+[is used to dock a ChromeOS window on the left, but the same shortcut doesn't take any effect on the Windows VDA. Some applications might use such shortcuts for a specific function for example, `Alt`+[is used by some Barcode Scanner as a prefix.

> **Note:**
>
> - This feature is enabled by default.

Following are the key combinations:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Shortcut key combination	Action on ChromeOS
Action on ChromeOS	For signing out
Ctrl+Shift+Refresh	Rotate the screen 90 degrees
Ctrl+Shift+L	For locking Chromebook
Alt+[	Dock a window on the left
Alt+]	Dock a window on the right, keys to side dock, snap, and restore windows.
Alt+”-“	Minimize the window
Alt+”+”	Maximize the window

> **Note:**
>
> - These system shortcuts might not have the same actions in the VDA, as these key combinations are ChromeOS system shortcuts.

Configuration

You can configure the feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.
2. Edit the file and set the value **sendSysShortcutForFullscreen** to **false**.

   The following is an example of JSON data:

```
"features" : {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3           "ime": {
4
5              "sendSysShortcutForFullscreen": false,
6            }
7
8    }
9
10  <!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy For managed devices and users, administrators can disable the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key.

   > **Notes:**
   >
   > You can apply this configuration on the following as well:
   >
   > - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   > - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

```
1  "features" :
2  {
3
4      "ime": {
5
6                  "sendSysShortcutForFullscreen": false
7                }
8
9    }
10
11  <!--NeedCopy-->
```

4. Save the changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Licensing

April 23, 2024

Asset ID

About this feature

Citrix Workspace app uses an Asset ID that administrators set through the Google Admin Console as a client name for sessions that are launched from enrolled Chromebooks.

How to configure

By default, Citrix Workspace app continues to generate a unique client ID for enrolled Chromebooks, which is similar to earlier versions. To use this feature, you must set a policy for Citrix Workspace app.

The data value that you enter can't have more than 15 characters. Values longer than 15 characters are truncated to 15 characters.

Configuring Asset ID

1. Log on to the Google Admin Console.
2. Go to `Device Management` > `Chrome` > `Devices Console` and add `Asset ID` for the device.
3. Edit the `Google Admin Console` policy and set the value of `useAssetID` to **`true`**. By default, the `useAssetID` is set to **`false`**.

```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "uniqueID": {

      "useAssetID": true
                  }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
15                }
16
17            }
18
19        }
20
21    }
22
23
24  <!--NeedCopy-->
```

Feature limitations:

- You must have a Google Admin policy that can be pushed. Otherwise, the current method of generating a unique client ID for managed Chromebooks remains in use.
- Do not enter a value more than 15 characters. Values longer than 15 characters are truncated to 15 characters.

Unique ID and Asset ID

A unique ID is applied as a prefix to the client name.

Citrix Workspace app uses an asset ID that administrators set through the **Google Admin** console as a client name for the sessions launched from enrolled Chromebooks.

How to configure

To configure an asset ID using the GUI, go to **Device Management** > **Chrome** > **Devices Console**, and add the **Asset ID** for the device.

To configure an asset ID and a unique ID manually, use the Google admin policy by including the following:

```
1  {
2
3      "settings": {
4
5          "Value": {
6
7              "settings_version": "1.0",
8                  "engine_settings": {
9
10                         "uniqueID" : {
11
12                                 "prefixKey" : "CR-",
13                                 "restrictNameLength" : true,
14                                 "useAssetID": false
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
15                                              }
16
17                                            }
18
19                }
20
21            }
22
23    }
24
25
26  <!--NeedCopy-->
```

List of uniqueID options and their descriptions:

- “prefixKey”: The prefix to be used before the client name. The default value is CR.
- “restrictNameLength”: Enables or disables the name length of the prefixKey.
- “useAssetID”: Asset ID that is set as a client name for sessions that are launched from enrolled Chromebooks.

Feature limitations:

- You must have a Google admin policy that can be pushed. Otherwise, the current method of generating a unique client ID for managed Chromebooks remains in use.
- Do not enter a value that has more than 15 characters. Values longer than 15 characters are truncated to 15 characters.

Multimedia

April 23, 2024

Audio

You can use a USB headset within a session to speak and to listen. You can also use buttons on the USB headset (such as mute and skip). The user experience is enriched by providing smooth audio output.

Adaptive audio

With Adaptive audio, you don’t need to configure the audio quality policies on the VDA. Adaptive audio optimizes settings for your environment. It replaces legacy audio compression formats to provide an excellent user experience.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For more information, see Adaptive Audio in the Citrix Virtual Apps and Desktops documentation.

Feature attributes

There are two feature attributes:

- **EnableAdaptiveAudio:** Set the value to true to enable the adaptive audio feature. Set the value to false to disable the feature.
- **EnableStereoRecording:** Stereo recording is an optional feature. By default, this feature is disabled. Set the attribute **EnableStereoRecording** value to **true** to enable stereo recording or set the value to **false** to disable the feature. This feature can be supported only when the adaptive audio feature is enabled. When the **EnableStereoRecording** attribute is set to true, the stereo recording is supported with echo cancellation disabled.

How to configure

You can configure the adaptive audio feature in the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js To configure adaptive audio using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit this file to configure the adaptive audio feature.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set the default value of **EnableAdaptiveAudio** to **true**. Set the default value of **EnableStereo-Recording** to **false**.

   The following is an example of JSON data:

```
"features" : {

    "audio" : {

    "EnableAdaptiveAudio": true
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6                }
7
8   }
9
10
11  "features" : {
12
13      "audio" : {
14
15          "EnableStereoRecording": false
16               }
17
18   }
19
20  <!--NeedCopy-->
```

4. Save the changes.

> **Note:**
>
> - To disable the feature, set the **EnableAdaptiveAudio** attribute to **false**.

Google admin policy On the on-premises deployment, administrators can enable the adaptive audio feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.

   The following is an example of JSON data:

```
1   "features" : {
2
3       "audio" : {
4
5           "EnableAdaptiveAudio": {
6
7               "type": "boolean" }
8
9                       }
10
11                  }
12
13
14  "features" : {
15
16      "audio" : {
17
18          "EnableStereoRecording": {
19
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            "type": "boolean" }

                 }

             }

<!--NeedCopy-->
```

4. Save the changes.

Plug and play audio device support

Previously, only a single audio playback and recording device was supported and displayed as **Citrix HDX Audio** irrespective of the real device name.

Starting with the 2301 version, we support multiple audio devices and redirect them to VDA. Now, when you redirect audio devices, you can view the real name of the audio device under the **Sound** settings > **Playback** and **Sound** settings > **Recording** on the VDA. The list of devices on the VDA is dynamically updated whenever an audio device is plugged in or removed.

> **Note:**
>
> By default, this feature is enabled.

Configuration

You can configure this feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js To disable plug and play audio device support using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit the file to configure the plug and play audio device support feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Set the value of **AudioRedirectionV4** to **false**. Following is an example of JSON data:

```
    "features" : {

        "audio" : {

          "AudioRedirectionV4": false
                }

         }

<!--NeedCopy-->
```

4. Save the changes.

Google admin policy On the on-premises deployment, administrators can disable the plug and play audio device feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **.txt** file under the **engine_settings** key.

   The following is an example of JSON data:

```
    "features" : {

        "audio" : {

          "AudioRedirectionV4": false
                }

         }

<!--NeedCopy-->
```

4. Save the changes.

Known Limitations

- On the VDA, the name of the built-in audio device is in English only. The issue occurs when you use ChromeOS-based devices. [RFHTMCRM-8667]

Webcam

Citrix Workspace app for ChromeOS provides an enhancement to webcam redirection functionality. H.264 hardware encoding for webcam input helps reduce CPU load and increases battery efficiency for

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Chromebook devices. These devices have encoders for H.264, which uses Intel functionality through the PPB_VideoEncoder API.

Citrix Workspace app for ChromeOS supports webcam redirection for both 32-bit and 64-bit applications.

Webcam redirection

Webcam redirection is available for both 32-bit and 64-bit applications. Support for webcam redirection with both 32-bit and 64-bit apps is limited to built-in webcams.

You can now use external webcams within Citrix Workspace app for ChromeOS virtual desktop and app sessions. The Citrix Workspace app detects newly connected external webcams and makes them available for use dynamically.

How to configure

Configure for webcam redirection for 64-bit as follows:

Configuring the webcam by using the configuration.js file and the Google Admin Console For Versions 2101 and later:

Configure webcam redirection using the following path: **HTML5_CONFIG > features > video**

> **Note:**
>
> We recommend that you use the **HTML5_CONFIG > features > video** path to configure webcam redirection. The other path continues to work for some time and will be removed in a future release.

Recommendations for webcam redirection

- Set the Citrix Delivery Controller Audio Quality policy to Low or Medium. When using low-powered Chromebooks, audio lags might occur if you do not set the Audio Quality policy.
- For the best performance, we recommend using high-end Chromebooks and low-latency networks with good bandwidth connections.
- Set the following registry key on a VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

  Name: OfferH264ToApp

  Type: REG_DWORD

  Value: 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This setting applies to the current user setting. For new users, set the registry key through the Windows Group Policy Object (GPO) Editor.

DISCLAIMER: Caution! Using the Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can't guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Microsoft Teams optimization

April 24, 2024

You can now use the following features of Microsoft Teams for virtual desktop and virtual app sessions:

- Optimized audio calls
- Optimized video calls
- Optimized screen sharing

It's supported only on VDA versions 1906 and later.

> **Notes:**
>
> - By default, screen sharing allows sharing of the entire screen. However, you can limit screen sharing to Citrix Workspace app content only. For more information, see Limit screen sharing of Citrix Workspace app content. To enable the screen sharing feature through the Google admin policy, see Microsoft Teams optimization settings.
> - To troubleshoot, and to change Microsoft Teams to optimized from unoptimized within your client session, see Troubleshooting for Microsoft Teams optimization.
> - During screen sharing using Microsoft Teams optimization, the red border around the shared window does not appear.
> - App sharing isn't supported.
> - Microsoft Teams optimization for audio calls, video calls, and screen sharing is generally available from release 2105.5 and later. We recommend that you update to the latest version of Citrix Workspace app for ChromeOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Video calls and screen sharing on external monitors

On your external monitor, you can now use the following features of Microsoft Teams during calls.

- Optimized video
- Optimized screen sharing

These features are available for Microsoft Teams calls within virtual desktops. They're also available for calls made through the Microsoft Teams virtual app, when you place the Microsoft Teams windows on an external monitor.

Notes (ChromeOS version 96 update)

- To avoid any impact of ChromeOS version 96 update on Microsoft Teams functioning, do the following before you update the ChromeOS:
- For users on a repackaged version of Citrix Workspace app, see Knowledge Center article CTX331648 and implement the steps.
- For all other users of Citrix Workspace app for ChromeOS, version 2110 and earlier, see Knowledge Center article CTX331653.

Microsoft Teams optimization settings

To enable screen sharing

To enable screen sharing using the Google admin policy, change the screen sharing value to **true** for **msTeamsOptimization** as follows.

For more information, see the article How to push policies through the Google Admin console.

```
{

  "settings": {

     "Value": {

       "settings_version": "1.0",
          "engine_settings": {

             "features":{

                "msTeamsOptimization":{

                "screenSharing" : true
                   }

                }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
18
19                }
20
21             }
22
23          }
24
25       }
26
27
28  <!--NeedCopy-->
```

To enable screen sharing for Bring your own device (BYOD) users (only for those using on-premises StoreFront):

Follow the steps in Using webconfig article and add the **chromeAppPreferences** value as follows:

For example:

```
1  chromeAppPreferences = {
2
3      "features":{
4
5          "msTeamsOptimization":{
6
7              "screenSharing":true
8               }
9
10              }
11
12              }
13
14 <!--NeedCopy-->
```

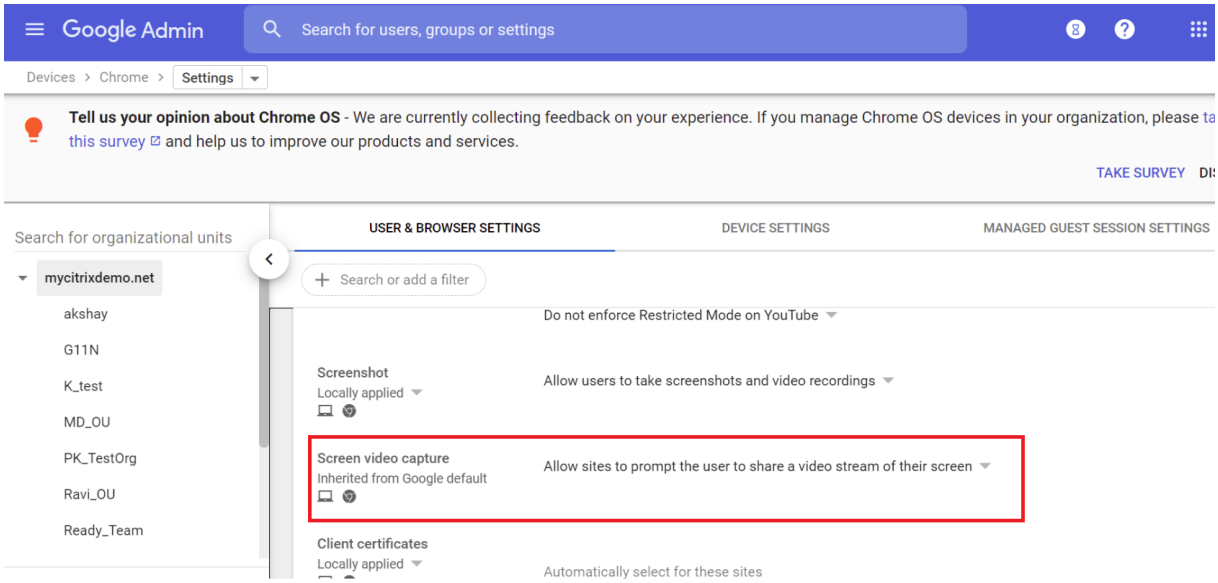
Settings in Google Admin Console

Ensure that the following settings are allowed in **Google Admin Console** for screen sharing optimization to work.

In **Google Admin Console**, under **Devices** > **Chrome** > **Settings**, select > **Allow sites to prompt the user to share a video stream of their screen** under **Screen Video Capture** for all three categories:

- **User & Browser Settings**
- **Device Settings**
- **Managed Guest Session Settings** (or an appropriate category).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Limit screen sharing of Citrix Workspace app content

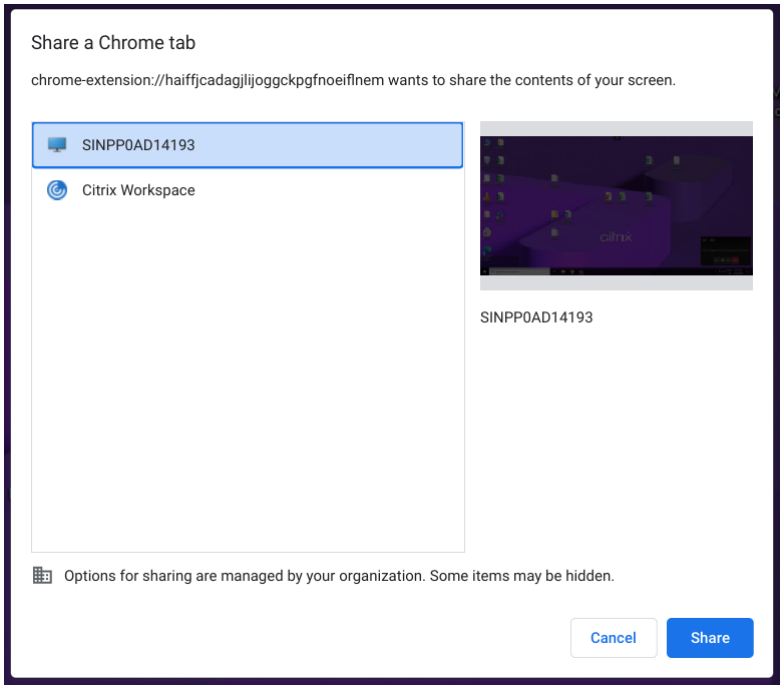
For Microsoft Teams optimization, administrators can limit screen sharing of apps and desktops that are opened only through Citrix Workspace app on managed Chrome devices.
When administrators turn this feature on, the end users can share resources that are opened only from Citrix Workspace app.

This feature is applicable to Chrome version M98 and later.

To configure the settings, use Google policies as follows:

1. Navigate to the **Google Admin** console > **Settings** > **User & browser settings**.
2. Go to **Screen video capture allowed by sites** > **Allow tab video capture (same site only) by these sites** and enter the Citrix Workspace app for ChromeOS app ID -haiffjcadagjlijoggckpgfnoeiflnem.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

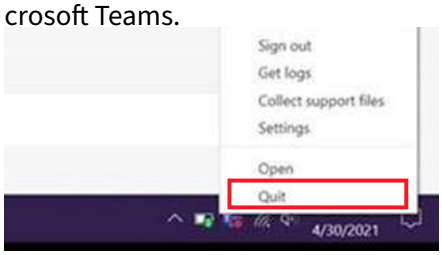


Now, the end users can select the tab and share content that is opened through Citrix Workspace app only.

Troubleshooting for Microsoft Teams optimization

To change Microsoft Teams to optimized from an unoptimized state within your client sessions, do the following:

- Quit Microsoft Teams by right-clicking the Microsoft Teams icon, then click **Quit.** Relaunch Microsoft Teams.



- If quitting does not work, log off from the session and log back on.
- If logging off and logging back on does not work, clear the cache in the directory **C:\Users\Administrator\App** on the VDA, then restart Microsoft Teams.

For more information, see Troubleshooting.

For troubleshooting on the shim library version, see the Microsoft Teams optimization logs section.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Support for dynamic e911

Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it provides the capability to:

- configure and route emergency calls
- notify security personnel

The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client 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 ChromeOS, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law.

Background blurring and effects in Microsoft Teams optimization

Starting with the 2303 release, Citrix Workspace app for ChromeOS supports background blurring and effects in Microsoft Teams optimization for video calls. You can either blur or replace the background effects that are provided by Microsoft Teams. This feature helps you to avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). This feature can be used with P2P and conference calls.

> **Notes:**
>
> - By default, this feature is disabled.
> - This feature is now integrated with the Microsoft Teams UI. Multi-window support is a prerequisite that needs a VDA update to 2112 or higher. For more information, see Multi-window meetings and chat.

Limitations

- Administrator and user-defined background replacement aren't supported.
- When you enable this feature, you might observe performance issues.
- After the ICA session is reconnected, the effect is off. However, the Microsoft Teams UI shows that the previous effect is still On by a tick mark. Citrix and Microsoft are working together to resolve this issue.

How to configure You can enable the background effect feature in one of the following ways:

- Configuration.js
- Google Admin Policy
- Global App Configuration service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration.js To configure background blurring and effects using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp** root folder.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

2. Edit the **configuration.js** file and set the default value of backgroundEffects to true.

   The following is an example of JSON data:

```
"features" :
{

    "msTeamsOptimization" : {

        "backgroundEffects" : true
     }

 }

<!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy On the on-premises deployment, administrators can enable the background effect feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.
   Following is an example of JSON data:

```
"features" :
{

    "msTeamsOptimization" : {

        "backgroundEffects" : true
     }

 }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
11  <!--NeedCopy-->
```

4. Save the changes.

Global App Configuration service On the cloud setup, administrators can enable the background effect feature by setting the **backgroundEffects** attribute to **True** in the Global App Configuration service.

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

Support for Dual Tone Multi Frequency (DTMF) with Microsoft Teams

Citrix Workspace app now supports Dual Tone Multi Frequency (DTMF) signaling interaction with telephony systems (for example, PSTN) and conference calls in Microsoft Teams. This feature is enabled by default.

Microsoft Teams Live Captions

Microsoft Teams optimization supports real-time transcription of what the speaker is saying when Live Captions is enabled in Microsoft Teams.

Support for secondary ringer

Starting with the 2312 release, you can use the secondary ringer feature to select a secondary device on which you want to get the incoming call notification. This feature is applicable only when Microsoft Teams is optimized.

For example, consider that you have set a speaker as the Secondary ringer, and your endpoint is connected to the headphones. In this case, Microsoft Teams sends the incoming call ringer to both the headphones and the speaker. You can't set a secondary ringer in the following cases:

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

> **Note**
>
> By default, this feature is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Known limitations in the feature

- When you enable this feature, you might hear the secondary ringer play two times with a slight lag. This issue is a bug in Microsoft Teams, and they plan to fix it in the upcoming Microsoft Teams release.

Configuration

You can configure the secondary ringer feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js

> **Notes:**
>
> Citrix recommends that you back up the **configuration.js** file before making changes.
> Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> Administrator-level credentials are required to edit the **configuration.js** file.

To enable the feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.
2. Edit the file and set the value **secondaryRingtone** to **true**.

   The following is an example of JSON data:

```
{

    "features":{

        "msTeamsOptimization":{

            "secondaryRingtone" : true
             }

         }

 }

<!--NeedCopy-->
```

3. Save the changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Google Admin Policy For managed devices and users, administrators can enable the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. You can apply this configuration to the following as well:
   - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

```
1        {
2
3            "settings": {
4
5                  "Value": {
6
7                     "settings_version": "1.0",
8                       "engine_settings": {
9
10                           "features":{
11
12                                   "msTeamsOptimization":{
13
14                                          "secondaryRingtone" :
                                               true  }
15
16                                                  }
17
18                                              }
19
20                                          }
21
22                                      }
23
24                 }
25
26  <!--NeedCopy-->
```

3. Save the changes.

Simulcast implementation for optimized Microsoft Teams video conference calls

Starting with the 2312 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

different endpoints are improved. It's done 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). The resolutions depend on several factors including endpoint capability, network conditions, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle. Thus, giving all users the optimum video experience.

Support for Zoom optimization

April 29, 2024

Starting with the 2402.1 version, Citrix Workspace app for ChromeOS supports integration with Zoom virtual desktop infrastructure (VDI) solution for optimized audio and video conferencing experience from within sessions.

> **Note:**
>
> This feature is enabled by default, however, the administrators must configure it. It's supported only on VDA versions 1906 and later.

Prerequisites

Administrators must configure:

- the DDC policy **VirtualChannelWhiteList** to use the Zoom virtual channels. For more information, see Virtual channel allow list policy settings in the documentation.
- the prerequisites for configuring Zoom VDI for ChromeOS.

Feature limitations

- The Zoom conferencing display window is limited to the primary monitor only.
- HID devices are not supported
- For other limitations see, Limitations of using Zoom VDI for ChromeOS.

How to configure

You can configure the feature in one of the following ways:

- Configuration.js
- Google Admin Policy

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration.js

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To configure the feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.
2. Edit the **configuration.js** file and add the Zoom URLs as required.

   The following is an example of JSON data:

```
"features" :
{

    "customVC": [
    {

        "streamName": "ZOOMHDX",
        "appId": "html=https://zoom.us/vdi/plugin"
     }
 ,
    {

        "streamName": "ZOOMHDC",
        "appId": "html=https://zoom.us/vdi/plugin"
     }
 ,
    {

        "streamName": "ZOOMPHX",
        "appId": "html=https://zoom.us/vdi/plugin"
     }

],
"customVCWhitelistURL": [
    {

        "url": "https://zoom.us/vdi/plugin",
        "permissions": [
            "media"
        ]
     }
 ,
    {

        "url": "https://zoom.us/vdi/webview",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
36          "permissions": [
37              "media"
38          ]
39      }
40
41  ]
42
43   }
44
45  <!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy

For managed devices and users, administrators can configure the feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key.

   > **Note:**
   >
   > You can apply this configuration on the following as well:
   >
   > - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
   > - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   > - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

```
1  {
2
3  "settings": {
4
5  "Value": {
6
7      "settings_version": "1.0",
8
9  "customVC": [
10    {
11
12        "streamName": "ZOOMHDX",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
13          "appId": "html=https://zoom.us/vdi/plugin"
14       }
15    ,
16       {
17
18          "streamName": "ZOOMHDC",
19          "appId": "html=https://zoom.us/vdi/plugin"
20       }
21    ,
22       {
23
24          "streamName": "ZOOMPHX",
25          "appId": "html=https://zoom.us/vdi/plugin"
26       }
27
28 ],
29 "customVCWhitelistURL": [
30    {
31
32          "url": "https://zoom.us/vdi/plugin",
33          "permissions": [
34              "media"
35          ]
36       }
37    ,
38       {
39
40          "url": "https://zoom.us/vdi/webview",
41          "permissions": [
42              "media"
43          ]
44       }
45
46 ]
47  }
48
49  }
50
51  }
52
53 <!--NeedCopy-->
```

4. Save the changes.

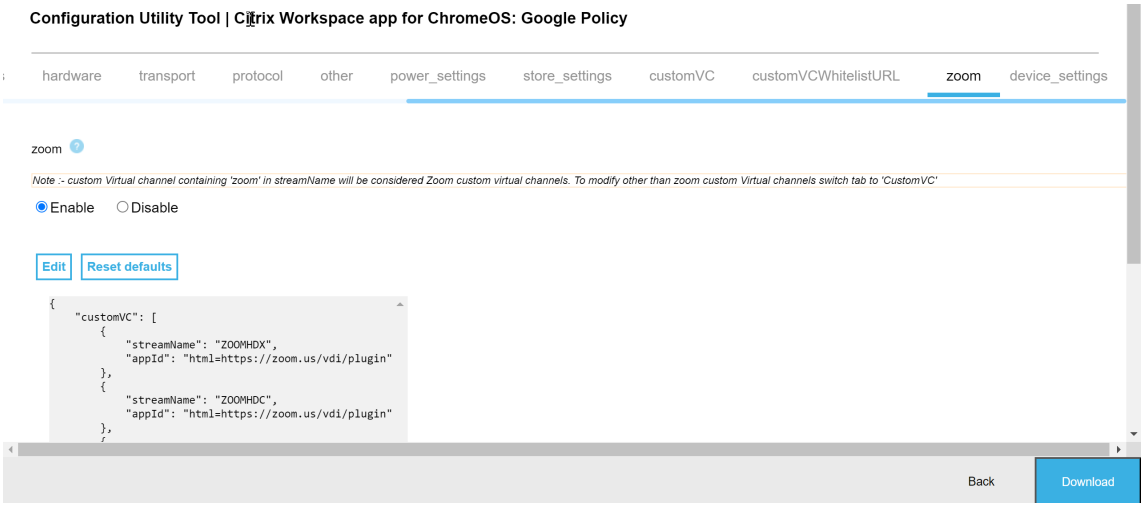
Configuration utility tool

To customize the feature:

1. Click Downloads.
2. Scroll to the **Configuration utility tool** section and expand the element.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Download and unzip the file.
4. Click the Configuration utility tool documentation link to understand how to use the tool.
5. Create a Google Policy configuration.
6. Scroll horizontally and select the **Zoom** tab. Enable the feature to continue.



7. Click **Download** to generate and save the **policy.txt** file.
8. Customize this feature as required by giving proper URLs.
9. Open Citrix Workspace app within the Google Admin Console.
10. Upload the generated **policy.txt** file, or copy and paste the contents.

Configuring Zoom VDI for ChromeOS

For more information, see the Zoom's support article Configuring Zoom VDI for ChromeOS.

Multi-monitor

April 23, 2024

Multi-monitor display

The multi-monitor display feature supports up to two external monitors (1 built-in device monitor + 2 external monitors). By default, the multi-monitor feature is set to enabled.

UI dialogs and toolbars appear only on the primary monitor. However, USB and smart card authentication dialogs span across monitors.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

How to configure

By default, the multi-monitor feature is set to enabled.

> **Note:**
>
> - If you're using Citrix Workspace app running on XenApp 6.5, set the **shadowing** policy to **Disabled** to use the multi-monitor feature.
> - In a desktop session, when the window is set to full screen, the **Display Resolution** option in **Preferences** is deactivated.
> - UI dialogs and toolbars appear only on the primary monitor. However, USB and smart card authentication dialogs span across monitors.

To disable enhanced multi-monitor display in kiosk mode

Enhanced multi-monitor display in kiosk mode is enabled by default.

To disable the feature in kiosk mode, edit the **configuration.js** file or the **Google Admin Console** policy and set the value of **kioskMultimonitor** to **false**.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "graphics": {

                        "multiMonitor": true,
                        "kioskMultimonitor": true
                    }

                }

            }

        }

    }

}
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> **Note:**
>
> To launch a session in kiosk mode, you must enable the **Unified Desktop** mode.

1. Launch a web browser and enter the following command: chrome://flags
2. From the list of flags, search for UnifiedDesktopMode and set it to **Enabled**.

To configure Unified Desktop mode

1. Log on to the Google Admin console.
2. Go to **Device management > Chrome Management > User Settings**.
3. Set the Unified Desktop policy to **Make Unified Desktop mode available to user**.
4. Click **Save**.

Multi-monitor performance

Citrix Workspace app for ChromeOS improves the overall performance and stability of sessions in multi-monitor scenarios. In earlier versions, when a session was running on multiple monitors, you experienced sluggish performance.

How to configure

Multi-monitor display in kiosk mode Enhanced multi-monitor display in kiosk mode is enabled by default.

To disable kiosk mode, edit the **configuration.js** file or the **Google Admin Console** policy and set the value of **kioskMultimonitor** to **false**.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "graphics": {

                        "kioskMultimonitor": false
                    }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
16
17                      }
18
19                  }
20
21              }
22
23          }
24
25      }
26
27
28  <!--NeedCopy-->
```

> **Note:**
>
> To launch a session in kiosk mode, you must enable the **Unified Desktop** mode.

1. Launch a web browser and enter the following command: chrome://flags
2. From the list of flags, search for UnifiedDesktopMode and set it to **Enabled**.

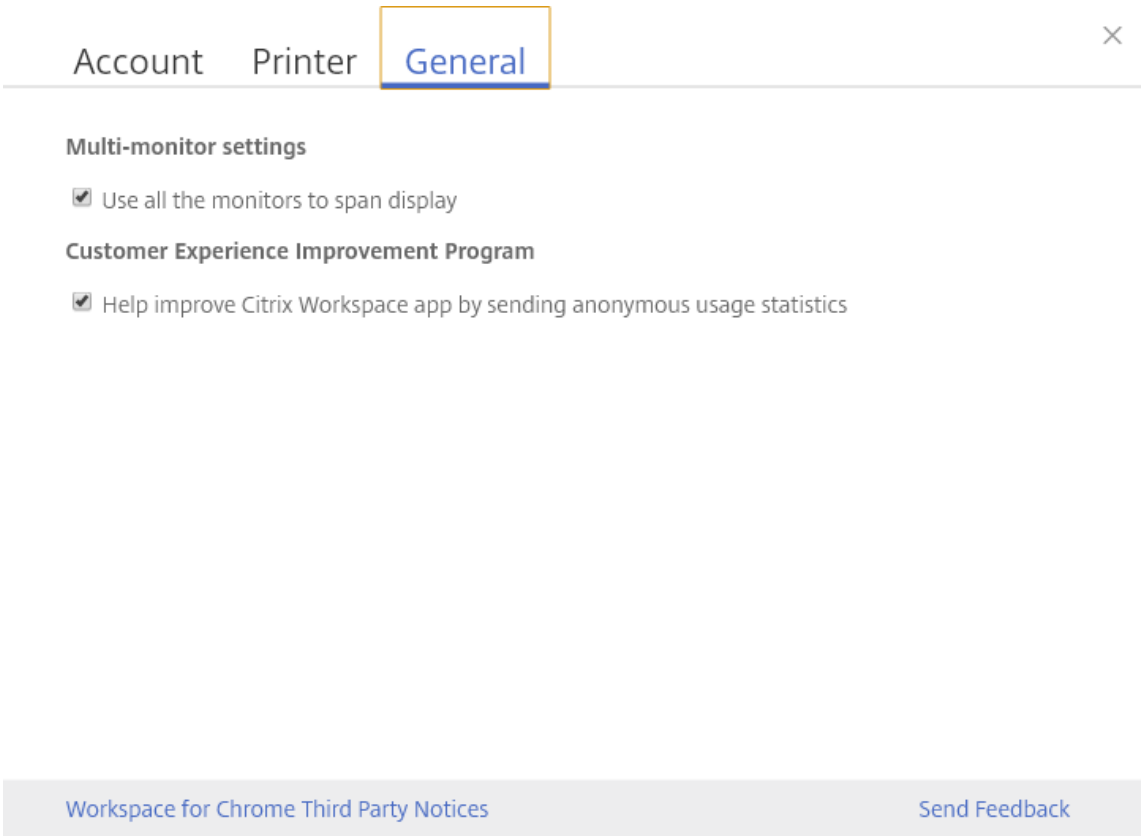
To configure Unified Desktop mode using Google Admin policy

1. Log on to the Google Admin console.
2. Go to **Device management > Chrome Management > User Settings**.
3. Set the Unified Desktop policy to **Make Unified Desktop mode available to user**.
4. Click **Save**.

To disable multi-monitor feature By default, multi-monitor is enabled.

1. Launch Citrix Workspace app for ChromeOS.
2. Select **Settings > General**.
3. Clear **Use all the monitors to span display**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Multi-monitor display is available on both desktops and applications.

When using a multi-monitor display, the desktop session can span across multiple monitors in two ways:

4. Windowed mode: The desktop session displays in single monitor mode.
5. Full-screen mode: When a desktop session is switched to full-screen mode, the session displays in multi-monitor mode only when **Use all the monitors to span display** is selected.

   For the display to span across monitors in a desktop session, select the **Use all the monitors to span display** option and click full-screen mode when the two monitors are connected.

   In an application session, when two monitors are connected and **Use all the monitors to span display** option **is selected,** the session automatically displays in a multi-monitor mode.

Using Citrix Virtual Desktops on dual monitors:

1. Click **Multimonitor** in the toolbar.

   The screen is now extended to both the monitors.

Feature limitations:

- Citrix Workspace app for ChromeOS does not support full-screen H.264 graphics mode for multiple monitors.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- The limit of the number of monitors isn't hard-coded. The total resolution to be managed and rendered affects the limitation.
  - This feature supports up to two external monitors (1 built-in device monitor + 2 external monitors). If you launch a session with the total screen resolution greater than [2 x (1920x1080)] pixels, you might experience screen lags. Monitor resolution limits can cause screen lags to occur.
  - The built-in screen of the latest Chromebooks supports a resolution greater than 1920x1080 pixels. The feature hasn't been tested on such devices.
- In multi-monitor mode, full-screen H264 is disabled because of issues found during testing.
  - When you use one single, large external monitor, the issue does not occur and H264 remains running. Selective H264 also runs in this scenario.
- When you use screens with different resolutions, you might experience performance issues.
- When you use built-in monitors with higher resolution and external monitors whose resolution is low, performance issues might occur.

Support for virtual desktops in multiple-monitor setups

You can now use your virtual desktop in full-screen mode across a subset of available monitors. Previously when you selected multi-monitor mode from the toolbar, the virtual desktop spanned across all available monitors. You can now drag your virtual desktop to span two monitors (out of more than two) and then select multi-monitor mode. A typical use case for this scenario is when you choose to run a video conferencing app on your native device monitor and want to view your virtual desktop contents in full-screen across your other two monitors during the call.

> **Note:**
>
> - To use this feature, under **General** settings > **Multi-monitor settings** > select the **Use all the monitors to span display** option.

Peripherals

April 23, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB device redirection

Citrix Workspace app for ChromeOS supports a wide range of USB peripherals. With this added functionality, you can create a Google policy to identify the PID/VID of the device to enable its use in Citrix Workspace. This support extends to new USB devices too.

How to configure

For information on configuring USB devices, see Knowledge Center article CTX200825.

Automatic redirection of USB devices in Kiosk mode

In kiosk mode, USB devices are redirected automatically inside a session without any manual intervention. In user and public modes, for the first time, you must manually redirect the USB device into the session from the toolbar or the Connection Center. This manual USB redirection is done to grant permission to the Chrome operating system for accessing the USB device. When a USB device is inserted, it's redirected into the session automatically.

> **Important:**
>
> - If you insert a USB device when many sessions are running, the USB redirects into the session that is in focus.
> - If there are no sessions in focus, the USB device isn't redirected into any session.
> - If a single session is running and if it isn't in focus when you insert the USB device, the USB device redirection might fail.

To redirect the USB device to a new session

> **Note:**
>
> To redirect the USB device to a new session, it's required to remove the USB device from the previous session.

1. Right-click the Citrix Workspace icon and select **Connection Center**. The Connection Center window appears.
2. Select a session or an application.
3. Click **Devices**.
4. Navigate to the **USB** section.
5. Click **Release All**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Double hop

Starting with the 2301 version, Citrix Workspace app supports double-hop scenarios. This feature is an enhancement to USB redirection.

For more information, see Double hop in the Citrix Virtual Apps and Desktops documentation.

Composite USB redirection

Previously, when a composite USB device was connected to the local device, it can only be used as a single device through USB redirection. The disadvantage was that the interfaces like audio and video also got redirected through USB, despite optimized channels. The interfaces weren't separate and due to this incapability, administrators can't decide which components to redirect through USB and which ones to redirect through the optimized virtual channel (like audio interface) to achieve the best performance.

Starting from the 2211 release, administrators can configure if certain interfaces of the device redirect to the session through USB redirection or not. The end user can now select and redirect a specific constituent interface of a composite USB device to the Citrix Workspace app session through USB redirection.

About composite USB redirection

USB 2.1 and later supports the notion of USB composite devices where many 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. Such devices are also 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 local device. Forwarding also blocks the local usage of the device for all applications on the local device, including the Citrix Workspace app.

Consider a USB headset device with both an audio device and the 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 a better performance when the audio is sent through an optimized HDX audio channel when compared to a generic channel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To resolve these issues, Citrix recommends you split the composite device and forward only the child interfaces that use a generic USB channel. Such a mechanism make sure that the other child devices are available for use by applications on the local device, including the Citrix Workspace app that provides optimized HDX experiences. This method allows the required devices to be forwarded and available to the remote session.

How to enable this feature

You can enable this feature in the following ways:

- Configuration.js
- Global App Configuration service
- Google Admin Policy

Configuration.js To configure composite USB redirection using the **configuration.js** file, do the following:

1. Locate the **configuration.js**file in the **ChromeApp root** folder.
2. Edit the **configuration.js** file to configure the composite USB redirection feature.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set **enableCompositeDeviceSplit** to **true**.

The following is an example of JSON data:

```
```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 
```

1. Save the changes.

> **Note:**
>
> - To disable the feature, set the **enableCompositeDeviceSplit** attribute to **false**.

Global App Configuration service On the cloud setup, administrators can enable the composite USB redirection feature by setting the **enableCompositeDeviceSplit** attribute to True in the Global App Configuration service.

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

Google admin policy On the on-premises deployment, administrators can enable the composite USB redirection feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key. Following is an example of JSON data:

```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

<!--NeedCopy-->
```

4. Save the changes.

Configuration

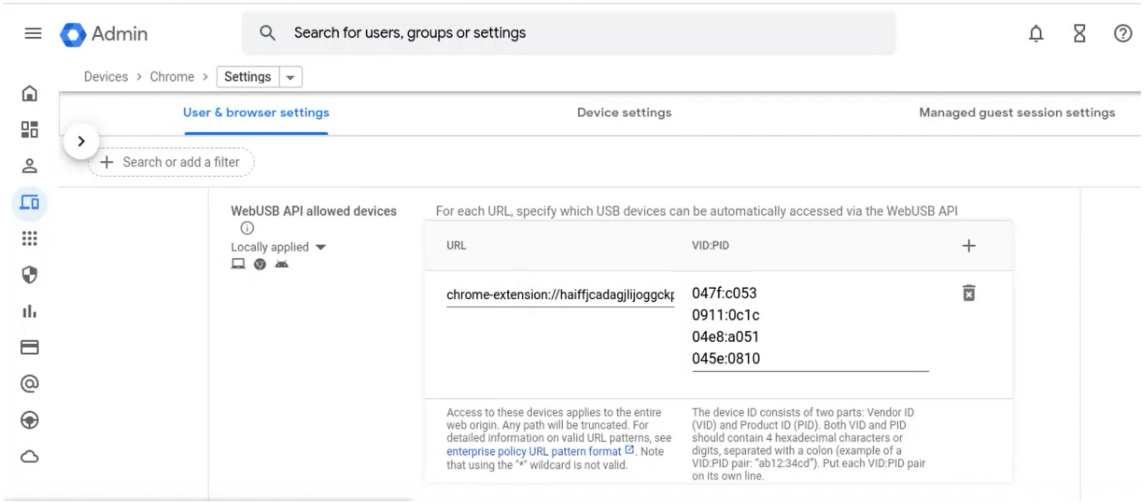
Prerequisites:

- Allow list of USB Devices with VID:PID values and enable policy for USB device redirection on Delivery Controller. For more information, see the knowledge center article CTX200825.
- This feature works on managed devices and not on BYOD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To enable the auto-detection of the USB:

1. Go to Google Admin Policy settings.
2. Select the **WebUSB API allowed devices** option.
3. Enter the Citrix Workspace app for the ChromeOS extension ID. For example, chrome-extension**:**`//haiffjcadagjlijoggckpgfnoeiflnem`.
4. Add the VID and PID of the device as follows:



   After adding the VID and PID values, the Citrix Workspace app can now automatically detect the devices in the session.

5. Apply the Google Admin Policy. For more information on Device rules and sample JSON data, see the following section.
6. Save the changes.

Device rules

Citrix Workspace app uses the device rules to decide, which USB devices to allow or prevent from forwarding to the remote session.

Following are the explanations of the keywords:

- **allow:** This section includes the list of devices and their child interfaces that can be redirected to the session.
- **deny:** This section includes the list of devices and their child interfaces that can't be redirected to the session.
- **autoRedirect:** This section includes the list of devices and their child interfaces that can be auto-redirected to the session through USB redirection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - Each object represents a device with the mandatory `vid` and `pid` values of the USB device. It's optional to have 'split', and 'interfaceClass'values.

- **vid, pid (mandatory):** Represents Vendor ID (VID) and Product ID (PID) of the USB device. Enter the values in Hexadecimal format.
- **split (optional):** Expects a boolean value that indicates whether the device to be split into child interfaces or not.
- **interfaceClass (optional):** Represents USB interface class. The allowed values are audio, video, hid, printer, storage, and so on.

The following is an example of JSON data:

```
{

"settings": {

"value": {

"settings_version": "1.0",
"device_settings": {

"deviceRules": {


    "allow": [
        {
 "vid": "11","pid": "22",  "split":true, "interfaceClass":["audio","
    video"] }
  //split device and allow redirection of 'audio' & 'video' interfaces.
    ],

    "deny": [
        {
 "vid": "33","pid": "44" }
 ,  //deny redirection of this whole device with vid= 33 & pid = 44,
    including all of its interfaces.
        {
 "vid": "77","pid": "88","split":true,"interfaceClass":["audio"] }
     //split device and deny the redirection of 'audio' interface only;
         remaining interfaces(if any) are redirected through USB.
    ],

    "autoRedirect": [
    {
 "vid": "55","pid": "66" }
 , //auto redirect the device when it's connected.
    {
 "vid": "55","pid": "66","split":true,"interfaceClass":["hid"] }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

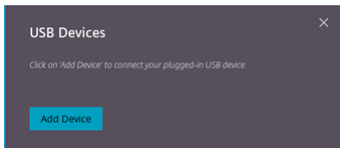
```
34    //split device and auto redirect only the 'hid' interface when the
          device is connected.
35      ]
36                    }
37
38                }
39
40            }
41
42        }
43
44   }
45
46  <!--NeedCopy-->
```

How to use this feature

To use the composite USB redirection feature:

1. Click the USB icon from the toolbar.

   If there are no USB devices connected, the following pop-up appears:

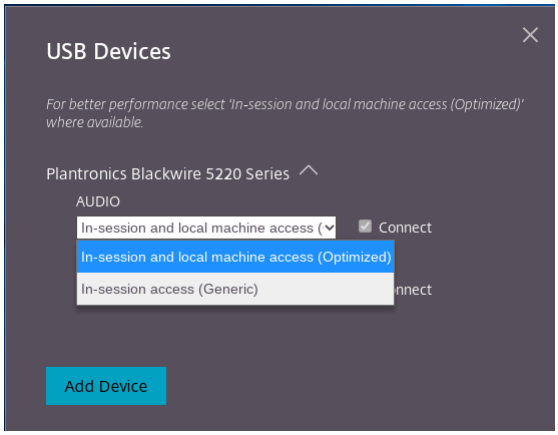
2. Connect a USB device to your local machine.
   The following pop-up might appear:

3. Click **USB Devices** to view and redirect the USB constituent. After a successful connection, the Citrix Workspace app detects the USB. For each USB constituent interface, you see a drop-down menu. The two options are:

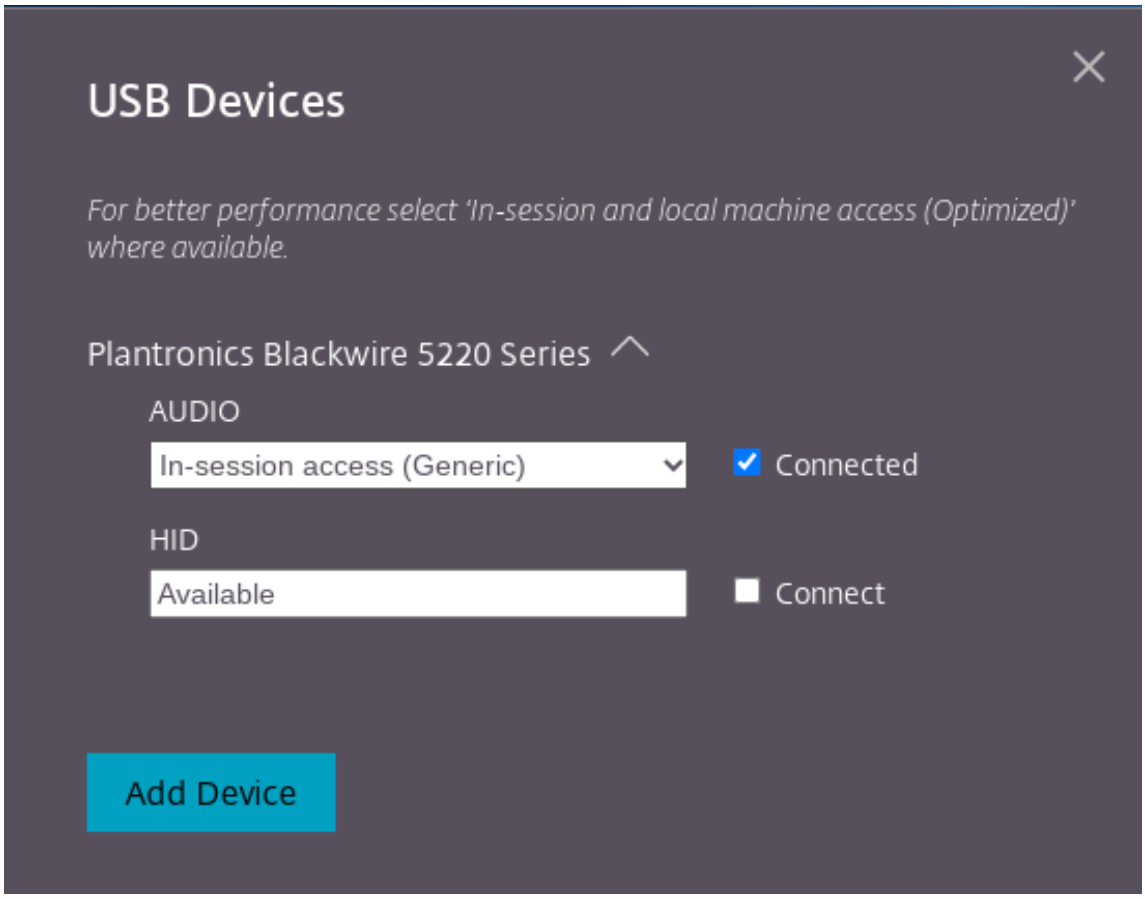
   - **In-session and local machine access (Optimized):** select this option if you want to access the USB on your device and in a session.
   - **In-session access (Generic):** select this option if you want to access the USB only in the session.

     For better performance, select **In-session and local machine access (Optimized)** option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Select **Connect** for redirecting the interface.



Upon successful redirection, the status changes to **Connected**.

> **Notes:**
>
> - To add a USB device manually, click **Add Device**. The Chrome picker dialog appears that lists the USB devices. You can select the device from the list.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - If a USB device connection is denied, the following error message appears:
>
>   "Your administrator has blocked the newly inserted device.
>   Contact your organization's administrator for assistance.

How to transfer the USB interface between the sessions

When you click the USB icon from the toolbar, a list of USB devices that are connected to your sessions appears. If the USB device is already in use in a different session you can see that the USB constituent shows **Connected to another session** status.

To redirect to the current session, select **Connect** which is placed opposite to the USB constituent. The status changes accordingly.

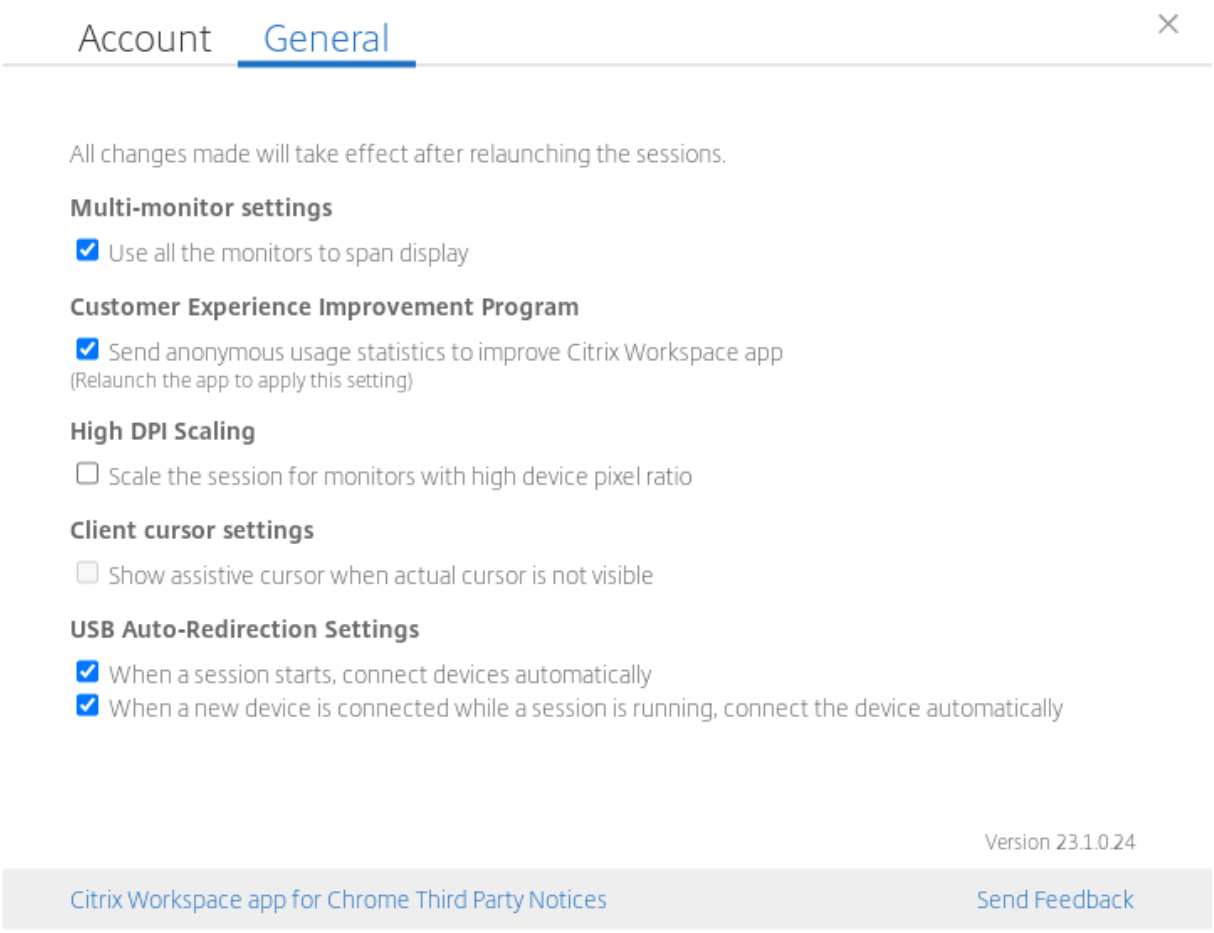
Composite USB automatic redirection settings

Previously, there was no option related to USB automatic redirection settings to set the end user preferences. As administrators control these policies, the end user has to manually redirect required USB devices on every session launch.

Starting with the 2301 version, the end user can select a preference for auto-redirection for any USB device within a Virtual Desktop session. Citrix Workspace app now provides app-level settings, where the end user can control the USB auto-redirection. The end user can set preferences and can save the settings across session launches.

There are two options: one at the session launch and the other while the session is ongoing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Note:

- This feature supports on-premises and cloud deployments and is available only for managed Chrome users.

Configure Composite USB Redirection through DDC policies

Previously, administrators used Google Admin policies to configure the client-side USB redirection.

Starting with the 2306 release, you can configure USB redirection through the DDC policies as well. Configurations through DDC policies allow administrators to have a unified and centralized way of defining policies and behavior. These policies are applicable for on-premises and cloud deployments on managed devices and users. This feature is supported on VDA versions 2212 and later.

Configuration

You can configure this feature in one of the following ways:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configuration.js
- Google Admin Policy

> **Note:**
>
> - The policy **enableDDCUSBPolicy** is set to **true** by default.

Configuration.js To disable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit the file.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set the value of **enableDDCUSBPolicy** to **false**. Following is an example of JSON data:

```
"features" : {

"usb" : {

   "enableDDCUSBPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Save the changes.

Google admin policy For managed devices and users, administrators can disable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the engine_settings key.
   Following is an example of JSON data:

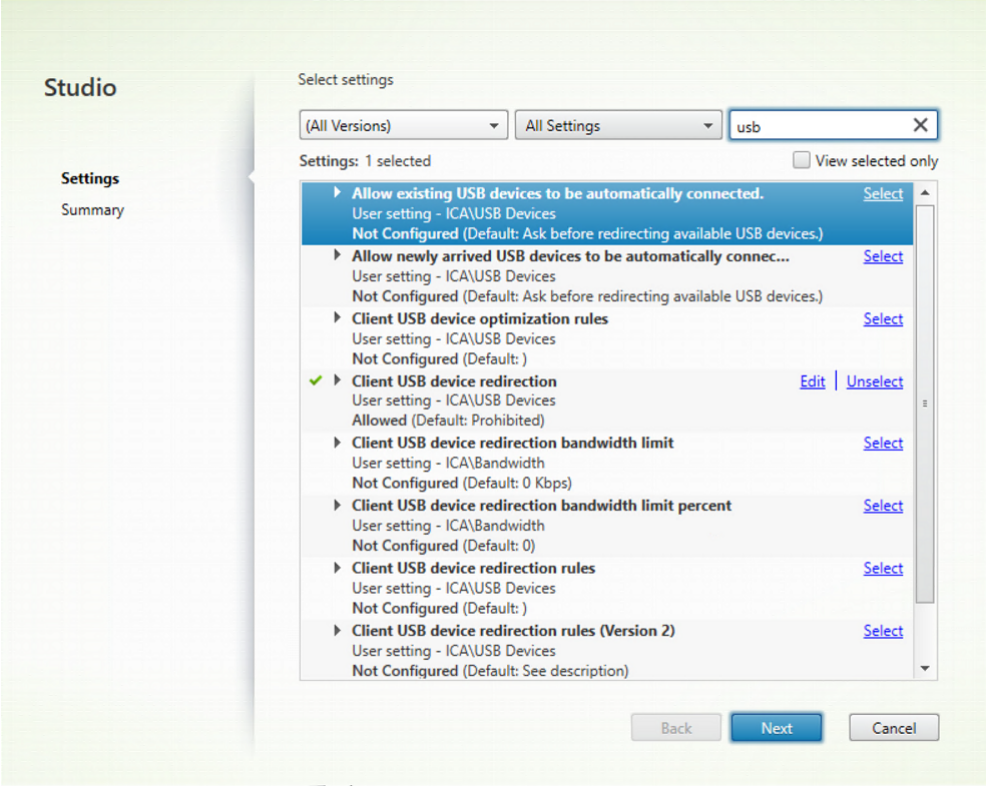
```
    "features" : {

    "usb" : {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        "enableDDCUSBPolicy": false
      }

  }

<!--NeedCopy-->
```

4. Save the changes.

DDC Policy The following screenshot displays the DDC policies that are related to USB redirection. This feature is supported on VDA versions 2212 and later.



For more information on the DDC policies that are related to USB redirection, see the following articles in the Citrix Virtual Apps and Desktops documentation:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Auto redirection of USB devices

To redirect USB devices automatically, you must follow the USB device rules.
You can configure USB device rules through:

- Google Admin Policy
- Client USB device redirection rules (Version 2)

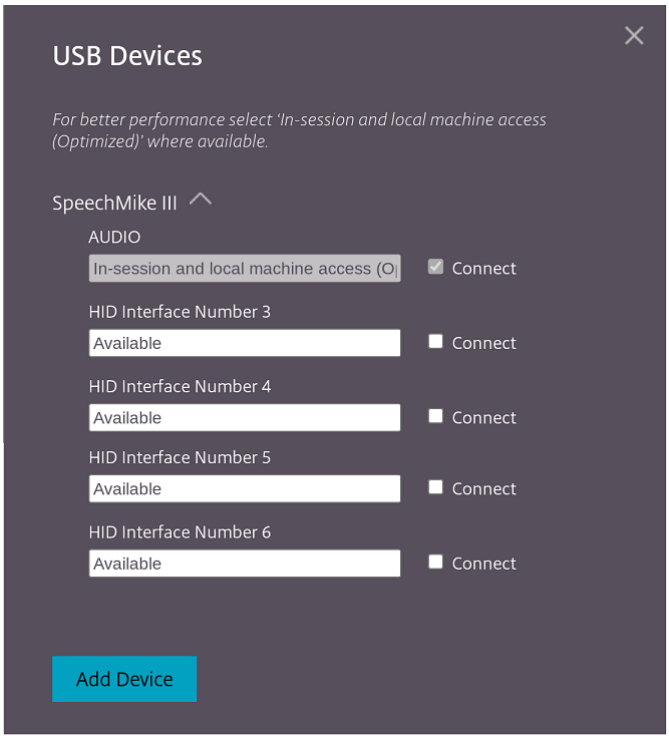
Enhancements to Composite USB device UI

Starting with the 2306 release, when the configuration of a Composite USB device is set to "split": true, the **USB Devices** UI displays the components based on interface numbers instead of interface classes.

For more information, see the Composite USB redirection article.

User interface

The following is an example:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enhancements to Composite USB redirection through DDC policies

Starting with the 2307 version, you can determine if a particular composite USB interface or class can redirect to VDA by default or not. If you have a composite USB connected to the ChromeOS device, then the configuration **enableDefaultAllowPolicy** helps you decide whether, by default, you can allow USB redirection through DDC policies. VDA versions 2212 and later support this feature.

How to use

When you set the attribute **enableDefaultAllowPolicy** to **true**, and if you redirect a particular interface class or interface number to the VDA, then you must add a policy rule to deny the other interface classes or numbers from being redirected. You can configure this feature through the DDC policy **Client USB device redirection rules (Version 2)**.

For more information, see USB device redirection rules (Version 2). In addition, you can configure the denied part through the Google Admin Policy, but only for the interface class level.

For more information, see Enhancements to Composite USB device UI.

Here's an example configuration through the DDC policy **Client USB device redirection rules (Version 2)**, where you allow the interface number 03 to redirect.

```
1 ```
2 "DENY: vid=1188 pid=A301 split=01 intf=00,01,02"
3 <!--NeedCopy--> ```
```

Here's an example configuration through the Google Admin Policy rule, where you allow the HID interface to redirect and deny the audio interface class.

```
1 ```
2 "deny": [
3     {
4  "vid":"05e9", "pid":"0428", "split":true, "interfaceClass":["audio"]
5      }
6
7 ]
8 <!--NeedCopy--> ```
```

Configuration You can configure this feature in one of the following ways:

- Configuration.js
- Google Admin Policy

> **Note:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - By default, the policy **enableDefaultAllowPolicy** is set to **true**.

Configuration.js To disable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit the file.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set the value of **enableDefaultAllowPolicy** to **false**.

   The following is an example of JSON data:

```
"features" : {

   "usb" : {

   "enableDefaultAllowPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Save the changes.

Google admin policy For managed devices and users, administrators can disable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management**> **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.

   The following is an example of JSON data:

```
'features' : {

    'usb' : {

    'enableDefaultAllowPolicy': {
 "type": "false" }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
      }

    }

<!--NeedCopy-->
```

4. Save the changes.

Serial COM port redirection

By default, Citrix Workspace app for ChromeOS maps COM5 as a preferred serial COM port for redirection.

How to configure

To configure serial COM port redirection, enable the feature by applying Citrix Virtual Apps and Desktops and Citrix DaaS port redirection policy settings. For more information on port redirection, see Port redirection policy settings.

> **Note:**
>
> By default, Citrix Workspace app for ChromeOS maps COM5 as a preferred serial COM port for redirection.

After enabling serial COM port redirection policy settings on the VDA, configure Citrix Workspace app for ChromeOS using one of the following methods:

- Google Admin Policy
- configuration.js file
- Changing the default mapping by issuing a command in an active ICA session.

Using Google Admin Policy to configure COM port redirection Use this method to redirect the serial COM port by editing the policy file.

> **Tip:**
>
> Citrix recommends that you configure the COM port using the policy file only when Citrix Workspace app for ChromeOS is repackaged.

Edit the Google Admin Policy by including the following:

```
    {

      "settings": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                "Value": {

                 "settings_version": "1.0",
                 "store_settings": {

                 "rf_web": {

                 "url": "<http://YourStoreWebURL>"
                   }

                   }
,
                  "engine_settings":{

                  "features" : {

                  "com" : {

       "portname" : "<COM4>", where COM4 indicates the port number that
        is set by the administrator.
                                                  }

                                              }

                                              }

                                              }

                                              }

                                             }


<!--NeedCopy-->
```

List of serial COM port name options and their descriptions:

- “portname”: Port number for the COM (serial) virtual channel. By default, the value is COM5.

Using the configuration.js file to configure COM port redirection Use this method to redirect the serial COM port by editing the **configuration.js** file. Locate the portname field in the configuration.js file and edit the value by changing the port number.

For example:

```
"com" :{


"portname" : "COM4"

 }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
7
8 <!--NeedCopy-->
```

> **Note:**
>
> Citrix recommends using the configuration.js file method to configure serial port redirection only when Citrix Workspace app for ChromeOS is repackaged and republished from StoreFront.

Issuing a command in an ICA session to configure COM port redirection Use this method to redirect the serial COM port. Run the following command in an active ICA session:

```
1     net use COM4 : \\Client\COM5
2 <!--NeedCopy-->
```

> **Tip:**
>
> In the example above, COM4 is the preferred serial port used for redirection.

Power settings

April 23, 2024

Awake setting

Citrix Workspace app for ChromeOS keeps managed Chromebook devices awake even when the users aren't active.

The awake setting feature is disabled by default.

How to configure

To enable the feature, edit the **Google Admin Console** policy and set the value of the **keep_awake_level** property under **power_settings** to either **"system"** or **"display"** and then restart the session.

The **"system"** level keeps the system awake, but allows the screen to be dimmed or turned off. The **"display"** level keeps the system awake and active.

```
1 {
2
3  "settings": {
4
5      "Value": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6
7           "settings_version": "1.0",
8           "power_settings": {
9
10              "keep_awake_level":  ” system ”  or  “ display ”
11               }
12
13             }
14
15          }
16
17      }
18
19  <!--NeedCopy-->
```

List of power-setting options with their descriptions:

- “keep_awake_level”: Keeps devices awake even when users aren’t active. You can choose either of the two values:
  - “system”: Keeps the system awake, but allows the screen to be dimmed or turned off.
  - “display”: Keeps the system awake and active.

> **Note:**
>
> For Kiosk mode, make sure that the **Allow app to manage power** setting in the **Google Admin** console is disabled.

Printing

April 23, 2024

PDF printing

The Citrix PDF Universal Printer driver enables users to print documents opened with hosted applications or applications that run on virtual desktops delivered by XenDesktop 7.6 and XenApp 7.6 or later. When a user selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF then opens in a new window for viewing and printing.

When printing a document opened with a hosted application or an application that runs on a virtual desktop, you can print the document to PDF. You can transfer the PDF to the local device to view and print from a locally attached printer. The file isn’t stored in Citrix Workspace app for ChromeOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important**
>
> Local PDF printing is supported only on XenApp and XenDesktop 7.6 or later.

How to configure

Requirements To access the Citrix Workspace app for ChromeOS download page, you need a MyCitrix account.

To enable users to print documents opened with hosted desktop and applications:

1. Download the Citrix PDF Printer and install the Citrix PDF Universal Printer driver on each VDA machine that delivers desktops or apps for Citrix Workspace app users. After installing the printer driver, restart the machine.
2. In Citrix Studio, select the **Policy node** in the left pane and either create a policy or edit an existing policy.

   For more information about configuring Citrix Virtual Apps and Desktops policies, see Policies.
3. Set the Auto-create PDF Universal Printer policy setting to **Enabled**.

Support for network printers

Previously, the Citrix PDF Printer option was used to print from the virtual desktop session. The print driver converted the file to PDF and transferred the PDF to the local device. The PDF was then opened in a new window for viewing and printing.

Starting with the 2305 release, Citrix Workspace app for ChromeOS supports network printing. End users can view the list of printers that are connected to their Chromebook inside the session. Users can select a printer directly without generating intermediate PDF files on the local device. This feature is supported on:

- VDA versions 2112 and later.
- ChromeOS version 112 and later.

> **Note:**
>
> - By default, this feature is enabled, and only the PDF format of metafile printing is supported.

For more information, see the following articles:

- Manage printers and print drivers in your environment in the Citrix Virtual Apps and Desktops documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Knowledge Center article on How to use Citrix Policy to Set a Default Session Printer - CTX232031.
- Knowledge Center article on Citrix Printing Quick Start Guide and Default configuration - CTX227534.

Configuration

You can disable this feature in one of the following ways:

- Configuration.js
- Google Admin Policy

> **Note:**
>
> - As a prerequisite, the IT administrator must enable the **Auto-create generic universal printer** policy on the Delivery Controller (DDC). For more information, see Client printers policy settings in the Citrix Virtual Apps and Desktops documentation.

Configuration.js To disable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the ChromeApp root folder.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

2. Edit the **configuration.js** file and set the default value of **networkPrinting** to false. Following is an example of JSON data:

```
{

  "features": {

     " networkPrinting ": {

          "enable": false
                    }

     }

 }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Save the changes.

Google Admin Policy IT administrators can disable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key. Following is an example of JSON data:

```
{

   "features": {

        " networkPrinting ": {

            "enable": false
                 }

         }

 }

<!--NeedCopy-->
```

4. Save the changes.

Seamless experience

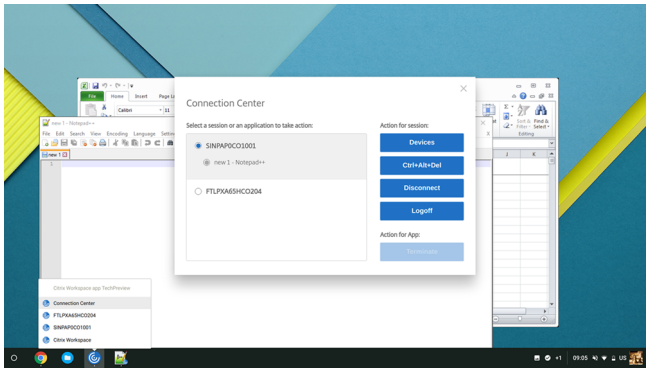
April 24, 2024

Connection Center

Connection Center helps application management in seamless sessions by providing a taskbar that lists all opened applications.

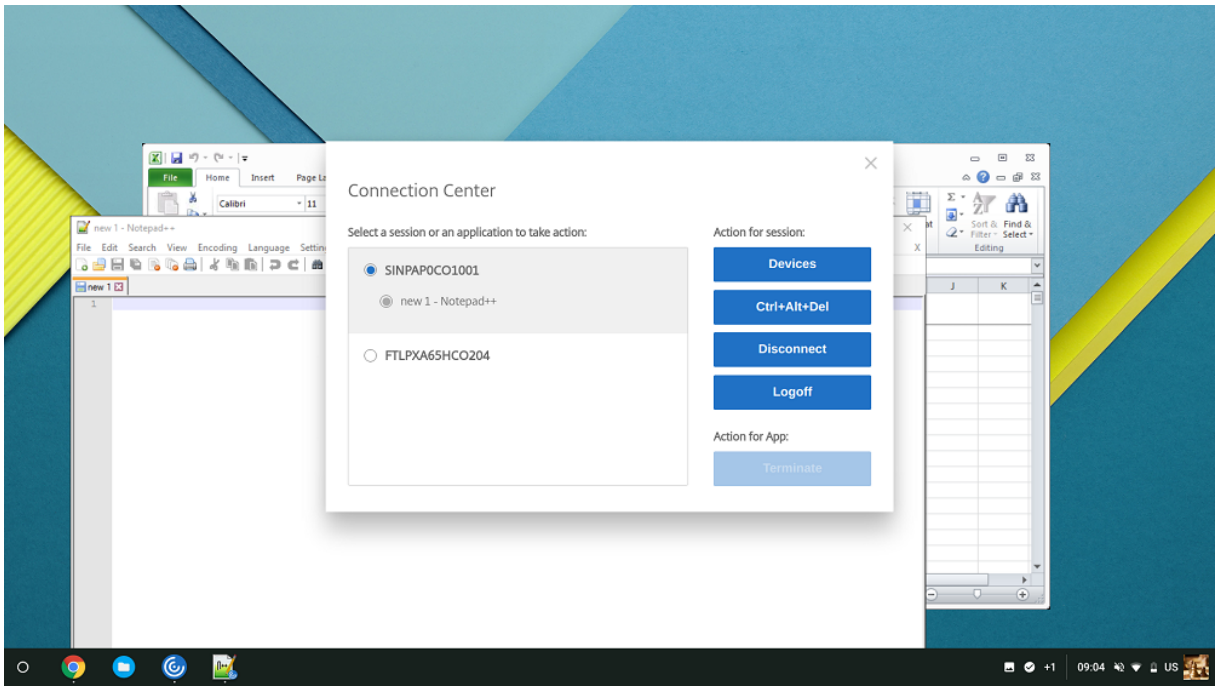
To launch the Connection Center, right-click the Citrix Workspace icon and then select **Connection Center**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Using the Connection Center, you can select an application and:

1. Display devices.
2. Send a Ctrl+Alt+Del command.
3. Disconnect from a session.
4. Logoff from the session.



You can also end an app using the Connection Center by selecting the radio button of the corresponding application and clicking **Terminate**.

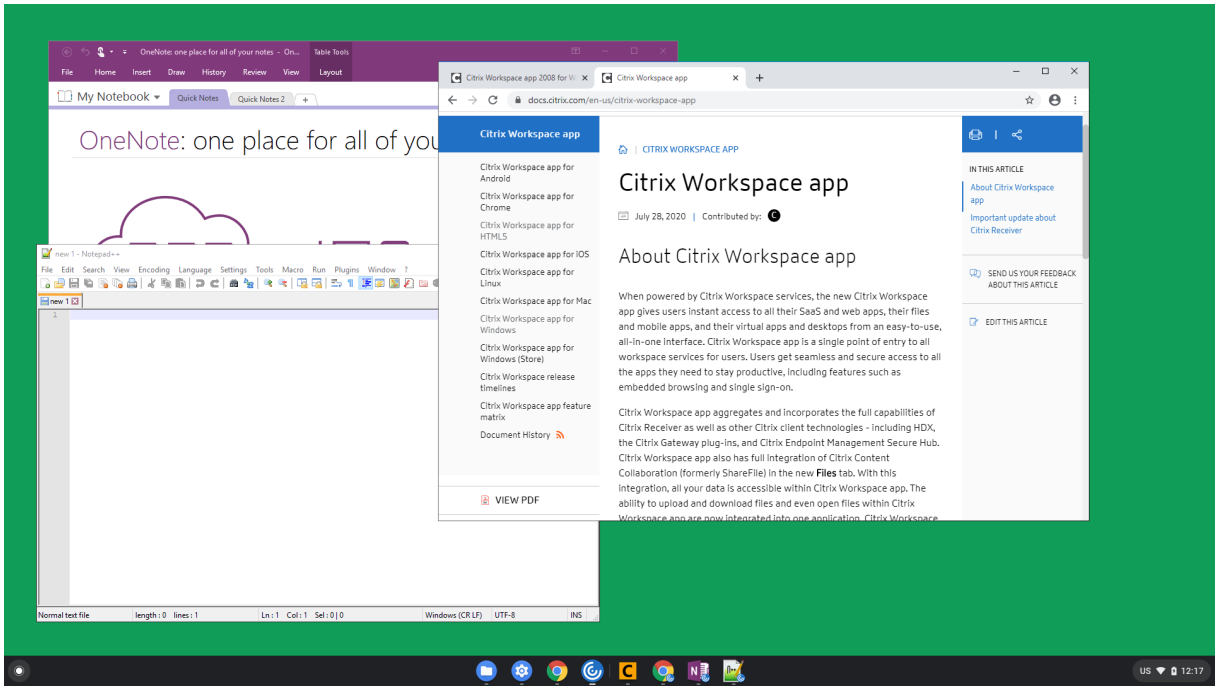
Seamless window integration

Citrix Workspace app for ChromeOS improves the user experience by adding seamless integration of multiple apps that are hosted in separate windows within an active session. Using this functionality,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace app for ChromeOS enables you to start apps in an independent user interface as compared to starting all apps for a session in a single window.

Seamless applications can be hosted in separate windows. With this functionality, remote applications are run natively on the client device.

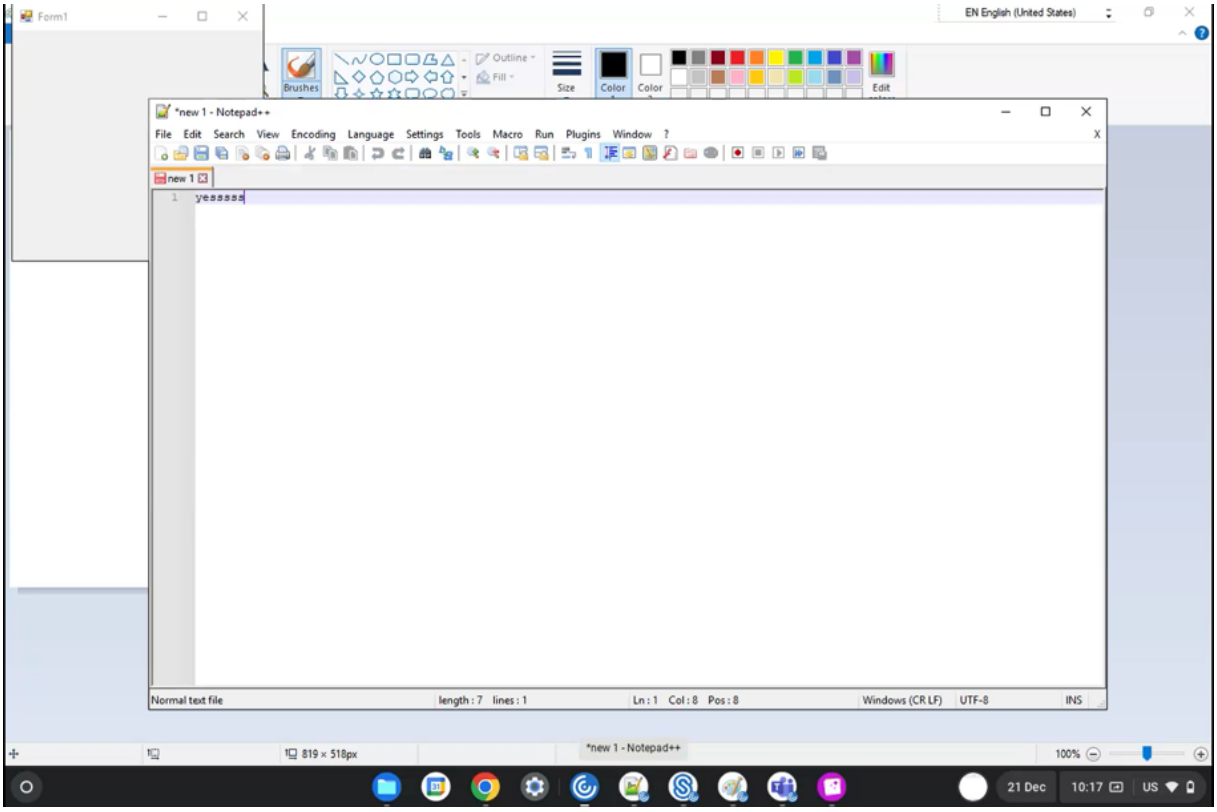


Feature limitations:

- Extra entries appear in the Chrome task bar. Click any of the entries to bring the selected session to the front.
- All opened apps in an active session run in a single window. Focusing on one app in an active session brings that window into focus along with all other apps belonging to that session.

Use the seamless app icon on the taskbar to quickly move between apps:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Tip:**
>
> All apps in one session run in a single window. When moving an app to a second monitor, all apps that are part of that session move to the second monitor.

App switch

Shows the apps that are opened inside a session.

> **Note:**
>
> This option is only for kiosk mode.

The app switcher enables users to switch between multiple apps running in the same session. The app that is in focus is highlighted.

How to configure

To configure, use the Google admin policy by including the following:

```
{

    "settings": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
4
5          "Value": {
6
7              "settings_version": "1.0",
8                  "engine_settings": {
9
10                     "ui": {
11
12                         "appSwitcher": {
13
14                             "showTaskbar": true,
15                             "showIconsOnly": false,
16                             "autoHide": false
17                                          }
18
19                            }
20
21                     }
22
23           }
24
25       }
26
27   }
28
29
30 <!--NeedCopy-->
```

List of app switch options with their descriptions:

- **showTaskbar**: If set to true, the taskbar appears at the bottom of the session. To hide the taskbar, set this option to false.
- **showIconsOnly**: If set to true, the taskbar icons appear. By default, the option is set to false.
- **autoHide**: If set to true, the taskbar is automatically hidden. By default, the option is set to false.

Taskbar icons

Apps and desktops that are configured using Citrix Virtual Apps and Desktops and Citrix DaaS in an active session are displayed as separate apps. You can see these apps in the taskbar (shelf) on the ChromeOS device. This feature applies to published applications and desktops. The functionality and behavior of this feature is similar to the taskbar experience that is provided by the Windows Operating system.

By default, this feature is enabled.

How to configure

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuring taskbar icons using Google Admin policy

> **Note:**
>
> Citrix recommends using this method only when Citrix Workspace app for ChromeOS is repackaged for users.

1. Log on to the Google Admin Console.
2. Go to **Device management > Chrome Management > User Settings**.
3. Add the following strings to the `policy.txt` file.

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

4. Click **Save** and close the file.

Configuring taskbar icons using the `web.config` in StoreFront

> **Note:**
>
> Citrix recommends that you use the `web.config` file method for configuration purposes only. You can use this method when the store version of Citrix Workspace app for ChromeOS is being used.

1. Open the `web.config` file for the Citrix Receiver for Web site. This file is in `C:\inetpub\wwwroot\Citrix\\\\<Storename>Web`, where the `Storename` is the name specified for the store when it was created.
2. Locate the **chromeAppPreferences** field and set its value with the configuration as a JSON string.

For example:

```
chromeAppPreferences='{

    "seamless":{

        "showInShelf":false
         }

         }

<!--NeedCopy-->
```

Configuring taskbar icons using the configuration.js file The **configuration.js** file is in the **ChromeApp root** folder. Access this file directly to modify Citrix Workspace app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Administrator-level credentials are required to edit the configuration.js file; after editing the file, repackage the app for the changes to take effect.

To change the ChromeOS taskbar using the configuration.js file:

1. Open the configuration.js file and set the **showInShelf** attribute to true.

For example:

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

Feature limitations:

1. When more than one instance of the same application is launched, the app icon isn't stacked and appears as two separate icons. For example, two instances of Notepad display two icons of Notepad in the taskbar.
2. App pinning isn't supported.

Session experience

May 14, 2024

Full-screen mode

How to configure

To configure your desktop session to always open in full-screen mode, edit the Google Admin Policy by including the following:

> **Note:**
>
> - By default, desktop sessions open in maximized windows, where the "window state"value is set to "maximized".

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
{


      "settings": {


                      "Value": {

                      "settings\_version": "1.0",
                      "engine\_settings": {

                      "ui": {

                      "sessionsize": {

                      "windowstate": "fullscreen"
                                }

                                      }

                                            }

                            }

 }

<!--NeedCopy-->
```

Session size

How to configure

The session size setting lets you customize resolutions for a session. Edit the Google admin policy by including the following:

```
{

    "settings": {

      "Value": {

            "settings_version": "1.0",
            "engine_settings": {

            "ui": {

                "sessionsize" : {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                    "minwidth" : 240,
                    "minheigh" : 120,
                    "available" : {

                            "default" : "Fit_To_Window",
                            "values" : [
                                        "Fit_To_Window",
                                        "Use_Device_Pixel_Ratio",
                                        "1280x800",
                                        "1440x900",
                                        "1600x1200"
                                    ]
                        }

                     }

                }

            }

        }

    }

 }


<!--NeedCopy-->
```

List of various resolution options and their descriptions:

- **minwidth**: 240: The minimum width for sessions.
- **minheight**: 120: The minimum height for sessions.
- **available**: Options to set resolution preferences for sessions.
  - **default**: The value that you set applies to the default resolution. By default, the value is set to "Fit_To_Window". You can change the default value as follows:
    - **values**: Other resolution values are:
      - **Fit_To_Window**: The default resolution value available. It matches the window size to emulate various screen resolutions.
      - **Use_Device_Pixel_Ratio**: Scales sessions to match the DPI of the device.
      - **1280x800**: Sets the session size to 1280 * 800 pixels.
      - **1440x900**: Sets the session size to 1440 * 900 pixels.
      - **1600x1200**: Sets the session size to 1600 * 1200 pixels.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Net promoter score

Citrix Workspace app for ChromeOS prompts you periodically for Net Promoter Score (NPS) feedback. The prompt asks you to rate your experience with Citrix Workspace app for ChromeOS. We use NPS feedback as a tool to measure customer satisfaction and to further improve the app.

You can rate your experience on a scale of 1–5, with 5 indicating that you're satisfied.

How to configure

To configure NPS, use the Google admin policy by including the following. If the option is set to true, the user can provide the rating.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "netPromoters": true
                           }

                 }

          }

      }

 }


<!--NeedCopy-->
```

Auto-launch of ICA sessions

Citrix Workspace app for ChromeOS supports auto-launch of ICA (Independent computing architecture) sessions on Google managed devices or users.

With this feature, you can access resources remotely from Citrix Workspace for the web. The downloaded ICA file starts automatically, with the Citrix Workspace app for ChromeOS, if it has been installed on the device. Previously, you were able to only download ICA files and open the files manually

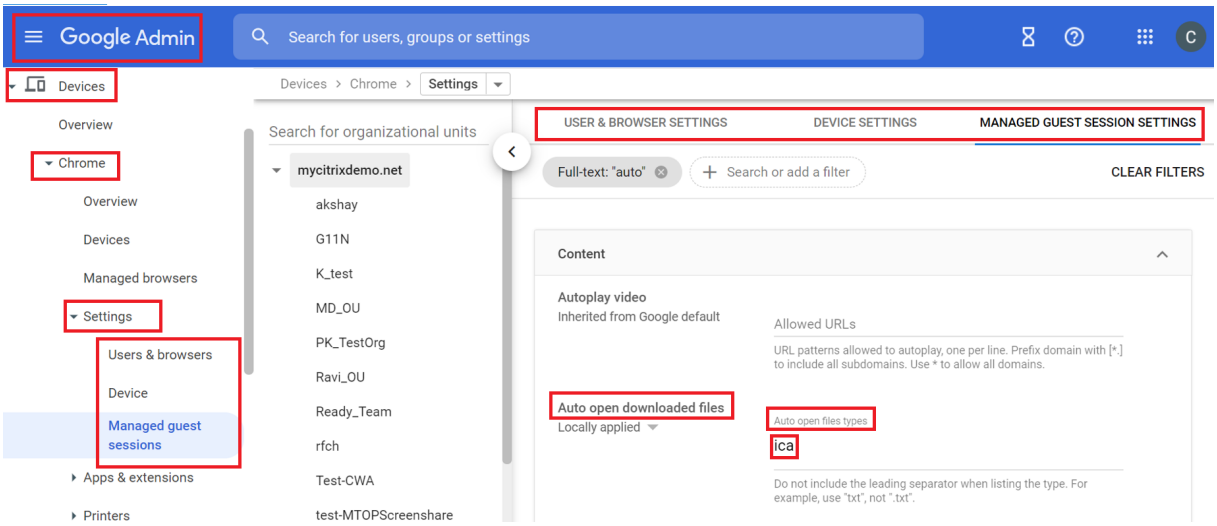
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

to start resources. Also, the ICA file wasn't deleted when opened and remained on the device. Now, the ICA file is automatically deleted from the device - once it's used to auto-launch the session.

How to configure

To configure the auto-launch of ICA sessions, log in as an administrator and do these steps:

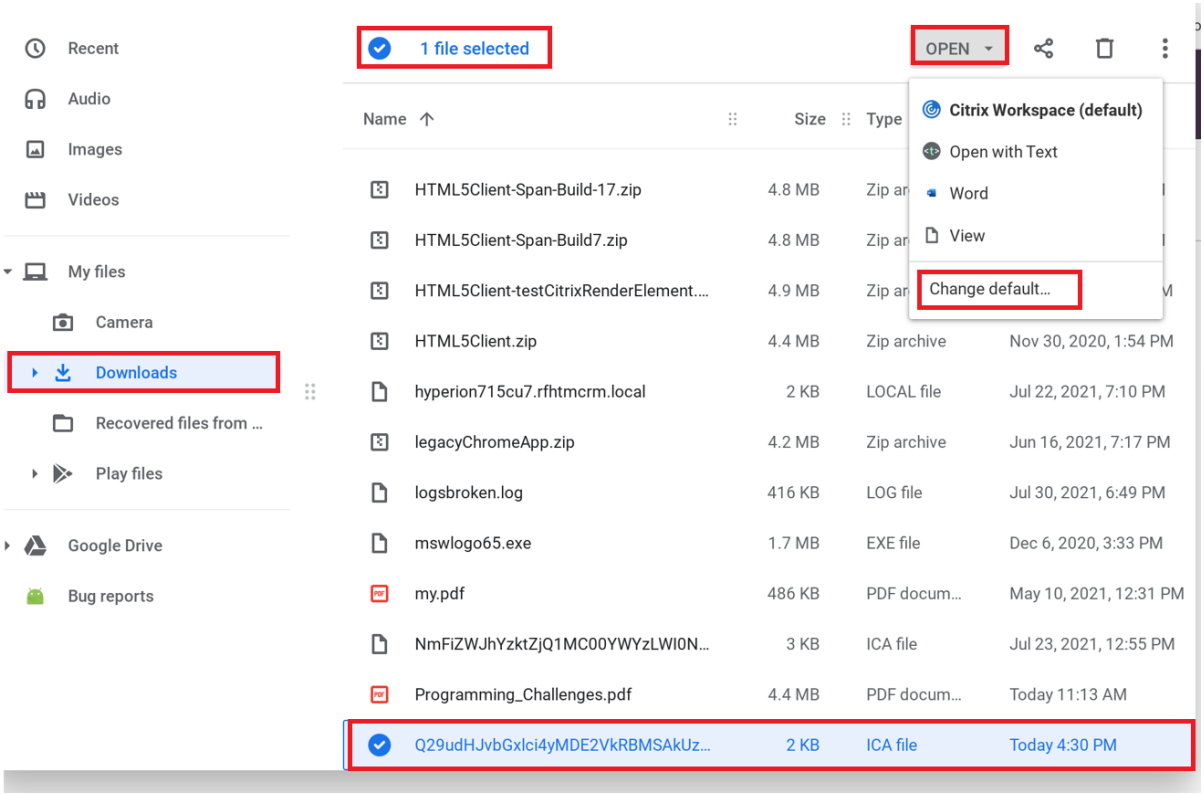
1. Log on to the **Google Admin** console.
2. In the **Google Admin** console, select **Devices > Chrome > Settings**.
3. Then, under **Settings**, select **Users & Browsers**, **Device**, and **Managed Guest Session Settings** (as appropriate), set **Auto-open downloaded files** and add **ica** under **Auto-open file types** for **User & Browser Settings**, **Device Settings**, and **Managed Guest Session Settings** as appropriate (for managed users and managed devices).



Then, ask your users to associate the ICA file with the Citrix Workspace app for ChromeOS on their ChromeOS devices as follows:

1. Open **File manager** and navigate to the previously downloaded ICA file.
2. Click the ICA file.
3. On the right side of the navigation bar, click **Open** and select the arrow beside it.
4. Then, select **Change default**.
5. A list of available apps appears.
6. Select **Citrix Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

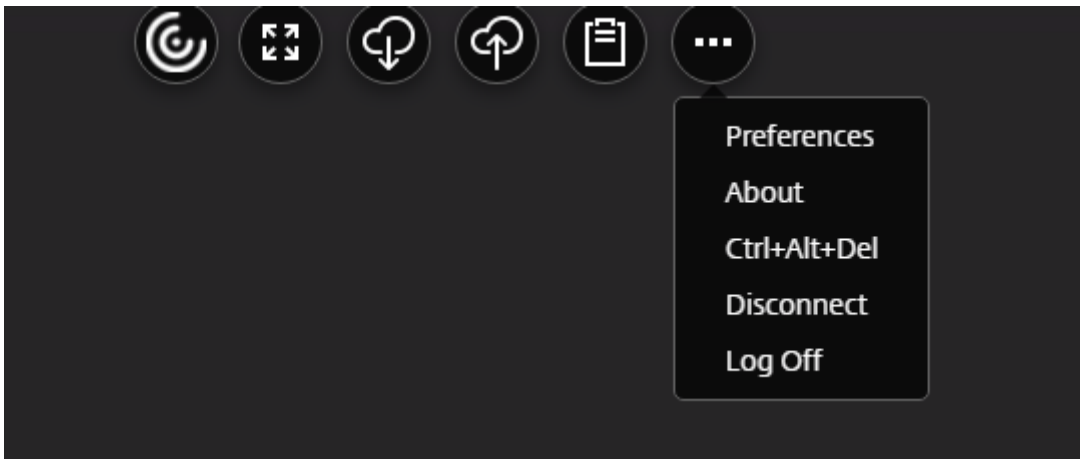


In-session toolbar and dialogs

The in-session toolbar is a floating toolbar that can be moved anywhere on the screen. The toolbar has a Citrix Workspace app icon embedded on it. A customized toolbar improves the user experience. This enhancement provides new options that are accessible from the toolbar to ease common tasks, such as:

- switching to full-screen mode
- uploading or downloading files
- Copy content from an active session to the clipboard to enable sharing between sessions
- accessing more options

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Note:**
>
> On the touch-enabled devices, the Citrix Workspace app icon appears at the top center to indicate the floating toolbar during desktop sessions. A menu button indicating the floating toolbar transforms to the Citrix Workspace icon when you move your cursor towards it.

How to configure

The toolbar is enabled by default.

To hide or customize individual toolbar items, edit the Google admin policy by including the following:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                "ui" : {

                    "toolbar" : {

                            "menubar" :true,
                            "usb": true,
                            "fileTransfer":true,
                            "about":true,
                            "lock":true,
                            "disconnect":true,
                            "logoff":true,
                            "fullscreen":true,
                            "multitouch":true,
                            "preferences":true,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                                "gestureGuide":true
                                      }

                            }

                        }

                }

        }

 }


<!--NeedCopy-->
```

List of in-session toolbar options and their descriptions:

- **menubar**: The toolbar appears when set to **true**, and is hidden when set to **false**.
- **usb**: Opens the USB devices dialog box. Contains the list of devices that can be redirected into the session. To redirect a USB device, select an appropriate device and click **Connect**.
- **fileTransfer**: Secure file transfer functionality between a user device and a Citrix Virtual Apps and Desktops and Citrix DaaS session. You can upload and download files to and from a session and seamlessly access data.
- **about**: Displays the third-party licenses page and provides the version number.
- **lock**: Sends "Ctrl+Alt+Del"to the session.
- **disconnect**: Disconnects the session.
- **logoff**: Logs off from the session.
- **fullscreen**: Adjusts the session to full-screen mode. If the session is connected with multiple monitors, the multi-monitor icon appears on the menu bar rather than a full-screen icon. A **Restore** icon appears on the menu bar while in full-screen mode. To restore maximized mode, click **Restore** in the toolbar UI.
- **multitouch**: Remotes all gestures to the virtual session, and the app behaves based on the gestures it supports.
- **preferences**: Provides options to customize CEIP and display resolution settings.
- **gestureGuide**: Provides the guide for gestures in touch mode.

To hide the toolbar configuration using the configuration.js file:

The `configuration.js` file is in the **ChromeApp root** folder. Edit this file directly to make changes to Citrix Workspace app for ChromeOS.

1. Open the configuration.js file and set the menubar attribute to false.

You can also hide an individual icon to prevent it from displaying in the toolbar. For example, to hide the Ctrl+Alt+Del button in the toolbar:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Open the configuration.js file and set the lock attribute to false.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

Session sharing

For session sharing, the applications must be hosted on the same machine and must be configured in seamless window mode with the same settings for parameters, such as window size, color depth, and encryption. Session sharing is enabled by default when a hosted application is made available.

Battery status indicator

The battery status of the device appears in the notification area within the virtual desktop session. Previously, the battery status indicator wasn't visible in the session, which sometimes led to a loss of productivity when the laptop shuts down after the battery runs out.

This feature is supported only on VDA versions 7.18 and later.

> **Note:**
>
> - With Microsoft Windows 10 VDA, the battery status indicator might take about 1 or 2 minutes to appear.

Service continuity

Service continuity removes or reduces the dependency on the availability of components that are involved in the connection process. You can launch the Citrix Virtual Apps and Desktops and Citrix DaaS regardless of the health status of the cloud services. In other words, service continuity allows you to connect to the DaaS apps and desktops during outages. As a prerequisite, your device must maintain a network connection to a resource location.

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

> **Notes:**
>
> - The service continuity feature is disabled.
> - If you previously enabled the service continuity feature and are using an older version of Citrix Workspace app for ChromeOS, you might be unable to use service continuity. To en-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> able this feature, it is recommended that you update the Citrix Workspace app to the latest version, which is 2402.1 or later and follow the instructions in the Knowledge Center article CTX632723.

Configuration

You can enable the service continuity feature in the following way:

- Google Admin Policy

Google Admin Policy For managed devices and users, administrators can enable the service continuity feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. You can apply this configuration to the following:
   - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

```
{

"settings": {

    "Value": {

        "settings_version": "1.0",
        "engine_settings": {

            "features": {

                "serviceContinuity":{

                    "enable": true
                     }

                 }

              }

          }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
23         }
24
25    }
26
27
28  <!--NeedCopy-->
```

Browser content redirection

Browser Content Redirection (BCR) redirects the remote browser's content to the client's device. BCR is a frameless-borderless web browser that runs within the remote desktop window and covers (overlays) the remote (VDA) browser's content area.

BCR redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint. Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA.

In other words, BCR provides the ability of rendering webpages in the allow list on the client side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

For more information on how to set up the allow list see:

- Browser content redirection Chrome extension
- Browser content redirection policy settings

Known issues in the feature

- On BCR overlay, when you open a website link in a new tab, it opens in the client browser instead of the session browser. [HDX-43206]

Known limitations in the feature

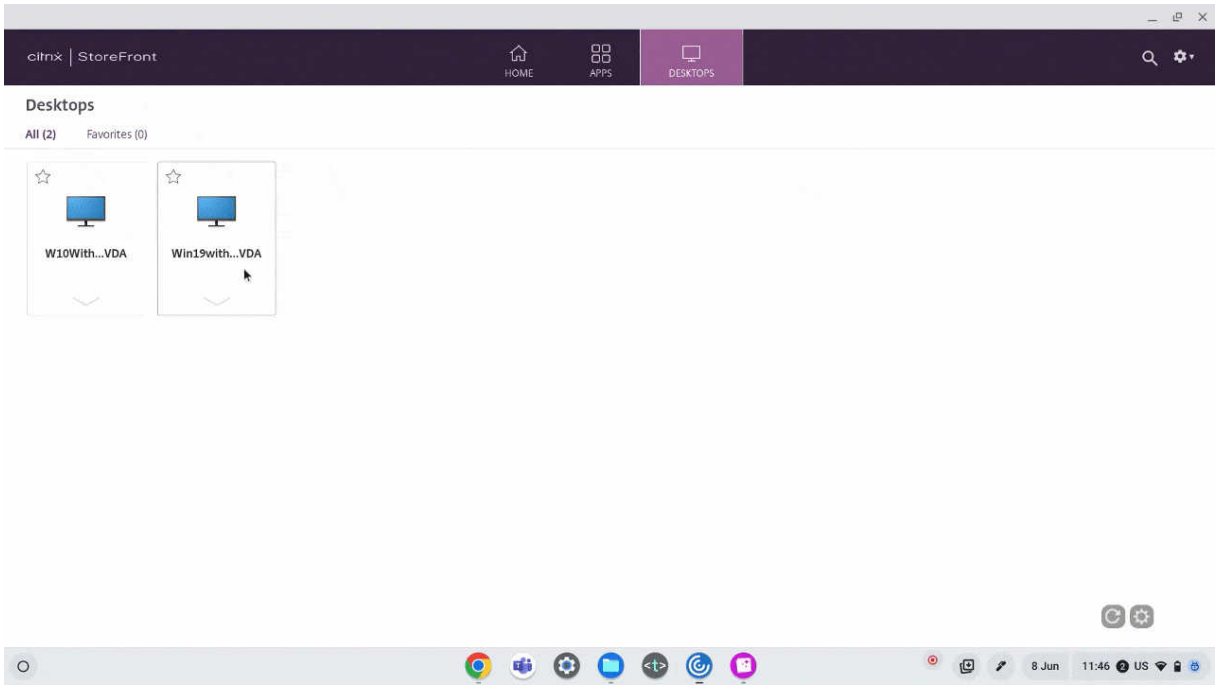
- This feature doesn't support:
  - Server fetch and client render scenario.
  - Integrated Windows Authentication (IWA) webserver.
  - Multimonitor feature.
- When you upload or download a file to some of the BCR-redirected websites, the ChromeOS file picker appears instead of a VDA session file picker. [HDX-43207]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Printing isn't supported from BCR-redirected pages.

Improved virtual apps and desktops launch experience

Starting with the 2306 release, the improved app and desktop launch experience provides timely and relevant information about the launch status.



Configure session launch notification display

Starting with 2307, administrators can either enable or disable the display of launch progress notifications using the following configuration.

If this configuration is enabled, you can see the session launch progress notifications on the lower right of the screen. If this configuration is disabled, you can't see the session launch progress notifications.

> **Note:**
>
> - By default, this configuration is enabled.

When notifications are disabled, end users lack the timely and relevant information about the launch status.

When notifications are enabled, end users see the launch progress in the lower right of the screen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurations You can configure this feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js To disable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.
2. Edit the file.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

3. Set the **CTXTUI** value to **false** to disable the display of launch progress notifications. Following is an example of JSON data:

```
{

"vc_channel":{

    "CTXTUI": false
     }

 }

<!--NeedCopy-->
```

4. Save the changes.

Google Admin Policy For managed devices and users, administrators can disable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key.

   The following is an example of JSON data:

```
{

    "settings": {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "vc_channel":

{
                      "CTXTUI": false                    }


             }

          }

     }

 }

<!--NeedCopy-->
```

4. Save the changes.

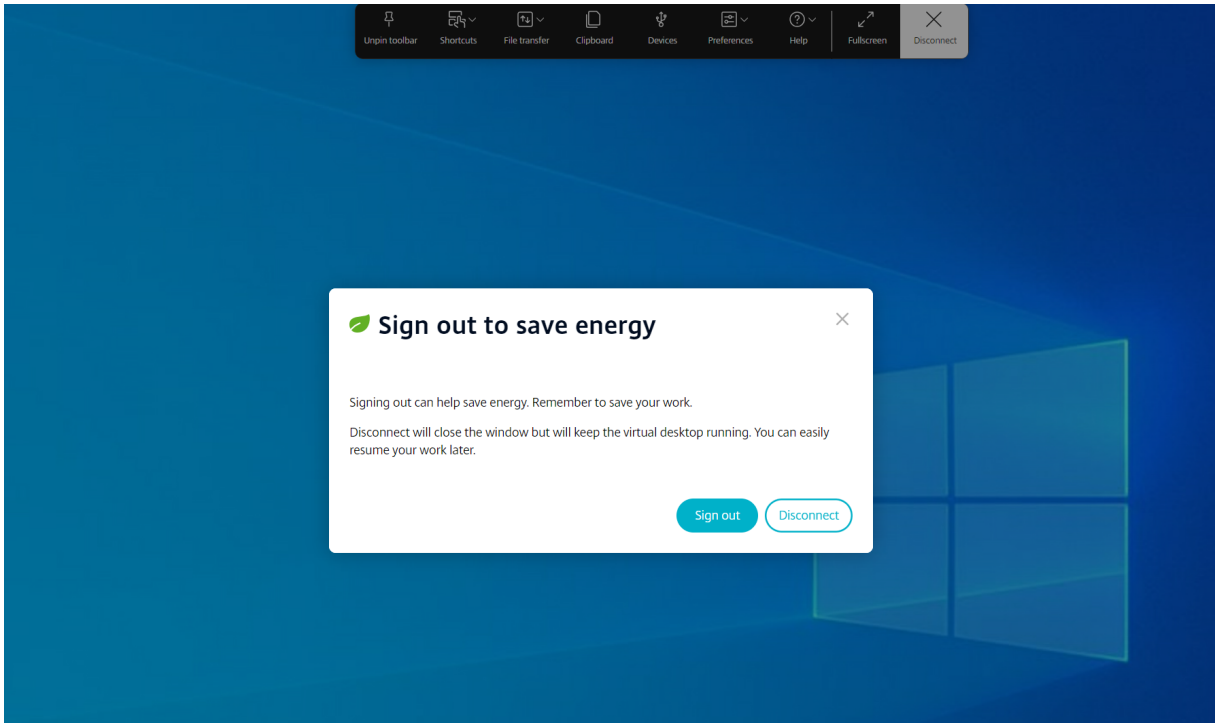
Sustainability initiative from Citrix Workspace app

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

Starting from the 2405 version, we have introduced a sustainability initiative that encourages users to conserve energy that might be used due to running unused virtual desktops.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



End users can exit from the session in two ways:

Sign out to save energy - This sustainability action shuts down the virtual machine and conserve energy. End users must make sure to save their work before signing out.

Disconnect to close the virtual desktop session window. However, the virtual session remains active until the next sign-in. End users can resume their work easily.

Store experience

April 24, 2024

Store settings

How to configure

To create a store, you identify and configure communications with the servers. You can provide the resources that you want to make available in the store. Then, optionally, you configure remote access to the store through Citrix Gateway. To configure store settings, edit the Google admin policy by including the following:

```
{
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
2
3     "settings": {
4
5         "Value": {
6
7             "settings_version": "1.0",
8             "store_settings": {
9
10                "name": "SampleStore",
11                "gateways": [{
12
13                    "url": "https: //yourcompany.gateway.com",
14                    "is_default": true
15                 }
16 ],
17                "beacons": {
18
19                    "internal": [{
20
21                        "url": "http: //yourcompany.internalwebsite.net
                              "
22                     }
23 ],
24                    "external": [{
25
26                        "url": "http: //www.yourcompany.externalwebsite
                              .com"
27                     }
28 ]
29                 }
30 ,
31                "rf_web": {
32
33                    "url": "http: //yourcompany.storefrontstoreweb.net"
34                 }
35
36             }
37
38         }
39
40     }
41
42 }
43
44
45 <!--NeedCopy-->
```

List of store setting options and their descriptions:

- “name”: Enter the Store name.
- “gateways”: Gateway URLs.

  Add gateway URLs in the format `https://gateway.domain.com` or `https://`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

yourcompany.gateway.com and click **Add** on the utility page.

You can set a default gateway if two or more gateway URLs are added.

To make a gateway the default, set the “is_default”flag to true. Otherwise, set the flag to false.

For example:

```
    {

        "settings": {

            "Value": {

            "settings_version": "1.0",
            "store_settings": {

                "name": "RTST",
                    "gateways": [{

                        "url": "https: //yourcompany.gateway.com"
                            ,
                        "is_default": true
                     }
,
                    {

                        "url": "https://gateway2.domain.com",
                        "is_default": false
                     }
]
                }

        }

    }

 }


<!--NeedCopy-->
```

- “internal”: Determines whether Citrix Workspace app connects to StoreFront directly or it connects through a gateway. For example, https://storefront.domain.com.
- “external”: Determines whether the specified network interface is available and allows traffic. For example, https://citrix.com.
- “rf_web”: Store URL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Support for multiple stores

Starting with the 2305 release, IT administrators can assign multiple stores to end users. Now, it's easy for end users to switch between multiple stores without needing to remember the exact store URL. This feature improves the user experience when accessing multiple stores.

How to configure

To configure multiple stores, IT administrators can edit the Google admin policy. The following is an example of JSON data:

```
{

      "settings_version": "1.0",
      "store_settings": {

            "name": "SampleStore",
            "gateways": [{

                  "url": " https: //yourcompany.gateway.com",
                  "is_default": true
             }
 ],
            "beacons": {

                  "internal": [{

                        "url": " http: //yourcompany.internalwebsite.
   net"
                   }
 ],
                  "external": [{

                  "url": " http: //www.yourcompany.externalwebsite.com"
                   }
 ]
             }
 ,
            "rf_web": {

                  "url": " http: //yourcompany.storefrontstoreweb.net"
             }
 ,
            "secondary_stores": [{

                  "name": " SampleStore",
                  "gateways": [{

                        "url": " https: //yourcompany.gateway.com ",
                        "is_default": true
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
39                      }
40  ],
41                     "beacons": {
42
43                          "internal": [{
44
45                           "url": " http: //yourcompany.internalwebsite.
      net "
46                            }
47  ],
48                           "external": [{
49
50                       "url": " http: //www.yourcompany.externalwebsite.
      com "
51                            }
52  ]
53                      }
54  ,
55                     "rf_web": {
56
57                     "url": " http: //yourcompany.storefrontstoreweb.net "
58                      }
59
60                }
61  , {
62
63                     "rf_web": {
64
65                     "url": " http: //yourcompany.storefrontstoreweb.net "
66                      }
67
68                }
69  ]
70          }
71
72  }
73
74  <!--NeedCopy-->
```

The attribute, **secondary_stores** allows you to configure multiple stores. An administrator can use the JSON structure multiple times. For more information on how to customize Citrix Workspace app for ChromeOS see, Configuration utility tool.

Multiple StoreFront

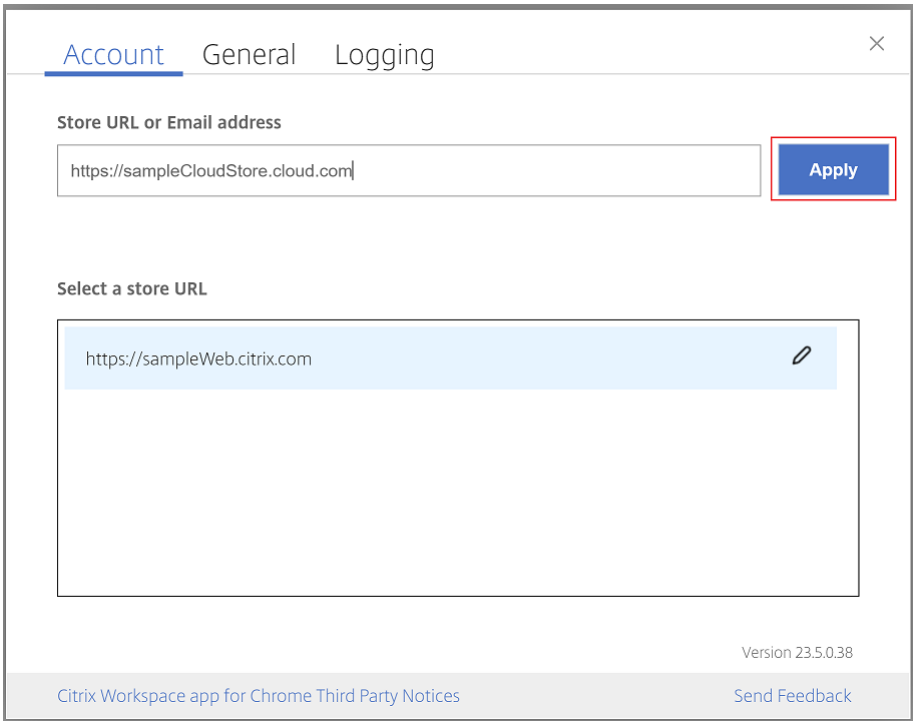
You can change the Store address without having to restart Citrix Workspace. Existing Citrix Workspace sessions, if any, continue to run uninterrupted.

To add stores:

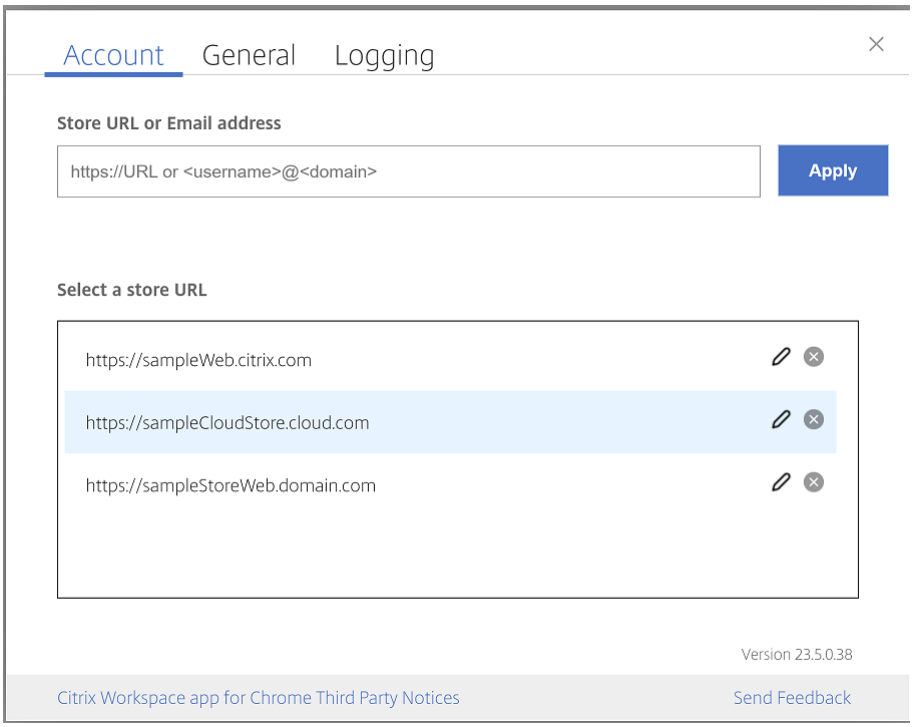
1. Click **Settings** in Citrix Workspace app for ChromeOS, and select the **Account** tab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Enter the StoreFront URL or email address in the **Store URL or Email address** field.
3. Click **Apply** to save the new store.



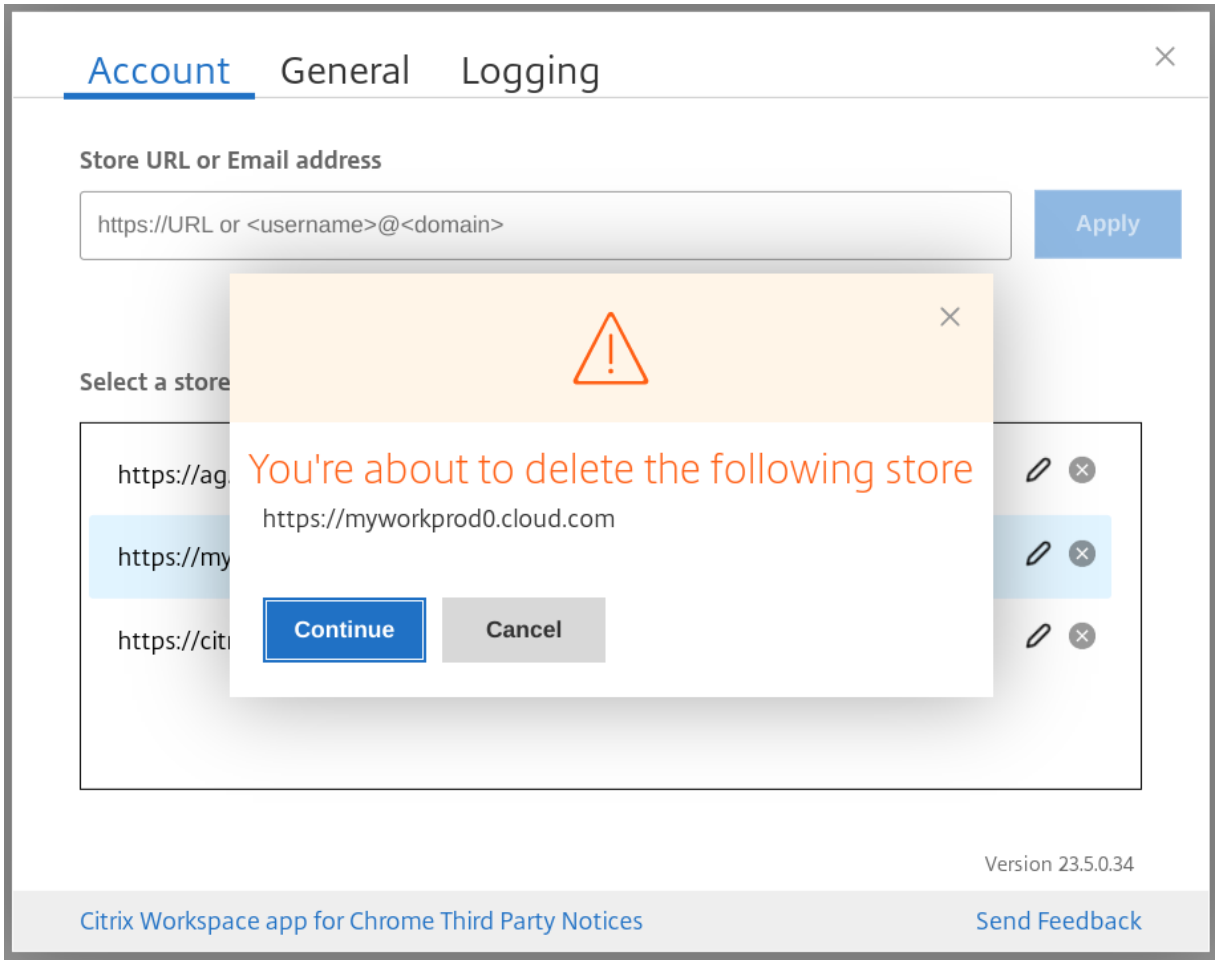
To switch stores, select a store from the **Select a store URL** list.



To delete a store from the list, click the **Delete** icon next to the store address you want to delete and

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

confirm deletion.



Reload store

In the Citrix Workspace app for ChromeOS window, a button is added for reload operation. When you click the button, the cookies of the store get cleared and the store page is reloaded.

Refresh store

Starting with the 2307 release, you can apply the following configurations to avoid duplicate instances of the published apps.

> **Note:**
>
> - By default, the configuration is disabled. When you enable this configuration, you don't see the duplicate instances of the published app. Click the icon to refresh the store.

You can configure this feature in one of the following ways:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

• Configuration.js
• Google Admin Policy

Configuration.js

To enable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp root** folder.

   > **Notes:**
   >
   > - Citrix recommends that you back up the **configuration.js** file before making changes.
   > - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
   > - Administrator-level credentials are required to edit the **configuration.js** file.

2. Edit the file and set **refreshStore** to **true**.

   The following is an example of JSON data:

   ```
   'ui' :{

     'refreshStore': true
    }

   <!--NeedCopy-->
   ```

3. Save the changes.

Google admin policy

For managed devices and users, administrators can enable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings**.

   > **Note:**
   >
   > You can apply this configuration on the following as well:
   >
   > - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   > - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> extension > Policy for extensions.

The following is an example of JSON data:

```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "ui": {

      "refreshStore": true
         }

       }

     }

    }

 }

<!--NeedCopy-->
```

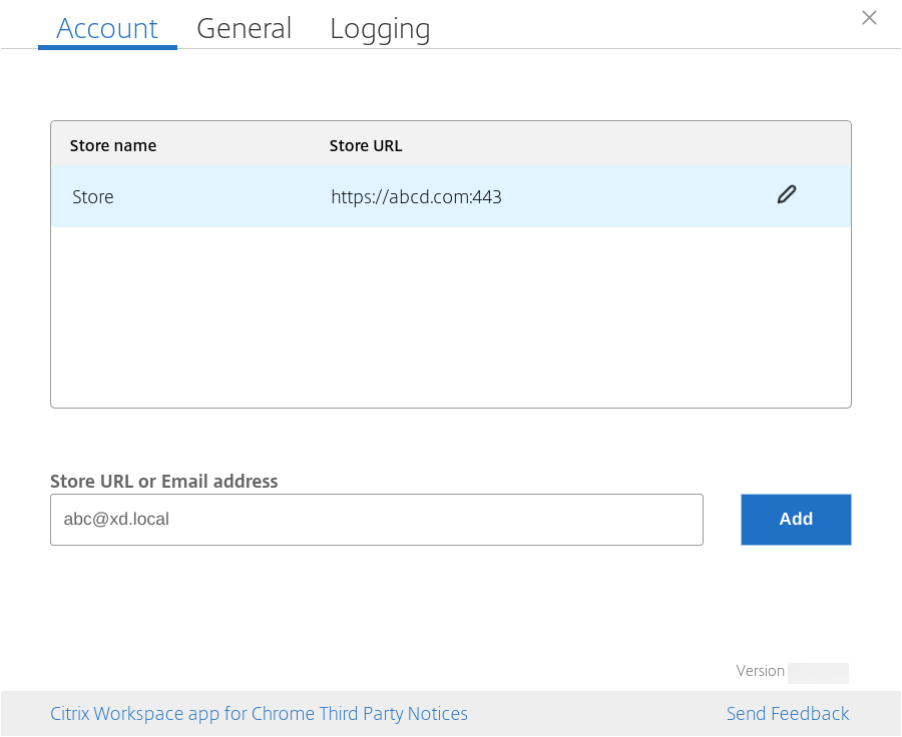
4. Save the changes.

Email-based store discovery

You can now use your email ID to access the Citrix Workspace app without the need to memorize the Store URL. The stores assigned to your account are automatically populated. Navigate to **Accounts** > **Store URL or Email address** drop-down menu to view the list of stores associated with your email.

> **Note:**
>
> You can still use the store URL to sign in.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



As an administrator, to maintain and auto-populate the store accounts, see Citrix Cloud API Overview as a prerequisite.

For more information, see Global App Configuration Service.

Short name for store URL

Previously, you were able to see the store URLs, but there was no provision to add or modify a short name for the store URLs. This arrangement made it difficult for the administrators and users to remember the store URLs.

Starting with the 2402 release, for managed users, administrators can push a custom store name along with the store URL from the Google Admin Console. This feature makes it easier for users to identify the different stores. Also, the administrator can decide if the user can edit the store name or not by setting the attribute **allowEditStoreName** to **true** or **false**. For more information, see the following configuration section.

For BYOD users, the store name is auto-generated. For example, Store, Store 1, Store 2, and so on. The stores are populated using the email-based store discovery feature. Users can edit the store name as required.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration

By default, BYOD users can edit the store name.

For managed devices and users, administrators can set the attribute **allowEditStoreName** to **true** to enable the feature using the Google Admin Console as follows.

> **Note:**
>
> - By default, the attribute **allowEditStoreName** is set to **false**.

Google Admin Policy To enable the policy, do the following:

1. Sign in to the Google Admin Console.
2. You can apply this configuration to the following as well:
   - **Device** > **Chrome** > **Apps and extensions** > **Users and browsers** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Kiosks** > Search for the extension > Policy for extensions.
   - **Device** > **Chrome** > **Apps and extensions** > **Managed guest sessions** > Search for the extension > Policy for extensions.

   The following is an example of JSON data:

```
{

"settings": {

    "Value": {

        "settings_version": "1.0",
        "store_settings": {

            "name": "Citrix store",
            "allowEditStoreName": true,
            "rf_web":
               {

                "url": "https://xyz.cloud.com"
                                                    }

                }
 ,
         }

     }

 }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
24
25 <!--NeedCopy-->
```

3. Save the changes.

> **Note**:
>
> In the code snippet, the attribute **name** refers to the short store name.

How to use the feature By default, BYOD users can edit the store name. For managed users, if your organization's administrator provides permission to edit the store name, you can. For more information, see Short name for store URL.

Touch and mobility support

April 24, 2024

Multi-touch mode

Citrix Workspace app for ChromeOS allows you to set **Multi-touch** as the default mode through the Google Admin Console. Multi-touch mode controls whether to enable multi-touch gestures.

You can toggle between Panning mode and Multi-touch mode. Earlier, panning mode was set as the default mode.

When you launch a session in a touch-enabled device, the gestures by default are handled in panning mode. You can switch to multi-touch mode using the toolbar. This feature provides a better user experience.

How to configure

To set the feature as the default, edit the **Google Admin Console** policy and set the value of **defaultMode** to **multitouch**.

```
1 {
2
3     "settings": {
4
5         "Value": {
6
7             "settings_version": "1.0",
8                         "engine_settings": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                                "ui": {

                                    "touch" : {

                                        "defaultMode" : "multitouch"
                                         }

                                    }

                                }

                            }

                        }


<!--NeedCopy-->
```

Support for Touch

Citrix Workspace app for ChromeOS now enhances touch support by allowing you to run sessions on touch-enabled Chrome devices in tablet mode. This feature includes support for gestures, multi-touch, and soft keyboard functionality.

The **Open keyboard** icon now appears on the session toolbar when a Chrome device is in tablet mode. When you use this feature or do a three-finger tap, the soft keyboard appears.

Gesture enhancements on touch devices

Starting with the 23.4.0 release, Citrix Workspace app enhances end user experience related to gestures, multi-touch, and soft keyboard functionality (Tablet mode). In your Citrix Workspace app sessions, you can use all the familiar multi-touch gestures, including the tap, swipe, and drag.

The following is the gesture guide:

To do this:	On Citrix Workspace app, do this:
Single click	One-finger tap
Right-click	Touch-hold-release
Open the on-screen keyboard	Three-finger tap (or from the toolbar, tap **Keyboard** icon)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To do this:	On Citrix Workspace app, do this:
Drag	Touch, hold, and slide
Enable cursor	Two-finger tap

Automatic Keyboard display

You can enable automatic keyboard display on a server by using the floating keyboard button that appears in an input field. For the automatic keyboard display feature to be available, verify that the server-side setting is enabled.

Feature limitations:

- Doing three fingers tap to fetch the soft keyboard does not work in multi-touch mode. It works only in panning mode.
- For the soft keyboard to work properly, always close it using the Open Keyboard icon on the session toolbar rather than the system-soft keyboard. If you close the soft keyboard using the system-soft keyboard, the soft keyboard might behave unexpectedly.

How to configure

To enable the server-side setting, complete these steps:

1. On the Delivery Controller, open Citrix Studio.
2. Select **Policies**.
3. Click **Create Policy**.
4. Search for **Automatic Keyboard Display** and select **Allowed**.

URL redirection

April 24, 2024

Host to client redirection

Content redirection allows you to control whether users access information by:

- using applications that are published on servers or

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- running applications locally on user devices.

Host to client redirection is one type of content redirection. It's supported only on Server OS VDAs (not Desktop OS VDAs) with Citrix XenApp and XenDesktop versions 7.15 LTSR and later.

For more information, see Host to client redirection - XenApp and XenDesktop in the XenApp and XenDesktop documentation.

When host to client redirection is enabled, URLs are intercepted on the server VDA and sent to the user device. Citrix Workspace app for ChromeOS displays a dialog prompting the user to select whether to open the URL within the session or on the local device. The dialog appears for every URL.

When host to client redirection is disabled, users open the URLs with web browsers or multimedia players on the server VDA. When host to client redirection is enabled, users can't disable it.

Host to client redirection was previously known as server to client redirection.

For more information, see General content redirection in the Citrix Virtual Apps and Desktops documentation.

Enhancements to URL redirection

Previously, when host-to-client redirection was enabled, URLs were intercepted on the server VDA and sent to the user's device. Citrix Workspace app for ChromeOS displayed a dialog box asking the user to select whether to open the URL within the session or on the local device. The dialog box appeared for every URL.

Starting with 2305, administrators can configure the URL redirection to open the links in the local device without extra dialog boxes. This enhancement improves the user experience.

> **Note:**
>
> - By default, this feature is disabled.

How to configure

You can enable this feature in one of the following ways:

- Configuration.js
- Google Admin Policy

Configuration.js To enable this feature using the **configuration.js** file, do the following:

1. Locate the **configuration.js** file in the **ChromeApp** root folder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Citrix recommends editing the **configuration.js** file only if the Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the **configuration.js** file.

2. Edit the **configuration.js** file and set the default value of **forceOpenInClient** to **true**. Following is an example of JSON data:

```
{

"features": {

        "UrlRedirection": {

        "forceOpenInClient": true
             }

     }

 }

<!--NeedCopy-->
```

3. Save the changes.

Google Admin Policy On the on-premises deployment, administrators can enable this feature using the Google Admin Policy as follows:

1. Sign in to the Google Admin Policy.
2. Go to **Device management** > **Chrome Management** > **User Settings**.
3. Add the following strings to the **policy.txt** file under the **engine_settings** key. Following is an example of JSON data:

```
 {

   "features": {

     "UrlRedirection": {

        "forceOpenInClient": true
                   }

             }

 }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

4. Save the changes.

Virtual channels

April 24, 2024

About Virtual channels

A virtual channel consists of a client-side virtual driver that communicates with a server-side application. Virtual channels are a necessary part of the remote computing experience with Citrix Virtual Apps and Desktops servers.

Virtual channels are used for:

- Printing
- Serial port mapping
- Clipboard
- Audio
- Multimedia
- Control channel
- EUEM
- USB
- File transfer
- Mobility
- Multi-touch
- Smart card
- Mobile receiver
- Microsoft Teams
- Input Method Editor
- Browser content redirection
- Client Drive Mapping
- Transparent User Interface

How to configure

All virtual channels are enabled by default. To disable a particular virtual channel, use the Google admin policy by including the following. Select the feature name under “vc_channel”and click **Add**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

on the utility page. For example:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                        "vc_channel": {

                            "<vc_name1>": false,
                            "<vc_name2>": false,
                            "<vc_name3>": false,
                            "<vc_namen>": false
                                        }

                                }

          }

      }

 }


<!--NeedCopy-->
```

To enable a particular “vc_channel”, select the feature and click **Remove** on the utility page.

> **Note:**
>
> The names can be from 1 to n. The last name “n”can’t have a comma after setting it to true or false.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "vc_channel": {

                        "CTXCPM ": false,
                        "CTXCAM ": false,
                        "CTXGUSB": false
                                    }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                                        }

            }

        }

 }


<!--NeedCopy-->
```

List of virtual channel options with their descriptions:

- "CTXCPM": PDF printing.
- "CTXCCM": Client serial port mapping.
- "CTXCLIP": Clipboard operations from session to VDA and from VDA to session.
- "CTXCAM": Client audio mapping.
- "CTXMM": Citrix multimedia redirection.
- "CTXCTL": Citrix control virtual channel.
- "CTXEUEM": End user experience monitoring.
- "CTXGUSB": Redirect USB devices to session.
- "CTXFILE": Secure file transfer happens between a user device and a Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session. You can upload and download files to and from a session and seamlessly access data.
- "CTXMTCH": Multi-touch remotes all gestures to the virtual session. The app behaves based on the gestures that it supports.
- "CTXSCRD": Smart card support.
- "CTXMOB": Mobile receiver virtual channel.
- "CTXMTOP": Microsoft Teams Virtual channel.
- "CTXIME": Input Method Editor.
- "CTXCSB": Browser content redirection.
- "CTXCDM": Client Drive Mapping.
- "CTXTUI": Transparent user interface.

Custom virtual channels

The virtual Channel SDK for Chrome enables third-party Chrome apps to write custom virtual channels. These channels are initialized with the app and desktop sessions that are launched using Citrix Workspace app or using the HDX SDK for Chrome.

In addition, the virtual channel SDK gives an easy way to write and receive data from the third-party Chrome app and the app and desktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

How to configure

To configure custom virtual channels, use the Google admin policy by including the following.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "customVC": [
                        {

                    "appId": "xyz",
                    "streamName": "abc"
                         }

                    ]
                 }

          }

      }

 }


<!--NeedCopy-->
```

List of CustomVC options with their descriptions:

- “appId”: ID of the chrome app that is implementing custom virtual channels.
- “streamName”: The virtual channel name.

Troubleshoot

April 24, 2024

How to collect logs

Citrix Workspace app for ChromeOS provides timestamps for the logs generated by the user device. Citrix Workspace app supports log collection for ongoing virtual desktop and app sessions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

As an end user, you can collect logs to assist with troubleshooting. Logs can be generated on both the user device and the machines. Logs can be for desktops and applications.

Previously, you can collect logs only for sessions launched after selecting **Start Logging** during an ongoing session. Now, the logs are collected for the ongoing and later sessions until you select **Stop Logging**.

To enable logging on user devices

1. On the user device, launch Citrix Workspace app and navigate to the login page.
2. Select the button with a settings image in the bottom-right corner.
3. In the **Settings** dialog, select **Start Logging**.

   Details of the collected log files are listed in the **Settings** dialog.
4. Select **Stop Logging** to end the collection of logs on the user device.

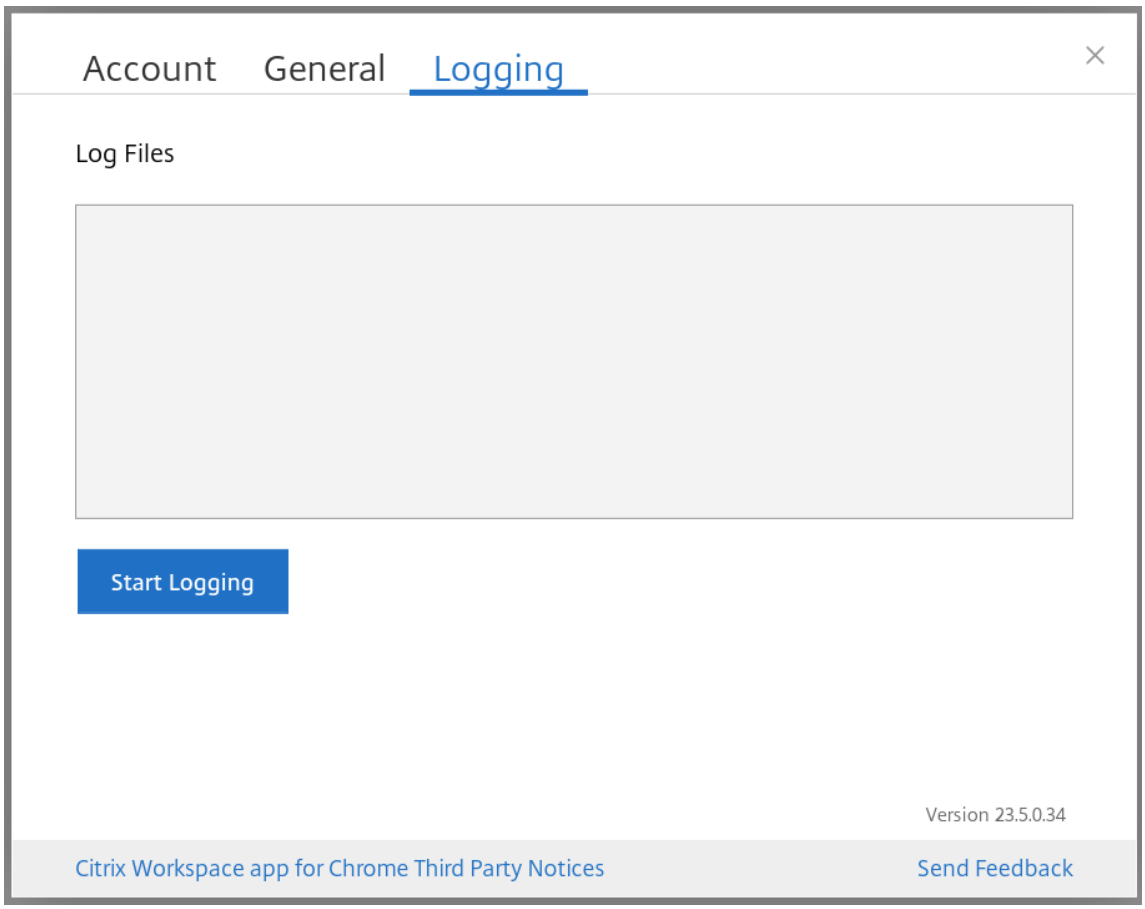
Client logs

> **Note:**
>
> - Starting with the 2207 release, the console logs are a part of the client logs.

1. Click the **Settings** button on the bottom right of the Citrix Workspace app **Sign In** screen.

2. Click the **Start Logging** button under **Logging** to enable collection of logs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

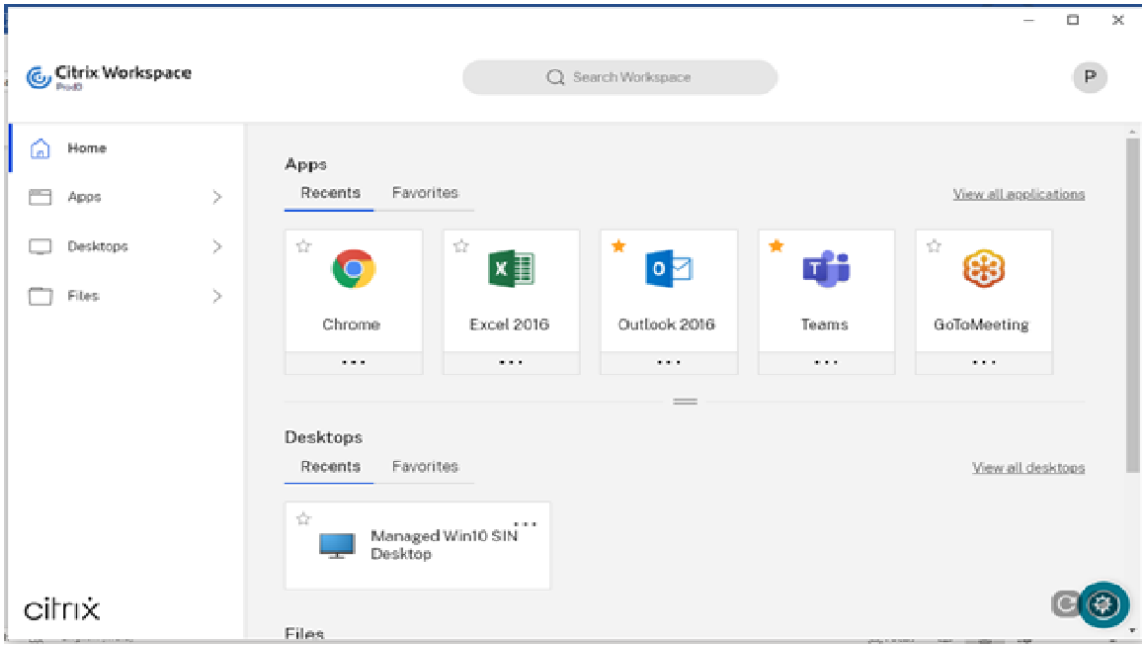


3. The **Start Logging** button changes to **Stop Logging**. This change indicates that collection of logs is enabled.

   Close the **Account** dialog box.

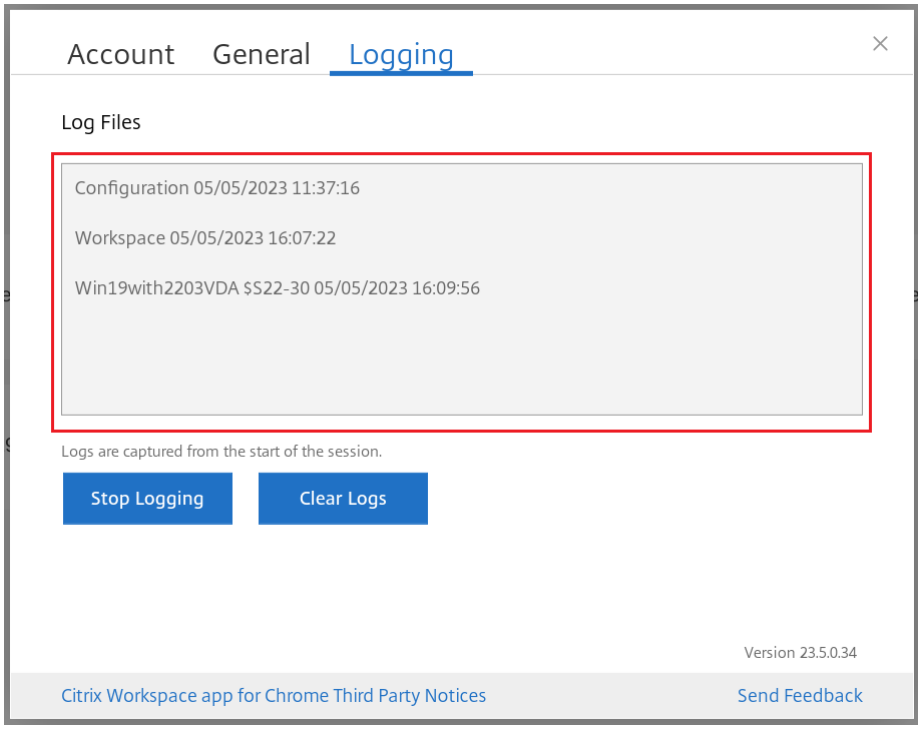
4. Sign into the Citrix Workspace app virtual desktop and launch your virtual app session and reproduce the issue to collect logs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Continue to work on the session to reproduce the issue.

5. Once the issue is reproduced, close the session.
6. Click the **Settings** button again to open the **Account** dialog box.
7. Select the **Logging** tab.
8. The **Logging** dialog box shows the list of **Log Files** captured.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. Moving the mouse on top of any of the Log files shows a small arrow at the right.

10. Click the arrow button to download and save the Log file.
11. Save all the log files listed under **Log files** and share it with the administrator or Citrix support engineer.
12. Click **Stop Logging**.

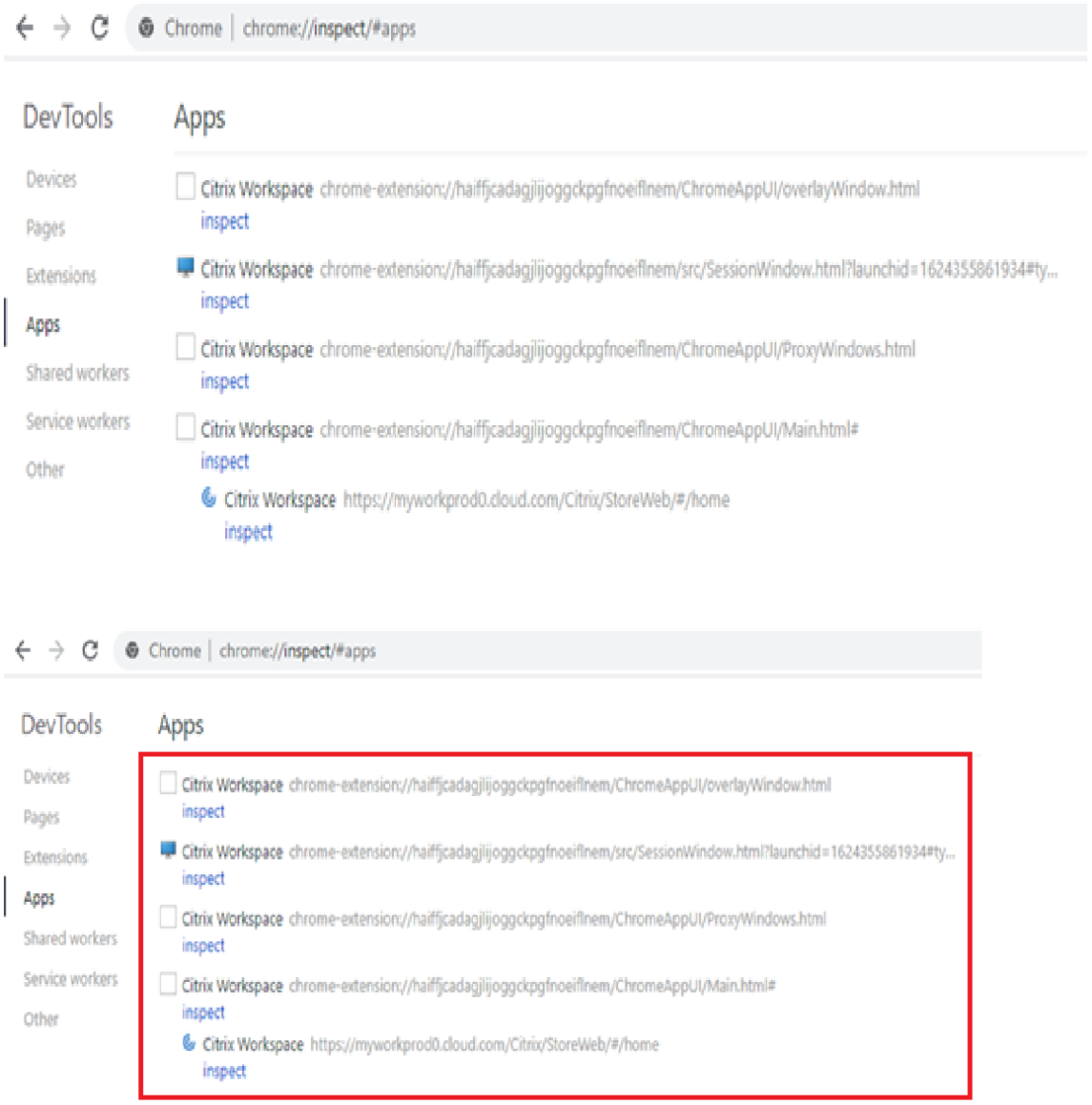
> **Note:**
>
> In Kiosk mode, files can be saved to a USB removable device.

Console logs

> **Note:**
>
> - Starting with the version 2207 and later, the console logs are a part of the client logs. Hence, collecting the client logs alone can suffice.

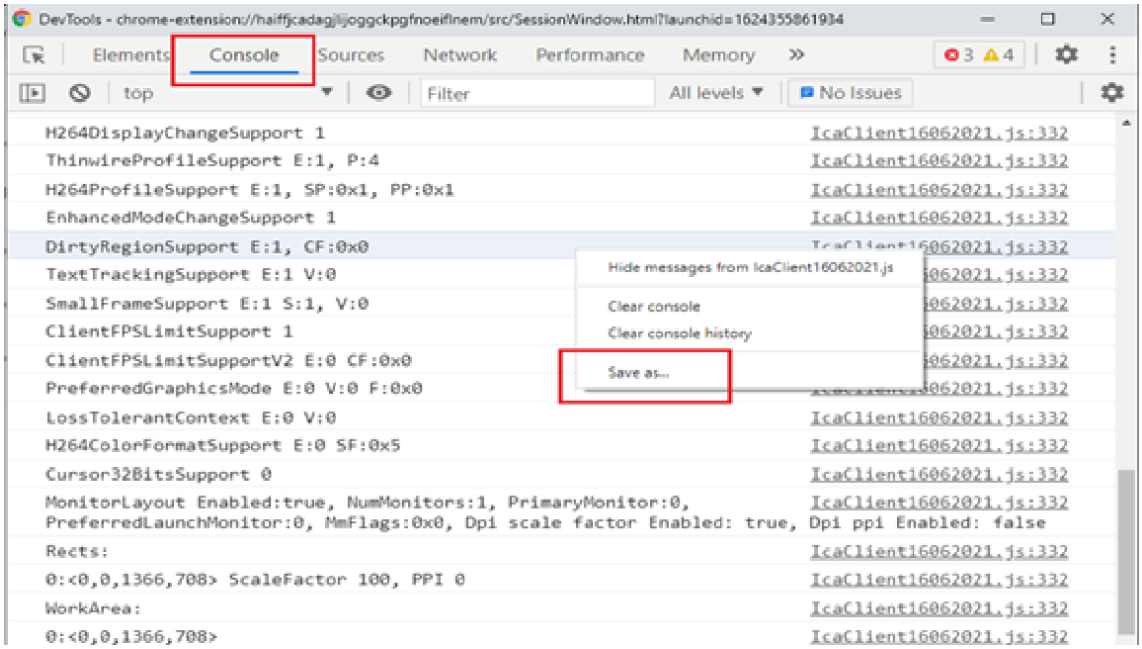
1. Open the **chrome://inspect/#apps** page in the Google Chrome browser of your Citrix Workspace app.
2. In the **Apps** tab, click **inspect** for all Citrix Workspace-related windows: SessionWindow.html, Main.html (and its child nodes).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. For each opened developer tool window, click **Console**. Then, save the entire log by right-clicking and selecting the **Save as** option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



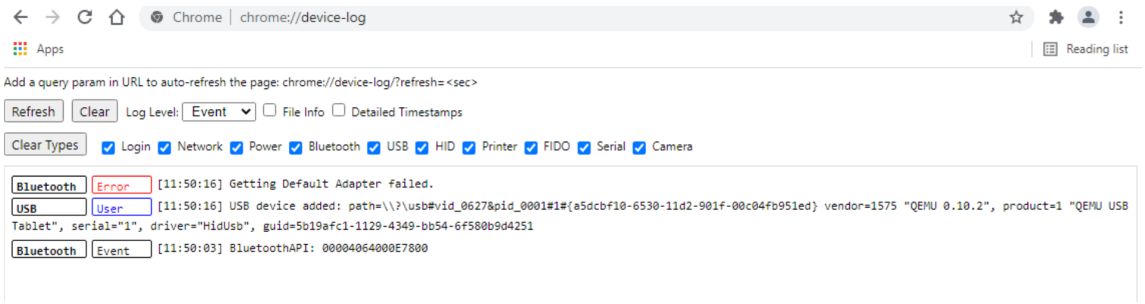
USB redirection logs

1. Follow the steps in Using Web.config for ChromeOS and enable moreLogs for USB by:

   Adding the moreLogs configuration value to chromeAppPreferences in the web.config file on the StoreFront:

   ```
   chromeAppPreferences ='{ "moreLogs":{ "usb":true } } '
   ```

2. Then, open a new tab in the Google Chrome browser and enter **chrome://device-log** and share the logs.



File transfer logs

The file transfer logs can be retrieved from both the client and the server.

To retrieve file transfer logs from the client:

1. Launch a browser.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Go to the following URL to start logging:
   <storefronturl>/clients/html5client/src/viewlog.html
   where <*storefronturl*> is the FQDN or IP address of the StoreFront server where the store is configured.

For more information on file transfer, see HTML5 and Chrome File Transfer Explained.

Microsoft Teams optimization logs

Microsoft Teams optimization supports the latest shim library version 1.8.0.12.

To know the current shim version that you use:

1. Launch the Microsoft Teams application and initiate a call with one of the users.
2. Maximize the Microsoft Teams window after the call is established.
3. Open the **On-screen keyboard** inside the session and click the **Ctrl + Alt + Shift + 1** keys.
   You can now view the log files under the downloads folder.
4. Open the `MSTeams Diagnostics Log <date><time>_vdi partner.txt` file and search for the shim version under **type_script**.
   Compare the shim version with 1.8.0.12.
5. (Optional) If the shim version isn't 1.8.0.12, contact your administrator to upgrade to the latest version.

Client logs in kiosk mode

To collect the logs in kiosk mode:

1. Connect a removable USB device to your Chromebook.
2. Download the log file.
3. Save the log file in the attached USB device.

   The log file is transferred to the USB device.

Shortcuts

- The keyboard shortcut Ctrl+ Alt + Shift +1 might not work in optimized Microsoft Teams within a virtual desktop. As a workaround, open the **On-Screen Keyboard** and use the shortcut. [RFHTMCRM-5441]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration utility tool

April 22, 2024

There are four options to customize Citrix Workspace app for ChromeOS:

- configuration.js
- web.config
- default.ica
- Google Policy

The four options are available on the configuration utility, which is a UI-based configuration web-page.

Download the Configuration utility tool from the Downloads page.

How to use the configuration utility tool

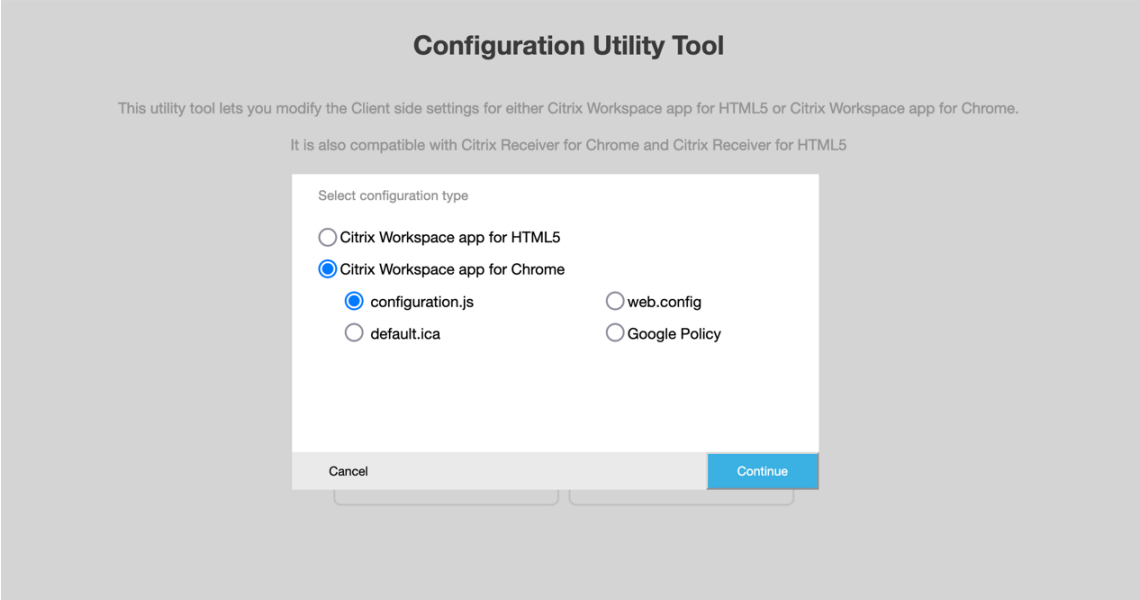
1. Click **Creat New.**
2. Select **Citrix Workspace app for Chrome** and choose one of the four configuration options. Then, click **Continue** to move ahead or Click **Cancel** to go back to the home page.

For configuration.js

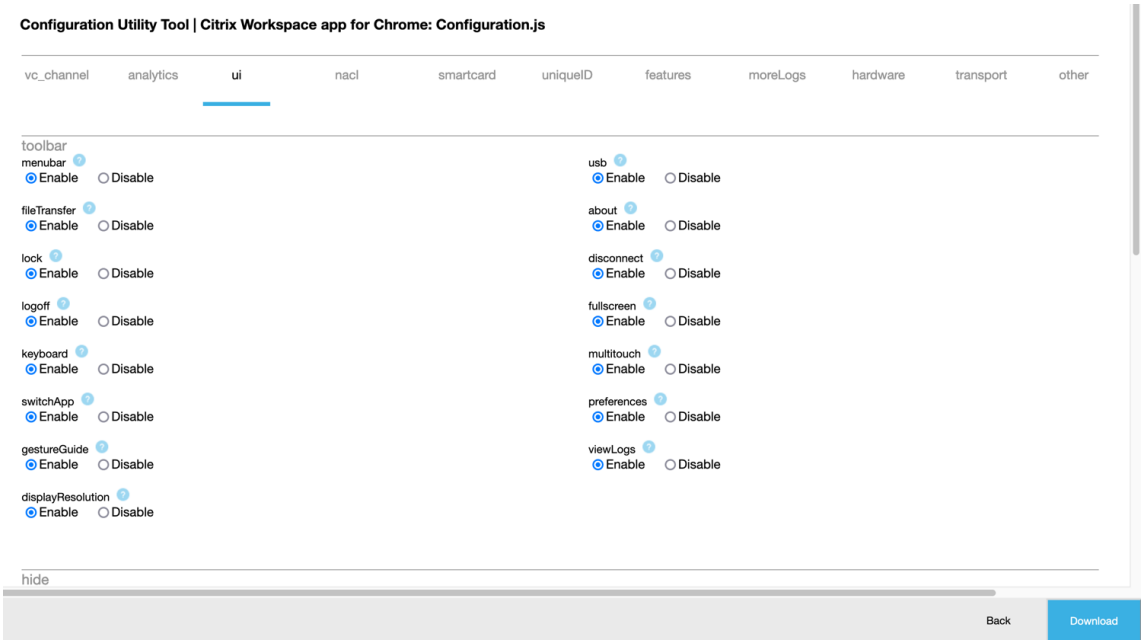
To create a configuration,

1. After selecting **configuration.js**, click **Continue** to configure or click **Cancel** to go back to the home page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. On the **Configuration Utility Tool**, select the features you want and choose their appropriate values.

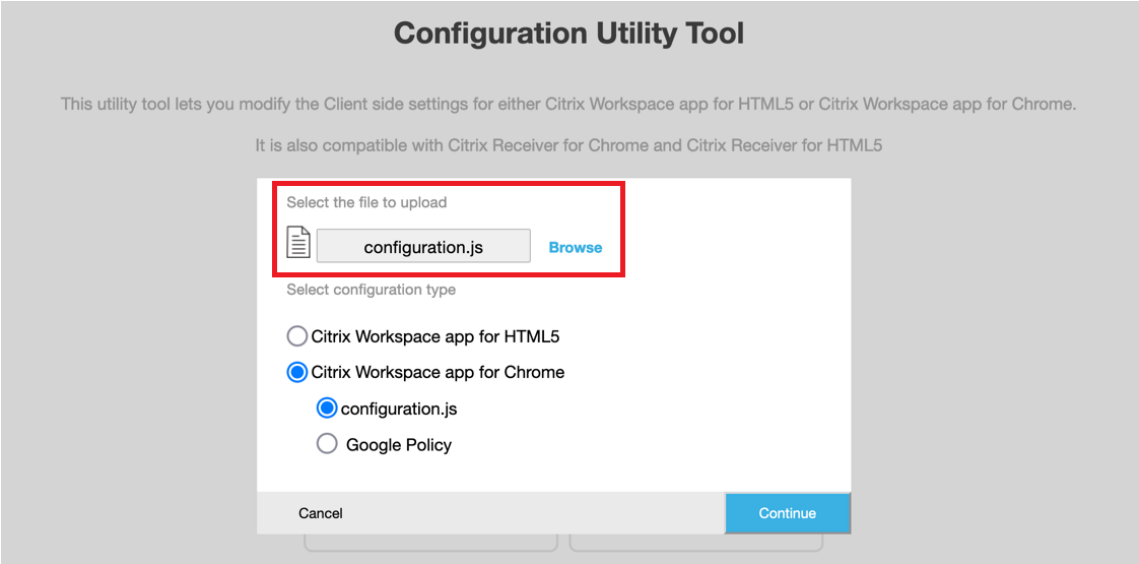


3. Click **Download** to download the configuration.js file.

To edit a configuration,

1. Click **Upload existing file.**
2. Select **Citrix Workspace app for Chrome** and select **configuration.js.**
3. Click **Browse** and navigate to the location of the configuration.js file to select and upload the file.

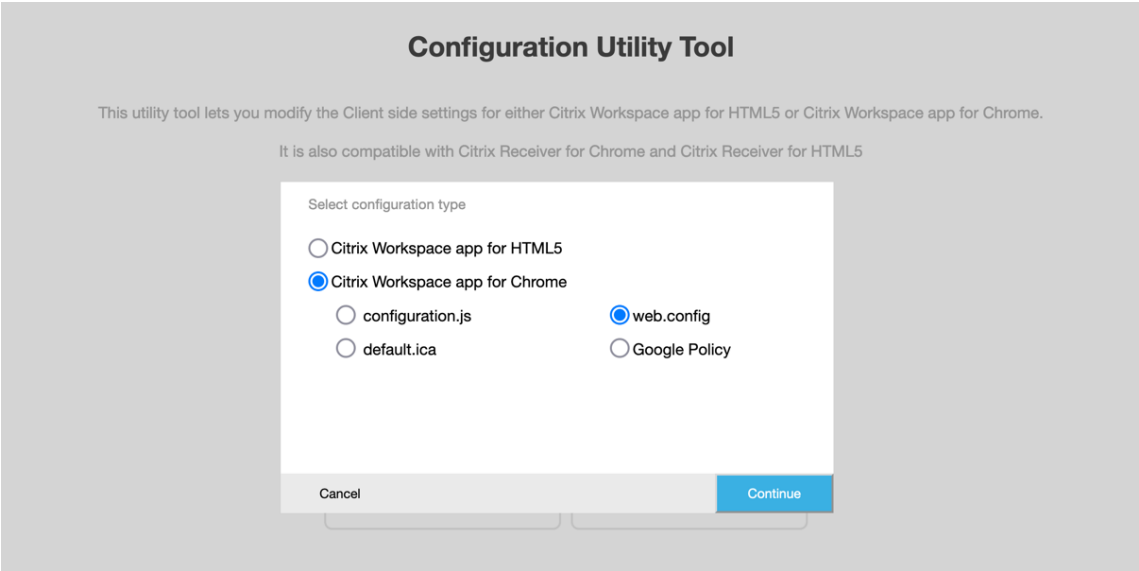
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Click **Continue** to configure or **Cancel** to go back to the home page.
5. Select the features that you want and choose their appropriate values.
6. Click **Download** to download the configuration.js file.

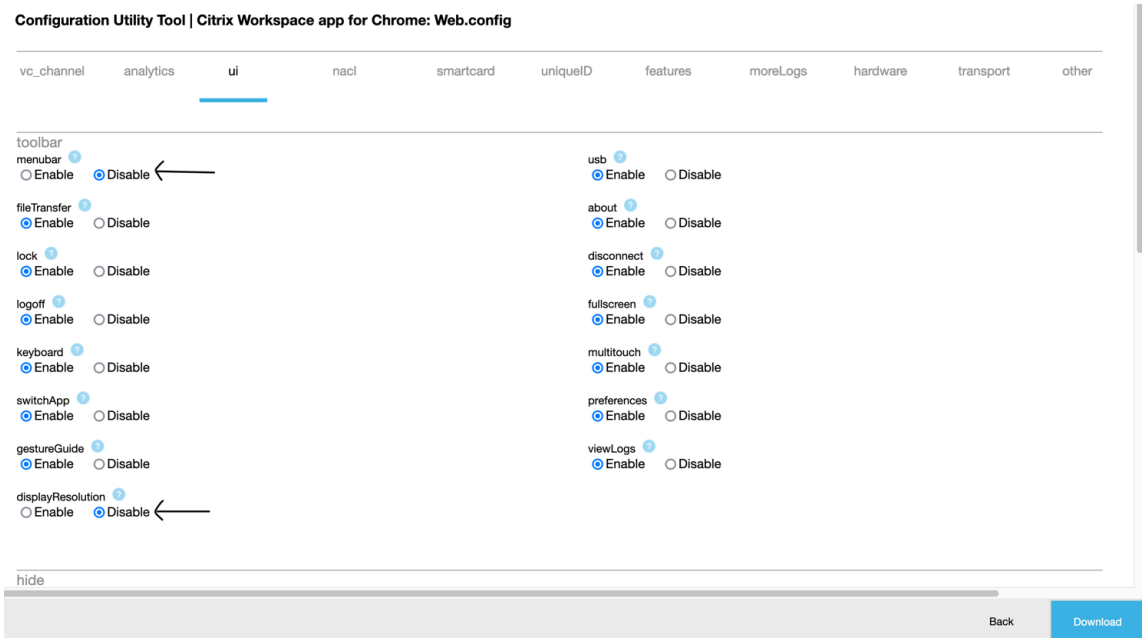
For web.config (in StoreFront)

1. After selecting **web.config**, click **Continue** to configure or click **Cancel** to go back to the home page.

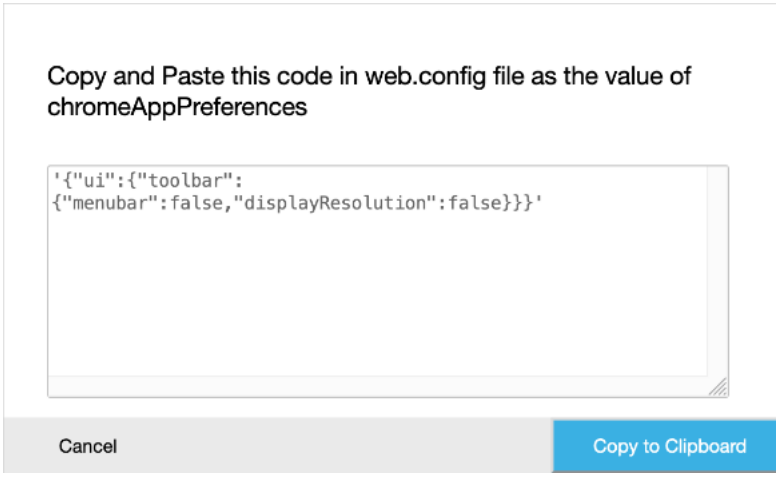


2. Select the settings that you want and their appropriate values and click **Download** (for example, select menubar: disable; displayResolution : disable)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Copy the contents in the dialog box.



4. Open the web.config file for the Citrix Receiver for Web Site. This file is typically at **C:\inetpub\wwwroot\Citrix\storenameWeb**, where a store name is the name specified for the store when it was created.
5. Locate the chromeAppPreferences field in the file and set its value with the JSON string copied from the dialog box.

```
chromeAppPreferences = '{

    "ui":{

        "toolbar":{

            "menubar":false,"displayResolution":false
             }
```

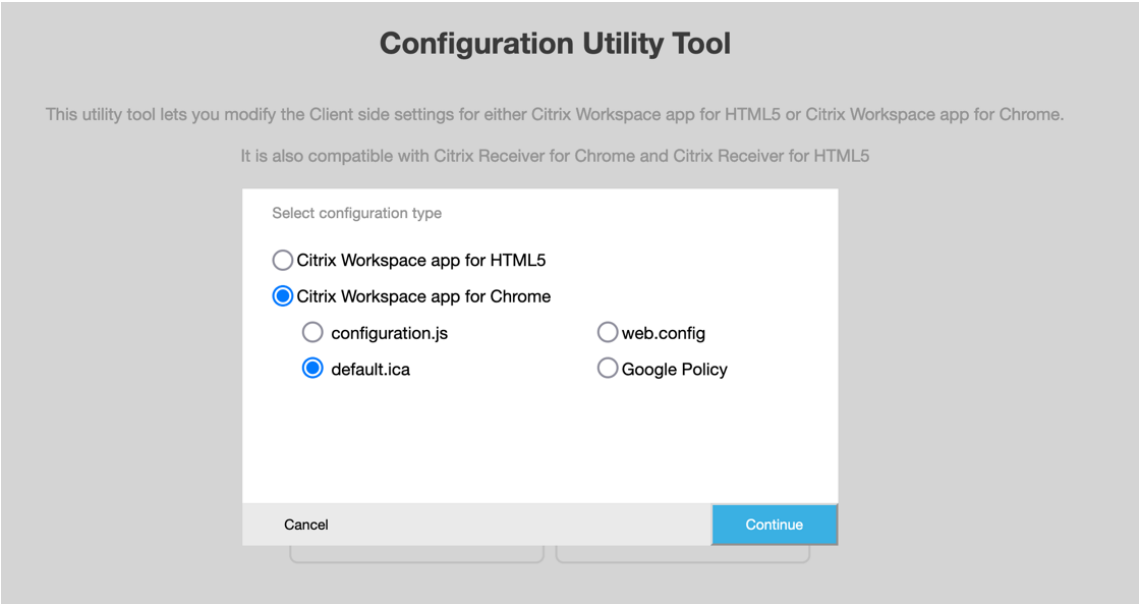
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                        }

                        }
 '
<!--NeedCopy-->
```

```
web.config  default.ica
    <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
  </serverSettings>
  <clientSettings>
    <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
      changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
      loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
      webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
    <storeProxy keepAliveURL="Home/KeepAlive">
      <resourcesProxy listURL="Resources/List" resourceDetails="default" />
      <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
        logoffURL="Sessions/Logoff" />
      <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
        getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
    </storeProxy>
    <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
      <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
      <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
        minimumSupportedOSVersion="10.6" />
      <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9]|\d\d).*Safari;MSIE \d\d;Tri
        launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
        singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflne
        chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}' />
      <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*((Firefox/((5[2-9]|[6789][0
        skipDoubleHopCheckWhenDisabled="false" />
    </pluginAssistant>
```

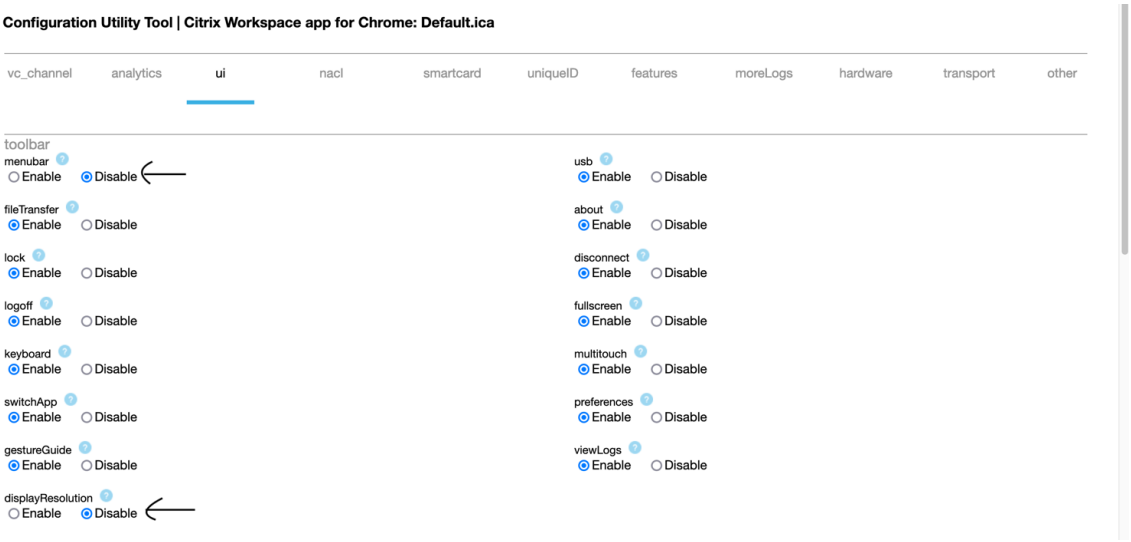
For default.ica

1. After selecting **default.ica**, click **Continue** to configure or click **Cancel** to go back to the home page.

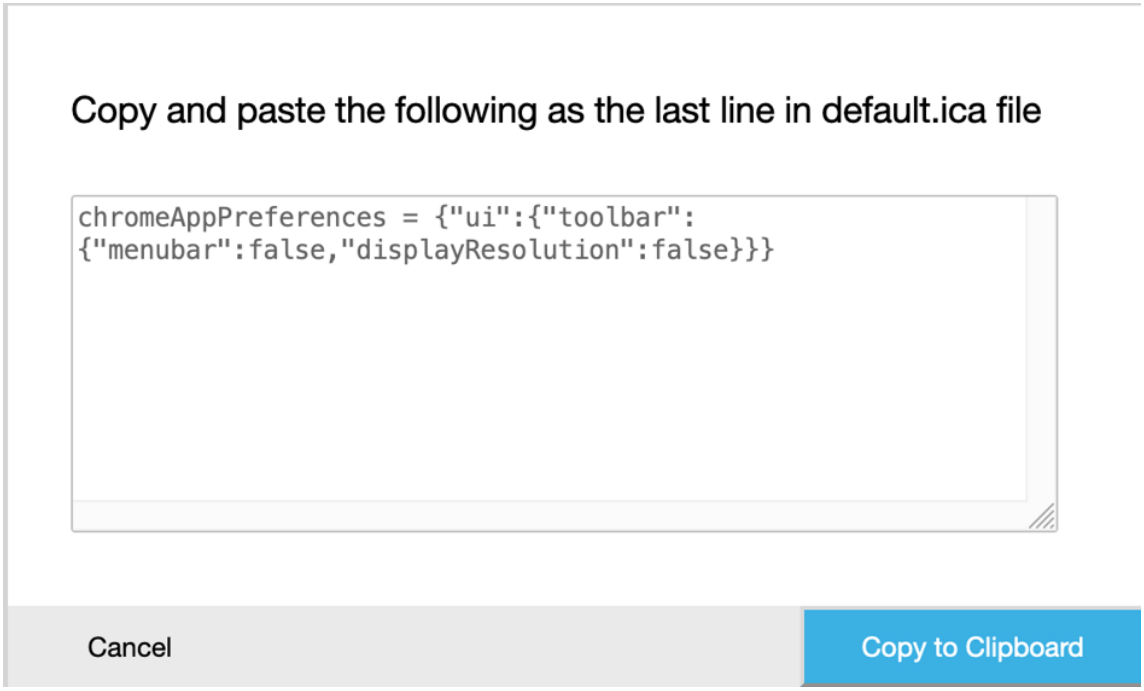


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Select the settings that you want and their appropriate values and click **Download** (for example, select **menubar** > **disable** and **displayResolution** > **disable**).

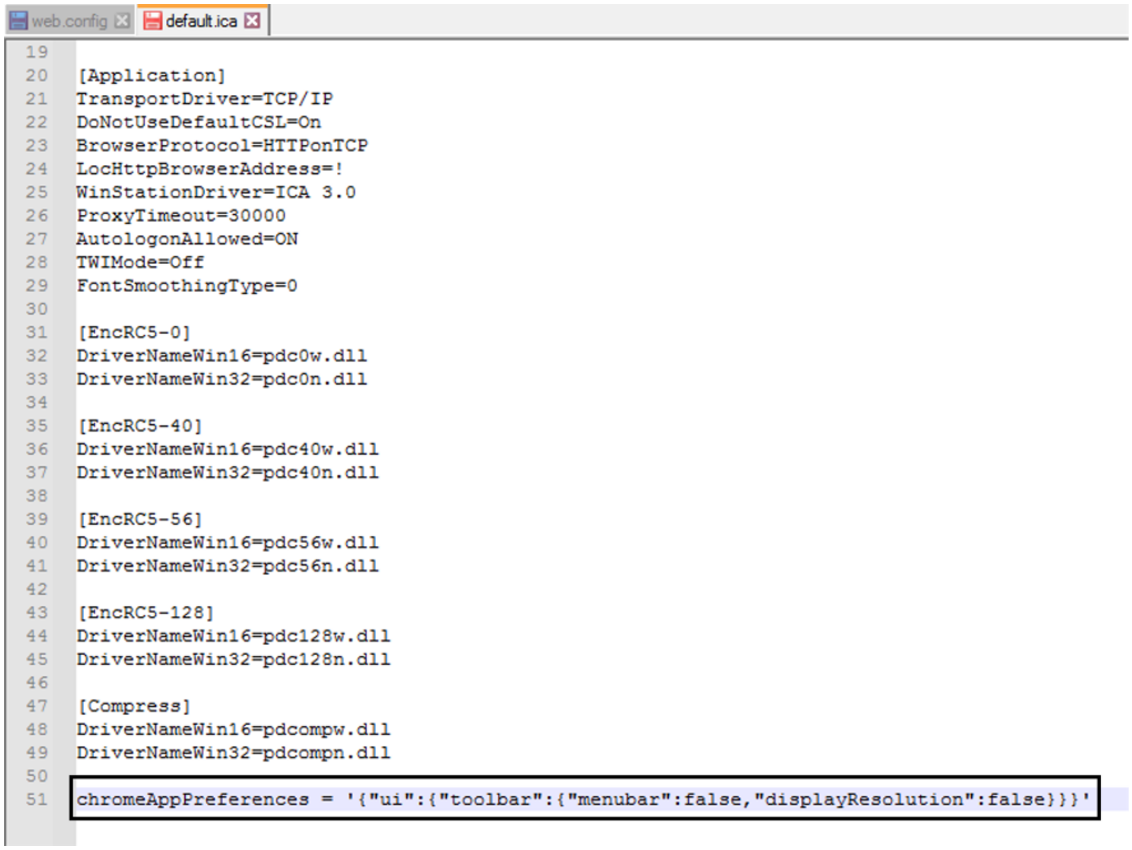


3. Copy the contents in the dialog box.



4. Open the default.ica file typically at **C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica** for Web interface customers, where the sitename is the name specified for the site when it was created. For StoreFront customers, the default.ica file is typically at **C:\inetpub\wwwroot\Citrix\<Storenam** where a store name is the name specified for the store when it was created.
5. Add the content in the last line of the default.ica file as shown.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

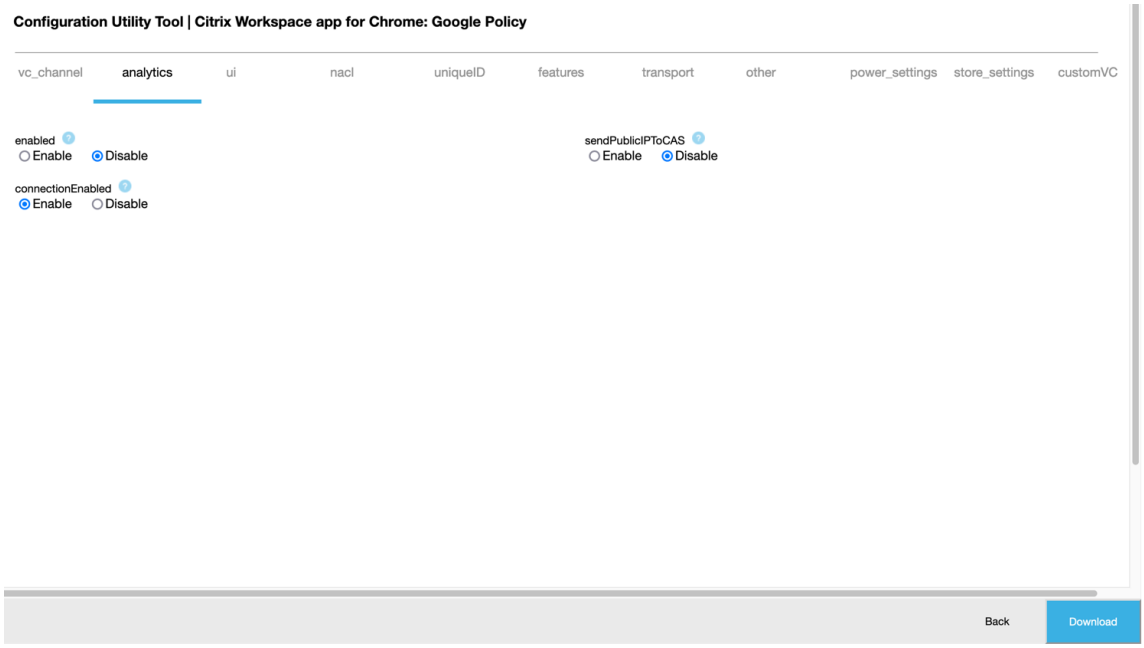


For Google policy

How to create a configuration

1. After selecting **Google Policy**, click **Continue** to configure or click **Cancel** to go back to the home page.
2. Select the settings that you want and their appropriate values and click **Download** (for example, select sendPublicIPToCas: disabled)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



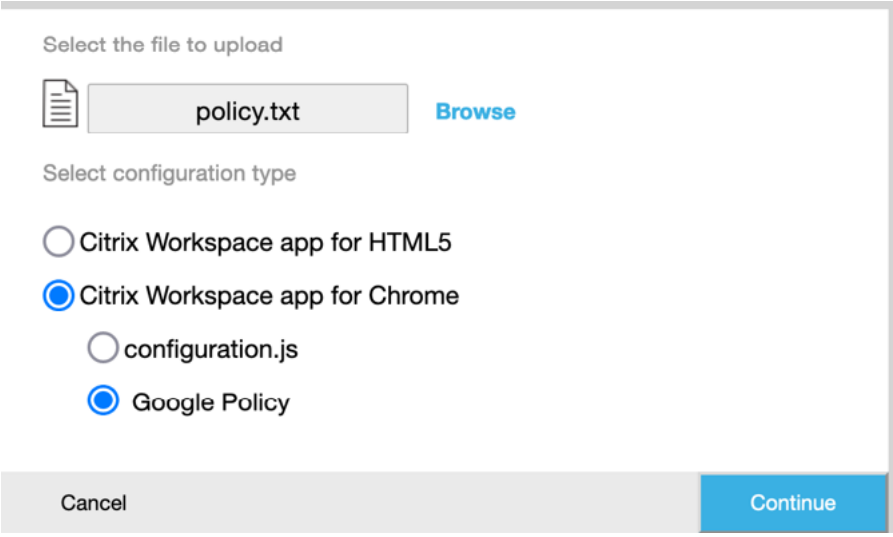
3. When you click **Download**, a **policy.txt** file is created.

How to edit a configuration

> **Feature limitation:**
>
> You can edit only the settings and the values that are present in the upload file (**policy.txt**). If you require to edit other policies, create a policy file to include the settings. For more information, see How to create a configuration.

1. Click **Upload existing file.**
2. Select **Citrix Workspace app for Chrome** and select **policy.txt**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Click **Browse** and navigate to the location of the **policy.txt** file to select and upload the file.
4. Click **Continue** to edit or click **Cancel** to go back to the home page.
5. Edit the settings by choosing their appropriate values.
6. Click **Download** to download the updated **policy.txt** file.

Authenticate

May 23, 2024

Smart card

Citrix Workspace app for ChromeOS supports USB smart card readers with StoreFront. You can use smart cards for the following purposes:

- Smart card sign-in authentication to Citrix Workspace app.
- Smart card-aware published apps to access local smart card devices.
- Smart cards for signing documents and email. For example, Microsoft Word and Outlook that are launched in ICA sessions.

Supported smart cards (with USB smart card readers) include:

- Personal Identity Verification (PIV)
- Common Access Cards (CAC)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prerequisites

- StoreFront versions 3.6 or later
- XenDesktop 7.6 or later
- XenApp 6.5 or later
- Citrix Virtual Apps and Desktops 1808 or later
- Citrix Workspace app 1808 or later

> **Important:**
>
> - For smart card authentication to StoreFront 3.5 and earlier, you require a custom script to enable smart card authentication. Contact Citrix Support for assistance.
> - To access the latest information on supported versions, see lifecycle milestones for Citrix Workspace app and Citrix Virtual Apps and Desktops.

Device configuration prerequisites

- Google Smart Card Connector is an app that interacts with the USB smart card readers on the device. The connector app reveals Personal Computer Smart Card (PCSC) Lite APIs to other apps including the Citrix Workspace app.
- Certificate providers are the middleware apps written by vendors that interact with the smart card connector. The middleware apps access the smart card reader, read certificates, and provide smart card certificates to ChromeOS.

  The middleware apps also implement signing functionality using PIN prompts.
  For example, CACKey.

  For more information, see Deploy Smartcards on ChromeOS.
- When you configure smart card authentication on StoreFront, Citrix Workspace app requests ChromeOS to provide client certificates on the smart card. ChromeOS presents the certificates as received from the providers. PIN prompts indicate authentication.

  Citrix Workspace app has an approved list of allowed operating systems for smart card authentication. StoreFront 3.6 and later approve the ChromeOS as well. For earlier versions of StoreFront, you can use a custom script to allow smart card authentication on ChromeOS. Contact Citrix support for custom script.
- Citrix Workspace app doesn't control the smart card authentication workflow with StoreFront. However, in a few cases StoreFront can request you to close the browser to clear cookies.

  To clear all the cookies and load the Store URL again, click the reload button in Citrix Workspace app for ChromeOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

At times, to clear cookies furthermore, you can sign out from the ChromeOS device.

- When you try to launch an app or a desktop session, Citrix Workspace app doesn't use smart card redirection. Instead, it interacts with the smart card connector app for PC/SC lite APIs.

  PIN prompts required for Windows sign-in appear within the session. Here, the Certificate providers have no role. Citrix Workspace app manages the in-session activities like double hop or signing email.

Smart Card limitations

- When you remove the smart card from the ChromeOS device, the smart card certificate is cached. The behavior is a known issue that exists in Google Chrome. Restart the ChromeOS device to clear the cache.
- When Citrix Workspace app for ChromeOS is repackaged, as an administrator, get the appID approval by Google. Doing so confirms that the smart card connector application passes through.
- Only one smart card reader is supported at a time.
- Virtual smart cards and fast-smart cards aren't supported.
- Smart cards aren't supported on Citrix Workspace (cloud).

To configure smart card support on your ChromeOS device

1. Install the smart card connector application. The smart card application is required for Personal Computer Smart Card (PCSC) support on the ChromeOS device. This application reads the smart card using the USB interface. You can install this application from the Chrome website.
2. Install the middleware application. A middleware application is required as an interface that communicates with the smart card and the other client certificates. For example, Charismathics or CACKey:

   - To install the Charismathics smart card extension or CACKey, see the instructions on the Chrome website.
   - For more information about middleware applications and smart card authentication, see the Google support site.

3. Configure smart card authentication using:

   - Citrix Gateway
   - StoreFront Management Console

   For information, see Configuring Smart Card Authentication and Configure the Authentication Service in the Citrix Gateway documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SAML authentication

To configure a single sign-on:

1. Set up the third-party Identity provider (IdP) for SAML authentication if it isn't already configured. For example, ADFS 2.0.

   For more information, see Knowledge Center article CTX133919.

2. Set up single sign-on with Google Apps using SAML IdP. The configuration enables users to apply a third-party identity to use Google apps instead of the Google Enterprise account.

   For more information, see Set-up single sign-on for managed Google Accounts using third-party Identity providers on Google support.

3. Configure Chrome devices to sign in through SAML IdP. The configuration enables users to sign in to Chrome devices using a third-party identity provider.

   For more information, see Configure SAML Single Sign-On for Chrome devices on Google support.

4. Configure Citrix Gateway to sign in through SAML IdP. The configuration enables users to sign in to Citrix Gateway using a third-party identity provider.

   For more information, see Configuring SAML Authentication.

5. Configure Citrix Virtual Apps and Desktops for Federated Authentication to sign in to Citrix Virtual Apps and Desktops sessions using dynamically generated certificates. You can do the action after the SAML sign-in instead of typing the user name and password combinations.

   For more information, see Federated Authentication Service.

   To achieve SSO for virtual apps and desktops, you must deploy a Federated Authentication Service (FAS).

   > **Note:**
   >
   > Without FAS, you're prompted for the Active Directory user name and password. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

6. Install and configure SAML SSO for the Chrome app extension on Chrome devices. For more information, see the Google website. This extension retrieves SAML cookies from the browser and provides them to Citrix Workspace. This extension must be configured with the following policy to allow Citrix Workspace to get SAML cookies.

   If you're repackaging Citrix Workspace app for ChromeOS, change the appId correctly. Also, change the domain to your company's SAML IdP domain.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
{

    "whitelist" : {

        "Value" : [
            {

            "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain" : "saml.yourcompany.com"
             }

        ]
      }

 }

<!--NeedCopy-->
```

7. Configure Citrix Workspace to use the Citrix Gateway configured for SAML sign-in. The configuration enables users to use the Citrix Gateway configured for SAML sign-in. For more information on ChromeOS configuration, see Knowledge Center article CTX141844.

Single sign-on for Citrix Workspace app using Okta as the IdP

April 24, 2024

You can configure the single sign-on (SSO) to Citrix Workspace app using Okta as the identity provider (IdP).

Prerequisites

The following prerequisites require administrator privileges:

- Citrix Cloud
- Cloud Connectors

  > **Note:**
  >
  > If you're new to Citrix Cloud, define a Resource Location, and have the connectors configured. It's recommended to have at least two cloud connectors deployed in production environments. For information on how to install Citrix Cloud Connector, see Cloud Connector Installation.

- Citrix Workspace app

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Federated Authentication Service (optional). For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops Service)
- AD domain joined VDA or physical AD joined devices
- Okta Tenant
- Okta Integrated Windows Authentication (IWA) Agent
- Okta Verify (Okta Verify can be downloaded from the app store) (optional)
- Active Directory (AD)

How to configure SSO

Following are the steps to configure SSO for Citrix Workspace app using Okta as an IdP:

1. Install Okta AD agent
2. Create an Okta OIDC web app integration
3. Configure Okta OIDC web application
4. Create Okta API token
5. Connect Citrix Cloud to your Okta organization
6. Enable Okta authentication for Workspaces
7. Configure Okta multifactor authentication (MFA) bypass
8. Set up Okta IWA Agent
9. Configure IdP Routing Rule
10. Configure Okta IdP with Google Admin Console
11. Configure SSO for Citrix Workspace app for ChromeOS using SAML SSO Chrome extension

Install Okta AD agent

Prerequisites:

Before installing the agent, make sure to fulfill the prerequisites mentioned in the Active Directory integration prerequisites link.

To install the Okta AD agent:

1. On the Okta Admin portal, click **Directory** > **Directory Integrations**.
2. Click **Add Directory** > **Add Active Directory**.
3. Review the installation requirements by following the workflow, which covers the Agent Architecture and Installation Requirements.
4. Click the **Set Up Active Directory** button and then click **Download Agent**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Install Okta AD Agent onto a Windows server by following the instruction provided in Install the Okta AD agent.

Create an Okta OIDC web app integration

To use Okta as an IdP, an Okta **OIDC - OpenID Connect** web application must be created so that the user credentials can be used with Citrix Cloud. This app starts the sign-in sequence and also handles redirection to the Citrix Workspace URL in case you sign out.

For more information, see Create an Okta OIDC web app integration.

Configure Okta OIDC web application

After the Okta OIDC app is created, configure it with the settings required for Citrix Cloud. These settings are required for authentication purposes when subscribers sign into Citrix Workspace with Okta.

For more information, see the Configure the Okta OIDC web application link.

Create Okta API token

For more information on how to create an Okta API token, see Create an Okta API token.

Connect Citrix Cloud to your Okta organization

For more information on how to connect Citrix Cloud, see Connect Citrix Cloud to your Okta organization.

Enable Okta authentication for Workspaces

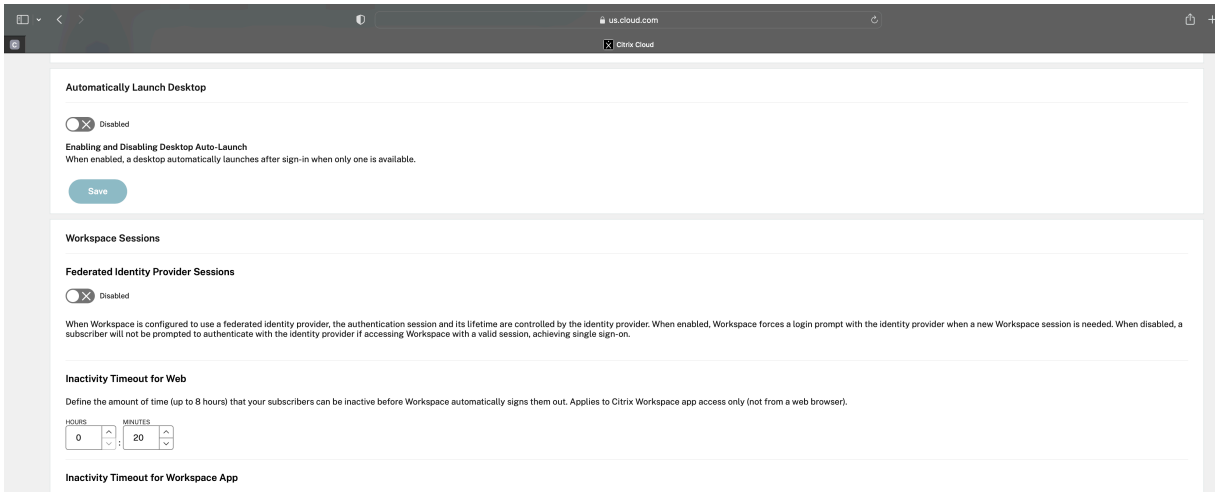
For more information on how to enable Okta authentication, see Enable Okta authentication for workspaces.

Configure Okta multifactor authentication (MFA) bypass

Create a Network Zone defining a set of IP addresses that must be whitelisted for accessing the setup. For more information, see Create zones for IP addresses.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Make sure to disable the option **Federated Identity Provider Sessions**. Navigate to the cloud console under **Workspace Configuration** > **Customize** > **Preferences** and disable **Federated Identity Provider Sessions**.



Set up Okta IWA Agent

Okta IWA Agent is a lightweight Internet Information Services (IIS) web agent that enables Desktop single sign-on (DSSO) on the Okta service.

DSSO is used if a domain-joined computer is accessing Citrix Cloud. This domain-joined computer doesn't require being prompted for authentication.

1. Make sure that the following list of prerequisites are fulfilled.

   For the list of prerequisites to install the Okta IWA Web agent, see Okta IWA Web agent installation prerequisites.

2. Install Okta IWA Agent.

   To install the Okta IWA Web agent, see Install the Okta IWA Web agent.

3. Configure a Windows browser for SSO.

   To configure Windows browser for SSO, see Configure Windows browsers for SSO.

4. Test the Okta IWA Web agent.

   After you download and install the Okta IWA Web agent, verify if the IWA server is working from a client machine.

   If the Okta agent is configured correctly, details related to **UserPrincipalName** and **SecurityIdentifier** appear.

   For more information on how to verify, see Test the Okta IWA Web agent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure IdP Routing Rule

To configure the **Identity Provider Routing Rule**, see Configure IdP Routing Rule.

> **Note:**
>
> From the **IdP(s)** field, make sure to select **OnPremDSSO**.

Configure Okta IdP with Google Admin Console

1. To create a Security Assertion Markup Language (SAML) application, see Create SAML app integrations.

   Make sure to enter a URL in the **Single sign-on URL** and **Audience URI (SP Entity ID)** field. For example, `https://admin.google.com`.

   > **Note:**
   >
   > You might have to modify the example URL after you create the SAML profile in the Google Admin Console. See the next steps for details.

2. Configure SAML with third-party IdP in the Google Admin Console.

   To create an SSO profile for your organization and assign the users, follow the steps mentioned in the Create a SAML SSO profile link.

   To get the Okta sign-in, sign-out, issuer, and other IdP information for the SAML profile, follow the steps mentioned in the Add a SAML IdP link.

3. To configure a SAML profile, see the How to Configure SAML 2.0 for Google Workspace link.
4. Configure a SAML profile in OKTA using Google SAML profile details to synchronize the profiles:

   a) Go to **Security** > **Authentication** > **SSO with third-party IdP** > **Third-party SSO profiles** > open your SAML profile.

   b) On the Okta dashboard page (IdP), add Google(Service Provider) SAML profile details.

   - Navigate to **Single sign-on URL > ACS URL**, and select the option **Use this for Recipient URL** and **Destination URL**.
   - Navigate to **Audience URI (SP Entity ID)** > **Entity ID**.

   After the IdP and SP(Service Provider) SAML profiles are synchronized, the sign-in page for managed users appear on the Okta sign in page on the Chromebook.

5. Assign users to your OKTA SAML application.

   For more information on how to assign users, see the Assign an app integration to a user link.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Validation checkpoints

- When users add the enterprise google account in the Chromebook, users can sign in with Okta credentials.
- After signing into the Chromebook, the user must be able open the Google Chrome browser and enter the Citrix Workspace URL.
- The user must be able to see the Citrix Workspace app UI. The user must be able to navigate to the virtual apps and desktops without being asked for the credentials.

> **Note:**
>
> If the SSO is unsuccessful, revise the step Configure Okta IdP with Google Admin Console.

Configure SSO for Citrix Workspace app for ChromeOS using SAML SSO Chrome extension

To configure SSO using the SAML extension, do the following:

1. Install and configure SAML SSO for the Chrome app extension on Chrome devices.

   To install the extension, click SAML SSO for Chrome Apps.

2. The extension retrieves SAML cookies from the browser and provides them to Citrix Workspace app for ChromeOS.
3. Configure the extension with the following policy to allow Citrix Workspace to get SAML cookies. Replace the domain with your company's Okta IdP domain.

```
{

    "whitelist" : {

        "Value" : [
            {

                "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
                "domain" : "<domain.okta.com>"
                 }

            ]
         }

 }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> If you're repackaging the Citrix Workspace app for ChromeOS, replace `haiffjcadagjlijoggckpgfn` with the repackaged appId.

4. Deploy FAS to achieve SSO to virtual apps and desktops.

   To achieve SSO to virtual apps and desktops, you can either deploy a Federated Authentication Service (FAS) or configure Citrix Workspace app.

   > **Note:**
   >
   > - Without FAS, you're prompted for the Active Directory user name and password. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

Single sign-on for Citrix Workspace app using Microsoft Azure as the IdP

April 24, 2024

You can configure Security Assertion Markup Language (SAML) single sign-on (SSO) for ChromeOS devices. Use Microsoft Entra ID (formerly known as Azure Active Directory) as a SAML IdP and Google Admin as the service provider (SP).

You can configure this feature for managed users only. We have added Citrix VMs to the local Active Directory (AD) that are created on Azure, as a use case. If you have on-premises AD-based VMs on Azure and Microsoft Entra ID users, follow this article.

Prerequisites

The following prerequisites require administrator privileges:

- Active Directory (AD)

  Install and configure an Active Domain Controller in your setup. For more information, see Installing AD DS by using Server Manager. To install Active Directory Domain Services using Server Manager, follow the steps 1 through 19.

- Certificate Authority (CA)

  Install CA. For more information, see Install the Certification Authority.

  A certificate authority can be installed and configured on any of the following machines:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - a new dedicated machine
  - an existing CA machine
  - an installation of this certificate authority component on Citrix Cloud Connector
  - the Active Directory machine

- Citrix Cloud and Citrix Cloud Connector

  If you're new to Citrix Cloud, define a Resource Location, and have the connectors configured. It's recommended you have at least two cloud connectors deployed in production environments. For information on how to install Citrix Cloud Connector, see Cloud Connector Installation.

- Global administrator account on Azure portal

  You must be a global administrator in Microsoft Entra ID. This privilege helps you to configure Citrix Cloud to use the Entra ID as an IdP. For information on the permissions that Citrix Cloud requests when connecting and using Entra ID, see Azure Active Directory Permissions for Citrix Cloud.

- Federated Authentication Service (optional).

  For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

- Global administrator account on Google admin console
- Citrix Workspace app

Get started

To get started, do the following:

- Join all the machines to the Domain before you configure the installed software or Roles on them.
- Install the Citrix Cloud Connector software on the respective machine, but don't configure anything yet.
- Install the Citrix FAS on the respective machine, but don't configure anything yet.

How to configure Citrix Cloud to use Azure AD as an IdP

> **Note:**
>
> Make sure you fulfill all the prerequisites.

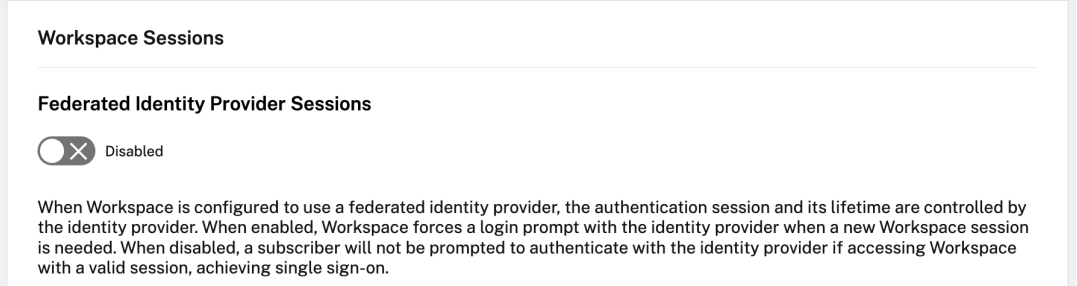
1. To connect Entra ID to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. To add administrators to Citrix Cloud from Entra ID, see Add administrators to Citrix Cloud from Azure AD.
3. To sign in to Citrix Cloud using Entra ID, see Sign-in to Citrix Cloud using Azure AD.
4. To enable advanced Entra ID capabilities, see Enable advanced Azure AD capabilities.
5. To reconnect to Entra ID for the updated app, see Reconnect to Azure AD for the updated app.
6. To reconnect Entra ID, see Reconnect to Azure AD for the updated app.
7. To sync accounts with Entra ID Connect, see Sync accounts.

   It's recommended you sync your on-premises AD accounts with the Entra ID.

> **Note:**
>
> Disable the login prompt for Federated Identity Provider Sessions in the Citrix Workspace Configuration.



Set up SSO and user provisioning between Microsoft Azure and ChromeOS on the Azure portal

After you set up the provisioning of SSO between a Microsoft Entra ID tenant and Google for ChromeOS, end users can sign in to an Azure authentication page instead of the Google sign-in screen on their ChromeOS devices.

For more information, see:

- The Google article Set-up SSO and user provisioning between Microsoft Azure and ChromeOS.

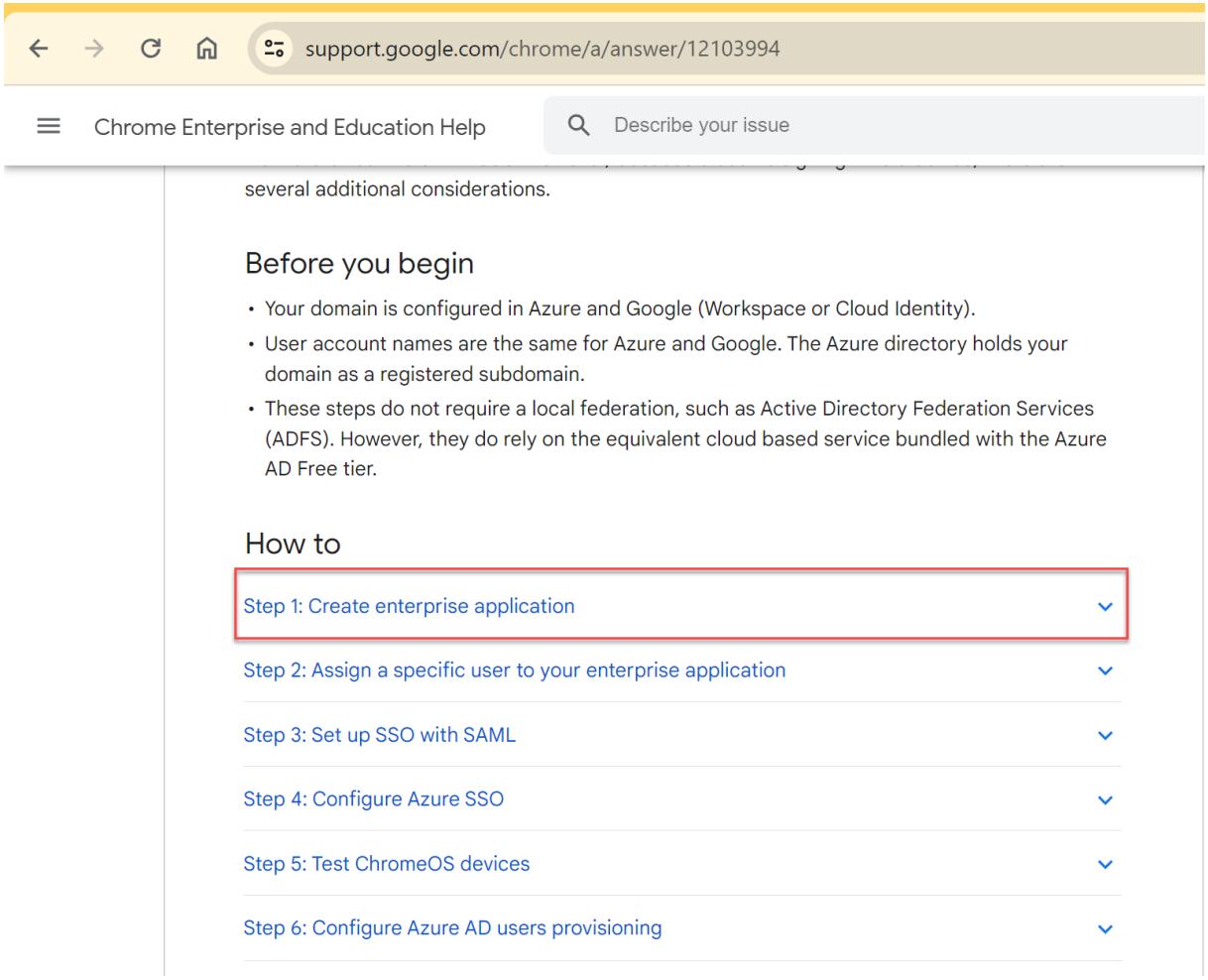
and

- The Microsoft tutorial Microsoft Entra ID SSO integration with Google Cloud / G Suite Connector by Microsoft.

To set up SSO on the Azure portal:

1. Create an enterprise application in the Microsoft Entra ID portal. For more information, see step 1 in the Google article Set-up SSO and user provisioning between Microsoft Azure and ChromeOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

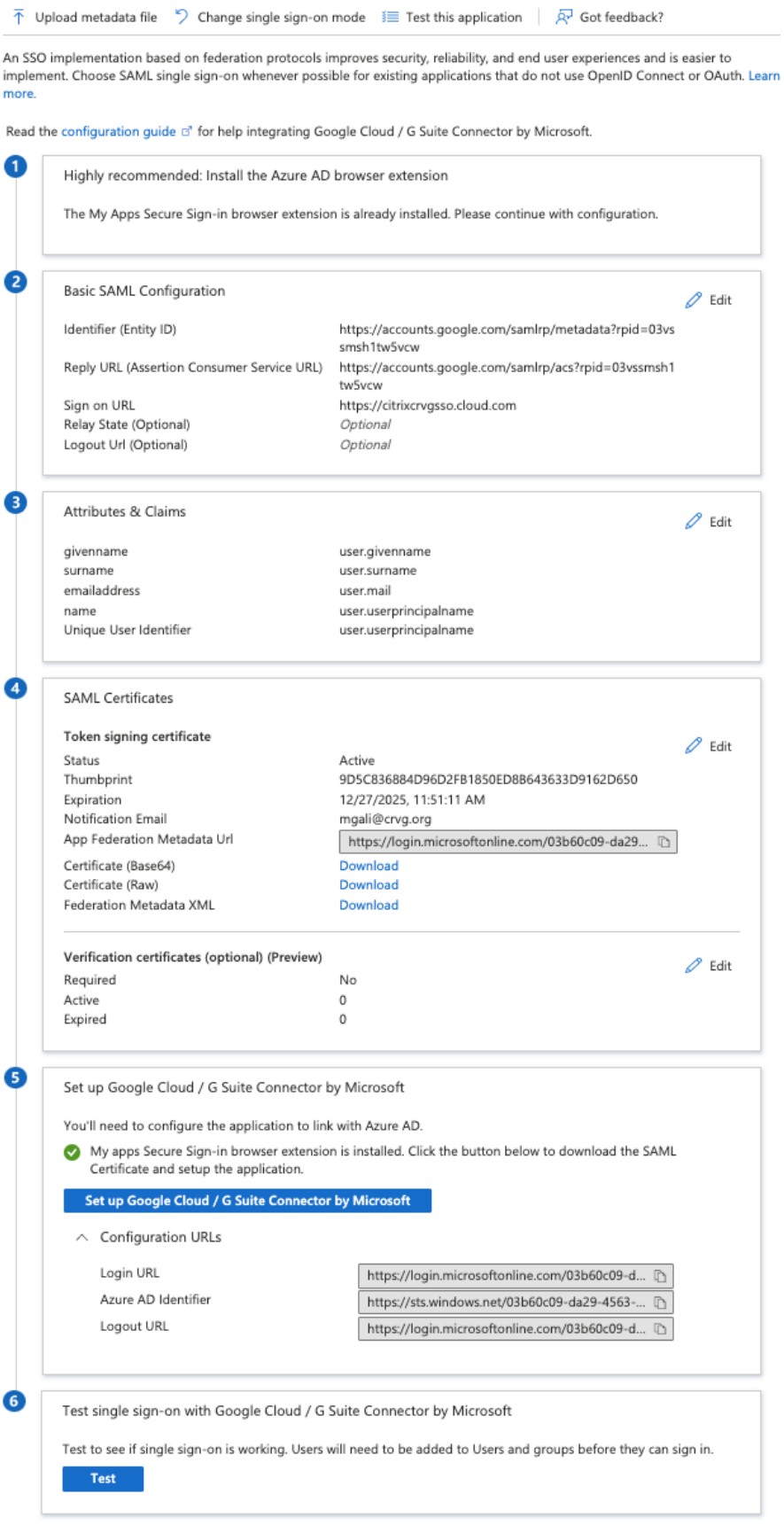


1. Assign a user or multiple users to the enterprise application that you created in step 1. For more information, see step 2 in the Google article Set-up SSO and user provisioning between Microsoft Azure and ChromeOS.
2. Set up SSO with SAML. For more information, see step 3 in the Google article Set-up SSO and user provisioning between Microsoft Azure and ChromeOS.

   > **Note:**
   >
   > It's recommended you change the Basic SAML configuration after the creation of the SAML policy in the Google Admin policy.

   After you set up URLs on the Azure portal for SAML-based single sign-on, the application appears as follows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Validation Checkpoint**
>
> When you enter the store URL, the Azure IdP's sign-in page must appear. If unsuccessful, revisit the Set-up SSO and user provisioning between Microsoft Azure and ChromeOS on the Azure Portal steps.

Configure SAML SSO profile with Google Admin Console

- Add the Domain, users, and create an OU. For more information, see A complete guide to Google Organizational Units.
- Create the SAML SSO profile with Microsoft Entra ID as the IdP. For more information, see Configuring SAML single sign-on (SSO) for Azure AD Users.

> **Validation Checkpoint**
>
> Using the Chromebook, you must be able to sign in to Citrix Workspace app using Azure credentials. When you enter the store URL in the browser, you must be able to sign in.

Configure SSO for Citrix Workspace app for ChromeOS using SAML SSO Chrome extension

To configure SSO using the SAML extension, do the following:

1. Install and configure SAML SSO for the Chrome app extension on Chrome devices.

   To install the extension, click SAML SSO for Chrome Apps.

2. The extension retrieves SAML cookies from the browser and provides them to the Citrix Workspace app for ChromeOS.

3. Configure the extension with the following policy to allow Citrix Workspace app to get SAML cookies. The following is the JSON data:

```
{

"allowlist": {

    "Value": [
        {

            "appId": "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain": "login.microsoftonline.com"
         }

    ]
 }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
15   }
16
17 <!--NeedCopy-->
```

> **Validation Checkpoint**
>
> When you start Citrix Workspace app with Azure IdP store and SSO extension, your sign-in to the Citrix Workspace app must be successful.

Deploy FAS to achieve SSO to virtual apps and desktops

To achieve SSO for virtual apps and desktops, you can deploy a Federated Authentication Service (FAS).

> **Note:**
>
> Without FAS, you're prompted for the Active Directory user name and password. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

SDK and API

April 23, 2024

HDX SDK

Citrix Workspace app for ChromeOS introduces an API (Experimental API) that allow third-party Chrome apps to lock, unlock, and disconnect from:

- Citrix Virtual Apps and Desktops
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session

Using this API, you can launch Citrix Workspace app for ChromeOS in both embedded mode and kiosk mode. Sessions launched in embedded mode function in ways similar to sessions launched kiosk mode.

For the SDK documentation, see HDX SDK for Citrix Workspace app for ChromeOS.

For HDX SDK examples, refer to the Citrix download page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) supports you to write server-side applications and client-side drivers for additional virtual channels using the ICA protocol.

The server-side virtual channel applications are on Citrix Virtual Apps or Citrix Virtual Apps and Desktops servers. This version of the SDK supports you to write new virtual channels for Citrix Workspace app for ChromeOS. If you want to write virtual drivers for other client platforms, contact Citrix.

The Virtual Channel SDK provides:

- An easy interface that can be used with the virtual channels in the Citrix Server API SDK (WFAPI SDK) to create new 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 the VC SDK documentation, see Citrix Virtual Channel SDK for Citrix Workspace app for ChromeOS.

Enhancements to Virtual Channel SDK

Starting with the 2305 release, Citrix Workspace app for ChromeOS supports Window Management APIs in the Virtual Channel SDK. Web APIs enable IT administrators to create interactive applications and customize them for their end users.

Procedure to consume the API in the third-party Chrome app

1. Install the latest version of Citrix Workspace app for ChromeOS. See the Citrix downloads page for details.
2. Add the third-party Chrome app to the allow list by adding the policy file for Citrix Workspace app for ChromeOS. Use the Chrome management settings to add the policy.

   For more details, see Manage Chrome Apps by organizational unit on Google support.

   To add the third-party Chrome app to the allow list, here's the sample `policy.txt` JSON data:

```
{

        "settings": {

                "Value": {

                "settings_version": "1.0",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                "store_settings": {

                "externalApps": [“ <3rdParty_App1_ExtnID>” ,“ <3
    rdParty_App2_ExtnID>” ]
                                    }

                            }

                    }

 }

<!--NeedCopy-->
```

> **Note:**
>
> <3rdParty_App1_ExtnID> is used as an example for the name of externalApps and can send messages to Citrix Workspace app for ChromeOS. Get your **appid** from the chrome://extensions site.

3. Launch the application or a desktop session in Citrix Workspace for ChromeOS as follows:

- Get the workspaceappID

```
var workspaceappID = "haiffjcadagjlijoggckpgfnoeiflnem ";
```

> **Note:**
>
> In this example, **workspaceappID** indicates the store version of Citrix Workspace app for ChromeOS. If you're using a repackaged version of Citrix Workspace app for ChromeOS, use the appropriate workspaceappID.

- Convert ICA data from INI to JSON format.

> **Note:**
>
> Typically, the ICA file is retrieved from StoreFront as an INI file. Use the following helper function to convert an ICA INI file into JSON.

```
//Helper function to convert ica in INI format to JSON
function convertICA_INI_TO_JSON(data){

var keyVals = {
 }
;
if (data) {

var dataArr;
if(data.indexOf('\r')==-1){

dataArr = data.split('\n');
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 }
else{

dataArr = data.split('\r\n');
 }

for (var i = 0; i \< dataArr.length; i++) {

var nameValue = dataArr[i].split('=', 2);
if (nameValue.length === 2) {

keyVals[nameValue[0]] = nameValue[1];
 }

// This is required as LaunchReference contains '=' as well. The above split('=',2) will not provide
// the complete LaunchReference. Ideally, something like the following should be used generically as well
// because there can be other variables that use the '=' character as part of the value.
if (nameValue[0] === "LaunchReference") {

var index = dataArr[i].indexOf('=');
var value = dataArr[i].substr(index + 1);
keyVals[nameValue[0]] = value;
 }

 }

console.log(keyVals);//to remove
return keyVals;
 }

return null;
 }


<!--NeedCopy-->
```

- Send an ICA message from the third-party Chrome app to Citrix Workspace app for ChromeOS.

```
var icaFileJson = {
... }
; // ICA file passed as JSON key value pairs.
var message = {

"method" : "launchSession",
"icaData" : icaJSON
 }
;
chrome.runtime.sendMessage(workspaceappID, message,
function(launchStatus) {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
13  if (launchStatus.success) {
14
15  // handle success.
16  console.log("Session launch was attempted successfully");
17   }
18   else {
19
20  // handle errors.
21  console.log("error during session launch: ", launchStatus.message
        );
22   }
23
24   }
25  );
26
27  <!--NeedCopy-->
```

For more details on **sendMesage** API commands, see the following links:

https://developer.chrome.com/extensions/runtime#event-onMessageExternal

https://developer.chrome.com/extensions/runtime#method-sendMessage

Manifest V3 support for SDK scenarios

Starting with the 2305 release, Citrix Workspace app for ChromeOS supports the HDX SDK with Chrome extensions having manifest version 3.

For more information, see Citrix Workspace app for ChromeOS HDX SDK in the developer guides documentation.

Deprecation

April 12, 2024

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Item	Deprecation announced in	Removed in	Alternative
None for now	-	-	-

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