Citrix Workspace app for ChromeOS

Contents

About this release

January 11, 2023

What's new in 2212

This release is compatible with ChromeOS version 108. In addition, this release addresses a few issues that help to improve overall performance and stability.

Fixed issues in 2212

- When you enable multi-touch mode, some touch actions might not work within the Citrix Workspace app session. [RFHTMCRM-8445]
- In the seamless app sessions, you might be unable to click on any links or elements on the BCR overlay. [HDX-42950] [RFHTMCRM-7428]

Known issues in 2212

- There are no known issues in this release.

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

2211

What's new

This release is compatible with ChromeOS version 107.

Automatic display of virtual keyboard

Starting from this release, 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.

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.

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

For information on how to configure, see Adaptive audio documentation.

Composite USB redirection

Previously, when a composite USB device was connected to the client machine, it was redirected only as a single device through USB redirection. With this type of redirection, interfaces like audio and video also got redirected through USB, despite optimized channels.

Starting from 2211 release, the end user can select and redirect a specific constituent interface of a composite USB device to the Citrix Workspace app session through USB redirection.

Administrators can configure if certain interfaces of the device are redirected to the session through USB redirection or not.

For more information, see Composite USB redirection documentation.

Fixed issues

- When you share your device screen to present a Virtual Desktop Infrastructure (VDI) session with the administrator, the end user can see both the administrator's and the end user's mouse pointer on the screen. [RFHTMCRM-7726]

2210.1

This release is compatible with ChromeOS version 106.

What's new

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

Fixed issues

There are no fixed issues in this release.

2210

This release is compatible with ChromeOS version 106.

What's new

Adaptive Audio [Technical Preview]

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

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

For information on how to configure, see Adaptive audio documentation.

Browser Content Redirection [Technical Preview]

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

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.
- In the Google Chrome browser seamless app sessions, you might be unable to click any links or elements on the BCR overlay. [HDX-42950]

Composite USB Redirection [Technical Preview]

Previously, when a composite USB device was connected to the client machine, it was redirected only as a single device through USB redirection. With this type of redirection, interfaces like audio and video also got redirected through USB, despite optimized channels.

Starting from 2210 release, the end user can select and redirect a specific constituent interface of a composite USB device to the Citrix Workspace app session through USB redirection.

Administrators can configure if certain interfaces of the device are redirected to the session through USB redirection or not.

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

Known issue in the feature

- In kiosk mode, when composite USB split functionality is enabled, the USB device might fail to redirect. The issue occurs when you disconnect and start the session. [RFHTMCRM-7952]

Fixed issues

There are no fixed issues in this release

2209

This release is compatible with ChromeOS version 105.

What's new

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.

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

Service continuity Technical preview

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.

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

Fixed issues

- In a session, when three or more participants are in the optimized Microsoft Teams meeting, the screen sharing might not work as expected. The issue happens intermittently. [RFHTMCRM-7409]
- When you join an external meeting from the optimized Microsoft Teams, the audio from the participant doesn't work as expected. The following error message appears: "Couldn't find a microphone". As a workaround, quit the Microsoft Teams app and rejoin. [CVADHELP-20625]

2208

This release is compatible with ChromeOS version 103.

What's new

Provision to disable LaunchDarkly service

Starting with this release, you can disable LaunchDarkly service on both on-premises and cloud stores.

For more information, see Feature flag management documentation.

Fixed issues

- In a session, when there are three or more participants in the optimized Microsoft Teams meeting, the video of the participants might freeze. The issue occurs intermittently. [RFHTMCRM-7251]
- When the third participant is added to the Microsoft Teams meeting or a peer-to-peer call, the audio might not work as expected. [CVADHELP-19840]
- In the optimized Microsoft Teams video call, when you add the third participant, the call drops. [CVADHELP-20586]

2207

This release is compatible with ChromeOS LTS Version 102 and ChromeOS version 102.

What's new

Logging enhancements

Previously, the client logs and console logs had to be collected separately. Starting with this release, the console logs are a part of the client logs.

For more information, see How to collect logs.

Clipboard supports HTML format

Starting with this release, 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.

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.

For more information, see Email-based store discovery.

Fixed issues

- When you start a desktop session using the ICA file, Citrix Workspace app logo appears instead of the desktop logo on the Chrome shelf. [RFHTMCRM-6701]
- When you click the **Disconnect** option from the in-session toolbar, the USB devices you connect to the session might not disconnect between VDA sessions. The issue occurs when you are in the Kiosk mode. [RFHTMCRM-7148]

2206.5.2

This release is compatible with ChromeOS version 101.

What's new

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't share resources that aren't opened from Citrix Workspace app.

For more information, see Microsoft Teams optimization settings.

Fixed issues

There are no fixed issues in this release.

2205.6

This release is compatible with ChromeOS version 101.

What's new

This release addresses issues that help to improve stability.

Fixed issues

- If the administrator has rolled out any settings through Global App Configuration Service (GACS), Citrix Workspace app might not apply those settings. [RFHTMCRM-7198]

2205.5

This release is compatible with ChromeOS version 101.

What's new

This release addresses issues that help to improve stability.

Fixed issues

There are no fixed issues in this release.

2203.2

What's new

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

Fixed issues

- After upgrading to version 2203, trying to use the keyboard inside a session fails. A few keys and key combinations using CTRL, ALT, Shift, Spacebar, and Caps Lock might not work as expected. [CVADHELP-19766]

2203.1

What's new

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

Fixed issues

- After upgrading to version 2203, trying to use the keyboard inside a session fails. A few keys like CTRL, ALT, Shift, Spacebar, and Caps Lock might not work as expected. [CVADHELP-19766]

2203

What's new

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

For more information, see 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`.

Session reliability enhancement

This feature enhances the user experience by having fewer dropped network connections when you're roaming. The session reconnection happens in a few seconds.

CEIP data to Citrix and Google Analytics

From this release, end users can:

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

For more information, see CEIP section as a whole and in particular Blocking CEIP section.

Change in USB redirection

To redirect the USB device to a new session, it's required to remove the USB device from the previous session.

For more information, see Automatic redirection of USB devices section.

Fixed issues

- When you set up a Microsoft Outlook meeting with Dutch regional settings and the option **Adjust the daylight saving time automatically** is enabled, the meeting invite in the remote calendar appears an hour early. [CVADHELP-17992]
- If there's any invalid JSON data in **web.config** or **default.ica** file, a dialog box appears to notify the end user at the time of signing into the store or when launching a session respectively. [RFHTMCRM-6681]

2202.1

What's new

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 configuration JSON using https://jsonlint.com/.
2. Follow the steps mentioned in Get started page to update:
   - Google Policy
   - web.config
   - default.ica
   - configuration.js

   We recommend using 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.

Fixed issues

- After you upgrade to the version 2202, store configuration using Beacons might not work as expected. [RFHTMCRM-6680]

2202

What's new

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

Fixed issues

- After you upgrade Citrix Workspace app to version 2201, and when you place the Chrome shelf on the left side of the screen, the mouse clicks are misaligned.

  The issue occurs in multi-monitor mode. [CVADHELP-18565]

- When you enable Microsoft Teams optimization, the incoming audio isn't available. [CVADHELP-19456].

2201

What's new

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

Fixed issues

- The Microsoft Teams video or screen sharing renders incorrectly when you connect to a primary external monitor and launch a desktop or an app session.

  The issue occurs when you are in multi-monitor mode and move the Microsoft Teams window to the external monitor. [RFHTMCRM-6424]

2112

What's new

Support for dynamic e911

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

- configure and route emergency calls
- notify security personnel

The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client that runs on the VDA.

Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112 for ChromeOS, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law.

Fixed issues

- When you connect to a primary external monitor and launch a desktop or an app session, Microsoft Teams video or screen sharing can go blank.

  The issue occurs when you are in the multi-monitor mode. In addition, when you move the Microsoft Teams window from the external monitor to the built-in display (secondary monitor). [RFHTMCRM-6134]

- When you launch sessions in a multi-monitor environment, the mouse clicks are misaligned. You might notice misalignment by a few pixels. The issue occurs when the Chrome shelf is positioned on the left. We recommend you position the Chrome shelf at the bottom of the screen. [RFHTMCRM-6069] [RFHTMCRM-5456] [CVADHELP-18565]
- A few application icons aren't visible on the Chrome shelf. The issue occurs when you enable **Settings** > **General** > **High DPI Scaling** using Citrix Workspace app. [RFHTMCRM-6078]
- After a fresh install of Citrix Workspace app, the logs for the first session opened aren't recorded. All the later session launches are recorded as per the functionality. [RFHTMCRM-6221]

2111.1

What's new

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

Fixed issues in 2111.1

- During auto-reconnect session launch in auto-launch mode, a blank window might pop up and block the session launch for users in Kiosk mode.
  [RFHTMCRM-6220]

2111

What's new

Troubleshooting enhancement

With this release, Citrix Workspace app supports log collection for ongoing virtual desktop and app sessions. Previously, you could 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**.

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.

Workspace with intelligence

With this release, Citrix Workspace app is optimized to take advantage of the Workspace intelligence features. This version unifies user workflows and provides an activity feed displaying relevant information. The microapps streamline end user workflows and approvals. For more information, see Workspace Intelligence Features - Microapps.

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.
- For all other users of Citrix Workspace app for ChromeOS, version 2110 and earlier, see Knowledge Center article CTX331653.

Fixed issues

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

2110

What's new

Optimized Microsoft Teams 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. Previously, if you moved your optimized Microsoft Teams windows to an external monitor, only the audio portion of calls was supported.

This enhancement requires VDA version 1906 or later.

Recommendation

- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

Fixed issues

- On devices where only intranet access is allowed, sessions might not start or there might be a delay. [RFHTMCRM-5440]
- In multi-monitor mode, the session might close intermittently. As a workaround, start the session again. [RFHTMCRM-5528]
- When you click **Disconnect** on your toolbar or through the HDX SDK for ChromeOS disconnect API, your desktop and app session windows might not close. This issue occurs after disabling the seamless virtual channel. [RFHTMCRM-6000]
- You might see disconnection of sessions in Citrix Workspace app 2108 and 2109 for ChromeOS. The issue occurs in VDA version 7.15. [RFHTMCRM-5859]

2109

What's new in 2109

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 **Use all the monitors to span display** option.

Battery status indicator

The battery status of the device now appears in the notification area within the virtual desktop session. Previously, the battery status indicator wasn't visible in the session. This 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.

Support for copying image clips

Using the standard keyboard shortcuts, you can now 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 while using apps such as Microsoft Word, Microsoft Paint, and Adobe Photoshop. Previously, this functionality was available only for text.

> **Notes:**
>
> - 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.

Auto-launch of ICA sessions

Citrix Workspace app for ChromeOS now 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 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 to start resources. Also, the ICA file wasn't deleted when opened and remained on the device. With this release, the ICA file is automatically deleted from the device - once it's used to auto-launch the session.

For more information, see Auto-launch of ICA sessions.

Note (HTTPS)

If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

Fixed issues

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

2108.2

What's new

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

Fixed issues

HDX SDK for ChromeOS embedded mode sessions might not launch. [RFHTMCRM-5738]

Known issues

- If the administrator has rolled out any settings through Global App Configuration Service (GACS), Citrix Workspace app might not apply those settings. [RFHTMCRM-7198]

Known issues in 2208

- In a session, when three or more participants are in the optimized Microsoft Teams meeting, the screen sharing functionality might not work as expected. As a workaround, quit the Teams app and rejoin. The issue occurs intermittently. [RFHTMCRM-7409]
- When you join an external meeting from the optimized Microsoft Teams, the audio from the participant doesn't work as expected. The following error message appears: "Couldn't find a microphone". As a workaround, quit the Teams app and rejoin. [CVADHELP-20625]
- 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]

Known issues in 2207

- In a session, when there are three or more participants in the optimized Microsoft Teams meeting, the video of the participants might freeze. The issue occurs intermittently. [RFHTMCRM-7251]

Known issues in 2206.5.2

- In a session, when there are three or more participants in the optimized Microsoft Teams meeting, the video of the participants might freeze. The issue occurs intermittently. [RFHTMCRM-7251]

Known issues in 2205.6

- When the third participant is added to the Microsoft Teams meeting or a peer-to-peer call, the audio might not work as expected. [CVADHELP-19840]

Known issues in 2205.5

- If the administrator has rolled out any settings through Global App Configuration Service (GACS), Citrix Workspace app might not apply those settings. [RFHTMCRM-7198]

Known issues in 2203

- In a session, when you use Microsoft Teams optimization, you might be unable to answer an incoming Microsoft Teams call or join a Microsoft Teams meeting. The issue occurs intermittently when the Virtual Desktop Infrastructure's (VDI's) shim version is 1.8.0.12. [CVADHELP-19567]
- Webcam redirection might not work in some Citrix Virtual Apps and Desktops or XenDesktop. [HDX-39396]

Known issues in 2202

- When you set up a Microsoft Outlook meeting with Dutch regional settings and the option **Adjust the daylight saving time automatically** is enabled, the meeting invite in the remote calendar appears an hour early. The issue occurs when the summer meeting is scheduled in winter. [CVADHELP-17992]

Known issues in 2112

- When you connect to a primary external monitor and launch a desktop or an app session, Microsoft Teams video or screen sharing renders incorrectly.

  The issue occurs when you are in the multi-monitor mode, and when you move the Microsoft Teams window from the external monitor to the built-in display (secondary monitor). [RFHTMCRM-6268]

Known issues in 2111.1

- After a fresh install of Citrix Workspace app, the logs for the first session opened aren't recorded. All the subsequent session launches are recorded as per the functionality. [RFHTMCRM-6221]
- If you get reconnected after getting disconnected from an active call on Microsoft Teams, the audio may sometimes not be available. [RFHTMCRM-6217]

Known issues in 2111

- During auto-reconnect session launch in auto-launch mode, a blank window might pop up and block the session launch for users in Kiosk mode.
  [RFHTMCRM-6220]

- When you launch sessions in a multi-monitor environment, the mouse clicks are misaligned by a few pixels. The issue occurs when the Chrome shelf is positioned on the left. We recommend you position the Chrome shelf at the bottom of the screen. [RFHTMCRM-5456] [CVADHELP-18565]
- A blank window might appear when you do certain actions like sending an email. Close the window and continue. [RFHTMCRM-6209]
- If an external monitor is made as the primary monitor, the Microsoft Teams video might go blank. [RFHTMCRM-6134]

Known issues in 2108

- 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]

Legacy documentation

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

Technical preview

Technical previews are available for customers to use in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance.

Limitations

- 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]
- 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 sign in issues. 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]

Prerequisites for installing

January 11, 2023

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 now supports ChromeOS Flex operating system.

> **Note:**
>
> 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 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 suites 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.

  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 2.4 GHz quad core CPU that supports 720p HD resolution.

Install

January 11, 2023

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. The users can search for Citrix Workspace and click **Add to Chrome**.

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.

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 have 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" :  \[
                    "ica",
                     "cr"
                 \]
              }

       }

   <!--NeedCopy-->
   ```

6. In Chrome, browse to chrome://extensions, select the **Developer mode** check box 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 whitelist your repackaged application 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 element in the file.

   ```
   pre codeblock <html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjlijoggc
   "... /> <!--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) versions 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

1. On the StoreFront server, administrator can use a text editor to open the web.config file for the Receiver for Web site, which is typically at **C:\inetpub\wwwroot\Citrix\storename** Web directory, where *storename* is the name specified for the store when it was created.
2. Locate the following element in the file:

   ```
   <html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem
   "... />
   ```

3. Add the value of the **chromeAppOrigins** attribute to a relevant ID. For example `chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem|chrome-extension://anjihnbmjbbpofafpmklejenkgnjfcdi`.

If you are an end user, and you want to access the backup build, do the following:

- On the Chrome Web store, search **Citrix Workspace Backup** and click **Add to Chrome**.

  Or

- Click the link https://chrome.google.com/webstore/detail/citrix-workspace-backup/anjihnbmjbbpofafpmklejenkgnjfcdi and click **Add to Chrome**.

> **Note:**
>
> To verify, see the version of the app. Usually the format is xx.x.5.x. Here, 5 indicates it's a backup build.

To access the EAR build

1. On the StoreFront server, administrator can use a text editor to open the web.config file for the Receiver for Web site, which is typically at **C:\inetpub\wwwroot\Citrix\storename** Web directory, where *storename* is the name specified for the store when it was created.
2. Locate the following element in the file:
   ```
   <html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem
   "... />
   ```
3. Add the value of the **chromeAppOrigins** attribute to a relevant ID. For example, `chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem|chrome-extension://lbfgjakkeeccemhonnolnmglmfmccaag`.

If you are an end user, and you want to access the EAR build, do the following:

- On the Chrome Web store, search **Citrix Workspace EAR** and click **Add to Chrome**.

  Or

- Click the link https://chrome.google.com/webstore/detail/citrix-workspace-backup/lbfgjakkeeccemhonnolnmglmfmccaag and click **Add to Chrome**.

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 are 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.

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.

Exclusions

The following features are not eligible for compatibility with ChromeOS LTS:

- Microsoft Teams Optimization
- Browser Content Redirection

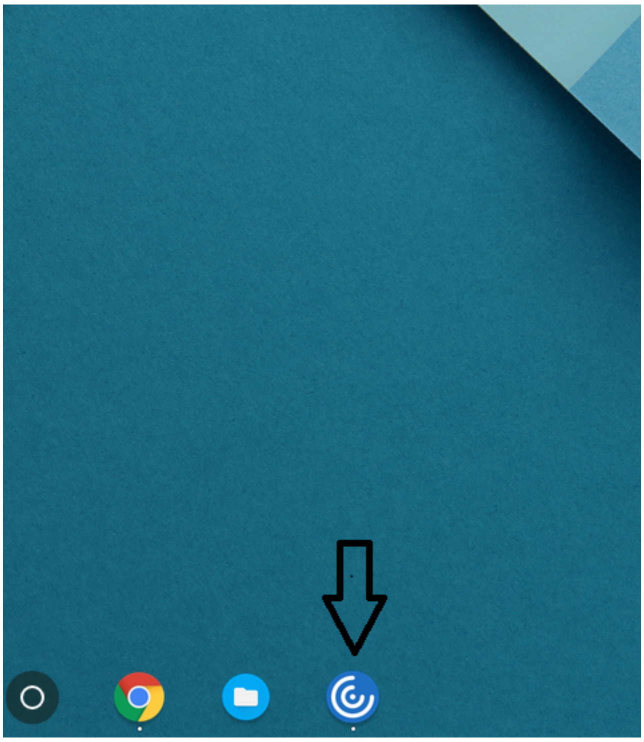
Updates to the excluded features are available on the latest version of ChromeOS on the stable channel along with the latest version of the Citrix Workspace app.

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 need to 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**.



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

January 11, 2023

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.

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 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, `haiffjcadagjlijoggckpgfnoei`).
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.
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 `haiffjcadagjlijoggckpgfnoei`
   .
   - 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:**
>
> 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.

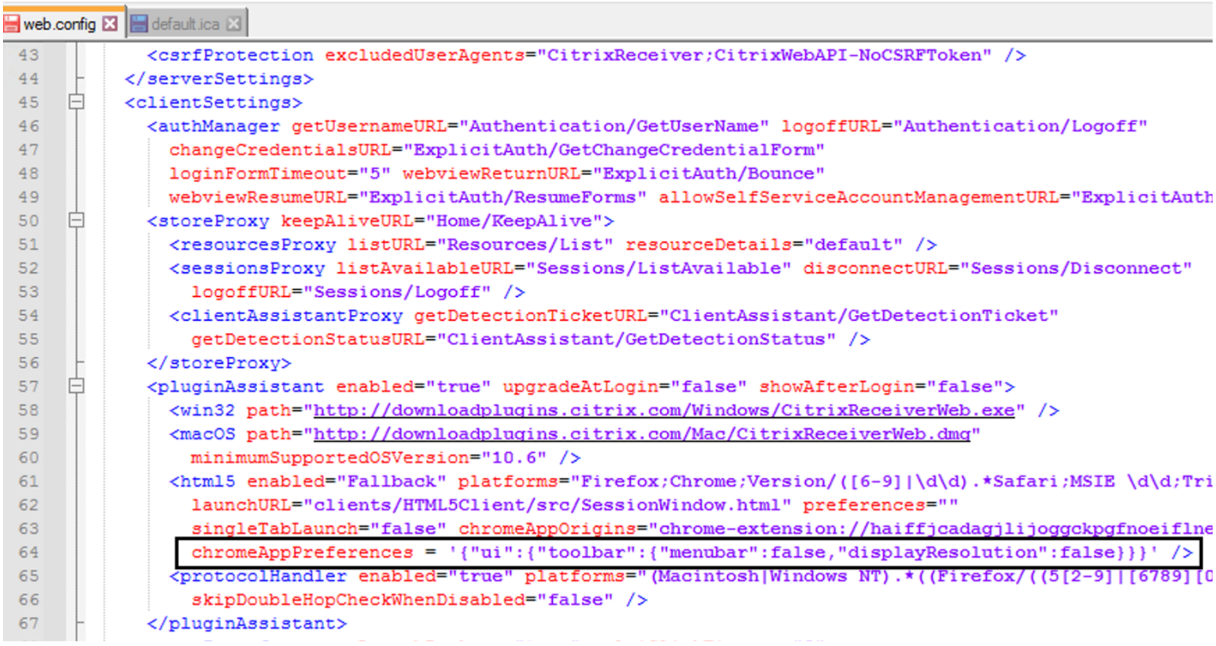
To change the configuration using the Web.config file method (only for those using on-prem StoreFront):

1. Open the **web.config** file for the Citrix Receiver for Web site. This file is in **C:\inetpub\wwwroot\Citrix\<stor**
   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}}}'

Another sample example is as follows,



```
      <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>
```

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.

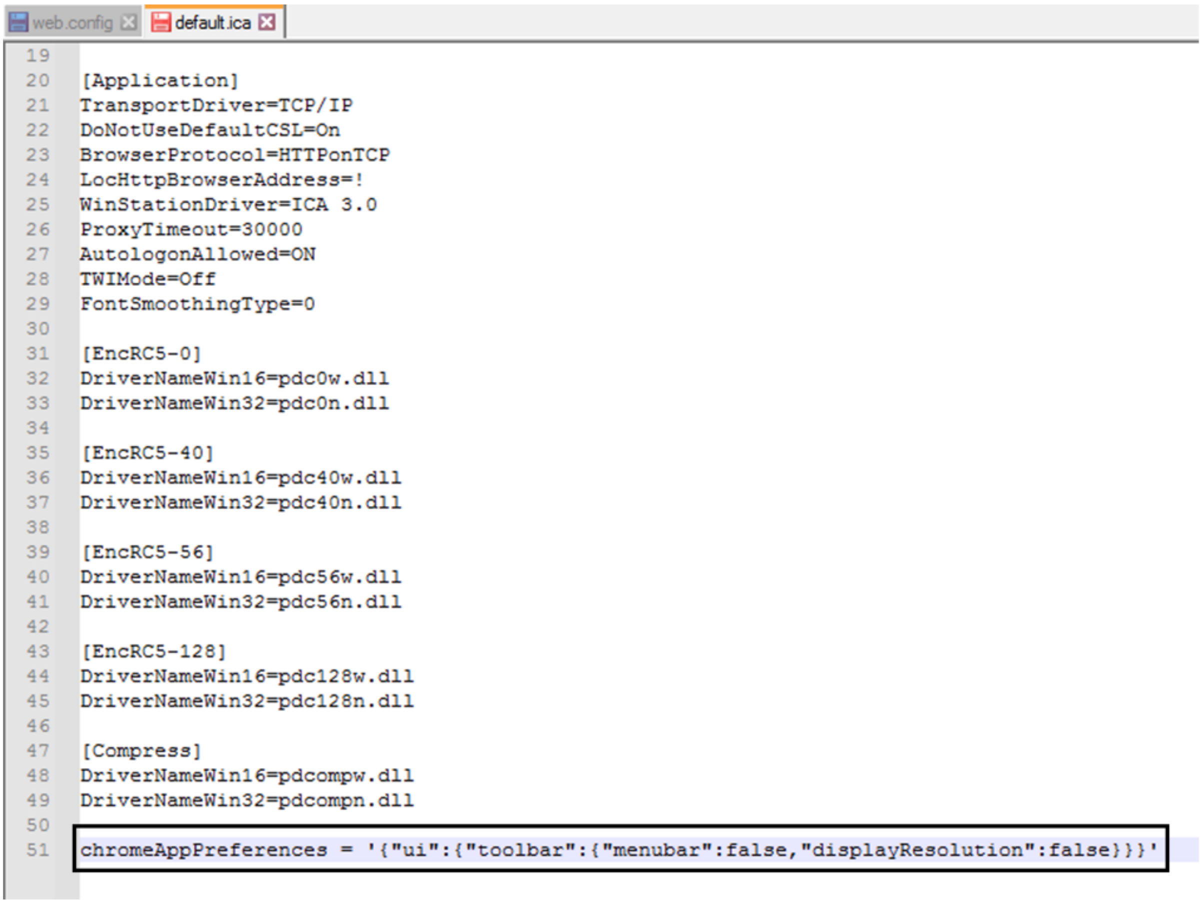
To change the configuration using the **default.ica** file:

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}}}

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



```

[Application]
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
TWIMode=Off
FontSmoothingType=0

[EncRC5-0]
DriverNameWin16=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll

[Compress]
DriverNameWin16=pdcompw.dll
DriverNameWin32=pdcompn.dll

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:

1. Install 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

January 11, 2023

Multi-touch mode

About this feature

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**.

```
{

    "settings": {

        "Value": {

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

                            "ui": {

                                "touch" : {

                                    "defaultMode" : "multitouch"
                                     }

                                }

                             }

                          }

                     }

                  }


<!--NeedCopy-->
```

Support for Touch

About this feature

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.

Automatic Keyboard display

About this feature

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 a three finger 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.

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
                 }

             }

         }

     }

 }


<!--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.

Customer Experience Improvement Program (CEIP)

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 European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK).

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

> **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 strings 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-->
```

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.

> **Note:**
>
> - Citrix recommends that you back up the configuration.js file before making changes.
> - Citrix recommends using this method only if 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-->
```

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.

This 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 strings 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

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

1. Launch 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:

Workspace app version	Session mode (Kiosk, Public/General)	Session type (desktop/application)	XenDesktop information (Delivery Controller and VDA versions)
Launch type (SDK/ICAFile/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

Content Collaboration Service integration

About this feature

Citrix Content Collaboration enables you to:

- Exchange documents easily and securely.
- Send large documents by email
- Securely handle document transfers to third parties.

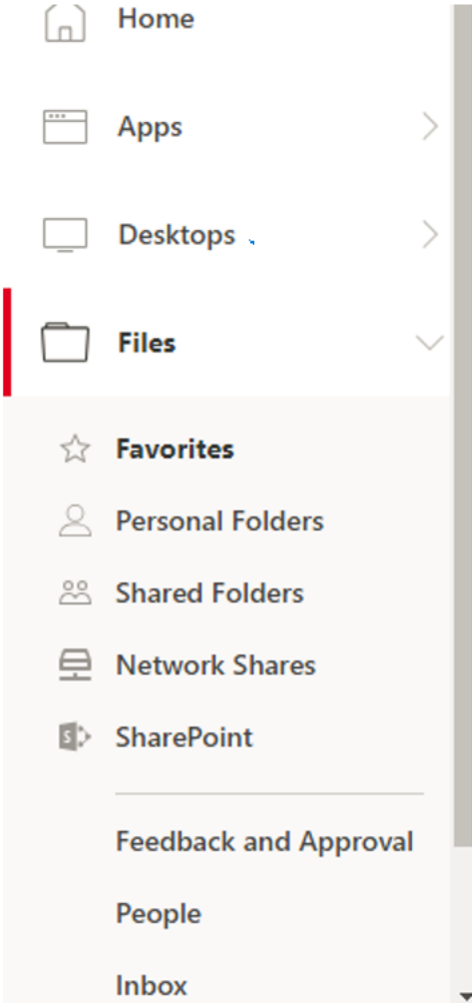
- Access a collaboration space.

Citrix Content Collaboration provides many ways to work, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

You can access Citrix Content Collaboration functionality from the Citrix Workspace app using the **Files** tab displayed within Citrix Workspace app. You can view the **Files** tab only if Content Collaboration Service is enabled in the Workspace configuration in the Citrix Cloud console.

> **Note:**
>
> Citrix Workspace app does not support Citrix Content Collaboration on Windows Server 2012 and Windows Server 2016. This exclusion is because of a security option set in the operating system.

The following image displays sample contents of the **Files** tab of the new Citrix Workspace app:



Feature limitations:

- Resetting Citrix Workspace app does not cause Citrix Content Collaboration to log off.
- Switching stores in Citrix Workspace app does not cause Citrix Content Collaboration to log off.

To enable Citrix Workspace app for ChromeOS for users to access resources hosted on Citrix Virtual Apps and Desktops, you must create a StoreFront store. You must also enable:

- WebSocket connections on Citrix Gateway
- Citrix Virtual Apps
- Citrix Virtual Apps and Desktops as required

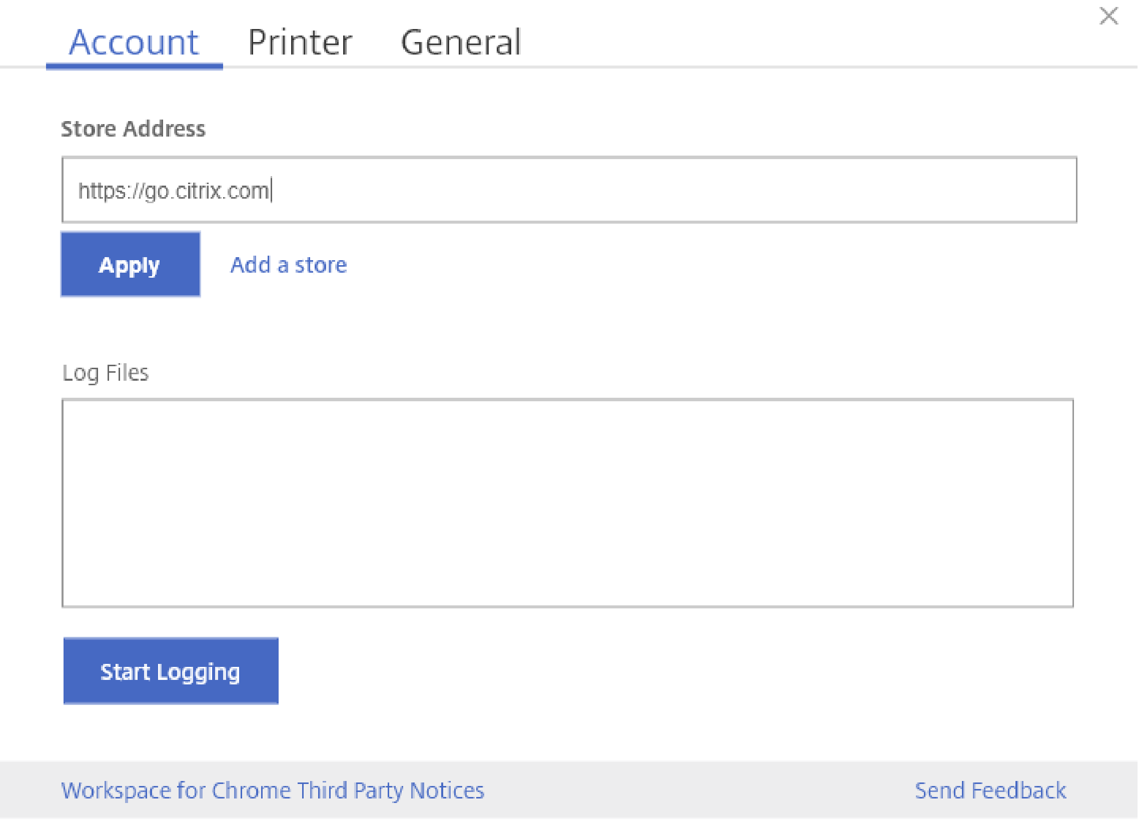
Multiple StoreFront

About this feature

You can change the Store address without having to restart Citrix Workspace. Existing Citrix Workspace sessions, if any, continue to run uninterrupted.

To add many stores and switch between them using ChromeOS:

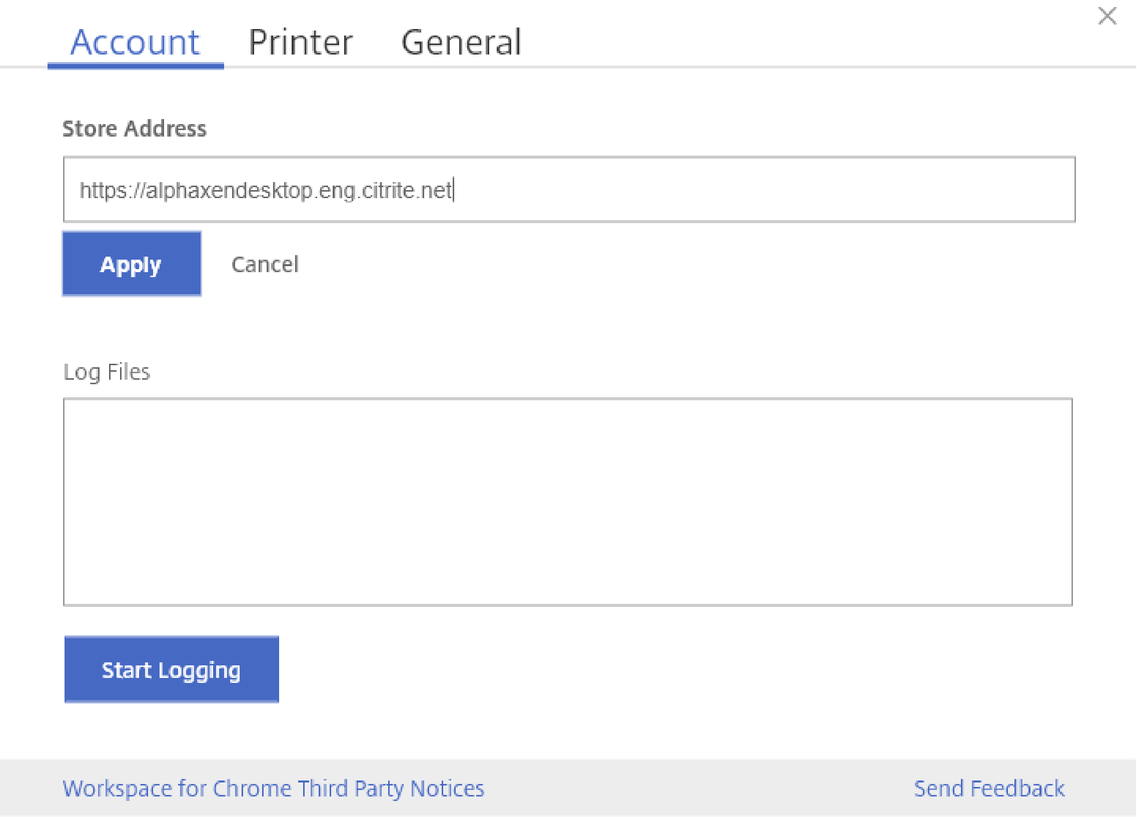
1. Click **Settings** in Citrix Workspace app for ChromeOS, and in the **Account** pane, click **Add a store**.



Store Address

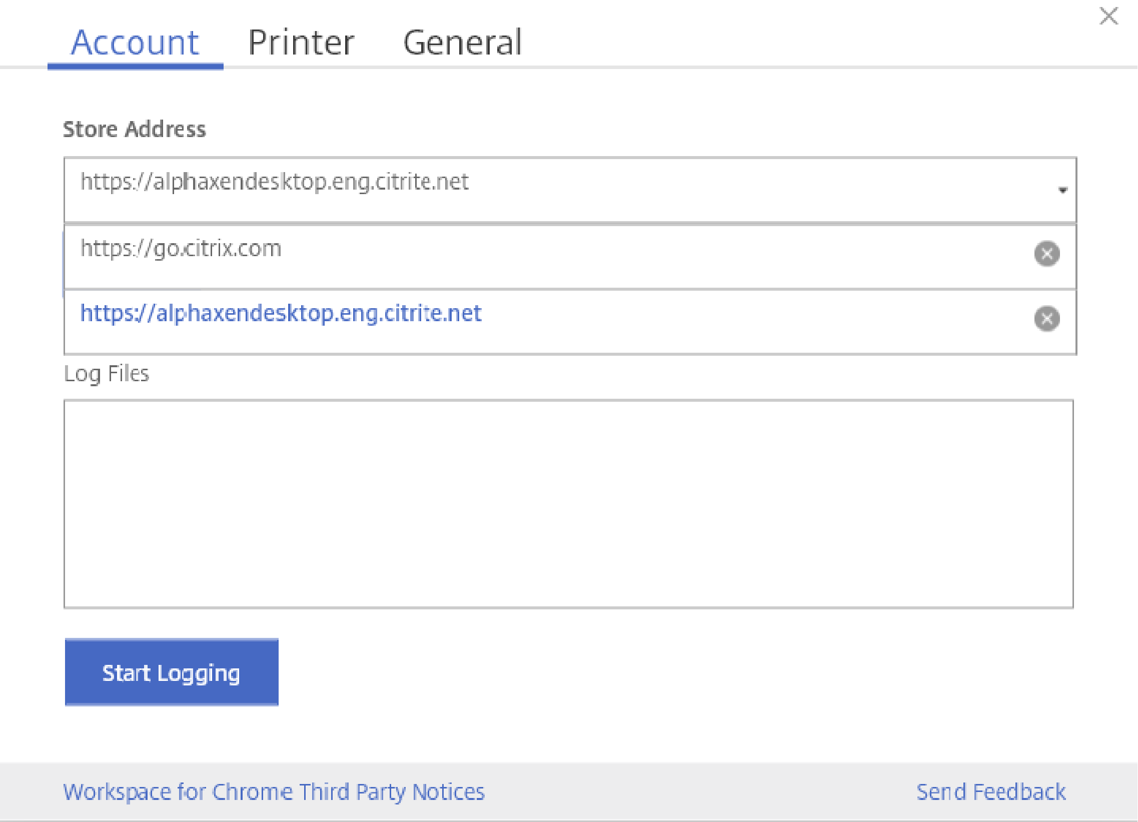
https://go.citrix.com

2. Enter the StoreFront URL in the **Store Address** field.
3. Click **Apply** to save the new store.

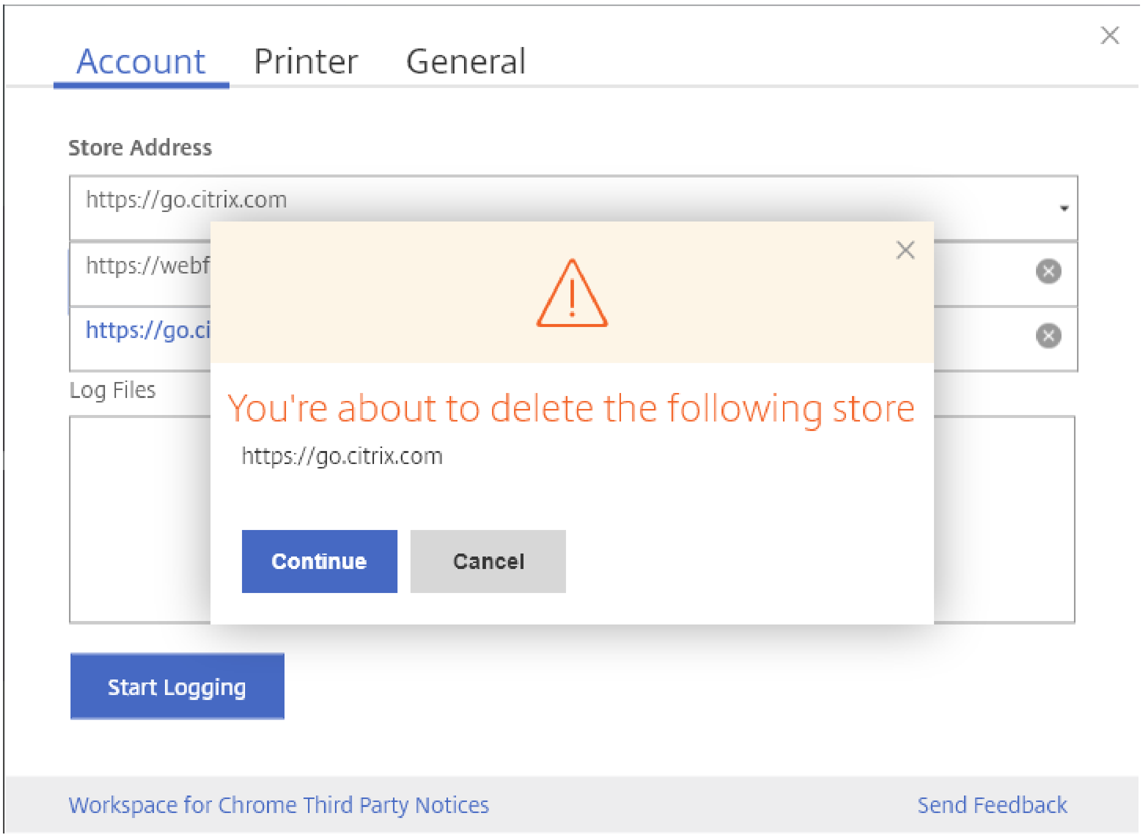


https://alphaxendesktop.eng.citrite.net

4. You can select an existing store from the drop-down list.


Account
Printer
General
Store Address
https://alphaxendesktop.eng.citrite.net
https://go.citrix.com
https://alphaxendesktop.eng.citrite.net
Log Files
Start Logging
Workspace for Chrome Third Party Notices
Send Feedback

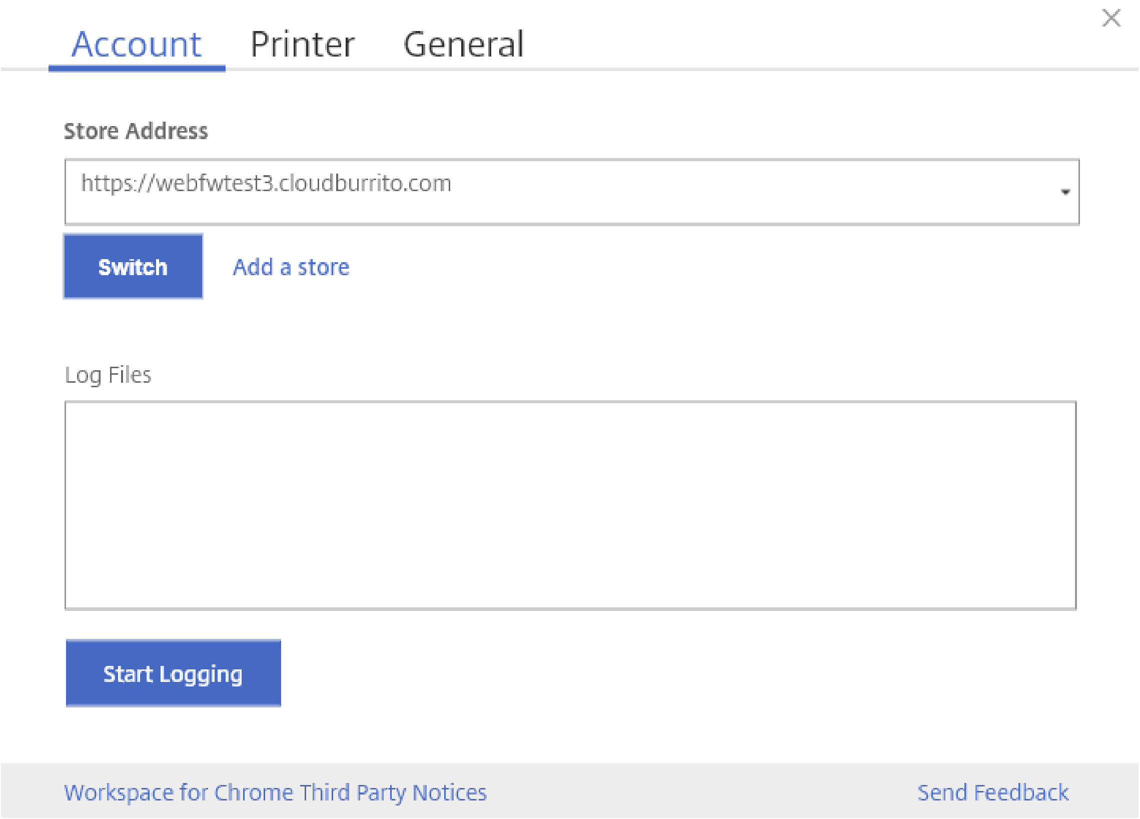
5. To delete a store from the list, click the **Delete** icon next to the store address you want to delete and confirm deletion.



You're about to delete the following store

https://go.citrix.com

6. When you select a different store from the drop down-list, the **Apply** button changes to **Switch**.
7. Click **Switch** to confirm that you want to switch to a different store.



Store Address

https://webfwtest3.cloudburrito.com

Log Files

Feature limitations:

- This feature is supported in user and public modes but not in kiosk mode.
- This feature supports adding up to five stores.

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).
- "h264Support": H.264 protocol support.
- "enabled": H.264 support capability in Thinwire.
- "losslessOverlays": Loss less overlays 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**.

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}}

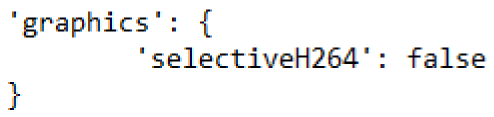
Configuring Selective H.264 using the configuration.js file

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:

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



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

> **Note:**
>
> - Citrix recommends that you back up the configuration.js file.
> - Citrix recommends using this method only when Citrix Workspace app for ChromeOS is repackaged for users.
> - Administrator-level credentials are required to edit the configuration.js file; after editing the file, repackage the app for the changes to take effect.

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.

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:

```
{


      "settings": {


                     "Value": {

```

```
                     "settings\_version": "1.0",
                     "engine\_settings": {

                     "ui": {

                     "sessionsize": {

                     "windowstate": "fullscreen"
                               }

                                       }

                                                }

                             }

                 }

 }

<!--NeedCopy-->
```

Window state on session launch

How to configure

To open desktop sessions in full-screen mode, edit the Google admin policy by including the following. By default, desktop sessions open in maximized windows, where the "window state" value is set to "maximized".

```
{

    "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" : {

                    "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.

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:

```
{

    "settings": {

        "Value": {

            "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"
                 }

             }

         }

     }

 }
```

```


<!--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://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.

Awake setting

About this feature

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.

```
{

 "settings": {

     "Value": {

         "settings_version": "1.0",
         "power_settings": {

             "keep_awake_level": ” system”  or  “display”
              }

            }

         }
```

```

    }

<!--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.

Virtual channels

About this feature

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.

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** 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
                                     }

                                    }

         }

     }

 }


<!--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.

CustomVC

About this feature

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.

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.

Net promoter score

About this feature

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-->
```

Multi-monitor display

About this feature

Multi-monitor supports up to two 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.

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
```

```
                   }

               }

            }

        }

     }

  }


<!--NeedCopy-->
```

> **Note:**
>
> To launch a session in kiosk mode, you must enable **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

About this feature

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
                   }

               }

            }

        }

     }

  }


<!--NeedCopy-->
```

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

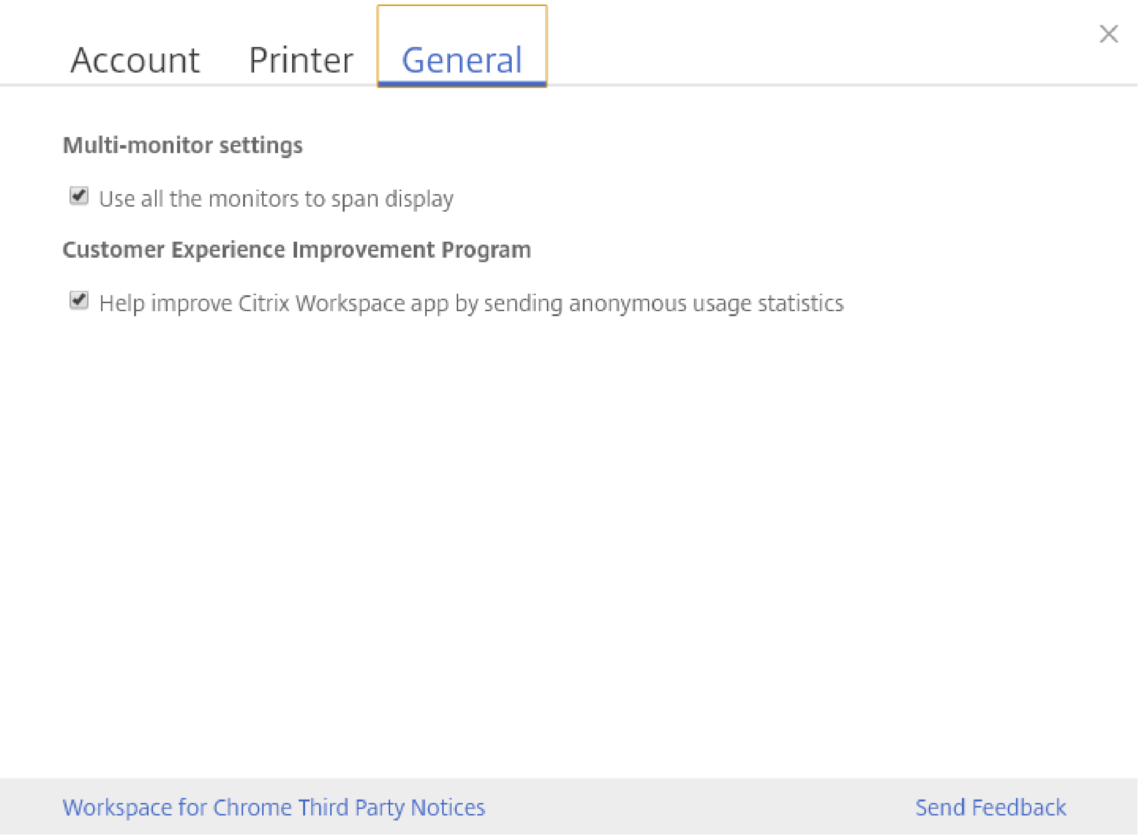
To configure Unified Desktop mode using Google Admin policy

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**.



Multi-monitor settings

☑ Use all the monitors to span display

Customer Experience Improvement Program

☑ Help improve Citrix Workspace app by sending anonymous usage statistics

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 **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.
- 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 two 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.

Microsoft Teams optimization

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.

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 (see Google policies), change the screen sharing value to **true** for msTeamsOptimization as follows:

```
{

  "settings": {

  "Value": {

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

```

```
   "features":{

   "msTeamsOptimization":{

    "screenSharing" : true
                   }

                }

             }

          }

      }

   }


<!--NeedCopy-->
```

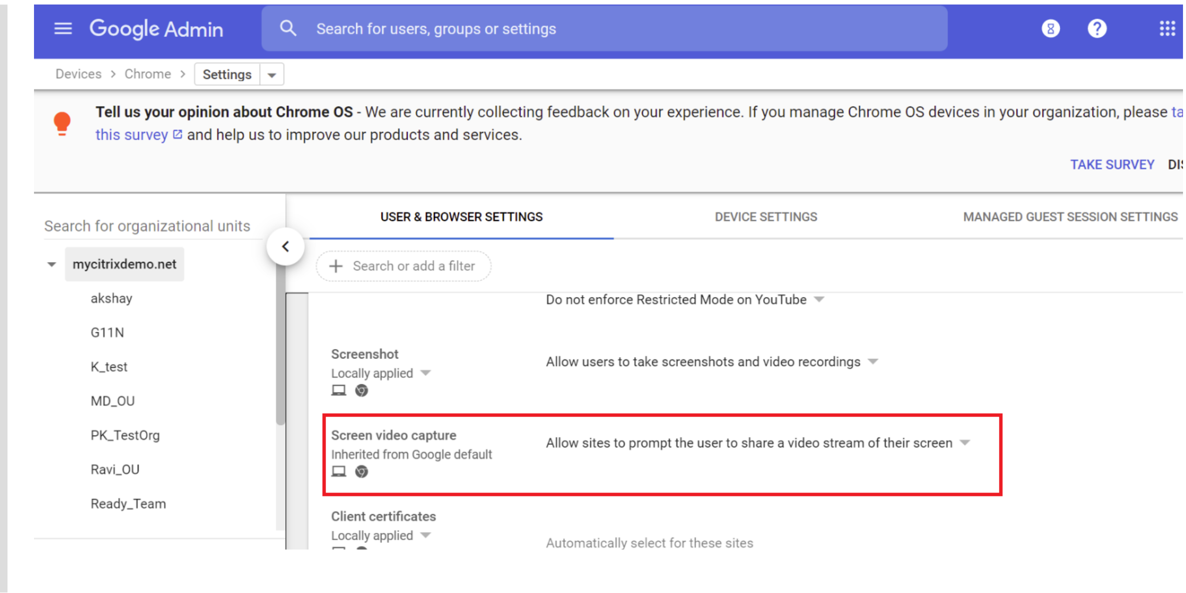
To enable screen sharing for Bring your own device (BYOD) users (only for those using on-prem StoreFront):

Follow the steps in Get started - Using webconfig and add the **chromeAppPreferences** value as follows:

For example:

```
chromeAppPreferences = '{ "features":{ "msTeamsOptimization":{ "screenSharing":true } } } '
```

> **Note:**
>
> Ensure that the following setting is 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** and **Managed Guest Session Settings** (or an appropriate category)



Google Admin
Search for users, groups or settings
Devices > Chrome > Settings

Tell us your opinion about Chrome OS - We are currently collecting feedback on your experience. If you manage Chrome OS devices in your organization, please ta this survey and help us to improve our products and services.

Do not enforce Restricted Mode on YouTube

Screenshot
Locally applied
Allow users to take screenshots and video recordings

Screen video capture
Inherited from Google default
Allow sites to prompt the user to share a video stream of their screen

Client certificates
Locally applied
Automatically select for these sites

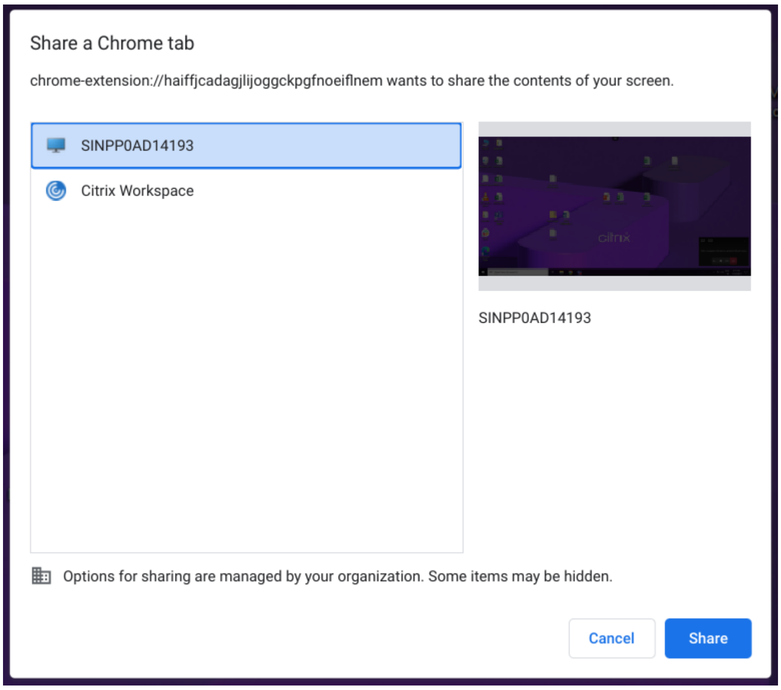
Limit screen sharing of Citrix Workspace app content

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't share resources that aren't opened 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.



Share a Chrome tab

chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem wants to share the contents of your screen.

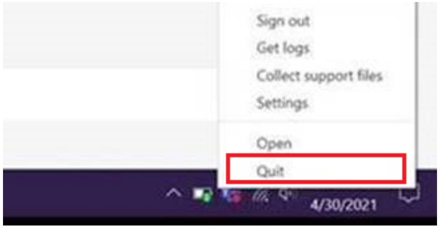
Options for sharing are managed by your organization. Some items may be hidden.

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 Microsoft Teams optimization logs section.

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.

Feature flag management

About this feature

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

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 ensure that your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Status page.

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 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.
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.

Webcam redirection for 64-bit

About this feature

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 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 2010 and earlier:

Configure webcam redirection using the following path: **HTML5_CONFIG > appPrefs > chromeApp > nacl > video**

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 best performance, we recommend using high-end Chromebooks and low-latency networks with good bandwidth connections.
- When you use the speaker of a system during a video conference call, you might hear an echo. As a workaround, use a headset.
- Set the following registry key on a VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

  Name: OfferH264ToApp

  Type: REG_DWORD

  Value: 1

> **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.

Serial COM port redirection

About this feature

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": {

              "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"

 }

<!--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:

```
    net use COM4 : \\Client\COM5
<!--NeedCopy-->
```

> **Tip:**
>
> In the example above, COM4 is the preferred serial port used for redirection.

Citrix Universal Print Driver

About this feature

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.

> **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.

Download the Citrix PDF Printer from the Citrix downloads page.

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**.

Google Drive access

About this feature

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

For example, if a user opens a file in Google Drive (for instance, a .DOC file attachment downloaded from Gmail), edits it, and saves it to Google Drive, the file can be accessed in a Citrix Virtual Apps hosted application. 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 published applications in Citrix Studio.
3. On the Citrix Virtual Apps or Citrix Virtual Apps and Desktops and Citrix DaaS VDA, https://accounts.google.com and `<https://ssl.gstatic.com>` have to be trusted and cookies from these sites should be enabled.

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.

Proxy connection support

The Citrix Workspace app for ChromeOS supports opening documents from 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-->
```

Auto-launch of ICA sessions

About this feature

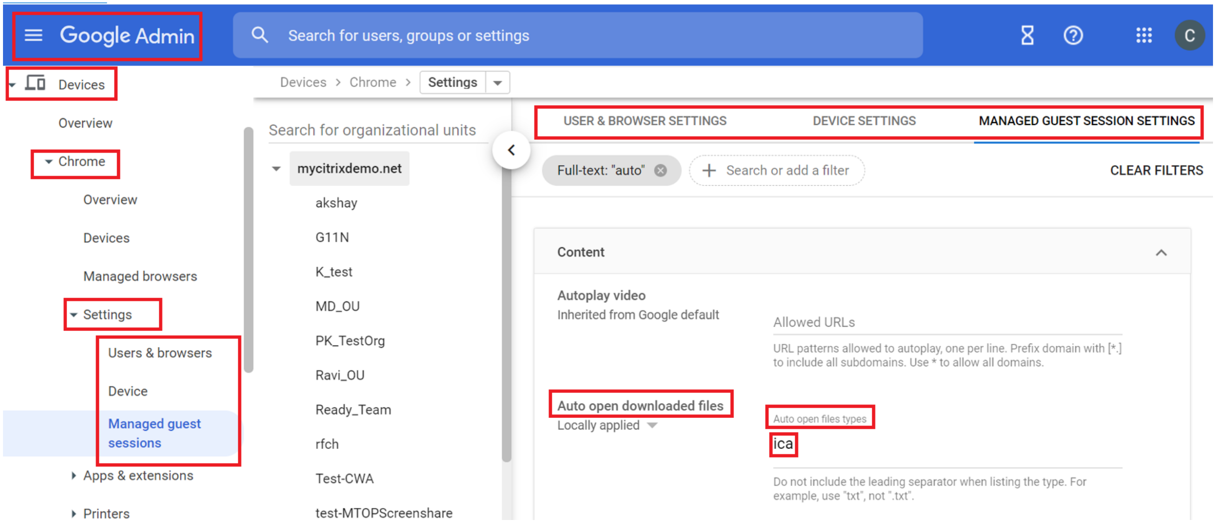
Citrix Workspace app for ChromeOS supports auto-launch of ICA (Independent computing architecture) sessions on Google managed devices or users.

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 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).



Autoplay video
Inherited from Google default

Allowed URLs

URL patterns allowed to autoplay, one per line. Prefix domain with [*.] to include all subdomains. Use * to allow all domains.

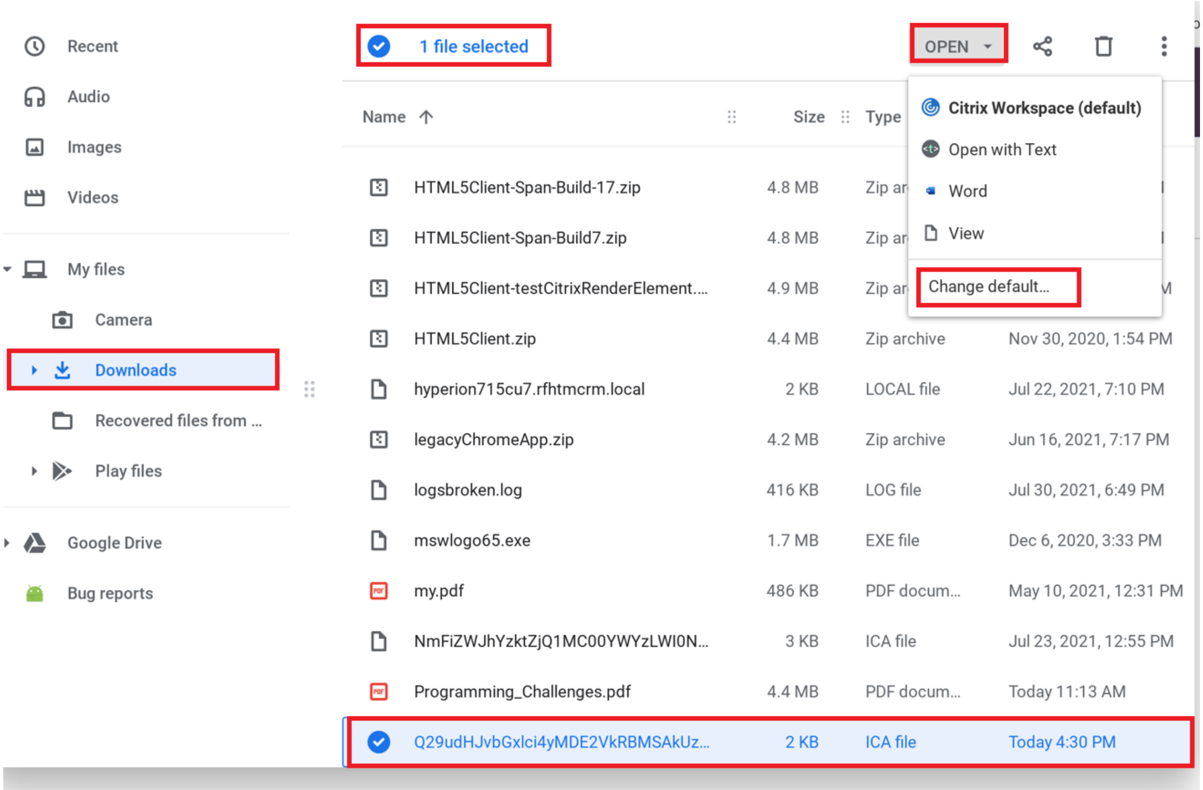
Auto open downloaded files
Locally applied

Auto open files types
ica

Do not include the leading separator when listing the type. For example, use "txt", not ".txt".

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**.



Name	Size	Type	
HTML5Client-Span-Build-17.zip	4.8 MB	Zip ar	
HTML5Client-Span-Build7.zip	4.8 MB	Zip ar	
HTML5Client-testCitrixRenderElement.…	4.9 MB	Zip ar	
HTML5Client.zip	4.4 MB	Zip archive	Nov 30, 2020, 1:54 PM
hyperion715cu7.rfhtmcrm.local	2 KB	LOCAL file	Jul 22, 2021, 7:10 PM
legacyChromeApp.zip	4.2 MB	Zip archive	Jun 16, 2021, 7:17 PM
logsbroken.log	416 KB	LOG file	Jul 30, 2021, 6:49 PM
mswlogo65.exe	1.7 MB	EXE file	Dec 6, 2020, 3:33 PM
my.pdf	486 KB	PDF docum…	May 10, 2021, 12:31 PM
NmFiZWJhYzktZjQ1MC00YWYzLWI0N…	3 KB	ICA file	Jul 23, 2021, 12:55 PM
Programming_Challenges.pdf	4.4 MB	PDF docum…	Today 11:13 AM
Q29udHJvbGxlci4yMDE2VkRBMSAkUz…	2 KB	ICA file	Today 4:30 PM

Kiosk mode

About this feature

Citrix Workspace app for ChromeOS kiosk mode provides the ability 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.

How to configure

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

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 should publish using the visibility options set to `Public/unlisted` to ensure interoperability with kiosk mode. Go to the Chrome Web Store Developer Dashboard

The store URL is read-only when kiosk mode is active and cannot be edited using the **Account** settings screen. However, you can change this setting by either repackaging the app with the .cr file or through

Google Policy Management using the 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": {

    "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-->
```

Excel shortcuts

How to configure

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

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 (see Google Policies), add the **sendAllKeys** attribute, and set the attribute to **false.**

Clipboard

About this feature

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.

How to configure

Configuring 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 and when you paste the data, the destination content carries the formatting as well. In addition, HTML format provides 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.

Shortcuts

About this feature

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, cannot be used with Citrix Workspace app for ChromeOS.

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

USB device redirection

About this feature

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, including the 3D Space mouse, other composite devices, Bloomberg keyboards, and the UC-Logic Tablet WP5540U.

How to configure

For information on configuring USB devices, see Knowledge Center article CTX200825.

Automatic redirection of USB devices

About this feature

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 multiple sessions are running, 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**.

File transfer

About this feature

Citrix Workspace app for ChromeOS provides secure file transfer functionality between a user device and a 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.

> **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.

How to configure

Configuring 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 requirent.

> **Note:**
>
> Citrix recommends that you back up the **configuration.js** file before modifying it. Administrator level credentials are required to edit the configuration.js file; After editing the file, repackage the app to make more modifications to 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 policy 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.

```
{

    "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 file uploads from device to remote session.
- "allowdownload": Allows downloads from device to remote session.
- "maxuploadsize": The maximum file size, in bytes, that can be uploaded. By default, set to 2,147,483,648 bytes (2 GB).
- "maxdownloadsize": The maximum file size, in bytes, that can be downloaded. By default, set to 2,147,483,648 bytes (2GB).

Taskbar icons

About this feature

Applications and desktops that are configured using Citrix Virtual Apps and Desktops and Citrix DaaS in an active session are displayed as separate apps in the taskbar (shelf) on a Chrome 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.

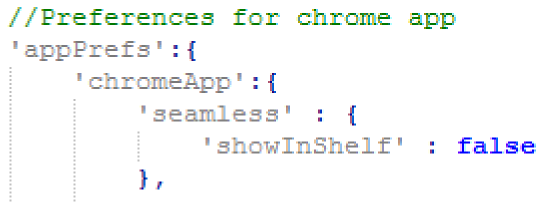
By default, this feature is enabled.

How to configure

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\<Storena 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}}

Configuring taskbar icons using the configuration.js file

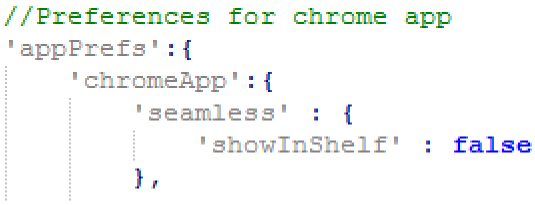
The **configuration.js** file is in the **ChromeApp root** folder. Access this file directly to modify Citrix Workspace app.

> **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:

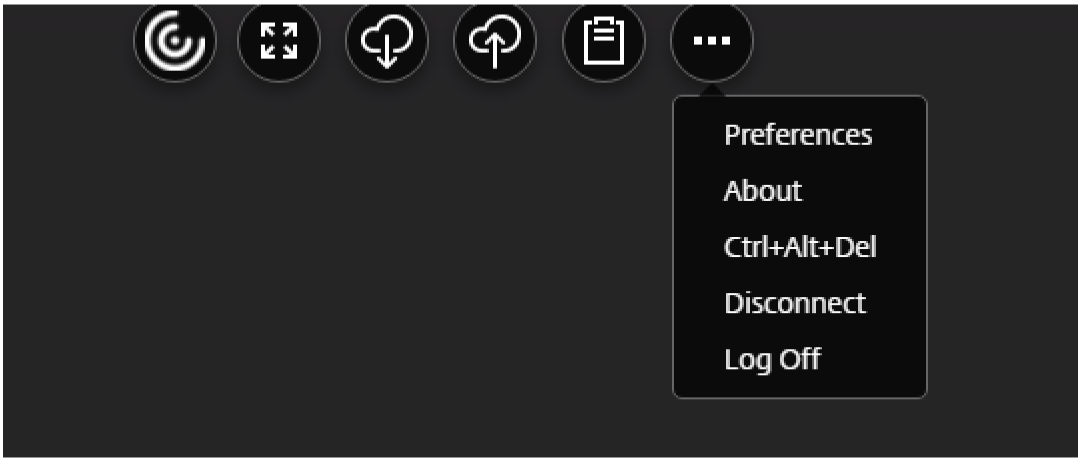
1. When more than one instance of the same application is launched, the app icon isn't stacked and appears as two separate icons. For example, two instances of Notepad display two icons of Notepad in the taskbar.
2. App pinning isn't supported.

In-session toolbar and dialogs

About this feature

The in-session toolbar is a floating toolbar that can be moved anywhere on the screen. The toolbar has 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



> **Note:**
>
> On the touch-enabled devices, the Citrix Workspace app icon appears at the top center to indicate the floating toolbar during desktop sessions. On non-touch-enabled devices, a menu button indicating the floating toolbar transforms to the 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,
                            "gestureGuide":true
                                  }

                      }

                 }

         }

     }

 }


<!--NeedCopy-->
```

List of in-session toolbar options and their descriptions:

- "menubar": 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 located 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:

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

> **Note:**
>
> - Citrix recommends that you back up the configuration.js file before making any changes to it.
> - Administrator-level credentials are required to edit the configuration.js file; after editing the file, repackage the app for the changes to take effect.

App switcher

About this feature

Shows the apps that are launched 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 an app switcher, use the Google admin policy by including the following:

```
{

    "settings": {

        "Value": {

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

                    "ui": {

                        "appSwitcher": {

                            "showTaskbar": true,
                            "showIconsOnly": false,
                            "autoHide": false
                                         }

                           }

                    }

         }

     }

 }


<!--NeedCopy-->
```

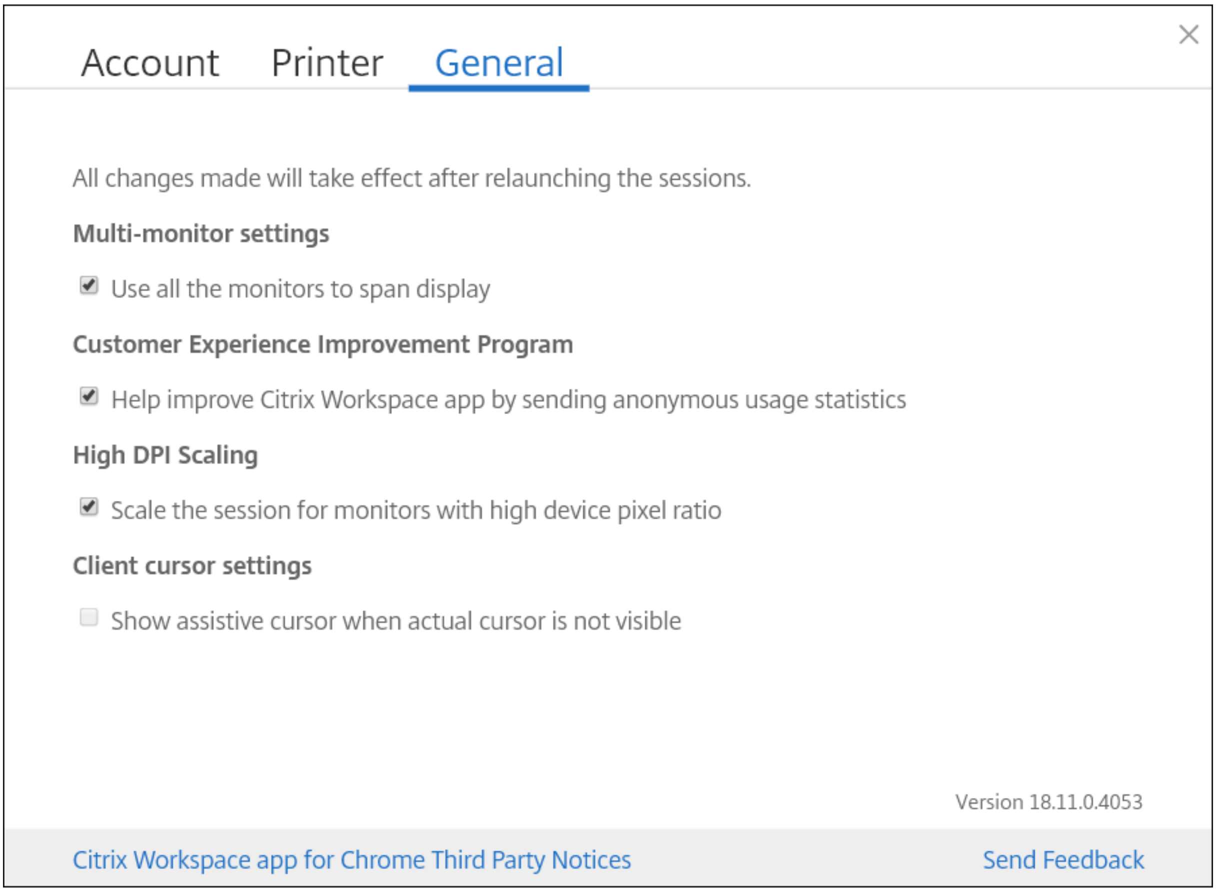
List of appSwitcher options with their descriptions:

- “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.

Assistive cursor

About this feature

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



All changes made will take effect after relaunching the sessions.

Multi-monitor settings

☑ Use all the monitors to span display

Customer Experience Improvement Program

☑ Help improve Citrix Workspace app by sending anonymous usage statistics

High DPI Scaling

☑ Scale the session for monitors with high device pixel ratio

Client cursor settings

☐ Show assistive cursor when actual cursor is not visible

Version 18.11.0.4053

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
                     }

                 }
```

```

             }

         }

 }


<!--NeedCopy-->
```

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

Splash screen

About this feature

Citrix Workspace app displays a splash screen on the first launch with the text "Citrix Workspace app extends the capabilities of Citrix Receiver."

How to configure

To configure the display of the splash screen, use the Google admin policy by including the following. It's enabled by default. To disable, set the enabled attribute under the splash screen to false.

```
{

    "settings": {

        "Value": {

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

                "ui": {

                    "splashScreen": true
                     }

```

```
                 }

             }

         }

 }


<!--NeedCopy-->
```

List of splash screen options with their descriptions:

- "splash screen": If set to true, the splash screen appears.

DPI scaling

About this feature

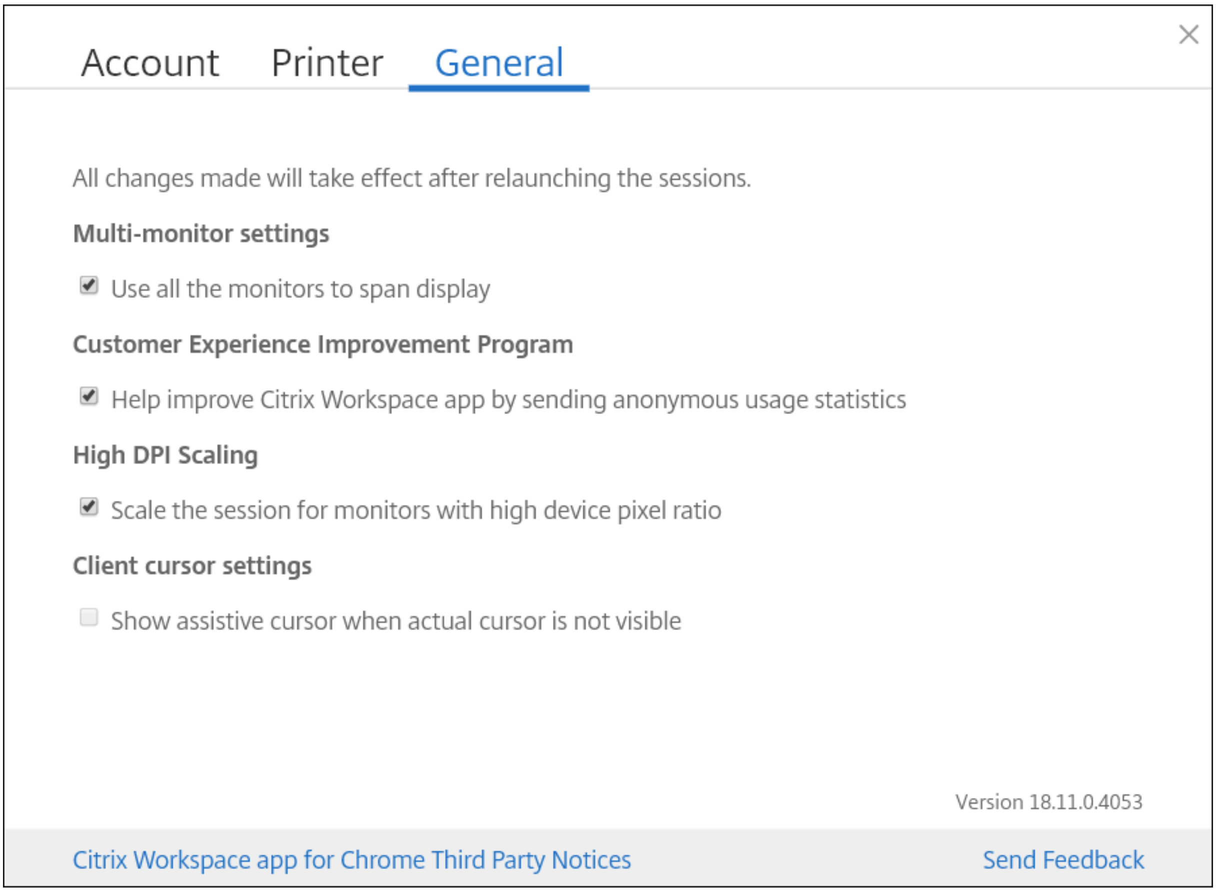
Citrix Workspace app for ChromeOS allows the operating system to control the resolution of app and desktop sessions and supports DPI client scaling for app sessions on a single monitor.

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** check box.

How to configure

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



All changes made will take effect after relaunching the sessions.

Multi-monitor settings

☑ Use all the monitors to span display

Customer Experience Improvement Program

☑ Help improve Citrix Workspace app by sending anonymous usage statistics

High DPI Scaling

☑ Scale the session for monitors with high device pixel ratio

Client cursor settings

☐ Show assistive cursor when actual cursor is not visible

Version 18.11.0.4053

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 **scaleToDPI** property to **false**.

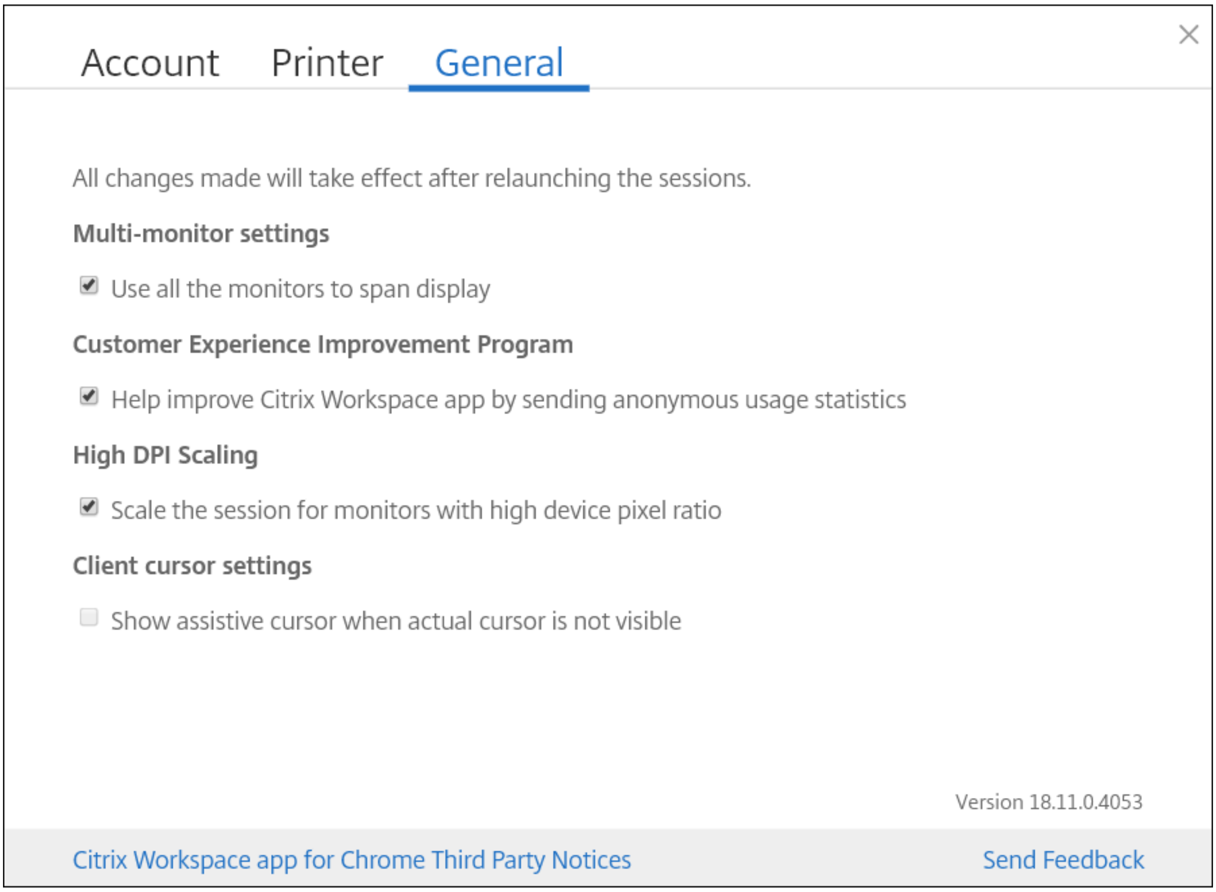
```
{

    "settings": {

                "Value": {

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

       'features' : {
```

```

       'graphics' : {

                'dpiSetting': {

                                'scaleToDPI': false
                                 }

                              }

                        }

                     }

                 }

             }

          }



<!--NeedCopy-->
```

Assistive cursor

About this feature

When a cursor isn't visible inside a desktop session, you can enable an assistive cursor. Launch the next session for the setting to take effect.



All changes made will take effect after relaunching the sessions.

Multi-monitor settings

☑ Use all the monitors to span display

Customer Experience Improvement Program

☑ Help improve Citrix Workspace app by sending anonymous usage statistics

High DPI Scaling

☑ Scale the session for monitors with high device pixel ratio

Client cursor settings

☐ Show assistive cursor when actual cursor is not visible

Version 18.11.0.4053

How to configure

The assistive cursor feature is disabled by default.

To enable the feature, edit the **Google Admin Console** policy and set the value of the **assistiveCursor** property under **ui** to **true** and then restart the session.

```
{

    "settings": {

        "Value": {

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

                "ui": {

                    "assistiveCursor": true
                     }

                }

            }

        }

    }


<!--NeedCopy-->
```

Note:

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

Native client

About this feature

Allows running native codes safely from a web browser that is independent of the user's operating system. This functionality allows web apps to run at near-native speeds.

How to configure

To configure a native client, use the Google admin policy by including the following. By default, the native client option is enabled. To disable it, set the enabled attribute under the native client to false.

```
{

    "settings": {

        "Value": {

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

                    "ui": {

                            "Nacl" : {

                                 "supportNacl" : true,
                                 "graphics": {

                                         "enable": true,
                                         "config": {

                                                "acceleration": 2
                                                     }

                                             }
 ,
                                 "video":    {

                                            "enable": true
                                              }

 ,
                                 "audio":    {

                                            "enable": true
                                              }

                              }

                      }

                  }

          }

      }

 }


<!--NeedCopy-->
```

List of native client options with their descriptions:

- "supportNacl": Supports native client.
- "graphics": Enables native client graphics module.
- "config": Selects h264 hardware or software decoder.
  - Software = 0
  - Hardware = 1
  - Hardware with fallback = 2
  - AutoDetect = 3

- "video": Enables webcam redirection.
- "audio": Enables audio input or microphone redirection.

Unique ID and Asset ID

About this feature

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:

```
{

    "settings": {

        "Value": {

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

                        "uniqueID" : {

                                 "prefixKey" : "CR-",
                                 "restrictNameLength" : true,
                                 "useAssetID": false
                                      }

                                   }

         }

     }

 }


```

```
<!--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:

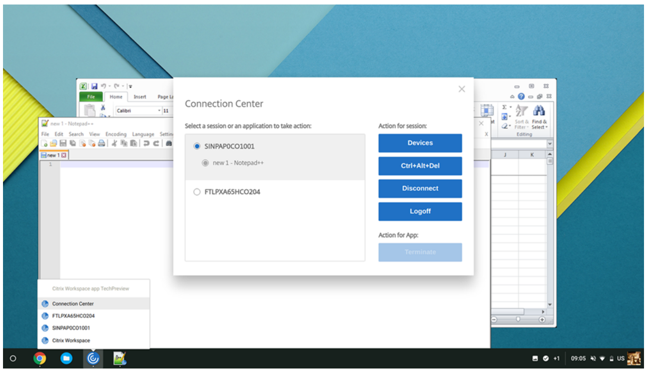
- You must have a Google admin policy that can be pushed. Otherwise, the current method of generating a unique client ID for managed Chromebooks remains in use.
- Do not enter a value that has more than 15 characters. Values longer than 15 characters are truncated to 15 characters.

Connection Center

About this feature

Connection Center helps application management in seamless sessions. This is done 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**.



Connection Center

Select a session or an application to take action:

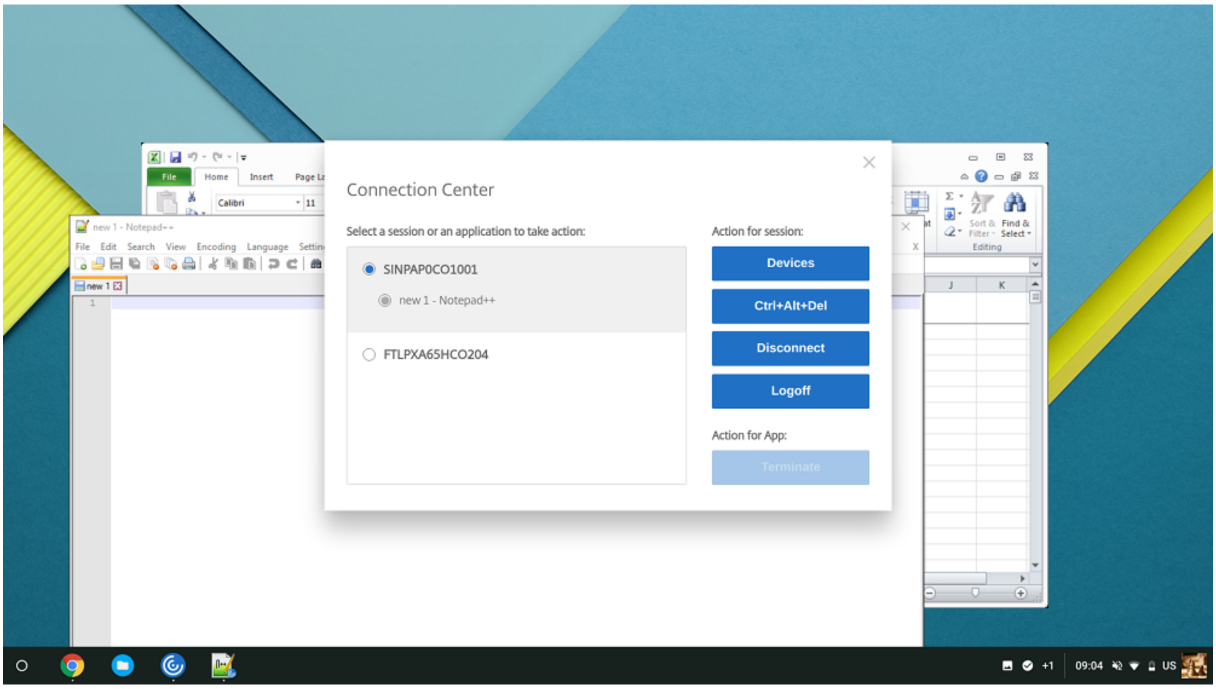
● SINPAP0CO1001

● new 1 - Notepad++

○ FTLPXA65HCO204

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.



Connection Center

Select a session or an application to take action:

● SINPAP0CO1001

● new 1 - Notepad++

○ FTLPXA65HCO204

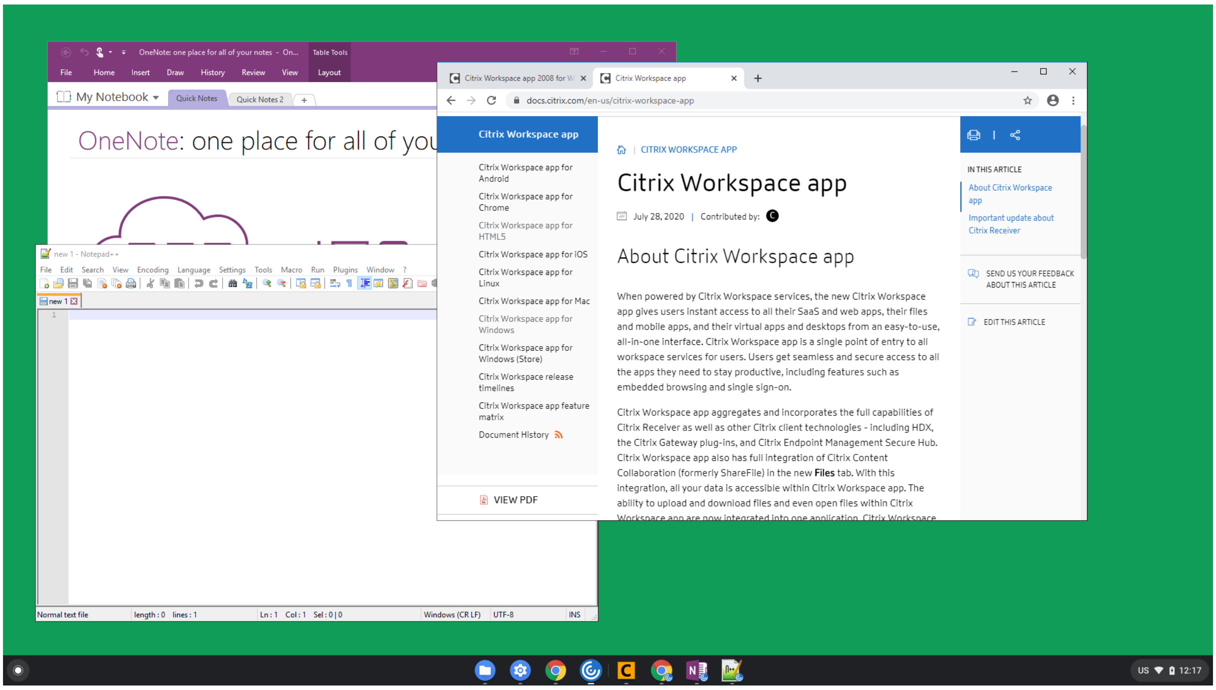
You can also terminate an app using the Connection Center by selecting the radio button of the corresponding application and clicking **Terminate**.

Seamless window integration

About this feature

Citrix Workspace app for ChromeOS improves the user experience by adding seamless integration of multiple apps hosted in separate windows within an active session. Using this functionality, Citrix Workspace app for ChromeOS enables you to launch applications in an independent user interface compared as opposed to launching 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.


OneNote: one place for all of your notes - On...
Table Tools
File
Home
Insert
Draw
History
Review
View
Layout
My Notebook
Quick Notes
Quick Notes 2
OneNote: one place for all of you
new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
Normal text file
length : 0 lines : 1
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS
Citrix Workspace app 2008 for W
Citrix Workspace app
docs.citrix.com/en-us/citrix-workspace-app
Citrix Workspace app
Citrix Workspace app for Android
Citrix Workspace app for Chrome
Citrix Workspace app for HTML5
Citrix Workspace app for iOS
Citrix Workspace app for Linux
Citrix Workspace app for Mac
Citrix Workspace app for Windows
Citrix Workspace app for Windows (Store)
Citrix Workspace release timelines
Citrix Workspace app feature matrix
Document History
VIEW PDF
CITRIX WORKSPACE APP
IN THIS ARTICLE
About Citrix Workspace app
Important update about Citrix Receiver
SEND US YOUR FEEDBACK ABOUT THIS ARTICLE
EDIT THIS ARTICLE
US
12:17

Citrix Workspace app

July 28, 2020 | Contributed by: C

About Citrix Workspace app

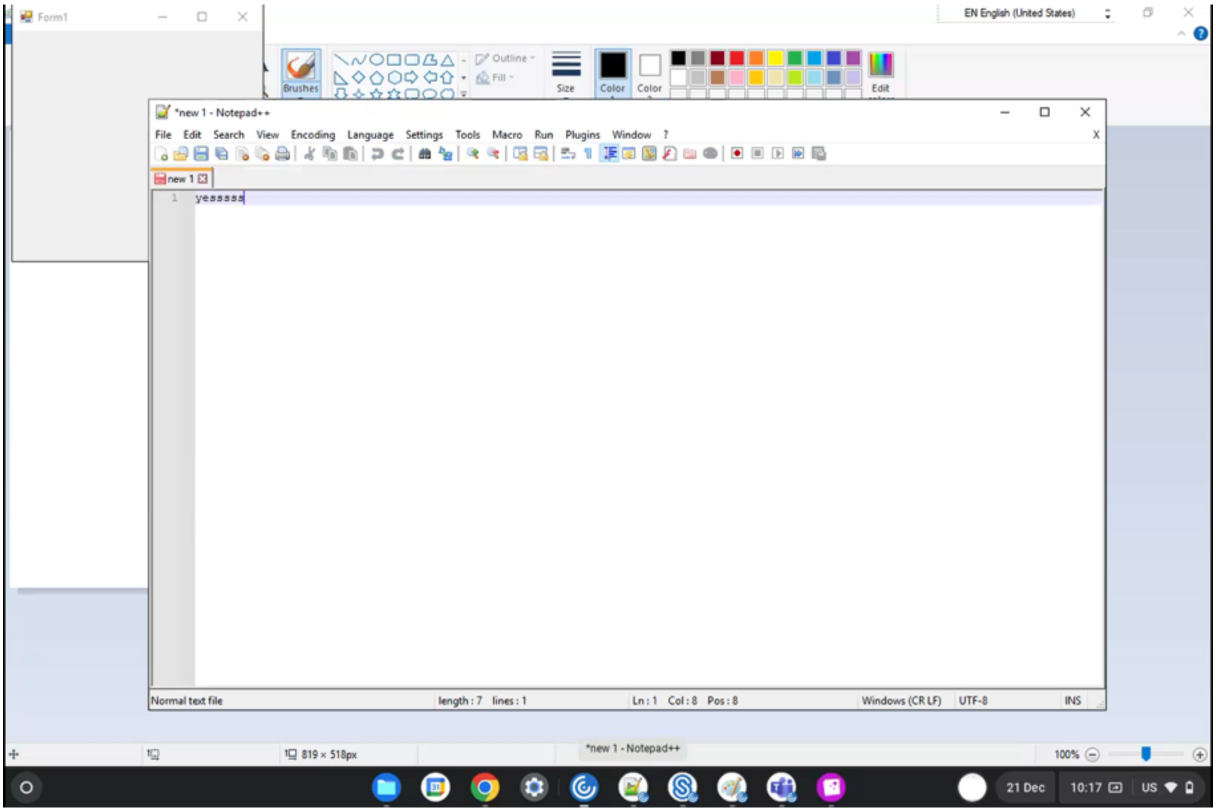
When powered by Citrix Workspace services, the new Citrix Workspace app gives users instant access to all their SaaS and web apps, their files and mobile apps, and their virtual apps and desktops from an easy-to-use, all-in-one interface. Citrix Workspace app is a single point of entry to all workspace services for users. Users get seamless and secure access to all the apps they need to stay productive, including features such as embedded browsing and single sign-on.

Citrix Workspace app aggregates and incorporates the full capabilities of Citrix Receiver as well as other Citrix client technologies - including HDX, the Citrix Gateway plug-ins, and Citrix Endpoint Management Secure Hub. Citrix Workspace app also has full integration of Citrix Content Collaboration (formerly ShareFile) in the new **Files** tab. With this integration, all your data is accessible within Citrix Workspace app. The ability to upload and download files and even open files within Citrix Workspace app are now integrated into one application. Citrix Workspace

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 session taskbar to quickly move between apps:



> **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.

Reload store

About this feature

In 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.

Audio

About this feature

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.

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 **EnableStereoRecording** to **false**.

   Following is an example of JSON data:

```
'features' : {

    'audio' : {

    'EnableAdaptiveAudio': true
             }

 }


'features' : {

    'audio' : {

        'EnableStereoRecording': false
             }

 }

<!--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.

   Following is an example of JSON data:

```
'features' : {

    'audio' : {

        'EnableAdaptiveAudio': {

            "type": "boolean" }

                     }

                 }


'features' : {

    'audio' : {

        'EnableStereoRecording': {

            "type": "boolean" }

                 }

             }

<!--NeedCopy-->
```

4. Save the changes.

Webcam

About this feature

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 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.

Session sharing

About this feature

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.

Host to client redirection

About this feature

Content redirection allows you to control whether users access information by:

- using applications that are published on servers or
- 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.

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.

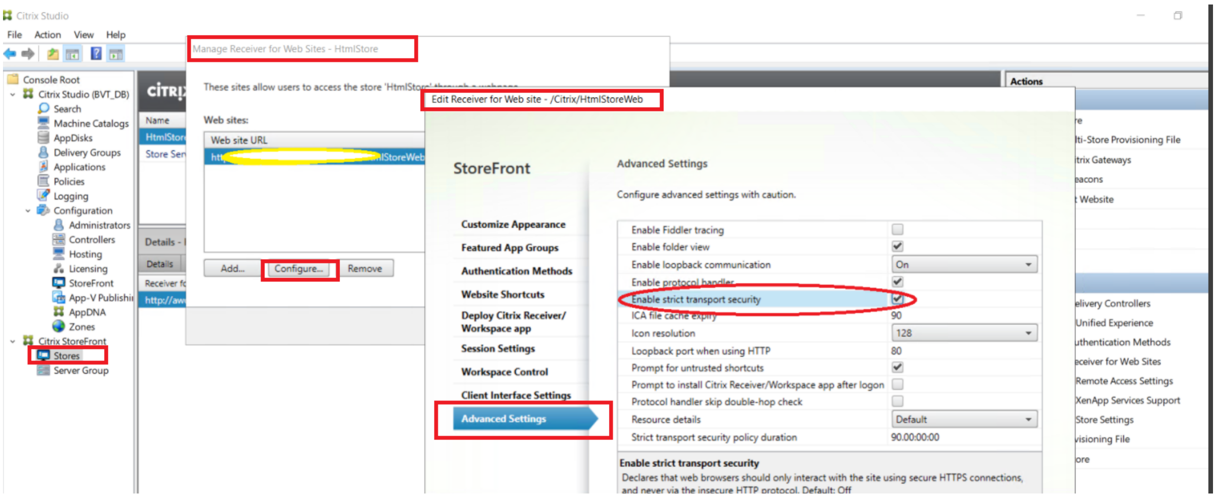
Security settings

How to configure

Citrix recommends using stores that are secure. Besides, it's a good practice to have HTTP strict transport security (HSTS) setting enabled for secure stores.

Do the following steps to enable the HSTS setting:

1. In **Citrix StoreFront**, under **Stores**, click the link of the particular store to enable the security settings.
2. The **Manage Receiver for Web Sites** dialog box appears.
3. Click **Configure**.
4. The **Edit Receiver for Web site** dialog box appears.
5. Click the **Advanced Settings** tab and select **Enable strict transport security**.



Edit Receiver for Web site - /Citrix/HtmlStoreWeb

Advanced Settings

Configure advanced settings with caution.

Enable Fiddler tracing	□
Enable folder view	☑
Enable loopback communication	On
Enable protocol handler	☑
Enable strict transport security	☑
ICA file cache expiry	90
Icon resolution	128
Loopback port when using HTTP	80
Prompt for untrusted shortcuts	☑
Prompt to install Citrix Receiver/Workspace app after logon	□
Protocol handler skip double-hop check	□
Resource details	Default
Strict transport security policy duration	90.00:00:00

Enable strict transport security
Declares that web browsers should only interact with the site using secure HTTPS connections, and never via the insecure HTTP protocol. Default: Off

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.

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 **Use all the monitors to span display** option.

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.

Workspace with intelligence

With this release, Citrix Workspace app is optimized to take advantage of the Workspace intelligence features. This version unifies user workflows and provides an activity feed displaying relevant information. The microapps streamline end user workflows and approvals. For more information, see Workspace Intelligence Features - Microapps.

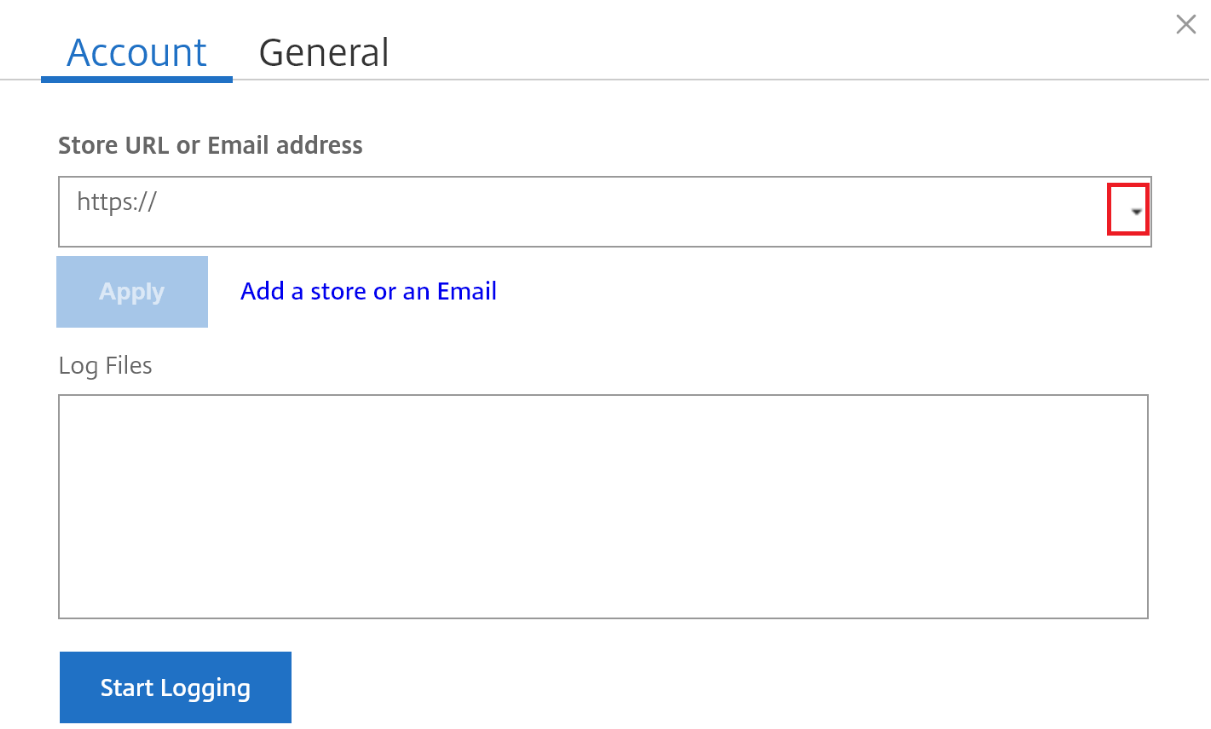
Troubleshooting enhancement

Citrix Workspace app supports log collection for ongoing virtual desktop and app sessions. 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**.

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.



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.

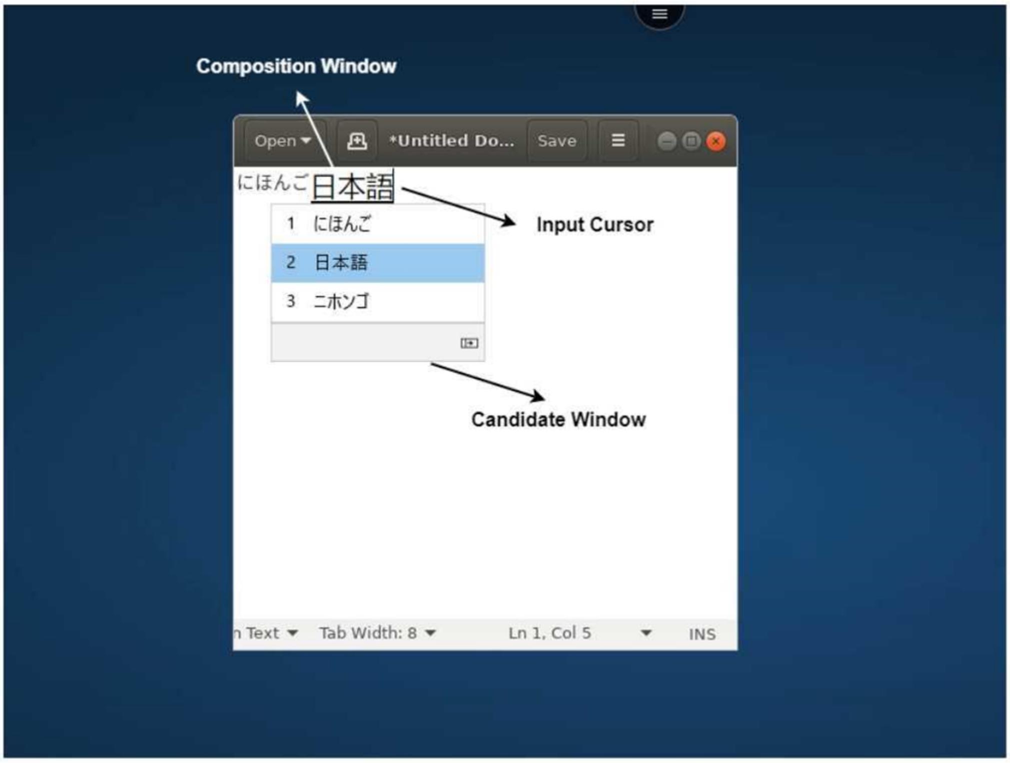
Generic client IME for east asian languages

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.

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.

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.



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.

Feature limitation:

- Character composition is unsuccessful within the Microsoft Excel cell. The issue happens when the cell is selected using a mouse click. [RFHTMCRM-6086]
- Multi-monitor sessions don't support the Generic client IME feature. Instead, use **Server IME**. To enable the **Server IME**:
  1. Change the VDA or the server keyboard language to Chinese, Japanese or Korean (CJK) as wished.
  2. Change the client or 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": {

        "features": {

          "ime": {

            "genericIME": false
           }

          }

        }

     }

     }

 }

<!--NeedCopy-->
```

Service continuity Technical preview

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.

> **Note:**
>
> This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form https://podio.com/webforms/27890077/2184098.

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]
- Printing is not supported from BCR-redirected pages.
- In the seamless app sessions, you might be unable to click on any links or elements on the BCR overlay. [HDX-42950]

Composite USB redirection

Previously, when a composite USB device was connected to the local device, it could 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 could not decide which component 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 are redirected 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 multiple child devices share a single connection with the same USB bus. Such devices employ a single configuration space and shared bus connection where a unique interface number 00-ff is used to identify each child device. 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 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.

To resolve these issues, Citrix recommends that you split the composite device and forward only the child interfaces that use a generic USB channel. Such a mechanism ensures 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**.

Following is an example of JSON data:

~~~
```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

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

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 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.

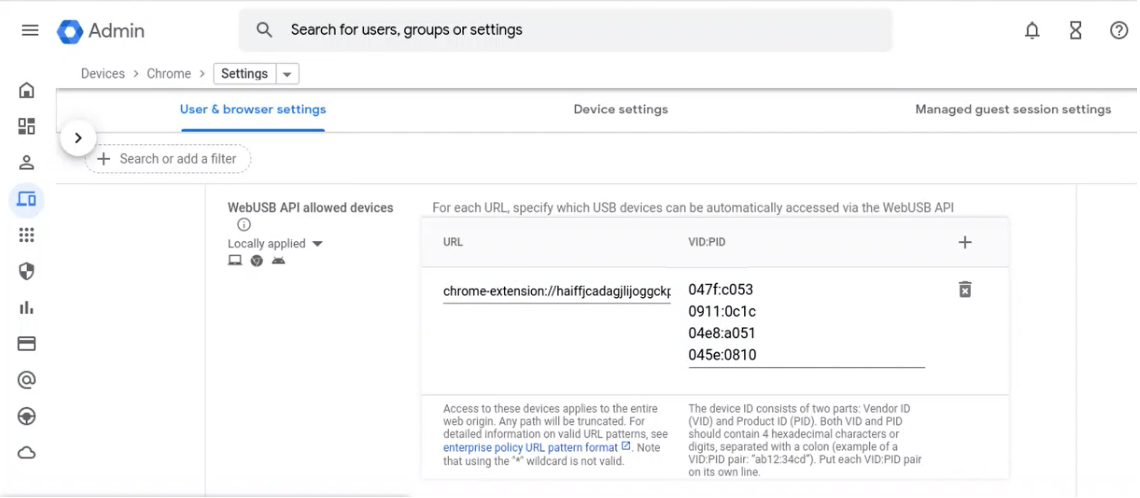
Configuration

Prerequisites:

- White list 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.

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:


Admin
Search for users, groups or settings
Devices > Chrome > Settings
User & browser settings
Device settings
Managed guest session settings
Search or add a filter
Locally applied

WebUSB API allowed devices

For each URL, specify which USB devices can be automatically accessed via the WebUSB API

URL	VID:PID
chrome-extension://haiffjcadagjlijoggckp	047f:c053 0911:0c1c 04e8:a051 045e:0810

Access to these devices applies to the entire web origin. Any path will be truncated. For detailed information on valid URL patterns, see enterprise policy URL pattern format. Note that using the "*" wildcard is not valid.

The device ID consists of two parts: Vendor ID (VID) and Product ID (PID). Both VID and PID should contain 4 hexadecimal characters or digits, separated with a colon (example of a VID:PID pair: "ab12:34cd"). Put each VID:PID pair on its own line.

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. Following is an example of JSON data:

```
{

"settings": {

        "Value": {

        "settings_version": "1.0",
            "device_settings": {

                "deviceRules": {

                            "allow": [{

                                    "vid": "046D",
                                    "pid": "C31C",
                                    "split": true,
                                    "interfaceClass": ["video", "hid"]
                                     }
 ,
                                    {

                                    "vid": "04E8",
                                    "pid": "A051",
                                    "split": true
                                     }
 ],
                                "deny": [{

                                    "vid": "0911",
                                    "pid": "0C1C",
                                    "split": true,
                                    "interfaceClass": ["audio"]
                                     }
 ],
                                "autoRedirect": [{

                                    "vid": "47F",
                                    "pid": "C053",
                                    "split": true,
                                    "interfaceClass": ["hid"]
                                     }
 ]
                                 }

                         }

                 }

         }

 }

<!--NeedCopy-->
```

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 explanation 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.

  > **Note:**
  >
  > - Each object represents a device with mandatory 'vid' and 'pid' values of the USB device. It is 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 Hexa decimal 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.

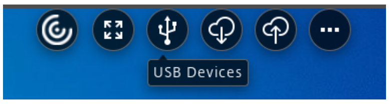
Following is an example of JSON data:

```
"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"] }
  //split device and auto redirect only the 'hid' interface when the device is connected.
    ]
 }

<!--NeedCopy-->
```

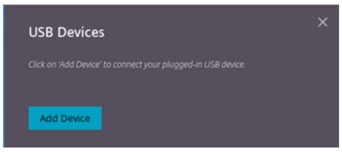
How to use this feature

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:



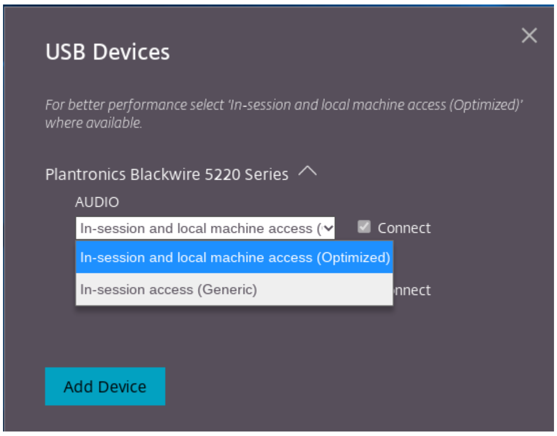
USB Devices

Click on 'Add Device' to connect your plugged-in USB device.

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.



USB Devices

For better performance select 'In-session and local machine access (Optimized)' where available.

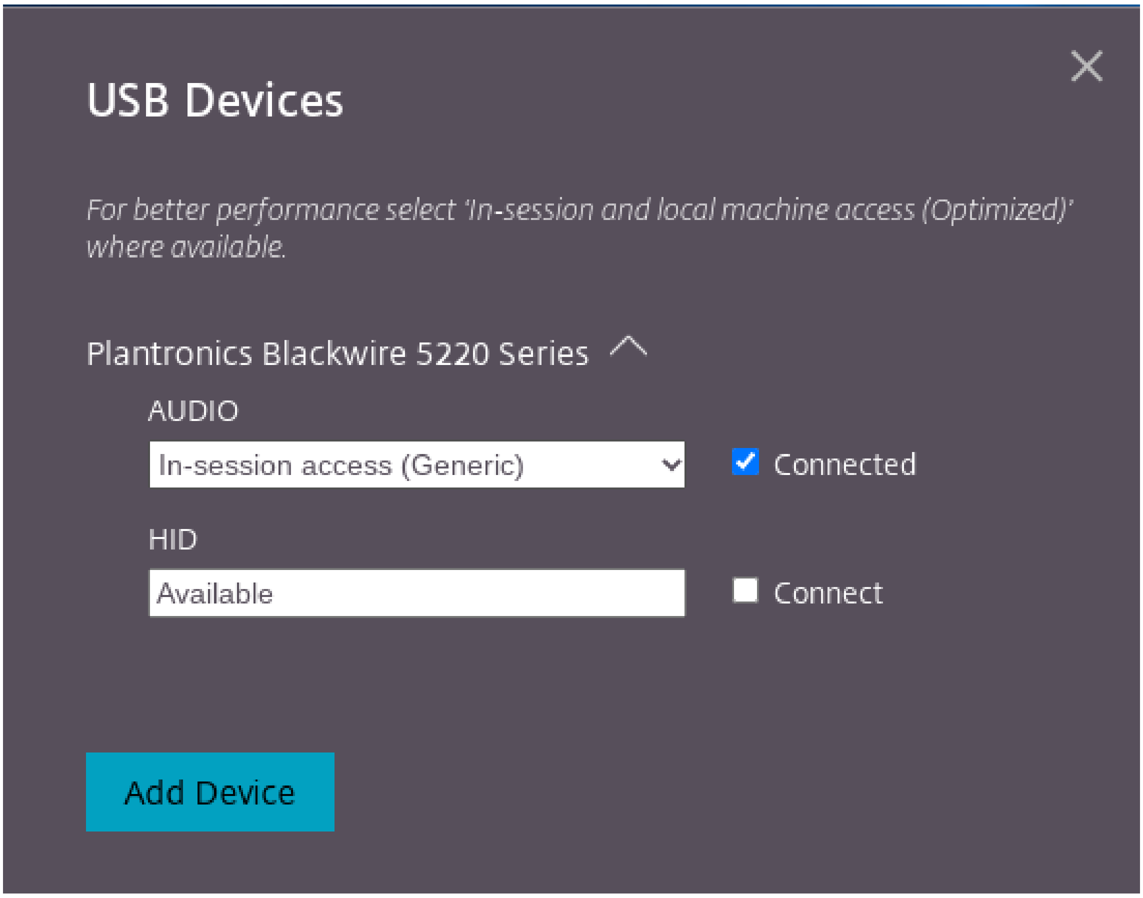
Plantronics Blackwire 5220 Series

AUDIO

In-session and local machine access (Optimized) ☑ Connect

In-session and local machine access (
In-session and local machine access (Optimized)
In-session access (Generic)
nnect
Add Device

4. Select **Connect** for redirecting the interface.



USB Devices

For better performance select 'In-session and local machine access (Optimized)' where available.

Plantronics Blackwire 5220 Series

AUDIO

In-session access (Generic) ☑ Connected

HID

Available □ Connect

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.
> - 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.

Troubleshoot

January 11, 2023

How to collect logs

Logging

Citrix Workspace app for ChromeOS provides timestamps for the logs generated by the user device.

As an end user, to assist with troubleshooting connection issues, logs can be generated on both the user device and the machines providing desktops and applications.

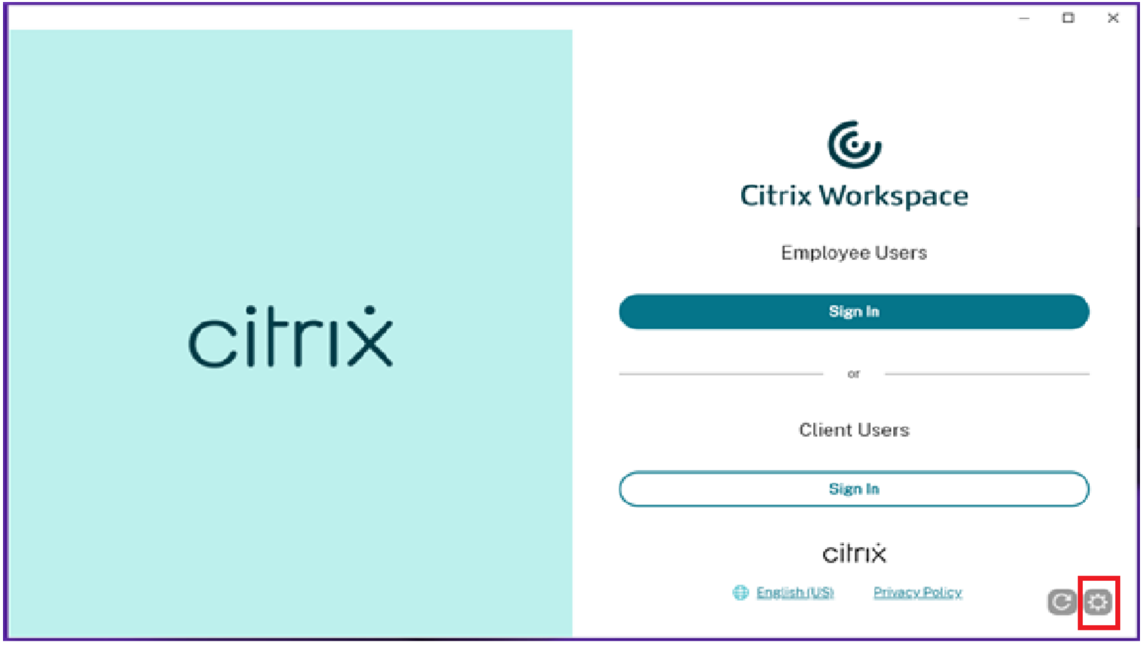
To enable logging on user devices

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**.

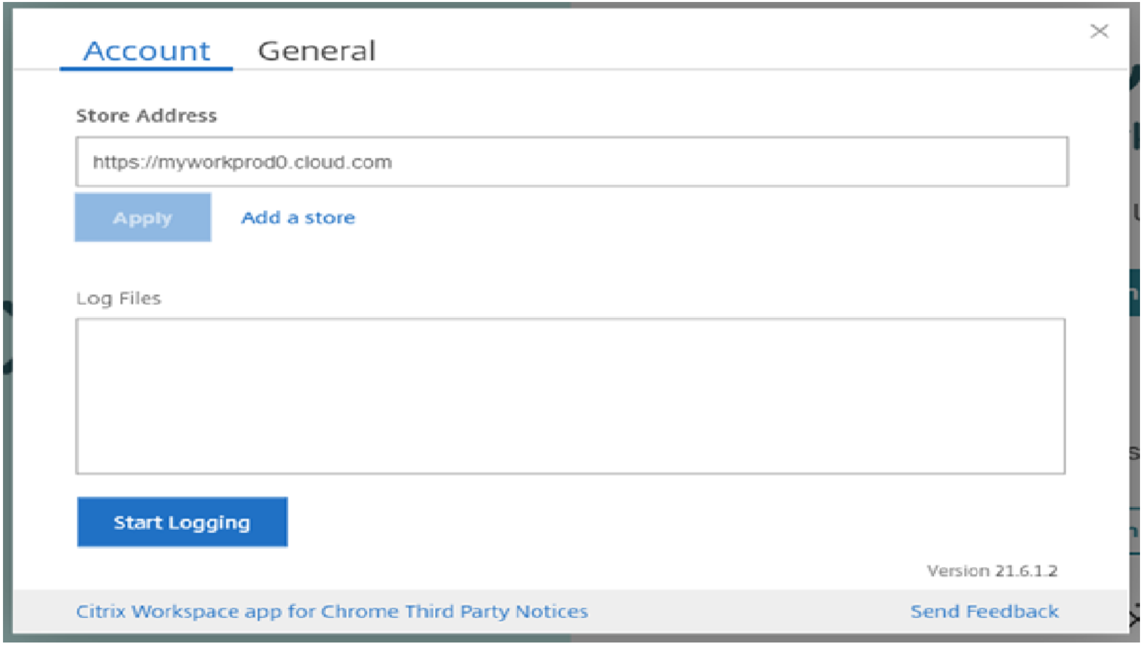
   Details of the collected log files are listed in the **Settings** dialog.
4. Select **Stop Logging** to end the collection of logs on the user device.

Client logs

1. Click the **Settings** button on the bottom right of the Citrix Workspace app **Sign In** screen.



2. Click the **Start Logging** button under **Account** to enable collection of logs.



Account General

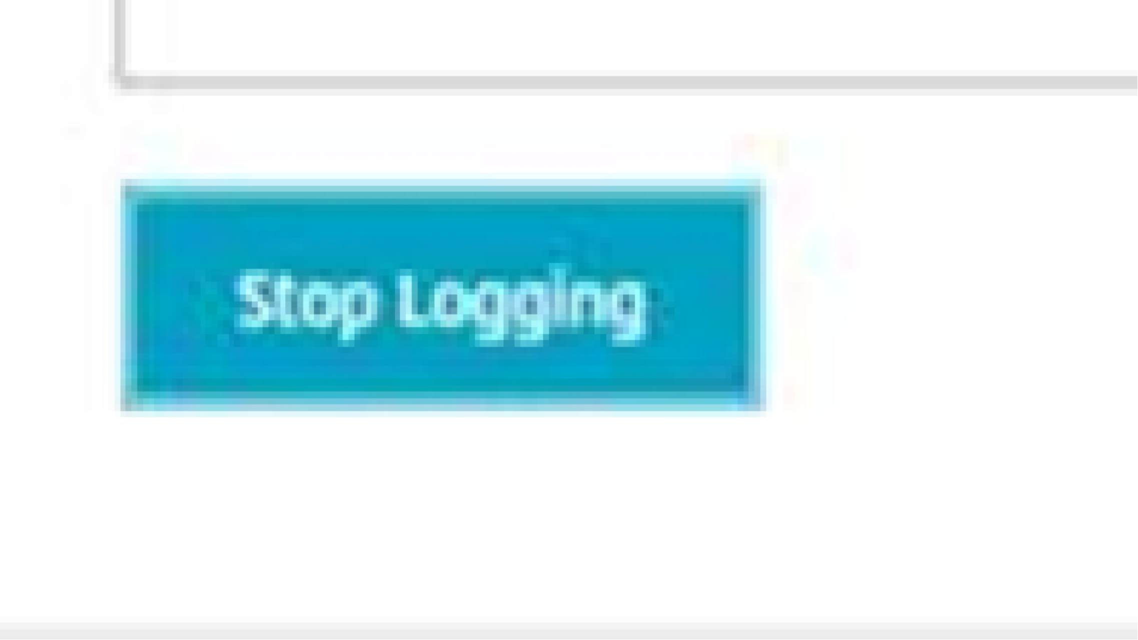
Store Address

https://myworkprod0.cloud.com

Log Files

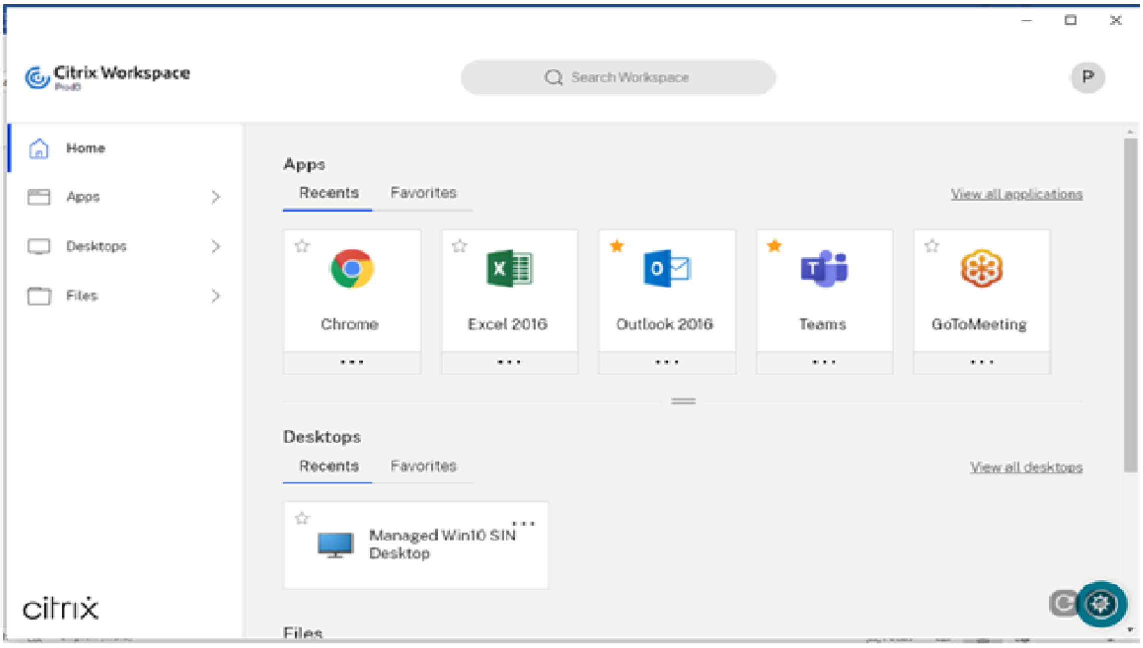
Version 21.6.1.2

3. The **Start Logging** button changes to **Stop Logging**. This change indicates that collection of logs is enabled.



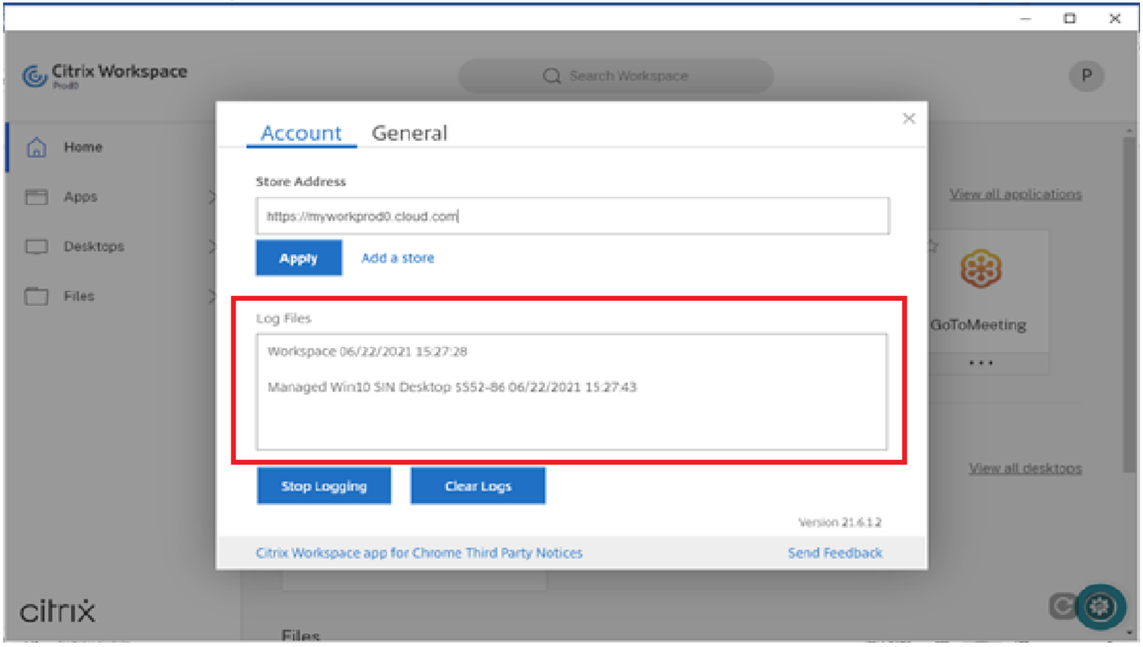
Close the **Account** dialog box.

4. Log into the Citrix Workspace app virtual desktop and launch your virtual app session and reproduce the issue to collect logs.



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. The **Account** dialog box shows the list of **Log Files** captured.



Store Address

https://myworkprod0.cloud.com

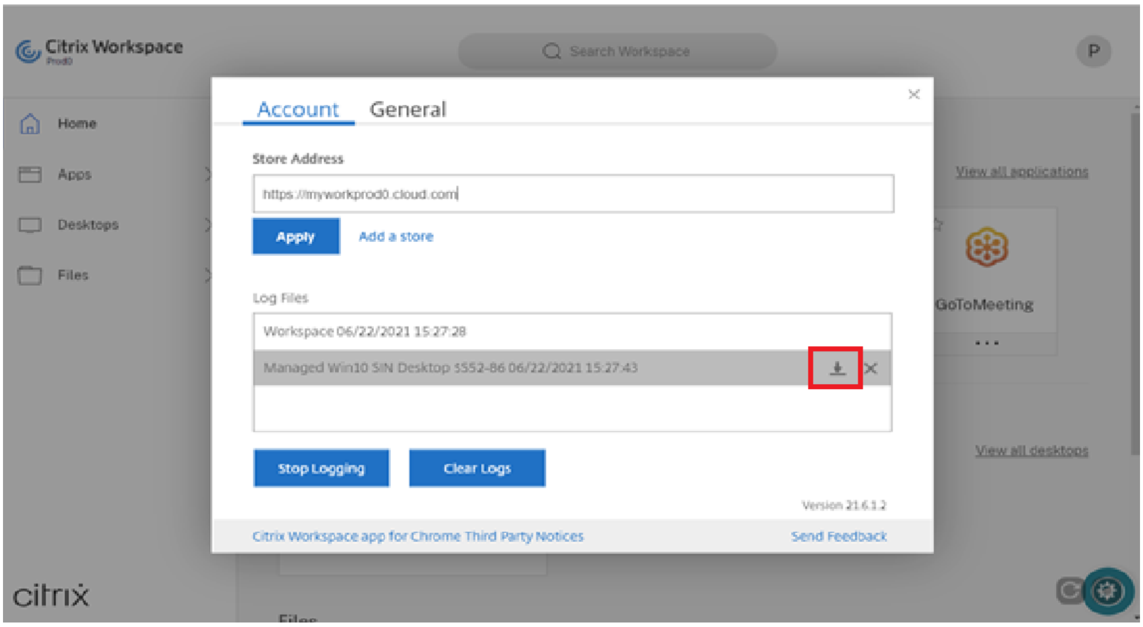
Log Files

Workspace 06/22/2021 15:27:28

Managed Win10 SIN Desktop 5552-86 06/22/2021 15:27:43

Version 21.6.1.2

8. Moving the mouse on top of any of the Log files shows a small arrow at the right.



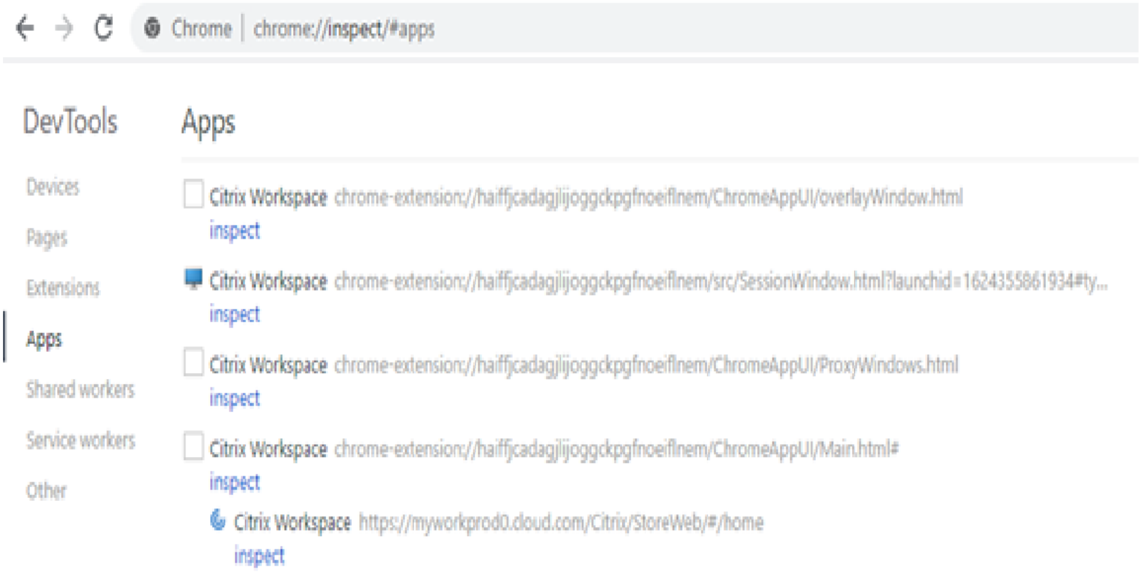
9. Click the arrow button to download and save the Log file.
10. Save all the log files listed under **Log files** and share it with the administrator or Citrix support engineer.
11. Click **Stop Logging**.

> **Note:**
>
> In the case of 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 **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).



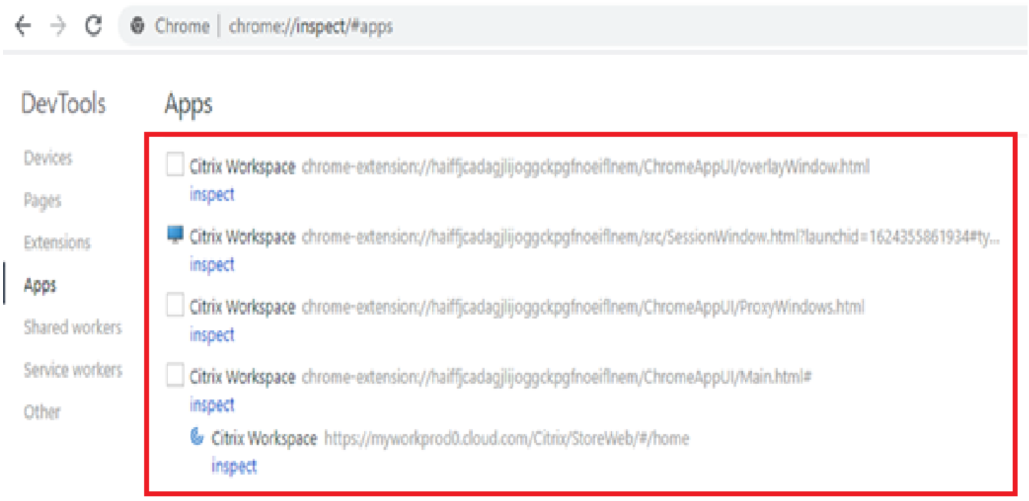
Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/overlayWindow.html
inspect

Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/src/SessionWindow.html?launchid=1624355861934#ty...
inspect

Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/ProxyWindows.html
inspect

Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/Main.html#
inspect

Citrix Workspace https://myworkprod0.cloud.com/Citrix/StoreWeb/#/home
inspect



Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/overlayWindow.html
inspect

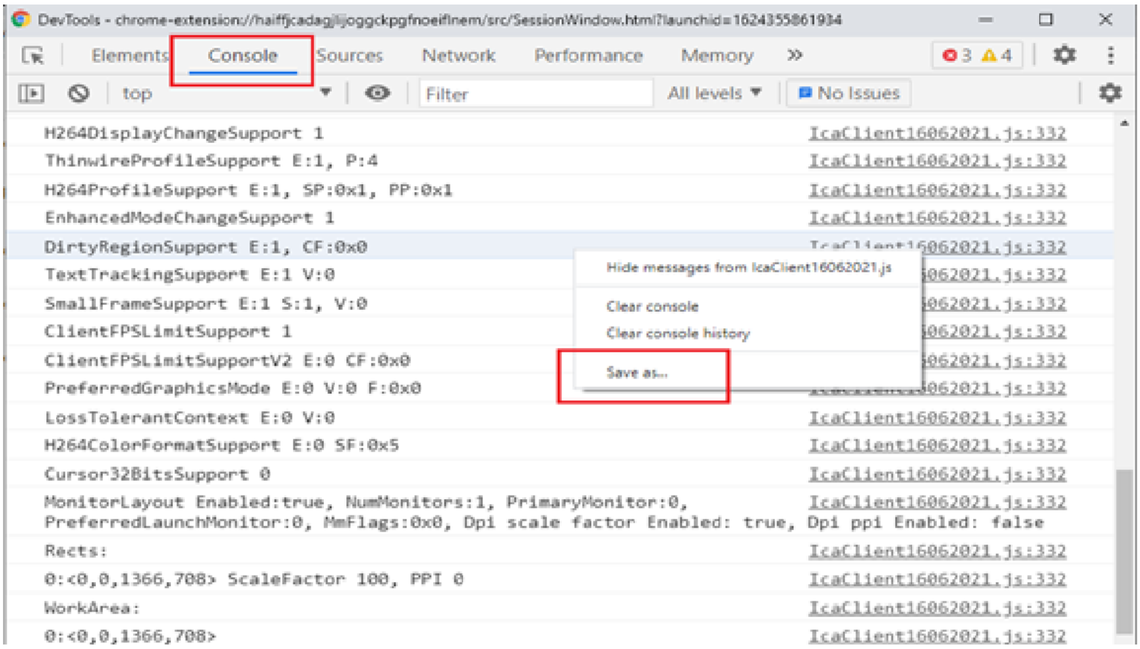
Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/src/SessionWindow.html?launchid=1624355861934#ty...
inspect

Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/ProxyWindows.html
inspect

Citrix Workspace chrome-extension://haiffjcadagjiijoggckpgfnoeiflnem/ChromeAppUI/Main.html#
inspect

Citrix Workspace https://myworkprod0.cloud.com/Citrix/StoreWeb/#/home
inspect

3. For each opened developer tool window, click **Console**. Then, save the entire log by right-clicking and selecting the **Save as** option.


DevTools - chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem/src/SessionWindow.html?launchid=1624355861934
Elements
Console
Sources
Network
Performance
Memory
3
4
top
Filter
All levels
No Issues
Hide messages from IcaClient16062021.js
Clear console
Clear console history
Save as...

```
H264DisplayChangeSupport 1                                   IcaClient16062021.js:332
ThinwireProfileSupport E:1, P:4                              IcaClient16062021.js:332
H264ProfileSupport E:1, SP:0x1, PP:0x1                       IcaClient16062021.js:332
EnhancedModeChangeSupport 1                                  IcaClient16062021.js:332
DirtyRegionSupport E:1, CF:0x0                               IcaClient16062021.js:332
TextTrackingSupport E:1 V:0                                          062021.js:332
SmallFrameSupport E:1 S:1, V:0                                       062021.js:332
ClientFPSLimitSupport 1                                              062021.js:332
ClientFPSLimitSupportV2 E:0 CF:0x0                                   062021.js:332
PreferredGraphicsMode E:0 V:0 F:0x0                                  062021.js:332
LossTolerantContext E:0 V:0                                  IcaClient16062021.js:332
H264ColorFormatSupport E:0 SF:0x5                            IcaClient16062021.js:332
Cursor32BitsSupport 0                                        IcaClient16062021.js:332
MonitorLayout Enabled:true, NumMonitors:1, PrimaryMonitor:0, IcaClient16062021.js:332
PreferredLaunchMonitor:0, MmFlags:0x0, Dpi scale factor Enabled: true, Dpi ppi Enabled: false
Rects:                                                       IcaClient16062021.js:332
0:<0,0,1366,708> ScaleFactor 100, PPI 0                      IcaClient16062021.js:332
WorkArea:                                                    IcaClient16062021.js:332
0:<0,0,1366,708>                                             IcaClient16062021.js:332
```

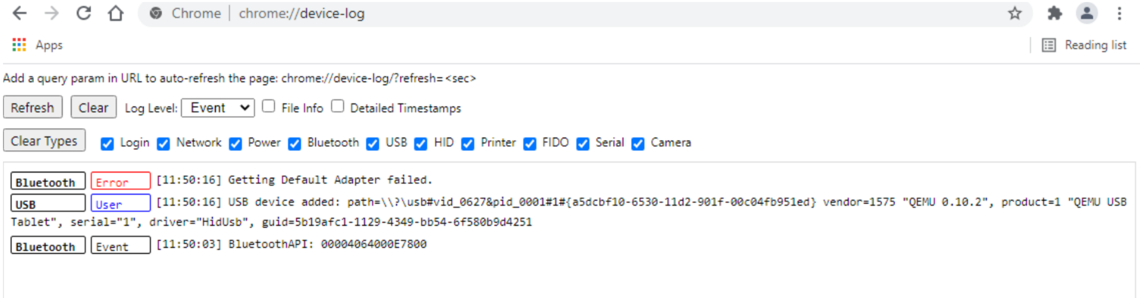
USB redirection logs

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.



Add a query param in URL to auto-refresh the page: chrome://device-log/?refresh=<sec>

Refresh | Clear | Log Level: Event | □ File Info | □ Detailed Timestamps

Clear Types | ☑ Login ☑ Network ☑ Power ☑ Bluetooth ☑ USB ☑ HID ☑ Printer ☑ FIDO ☑ Serial ☑ Camera

```
Bluetooth  Error  [11:50:16] Getting Default Adapter failed.
USB  User  [11:50:16] USB device added: path=\\?\usb#vid_0627&pid_0001#1#{a5dcbf10-6530-11d2-901f-00c04fb951ed} vendor=1575 "QEMU 0.10.2", product=1 "QEMU USB Tablet", serial="1", driver="HidUsb", guid=5b19afc1-1129-4349-bb54-6f580b9d4251
Bluetooth  Event  [11:50:03] BluetoothAPI: 00004064000E7800
```

File transfer logs

The file transfer logs can be retrieved from both the client and the server.

To retriever file transfer logs from the client:

1. Launch a browser.
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 **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 is not 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.

Configuration utility tool

January 11, 2023

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 webpage.

To download the Configuration utility tool, see Knowledge center article CTX229141.

How to use the configuration utility tool

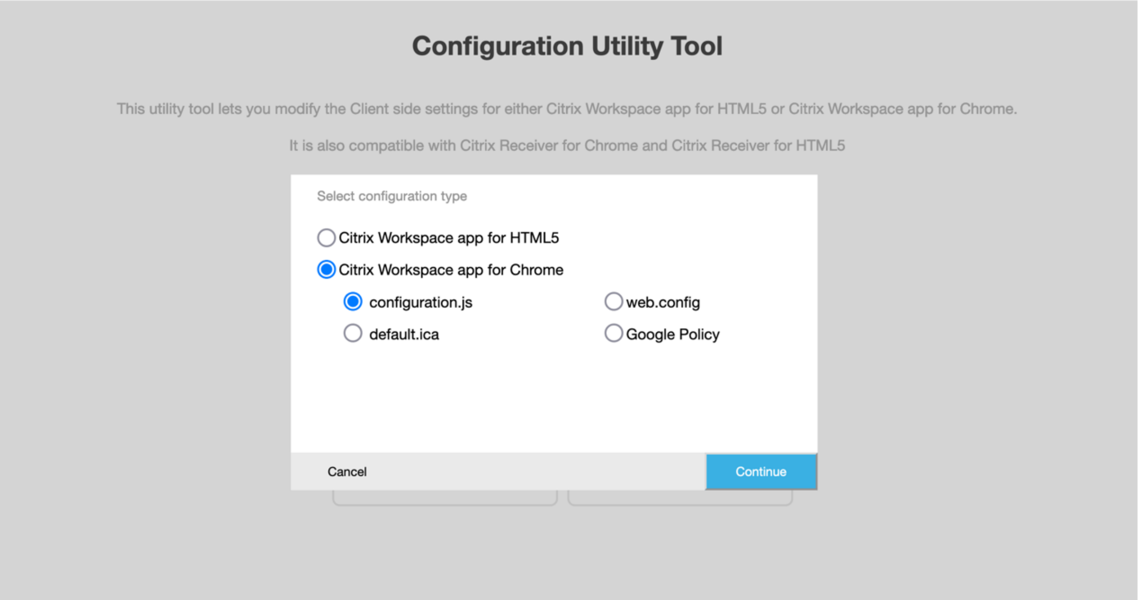
1. Click **Creat New.**

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.



Configuration Utility Tool

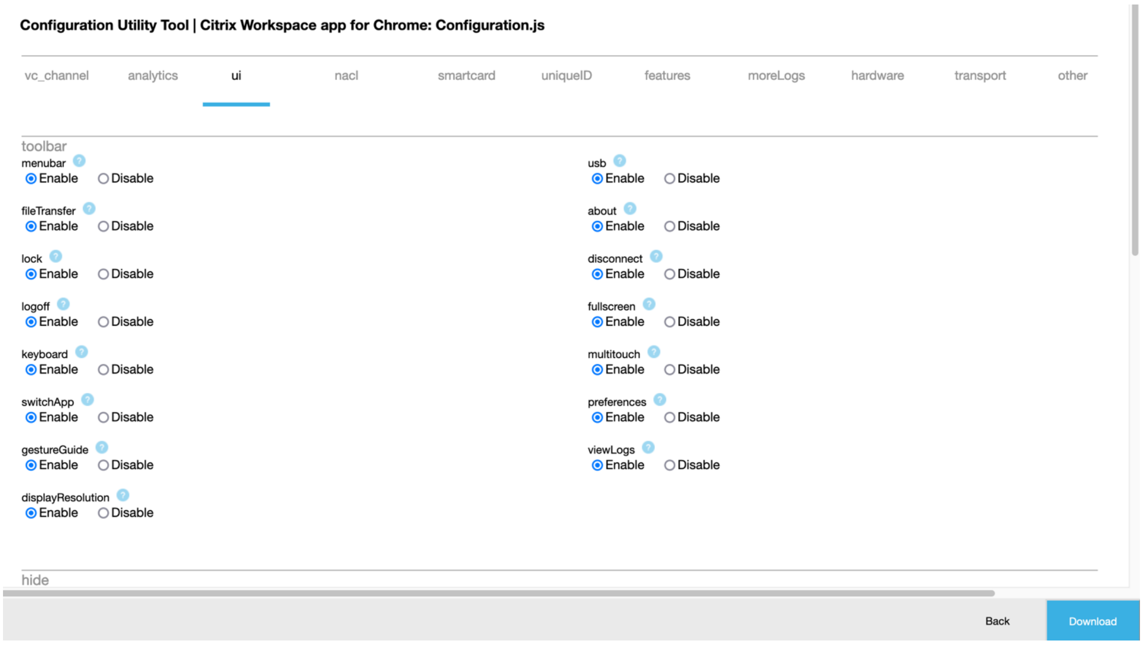
This utility tool lets you modify the Client side settings for either Citrix Workspace app for HTML5 or Citrix Workspace app for Chrome.

It is also compatible with Citrix Receiver for Chrome and Citrix Receiver for HTML5

Select configuration type

○ Citrix Workspace app for HTML5
● Citrix Workspace app for Chrome
● configuration.js ○ web.config
○ default.ica ○ Google Policy

2. On the **Configuration Utility Tool**, select the feature you want and choose their appropriate values.



Configuration Utility Tool | Citrix Workspace app for Chrome: Configuration.js

toolbar

menubar
● Enable ○ Disable

fileTransfer
● Enable ○ Disable

lock
● Enable ○ Disable

logoff
● Enable ○ Disable

keyboard
● Enable ○ Disable

switchApp
● Enable ○ Disable

gestureGuide
● Enable ○ Disable

displayResolution
● Enable ○ Disable

usb
● Enable ○ Disable

about
● Enable ○ Disable

disconnect
● Enable ○ Disable

fullscreen
● Enable ○ Disable

multitouch
● Enable ○ Disable

preferences
● Enable ○ Disable

viewLogs
● Enable ○ Disable

hide

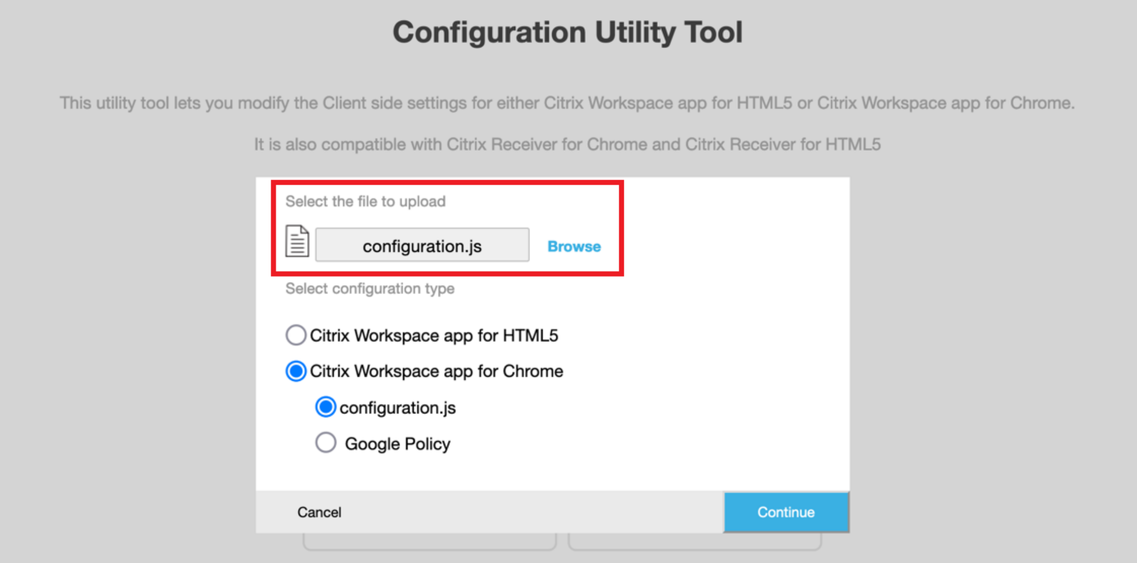
3. Click **Download** to download the configuration.js file.

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.



Configuration Utility Tool

This utility tool lets you modify the Client side settings for either Citrix Workspace app for HTML5 or Citrix Workspace app for Chrome.

It is also compatible with Citrix Receiver for Chrome and Citrix Receiver for HTML5

Select the file to upload

configuration.js

Select configuration type

○ Citrix Workspace app for HTML5

● Citrix Workspace app for Chrome

● configuration.js

○ Google Policy

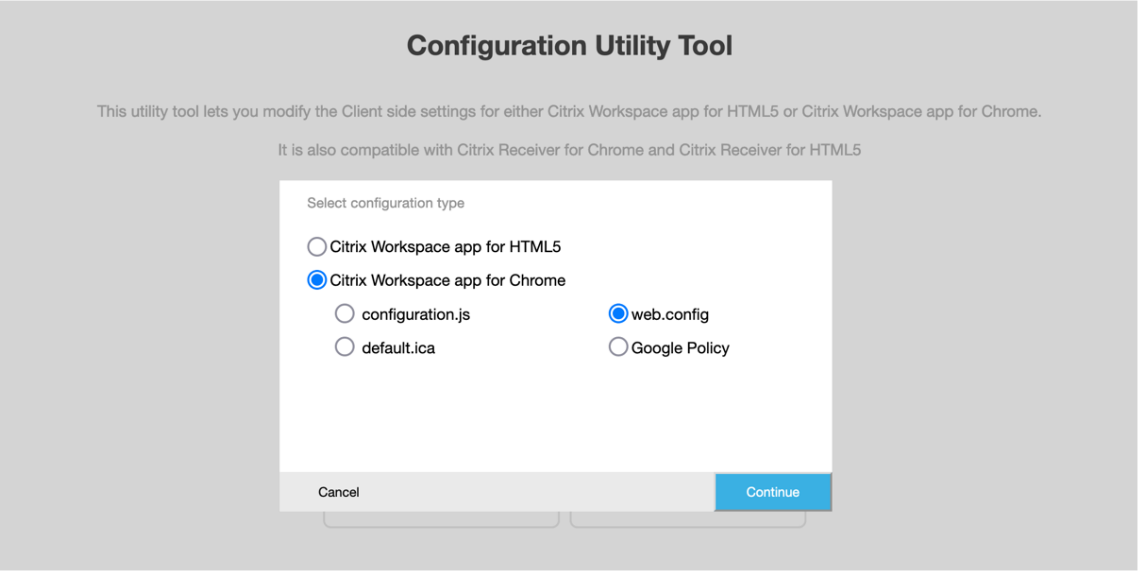
4. Click **Continue** to configure or **Cancel** to go back to the home page.

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.



Configuration Utility Tool

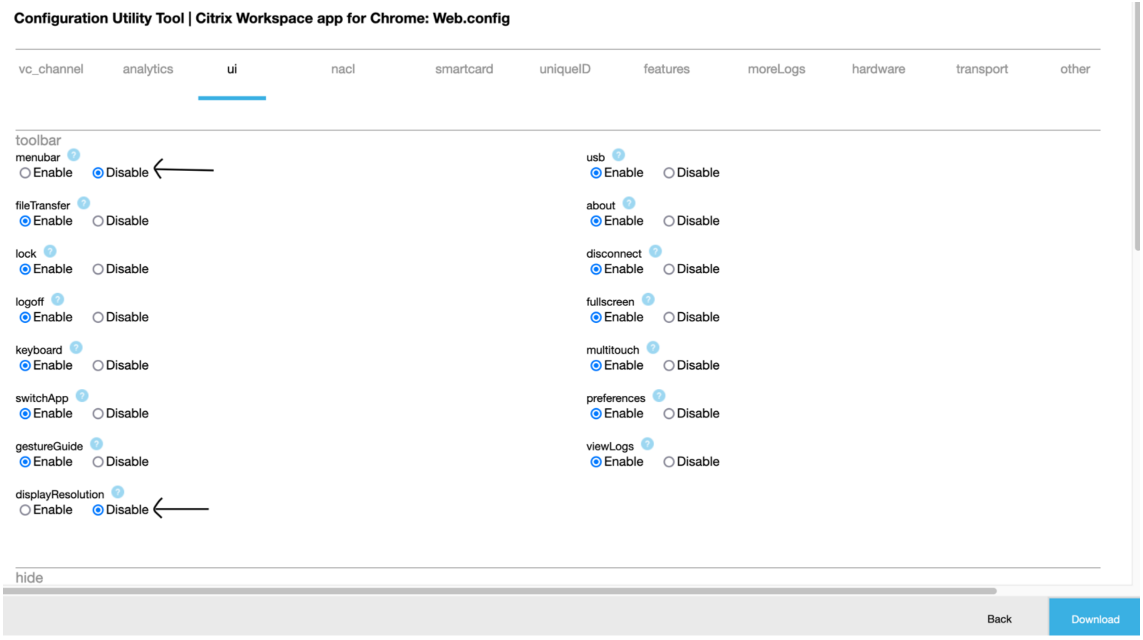
This utility tool lets you modify the Client side settings for either Citrix Workspace app for HTML5 or Citrix Workspace app for Chrome.

It is also compatible with Citrix Receiver for Chrome and Citrix Receiver for HTML5

Select configuration type

○ Citrix Workspace app for HTML5
● Citrix Workspace app for Chrome
○ configuration.js ● web.config
○ default.ica ○ Google Policy

2. Select the settings that you want and their appropriate values and click **Download** (for example, select menubar: disable; displayResolution : disable)



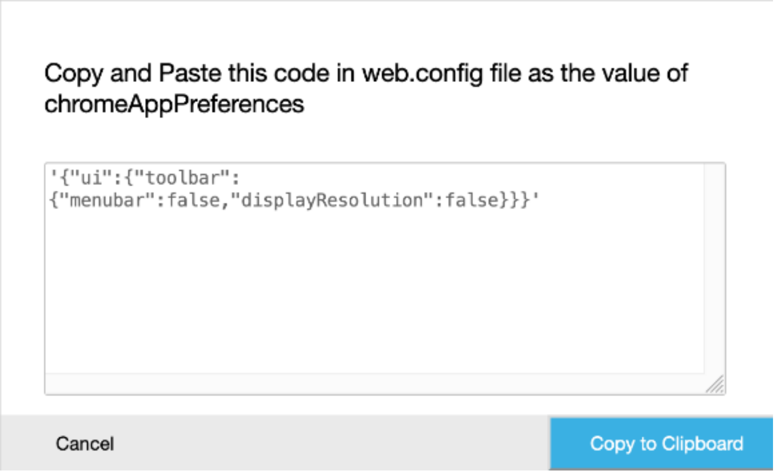
Configuration Utility Tool | Citrix Workspace app for Chrome: Web.config

toolbar

menubar: ○ Enable ● Disable
fileTransfer: ● Enable ○ Disable
lock: ● Enable ○ Disable
logoff: ● Enable ○ Disable
keyboard: ● Enable ○ Disable
switchApp: ● Enable ○ Disable
gestureGuide: ● Enable ○ Disable
displayResolution: ○ Enable ● Disable
usb: ● Enable ○ Disable
about: ● Enable ○ Disable
disconnect: ● Enable ○ Disable
fullscreen: ● Enable ○ Disable
multitouch: ● Enable ○ Disable
preferences: ● Enable ○ Disable
viewLogs: ● Enable ○ Disable

hide

3. Copy the contents in the dialog box.



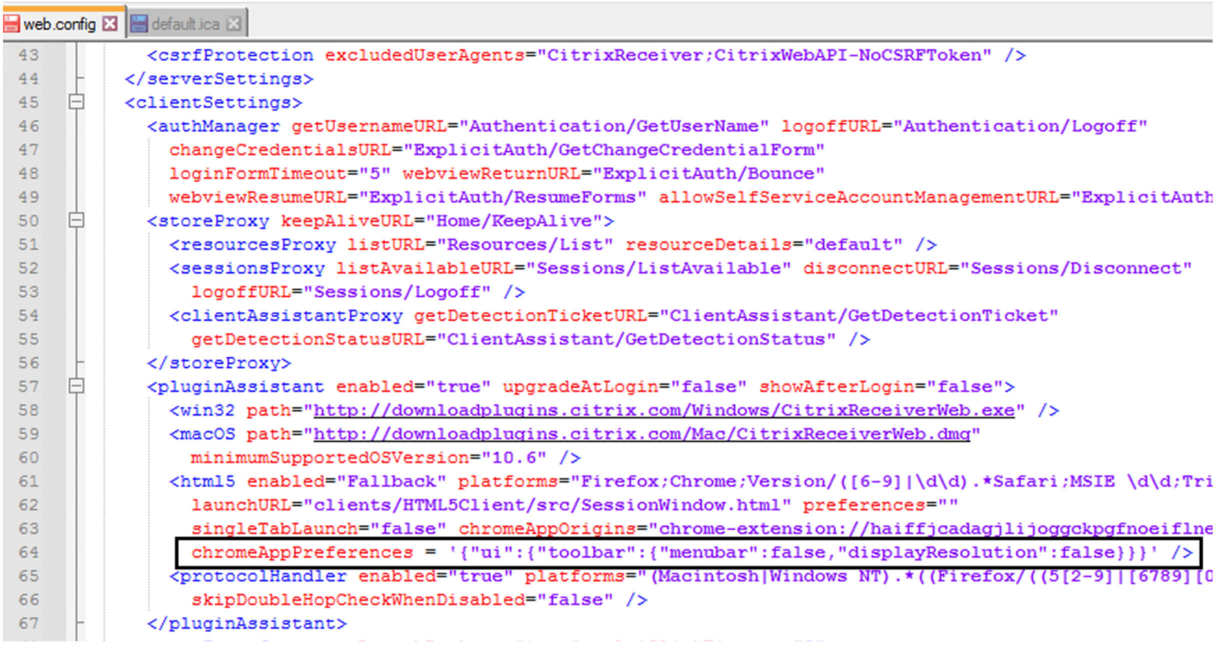
Copy and Paste this code in web.config file as the value of chromeAppPreferences

```
'{"ui":{"toolbar":
{"menubar":false,"displayResolution":false}}}'
```

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.

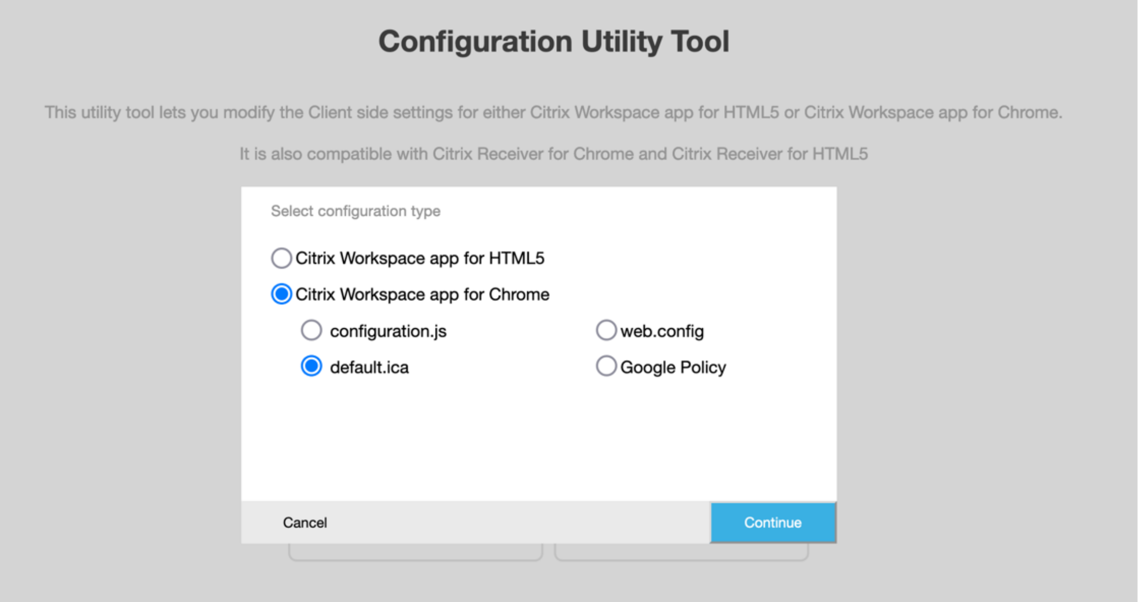
   chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'



```
      <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.



Configuration Utility Tool

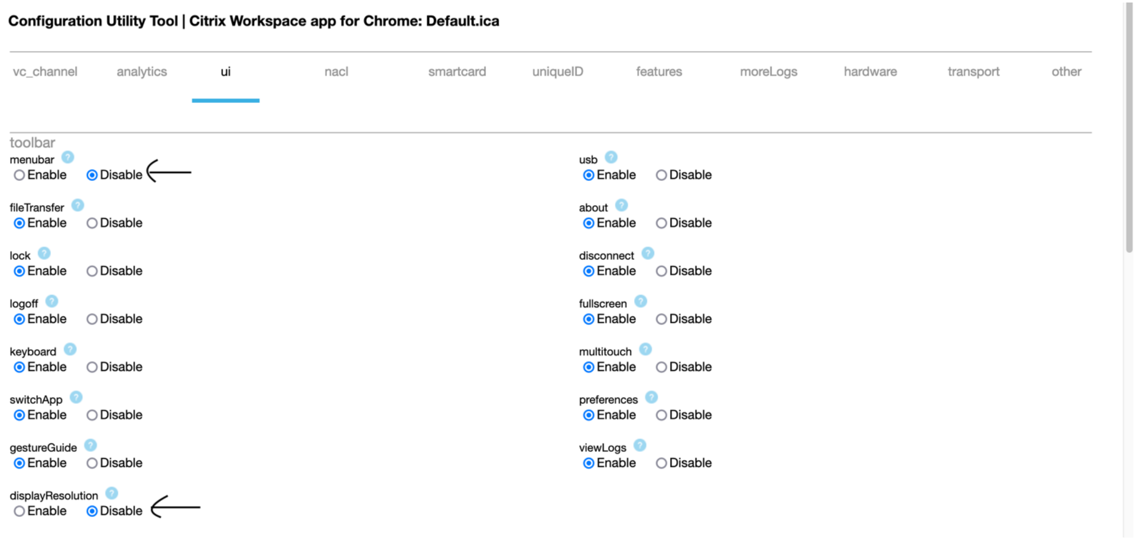
This utility tool lets you modify the Client side settings for either Citrix Workspace app for HTML5 or Citrix Workspace app for Chrome.

It is also compatible with Citrix Receiver for Chrome and Citrix Receiver for HTML5

Select configuration type

○ Citrix Workspace app for HTML5
● Citrix Workspace app for Chrome
○ configuration.js ○ web.config
● default.ica ○ Google Policy

2. Select the settings that you want and their appropriate values and click **Download** (for example, select menubar: disable, displayResolution: disable).

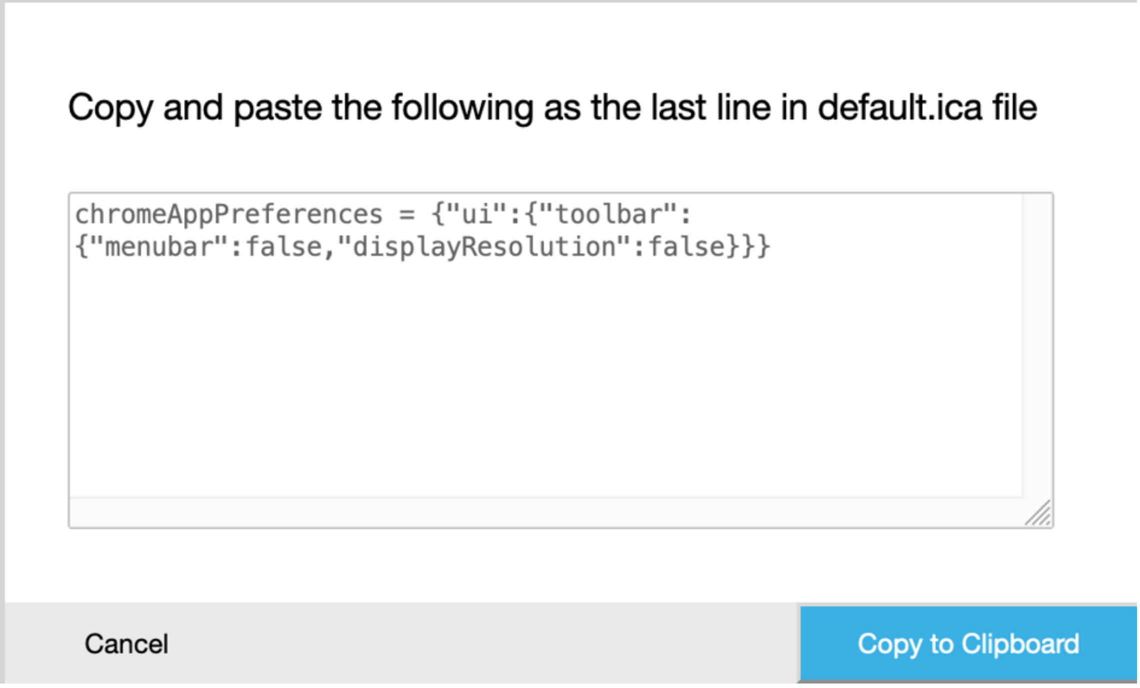


Configuration Utility Tool | Citrix Workspace app for Chrome: Default.ica

toolbar

menubar: ○ Enable ● Disable
fileTransfer: ● Enable ○ Disable
lock: ● Enable ○ Disable
logoff: ● Enable ○ Disable
keyboard: ● Enable ○ Disable
switchApp: ● Enable ○ Disable
gestureGuide: ● Enable ○ Disable
displayResolution: ○ Enable ● Disable
usb: ● Enable ○ Disable
about: ● Enable ○ Disable
disconnect: ● Enable ○ Disable
fullscreen: ● Enable ○ Disable
multitouch: ● Enable ○ Disable
preferences: ● Enable ○ Disable
viewLogs: ● Enable ○ Disable

3. Copy the contents in the dialog box.

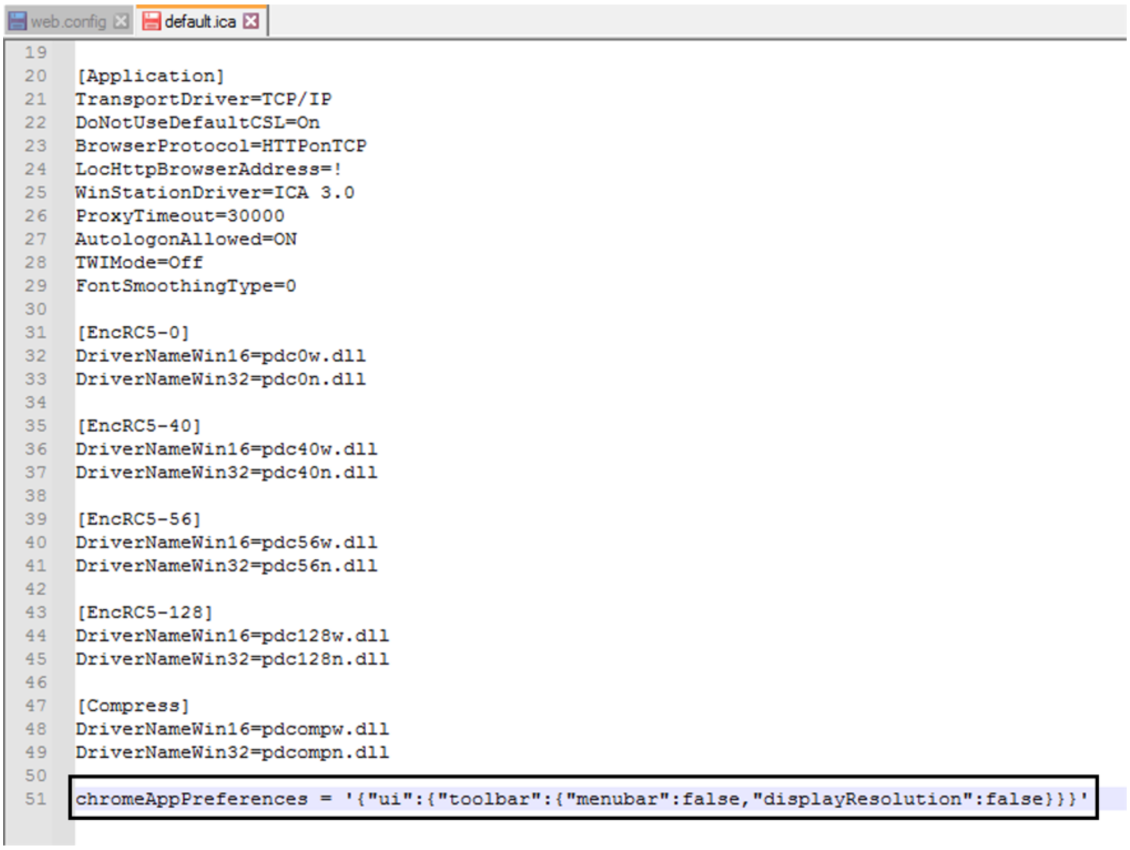


Copy and paste the following as the last line in default.ica file

```
chromeAppPreferences = {"ui":{"toolbar":
{"menubar":false,"displayResolution":false}}}
```

4. Open the default.ica file typically at **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 typically at **C:\inetpub\wwwroot\Citrix\<Storename>** 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.



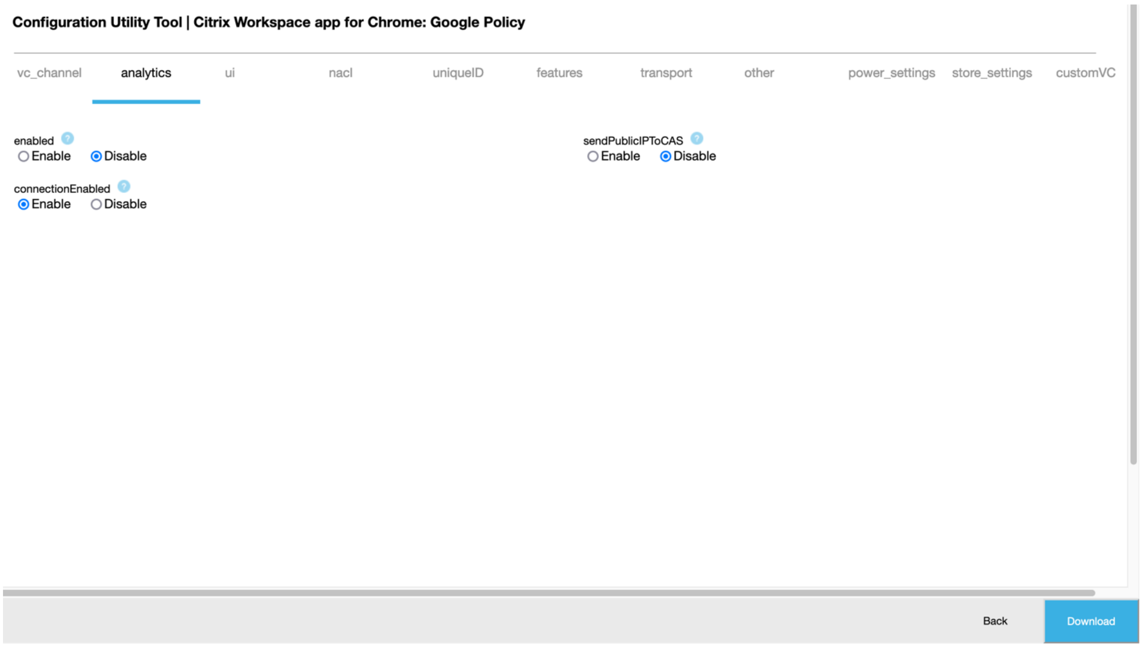
```
[Application]
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
TWIMode=Off
FontSmoothingType=0

[EncRC5-0]
DriverNameWin16=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll

[Compress]
DriverNameWin16=pdcompw.dll
DriverNameWin32=pdcompn.dll

chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'
```

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)

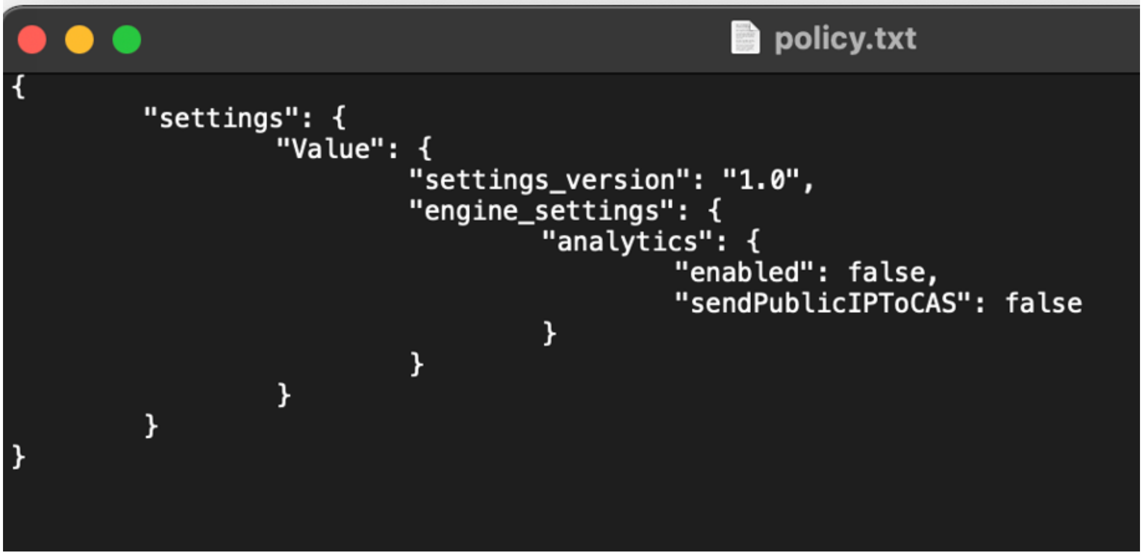


enabled
○ Enable ● Disable

connectionEnabled
● Enable ○ Disable

sendPublicIPToCAS
○ Enable ● Disable

3. When you click **Download**, a policy.txt file is created.



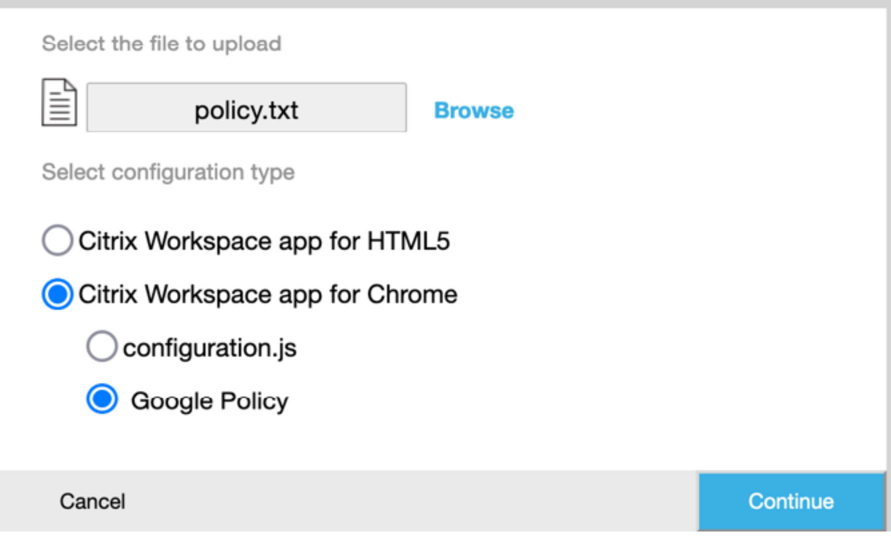
```
{
        "settings": {
                "Value": {
                        "settings_version": "1.0",
                        "engine_settings": {
                                "analytics": {
                                        "enabled": false,
                                        "sendPublicIPToCAS": false
                                }
                        }
                }
        }
}
```

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.



Select the file to upload

policy.txt Browse

Select configuration type

○ Citrix Workspace app for HTML5

● Citrix Workspace app for Chrome

○ configuration.js

● Google Policy

Cancel Continue

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 home page.
5. Edit the settings by choosing their appropriate values.
6. Click **Download** to download the updated policy.txt file.

Authenticate

January 11, 2023

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)

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 exposes 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 custom script to allow smart card authentication on ChromeOS. Contact Citrix support for custom script.
- Citrix Workspace app doesn't control 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 the load Store URL again, click the reload button in Citrix Workspace app for ChromeOS.

  At times, to clear cookies furthermore, you can sign out from the ChromeOS device.
- When you attempt 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.

SAML authentication

To configure 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 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 allow 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.

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.

```
{

    "whitelist" : {

        "Value" : [
            {

            "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain" : "saml.yourcompany.com"
             }

        ]
      }
```

```

 }

<!--NeedCopy-->
```

7. Configure Citrix Workspace to use 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.

SDK and API

January 11, 2023

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 Chrome.

For HDX SDK examples, refer to the Citrix download page.

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 Chrome.

For VC SDK examples, refer to VC SDK examples.

Procedure to consume the API in the third-party Chrome app

1. Install the latest version of Citrix Workspace app for ChromeOS. See Citrix downloads page for details.
2. Whitelist the third-party Chrome app 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.
   The Sample policy.txt file to whitelist the third-party Chrome app is as below:

```
{

      "settings": {

             "Value": {

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

             "externalApps": [ “<3rdParty_App1_ExtnID>” , “<3rdParty_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');
 }
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) {

if (launchStatus.success) {

// handle success.
console.log("Session launch was attempted successfully");
 }
 else {

// handle errors.
console.log("error during session launch: ", launchStatus.message
        );
    }

    }
  );

  <!--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

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