Citrix Workspace™ app for HTML5

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

Contents

Citrix Workspace™ app for HTML5 3

About this release 4

Features in Technical Preview 33

Citrix Workspace app for HTML5 - Preview 37

Prerequisites for installing 41

Install 45

Get Started 56

Configure 57

Customer Experience Improvement Program (CEIP) 69

Peripherals 74

File handling 79

Keyboard 83

Session experience 92

Multi-monitor 128

Multimedia 135

HDX™ transport 148

Touch and mobility support 149

Printing 153

deviceTRUST 156

Troubleshoot 159

Secure 168

Authenticate 170

SDK 171

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

Deprecation **175**

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

Citrix Workspace™ app for HTML5

September 7, 2025

Citrix Workspace app for HTML5 is hosted on servers for on-premises deployments, and Content Delivery Network (CDN) for cloud deployment. Citrix Workspace app enables users to access virtual desktops and hosted apps from a web browser.

Resources delivered by Citrix Virtual Apps and Desktops are aggregated in a store. It's then made available through a Citrix Receiver for Web site. With Citrix Workspace app for HTML5 enabled on the site, users can access desktops and apps within their web browsers.

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

Citrix® recommends the following:

- For a secure connection, open Citrix Workspace app sessions from HTTPS-based stores. Some features might not function when using HTTP-based stores.

There's no need for the users to install Citrix Workspace app locally on their devices, as it's a zero install client.

You receive centrally managed app and desktop selection experience from when you use Citrix Workspace app with the centralized customization and branding capabilities of 3.0.

For information about the features available in Citrix Workspace app for HTML5, see Citrix Workspace app feature matrix.

For information about deprecated items, see the Deprecation page.

Language support

Citrix Workspace app for HTML5 is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for HTML5, see Language support.

Reference articles

- Global App Configuration service
- Optimization for Microsoft Teams
- Microsoft Teams optimization in Citrix Virtual Apps and Desktops environments
- Tech Brief: Workspace Single Sign-On
- Tech Paper: Citrix Workspace app quick start guide

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

- Tech Brief: Citrix Workspace
- Developer documentation - Citrix Workspace app for HTML5 HDX SDK
- Developer documentation - Citrix Virtual Channel SDK for Citrix Workspace app for HTML5
- Citrix Workspace app release timelines

What's new in related products

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

Legacy documentation

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

About this release

October 13, 2026

Learn about new features, enhancements, fixed issues, and known issues for Citrix Workspace app for HTML5.

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

What's new in 2607

Following are the new features and enhancements:

- Integration of deviceTRUST with Citrix Workspace app for HTML5
- Synchronization for Lock Key States
- Auto Client Reconnect
- Give or Take Control in Microsoft Teams Optimization
- Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

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

Integration of deviceTRUST with Citrix Workspace app for HTML5

Starting with version 2607, Citrix Workspace app for HTML5 supports deviceTRUST integration, enhancing security through continuous device posture checks within sessions. This integration ensures only compliant devices that can access Citrix Virtual Apps and Desktops through browser.

About the feature deviceTRUST provides continuous device posture monitoring and assessment capabilities for html5 devices accessing Citrix environments. The integration uses web-based APIs to collect device information and enforce security policies based on device compliance status.

> **Note:**
>
> For more information about deviceTRUST, see deviceTRUST Platform.

Benefits This integration provides:

- **Continuous security monitoring** - Real-time device posture assessment during active sessions
- **Policy enforcement** - Automated responses based on device compliance status
- **Enhanced visibility** - Comprehensive device information for security administrators
- **Seamless user experience** - Transparent security checks without user intervention

For more information on how to configure, see deviceTRUST

Synchronization for Lock Key States

Starting with version 2607, Citrix Workspace app for HTML5 introduces enhanced synchronization for lock key states (Caps Lock, Num Lock, and Scroll Lock) with the client state. This feature ensures consistent behavior of Caps Lock, Num Lock, and Scroll Lock within your session and it continues even when you switch to your local tasks. It remains consistent when you return to the session.

Auto Client Reconnect

Starting with version 2607, Auto Client Reconnect (ACR) feature ensures session continuity by automatically re-establishing connections when Session Reliability cannot recover an interrupted session. If the Session Reliability timeout expires before network connectivity is restored, the Citrix Workspace app attempts to reconnect to the same session. This reconnection uses a server-issued reconnect cookie, allowing you to resume your session from where you left off without needing to reauthenticate. For more information, see Auto Client Reconnect.

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

Give or Take Control in Microsoft Teams Optimization

Starting with version 2607, you can manage screen sharing control during meetings. This feature allows participants to interact with a shared screen using keyboard, mouse, and clipboard input. For more information, see Give or Take Control in Microsoft Teams Optimization

Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

Starting with version 2607, Citrix Workspace app for HTML5 introduces an enhanced Connection Strength Indicator, designed to provide a more intuitive and user-friendly experience.

The key improvements include:

- **Expanded device details:** Access comprehensive information, such as client device's CPU status.
- **Proactive notifications:** Receive alerts in the toolbar notch when your connection strength drops.
- **Actionable recommendations:** Get clear suggestions to resolve connectivity issues when your connection strength falls below optimal levels.
- **15-minute connection history:** Review a visual history of your connection strength over the past 15 minutes to assist with troubleshooting and analysis.

For more infromation, see Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

Fixed issues in 2607

- When the Microsoft Teams optimized secondary ringtone is enabled, the ringtone does not play in the Citrix Workspace app for HTML5 client. Citrix Workspace app for HTML5 SDK must be updated to utilize the new Microsoft assets URL. To enable media loading from the Microsoft Content Delivery Network (CDN), add https://*.onecdn.static.microsoft to the `media-src` directive within the Content Security Policy (CSP) meta tag in `HDXEngine.html`. [RFHTMCRM-18368]
- When you use Client Drive Mapping (CDM) to save a Microsoft Excel file to a mapped local folder using the **Save** or **Save As** option, the save operation might fail and the file might not be created. [CVADHELP-34582]
- When you copy an entire table or a worksheet from Microsoft Excel within a Citrix Workspace app for HTML5 session, the copy operation might fail and a clipboard error message might appear. [CVADHELP-33926]

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

Known issues in 2607

- When switching between fullscreen and restored view modes within a Citrix Workspace app for HTML5 session on macOS browsers, the fullscreen/restore toolbar button might not update correctly if you use keyboard shortcuts, such as F11.

  As a workaround, use the **Fullscreen** or **Restore** options directly from the in-session toolbar instead of keyboard shortcuts. [RFHTMCRM-17586]

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

Earlier releases

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

2603.10

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues

- When you start a resource from DaaS using Citrix Workspace app for HTML5, the session might fail on the first attempt if the target VDA is powered off and takes more than three minutes to start and register, though the subsequent attempt succeeds. [CCVADHELP-5191]
- When you try to create a file using the Windows **Save** dialog on a drive that Client Drive Mapping (CDM) maps in Citrix Workspace app for HTML5 session, the file creation might fail. [CVADHELP-32584]
- During a desktop session, the mouse cursor might intermittently stop responding, failing to update its shape (for example, the mouse cursor remains an arrow instead of changing to a text cursor). [CVADHELP-33365]
- The **Auto-fit Screen** (**Fit_To_Window**) setting, configured through Global App Configuration Service (GACS), might not persist when a session reconnects. This causes sessions to reset to default Device Pixel Ratio (DPR) mode. [CVADHELP-33365]

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

- When you use Client Drive Mapping (CDM) to map files or folders within Citrix Workspace app for HTML5, some files might be missing in the mapped network drive. [CVADHELP-33220]
- You can't paste the content between your local endpoint and Citrix Workspace app for HTML5 session through Clipboard Toolbar, unless you manually click the clipboard dialog. [CVADHELP-33180]

2603

What's new

Following are the new features and enhancements:

- Keyboard input mode refinement
- Audio quality improvement with reliable transport protocols
- AOT log content enhancement
- Support for single-tenant Microsoft Entra ID

Keyboard input mode refinement Starting with version 2603, Citrix Workspace app for HTML5 introduces a refined user interface for selecting keyboard input modes, replacing the deprecated scancode configuration option. This enhancement allows users to modify keyboard settings during an active session with immediate effect.

About this feature This feature provides improved keyboard input management with the following key capabilities:

- **Real-time configuration changes**: Users can modify keyboard input settings during an active session without requiring a session restart.
- **Enhanced user interface**: A new streamlined interface allows users to select keyboard input modes directly from the session preferences dialog.
- **Three input modes**: The feature supports **Automatic**, **Unicode**, and **Scancode** input modes to accommodate different use cases and scenarios.
- **Intelligent automatic mode**: When **Automatic** mode is selected, the system intelligently determines the optimal input method:
  - Citrix Workspace app for HTML5 session running on Mac client connecting to Mac VDA: Scancode mode
  - All other scenarios: Unicode mode

For more information about keyboard configuration, see Keyboard input mode refinement.

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

Audio quality improvement with reliable transport protocols Starting with version 2603, Citrix Workspace app for HTML5 delivers enhanced audio redirection that creates a smoother and more consistent audio playback and recording experience. The application improves audio quality, particularly when you use reliable transport protocols such as TCP and EDT Reliable.

About this feature This feature delivers significant improvements to audio performance with the following key benefits:

- **Improved audio quality**: The application processes audio more effectively and delivers clearer sound with less distortion during playback and recording sessions.
- **Consistent audio experience**: Reliable transport protocols maintain stable audio streaming with fewer interruptions or dropouts.
- **Optimized for reliable transports**: The enhancement performs better when you use TCP and EDT Reliable transport protocols, delivering more predictable audio.
- **Seamless user experience**: Users experience smoother audio transitions and better overall session quality without configuring additional settings.

Prerequisites To use this feature, ensure that you enable the **Adaptive Audio** feature.

For more information about audio configuration, see Adaptive audio.

AOT log content enhancement Starting with version 2603, Citrix Workspace app for HTML5 expands AOT (Always On Tracing) log functionality to support log uploads to centralized servers for on-premises setups that include a gateway in the path. This enhancement extends diagnostic capabilities and provides administrators with greater flexibility in troubleshooting environments.

About this feature This feature delivers enhanced diagnostic capabilities with the following key improvements:

- **Expanded gateway support**: AOT logs now upload successfully to centralized log servers in on-premises environments that include a gateway in the connection path.
- **Improved troubleshooting coverage**: Administrators can capture and analyze diagnostic data across more diverse network configurations and deployment scenarios.
- **Flexible configuration control**: You can now disable the AOT feature entirely when diagnostic logging is not required for your environment.
- **Enhanced compatibility**: The feature works seamlessly with existing on-premises setups while extending to previously unsupported gateway configurations.

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

> **Note:**
>
> In Citrix Workspace app for HTML5 2603, AOT log uploads to centralized log servers support both on-premises setups without a gateway and on-premises setups with a gateway in the path.

For more information about AOT configuration and troubleshooting, see Upload AOT logs to centralized AOT log server.

Support for single-tenant Microsoft Entra ID This feature lets you use single sign-on (SSO) with Microsoft Entra ID credentials to access virtual apps and desktops on Microsoft Entra hybrid-joined session hosts. To configure VDA SSO, use your customer-specific single-tenant Entra ID client app. For more information, see Microsoft Entra single sign-on.

Fixed issues

- When upgrading from Citrix Workspace app for HTML5 2509 to a newer version, some features such as audio and PDF printing might not function properly on the first launch after the upgrade. [RFHTMCRM-16799]
- In high-latency network environments, after the version upgrade, the first session launch might take 30-40 seconds to render. The app now loads scripts to improve startup performance. [CVADHELP-30593]
- When users launch a published app with Citrix Workspace app for HTML5 for the first time, the bottom of the app session window is truncated. This makes the status bar invisible and offsets the mouse position.[CVADHELP-32506]

2511

What's new

Following are the new features and enhancements:

- Default audio device selection
- Support for Microsoft Entra ID single sign-on
- Always on tracing (AOT)

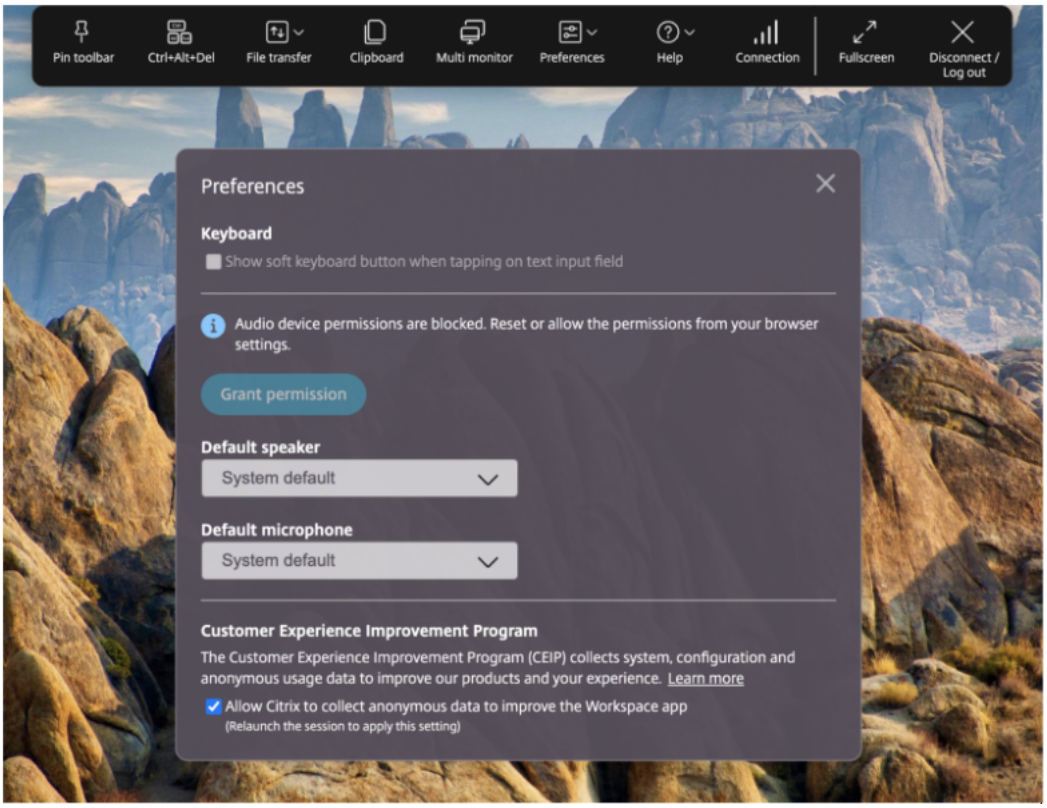
Default audio device selection Starting with version 2511, Citrix Workspace app for HTML5 lets users select and save their preferred audio speaker and microphone devices from the session toolbar for each VDA.

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

About this feature This feature offers a more customized audio experience with the following key features when connected to a virtual desktop:

- **Device selection:** Users can assign different input and output audio devices to different VDAs. For example, you can have two different VDAs, each using a separate default speaker (one built-in speaker and one headset). The exact audio device can be selected for each active VDA from the **Preferences** section. The selected device becomes the default device from the same session.
- **Configuration persistence**: The system preserves the selected configuration for the next session, ensuring a seamless experience.
- **Microphone permission:** Users must grant microphone permission to select default audio devices. If the permission is in the "prompt"state (neither granted nor denied), users must grant access. If the permission is **denied**, users must reset the permission before granting access.

If microphone permission is ***denied**, default audio device selection is disabled and the following dialog appears:



Known limitations in the feature

- This feature is not applicable for published applications and mobile session launches.
- The feature is not applicable to the Mozilla Firefox browser in macOS.

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

- The feature doesn't list audio output devices in the Apple's Safari browser.

For more information about the feature and configuration, see Default audio device selection.

Entra ID single sign-on support for VDA with Azure AD credentials Starting with version 2511, Citrix Workspace app for HTML5 now provides seamless single sign-on (SSO) experience for VDAs with Entra ID credentials. This feature eliminates the need for users to enter credentials when launching HDX sessions with Microsoft Entra ID joined VDAs, providing a streamlined authentication experience.

With this feature, users with Entra ID-joined VDAs get seamless authentication and do not need to enter credentials each time they launch a VDA. For seamless single sign-on (SSO) to Entra VDAs, enable pop-ups in your browser settings because blocked pop-ups can prevent successful SSO.

Applicability This feature applies to app and desktop session launches with pure and hybrid Entra ID joined VDAs of version 2507 and above with the specified OS versions.

Known limitations A pop-up window opens during session launch. The pop-up behavior varies depending on your browser and browsing mode (normal or incognito).

For more information, see Entra ID single sign-on support for VDA with Azure AD credentials.

Always On Tracing (AOT) Citrix Workspace app for HTML5 now supports Always On Tracing (AOT), a modern diagnostic framework from Citrix that continuously captures relevant log data across the Citrix Virtual Apps and Desktops environment. This feature simplifies troubleshooting for IT administrators and Citrix support teams by automatically capturing log data for user sessions and system events, eliminating the need to reproduce issues.

AOT makes logs easily accessible and readable without engineering-level expertise, enabling self-service diagnostics to reduce dependency on Citrix Support and improve mean-time-to-resolution.

Benefits AOT provides significant value to customers by:

- **Automatically capturing log data** for user sessions and system events without manual intervention
- **Eliminating the need to reproduce issues** since logs are continuously collected during normal operations
- **Making logs easily accessible and readable** without requiring engineering-level expertise
- **Enabling self-service diagnostics** to reduce dependency on Citrix Support
- **Improving mean-time-to-resolution** for troubleshooting scenarios

For more information, see Always On Tracing.

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

Fixed issues

There are no new fixed issues in this release.

2509

What's new

High DPI support for multiple monitors Citrix Workspace app for HTML5 supports DPI scaling for app and desktop sessions on single and multi-monitor sessions. This feature is mostly used with large-size and high-resolution monitors to display applications, text, images, and other graphical elements in a size that can be viewed comfortably.

> **Note:**
>
> This feature is enabled by default for app and desktop sessions.

Benefits This feature automatically adjusts virtual desktop and app sessions based on device DPI, ensuring content appears perfectly sized and sharp without blurriness. Apps and desktops are intelligently scaled based on monitor resolution and device pixel ratio for optimal readability and usability.

For more information about how to configure, see High DPI support for multiple monitors.

Enhanced Alt+ key shortcuts support in double-hop RDP scenarios Previously, **Alt + key** combinations such as **Alt + Tab** or **Alt + F** did not work properly in double-hop RDP sessions when using Scancode and Unicode mode.

With the 2509 version, **Alt + key** shortcut combinations now function correctly in double-hop scenarios, providing improved keyboard interaction for nested RDP connections.

Generic Client IME enhancement for Citrix Workspace app for HTML5 on Chromebook with multi monitors Previously, enabling the multi-monitor configuration for the IME resulted in duplicate input on secondary displays in ChromeOS.

With the 2509 version, we now use the browser API to manage the relationship between key and input events, preventing duplicate characters from being entered per keystroke.

Configuration for blocking Global App Configuration service (GACS) requests With the 2509 version, administrators can block Global App Configuration service (GACS) requests using configuration.js for on-prem stores. The attribute name is **disableGACS**. When you set this attribute to **true**, Citrix Workspace app doesn't connect to any GACS endpoints.

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

> **Note:**
>
> The attribute **disableGACS** is set as **false** by default.

For more information about how to configure, see Configuration for blocking Global App Configuration service (GACS) requests.

Configuration for blocking feature flag requests With the 2509 version, administrators can block feature flag requests using configuration.js for on-prem stores. The attribute name is **disableFeatureFlag**. When you set this attribute to **true**, Citrix Workspace app doesn't connect to any feature flag endpoints.

> **Note:**
>
> The attribute **disableFeatureFlag** is set as **false** by default.

For more information about how to configure, see Configuration for blocking Global App Configuration service (GACS) requests.

Enhanced session toolbar notch size The 2509 version of Citrix Workspace app for HTML5 features a redesigned, smaller notch in the session window that you can drag and drop to any window edge. The notch design provides an optimal size, and the cursor pointer changes when you hover over it. This update addresses user feedback about wasted screen space and replaces the unclear orange indicator with a recognizable warning icon when Connection State Indicator (CSI) detects network issues.

> **Note:**
>
> When you use Citrix Workspace app for HTML5 version 2509 or later, this feature is automatically enabled for desktop sessions and requires no client-side configuration.

Fixed issues

- In a Citrix Workspace app for HTML5 session, audio recording might intermittently fail. The issue occurs if the store page configured with NetScaler Gateway signs out. [RFHTMCRM-16572]
- The Citrix Workspace app for HTML5 client intermittently fails to detect the webcam after you remove and reattach it. [RFHTMCRM-15775]
- When you disconnect a Citrix Workspace app for HTML5 session by closing the browser page or clicking the disconnect button, the event viewer in VDA displays 'RPM error 12'.[CVADHELP-27958]

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

2505.10

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues

- When Citrix Workspace app for HTML5 sessions are running on Chrome browser in iOS devices, the Microsoft Teams optimization might not work. [RFHTMCRM-16068]
- When you start Citrix Workspace app for HTML5 sessions on mobile devices, an extra blank window might appear. The issue occurs when users click the **Allow pop-up** dialog during session launch on mobile devices. [RFHTMCRM-16009]
- When you download files larger than 2 GB from a session to local storage, the Citrix Workspace app for HTML5 session window might close unexpectedly. The issue occurs when the maximum download file size limit is set to more than 2 GB. [CVADHELP-28735]

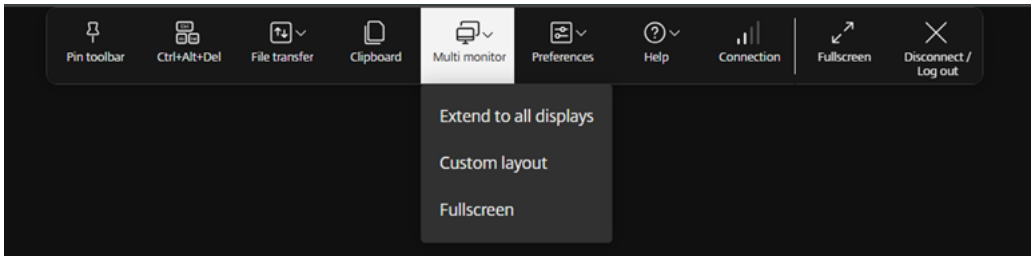
2505

What's new

Following are the new features and enhancements:

- Enhanced multi-monitor support with auto-detection and custom display selector
- Disable downloading of Citrix Workspace™ app logs in error dialogs

Enhanced multi-monitor support with auto-detection and custom display selector Starting with version 2505, new options have been added under **Multi monitor** icon in the toolbar, which appears only when more than one screen is connected. The multi-monitor selector allows users to choose which displays to use in full-screen mode for app and desktop sessions.



As long as the layout remains the same at the client OS, it is remembered when you disconnect and reconnect to the same session.

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

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

System requirements This feature is only supported on Google Chrome and Microsoft Edge Chromium browsers on Windows OS.

Prerequisites

- Ensure that the new toolbar feature is enabled. For more information, see Improved in-session toolbar.
- Allow permissions:
  - **Window management permission** that is important for websites that must access information about different monitors and manage windows across them
  - **Browser pop-up permission** to manage whether websites can open new windows or tabs without your direct interaction.

Known limitations

- On the external monitor, resource windows aren't in full-screen mode. Instead, it is in windowed mode with a size equal to the external monitor size. We recommend manually switching to full-screen for a better user experience on each of the external monitor windows.

  To switch fullscreen, use the F11 key on Windows and your Mac, move the pointer to the green button in the top-left corner of the window, then choose **Enter Full Screen** from the menu.
- The multi-monitor selection is not saved between sessions. You must manually select your preferred monitors each time you start a new session by clicking the multi-monitor icon on the toolbar.
- Multi-monitor state goes into single monitor **Fullscreen** state by default on external monitor layout change when the session is in active state.

For more information on how to configure, see Enhanced multi-monitor support with auto-detection and custom display selector.

Disable downloading of Citrix Workspace app logs in error dialogs Starting with the version 2505, admins can hide the **Download Log** button in all error dialogs for both app and desktop sessions in Citrix Workspace app for HTML5 (cloud and on-prem).

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

> **Note:**
>
> This feature is disabled by default. In other words, the user has an option to download logs from the error dialog.

For more information, see Disable downloading of Citrix Workspace app logs in error dialogs.

Fixed issues

- When you are inside a published desktop session through Citrix Workspace app for HTML5, you might intermittently see a white screen during the sessions. [CVADHELP-28120]
- When a user starts a Citrix Workspace app for HTML5 session in a mobile browser with all the required permissions, audio doesn't play. In addition, the speaker icon shows a red indicator, even though audio output devices appear. [RFHTMCRM-15621]
- When you start Citrix Workspace app for HTML5 lease in Firefox, the session fails to start. [RFHTMCRM-15130]
- When you start an HTML5 session, some published apps might fail to open, causing the session to remain indefinitely in the 'Preparing Windows' launch state. [CVADHELP-28010]
- In a multi-monitor set up, when you start a Citrix Workspace app for HTML5 session on high-resolution monitors, the session might close unexpectedly without warning. [CVADHELP-27671]

2502.10

This release addresses areas that improve overall performance and stability.

Fixed issues

- When you start an HTML5 session, some published apps might fail to open, causing the session to remain indefinitely in the 'Preparing Windows' launch state. [CVADHELP-28010] [CVADHELP-28039]

2502

The following are the features:

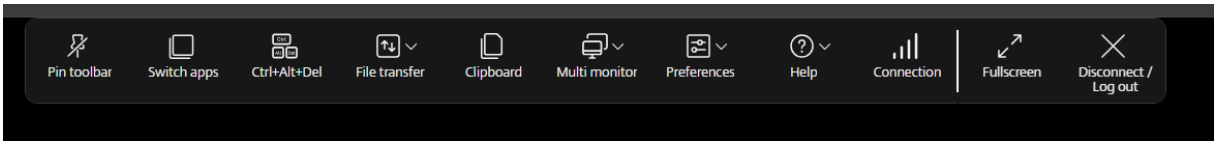
- Enhancements to the improved in-session toolbar
- Connection strength indicator
- Service continuity [Technical Preview]

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

- Support for horizontal scrolling on trackpad
- Session launch diagnostics
- Enhanced seamless app launch and resizing experience
- Support for Unified Communications (UC) SDK

Enhancements to the improved in-session toolbar

Starting with the 2502 version, this feature is enabled by default. To disable the feature, follow the configuration steps mentioned in this article.



> **Note:**
>
> The new toolbar isn't supported if the Citrix Workspace app for HTML5 session is launched in a mobile browser.

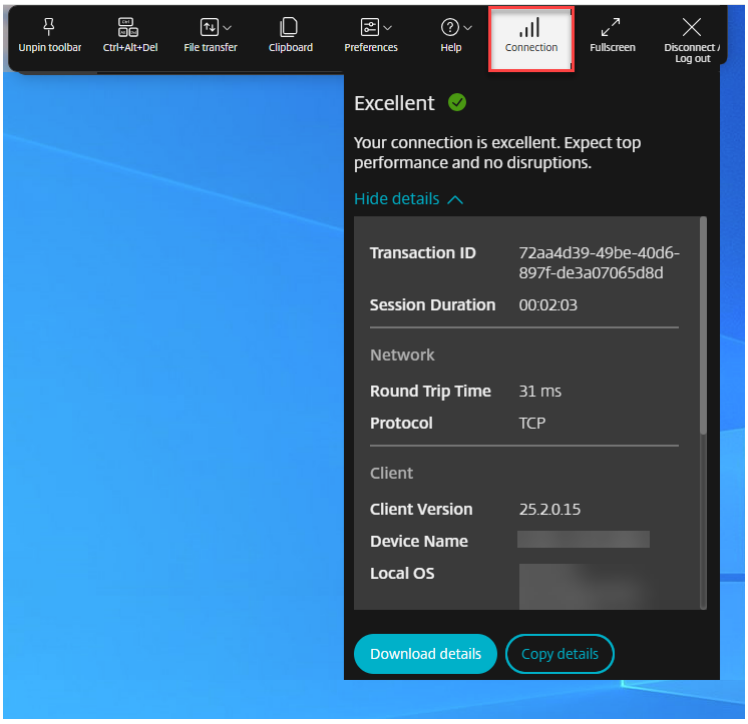
For more information, see Enhancements to the improved in-session toolbar.

Connection strength indicator

Starting with the version 2502, Citrix Workspace app for HTML5 supports the Connection Strength Indicator (CSI) on the in-session toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy (or download) diagnostic information to share with IT for advanced troubleshooting.

> **Notes:**
>
> - This feature is enabled by default.
> - When you open the session, you can see the Connection Details icon on the in-session toolbar, provided the new toolbar feature is enabled.

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



For more information, see the Connection strength indicator.

Support for Unified Communications (UC) SDK

The Citrix Unified Communications SDK allows Unified Communications vendors, Cloud contact center providers, Communications Platform as a Service (CPaaS) providers, or any WebRTC-based communications vendors to integrate seamlessly with electron-based desktop or browser-based applications.

For more information, see Support for Unified Communications (UC) SDK.

For additional information about architecture, see Unified Communications (UC) SDK, which is a tech zone article.

Technical Preview in 2502

- Service continuity

Enhanced seamless app launch and resizing experience

Starting with the 2502 version, Citrix Workspace app for HTML5 ensures an enhanced app launch experience. You experience a seamless, flicker-free transition to your apps without intermediate screens.

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

The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

Session launch diagnostics

Starting with the 2502 version, we've implemented an improved support process for session failures. Help desk administrators are now equipped with comprehensive insights into failure paths, allowing them to effectively triage and significantly reduce the number of support cases related to session failures.

For more information, see Session launch diagnostics in the Citrix Monitor documentation.

Support for horizontal scrolling on trackpad

Starting with the 2502 version, horizontal scrolling using the trackpad is supported within the session.

Fixed issues

- When the secure ICA® feature is disabled in the delivery group properties, the session might not start. [RFHTMCRM-14974]

2411

What's new

The following are the features:

- Enhanced desktop launch experience
- Enhanced virtual desktop screen resizing experience
- Enhanced session reliability
- Improved in-session toolbar
- Sustainability initiative from Citrix Workspace app
- Enhanced log collection
- View endpoint telemetry in Citrix Director
- Progressive Web App version of Citrix Workspace app for HTML5 for StoreFront
- Citrix VDA for macOS - clipboard and keyboard shortcuts
- Enhanced keyboard and IME diagnostics tool

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

Enhanced desktop launch experience Starting with version 2411, Citrix Workspace app for HTML5 ensures an enhanced desktop launch experience. You can experience a seamless, flicker-free transition to your desktop without intermediate screens. The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

Enhanced virtual desktop screen resizing experience Starting with the 2411 version, Citrix Workspace app for HTML5 ensures a smooth transition and prevents dark screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

Enhanced session reliability The following improvements address network disruptions, ensuring a better user experience by reconnecting the session reliably:

- When you switch between Internet Service Providers (ISP), the session becomes unresponsive. With the fix, you can reconnect to the session during ISP switches.
- When you switch networks and one Wi-Fi connection lacks internet connectivity, the session reliability feature might fail. With the fix, you can now reconnect to the session during a network switch.

Improved in-session toolbar Starting with the 2411 version, an enhanced toolbar UI appears when you start a desktop session. The look and feel of the in-session toolbar UI has changed. The toolbar UI is designed to enhance the end user experience by organizing the options in a user-friendly manner.

> **Note:**
>
> This feature is disabled by default.

For more information, see Improved in-session toolbar.

Sustainability initiative from Citrix Workspace app Starting from the 2411 version, admins can customize the disconnect and log out dialog box contents in the **Save energy** screen.

> **Notes:**
>
> - This feature is disabled by default.
> - This feature is available on both cloud and on-premises stores.

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

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

Enhanced log collection Starting with version 2411, users can download Citrix Workspace app logs in a zip file, simplifying log retrieval and analysis for better troubleshooting and an improved user experience.

For more information, see Enhanced log collection.

View endpoint telemetry in Citrix Director This feature enhances the ability of admins to view endpoint telemetry data directly in Citrix Director.

Prerequisites

- Citrix Workspace app for HTML5 2411 and later
- VDA version 2411 and later
- Citrix Director

Citrix VDA for macOS - clipboard and keyboard shortcuts Starting with the 2411 release, Citrix Workspace app supports Citrix VDA for macOS.
For more information, see Support for macOS VDA: clipboard and keyboard shortcuts.

Enhanced keyboard and IME diagnostics tool Starting with version 2411, Citrix Workspace app for HTML5 supports a new self-service command line tool hosted in Windows Virtual Delivery Agent (VDA) to diagnose keyboard and Input Method Editor (IME) related issues. This tool meets various user requirements, provides platform versatility, and caters to personalized needs. The keyboard and IME functions depend on different configurations and capabilities in VDA and Citrix Workspace apps. Incorrect settings in the VDA or client-side might result in unexpected input behavior.

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

Technical Preview in 2411

- Progressive Web App version of Citrix Workspace app for HTML5 for StoreFront

Fixed issues in 2411

- Audio mapping works after the Citrix Workspace app for HTML5 session starts, but stops working after some time when the StoreFront page signs out. [CVADHELP-26423]
- When accessing an HTML5 session from Citrix Gateway, and third-party access is blocked through URL rewrite on Citrix Gateway, Citrix Workspace app, and desktop sessions might not start successfully. This issue occurs on Citrix Workspace app for HTML5 versions 2404.1 or later for StoreFront stores. [CVADHELP-26253]

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

- When you access an HTML5 session from Citrix Gateway using Chromium-based browsers, and the third-party access is blocked through the URL rewrite on Citrix Gateway, the browser's renderer process consumes excessive memory. This action causes the app to become unresponsive.
  In addition, the webpage displays the following error:
  "Not enough memory to open this page."[CVADHELP-25942]

Known issues in 2411

There are no new known issues in this release.

2409

What's new

Feature flag management Citrix is changing the way that it manages feature flags, allowing access to preview features and enabling dynamic management of features in production.

To ensure optimal functioning of the *App switcher* feature, which is under feature flag, ensure to enable traffic to the URL `features.netscalergateway.net`and to use Citrix Workspace app for HTML5 version 2409 and later.

For more information about the known issues and workaround in this feature, see Feature flag management.

Fixed issues

- When you upgrade Citrix Workspace app for HTML5 to the 2404.1 version, a session might not start. The issue occurs when the encryption is set to RC5-128. [RFHTMCRM-13828]

2408

What's new

HDX™ adaptive throughput Starting with the 2408 version, HDX adaptive throughput is supported. This feature intelligently fine-tunes the peak throughput of the ICA session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high-latency networks.

This feature provides better interactivity, faster file transfers, smoother video playback, and a higher frame rate and resolution resulting in an enhanced user experience.

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

Session interactivity is constantly measured to determine whether any data streams within the ICA session adversely affect interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

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

Technical Preview

- Secure HDX
- Improved in-session toolbar

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

Fixed issues

There are no fixed issues in this release.

2404.1

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues

- Global App Configuration service (GACS) settings for Citrix Workspace app for HTML5 don't apply when end users start a session for the first time. With the fix, GACS settings are applied when the user starts the session for the first time and thereafter. Also, end users might be prompted to restart the session to ensure compliance. [RFHTMCRM-12494]

2404

What's new

This release addresses areas that improve overall performance and stability.

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

Fixed issues

When you click **Multimonitor** from the session toolbar, the session might not extend automatically. The issue occurs when you use Citrix Workspace app for HTML5 version that is earlier than 2404, and the Google Chromium browser version is equal to or greater than v125.0.0. [RFHTMCRM-12454]

2402

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues

- If you're on an optimized Microsoft Teams call and decide to stop sharing your screen, you might observe a blank rectangle in place of the video section. [RFHTMCRM-11689]
- During the session, when you scroll horizontally to access the input area on the right, the soft keyboard might appear on the upper left of the screen.

  The issue occurs when you:

  - set the display resolution to custom.
  - enable multi-touch mode. [CVADHELP-24460] [RFHTMCRM-12106]
- When using Citrix Workspace app for HTML5 on iOS devices, the **Delete** key deletes two characters at once. The issue occurs when you switch keyboard languages from Chinese Traditional to English. [CVADHELP-24216] [RFHTMCRM-11787]
- When you attempt to disconnect a virtual app or desktop session through the toolbar > **...** > **Disconnect** button on cloud stores, the session remains active in Citrix Studio. However, the session status changes to inactive after a couple of minutes. [RFHTMCRM-11642]
- When Citrix Workspace app for HTML5 is set to be consumed from the content delivery network (CDN), the session might fail. The issue occurs when you use the HDX SDK using HTML5. [RFHTMCRM-11765]
- When you start an app session, horizontal and vertical scroll bars appear even when you set the display resolution to autofit. [RFHTMCRM-11650]
- When you start a Citrix Workspace app for HTML5 session and disconnect it from the session toolbar, the session remains active in Citrix Studio. The issue occurs when you are on the on-premises deployment. [RFHTMCRM-12017]

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

- When you start a virtual desktop session using the Safari browser, the webcam might not work properly. [RFHTMCRM-12348]
- When you start a virtual desktop session followed by an app session, both vertical and horizontal scroll bars appear in the app session. [RFHTMCRM-12245]
- On cloud deployments, when you start the HTML5 session for the first time, a spinner appears indefinitely. [RFHTMCRM-11754]
- When you start a Linux VDA session, the time reflected in the session might not match the local time zone of the end user's device. [RFHTMCRM-11602]

2312

What's new

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

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

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

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

For more information, see Support for secondary ringer.

Simulcast implementation for optimized Microsoft Teams video conference calls Starting with the 2312 release, by default, simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved. We're adapting to the proper resolution for the best call experience for all callers.

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

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

Fixed issues

- On iOS devices, when you start a session, the clipboard data from the previous HTML5 session is pasted without your consent. The issue might occur when you use key combinations like **Ctrl+a** and **Ctrl+x** with an external keyboard or keep typing when you switch between two applications. [RFHTMCRM-10834] [CVADHELP-23753]
- When you use LongCommandLine arguments to start a session, the session might fail to start. The issue occurs when you use the Apple Safari browser on macOS and iOS devices. [CVADHELP-23753]

Known issues

Known issues in 2603.10

- When **USIP** mode is enabled on the NetScaler ADC, Citrix Workspace app for HTML5 session started through the Gateway might fail. This issue occurs if the client resides in a different subnet than the STA/VDA servers. The issue might display error messages, such as "VDA connection refused"or "Cannot connect to server". For more information, see NetScaler USIP.

  Refer to Slow Response to the Client Requests when USIP Mode is Enabled on ADC. [NSHELP-43974]

  As a workaround, you can follow one of the two options:

  - Disable **USIP** on the NetScaler ADC if it is not required.
  - If **USIP** mode must remain enabled, then the default route on the DDCs must point to the ADC appliance as the default gateway.

- When you enable **Secure ICA** encryption on the server (delivery group), Citrix Workspace app for HTML5 sessions might fail to start. [CVADHELP-33623]

  As a workaround, configure **Secure HDX** which is more secure. For more information, see Secure HDX™.

  > **Note**
  >
  > If you have **Secure ICA** enabled on a delivery group where you intend to use Secure HDX, you must disable **Secure ICA** first. To do that, perform the following steps:
  >
  > - Edit the delivery group.
  > - Navigate to **User Settings**.
  > - Disable **Secure ICA**

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

Known issues in 2603

There are no new known issues in the release.

Known issues in 2511

- When you upgrade from Citrix Workspace app for HTML5 2509 to 2511, few features like audio, PDF printing might not work upon first launch after upgrade. On subsequent launches the issue isn't observed. [RFHTMCRM-16799]

Known issues in 2505

- When you start an HTML5 session and play a video using apps that use a custom cursor, like VLC player, the cursor might appear incorrectly when you hover over the playback content. [RFHTMCRM-13676]
- When end users start a session using Citrix Workspace app for HTML5, the browser prompts them with a microphone permission dialog box. [RFHTMCRM-14984]
- When you start a virtual desktop session using Citrix Workspace app for HTML5, the desktop doesn't open on the first attempt. The session starts only on the second try if you keep the first browser tab open.

  The issue occurs when **rate limit identifier** is enabled on NetScaler® Gateway (Rate limiting).

  As a workaround, set the **rate limit identifier** to at least 20 to prevent intermittent session failures. You can also run `ns limitIdentifier rate_id_URL_IP -threshold 20` to adjust the setting. [CVADHELP-27592]

Known issues in 2502

- In a multi-monitor setup, typing characters on the second screen of ChromeOS devices causes the keyboard to send double strokes. For example, pressing 't' results in 'tt.' [CVADHELP-27464]

  As a workaround:

  Upgrade Citrix Workspace app for HTML5 to version 2409 or later, and ensure that traffic is allowed to the URL `features.netscalergateway.net`. If upgrading isn't possible, disable the IME multi-monitor feature in the configuration settings:

```
'features' : {

    'ime': {

```

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

```
            'multiMonitor' : false
             }

    }
```

Known issue in 2404.1

- For Citrix Workspace app versions 2404.1 or later on StoreFront, when third-party access is blocked via URL rewrite on Citrix Gateway, the app and desktop sessions mightn't launch successfully. The workaround is to disable the URL rewrite policy applied on the Gateway. [CVADHELP-26253]

Known issues in 2402

- If you attempt to download files or modify files inside the mapped drive from VDA using apps that rely on temporary file, data might get corrupted. For example, browsers, Microsoft office apps such as Excel. [RFHTMCRM-12156] [CVADHELP-24459]
- When you attempt to disconnect a virtual app or desktop session through the toolbar > **...** > **Disconnect** button, the session remains active in Citrix Studio. The issue occurs with the on-premises store that is configured with Citrix Gateway. [HDX-60157]

Known issues in 2310

- When you start a desktop session using Citrix Workspace app for HTML5 on the Google Chrome browser, green blocks are visible on the display screen that blocks the UI. The issue might occur when you move an application window inside the launched desktop. [CVADHELP-23377]
- When accessing an HTML5 session from Citrix Gateway using Chromium-based browsers with third-party access blocked through the URL rewrite on Citrix Gateway, the browser's renderer process consumes excessive memory. This action causes the app to become unresponsive. In addition, the webpage displays the following error:
  "Not enough memory to open this page."

  The issue affects Citrix Workspace app for HTML5 versions 2310 and later. As a workaround, disable analytics on the StoreFront server. [CVADHELP-25942]

Known issues in 2203

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

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

Known issues in 2202

- When you use Microsoft Teams optimization and share the screen, a red border that indicates the screen sharing is unavailable. [RFHTMCRM-6360]

Known issues in 2108.2

- When **Use Video Codec for Compression** is set to **For the Entire Screen** in Citrix Studio, a multi-monitor session might render incorrectly. We recommend changing the setting to **Use when preferred** in multi-monitor sessions. [RFHTMCRM-5523]

Known issues in 2105.5

- The input of the first character might not appear exactly at the location of the workspace session's cursor position. [RFHTMCRM-4909]
- When a CJK Generic Client IME user single-clicks a cell to type in Microsoft Excel, the Candidate and Composition Window UI might not appear at the focus position. As a workaround, double-click the cell. [RFHTMCRM-5185]

Legacy documentation

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

Known limitations

- Disconnecting from a session: When you disconnect from a session by closing a tab or closing the browser, the server might not get notified that the session was disconnected. As a result, the session on the server remains active for the default 180 seconds or the configured session reliability timeout.

  Recommendation: We recommend that you disconnect the session through the toolbar option.
- 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]
- 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]
- In a session, when you try to send **command + R** key combination prompts to disconnect the session instead of remoting to the session. The issue occurs when you use the Safari browser application. [RFHTMCRM-6415]

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

- When you use Microsoft Teams optimization and share the screen, a red border that indicates the screen sharing is unavailable. [RFHTMCRM-6360]
- External mouse and keyboard aren't supported with Citrix Workspace app for HTML5 in any browser on Android or iOS operating systems. [RFHTMCRM-6623]
- When you close the browser or the browser tab to disconnect the session, the session state might remain active on the server (Delivery Controller™) for sometime. The issue occurs intermittently.

  As a workaround, use the **Disconnect** option from the secondary menu in the session toolbar. [RFHTMCRM-5457]
- Horizontal scroll from a touchpad isn't supported.
- When you connect multiple audio devices in a session, you can hear audio from one device only. You might not be able to switch to the other audio device. [HDX-49312]
- In a session, you might not hear the audio from some applications when you disconnect and reconnect to your previous session though toolbar. [HDX-49313]
- Anonymous logins to Citrix Virtual Apps and Desktops from devices with different Device IDs across sessions can sometimes lead to an incorrect user or device license count.
- In a session, when you open Microsoft Excel and do a cut-and-paste operation using a keyboard, the text in the cell isn't cleared after the cut action. [RFHTMCRM-10426]
- When you transfer files using Client Drive Mapping functionality from your local device to the VDA and conversely, data might get corrupted. [RFHTMCRM-11474]
- When you start a desktop session using Citrix Workspace app, green blocks are visible on the display screen that blocks the UI. The issue might occur when you move an application window inside the launched desktop. [CVADHELP-23377]
- When you use Citrix Workspace app for HTML5 to access published desktops, resizing the window might not work when you adjust the browser window size. The issue occurs when the multi-monitor feature configuration is disabled in Citrix Workspace app for HTML5. In addition, this issue occurs when you have Citrix Virtual Apps and Desktops versions 2308 through 2411.

  As a workaround, enable the multi-monitor feature. To enable:

  1. Locate the **configuration.js** file. The **configuration.js** file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder.
  2. Edit the **configuration.js** file and set the value of the **trueMMSupportForHTML5** property to **true**.
     For example,

```
var HTML5_CONFIG =
```

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

```
{

    'features': {

        'graphics': {

            'multiMonitor': true,
                'trueMMSupportForHTML5': false
                    }

                }

 }
;
```

For more information, see Multi-monitor.

- In a cloud setup, when using the Citrix PDF printer to print a file and save it as a PDF on a local machine, the content in the resulting PDF is neither editable nor selectable. The issue occurs because the Citrix PDF printer creates image files instead of generating editable text in PDFs. As a workaround, disable the Enhanced PDF printing experience feature. [CVADHELP-26286]
- When you launch sessions from an internal network with Citrix Virtual Apps and Desktops 2507 DaaS that has NLS configured and Network Telemetry Policy or HDX direct enabled on the DDC, sessions might fail to launch. As a workaround, disable the Network Telemetry Policy or HDX direct policy and manually reset the TLS listener on 443 (SSLEnabled off). [CVADHELP-29648]
- When you switch from fullscreen to restore and vice versa, the **Fullscreen** or **Restore** toolbar button doesn't update correctly. The issue occurs when you use keyboard shortcuts like F11 in the Citrix Workspace app for HTML5 session on macOS browsers.

  As a workaround, use the **Restore** or **Fullscreen** option from the toolbar instead of keyboard shortcuts. [RFHTMCRM-17586]

Deprecation

For information about deprecated items, see the Deprecation page.

Legacy documentation

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

Third-party notices

Citrix Workspace app for HTML5 might include third-party software licensed under the terms defined in the following document:

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

Citrix Workspace app for HTML5 Third-Party Notices (PDF download)

Features in Technical Preview

July 10, 2026

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

List of features in Technical Preview

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

Title	Available from version	Enablement form (Click the icon)	Feedback form (Click the icon)
Progressive Web App version of Citrix Workspace app for HTML5 for StoreFront	2411	You can configure the feature	
Service continuity	2502		

Progressive Web App version of Citrix Workspace app for HTML5 for StoreFront

This feature is in technical preview from 2411 release.

The Progressive Web App (PWA) version support for Citrix Workspace app for HTML5 with StoreFront gives you a simplified, native-like Citrix Workspace app experience that you can easily install from your web browser. This feature is supported only on desktop browsers.

Benefits

The following are some of the advantages of using the PWA version:

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

- Native app-like behavior: PWAs can look, behave, and feel like native apps, which can improve the user experience.
- Home screen access: PWAs can be added to a device's home screen like a native app, which saves storage space.
- Secure: PWAs use HTTPS to ensure that sensitive information is sent through encrypted lines and that the site's content can only be altered with the owner's permission.

> **Notes:**
>
> This feature is disabled by default.

Configurations

Admins can enable this feature on the StoreFront Management Console. For more information, see Progressive Web App.

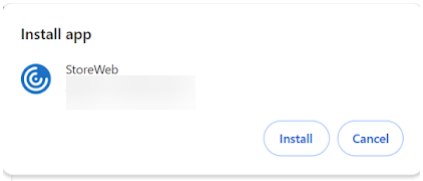
Install PWA using Google Chrome

End users can install the store website as follows:

1. Open the store in the Google Chrome browser.
2. Click the following icon in the toolbar.

   The option to install PWA appears.

3. Click **Install** to add your store as PWA to your desktop, Start menu, Launchpad, or similar.

Install PWA using Microsoft Edge

End users can install the store website as follows:

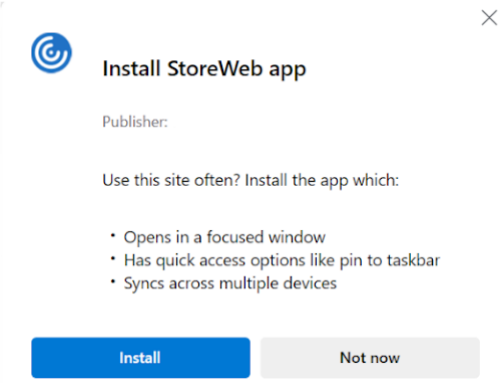
1. Open the store in the Microsoft Edge browser.

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

2. Click the following icon in the address bar.

   The option to install PWA appears.

3. Click **Install** to add your store as PWA to your desktop, Start menu, Launchpad, or similar:

   If you have multiple StoreFront™ stores, you can install each store website separately. Each installation generates a shortcut named `Store website name`, which can be renamed accordingly.

Known limitations in the feature

- When you set single tab mode on the StoreFront deployment, it does not apply to PWA launches.
- Clicking the shortcut icon opens a new window that hosts the store page.
- Hybrid scenarios during session-shared app launches are not supported. For example, launching an app from the PWA and then trying to launch a session-shared app in the browser does not work.
- Switching from the PWA session window to the browser window does not work.

Service continuity

This feature is in technical preview from 2502 release.

Service continuity removes or reduces the dependency on the availability of components 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.

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

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

> **Note:**
>
> This feature is disabled by default. To get it enabled in your environment, fill the form:.

Prerequisite

In case a store page or Citrix Workspace app for HTML5 page is inaccessible over the network, the Citrix Workspace app for HTML5 binaries must cache for service continuity to work, and they require at least one successful regular launch for caching.

Known limitations in the feature

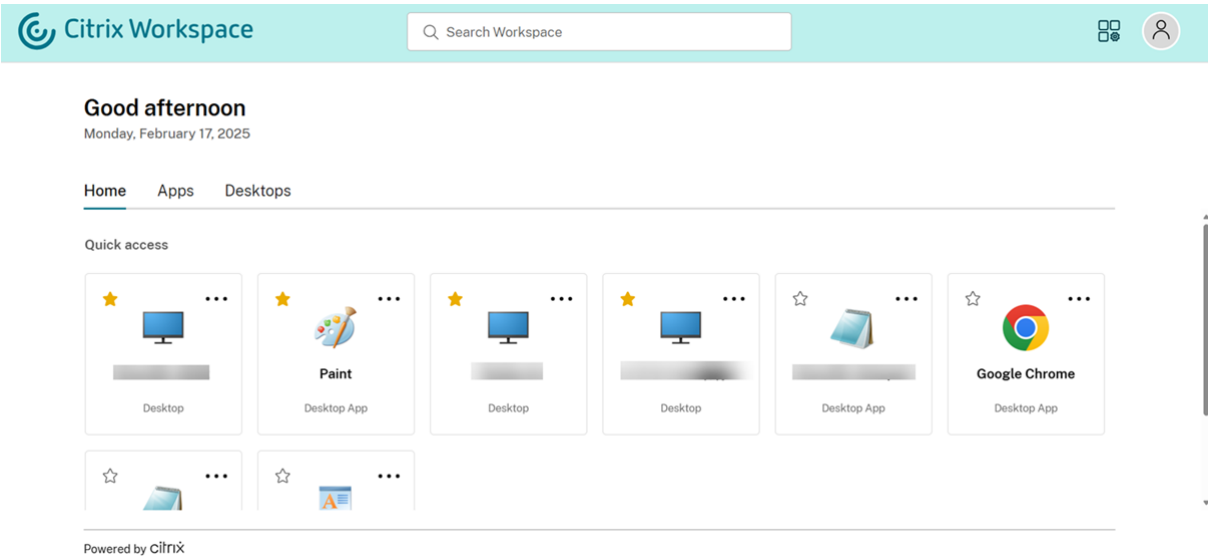
- In Citrix Workspace app for HTML5, the service continuity feature isn't supported on the Apple Safari and Mozilla Firefox browsers. It supports only Chromium browsers (Google Chrome and Microsoft Edge).
- Service continuity doesn't support showing an offline banner on the login page.
- Lease files download five minutes after the store page is authenticated. If the store page refreshes, it takes another five minutes to download the lease files.
- If the store URL can't be accessed, the offline mode that displays cached resources might be delayed, which also delays the session launch.

Known issues in the feature

- When the VDA is powered off, the lease launch can't start and gets stuck on the progress message "Connection leases are being resolved."The workaround is to wait a while and then attempt to relaunch the session. [RFHTMCRM-15129]

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

Collect Workspace UI - store page logs



To collect and download the logs for the store page:

1. Press **Ctrl + Shift + L** on the store page to enable logging.
2. Reproduce the issue.
3. Press **Ctrl + Shift + /** to download the logs.
4. Press **Ctrl + Shift + L** again to stop logging.

> **Note:**
>
> When the page reloads, the logs might reset.

For more information on Citrix Workspace app for HTML5 logging, see How to collect logs.

Technical Preview to General Availability (GA)

Feature name	General availability version
Secure HDX™	2503

Citrix Workspace app for HTML5 - Preview

September 22, 2026

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

This documentation describes the features and configuration of Citrix Workspace app for HTML5 2607. This version is the preview for the latest version of Citrix Workspace app for HTML5.

EAR build

EAR build is for the purpose of testing or validation with the intent to make organizations ready for the upcoming release and is NOT advised to be deployed in production environments.

Install the EAR build from Citrix Downloads.

What's new

Following are the new features and enhancements:

- Integration of deviceTRUST with Citrix Workspace app for HTML5
- Synchronization for Lock Key States
- Auto Client Reconnect
- Give or Take Control in Microsoft Teams Optimization
- Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

Integration of deviceTRUST with Citrix Workspace app for HTML5

Starting with version 2607, Citrix Workspace app for HTML5 supports deviceTRUST integration, enhancing security through continuous device posture checks within sessions. This integration ensures only compliant devices that can access Citrix Virtual Apps and Desktops through browser.

About the feature deviceTRUST provides continuous device posture monitoring and assessment capabilities for html5 devices accessing Citrix environments. The integration uses web-based APIs to collect device information and enforce security policies based on device compliance status.

> **Note:**
>
> For more information about deviceTRUST, see deviceTRUST Platform.

Benefits This integration provides:

- **Continuous security monitoring** - Real-time device posture assessment during active sessions
- **Policy enforcement** - Automated responses based on device compliance status
- **Enhanced visibility** - Comprehensive device information for security administrators
- **Seamless user experience** - Transparent security checks without user intervention

For more information on how to configure, see deviceTRUST

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

Synchronization for Lock Key States

Starting with version 2607, Citrix Workspace app for HTML5 introduces enhanced synchronization for lock key states (Caps Lock, Num Lock, and Scroll Lock) with the client state. This feature ensures consistent behavior of Caps Lock, Num Lock, and Scroll Lock within your session and it continues even when you switch to your local tasks. It remains consistent when you return to the session.

Auto Client Reconnect

Starting with version 2607, Auto Client Reconnect (ACR) feature ensures session continuity by automatically re-establishing connections when Session Reliability cannot recover an interrupted session. If the Session Reliability timeout expires before network connectivity is restored, the Citrix Workspace app attempts to reconnect to the same session. This reconnection uses a server-issued reconnect cookie, allowing you to resume your session from where you left off without needing to reauthenticate. For more information, see Auto Client Reconnect.

Give or Take Control in Microsoft Teams Optimization

Starting with version 2607, you can manage screen sharing control during meetings. This feature allows participants to interact with a shared screen using keyboard, mouse, and clipboard input. For more information, see Give or Take Control in Microsoft Teams Optimization

Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

Starting with version 2607, Citrix Workspace app for HTML5 introduces an enhanced Connection Strength Indicator, designed to provide a more intuitive and user-friendly experience.

The key improvements include:

- **Expanded device details:** Access comprehensive information, such as client device's CPU status.
- **Proactive notifications:** Receive alerts in the toolbar notch when your connection strength drops.
- **Actionable recommendations:** Get clear suggestions to resolve connectivity issues when your connection strength falls below optimal levels.
- **15-minute connection history:** Review a visual history of your connection strength over the past 15 minutes to assist with troubleshooting and analysis.

For more infromation, see Enhancement to Connection Strength Indicator on Citrix Viewer Toolbar

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

Fixed issues

- When the Microsoft Teams optimized secondary ringtone is enabled, the ringtone does not play in the Citrix Workspace app for HTML5 client. Citrix Workspace app for HTML5 SDK must be updated to utilize the new Microsoft assets URL. To enable media loading from the Microsoft Content Delivery Network (CDN), add https://*.onecdn.static.microsoft to the `media-src` directive within the Content Security Policy (CSP) meta tag in `HDXEngine.html`. [RFHTMCRM-18368]
- When you use Client Drive Mapping (CDM) to save a Microsoft Excel file to a mapped local folder using the **Save** or **Save As** option, the save operation might fail and the file might not be created. [CVADHELP-34582]
- When you copy an entire table or a worksheet from Microsoft Excel within a Citrix Workspace app for HTML5 session, the copy operation might fail and a clipboard error message might appear. [CVADHELP-33926]

Known issues

- When switching between fullscreen and restored view modes within a Citrix Workspace app for HTML5 session on macOS browsers, the fullscreen/restore toolbar button might not update correctly if you use keyboard shortcuts, such as F11.

  As a workaround, use the **Fullscreen** or **Restore** options directly from the in-session toolbar instead of keyboard shortcuts. [RFHTMCRM-17586]

Citrix Workspace app for HTML5 - Preview feedback

You can give the EAR feedback at: https://forms.office.com/r/KGpv2TzgB4.

> **Important:**
>
> The Early Adopter Release (EAR) documentation is available for information purposes only.
> It isn't a commitment, promise, or legal obligation to deliver any material, code, or functionality and must not be relied upon in making Citrix product purchase decisions.
> The development, release, and timing of any features or functionality described in the EAR documentation remain at our sole discretion and are subject to change without notice or consultation.
> Citrix does not accept support cases for EAR but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

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

Technical Preview

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

Prerequisites for installing

September 23, 2026

System requirements and compatibility

This topic lists the supported Citrix product versions for Citrix Workspace app and the requirements for users to access virtual desktops and applications.

We assume that all computers meet the minimum hardware requirements for the installed operating system.

Requirements

Users require devices running the following web browsers and operating systems to access desktops and applications using Citrix Workspace app for HTML5. All browsers are supported only on their latest versions. For a secure connection, open Citrix Workspace app sessions from HTTPS-based stores. Some features might not function when using HTTP-based stores. Observe the padlock icon on the address bar. If it is locked, then the connection is secure. If not secure, update the certificate.

The Citrix Workspace app for HTML5 uses WebSocket to establish session connections. When you access the app from an HTTPS-based StoreFront or Citrix Cloud, browsers require a Secure WebSocket (WSS) connection. Browsers block plain WebSocket (WS) connections on HTTPS pages due to mixed content security policies.

For direct connections to the Virtual Delivery Agent (VDA) without a Citrix Gateway, you must enable SSL on the VDA. This supports end-to-end WSS connections.

Plain WebSocket (WS) connections are only available in on-premises deployments where StoreFront is accessed over HTTP.

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

Browsers

- Apple Safari
- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

> **Note:**
>
> Microsoft and Citrix Workspace app have removed the support for Internet Explorer.

Operating systems

- Windows 11
- Windows 10
- Windows Phone 10
- Windows 8.1
- Windows 8 Pro and Enterprise (32-bit and 64-bit editions)
- Windows 7 Service Pack 1 (32-bit and 64-bit editions)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- macOS X 10.8 and later
- ChromeOS (latest version)
- iOS (latest version)
- Android (latest version)

Microsoft Internet Information Services (IIS) hardening

To configure StoreFront™ with an IIS configuration, see:

- File name extensions.
- Verbs.

WebAssembly file After you upgrade Citrix Workspace™ app to the latest version:

- an older version 21.1.0.5 (2101) of the app might appear in the **About** dialog.
- a session might fail to start.
- the published app session might fail to open with the following error:

  ‘‘Citrix Workspace app cannot connect to the server.’’

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

The issue occurs due to the inaccessibility of the **WebAssembly (.wasm)** file type by the browser. It must be accessible in the network, and environment where third-party apps like VPN, proxy servers are a part of the setup.

If the **.wasm** files are blocked in your network, to resolve it, verify the **.wasm** file MIME type is application/wasm, and is allowed in the network.

Supportability matrix

Citrix Workspace app for HTML5 supports access to desktops and applications through the following versions of StoreFront. Stores must be accessed through the Citrix Receiver for Web site. Citrix recommends the following:

- StoreFront 2.5 (or later)
- Citrix Workspace app for HTML5 allows you to upgrade from any version of StoreFront 2.5 or later.

When users connect through Citrix Gateway, Citrix Workspace app can be used to access desktops and applications that are delivered through:

- all the versions of Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- StoreFront that supports desktops and applications.

For direct connections through StoreFront without Citrix Gateway, Citrix Workspace app can be used to access desktops and applications through the following product versions:

- XenDesktop 7.6 and later

> **Note:**
>
> Admins need to install Citrix Workspace app for HTML5 on the StoreFront server to make it accessible for the end users. Therefore, the build is in the form of the Windows binary. However, HTML5 doesn't require any installation on the client side.

Connections

In a production environment, Citrix® recommends:

- securing communications between Citrix Receiver for Web site and users'devices with Citrix Gateway and HTTPS. Also, you must have an SSL-enabled VDA.

  For more information, see the Knowledge Center article SSL configuration on VDA

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

- using SSL certificates with a key size of at least 1024 bits throughout the environment where, Citrix Workspace app for HTML5 is deployed.

Citrix Workspace app enables users to 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 HTML5 now supports CloudBridge disabling compression and printer compression and using HDX Insight analytics to display in the CloudBridge Insight Center.

- CloudBridge 7.4 and later

> **Note:**
>
> - If you're using SecureICA to encrypt communications between users'devices and your Citrix Virtual Apps and Desktops and Citrix DaaS or Citrix Virtual Apps servers, Citrix Workspace app for HTML5 supports **Basic** encryption only. If you use other encryption levels, sessions don't start.
> - When **USIP** mode is enabled on the NetScaler ADC, Citrix Workspace app for HTML5 session started through the Gateway might fail. This issue occurs if the client resides in a different subnet than the STA/VDA servers. The issue might display the following error messages:
>
>   - VDA connection refused
>   - Cannot connect to server
>
>   For more information, see NetScaler USIP.
>
>   Refer to Slow Response to the Client Requests when USIP Mode is Enabled on ADC.

Cryptographic hash function

For Citrix Workspace app for HTML5 connections, use the SHA256 certificate because modern browsers have deprecated SHA1 and no longer support it.

Cipher suite

If there's an issue to connect the SSL-enabled VDA with Citrix Workspace app for HTML5, configure the cipher suites as specified in the following table:

Citrix Virtual Apps and Desktops™ version	Link to the TLS section
Long-Term Service Releases (LTSRs)	

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

Citrix Virtual Apps and Desktops™ version	Link to the TLS section
2507 LTSR	TLS Settings on VDAs
2402 LTSR	TLS Settings on VDAs
2203 LTSR	TLS Settings on VDAs
1912 LTSR	TLS Settings on VDAs
Current release (CRs)	
2603	TLS/DTLS Settings on a VDA
2511	TLS/DTLS Settings on a VDA
2503	TLS/DTLS Settings on a VDA
2411	Manually Configure TLS on a VDA
2407	Manually Configure TLS on a VDA
2311	TLS Settings on VDAs
2308	TLS Settings on VDAs
2305	TLS Settings on VDAs
2303	TLS Settings on VDAs
2212	TLS Settings on VDAs
2209	TLS Settings on VDAs
2206	TLS Settings on VDAs

Install

July 2, 2026

StoreFront

Enable Citrix Workspace app for HTML5 on the Citrix Receiver
for Web site. The StoreFront store provides the desktops and applications for Citrix Workspace app for HTML5 users.

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

> **Important:**
>
> In multiple-server StoreFront deployments, use only one server at a time to change the configuration of the server group. Verify the Citrix StoreFront management console isn't running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so you update the other servers in the deployment.

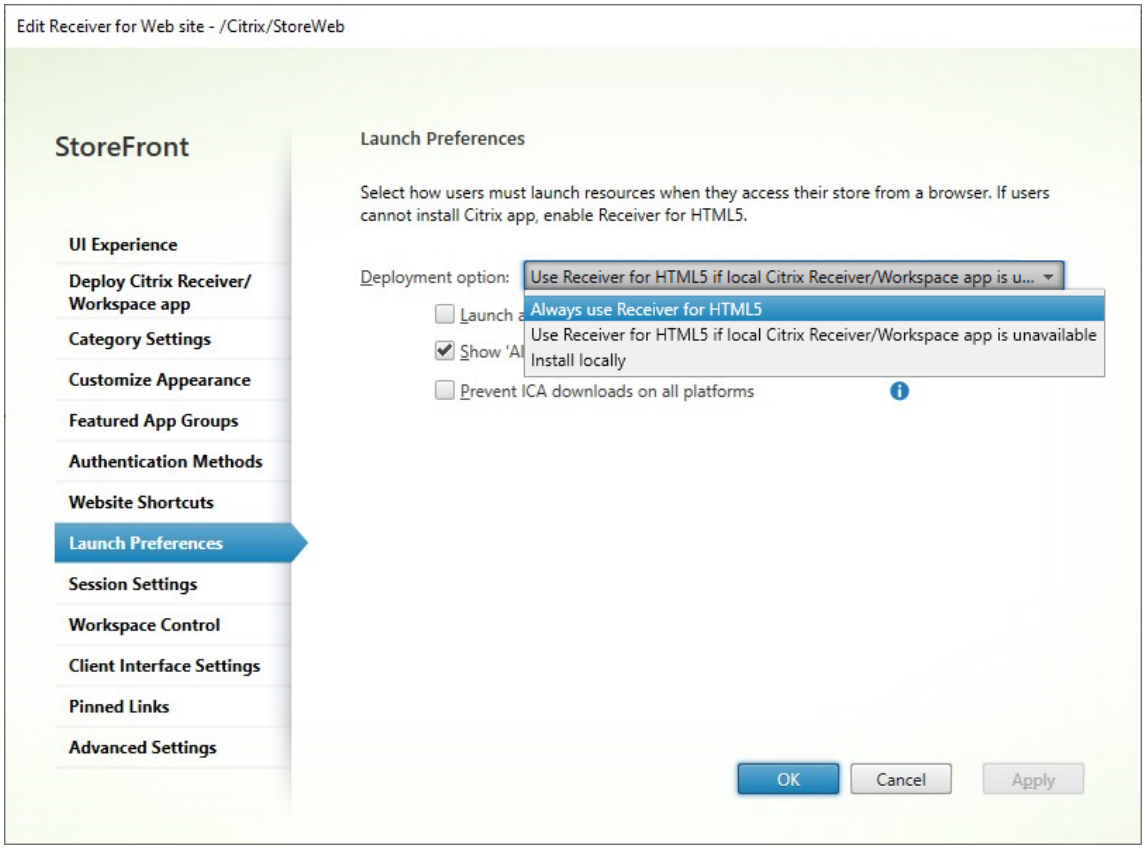
1. Deploy StoreFront and create a store aggregating the desktops and applications you want to make available to Citrix Workspace app for HTML5 users.

   A Citrix Receiver for Web site is created automatically for new stores. For more information about creating StoreFront stores, see Create or remove a store.

2. In the Citrix StoreFront management console, do the following steps:

   - On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
   - In the left pane, select **Stores** and in the **Action** pane, select **Manage Receiver for Web Sites**, and click **Configure**.
   - Select **Deploy Citrix Receiver/Citrix Workspace app**.

3. Enable Citrix Workspace app for HTML5 by selecting one of the options.



   - Select **Use Receiver for HTML5 if local Citrix Receiver/Citrix Workspace app is unavailable** option, if you want to access desktops and applications from the site using the locally

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

installed Citrix Workspace app, example, Citrix Workspace app for Windows.

If you haven't installed any Citrix Workspace app, you can access desktops and applications from the site using Citrix Workspace app for HTML5.

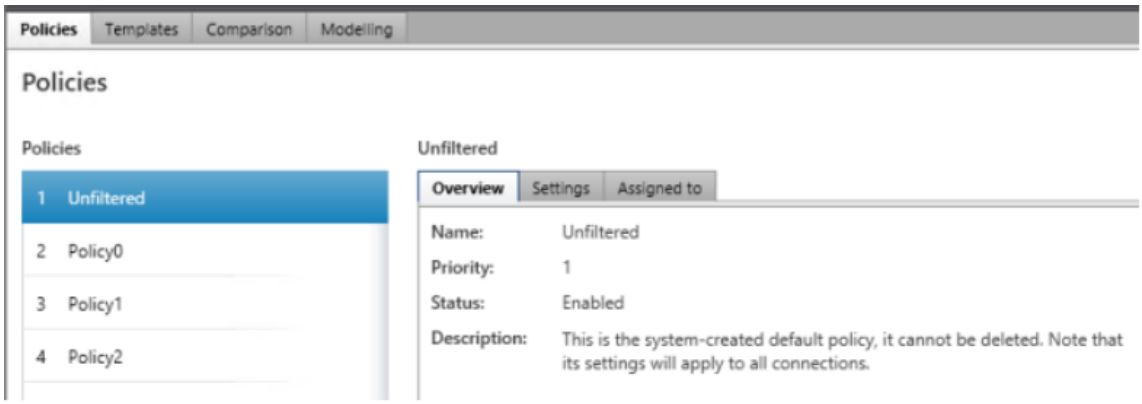
Windows and macOS users without Citrix Workspace app for HTML5 are prompted to install it every time they sign in to the site. They can use Citrix Workspace app for HTML5 if they're unable to install Citrix Workspace app.

When you select **Use Receiver for HTML5 if local Citrix Receiver/Citrix Workspace app is unavailable**, the **Change Citrix Receiver** option appears. This option allows you to switch to the light version or the local Citrix Workspace app dynamically based on the application or the desktop that you want to launch. Also, you can view the **Change Citrix Receiver** option under the Profile option.

- If you want to use Citrix Workspace app for HTML5 to access applications or desktops from Citrix Virtual Apps and Desktops, select **Always use Receiver for HTML5**.

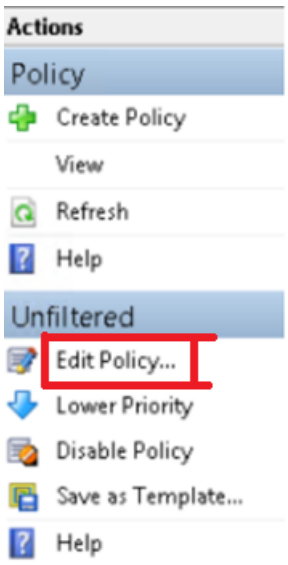
WebSocket

1. Go to the Group Policy Management Console or Citrix Studio and select **Policy** to configure the policies.
2. In the middle pane, under **Policies**, either modify an existing policy or create a policy.

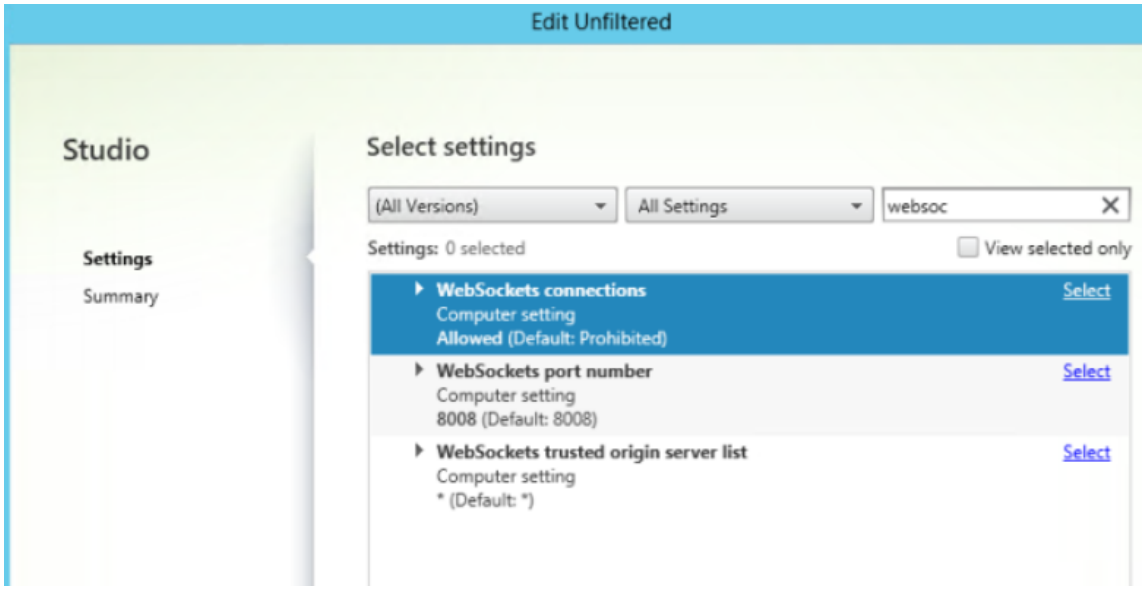


3. To edit an existing policy, in the right pane, under **Actions**, select **Edit Policy**….

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

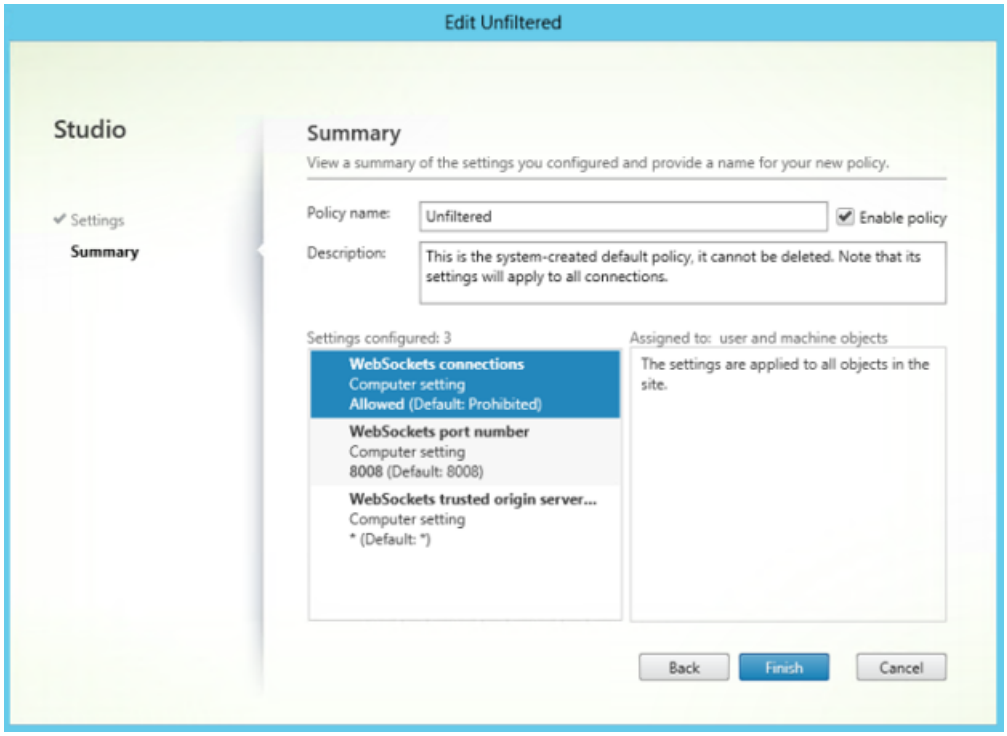


4. The **Edit Unfiltered** window appears. Type **websoc** and select **Enter**. The three WebSockets related policy settings are filtered.



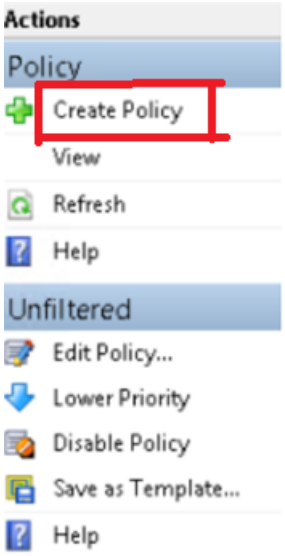
5. Click **Select** for each policy, select **Allowed**, and then click **OK**.
6. Leave the default value, select **OK**, and then click **Next**.
7. Enter a policy name or leave the default value. Verify that you select **Enable policy** and then click **Finish**.

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



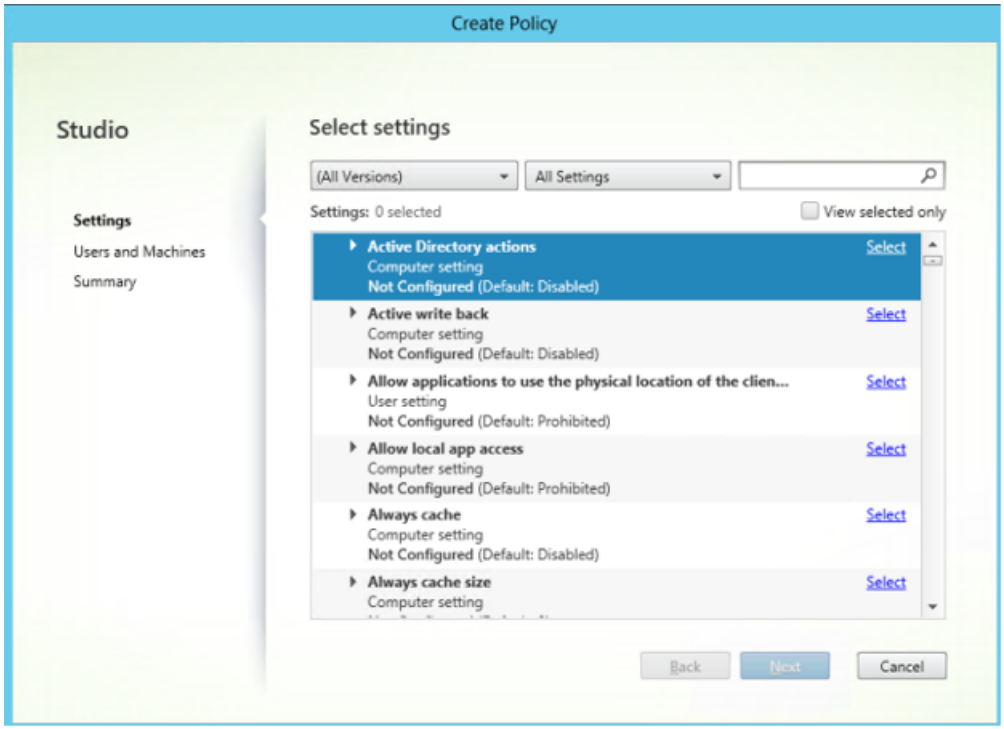
> **Note:**
>
> If you modify an existing default (unfiltered) policy, the option **Assign policy to user and machine objects** isn't available. So, we recommend you either modify an existing (not default) policy or create a policy.

8. To create a policy in Citrix Studio, under **Actions**, select **Policy** and then click **Create Policy**. The **Create Policy** window opens.

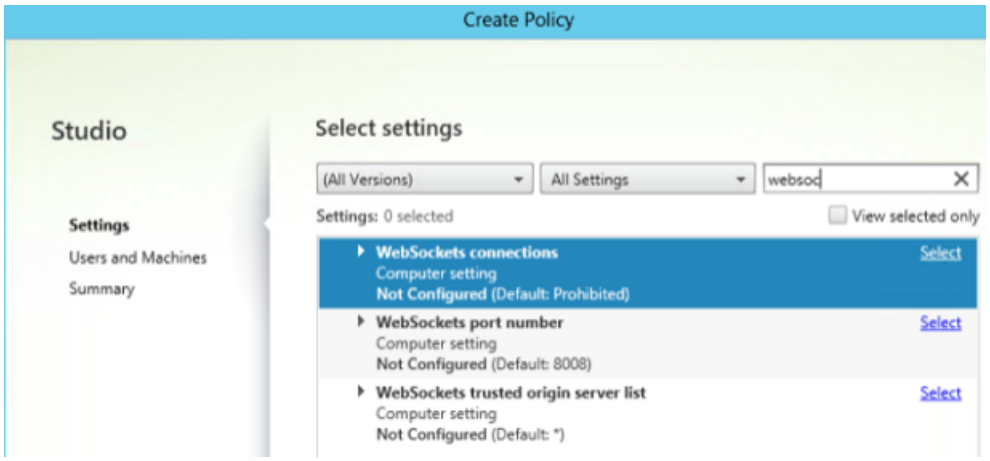


9. In the search field, type **websoc** and select **Enter**. The search filters all three WebSockets related policy settings.

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

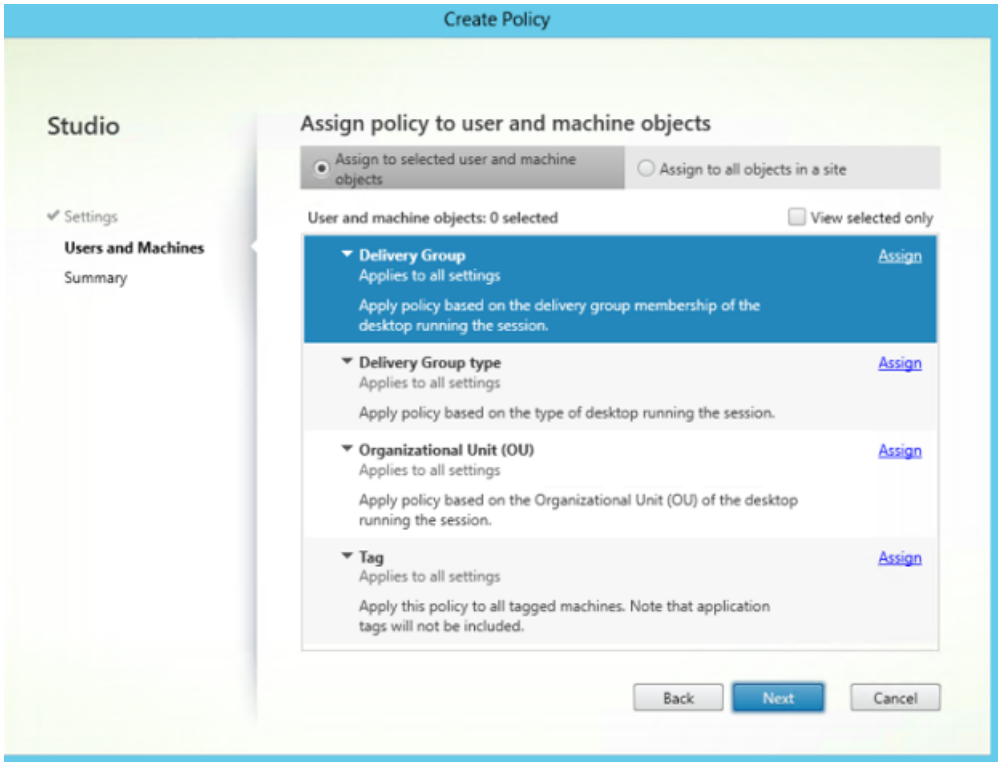


10. Click **Select** for each policy, and then select **Next**.

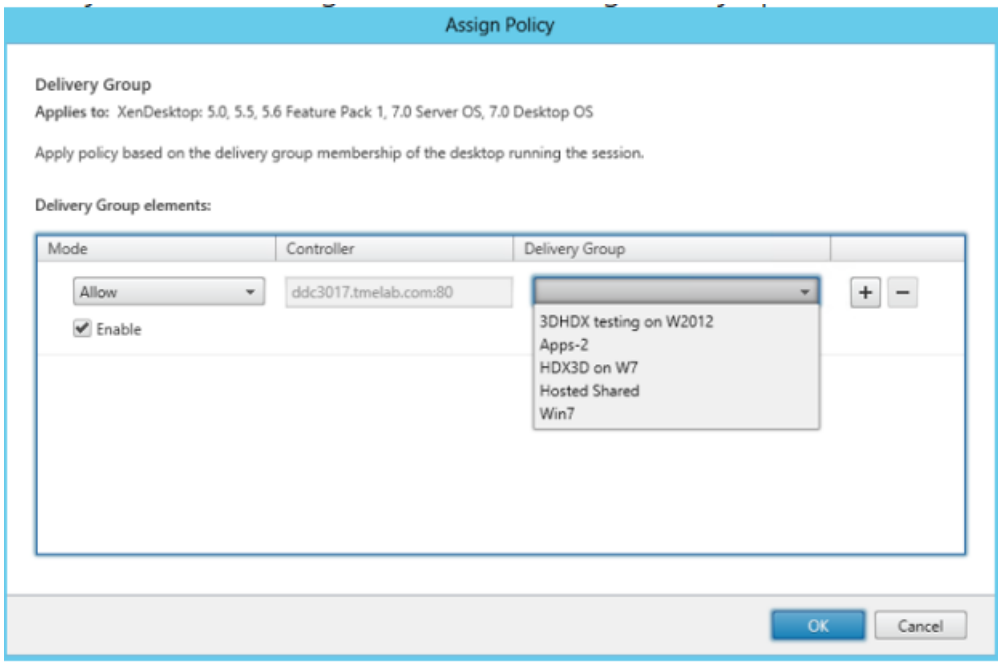


11. Assign the permission based on the Delivery Group. Select **Delivery Group** and click **Assign**.

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

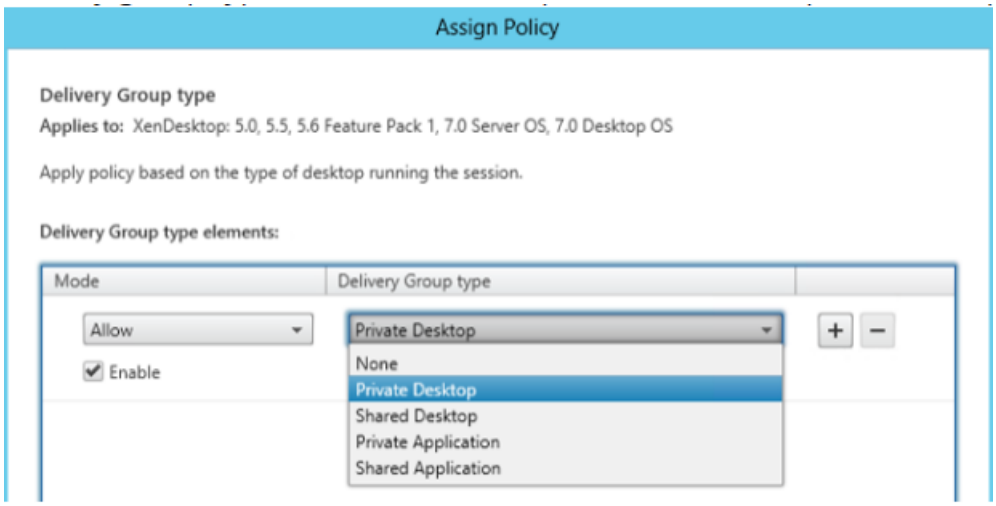


12. The **Assign Policy** window appears. Select the appropriate Delivery Group from the list and click **OK**.

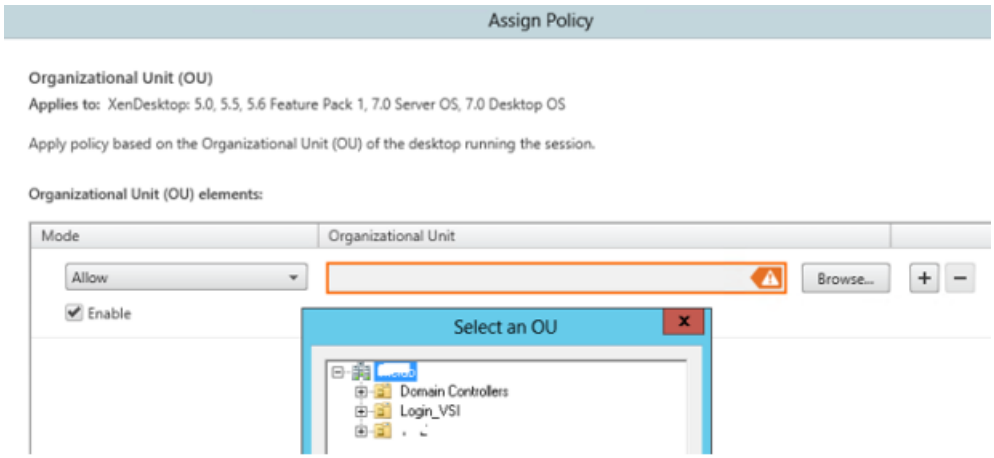


13. Select the **Delivery Group type** and click **Assign**. You can select the Delivery Group from the list.

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

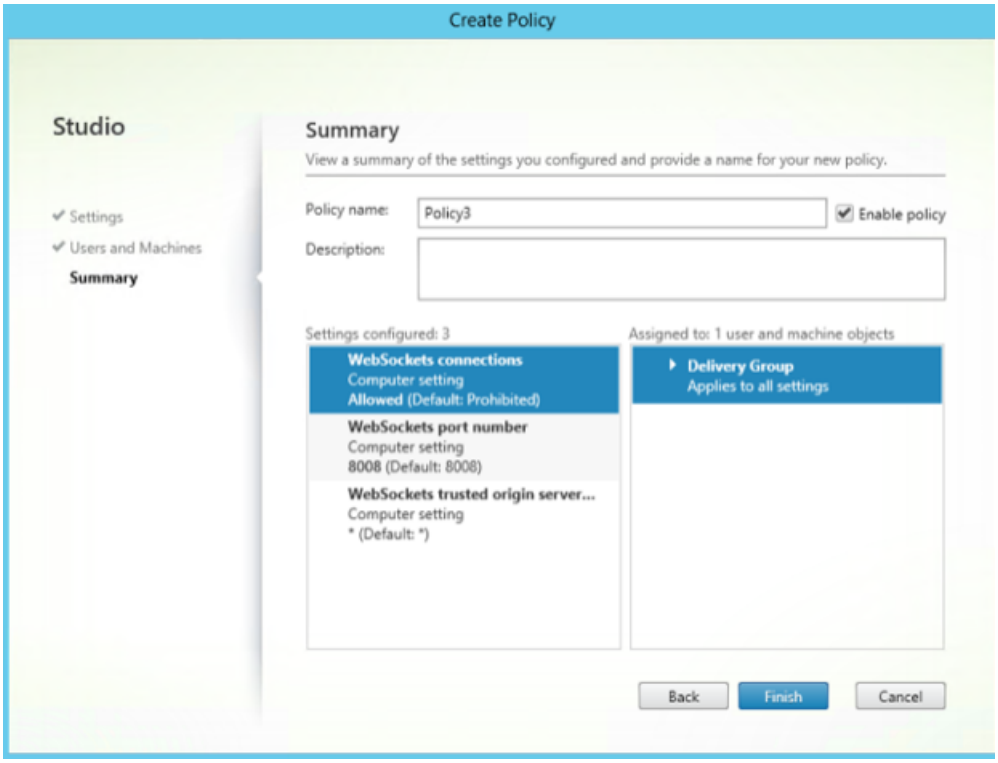


14. If you select **Organizational Unit (OU)**, you can select a specific OU from your Active Directory environment.



15. On the **Summary** window, review your policy settings, and click **Finish**.

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



16. If you changed the port used when you allowed WebSocket connections on Citrix Virtual Apps or Citrix Virtual Apps and Desktops, complete the following steps.

    To change the WebSocket port for the Citrix Workspace app for a Web site:

    a) Use a text editor to open the web.config file for the Citrix Receiver for Web site. It is in the C:\inetpub\wwwroot\Citrix\storenameWeb directory. The **storename** is the name specified for the store when it was created.

    b) Locate the following elements in the file.

    ```
    <html5 ... preferences=""... />
    ```

    c) Set the value of the preferences attribute to **wsPort:portnumber;**, where **portnumber** is the port that you configured in the policy.

To verify HTML5 by accessing the desktop and applications using a web browser

1. Log on to the StoreFront using the URL, `http://<XDControllerIPaddressorFQDN>/Citrix/StoreWeb` using domain credentials based on the permission (users/groups) in the Delivery Group. When you select **Use Receiver for HTML5 if local CItrix Receiver/Citrix Workspace app is unavailable**, a page appears. Use the light version to access HTML5.

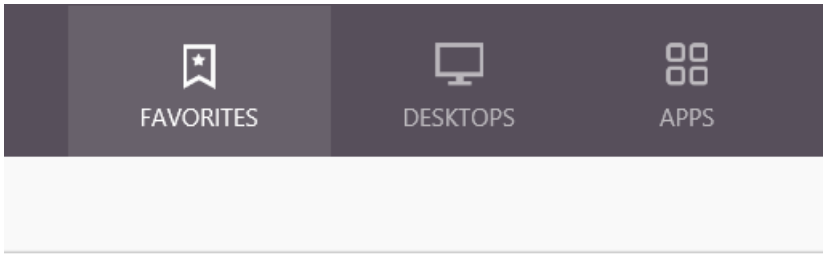
   You have the following two options:

   - Citrix Receiver™ Plug-in

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

- Receiver for HTML5

2. Click **Log On**.
3. Enter the correct User name and Password.
4. The page displays all the apps and desktops that you have access to. You can launch desktops and applications using an HTML5 browser. The desktops and applications are launched in a new tab.



To view Citrix Receiver for HTML5 logs by navigating to the log page

1. Log on to the Citrix Receiver for Web site.
   - For Citrix Workspace app 1908 for HTML5 and later, open a new tab and navigate to **siteurl/Clients/HTML5Client/src/SessionWindow.html#engineType=log**, where **siteurl** is the URL of the Citrix Receiver for Web site (`http://server.domain/Citrix/StoreWeb`).
   - For Citrix Workspace app 1907 and earlier, open a new tab and navigate to siteurl/-Clients/HTML5Client/src/ViewLog.html, where **siteurl** is the URL of the Citrix Receiver for Web site (`http://server.domain/Citrix/StoreWeb`).

Direct connections to Citrix Virtual Apps and Desktops and Citrix DaaS

Citrix Workspace app for HTML5 uses the WebSocket protocol to access virtual desktops and hosted applications. By default, WebSocket connections are prohibited on Citrix Virtual Apps and Desktops and Citrix DaaS (formerly the Citrix Virtual Apps and Desktops service).

If you enable users to access resources from the local network without connecting through Citrix Gateway, allow WebSocket connections on Citrix Virtual Apps and Desktops and Citrix DaaS.

For more information about creating HTTP profiles, see HTTP Configurations.

> **Warning:**
>
> Editing the registry 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

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

> the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Citrix Provisioning™ Services

To deploy provisioned (non-persistent) machines using Citrix Provisioning Services, create the machine catalog and delivery group on which you want to enable Citrix Workspace app for HTML5 connections. Verify that the configured WebSocket policies apply to your machine catalog.

Restart the machine to apply the WebSocket policies. For Citrix Provisioning Services-based machines that are configured to use persistent write cache files and machines deployed using MCS (that have separate identity disks), the policies are persisted when the machines restart. However, for Citrix Provisioning Services-based machine catalogs that use temporary write cache files, these policies must be applied to the *vDisk*. Otherwise, the policies aren't implemented successfully on target devices.

Complete the following steps to ensure that the policies are correctly applied to the vDisk.

1. Using the Citrix Provisioning Console, shut down a target device that is part of the machine catalog and delivery group. Change the access type of the target device from Production to Maintenance.

   For details, see Target Devices. You must use a target device that is a part of the machine catalog and delivery group. Otherwise, the policies aren't applied.

2. Create a version of your vDisk and set the Access to Maintenance. For details, see Manually updating a vDisk image.

3. Start the maintenance target device, selecting the maintenance vDisk version from the boot menu. Verify that the following keys are added to the registry.

   a) HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPolicies\AcceptWebSocketsConnections
   b) HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WebSocketsPort
   c) HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WSTrustedOriginServerList

4. Shut down the target device, change the target device access type back to Production, and promote the new vDisk version to production. Then, start the target device and restart any other target devices currently running from the existing vDisk.

If you don't use vDisk versioning, you can apply the policies to your base vDisk image. You can apply the policy by shutting down all the target devices that use the vDisk. Place the vDisk in Private Image mode, and then start the target device to update the image.

To Upgrade Citrix Workspace app for HTML5 on StoreFront

To upgrade to the new Citrix Workspace app, do the following steps on each StoreFront server:

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

- Verify the current version of Citrix Workspace app for HTML5.
- Download CitrixHTML5Client-x64.exe.
- Copy CitrixHTML5Client-x64.exe to the StoreFront machine.
- Install CitrixHTML5Client-x64.exe as an administrator to update Citrix Workspace app for HTML5.
- Refresh the StoreFront console.

Get Started

September 7, 2025

Set up

Citrix Workspace app for HTML5 integrates with Citrix Receiver for Website. To access their virtual desktops and hosted applications, users navigate to a Citrix Receiver for Website using a compatible browser that run on a supported operating system.

The user experience with Citrix Workspace app for HTML5 is as follows:

- If you did not configure the site to always use Citrix Workspace app, the site tries to determine whether Citrix Workspace app is installed locally. Installation can be on devices that run Windows and macOS. When Citrix Workspace app isn't detected, users are prompted to download and install the appropriate Citrix Workspace app for their platform. For users who are unable to install Citrix Workspace app, the issue happens every time they log on to the Citrix Receiver for Website. Users who already have Citrix Workspace app installed locally must use the same version to access resources from the site. The users aren't given the option to use Citrix Workspace app for HTML5.

  When you configure the Citrix Receiver for Website to always use Citrix Workspace app, all users must access resources from the site through Citrix Workspace app. This action is regardless of whether the user has a locally installed version of Citrix Workspace app or not.
- When users access a desktop or an application through Citrix Workspace app, the resource starts in a new browser tab or window. The action depends on the user's browser settings. You can configure Citrix Workspace app so that resources are always started in the same tab as the Citrix Receiver for Website.
- When a user starts an extra application, Citrix Workspace app for HTML5 checks whether the application can be started within an existing session before creating a session. This check enables

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

users to access many applications over a single connection so that the available resources are used more efficiently.

- Citrix Workspace app for HTML5 supports displaying titles of the applications and desktops in parentheses (for example, VDA(1) and VDA(2)) in the browser tab. To enable this feature, select **Launch applications in the same tab as Receiver for Web** in StoreFront. For more information, see Configure.

Configure

September 22, 2026

Feature flag management

Feature flags are used to enable or disable features dynamically. If an issue occurs with Citrix Workspace™ app in production, the affected feature can be disabled dynamically, even after the feature is shipped.

How to configure

No configurations are needed to enable traffic for feature management, except when a firewall or proxy is blocking outbound traffic. In such cases, you need to enable traffic using specific URLs or IP addresses, depending on your policy requirements.

> **Note:**
>
> - Once we've applied feature flags, you'll see the feature flag updates after the next launch of your Citrix Workspace app. When you're in the Incognito mode also, you'll see the updates after the next launch.

To date, for cloud customers, there's no access to StoreFront to customize Citrix Workspace app for HTML5.

Enable traffic for feature flag management For Citrix Workspace app version 2409 and later:

To ensure optimal functionality and access to preview features, you need to enable traffic to the URL `features.netscalergateway.net`.

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

Known issues and workaround If you can't upgrade to Citrix Workspace app for HTML5 2409 or later and experience inconsistencies with the following feature in versions older than 2409, set the recommended configuration values as follows:

- When you start an app session, a white bar might appear inside the session. As a workaround, disable the Enhanced app switcher support feature. For more information about the configuration, see Enhanced app switcher support. [CVADHELP-18625]
- When you use Citrix Workspace app for HTML5 versions 2308 or 2309 with the F5 Load Balancer, sessions intermittently fail to start or become unresponsive. The issue occurs after the feature flag management is deprecated for versions before 2409. As a workaround:

  1. Navigate to `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` in the StoreFront server and locate `configuration.js` file.
  2. Navigate to the end of the file and paste the following:

```
//Script to disable CGP WASM
Object.defineProperty(globalThis["HTML5_CONFIG"]["transport"],
    'wasmCgpEnabled', {

get() {

    return false;
     }
 ,
set(value) {

     }
 ,
configurable: true,
enumerable: true,
 }
 );
```

  3. Click Save. [RFHTMCRM-14936]

- In a multi-monitor setup, typing characters on the second screen of ChromeOS devices causes the keyboard to send double strokes. For example, pressing 't' results in 'tt.'[CVADHELP-27464]

  As a workaround:

  Upgrade Citrix Workspace app for HTML5 to version 2409 or later, and ensure that traffic is allowed to the URL `features.netscalergateway.net`. If upgrading isn't possible, disable the IME multi-monitor feature in the configuration settings:

```
'features' : {

    'ime': {

```

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

```
            'multiMonitor' : false
             }

    }
```

Global App Configuration service

Administrators can customize user settings for sessions that are launched in Citrix Workspace app by using the Global App Configuration service. Administrators can customize user settings for on-premises and Workspace (Cloud) deployments.

Previously, administrators could only use the **configuration.js** for this purpose, and it was applicable only for StoreFront users.

Limitation in the feature

- Global App Config service settings might not work as expected if you've installed the AdBlock extension on the browser. [CVADHELP-23003]
- Custom domain URLs feature doesn't adhere to the Global App Configuration service (GACS) settings.

How to configure

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

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

> **Notes:**
>
> - This feature is available for workspace and HTTPS-based stores only.
> - For the Global App Configuration service to work, verify that your users can access the URL .

Clipboard

Before introducing this feature, Citrix Workspace app did not support copying and pasting HTML-formatted text from a local application to another application using the Paste Special feature. As a result, the targeted app (in this case, Microsoft Excel) wouldn't keep its HTML formatting characteristics.

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

Citrix Workspace app for HTML5 supports HTML format in addition to plain text between the client and a session. This support is useful for Office apps and browsers. Enhanced clipboard support is available on Chrome and Safari browsers only. You can copy HTML content and keep formatting. When copying a link in Chrome, a <img> tag is added in HTML format, which effectively allows you to copy images and text. This HTML formatting feature is richer than plain text but doesn't work in all applications.

For more information, see Client clipboard redirection in the Citrix Virtual Apps and Desktops documentation.

Enhanced clipboard experience

You can copy and paste text between the session and the end user's device. You can do it when you launch multiple Virtual Desktops hosted applications or desktops on Windows, Mac, or Chrome operating systems using the browser based Citrix Workspace app for HTML5.

With this feature, you can use the **Ctrl C** and **Ctrl V** hotkeys (for Windows or Chrome operating systems) and **CMD C** and **CMD V** hotkeys (for Mac operating system) to copy and paste.

This feature is enabled by default.

On Firefox and Edge browsers, to copy the text from a remote session to a local device, press **Ctrl C** and then click **Confirm**.

Disable the copy confirmation dialog by selecting the **Disable Copy Confirmation** checkbox in **Preferences** on the toolbar. Clear the checkbox to enable the option again.

To disable the enhanced clipboard experience

To disable this feature, edit the **configuration.js** file located inside the **HTML5Client** folder (`C:\Program Files\Citrix\Receiver StoreFront\HTML5Client`) and set the value of **directClipboard** to **false**.

Known limitations in the feature

- You can copy and paste only HTML, plain text, images, but not files.
- This feature doesn't support large data.
- The **Ctrl** key might remain stuck in the down position. This issue occurs when you press the right **Ctrl** key for a long time and then press **C** to copy the text. As a workaround, click the right **Ctrl** key multiple times.
- Occasionally, copying text requires an extra click through the **Copy** confirmation dialog when you use Google Chrome, Safari, Edge, and Firefox browsers.

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

- Use the **Ctrl c** or **CMD C** and **Ctrl V** or **CMD V** keys to copy and paste. Occasionally, using the **Edit** menu or right-click option to copy the text might require an extra click using the **Confirm** dialog.
- The right-click functionality works only when you copy and paste from your virtual desktop and app sessions to your local device. It doesn't work when you copy and paste from the local device to your virtual desktop and app sessions.

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
- Adobe Photoshop

Previously, this functionality was available only for text for the Google Chrome browser and the Microsoft Edge (Chromium) browser with HTTPS stores. This functionality is now available for text and images. It's applicable on the Google Chrome browser and the Microsoft Edge (Chromium) browser with HTTPS stores.

	Supported clipboard actions
Google Chrome browser and Microsoft Edge (Chromium) browser with HTTPS stores	Image clip copy and paste support. Text copy and paste support
Mozilla Firefox, HTTP stores	Text copy and paste support

> **Notes:**
>
> - In general, for security reasons, we recommend you use only HTTPS-based stores.
> - Due to network bandwidth constraints, sessions might become unresponsive when you try to copy and paste an image clip larger than 2 MB.
> - In Microsoft Windows OS and ChromeOS devices, use Ctrl + C and Ctrl + V for copy and paste. In Apple Mac devices, use Command + C and Command + V for copy and paste.
> - The right-click functionality works only when you copy and paste from your virtual desktop and app sessions to your local device. It doesn't work when you copy and paste from the local device to your virtual desktop and app sessions.
> - We've tested this feature with BMP, PNG, JPEG, and GIF formats.

Clipboard supports HTML format You can use HTML format for clipboard operations between the virtual desktop and the endpoint device. When you copy the HTML data, the source content format

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

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.

Switch apps

This feature enables an end user to switch between many published apps in the same session. When you open or close an app, the app count updates accordingly. If some apps are opened in another session, the app count includes all the opened ones.

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

How to use

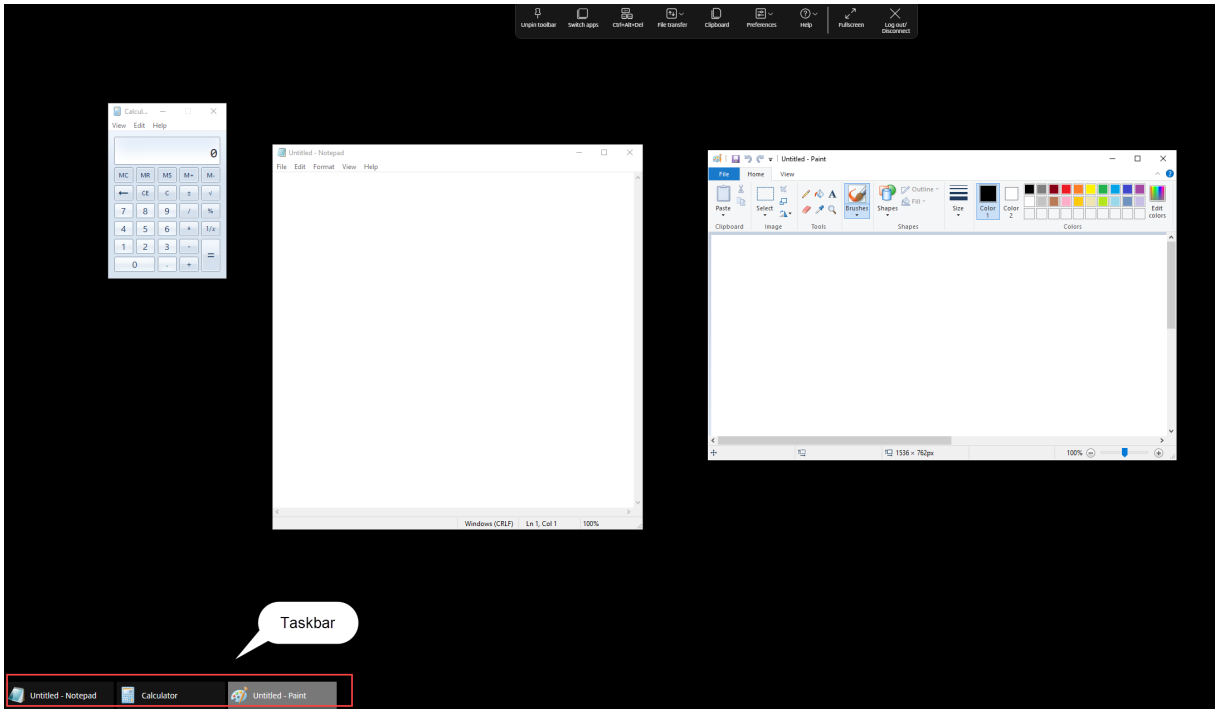
You can effortlessly switch between applications in a browser tab by using the switch app functionality. This feature has two modes:

- Taskbar mode
- Grid-view mode

Taskbar mode

This mode optimizes sessions running on larger screens like laptops and desktops. For apps launched from the same VDA, the taskbar allows easy navigation between the apps.

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



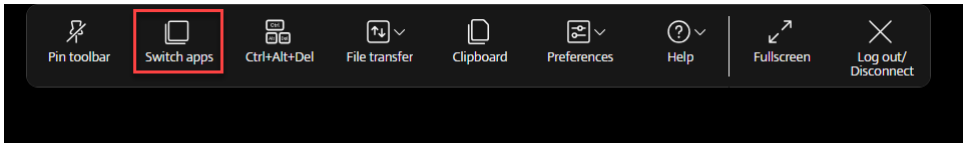
The taskbar shows all the apps currently active in the session, allowing users to switch between them easily. In the right-click menu of the app switcher, users have two preference options that are remembered for the next launch.

- Auto-hide: The app switcher automatically hides the taskbar when not in use and reappears when the user hovers the mouse pointer at the bottom of the screen.
- Show icons only: Only the icons of the apps are displayed, with their titles hidden.



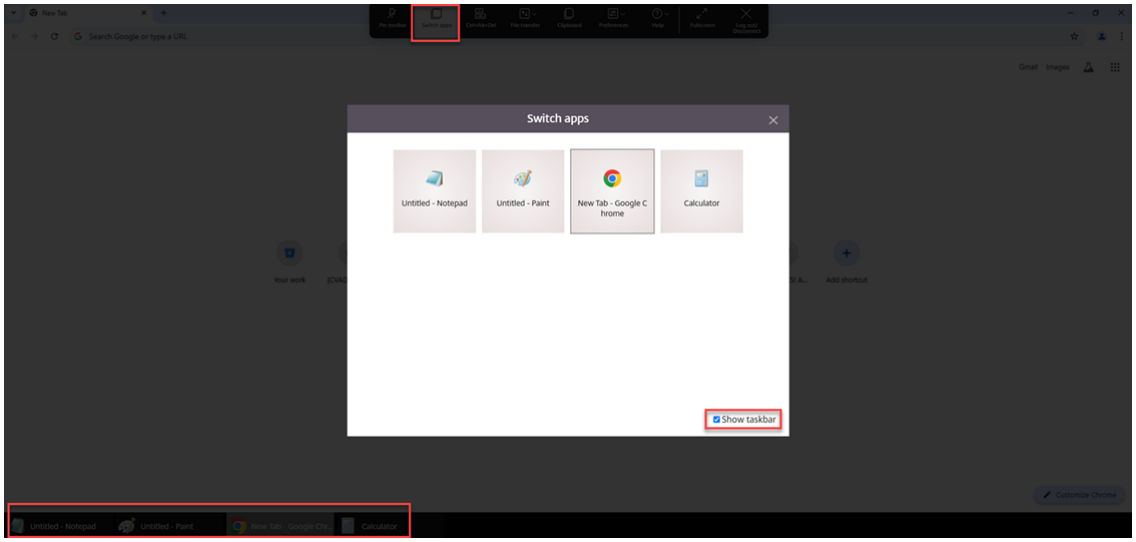
Grid-view mode

This mode optimizes the sessions running on mobile or touch devices. To bring the grid into view, touch or tap the **Switch apps** icon in the toolbar.



The grid view displays apps that are launched from the same VDA, providing users on mobile devices with a clearer and larger view compared to the regular taskbar. Also, there is an option to enable or disable the app switcher taskbar, allowing users to adjust the viewport size as needed.

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



Enhanced app switcher support

When you launch a published application session in full-screen or kiosk mode, the session doesn't overlap with the desktop taskbar. The app switcher no longer hides the session. This enhancement is supported only in single-monitor mode.

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

How to configure

You can disable the feature in the following ways:

- Configuration.js
- Global App Configuration service

Configuration.js In Citrix Workspace app for HTML5, the `configuration.js` file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

> **Notes:**
>
> - Citrix recommends that you back up the `configuration.js` file before modifying it.
> - Administrator-level credentials are required to edit the `configuration.js` file.

To disable the feature:

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

1. Navigate to the `configuration.js` file in the `HTML5Client` folder.
2. Add the `enhancedAppswitcher` attribute and set the attribute to **`false`**. For example:

```
'ui': {

    'appSwitcher': {

        'enhancedAppSwitcher': false
     }

 }
```

> **Note:**
>
> The `configuration.js` file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder on the StoreFront machine.

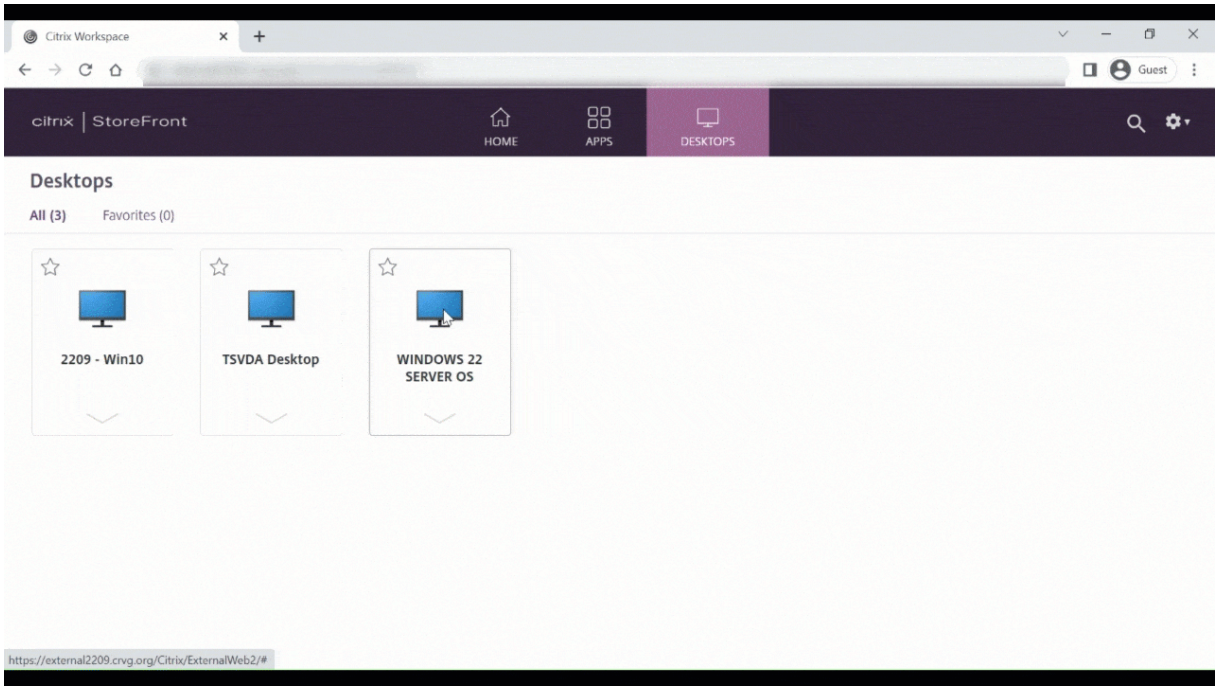
Global App Configuration service On the cloud setup, administrators can disable the enhanced switch apps feature by setting the **Enhanced App Switcher Support** attribute to **False**.

Improved virtual apps and desktops launch experience

Starting with the 2306 release, the improved app and desktop launch experience provide timely and relevant information about the launch status.

> **Note:**
>
> Administrators must upgrade HDX SDK files to use Citrix Workspace app for HTML5 2306 version. The older HDX SDK files are incompatible with the 2306 version and later. To download the latest HDX SDK files, click here. For more information, see the Citrix Workspace app for HTML5 HDX SDK developer docs.

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

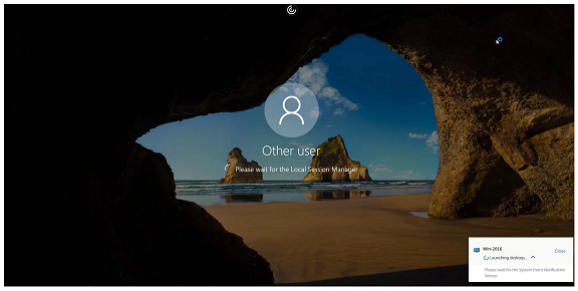


Configure session launch notification display

Starting with 2307, administrators can enable or disable the display of launch progress notifications using the following configuration. If this configuration is enabled, you see the session launch progress notifications on the lower right of the screen. If this configuration is disabled, you can't see the session launch progress notifications.

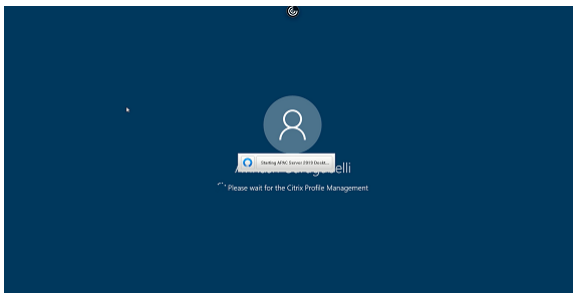
> **Note:**
>
> - By default, this configuration is enabled.

The following screenshot appears when notifications are enabled.



The following screenshot appears when notifications are disabled.

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



How to configure You can configure this feature in the following way:

In Citrix Workspace app for HTML5, the **configuration.js** file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the feature, do the following:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **CTXTUI** attribute and set the attribute to **false**.

   The following is an example of JSON data:

   ```
   {

    "vc_channel": {

    "CTXTUI": false
      }

    }
   ```

3. Save the changes.

Configuration for blocking Global App Configuration service (GACS) requests

With the 2509 version, administrators can block Global App Configuration service (GACS) requests using configuration.js for on-prem stores. The attribute name is **disableGACS**. When you set this attribute to **true**, Citrix Workspace app doesn't connect to any GACS endpoints.

> **Note:**
>
> The attribute **disableGACS** is set as **false** by default.

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

How to configure

> **Notes:**
>
> - Citrix recommends you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.
> - The **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder.

To set **disableGACS** to **true** using configuration.js:

1. Navigate to the **configuration.js** file.
2. Add the **disableGACS** setting and set the **disableGACS** attribute to **true**.

   The following is an example of JSON data:

```
{

  "thirdPartyServices": {

        "disableGACS": true
           }

 }
```

3. Save the changes.

Configuration for blocking feature flag requests

With the 2509 version, administrators can block feature flag requests using configuration.js for on-prem stores. The attribute name is **disableFeatureFlag**. When you set this attribute to **true**, Citrix Workspace app doesn't connect to any feature flag endpoints.

> **Note:**
>
> The attribute **disableFeatureFlag** is set as **false** by default.

How to configure

> **Notes:**
>
> - Citrix recommends you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.

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

> - The **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder.

To set **disableFeatureFlag** to **true** using configuration.js:

1. Navigate to the **configuration.js** file.
2. Add the **disableFeatureFlag** setting and set the **disableFeatureFlag** attribute to **true**.

   The following is an example of JSON data:

```
{

  "thirdPartyServices": {

        "disableFeatureFlag": true
           }

 }
```

3. Save the changes.

Customer Experience Improvement Program (CEIP)

May 7, 2026

The Citrix Customer Experience Improvement Program (CEIP) collects configuration and usage data from the Citrix Workspace™ app and automatically sends it to Citrix Analytics. This data enables Citrix to analyze the performance and enhance the quality, functionality, and performance of the Citrix Workspace app, optimize resource allocation for product development, and support service levels through effective staffing and infrastructure investment.

All data is used and analyzed solely in aggregate form, ensuring that no individual user or device is singled out or specifically analyzed. Citrix does not collect any Personally Identifiable Information (PII) through CEIP, and all data collection is in accordance with relevant industry data privacy and security standards.

Tools used to gather CEIP Data

Citrix Workspace app for HTML5 uses Citrix Analytics to collect the CEIP data. You can either disable or block CEIP data.

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

Data collected

Data Collected	Description	What we Use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app for HTML5 and automatically sends the data to Citrix Analytics.	This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app.

Additional Information

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

CEIP data to Citrix Analytics

End users can:

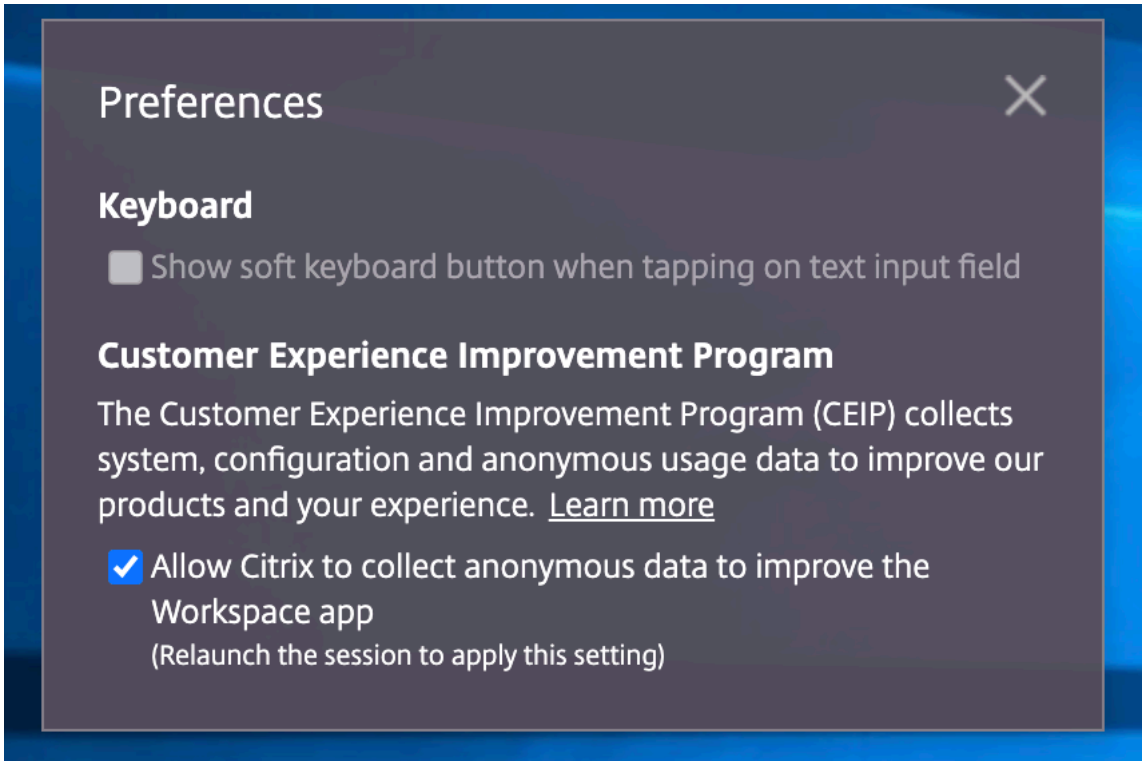
- decide whether to send the usage data to Citrix Analytics or not
- block CEIP through GUI

To disable CEIP using GUI

> **Note:**
>
> You can modify the CEIP settings using the GUI only when the administrator has enabled it using `configuration.js`.

1. Open Citrix Workspace app for HTML5.
2. From the toolbar, select **Preferences**.

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



3. Clear **Allow Citrix to collect anonymous data to improve the Workspace app**.

> **Note:**
>
> Relaunch the session for the changes to take effect.

Admins can:

- disable sending the CEIP usage data using configuration.js
- block CEIP through GUI
- block CEIP through configuration.js

To disable CEIP using configuration.js

> **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.

In Citrix Workspace app for HTML5, the `configuration.js` file is in the **HTML5Client** folder. Edit this file to configure Citrix Workspace app for HTML5.

Set the **enabled** attribute under **analytics** to **false** in the `configuration.js` file.

```
1 'analytics':{
```

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

```
2
3       'enabled':false,
4   }
```

Blocking CEIP

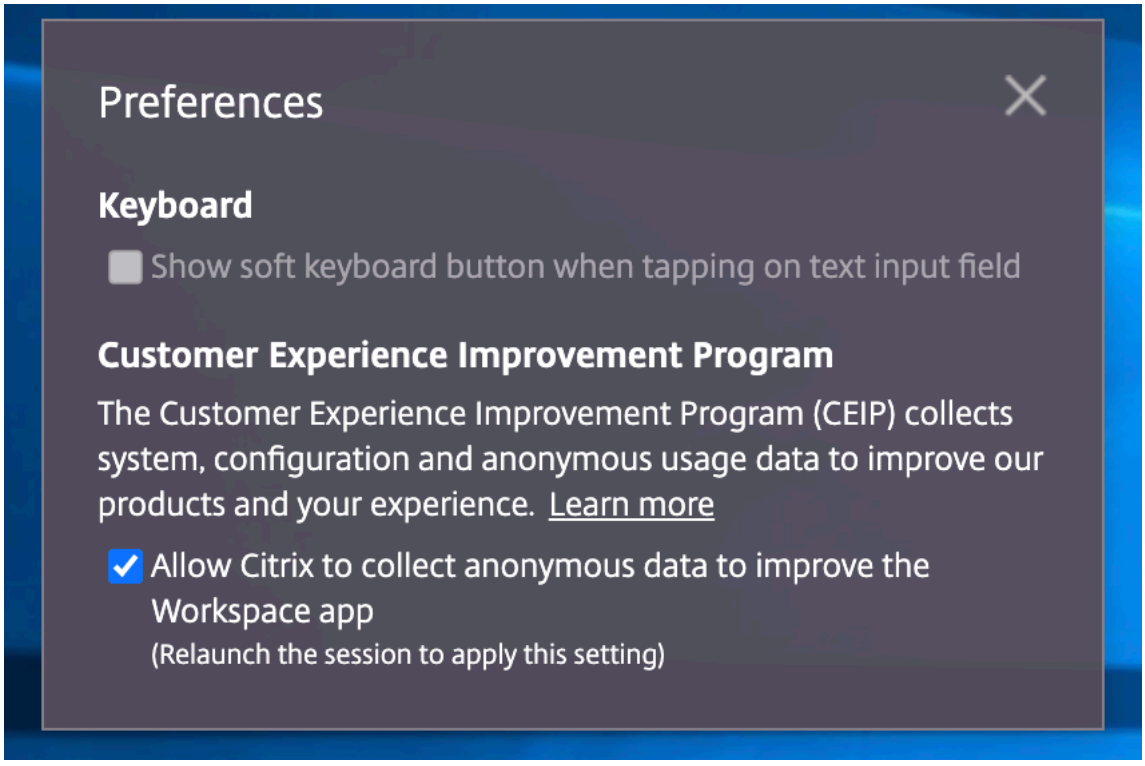
Administrators are allowed to block CEIP through the following:

- Block CEIP using GUI
- Block CEIP using `configuration.js` file

To block CEIP using GUI

> **Note:**
>
> You can modify the CEIP settings using the GUI only when the administrator has enabled it using `configuration.js`.

1. Open Citrix Workspace app for HTML5.
2. From the toolbar, select **Preferences**.



3. Clear **Allow Citrix to collect anonymous data to improve the Workspace app**.

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

> **Notes:**
>
> - Relaunch the session for the changes to take effect.
> - Blocking CEIP using GUI configuration takes precedence over the configuration made through the **configuration.js** file. Thus, CEIP data isn't sent to Citrix.

To block CEIP using the configuration.js file Open the `configuration.js` file, add the **connectionEnabled** attribute, and set the attribute to **false**:

```
'analytics':{

    'connectionEnabled':false,
              }
```

Specific CEIP data

The specific CEIP data elements collected by Citrix Analytics are:

Citrix Workspace app version	Session mode (Kiosk, Public/General)	Session type (desktop/application)	XenDesktop information (Delivery Controller and VDA versions)
Launch type (SDK/I-CAFile/FTA/Store and so on)	Time zone of the session	Language of the session	Client keyboard layout
Network socket type (HTTPS/HTTP)	Feature usage (clipboard, file transfer, app switcher, printing, USB, smart card, and so on)	Device pixel ratio	Microsoft Teams usage
Reconnection timeout	Multi-Monitor	Global App Configuration service	New toolbar usage
PID/VID of the USB devices	Audio/Webcam device names		

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

Peripherals

March 5, 2025

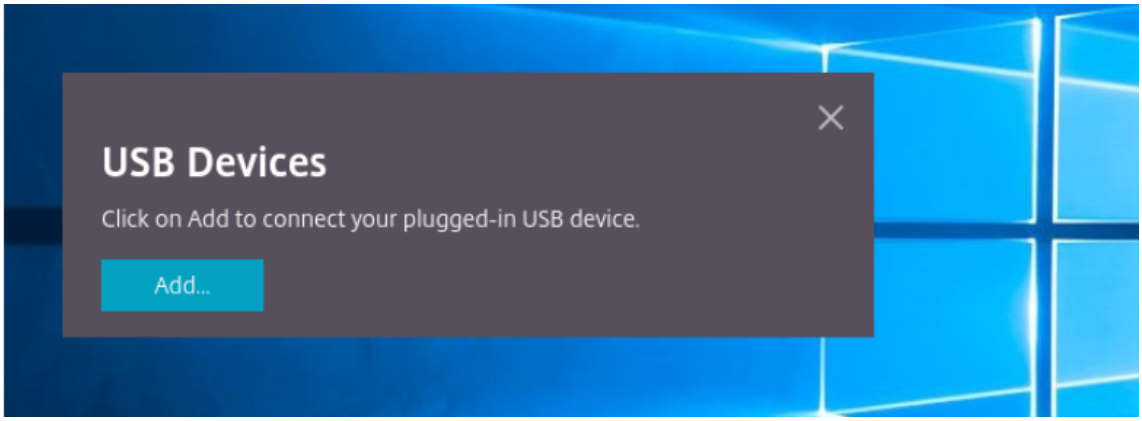
USB device redirection

Generic USB device redirection is supported on Chrome browsers (Version 61 and later) running on Chrome, Mac, and Linux operating systems. This feature is supported on sessions launched over secure HTTPS connections. This feature supports redirection of two USB devices simultaneously.

1. **Redirecting a USB device** As a prerequisite, enable the USB redirection policy on the server. For more information, see Enabling USB redirection on the server.
2. Connect the USB device to the machine.
3. Click the **USB Devices** icon available on the in-session toolbar.

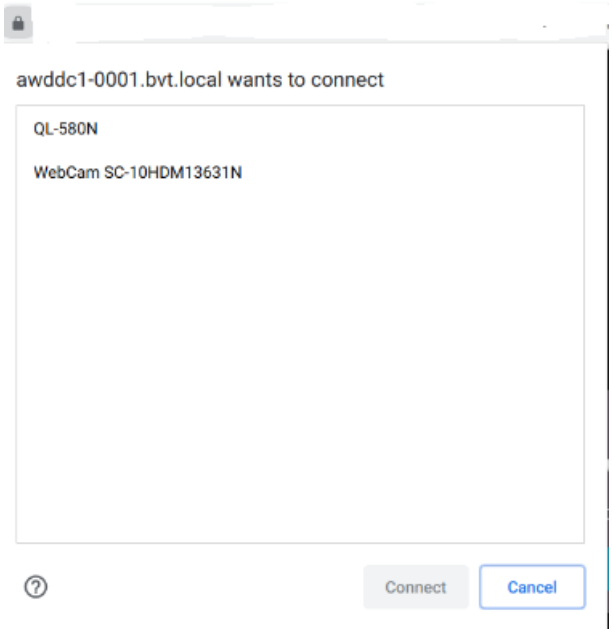


4. In the **USB Devices** dialog box, click **Add**.



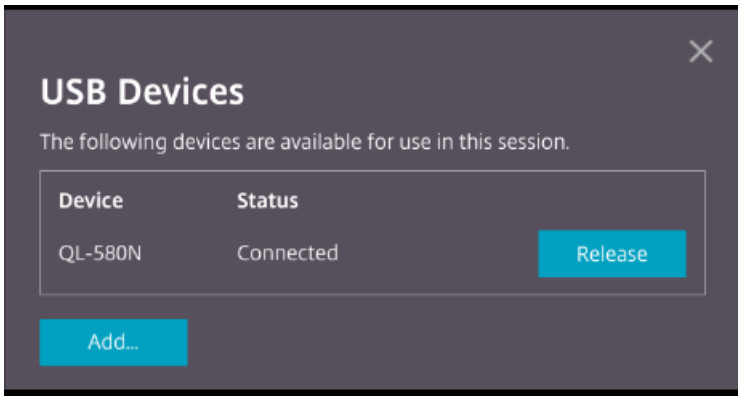
This action opens a Chrome dialog box that displays a list of devices.

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

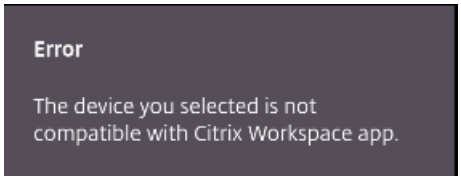


> **Note:**
>
> The Chrome dialog box displays USB devices that might not always be redirected through Citrix Workspace app for HTML5. The USB devices that can be redirected through Citrix Workspace app for HTML5 are displayed in the USB devices dialog box within the app.

5. Select the devices to be redirected and then click **Connect**. After successful redirection, you're returned to the **USB Devices** dialog box, and the device appears as **Connected**.

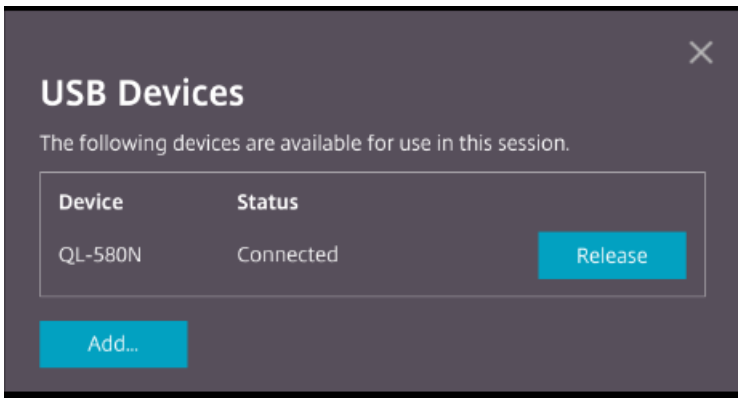


6. When you try to redirect a USB device that is not supported by Citrix Workspace app, the following error message appears.

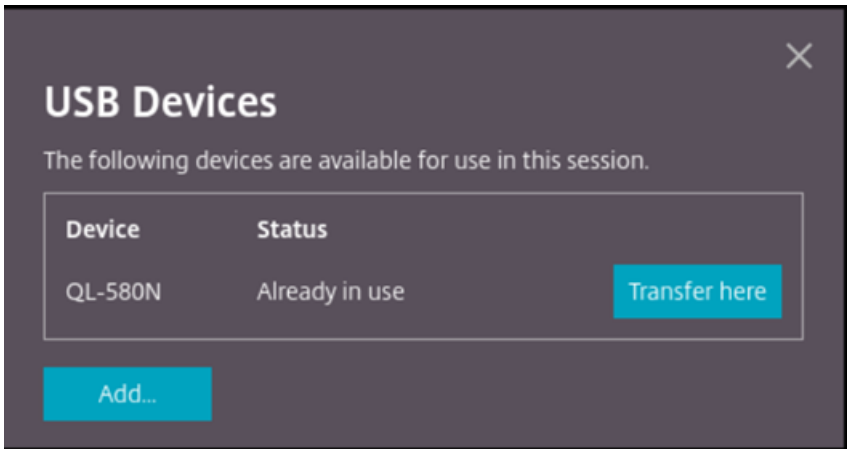


7. Click **Release** to release a device from the remote session.

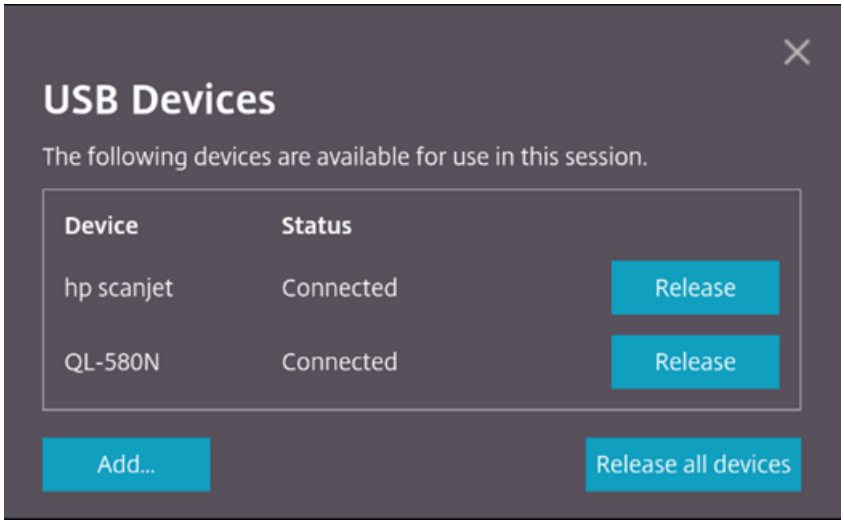
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. If you launch more than one session, USB devices that are connected inside a different session show as **Already in use**. Click **Transfer here** to transfer the devices to the current session.

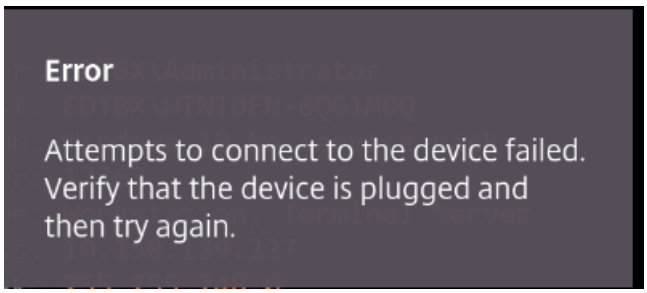


9. When you redirect more than one USB device to a session, click **Release all devices** to remove the devices from the session.



10. When you disconnect a redirected USB device from the machine without clicking **Release**, the following error message appears.

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



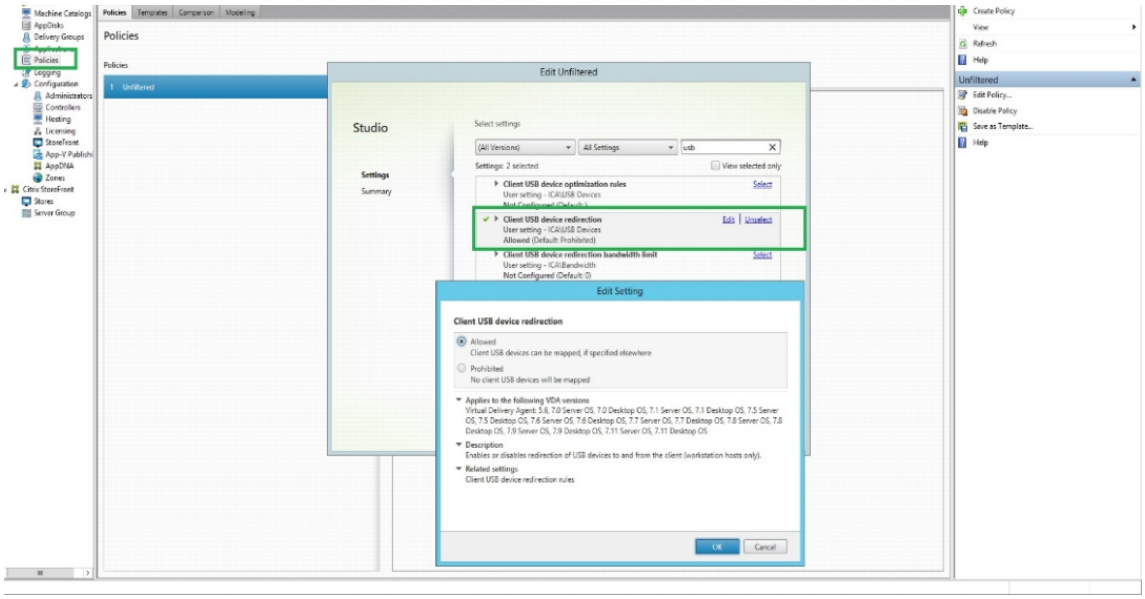
The USB device redirection feature is applicable only to USB devices, where the client operating systems such as macOS and Chrome don't load the device drivers by default. For example, the feature is relevant to the Brother QL-580N Label Printer.

In case you're unable to redirect USB devices on a Linux operating system, try setting up the user accounts and provide permissions to open the USB devices. For more information, see Google developers' document.

Enabling USB redirection on the server

Do the following to enable the USB device redirection on the server:

- Enable the policy for USB device redirection on the **Domain Controller**.



Configuring USB redirection for Citrix HTML5 client

By default, the USB device redirection feature is enabled on the client if the USB device redirection policy is enabled on the server.

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

To disable it, edit the configuration.js file and set the value of **usb** under **toolbar** to **false**. This setting is applicable to the StoreFront. The configuration.js file is in C:\program Files\Citrix **actual path**\HTML5Client.

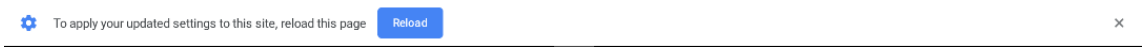
```
    'ui' : {

        'toolbar' : {

                'usb' : false
         }
,
     }
```

Behavior of Chrome browser

- When you click the padlock icon, the browser tab shows the Secure Connection dialog box. You can see the USB devices for which the browser tab has received user permission. Although there are multiple USB devices, only the devices that the Citrix HTML5 client can redirect appear in the Citrix **USB Devices** dialog box. Those devices can be used inside a remote session.
- If you want to revoke access permissions granted to the browser tab, click the x icon next to the USB device. As a result, the **Reload** button appears. If you click **Reload**, the session closes. Relaunch the session for the changes to take effect.



Known limitations in the feature

- The USB device redirection feature applies to virtual sessions initiated from the Google Chrome browser on a ChromeOS device. However, USB redirection doesn't work in virtual sessions launched from browsers on Windows OS, macOS, and other operating systems.
- Only USB Type A devices can be redirected to the session. But, you can connect Type A devices through a Type C connector.
- Releasing a USB hub device might not result in releasing connected **USB Type A** devices.
- Redirection of HID devices, Mass Storage devices, and Web cameras might result in low performance. The audio and video functionality might not perform as expected, exhibiting delays or glitchy displays. It is recommended to use the corresponding optimized virtual channel (VC), for example, CDM for accessing Mass Storage devices.
- This feature has been tested and is supported on VDAs running on Windows 10.
- This feature has been tested for up to two USB devices simultaneously.

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

File handling

September 7, 2025

File Transfer

By default, users can:

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

Administrators can selectively enable or disable file transfer, uploads, or downloads through policies in Citrix Studio.

Citrix Workspace app for HTML5 supports downloading files on a MacBook using the Safari browser.

Requirements

- XenApp and 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

Known limitations in the feature

- 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.

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

File Transfer policies

By default, file transfer is enabled. Use Citrix Studio to change these policies, located under **User Setting > ICA\File Redirection**. Consider the following when using file transfer policies:

- **File transfer for Citrix Workspace app for ChromeOS/HTML5**: Allows or prevents end users to transfer files between *Citrix Virtual Apps and Desktops* session and the end user's device.

  Allows or prevents end users to transfer files between *Citrix DaaS* session and the end user's device.
- **Upload file for Citrix Workspace app for ChromeOS/HTML5**: Allows or prevents users from uploading files. It can be from the user's device to a *Citrix Virtual Apps and Desktops* session or *Citrix DaaS* session.
- **Download file for Citrix Workspace app for ChromeOS/HTML5**: Allows or prevents users from downloading files. It can be from a *Citrix Virtual Apps and Desktops* session or *Citrix DaaS* session to the user's device.

Client Drive Mapping

Starting with the 2303 version, the Client Drive Mapping (CDM) feature supports folder mapping on the local machine so they're accessible from within a session. You can map any folder from the local machine, if the folder doesn't contain system files.

The end user can do the following operations:

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

This feature provides the advantage of accessing both virtual desktop drives and local machine drives together in the file explorer within the HDX™ session. This feature is supported on desktop platforms, Google Chrome, and Microsoft Edge Chromium browsers only.

> **Note:**
>
> - By default, this feature is enabled.
> - Cloud-based drives, for example, OneDrive and Google Drive can be mapped provided it's supported by the cloud provider.

Known limitations in the feature

- You can't rename files and folders inside the mapped drive.

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

- Mappings will only have the name of the folder and not the full path.
- If your local folder has hidden files, and you mapped the same folder, the hidden files are visible inside the session in the mapped drive.
- You can't change the file property to read-only access in the mapped drive.
- When you map a folder from the removable device and if you remove the device during an active session, you can't use the mapped drive inside the session. You must remove the mapping manually.

Known issues in the feature

- When you use the CDM feature on mobile platforms, the dialog box gets truncated from the top.

How to configure

You can configure the CDM feature in the following way:

- Configuration.js

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

Configuration.js The **configuration.js** file is located in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the CDM feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the feature:

1. Locate and edit the **configuration.js** file in the **HTML5Client** folder.
2. Add the **clientDriveMapping** attribute and set the attribute **enabled** to **false**. For example,

```
1  `features':
2      {
3
4        'clientDriveMapping' :
5          {
6
```

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

```
        'enabled' : false,
            'availableAccessLevels': [1, 2, 3],
             // 1 - Read-Write Access, 2 - Read-Only Access, 3 -
                No-Access
            //drop-down options
           'accessLevel': 1
            // 1 - Read-Write Access, 2 - Read-Only Access, 3 - No
               -Access
            //admin sets these values
         }

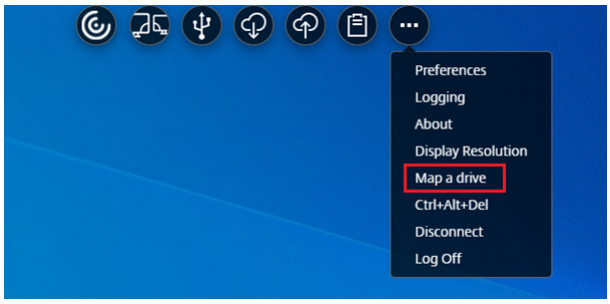
    }
```

3. Save the changes.

Access level When you enable the feature, you can set the folder or drive access levels. For example, if an administrator sets **availableAccessLevels** as **[2, 3]**, the end user can view the **Read-Only Access** and **No-Access** options in the drop-down list.

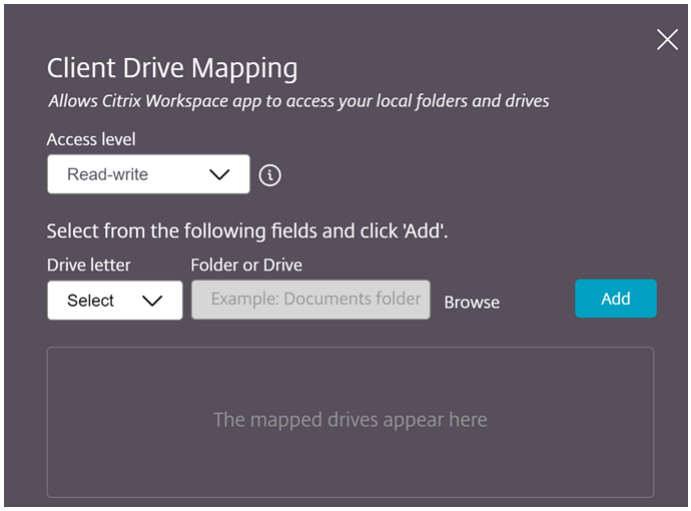
How to use the feature

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

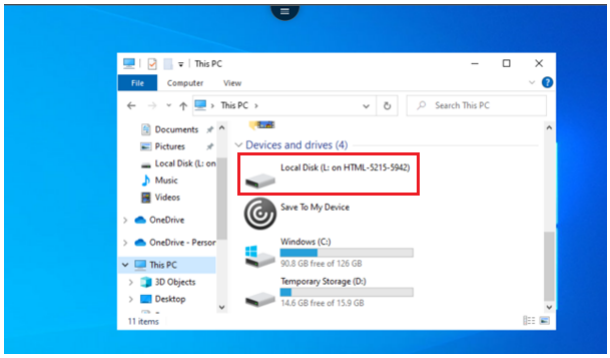


2. Select the **Access level** for the folder or the drive. The drop-down list option that you see depends upon on the access level set by your organization's IT administrator for your profile.

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



3. Select a **Drive letter** and click **Browse** to navigate to your folder or drive in your local machine.



4. Click **Add**.
5. Disconnect and reconnect the session.

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

Keyboard

May 7, 2026

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.

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

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 composed 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. Also, it gives an improved display in the composition and the candidate window.

Prerequisites:

- For Linux VDA, enable **Client keyboard layout sync and IME improvement** policy.
- For Windows VDA, enable **Unicode Keyboard Layout Mapping**, **Client Keyboard Layout Sync**, and **IME Improvement policies**.
- Use Citrix Linux VDA version 2012 and later. For Citrix Windows VDA, all the currently available Windows VDA versions support the generic client IME feature.
- The browser language must be Japanese, Chinese (Simplified), Chinese (Traditional), or Korean.
- Use Google Chrome, Mozilla Firefox, Apple Safari 13 or later, or Microsoft Edge.

> **Note:**
>
> - For macOS, iOS, and Android platforms, modify the system language of the devices to either of the CJK languages. The browser language gets updated automatically.
> - For Windows, Linux, and ChromeOS platforms, modify the browser language to either of the CJK languages.

Configuration:

Starting with version 2105, the Generic Client IME feature is enabled by default for East Asian language (Chinese, Japanese, and Korean) input. As an administrator, you can enable or disable the feature separately for each East Asian language using the **configuration.js** file on the StoreFront server (C:\ProgramFiles\Citrix\Receiver StoreFront\HTML5Client).

To disable this feature for a browser language, edit the **configuration.js** file and set `features.ime.mode.<languageID>` to `seamlessIme`. If **seamlessIme** is set, the Generic Client IME feature is disabled.

configuration.js:

```
    var HTML5_CONFIG = {

       'features': {

            'ime': {

                'mode': {

```

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

```
                    'ja': 'seamlessIme',
                    'zh': 'seamlessIme',
                    'ko': 'seamlessIme'
                }

            }

        }

}
```

To disable the generic client IME feature for one specific language, for example, Japanese, add the JSON as follows:

```
var HTML5_CONFIG = {

        'features': {

            'ime': {

                'mode': {

                    'ja': 'seamlessIme'
                }

            }

        }

}
```

To **enable** this feature for a browser language, edit the **configuration.js** file and set `features.ime.mode.<languageID>` to `ctxIme`, or leave the **mode** property empty ({}), which is the **default** behavior.

configuration.js:

```
var HTML5_CONFIG = {

    'features': {

        'ime': {

            'mode': {

                'ja': 'ctxIme',
                'zh': 'ctxIme',
                'ko': 'ctxIme'
                }

            }

```

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

```
16        }
17
18    }
```

> **Note:**
>
> The configurations determine if East Asian language input uses `seamlessIme` or `ctxIme`. It has no effect on any other language input.

Feature Limitation:

Generic client IME is now supported when you use an extended screen with Citrix Workspace app for HTML5 on Windows, Mac, Linux, ChromeOS, iOS, and Android client platforms. However, for multi-monitor sessions that are not yet supported, you can use **Server IME** instead.

To enable the **Server IME**:

```
1.  Change the VDA or the server keyboard language to Chinese, Japanese
    or Korean (CJK) as required.
2.  Change the client device keyboard language to English.
```

Support for Microsoft Windows logo key and other keyboard shortcuts

The following adds support for the key combinations with the Microsoft Windows logo key in your sessions that runs on Microsoft Windows. The shortcut keys are functional only when you select the **Fullscreen** option in the session toolbar.

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

Also, we're now supporting the following keyboard shortcuts in your sessions that run on Microsoft Windows:

- Alt + Tab
- Esc key

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

- Ctrl + N
- Ctrl + T
- Ctrl + W

For the sessions that run on macOS, we now support the following extra keyboard shortcuts:

- Esc Key
- Command + N
- Command + T
- Command + W
- Ctrl + N
- Ctrl + T
- Ctrl + W

Keyboard shortcuts

This feature allows redirecting a few other shortcuts in full-screen mode. The default settings for Microsoft Windows logo key and other keyboard shortcuts are as follows:

HTML5_CONFIG > **features** > **keyboard** > **captureAllKeys**.

The default value of **captureAllKeys** is set to **true**. To change the default settings, open the **configuration.js** file and set the attribute to **false**.

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

Scancode input mode

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

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

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

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

How to configure

You can configure the Scancode input method in the following way:

- Configuration.js

Configuration.js

> **Notes:**
>
> - Citrix recommends you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.
> - The **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder.

To enable the Scancode support feature, do the following:

1. Navigate to the **configuration.js** file.
2. Edit the file and set the **scancode** attribute to **true**.

   The following is an example of JSON data:

   ```
   'features' : {

           'ime': {

               'scancode': true,
       }

    }
   ```

3. Save the changes.

Citrix VDA for macOS - clipboard and keyboard shortcuts

Starting with the 2411 release, Citrix Workspace™ app supports Citrix VDA for macOS.
For more information, see Citrix Virtual Delivery Agent for macOS.

The following is an enhancement:

- Previously, on Mac clients, the **Command** key was always mapped to the **Control** key in the Citrix Workspace app, preventing **Command+C** and **Command+V**, that is, copy and paste shortcuts from working.

  Starting with the 2411 release, you can send **Command+C** and **Command+V** events when interacting with a Mac VDA. This ensures the correct interpretation of Command key presses.

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

Enhanced keyboard and IME diagnostics tool

Starting with version 2411, Citrix Workspace app for HTML5 supports a new self-service command line tool hosted in Windows Virtual Delivery Agent (VDA) to diagnose keyboard and Input Method Editor (IME) related issues. This tool meets various user requirements, provides platform versatility, and caters to personalized needs. The keyboard and IME functions depend on different configurations and capabilities in VDA and Citrix Workspace apps. Incorrect settings in the VDA or client-side might result in unexpected input behavior.

With this tool, you can easily identify issues that were previously difficult to find. They are:

- **Client keyboard layout and VDA keyboard layout inconsistency**: The tool checks if the client keyboard layout matches the VDA keyboard layout.
- **Keyboard input mode selection for Touch devices**: The tool checks the VDA policy and the selected keyboard input mode, and client device type to confirm if keyboard functions work well.
- **Generic client IME check for East-Asian language input**: The tool checks the client keyboard, IME settings, and VDA policies to confirm if the feature generic client IME works well for typing Chinese, Japanese, and Korean languages.

Prerequisites

- Citrix Workspace app for HTML5 2411 or later.
- Windows VDA 2411 or later.

This command line tool is hosted in Windows VDA as `CtxKbImeDiagnostics.exe`.

Interface	Description	Note
`CtxKbimeDiagnostics`	Shows diagnostic results for the current user's ICA® sessions.	If the user has admin privileges, it shows the diagnostic for all active ICA sessions. If the user has no admin privileges, it shows the diagnostics for the current user's ICA sessions.
`CtxKbimeDiagnostics [-v]`	Shows setting information and diagnostic results for the current user's ICA sessions.	If the user has admin privileges, it shows the diagnostics for all active ICA sessions.
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	Shows setting information and diagnostic results for the current session.	

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

Interface	Description	Note
`CtxKbimeDiagnostics [-s Session_Id]`	Specific to a session and shows the respective diagnostic results for this session.	If the user has admin privileges, they can query other ICA sessions. If the user has no admin privileges, the user can only query their own ICA sessions.
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	Specific to a session and shows all setting information and diagnostic results for this session.	If the user has admin privileges, they can query other ICA sessions. If the user has no admin privileges, the user can only query their own ICA sessions.
`CtxKbimeDiagnostics [-h]`	Shows supported args/parameters and examples.	“Help”interface
`CtxKbimeDiagnostics [-V]`	Shows the current tool version	

Enhanced Alt+ key shortcuts support in double-hop RDP scenarios

Previously, **Alt + key** combinations such as **Alt + Tab** or **Alt + F** did not work properly in double-hop RDP sessions when using Scancode and Unicode mode.

With the 2509 version, **Alt + key** shortcut combinations now function correctly in double-hop scenarios, providing improved keyboard interaction for nested RDP connections.

Generic Client IME enhancement for Citrix Workspace app for HTML5 on Chromebook with multi monitors

Previously, enabling the multi-monitor configuration for the IME resulted in duplicate input on secondary displays in ChromeOS.

With the 2509 version, we now use the browser API to manage the relationship between key and input events, preventing duplicate characters from being entered per keystroke.

Keyboard input mode refinement

Starting with version 2603, Citrix Workspace app for HTML5 introduces a refined user interface for selecting keyboard input modes, replacing the deprecated scancode configuration option. This en-

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

hancement allows users to modify keyboard settings during an active session with immediate effect.

About this feature

This feature provides improved keyboard input management with the following key capabilities:

- **Real-time configuration changes**: Users can modify keyboard input settings during an active session without requiring a session restart.
- **Enhanced user interface**: A new streamlined interface allows users to select keyboard input modes directly from the session preferences dialog.
- **Three input modes**: The feature supports **Automatic**, **Unicode**, and **Scancode** input modes to accommodate different use cases and scenarios.
- **Intelligent automatic mode**: When **Automatic** mode is selected, the system intelligently determines the optimal input method:
  - Citrix Workspace app for HTML5 session running on Mac client connecting to Mac VDA: Scancode mode
  - All other scenarios: Unicode mode

Configuration changes

The previous **Scancode** configuration method is deprecated as of Citrix Workspace app for HTML5 2603:

Deprecated configuration:

```
"features": {

    "ime": {

        "scancode": true
     }

 }
```

New configuration method:

```
"features": {

    "ime": {

        "inputMode": "Scancode"
     }

```

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

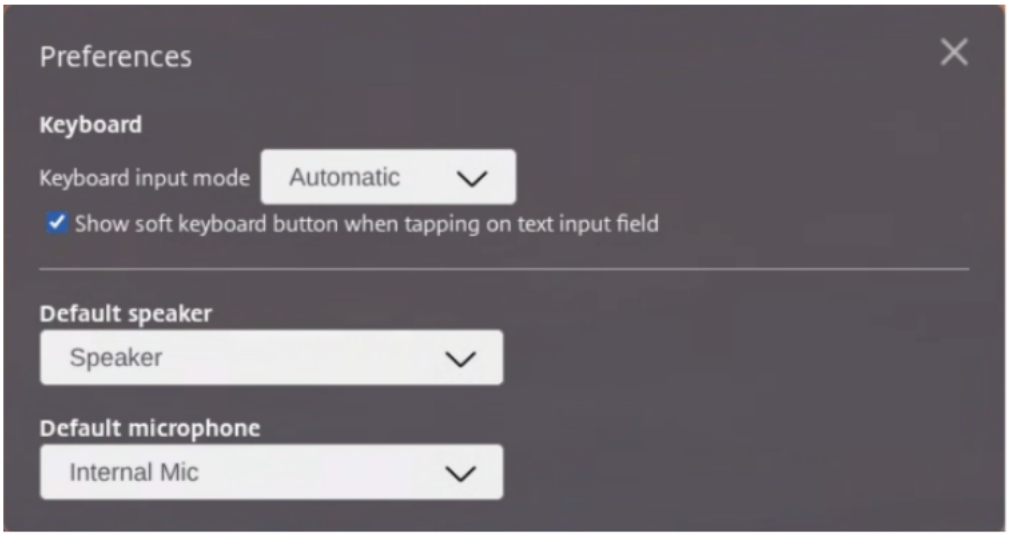
```
8   }
```

> **Note:**
>
> If you have configured the deprecated scancode setting in a previous version, it will be ignored in Citrix Workspace app for HTML5 2603 and later. The application automatically falls back to **Automatic** input mode.

In-session preferences

End users can change keyboard input modes during an active session:

1. Open the **Session Preferences** dialog from the toolbar.
2. Navigate to the **Keyboard** section.
3. Select the desired input mode from the dropdown menu.



   Changes take effect immediately without requiring a session restart.

For more information about keyboard configuration, see Keyboard.

Session experience

September 22, 2026

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

High DPI support for multiple monitors

Citrix Workspace app for HTML5 supports DPI scaling for app and desktop sessions on single and multi-monitor sessions. This feature is mostly used with large-size and high-resolution monitors to display applications, text, images, and other graphical elements in a size that can be viewed comfortably.

> **Note:**
>
> This feature is enabled by default for app and desktop sessions.

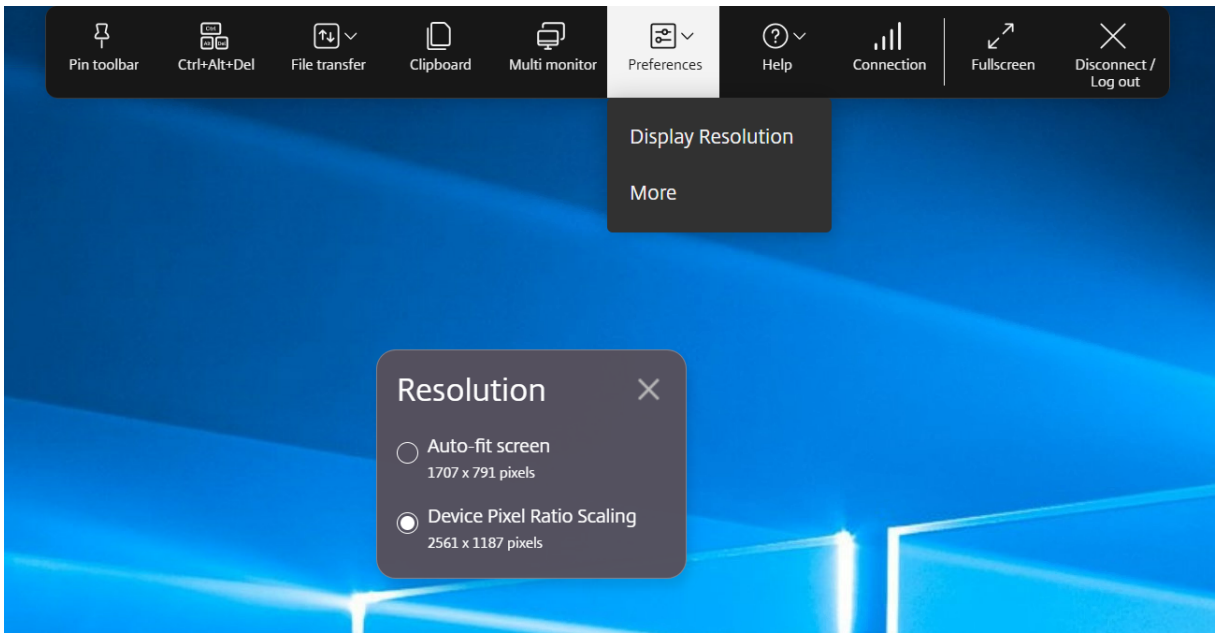
Benefits

This feature automatically adjusts virtual desktop and app sessions based on device DPI, ensuring content appears perfectly sized and sharp without blurriness. Apps and desktops are intelligently scaled based on monitor resolution and device pixel ratio for optimal readability and usability.

How to configure

- End users can disable this feature using session toolbar.
- Administrators can disable this feature using Configuration.js.

Session toolbar In the Citrix Workspace app for HTML5 session, end users can disable this feature using the **Toolbar** > **Preferences** > **Display Resolution** > select **Auto-fit screen** option to disable the High DPI scaling.



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

Configuration.js Administrators can disable using **configuration.js**.

> **Notes:**
>
> - Citrix recommends you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.
> - The **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder.

To disable the feature, do the following:

1. Navigate to the **configuration.js** file.
2. Edit the file and set the **scaleToDPI** attribute to **false**.

   The following is an example of JSON data:

```
{

  "features": {

      "graphics": {

          "dpiSetting": {

              "scaleToDPI": false
           }

       }

   }

 }
```

3. Save the changes.

Session reliability

The session reliability feature ensures that sessions remain active on the user's screen even if there is a disruption in network connectivity. Users continue to see the application they're using until network connectivity resumes.

When connectivity is lost, the session remains active on the server. To alert the user about the connectivity issue, the display becomes unresponsive and a reconnect overlay screen appears. Until connectivity resumes on the other side of the tunnel, session reliability reconnects users without reauthentication prompts.

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

> **Note:**
>
> The **session reliability timeout** policy setting has a default value of 180 seconds or three minutes. Though you can extend the time the session reliability keeps a session open, this feature is convenient to the user.

For more information about the feature, see Session reliability in the Citrix Virtual Apps and Desktops documentation.

> **Important**
>
> With the session reliability feature enabled, the default ports for session communication are 2598 for non-SSL VDA and 443 for SSL VDA.

You can use session reliability with Gateway and SSL VDAs. When using a non-SSL VDA with Citrix Gateway, data encryption happens between the user device and Citrix Gateway.
When using SSL VDA with Citrix Gateway, data encryption happens from the user device to VDA.

Using session reliability policies

- The **session reliability connections** policy setting allows or prevents session reliability.
- The **session reliability timeout policy** setting has a default value of 180 seconds or three minutes. Though you can extend the time the session reliability keeps a session open, this feature is convenient to the user. Therefore, it does not prompt the user to re-authenticate.

> **Tips**
>
> - Extending session reliability timeouts might cause a user to get distracted and walk away from the device, leaving the session accessible to unauthorized users.
>   By default, incoming session reliability connections use port 2598, unless you change the port number in the session reliability port number policy setting.
>   If you use session reliability, it closes, or disconnects, the user session after the amount of time you specify in the **Session reliability timeout** policy setting.
> - Session reliability is enabled by default on the server. To disable this feature, configure the policy managed by the server.

Configuring session reliability from Citrix Studio

By default, session reliability is enabled.

To disable session reliability:

1. Launch Citrix Studio.

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

2. Open the **Session Reliability connections** policy.
3. Set the policy to **Prohibited**.

Configuring session reliability timeout

By default, the session reliability timeout is set to 180 seconds.

> **Note:**
>
> Session reliability timeout policy can be configured only with XenApp and XenDesktop 7.11 and later.

To modify session reliability timeout:

1. Launch Citrix Studio.
2. Open the **Session reliability timeout** policy.
3. Edit the timeout value.
4. Click **OK**.

Enhanced session reliability

The following improvements address network disruptions, ensuring a better user experience by re-connecting the session reliably:

- When you switch between Internet Service Providers (ISPs), the session becomes unresponsive. With the fix, you can reconnect to the session during ISP switches.
- When you switch networks and one Wi-Fi connection lacks internet connectivity, the session reliability feature might fail. With the fix, you can now reconnect to the session during a network switch.

Auto Client Reconnect

Starting with version 2607, Auto Client Reconnect (ACR) feature ensures session continuity by automatically re-establishing connections when Session Reliability cannot recover an interrupted session. If the Session Reliability timeout expires before network connectivity is restored, the Citrix Workspace app attempts to reconnect to the same session. This reconnection uses a server-issued reconnect cookie, allowing you to resume your session from where you left off without needing to reauthenticate.

Session reliability and auto client reconnect operate in following sequence:

- **Network Interruption:** Session Reliability keeps the session active on the server. The session screen freezes and a reconnect notification with a countdown timer appears.

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

- **Session Reliability Timeout:** If network connectivity is not restored before the Session Reliability timeout expires, the session disconnects. ACR initiates reconnection attempts to the same session for the duration of the ACR timeout.
- **ACR Timeout:** If ACR fails to reconnect within its specified timeout, the reconnection attempts stops. You receive a prompt to manually reconnect or end the session.

> **Note**
>
> The displayed countdown timer reflects the combined duration of both Session Reliability and ACR timeouts. For example, with default policy values (Session Reliability: 180 seconds, ACR: 120 seconds), the total countdown is five minutes.

Configuring Auto Client Reconnect

ACR is controlled exclusively by Citrix policies configured on the server. There are no client-side configuration options within Citrix Workspace app for HTML5.

Key policy settings include:

- Auto client reconnect: Enables or disables the feature. Enabled by default.
- Auto client reconnect timeout: Specifies the duration (in seconds) for which the Citrix Workspace app attempts to reconnect. The default value is 120 seconds.

For more information, refer to Auto Client Reconnect in the Citrix Virtual Apps and Desktops documentation.

Known Limitations

- ACR is not supported for sessions accessed through Citrix Gateway if the **Session reliability connections** policy is disabled. To enable ACR in a Citrix Gateway deployment, ensure **Session reliability connections** is set to **Allowed**.
- ACR requires the enhanced in-session toolbar. If this toolbar is disabled, ACR functionality is unavailable.

Toolbar

By default, the enhanced toolbar feature is enabled.

To hide the toolbar:

1. While logged in as an administrator, access the **configuration.js** file in `C:\ProgramFiles\Citrix\<actual path>\HTML5Client`.

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

2. Search the configuration.js file to locate '**menubar key**.'
3. In the **configuration.js** file, set **"menubar":false**.

You can also hide an individual icon to prevent it from showing up in the toolbar. For example, to hide the **ctrl+alt+del** button in the toolbar:

1. While logged in as an administrator, access the **configuration.js** file in **C:\ProgramFiles\Citrix<actual path>\HTML5Client**.
2. Search the configuration.js file to locate '**lock**.'
3. In the **configuration.js** file, set **lock:false**.

URL redirection

URL redirection allows you to control whether users access the URL by using:

- browser published on servers
  or
- browser that run on user devices

URL (Host to client) redirection is one type of content redirection. It's supported only on Server OS VDAs (not Desktop OS VDAs).

When the URL redirection is enabled, the URLs are intercepted on the server VDA and sent to the user device. Citrix Workspace app for HTML5 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 the URL redirection is disabled, users open the URLs with web browsers or multimedia players on the server VDA. When the URL redirection is enabled, users can't disable it.

URL redirection was previously known as server to client redirection or host to client redirection.

For more information, see General content redirection.

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 setting sometimes led to a loss of productivity when the laptop shuts down after the battery runs out.

The newly available battery status indicator feature is supported on Google Chrome and Microsoft Edge (Chromium) browsers. It's 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

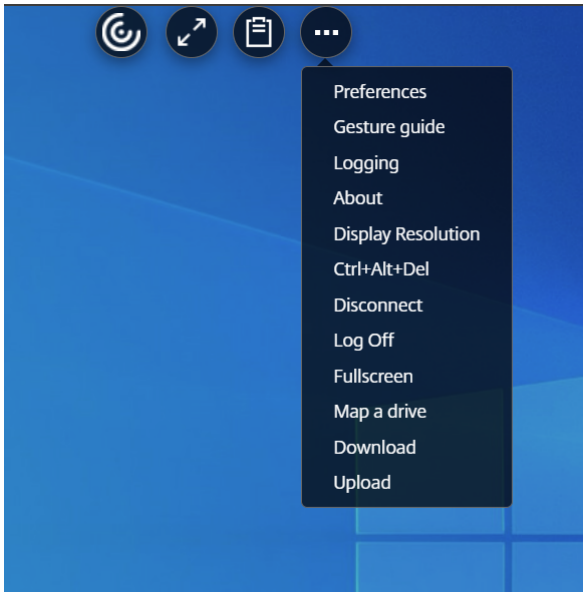
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> appear.

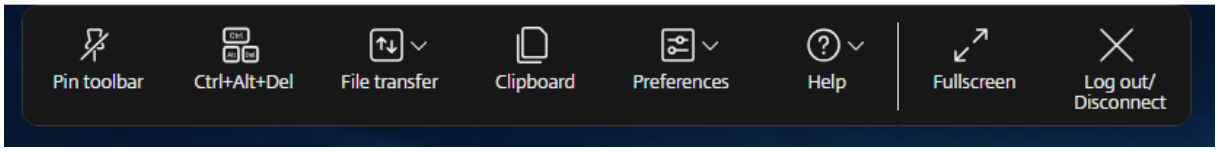
Improved in-session toolbar

Starting with the 2411 version, an enhanced toolbar UI appears when you start a desktop session. The look and feel of the in-session toolbar UI has changed. The toolbar UI is designed to enhance the end user experience by organizing the options in a user-friendly manner.

Old toolbar UI



New toolbar UI



> **Note:**
>
> This feature is disabled by default. To enable the feature, follow the configuration steps.

Known issues in the feature

- When you move the toolbar notch in the session, the tooltip for the notch doesn't appear. [RFHTMCRM-14281]

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

How to configure

You can configure the new toolbar feature for on-premises setups as follows:

Configuration.js** In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To enable the new toolbar feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the `switchToNewToolbar` attribute and set the attribute to **true**. For example:

```
{

    'ui': {

        'toolbar': {

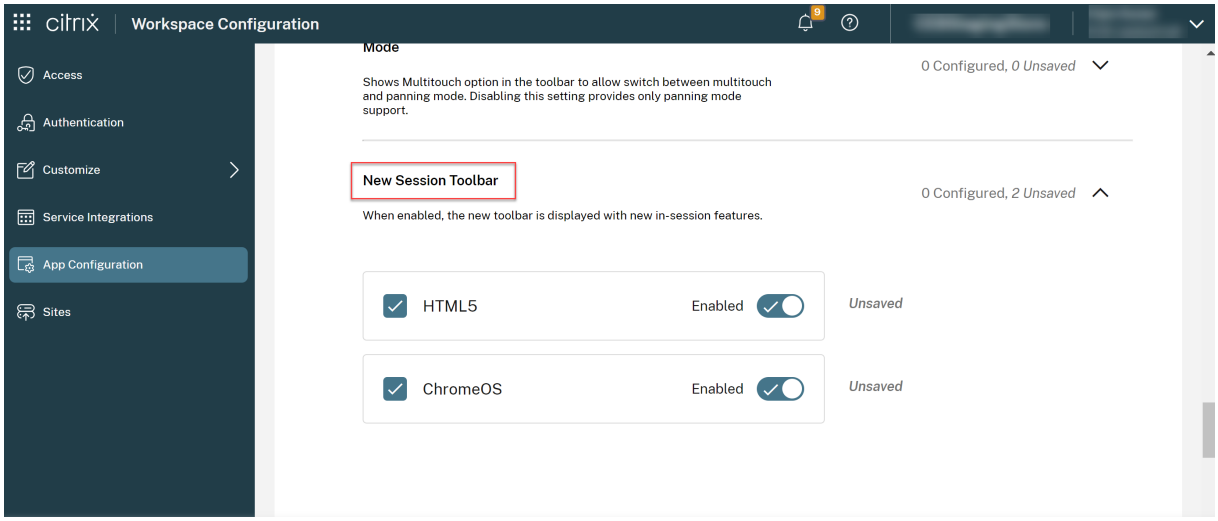
            'switchToNewToolbar': true,
        }

    }

}
```

Global App Configuration service On the cloud setup, administrators can enable or disable the improved toolbar feature by navigating to **Workspace Configuration** > **App Configuration** > **Session Experience** > **Toolbar** > **New Session Toolbar**. Select the checkbox and respective toggle button to enable the feature.

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

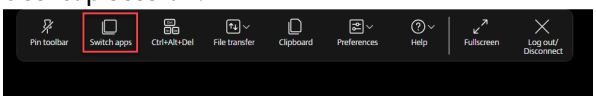
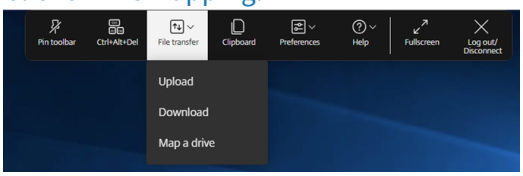


Icons and Actions

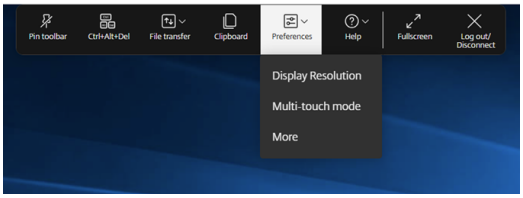
> **Note:**
>
> The icons are visible to the end users only if their organization's admin has enabled the specific feature.

Icon or Action	Description
Toolbar notch	When you start an app or a desktop session, the toolbar notch appears at the top of the screen. When you click the notch, the toolbar appears in the unpinned state. Drag and reposition the toolbar notch onto any side of the screen. After you release the mouse, the notch will automatically align itself with the nearest edge.
Pin	When you pin it, you can drag and reposition the toolbar onto any side of the screen. After you release the mouse, the toolbar automatically aligns itself with the nearest edge. The advantage of pinning the toolbar is that it doesn't minimize into a notch after you complete an action that involves toolbar icons.
Unpin	When you unpin the toolbar, it minimizes into a notch after you complete an action that involves toolbar icons. You can drag and reposition the toolbar notch onto any side of the screen.

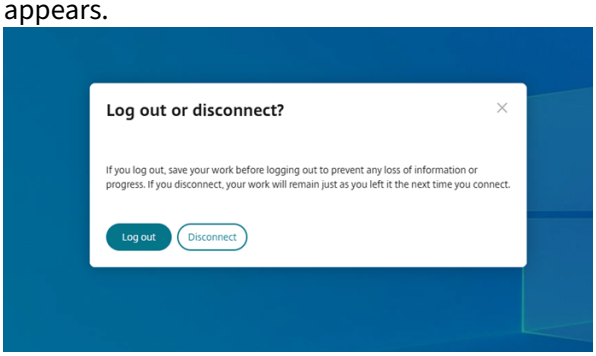
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Icon or Action	Description
Switch apps	Click the icon to view the already opened apps in the same VDA. This icon doesn't appear in the desktop session. 
Ctrl+Alt+Del	You can perform the **Ctrl+Alt+Del** function with the click of a button. This option helps users to sign out, switch users, lock the system, or access the Task Manager.
File transfer	• **Upload and Download**: you can upload or download a file between a user device and a session. For more information, see File handling. • **Map a drive**: The Client Drive Mapping (CDM) feature allows you to access your local folders and drives from Citrix Workspace app. For more information, see Client Drive Mapping. 
Clipboard	You can use the clipboard option to copy and paste plain text and HTML data from the VDA to the local device and back. For more information, see Clipboard.
Devices	Click to open the **USB Devices** dialog box. Click **Add** to view the USB devices connected to the local device. The dialog box lists the devices that can be redirected to the session. To redirect the USB devices, select an appropriate device and click **Connect**. For more information, see USB device redirection. **Note:** You can view the **Devices** icon only if your IT administrator provides access to connect USB devices through policy settings.

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

Icon or Action	Description
Preferences	• **Display Resolution**: select the size of the resolution for the session display. By default, the screen resolution is set to **Auto-fit** screen. • **Multi-touch mode**: click to use the multi-touch mode. You can toggle between Panning and Multi-touch mode. This option is applicable to touch-screen devices. For more information, see Touch and mobility support. • **More**: displays preferences about the soft keyboard button and Citrix Customer Experience Improvement Program (CEIP). 
Help	• **Gesture Guide** –a gesture guide appears with details on how to use finger taps. This option is applicable only to touch-screen devices. • **About** –displays the current version of the Citrix Workspace™ app that you're using.
Fullscreen	You can switch your screen from windowed mode to full-screen mode. In Citrix Workspace app for HTML5, the fullscreen icon action doesn't span the session across monitors. However, if you select the monitors from the custom layout and the session spans to the respective monitors, then when you restore, the **Fullscreen** icon gets replaced by the **Extend** option. When you click the **Extend** icon, the session spans to the previously selected monitors.

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

Icon or Action	Description
Disconnect	The disconnect action keeps the virtual desktop running. Log out to save energy. **Note:** When admin configures both **Log out** and **Disconnect** options, the following message appears.  **Log out to save energy**: the logout action shuts down the virtual machine and conserves energy. End users must make sure to save their work before logging out. **Disconnect**: closes the virtual desktop session window. However, the virtual session remains active until the next sign-in. End users can resume their work easily. The **Sustainability leaf icon** appears only when the sustainability feature is enabled. For more information, see Sustainability initiative from Citrix Workspace app.

Sustainability initiative from Citrix Workspace app

Starting from the 2405 version, we have introduced a sustainability initiative that encourages users to conserve energy that might be used due to running unused virtual desktops.

Starting from the 2411 version, admins can customize the disconnect and log out dialog box contents.

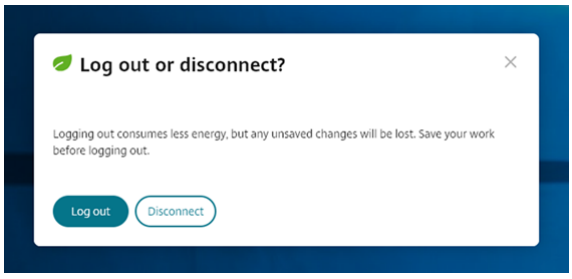
With this feature enabled, when users tap on the **X** icon to disconnect the session, a prompt is displayed to log out from the desktop session. This feature can be helpful in enterprises that use Windows OS policies to shut down VMs when no users are logged in.

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

> **Notes:**
>
> - This feature is disabled by default.
> - This feature is available on both cloud and on-premises store.
> - To use this feature, you must enable the new toolbar feature. To enable, see the configuration section in the Improved in-session toolbar feature.

To enable this feature, do the following:

1. Navigate to Citrix Studio.
2. Click **Delivery Groups** from the left navigation pane.
3. Select the required VDA from the **Delivery Group** section.
4. Click the **Edit** icon. The **Edit Delivery Group** page appears.
5. Click **Desktops** from the left navigation pane.
6. Select the required VDA where you must add the keywords.
7. Click **Edit**. The **Edit Desktop** page appears.
8. Set the `ICA-LogOffOnClose` keyword to **`true`** in the **Description** field.
9. Click **OK**. The following dialog box appears when you close the virtual desktop.



End users can exit from the session in two ways:

Log out to save energy - This sustainability action shuts down the virtual machine to conserve energy. End users must make sure to save their work before signing out.

Disconnect to close the virtual desktop session window. However, the virtual session remains active until the next sign-in. End users can resume their work easily.

Customizing the text in the Save Energy screen

Starting from the 2411 version, admins can customize the disconnect and log out dialog box contents in the Save energy screen.

> **Notes:**
>
> - This feature is disabled by default.
> - This feature is available on both cloud and on-premises store.

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

> - To use this feature, you must enable the new toolbar feature. To enable, see the configuration section in the Improved in-session toolbar feature.

Prerequisites

The minimum on-prem StoreFront™ version required is 2407.

Configure

Admins can customize the sustainability dialog box contents using the following keywords in DDC for both on-premises and cloud setup:

> **Note:**
>
> The maximum number of characters allowed in the **Description** field is 200.

Keyword	Description
ICA-LogOffOnClose	Keyword for enabling or disabling Sustainability. The default value is **false**.
ICA-Icon	Keyword for enabling or disabling Sustainability leaf Icon. Even if this setting is empty, the **ICA-LogOffOnClose** setting applies.
ICA-PromptMessage	Keyword for customizing the prompt message that appears in the dialog box. If you haven't given a customized message, then the default message applies.
ICA-Title	The keyword for customizing the title that appears in the dialog box. If you haven't given a customized message, then the default message applies.

> **Notes:**
>
> - The disconnect and log out dialog boxes appear according to the parsed key.
> - If you choose not to use the sustainability feature, then the admin can configure the key **LogOffOnClose** to **false**. However, the user sees the default dialog box, and can choose to click the **Don't ask me again** checkbox. When the user clicks this option, the session disconnects, but the dialog box doesn't appear in subsequent sessions.

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

Customization:

To customize the text in the Save Energy screen, do the following:

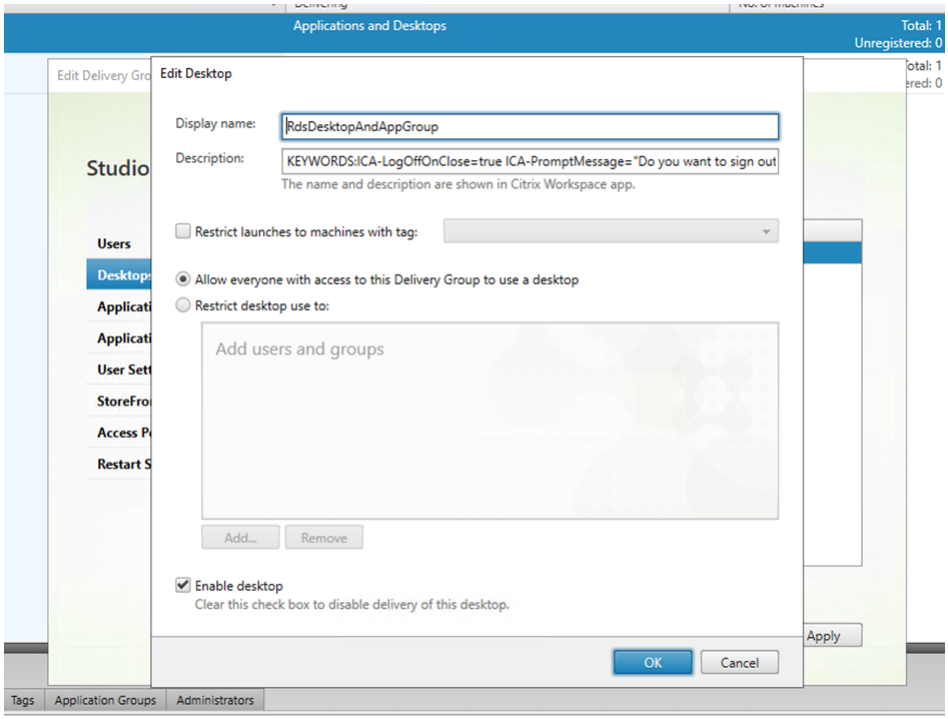
1. Follow steps 1–8 from the preceding section.
2. Set the `ICA-PromptMessage` keyword to the required text in the Description field.
3. Set the `ICA-Title` keyword to the required text in the Description field.
4. Set the `ICA-Icon` keyword to true or false.

   Example:

   ```
   KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the session?" ICA-Title="Sign out or disconnect" ICA-Icon=true
   ```

   The following screenshot displays how to edit desktop group dialogs:

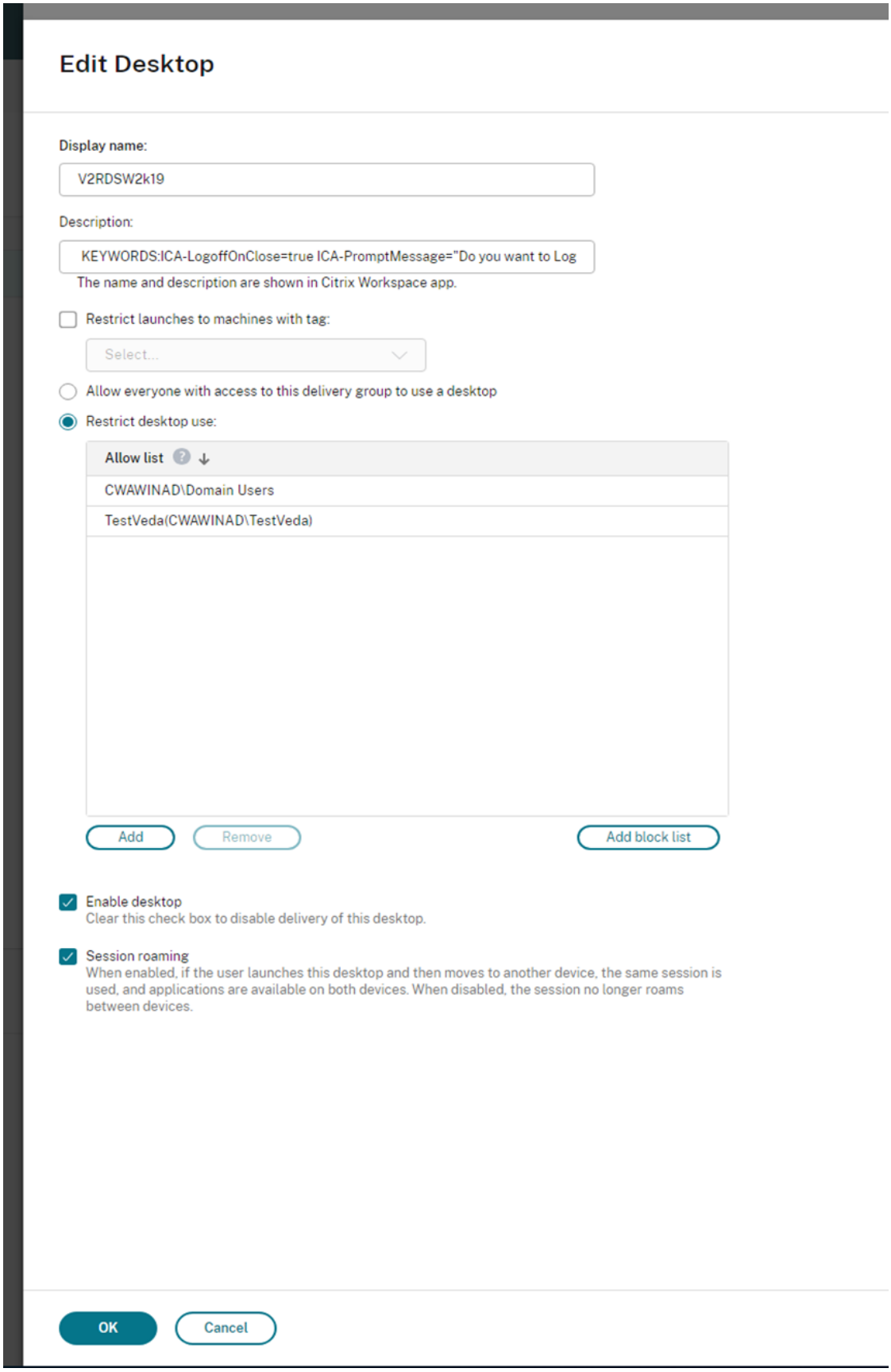
   For on-premises setups



State

   For cloud setups

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



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

The keywords are assigned by default for new desktop machines assigned to the group. For existing desktop machines, you must run the following PowerShell commands for changes to apply:

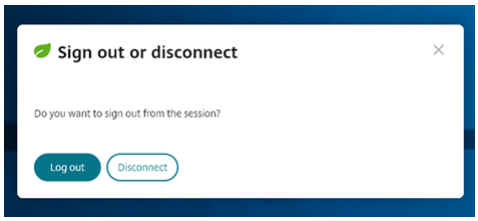
```
$dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'
    ,'Uid'

$apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
    -Property 'Description' )

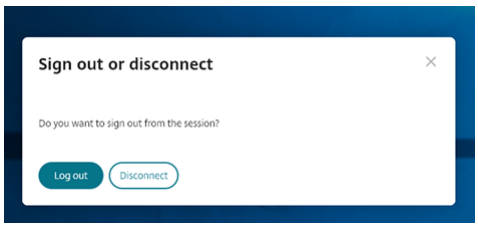
Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set
    -BrokerMachine -Description $apr[0].Description
```

With this PowerShell script, it's possible to have multiple assignment policy rules for a single Delivery Group. Using Citrix Studio also, you can configure multiple Assignment policy rules, each with a unique description value, and a possible set of different keywords.

5. Click **OK**. The following dialog box appears when you close the virtual desktop:



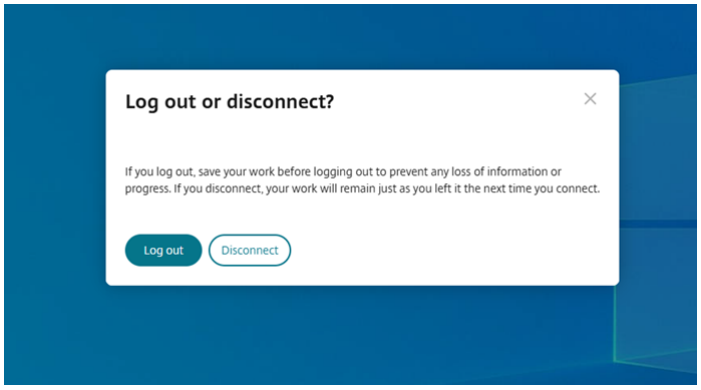
When `ICA-Icon=false`, the Leaf icon doesn't appear.



End user experience

When users tap on the **X** icon to disconnect the session, the following prompt appears:

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



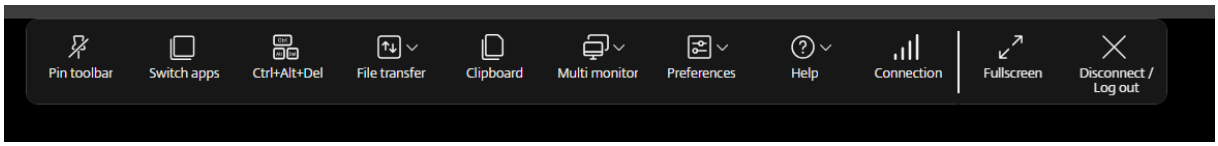
End users can exit from the session in the following two ways:

- **Log out to save energy** - This sustainability action shuts down the virtual machine and conserves energy. End users must make sure to save their work before logging out.
- **Disconnect** - click **Disconnect** to close the virtual desktop session window. However, the virtual session remains active until the next sign-in. End users can resume their work easily.

> **Note:**
>
> The sustainability leaf icon appears only when your admin has enabled the sustainability feature.

Enhancements to the improved in-session toolbar

Starting with the 2502 version, this feature is enabled by default. To disable the feature, follow the configuration steps mentioned in this article.



> **Note:**
>
> The new toolbar isn't supported if the Citrix Workspace app for HTML5 session is launched in a mobile browser.

How to configure You can disable the new toolbar UI by using:

- Configuration.js
- Global App Configuration service

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

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

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the new toolbar feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the `switchToNewToolbar` attribute and set the attribute to **false**. For example:

```
{

    'ui': {

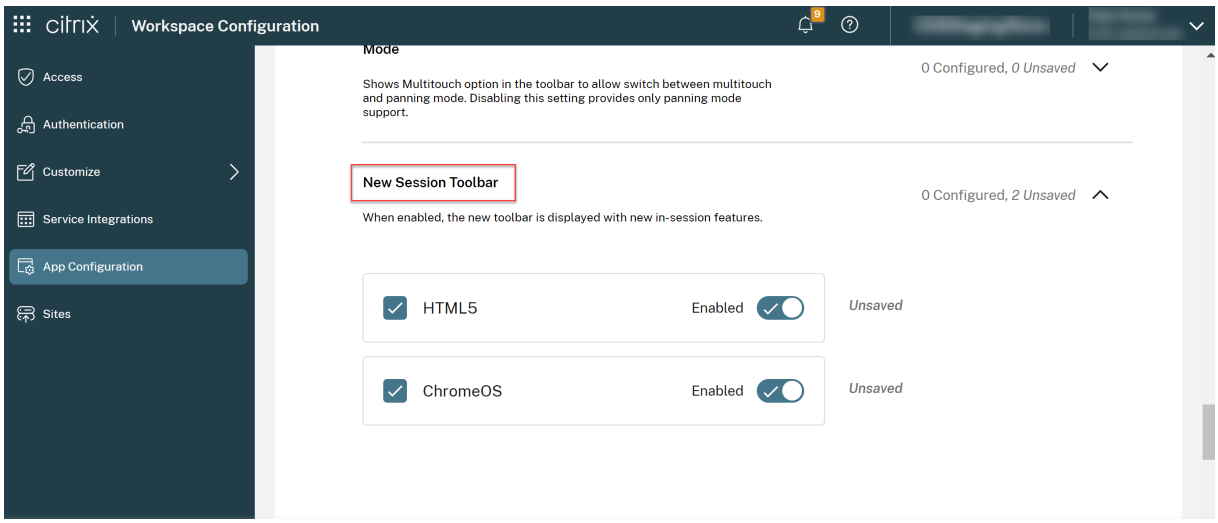
        'toolbar': {

            'switchToNewToolbar': false,
        }

    }

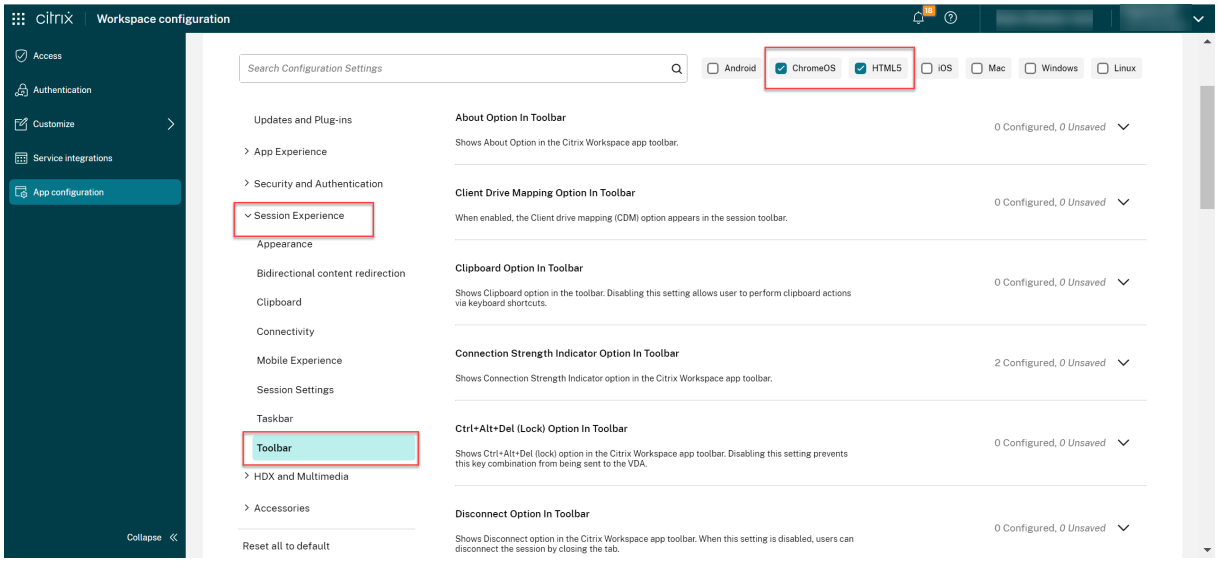
}
```

Global App Configuration service On the cloud setup, administrators can disable the new toolbar feature by navigating to **Workspace Configuration** > **App Configuration** > **Session Experience** > **Toolbar** > **New Session Toolbar**. Clear the checkbox and respective toggle button to disable the feature.



Toolbar customization Admins can customize the toolbar, choosing what options must be viewed by the end user. You can customize it using the Global App Configuration service.

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



To enable a particular feature, administrators can:

1. Navigate to **Workspace Configuration** > **App Configuration** > **Session Experience** > **Toolbar**.
2. Select the checkbox **HTML5**.
3. Scroll and click the down arrow.
4. Select the platform checkbox and click the toggle button to enable or disable the option in the toolbar
5. Save and publish the changes.

The following table displays the toolbar options that the admin can configure:

Option	Description
About Option In Toolbar	Shows About Option in the Citrix Workspace app toolbar.
Client drive mapping option in toolbar	When enabled, the Client drive mapping (CDM) option appears in the session toolbar.
Clipboard Option In Toolbar	Shows Clipboard option in the toolbar. Disabling this setting allows user to perform clipboard actions via keyboard shortcuts.
Connection Strength Indicator Option In Toolbar	Shows Connection Strength Indicator option in the Citrix Workspace app toolbar. **Note:** This option applies only to the new toolbar.
Ctrl+Alt+Del (Lock) Option In Toolbar	Shows Ctrl+Alt+Del (lock) option in the Citrix Workspace app toolbar. Disabling this setting prevents this key combination from being sent to the VDA.

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

Option	Description
Disconnect Option In Toolbar	Shows Disconnect option in the Citrix Workspace app toolbar. When this setting is disabled, users can disconnect the session by closing the tab.
Display Resolution Option In Toolbar	Shows Display Resolution option in the Citrix Workspace app toolbar that allows users to select different session resolutions. Disabling this setting matches the resolution to the browser tab size.
File Upload & Download Options In Toolbar	Shows File Upload and Download option in the Citrix Workspace app toolbar. When this setting is disabled, users can still use drag/drop and Send my device within the VDA.
Fullscreen Option In Toolbar	Shows Fullscreen option in the Citrix Workspace app toolbar. When this setting is disabled, users can use a browser shortcut to make the session fullscreen.
Gesture Guide Option In Toolbar	Shows Gesture guide option in the Citrix Workspace app toolbar.
In-session Toolbar	Enables a floating toolbar within the session.
Logging Option In Toolbar	Shows View logs option in the Citrix Workspace app toolbar that allows users to view logs generated for a session.
Logoff Option In Toolbar	Shows the Logout option in the Citrix Workspace app toolbar. When this setting is disabled, users can Logout via the Start menu or close all the apps within the session.
Multi-monitor Option In Toolbar	Shows Multi-monitor option in the Citrix Workspace app toolbar when at least one external monitor is connected.
Multitouch Option In Toolbar To Allow Switching Between Multitouch And Panning Mode	Shows Multitouch option in the toolbar to allow switch between multitouch and panning mode. Disabling this setting provides only panning mode support.
Pin option in toolbar	When enabled, the Pin/Unpin option appears in the session toolbar. **Note:** This option applies only to the new toolbar.

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

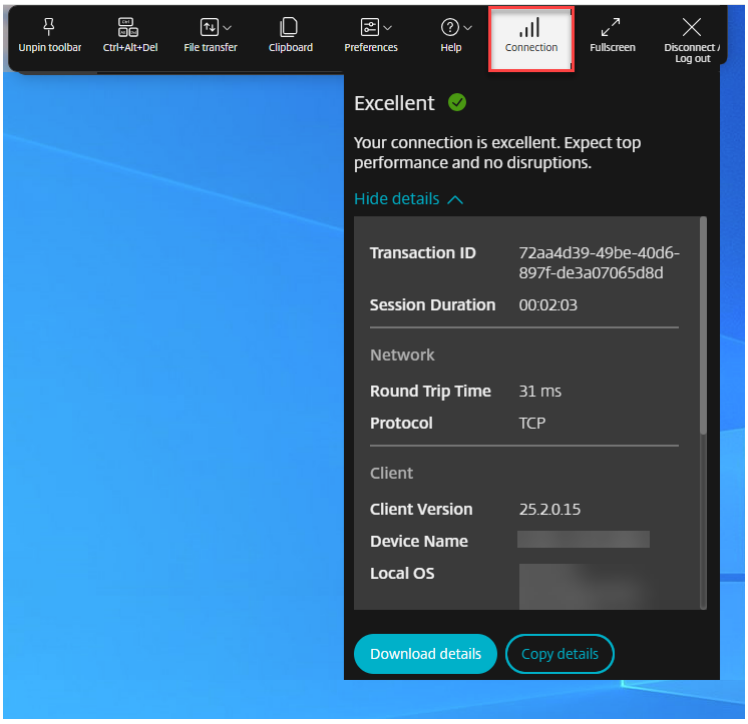
Option	Description
Preferences Option In Toolbar	Shows Preferences option in the Citrix Workspace app toolbar.
Switch Apps Option In Toolbar	Shows Switch apps option in toolbar for virtual app session to allow switching between the apps. Disabling this removes the option to switch apps.
USB Devices Option In Toolbar	Shows USB Devices option in the Citrix Workspace app toolbar. Disabling this setting prevents access to any USB devices within the Citrix Workspace app.

Connection strength indicator

Starting with the version 2502, Citrix Workspace app for HTML5 supports the Connection Strength Indicator (CSI) on the in-session toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy (or download) diagnostic information to share with IT for advanced troubleshooting.

> **Notes:**
>
> - This feature is enabled by default.
> - When you open the session, you can see the Connection Details icon on the in-session toolbar, provided the new toolbar feature is enabled.

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



Benefits

- Immediate feedback: The network strength icon gently nudges users when network issues are detected.
- Enhanced troubleshooting: Real-time stats and diagnostics help users and IT teams quickly identify and resolve connectivity issues.

Prerequisites This feature is available only when a session is opened using:

- Citrix Virtual Apps and Desktops™ version 2407 or later
- Citrix Virtual Apps and Desktops version 2402 LTSR CU1 or later

Known issue in the feature With Citrix Virtual Apps and Desktops version 2411, the Connection Strength Indicator (CSI) on the in-session toolbar doesn't display the protocol information such as RTT and Bandwidth (in EDT protocol) [XASUP-6810].

How to configure You can disable the feature by using:

- Configuration.js
- Global App Configuration service

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

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the new toolbar feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the `connectionStrengthIndicator` attribute and set the attribute to **false**. For example:

```
{

    'ui': {

        'toolbar': {

            'connectionStrengthIndicator': false,
        }

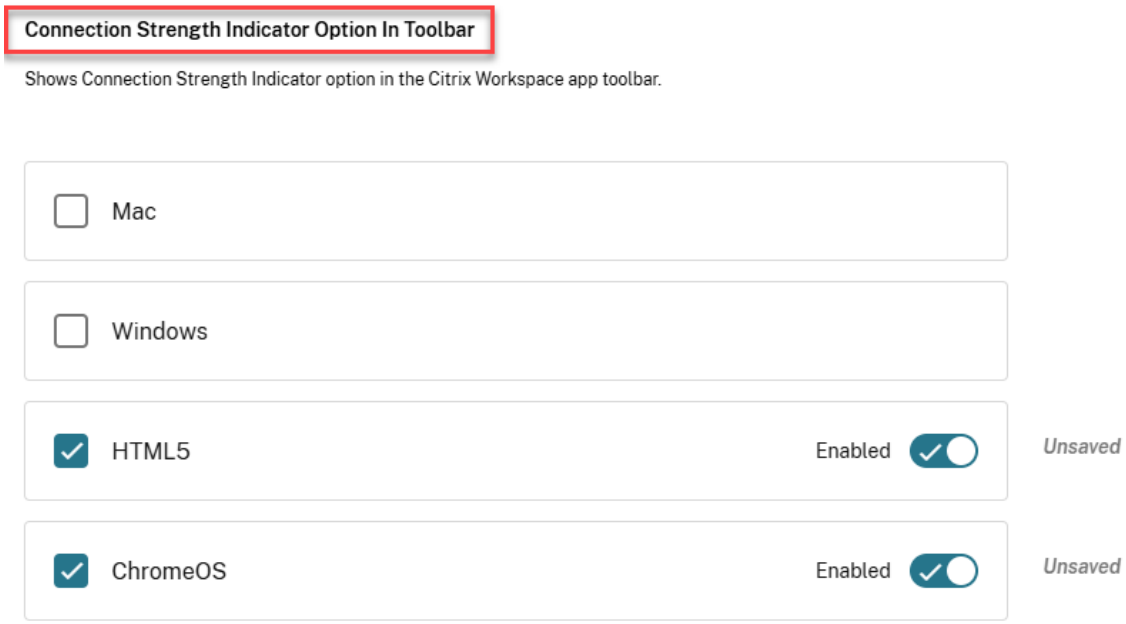
    }

}
```

Global App Configuration service Administrators can disable the feature by navigating to **Workspace Configuration** > **App Configuration** > **Session Experience** > **Toolbar** > **Connection Strength Indicator**.

Clear the checkbox and respective toggle button to disable the feature.

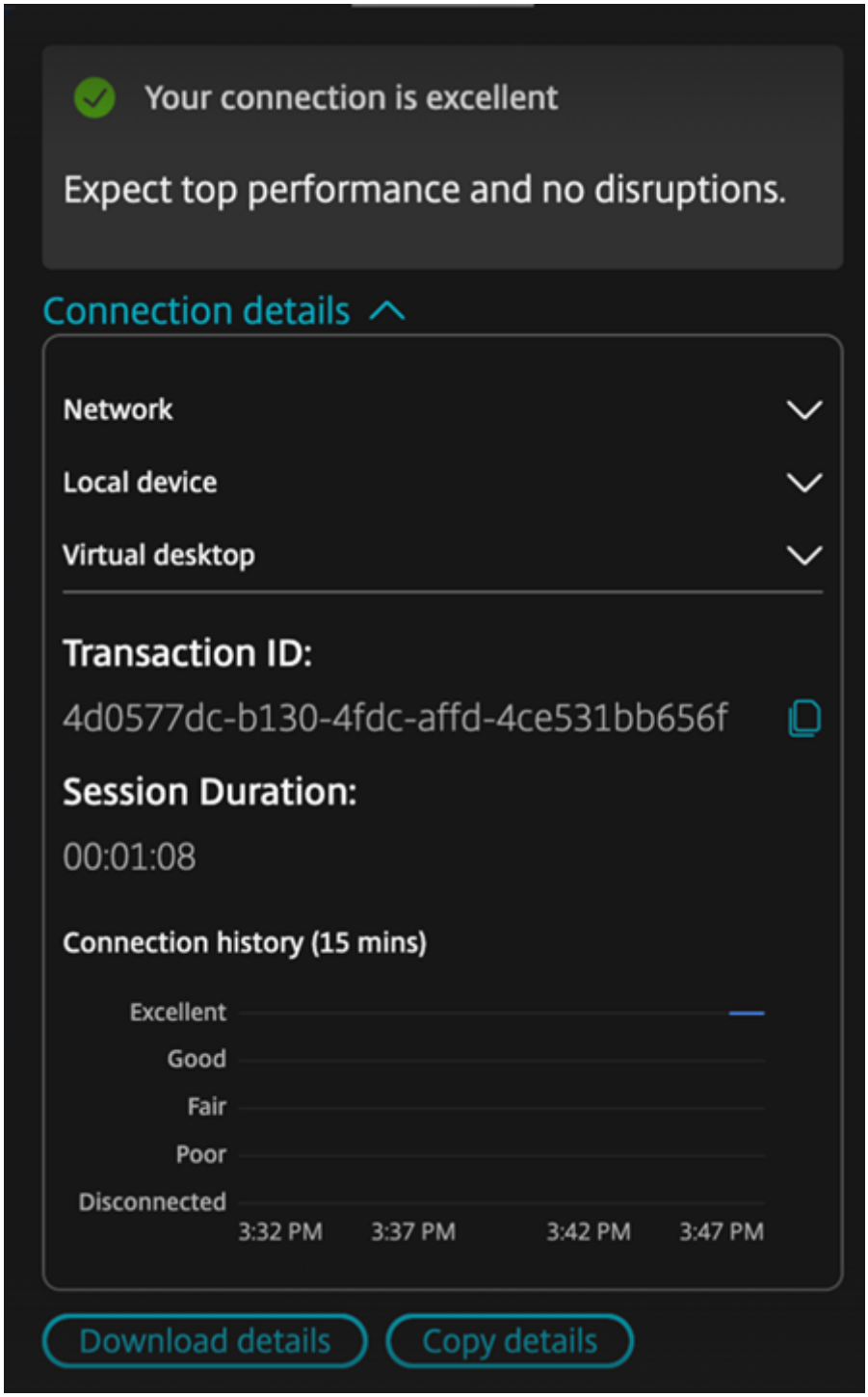
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enhancement to Connection Strength Indicator

Starting with version 2607, Citrix Workspace app for HTML5 introduces an enhanced Connection Strength Indicator, designed to provide a more intuitive and user-friendly experience.

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



The key improvements include:

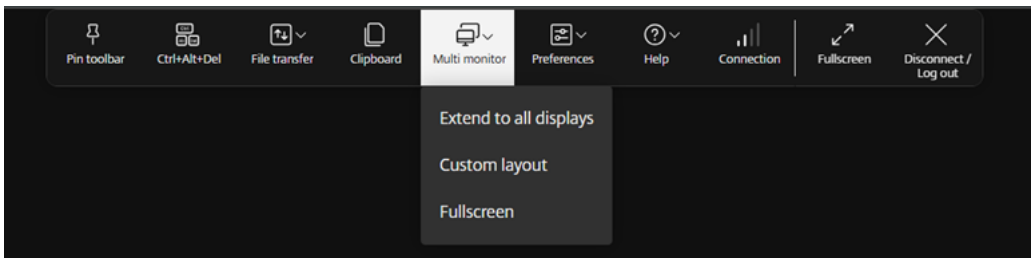
- **Expanded device details:** Access comprehensive information, such as client device's CPU status.
- **Proactive notifications:** Receive alerts in the toolbar notch when your connection strength drops.

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

- **Actionable recommendations:** Get clear suggestions to resolve connectivity issues when your connection strength falls below optimal levels.
- **15-minute connection history:** Review a visual history of your connection strength over the past 15 minutes to assist with troubleshooting and analysis.

Enhanced multi-monitor support with auto-detection and custom display selector

Starting with version 2505, new options have been added under **Multi monitor** icon in the toolbar, which appears only when more than one screen is connected. The multi-monitor selector allows users to choose which displays to use in full-screen mode for app and desktop sessions.



As long as the layout remains the same at the client OS, it is remembered when you disconnect and reconnect to the same session.

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

System requirements

This feature is only supported on Google Chrome and Microsoft Edge Chromium browsers on Windows OS.

Prerequisites

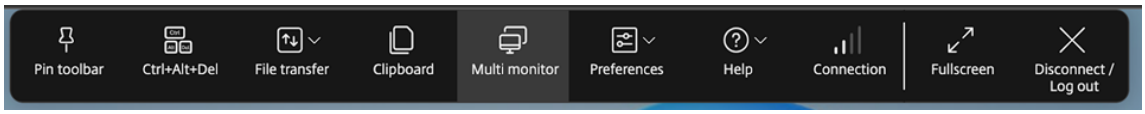
- Ensure that the new toolbar feature is enabled. For more information, see Improved in-session toolbar.
- Allow permissions:
  - **Window management permission** that is important for websites that must access information about different monitors and manage windows across them
  - **Browser pop-up permission** to manage whether websites can open new windows or tabs without your direct interaction.

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

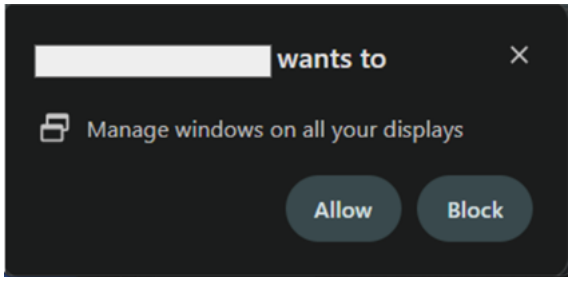
Permission workflow

Perform the following steps:

1. As a first-time user, when you click the multi-monitor selector icon, the following pop-up appears seeking permission to use the multi-monitor setup.

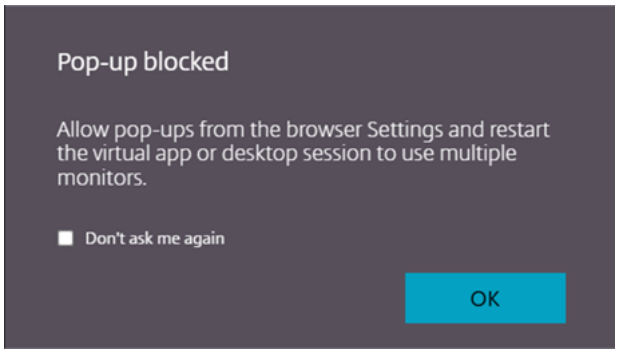


   The pop-up appears from the browser to seek permission to use multiple monitors.

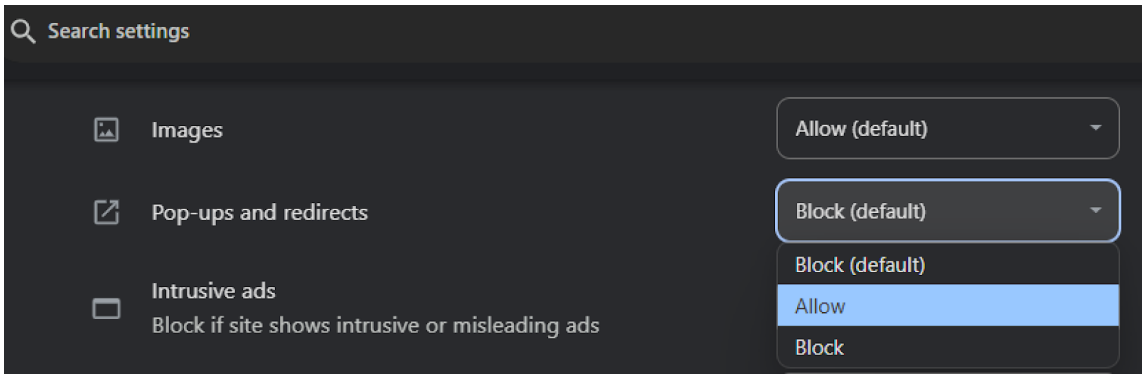


2. If you click **Block**, you can't use multiple monitors. To enable permissions manually, refer Enable the multi-monitor permissions manually.

   If you click **Allow**, the pop-up appears to let you know about the pop-up blockers.



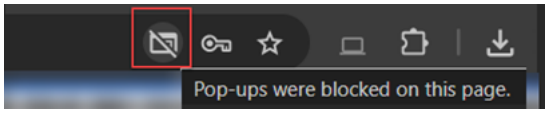
3. Click **OK**, and navigate to the browser settings and select **Always allow pop-ups**.



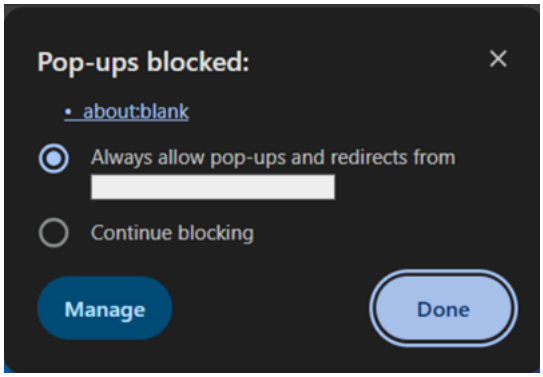
© 1997–2026 Citrix Systems, Inc. All rights reserved.

(or)

Click the pop-up icon on the browser address bar.



Select **Always allow pop-ups** as shown.



Enable the multi-monitor permissions manually

If you click **Block** in the multi-monitor pop-up permissions, the multi-monitor icon doesn't appear. Instead, the full-screen icon appears on the toolbar that takes you to the older behavior.

To manually re-enable the multi-monitor permissions on Microsoft Chromium Edge:

1. Click **ellipses (⊠)** in the top-right corner and select **Settings**.
2. Navigate to **Cookies and site permissions** > **All permissions**
3. Scroll down and click **Window management**.
4. Select **Allow** for sites requesting window placement permissions.

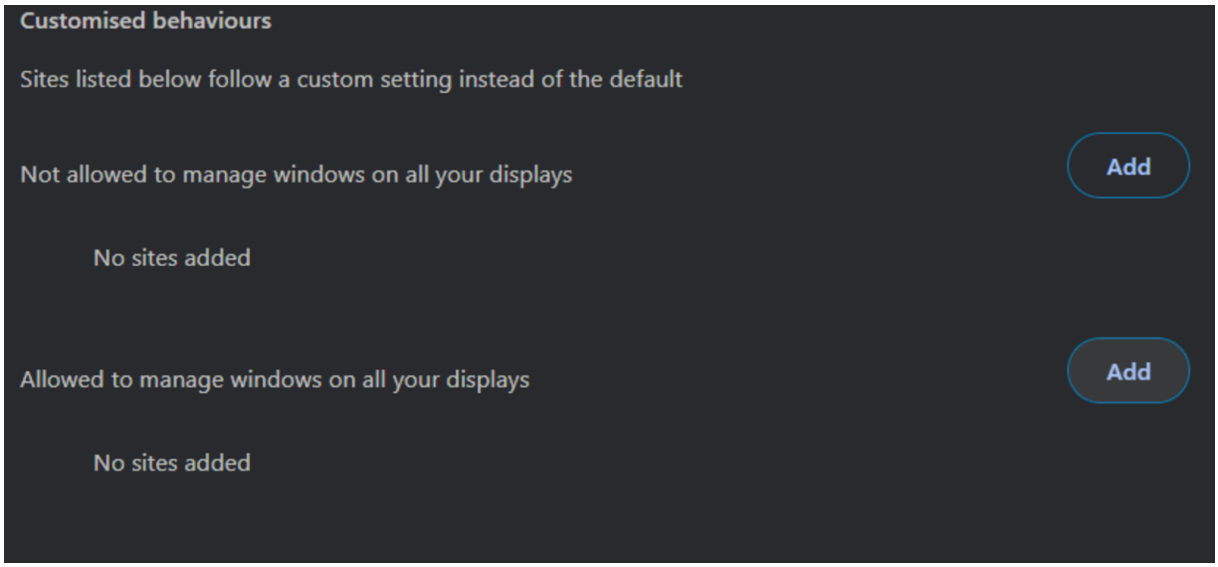


To manually re-enable the multi-monitor permissions on Google Chrome:

1. Click **ellipses (⊠)** in the top-right corner.
2. Select **Settings.**

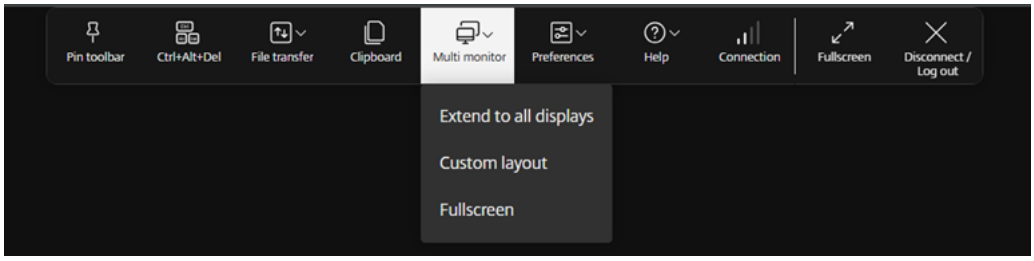
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the left-hand menu, click **Privacy and security**.
4. Click **Site Settings**.
5. Scroll down to **Permissions** and click **Additional permissions**.
6. Click **Window management**.
7. Click **Add** to add a site to **Allow** window placement under **Allowed to manage windows on all your displays**.



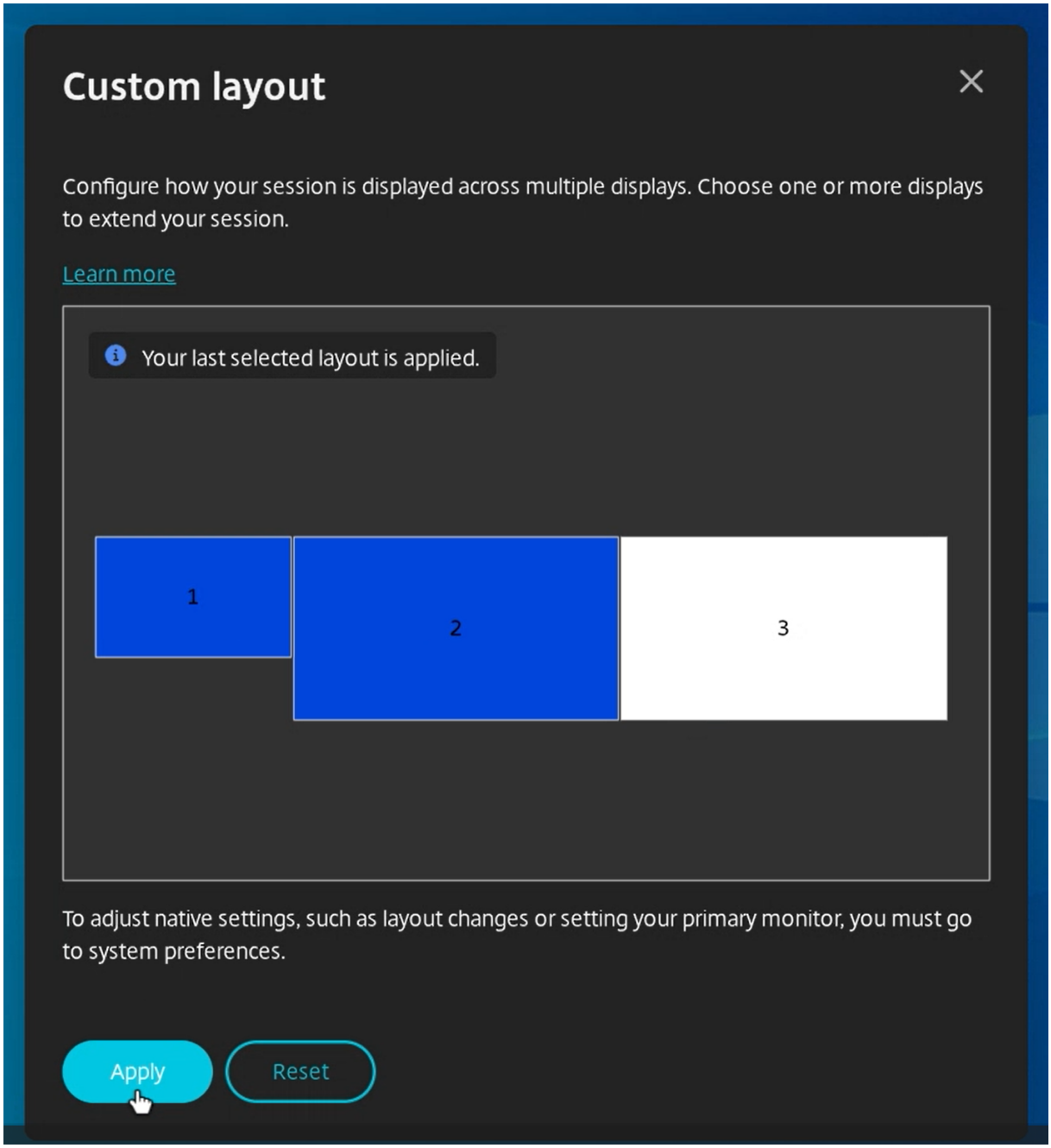
Multi-monitor icon

The **Multi monitor** toolbar icon includes three drop-down menu options for desktop and app sessions in full-screen mode:



- **Extend to all displays:** The session switches to full-screen mode on primary screen and maximized mode on all connected screens.
- **Custom Layout:** This option opens a custom monitor selector displaying the monitor layout. With this feature, you can configure how your session appears across the monitors. Users can click the rectangles in the selector to choose which screens to use and then click **Apply** to span the session on those monitors. The layout box arrangement depends on how the monitors are connected.

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



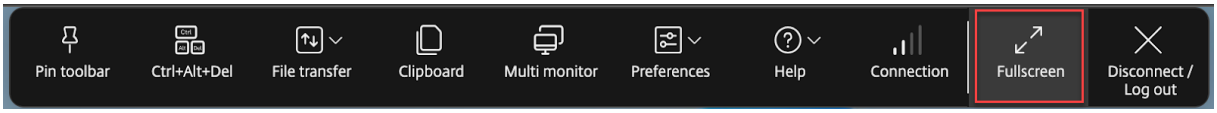
- **Fullscreen:** The session layout changes to full-screen mode using screens that intersect with the session window.

Use case for custom layout Assume that you have two monitors connected to your device. You can choose to run a video conferencing app on your native device monitor and view your virtual desktop contents in full-screen across your other two monitors during the call.

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

Fullscreen and Extend options

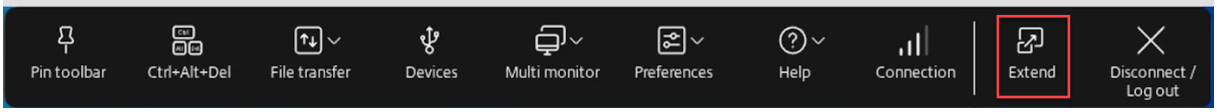
The **Fullscreen** or **Extend** button in the new toolbar is a multi-purpose option button. You can switch your screen from windowed mode to full-screen mode.



The **Fullscreen** icon action either takes the session to full-screen mode or if you reposition your virtual desktop between more than one adjacent monitor (a subset of available monitors), then the session spans across these monitors.

For more information, see Multi-monitor setups.

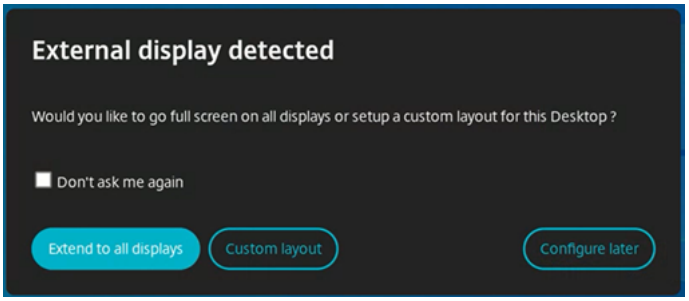
Extend option If you select the monitors from the custom layout and the session spans to the respective monitors, when you restore, the **Fullscreen** icon gets replaced by the **Extend** option. When you click the **Extend** icon, the session spans to the previously selected monitors.



Multi-monitor plug and unplug actions

When a new monitor is plugged in (connected), a notification asking the user to make a selection appear.

Users can select **Don't ask me again** to mute this notification.



Known limitations

- On the external monitor, resource windows aren't in full-screen mode. Instead, it is in windowed mode with a size equal to the external monitor size. We recommend manually switching to full-screen for a better user experience on each of the external monitor windows.

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

To switch fullscreen, use the F11 key on Windows and your Mac, move the pointer to the green button in the top-left corner of the window, then choose **Enter Full Screen** from the menu.

- The multi-monitor selection is not saved between sessions. You must manually select your preferred monitors each time you start a new session by clicking the multi-monitor icon on the toolbar.
- Multi-monitor state goes into single monitor **Fullscreen** state by default on external monitor layout change when the session is in active state.

How to configure

This feature is enabled by default. You can disable the feature in the following way.

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To enable the new toolbar feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the *enableMultiMonitorCustomLayout* attribute and set the attribute to *False*. For example:

```
{

'features': {

    'graphics':
            {

            'multiMonitor': true,
            'enableMultiMonitorCustomLayout': false
             }

             }


 }
```

3. Save the changes. Restart the StoreFront services (if necessary)

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

Enhanced session toolbar notch size

The 2509 version of Citrix Workspace app for HTML5 features a redesigned, smaller notch in the session window that you can drag and drop to any window edge. The notch design provides an optimal size, and the cursor pointer changes when you hover over it. This update addresses user feedback about wasted screen space and replaces the unclear orange indicator with a recognizable warning icon when Connection State Indicator (CSI) detects network issues.

> **Note:**
>
> When you use Citrix Workspace app for HTML5 version 2509 or later, this feature is automatically enabled for desktop sessions and requires no client-side configuration.

Enhanced desktop launch experience

Starting with version 2411, Citrix Workspace app for HTML5 ensures an enhanced desktop launch experience. You experience a seamless, flicker-free transition to your desktop without intermediate screens. The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

Enhanced virtual desktop screen resizing experience

Starting with the 2411 version, Citrix Workspace app for HTML5 ensures a smooth transition and prevents dark screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

Enhanced seamless app launch and resizing experience

Starting with the 2502 version, Citrix Workspace app for HTML5 ensures an enhanced app launch experience. You experience a seamless, flicker-free transition to your apps without intermediate screens. The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

Support for horizontal scrolling on trackpad

Starting with the 2502 version, horizontal scrolling using the trackpad is supported within the session.

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

Disable downloading of Citrix Workspace app logs in error dialogs

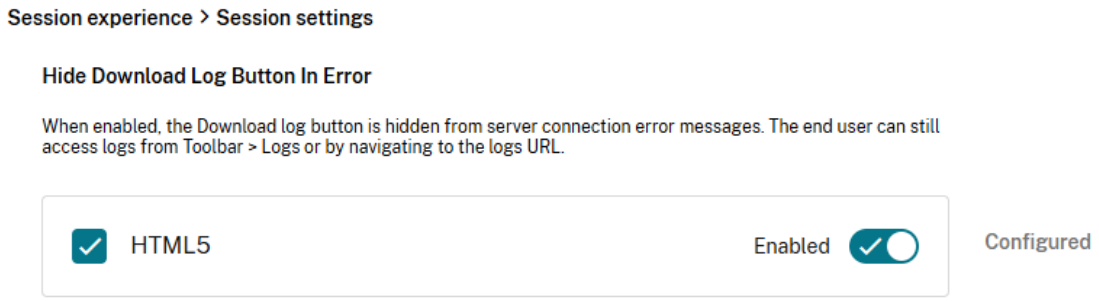
Starting with the version 2505, admins can hide the **Download Log** button in all error dialogs for both app and desktop sessions in Citrix Workspace app for HTML5 (cloud and on-prem).

> **Note:**
>
> This feature is disabled by default. In other words, the user has an option to download logs from the error dialog.

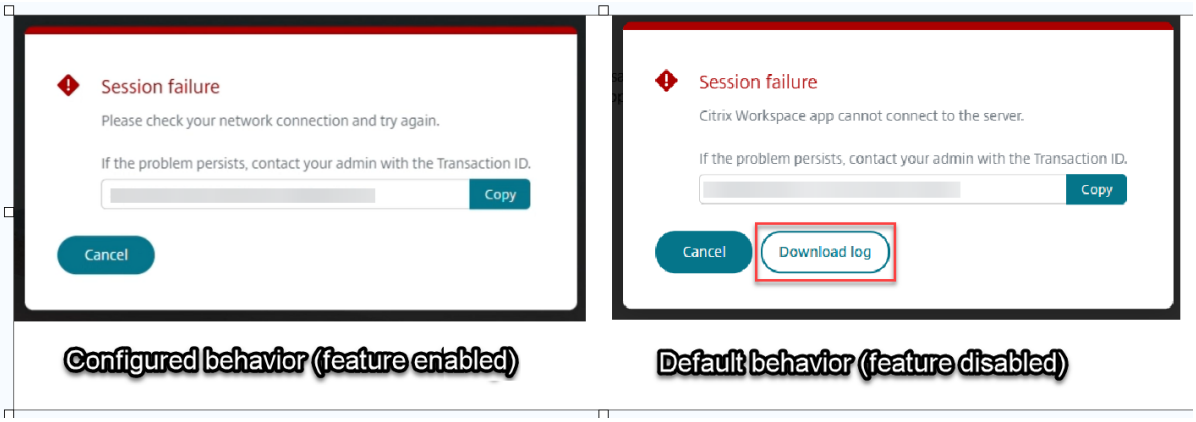
How to configure

This feature is disabled by default. You can enable the feature using the Global App Configuration service.

Global App Configuration service Administrators can enable this feature by navigating to **Workspace Configuration** > **App Configuration** > **Session Experience** > **Session settings** > **Hide Download Log Button In Error**. Select the checkbox and respective toggle button to disable downloading of logs.



When enabled, users can't see the **Download log** button in error dialogs. However, users can still access logs from the toolbar using the **Collect logs** option unless this option is also disabled.



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

In cases where both **Collect logs** from toolbar and in **Download logs** in error dialog is hidden, logs can still be accessed with the logs URL like: `https://<storeurl-with-path>SessionWindow.<version>.html#engineType=log`

> **Important:**
>
> To fully restrict log access, you must disable the **View logs** setting and enable the **Hide Download Log Button In Error** setting in Global App Configuration service.

Use case

Using Citrix Workspace app for HTML5 in kiosk mode where access to native application is restricted, users can inadvertently access Windows Explorer of the client device when trying to download logs from error dialogs.

Troubleshooting

Problem: The **Download Log** button still appears after you enable the setting.

Cause: There might be a delay in Global App Configuration Service settings propagation, or the local-Storage on the client isn't updated.

Solution: Clear your browser cache and localStorage to ensure that the latest settings are fetched by the client.

Multi-monitor

May 7, 2026

Multi-monitor support

Previously, the multi-monitor display feature allowed you to open an extra browser tab of the desktop or app session that you were connected to. You were able to drag the additional browser tab to the external monitor.

Now, Citrix Workspace app supports multiple monitors with one click without manual intervention. If there are no external monitors attached to the device, the multi-monitor icon on the in-session toolbar is hidden. When you connect an external monitor with the required permissions, the multi-monitor icon is visible. After you click the icon, you can see the window span across all the connected monitors.

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

This feature is enabled by default.

To disable the feature, edit the **configuration.js** file. The **configuration.js** file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit the **configuration.js** file and set the value of the **trueMMSupportForHTML5** property to **false**.

For example,

```
```
var HTML5_CONFIG =
{

    'features': {

        'graphics': {

            'multiMonitor': true,
                'trueMMSupportForHTML5': false
                    }

                 }

 }
 ;
```
```

> **Note:**
>
> - When you disable the feature, you continue to see the old behavior. You can see an extra browser tab of the desktop or the app session when you click the multi-monitor icon.

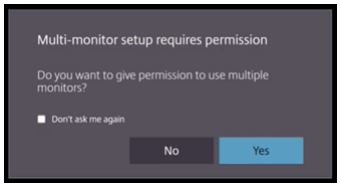
The multi-monitor feature supports the following:

- You can use up to two external monitors.
- You can use different display layouts of the multi-monitor.
- This feature is only supported on Google Chrome and Microsoft Edge Chromium browsers on Windows.
- The macOS devices support the older behavior. That is, when you click the **Multimonitor** icon on the toolbar, a secondary window of the desktop or application session appears to which you're connected. You can then drag the secondary window to the secondary monitor.
- You can use your virtual desktop in full-screen mode across a subset of available monitors. You can drag your virtual desktop to span to two monitors (out of more than two) and then select multi-monitor mode. A typical use case for this scenario is:
    - when you 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.

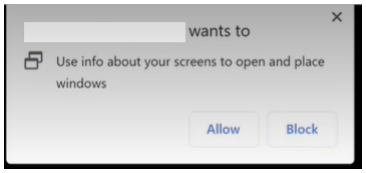
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To use the feature

1. As a first-time user, when you start a session, the following pop-up appears seeking your permission to use the multi-monitor setup.

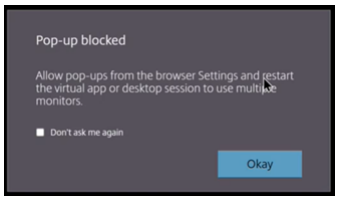


2. Click **Yes**.



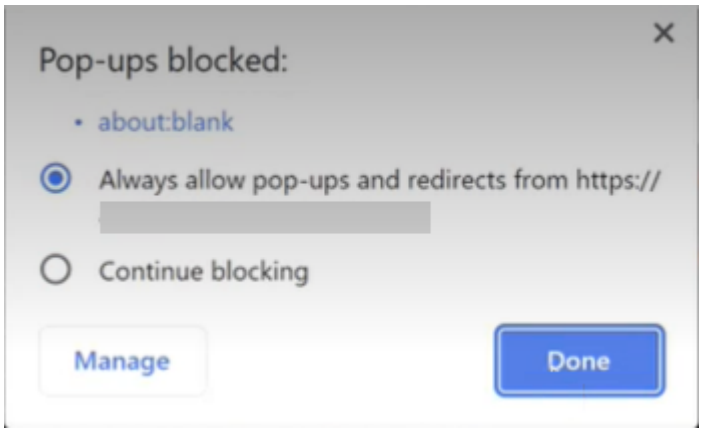
The pop-up appears from the browser to seek permission to use multiple monitors. If you click **Block**, you can't use multiple monitors.

3. Click **Allow**.



The pop-up appears to let you know about the pop-up blockers.

4. Click **Okay**. Navigate to the browser settings and select **Always allow pop-ups**.



5. Click **Done**.

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

> **Note:**
>
> Make sure to restart the session for the changes to take effect.

6. On your primary monitor, click the multi-monitor icon .

   You can see the window span across all the connected monitors.

> **Important:**
>
> If you deny multi-monitor permissions, the multi-monitor icon doesn't appear. Instead, the full-screen icon appears on the toolbar, which takes you to the older behavior. To manually re-enable the multi-monitor permissions, go to the browser **Settings** > **Privacy and security** > **Site Settings** > **Permissions** > **Additional permissions**, and allow **Window placement**.

Notes

- On the external monitor, resource windows aren't in full-screen mode. Instead, it is in windowed mode with a size equal to the external monitor size. We recommend manually switching to full-screen for a better user experience on each of the external monitor windows. Use the F11 key on Windows. On your Mac, move the pointer to the green button in the top-left corner of the window, then choose **Enter Full Screen** from the menu.
- Multi-monitor state isn't remembered across sessions on different devices. So, you must manually click the multi-monitor icon on the toolbar for every session.

Known limitations in the feature

- In a multi-monitor setup, the session gets restored to the single monitor mode when:
  - you use Microsoft Teams to share the screen on the primary monitor.
  - you select the **Logging** or the **Upload** option on the toolbar.
    Click the multi-monitor icon to continue using multiple monitors.

Multi-monitor support through the session toolbar

This feature is an old behavior that lets you create a secondary window of the desktop or application session to which you're connected. You can then drag the secondary window to the secondary monitor. The multi-monitor display feature is available for both desktop and application sessions.

To use the multi-monitor display feature, do the following:

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

1. Click the **Multimonitor** icon on the session toolbar.



   A secondary window with a 1024x768 resolution appears. It also updates the server with the dual monitor information.

2. You can now drag and resize the secondary window and even go to full-screen mode on one or both monitors.

   Every time you resize the window, the secondary window resolution is updated on the server.

   To exit multi-monitor mode, close the secondary window.

Even though the resolution details of the secondary monitor are unknown to Citrix Workspace app, multi-monitor mode gives you the flexibility of resizing to adjust to the resolution.

For the session to take focus, click the **Multimonitor** icon on the toolbar.

This feature is enabled by default.

To disable the feature, edit the **configuration.js** file and set the value of the **multiMonitor** property to **false**.

```
    'ui' : {

        'toolbar' : {

            'multiMonitor' : false
             }

         }
,
```

Using Citrix Virtual Desktops™ on dual monitors:

1. Click **Multimonitor** in the toolbar.
2. An extended window is created. Drag the window to the extended monitor.

   The screen is now extended to both the monitors.

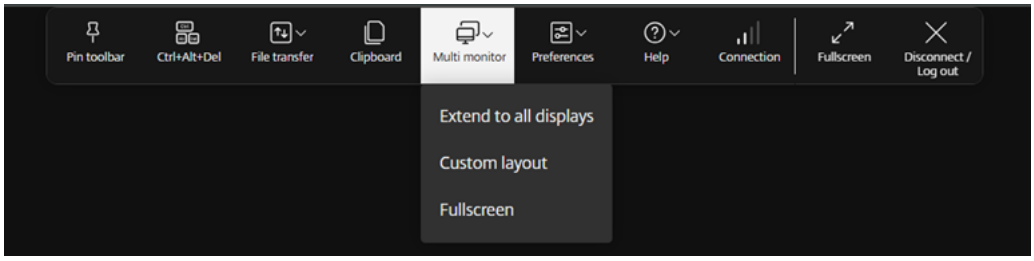
Known limitations in the feature

- On a macOS device, the secondary window opens as a new tab in Chrome.

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

Enhanced multi-monitor support with auto-detection and custom display selector

Starting with version 2505, new options have been added under **Multi monitor** icon in the toolbar, which appears only when more than one screen is connected. The multi-monitor selector allows users to choose which displays to use in full-screen mode for app and desktop sessions.



As long as the layout remains the same at the client OS, it is remembered when you disconnect and reconnect to the same session.

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

System requirements

This feature is only supported on Google Chrome and Microsoft Edge Chromium browsers on Windows OS.

Prerequisites

- Ensure that the new toolbar feature is enabled. For more information, see Improved in-session toolbar.
- Allow permissions:
  - **Window management permission** that is important for websites that must access information about different monitors and manage windows across them
  - **Browser pop-up permission** to manage whether websites can open new windows or tabs without your direct interaction.

Known limitations

- On the external monitor, resource windows aren't in full-screen mode. Instead, it is in windowed mode with a size equal to the external monitor size. We recommend manually switching to full-screen for a better user experience on each of the external monitor windows.

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

To switch fullscreen, use the F11 key on Windows and your Mac, move the pointer to the green button in the top-left corner of the window, then choose **Enter Full Screen** from the menu.

- The multi-monitor selection is not saved between sessions. You must manually select your preferred monitors each time you start a new session by clicking the multi-monitor icon on the toolbar.
- Multi-monitor state goes into single monitor **Fullscreen** state by default on external monitor layout change when the session is in active state.

For more information on how to configure, see Enhanced multi-monitor support with auto-detection and custom display selector.

High DPI support for multiple monitors

Citrix Workspace app for HTML5 supports DPI scaling for app and desktop sessions on single and multi-monitor sessions. This feature is mostly used with large-size and high-resolution monitors to display applications, text, images, and other graphical elements in a size that can be viewed comfortably.

> **Note:**
>
> This feature is enabled by default for app and desktop sessions.

Benefits

This feature automatically adjusts virtual desktop and app sessions based on device DPI, ensuring content appears perfectly sized and sharp without blurriness. Apps and desktops are intelligently scaled based on monitor resolution and device pixel ratio for optimal readability and usability.

For more information about how to configure, see High DPI support for multiple monitors.

Generic Client IME enhancement for Citrix Workspace app for HTML5 on Chromebook with multi monitors

Previously, enabling the multi-monitor configuration for the IME resulted in duplicate input on secondary displays in ChromeOS.

With the 2509 version, we now use the browser API to manage the relationship between key and input events, preventing duplicate characters from being entered per keystroke.

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

Multimedia

September 18, 2026

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.

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

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 value to true to enable stereo recording for the Google Chrome browser 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 the Google Chrome browser with echo cancellation disabled. The Apple Safari and Mozilla Firefox browsers can't support stereo recording.

How to Configure

You can configure the adaptive audio feature as follows:

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure adaptive audio.

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

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To configure adaptive audio:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **EnableAdaptiveAudio** attribute and set the attribute to **true**. Add the **EnableStereoRecording** and set the attribute to **false**. For example,

```
'features' : {

  'audio' : {

    'EnableAdaptiveAudio': true
             }

           }
```

```
'features' : {

  'audio' : {

    'EnableStereoRecording': false
           }

         }
```

1. Click Save.

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

Known limitations in the feature

- The Mozilla Firefox browser doesn't support resampling for recording. In some abnormal cases, recording on Mozilla Firefox might fail.

  The adaptive audio support for recording is disabled when the Mozilla Firefox browser is used.
- The Apple Safari and Mozilla Firefox browsers don't support stereo recording because of a limitation in the browser.

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

Plug and Play audio device support

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

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

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

How to configure

You can use **configuration.js** to configure this feature as follows:

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the feature:

1. Navigate to the **configuration.js** file.

   > **Note:**
   >
   > The **configuration.js** file is located under the `C:\Program Files\Citrix\HTMLClient` folder.

2. Edit the file and locate the **AudioRedirectionV4** attribute. Set the attribute to **false**.

   For example,

   ```
   'features' : {

       'audio' : {

           'AudioRedirectionV4': false
                }

        }
   ```

3. Save the changes.

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

Known limitations in the feature

- On the VDA, the name of the built-in audio device is in English only. The issue occurs when you use ChromeOS-based devices. [RFHTMCRM-8667]
- This feature is supported on Microsoft Chromium Edge and Google Chrome browsers only.

Webcam

Citrix Workspace app supports webcam optimizations for both 32-bit and 64-bit applications with built-in webcams.

Webcam redirection

To configure webcam redirection:

1. Open the **configuration.js** file.
2. Navigate to **HTML5_CONFIG** > **features** > **video** > **config** > **codecType**.

   > **Note:**
   >
   > - The Google Chrome and Microsoft Edge Chromium browsers use both hardware and software codecs. The Mozilla Firefox and Apple Safari browsers use only software codec.

3. Select the **codecType** value:

- 1 - HARDWARE_CODEC with SOFTWARE_CODEC fallback (default)
- 2 - Only SOFTWARE_CODEC
- 3 - Only HARDWARE_CODEC

Enhanced support for webcam redirection

Webcam redirection support is available not just for Google Chrome and Microsoft Edge (Chromium) browsers, but it also available on Mozilla Firefox and Apple Safari browsers.

Microsoft Teams optimization

Microsoft Teams optimization supports audio call, video call, and screen sharing functionalities on the Google Chrome browser only. The minimum Google Chrome version required is m97 and later.

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

> **Note:**
>
> - The Microsoft Teams optimization applies to the Microsoft Teams desktop version and not the web version on the VDA.
> - The screen sharing functionality is enabled by default.

Feature limitation:

- When you use Microsoft Teams optimization and share the screen, a red border that indicates the screen sharing is unavailable. [RFHTMCRM-6360]
- When you use Microsoft Teams optimization, the screen sharing functionality is disabled by default. After you enable it, you can share the local device contents. [RFHTMCRM-6156]

Known issues in the feature:

- Microsoft Teams optimization is supported on the Google Chrome browser only. [RFHTMCRM-6194] [RFHTMCRM-4724]

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

Screen sharing

Starting with version 2209, by default, the screen sharing is enabled. The end users can now share apps and tabs that are opened through Citrix Workspace app. During screen sharing, the blue border appears around the shared window.

To share the entire screen, administrators can edit the **configuration.js** file located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder and change the **shareAllContent** attribute to **true**. When this feature is on, the end users can share the entire screen including the resources that aren't opened from Citrix Workspace app.

For example,

```
    'msTeamsOptimization':{

                        'screenSharing' : true,
                        'shareAllContent' : true
                        'seamlessApps' : true,
                        'webcamSupportInMM' : true,
                        'originTrialToken' : {

                                'chrome': "",
                         }
,
                         }
```

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

Give or Take Control in Microsoft Teams Optimization

Starting with version 2607, you can manage screen sharing control during meetings. This feature allows participants to interact with a shared screen using keyboard, mouse, and clipboard input.

You use the **Give control** button to grant control of your shared screen to other meeting participants. You and the other participant both control the shared screen. You can take back the control at any time.

During a screen sharing session, any participant can request control access through the **Request control** button. The screen sharer can approve or deny this request. When you have control, you manage the keyboard and mouse input on the shared screen. Release control to stop sharing control.

You can use screen sharing control in the following scenarios:

- Sharing a Citrix Workspace app tab through Chrome's **Chrome Tab** picker, including the main session tab or any secondary or extended-display tab.

The screen sharing control is unavailable in the following scenarios:

- Sharing content outside the Citrix session, for example, a non-Citrix Workspace app browser tab.
- Sharing an **Entire screen** or an **Application window** through Chrome's picker.

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:

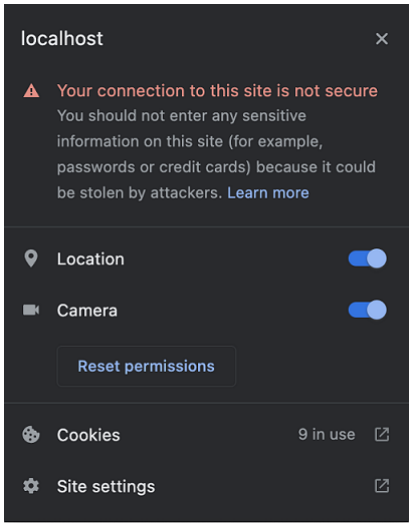
- configure and route emergency calls
- notify security personnel

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 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 2202 for HTML5, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law.

For Microsoft Teams optimization e911 calling, enable **Location** access as shown:

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



Background blurring and effects in Microsoft Teams optimization

Starting with the 2303 release, Citrix Workspace app for HTML5 supports background blurring and effects in Microsoft Teams optimization for video calls. You can either blur or replace the background effects provided by Microsoft Teams to avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). This feature can be used with P2P and conference calls.

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

Known limitations in the feature

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

How to configure You can configure the background effect feature as follows:

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file

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

to configure the background effect feature.

> **NOTES:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To enable background effect:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **backgroundEffects** attribute and set the attribute to **true**. For example,

```
'features' : {

        'msTeamsOptimization' :
        {

            'backgroundEffects' : true
         }

    }
```

3. Save the changes.

Multi-window chat and meetings for Microsoft Teams

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

For details about the pop-out window feature, see Pop out a chat in Microsoft Teams. For troubleshooting see, CTX253754.

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

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

Live Captions in Microsoft Teams

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

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

Support for secondary ringer

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

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

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

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

How to configure You can enable the secondary ringer feature in the following way:

Configuration.js

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before making changes.
> - Administrator-level credentials are required to edit the **configuration.js** file.

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

1. Navigate to the **configuration.js** file.

   > **Note:**
   >
   > The **configuration.js** file is located under the `C:\Program Files\Citrix\HTMLClient` folder.

2. Edit the file and set the value of **secondaryRingtone** to **true**.

   The following is an example of JSON data:

```
{

    'features':{

        'msTeamsOptimization':{

            'secondaryRingtone' : true
             }

         }
```

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

```
11
12
13  }
```

3. Save the changes.

Simulcast implementation for optimized Microsoft Teams video conference calls

Starting with the 2312 release, by default, simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved. We're adapting to the proper resolution for the best call experience for all callers.

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

Default audio device selection

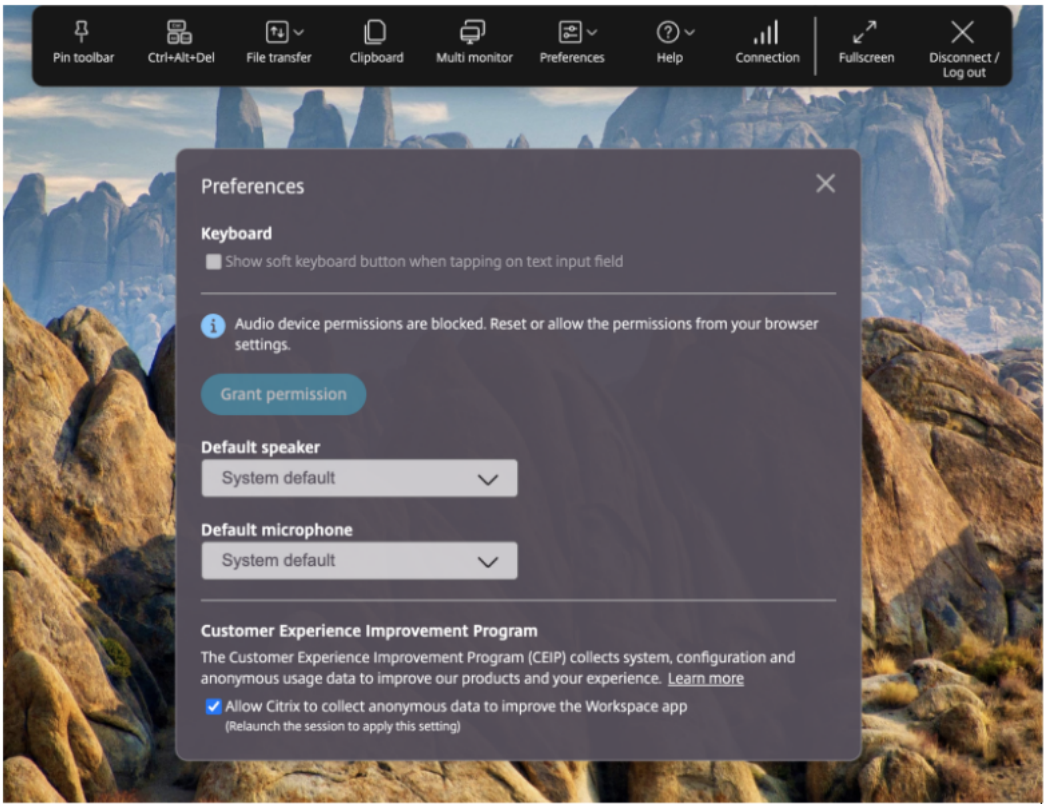
Starting with version 2511, Citrix Workspace app for HTML5 lets users select and save their preferred audio speaker and microphone devices from the session toolbar for each VDA.

About this feature This feature offers a more customized audio experience with the following key features when connected to a virtual desktop:

- **Device selection:** Users can assign different input and output audio devices to different VDAs. For example, you can have two different VDAs, each using a separate default speaker (one built-in speaker and one headset). The exact audio device can be selected for each active VDA from the **Preferences** section. The selected device becomes the default device from the same session.
- **Configuration persistence**: The system preserves the selected configuration for the next session, ensuring a seamless experience.
- **Microphone permission:** Users must grant microphone permission to select default audio devices. If the permission is in the "prompt"state (neither granted nor denied), users must grant access. If the permission is **denied**, users must reset the permission before granting access.

If microphone permission is ***denied**, default audio device selection is disabled and the following dialog appears:

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



Notes:

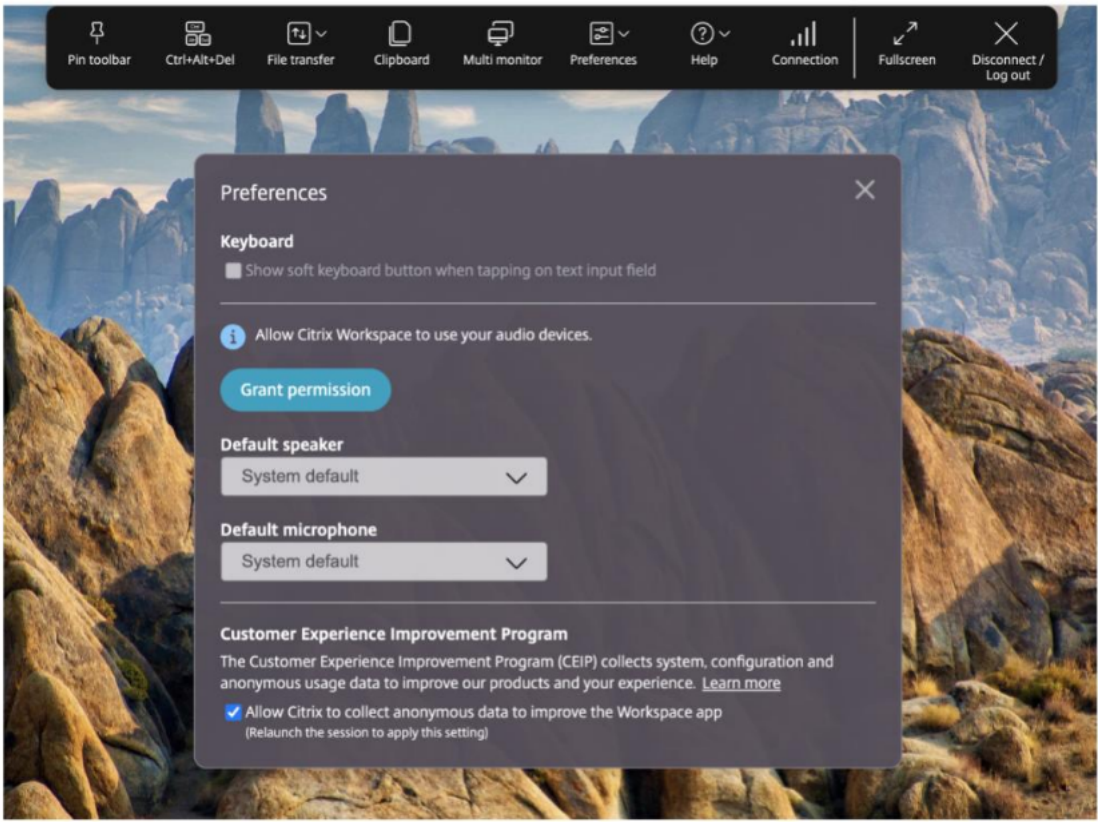
- Users can adjust settings in the **Preferences** section to prevent the system from preserving the selected configuration for the next session.
- This feature does not apply to pooled desktop environments because users connect to different VDAs each time they sign in.
- When you use Citrix Workspace app for HTML5 in incognito mode, the default audio device settings isn't retained.

Prerequisites Enable the Plug and play audio device support feature (enabled by default). If the feature is disabled, see Plug and play audio device support configuration to enable it.

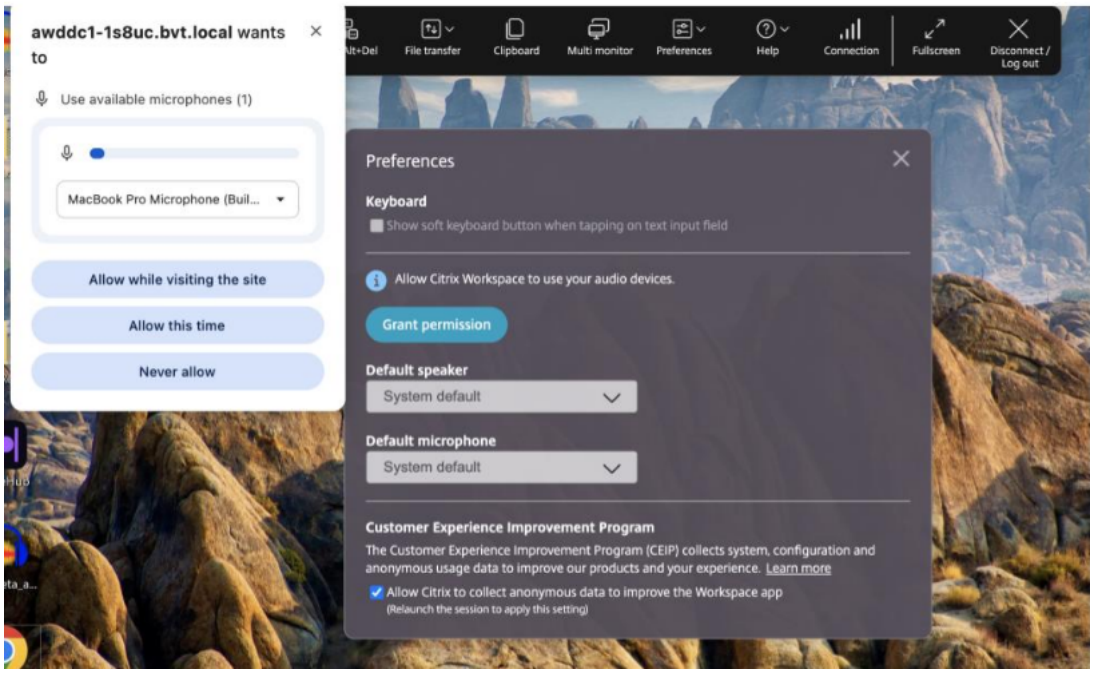
How to enable microphone permission When microphone permission is in the **prompt** state, default audio device selection is disabled. To grant permission, follow these steps:

1. Click **Grant Permission** from the **Preferences** dialog.

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



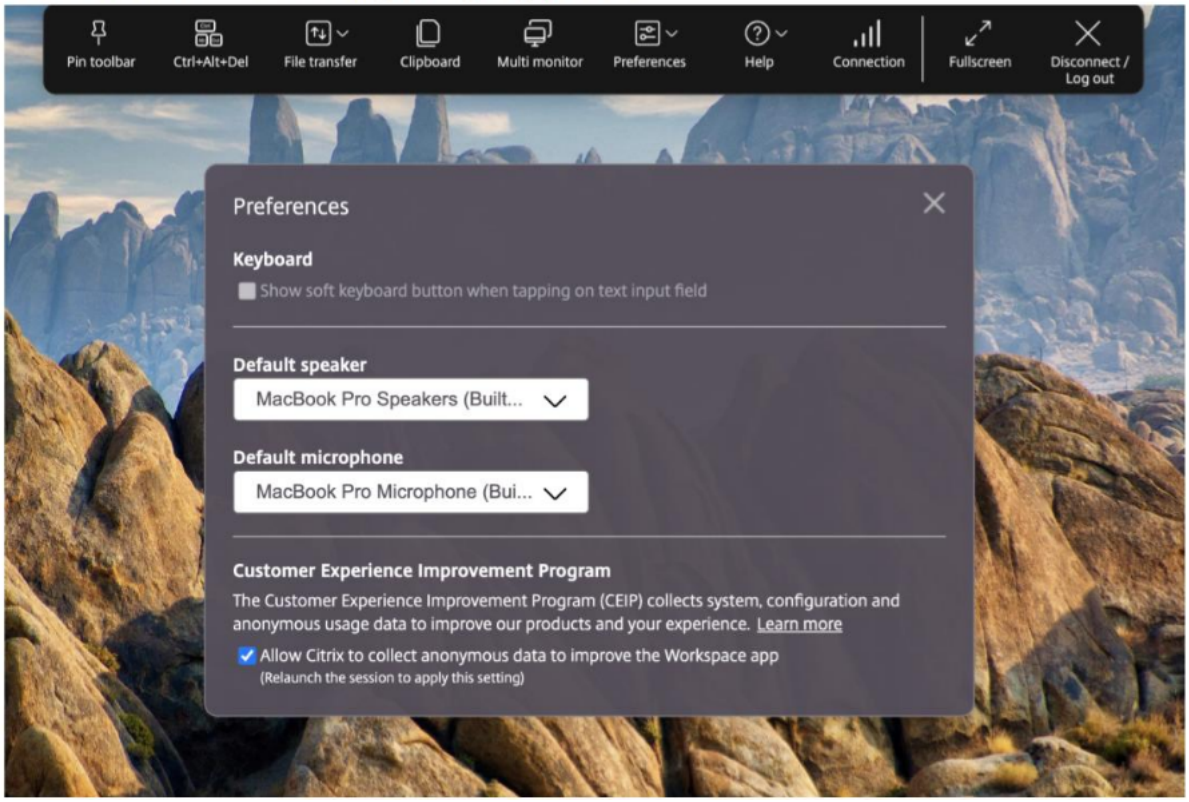
1. Allow microphone access using the browser permission pop-up.



How to select specific audio devices To select the specific audio device, do the following:

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

1. Navigate to the **Preferences** section on the session toolbar.
2. Click **More**. The following image appears:



1. Select the device that you want from the **Default speaker** drop-down list.
2. Select the device that you want from the **Default microphone** drop-down list.

> **Note:**
>
> If the selected audio device for a VDA becomes unavailable or is unplugged, the session automatically switches to the client's endpoint-assigned default audio device.

Known limitations in the feature

- This feature is not applicable for published applications and mobile session launches.
- The feature is not applicable to the Mozilla Firefox browser in macOS.
- The feature doesn't list audio output devices in the Apple's Safari browser.

Audio quality improvement with reliable transport protocols

Starting with version 2603, Citrix Workspace app for HTML5 delivers enhanced audio redirection that creates a smoother and more consistent audio playback and recording experience. The application

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

improves audio quality, particularly when you use reliable transport protocols such as TCP and EDT Reliable.

About this feature

This feature delivers significant improvements to audio performance with the following key benefits:

- **Improved audio quality**: The application processes audio more effectively and delivers clearer sound with less distortion during playback and recording sessions.
- **Consistent audio experience**: Reliable transport protocols maintain stable audio streaming with fewer interruptions or dropouts.
- **Optimized for reliable transports**: The enhancement performs better when you use TCP and EDT Reliable transport protocols, delivering more predictable audio.
- **Seamless user experience**: Users experience smoother audio transitions and better overall session quality without configuring additional settings.

Prerequisites

To use this feature, ensure that you enable the **Adaptive Audio** feature (enabled by default).

For more information about audio configuration, see Adaptive audio.

HDX™ transport

September 7, 2025

HDX adaptive throughput

Starting with the 2408 version, HDX adaptive throughput is supported. This feature intelligently fine-tunes the peak throughput of the ICA® session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high-latency networks.

This feature provides better interactivity, faster file transfers, smoother video playback, and a higher frame rate and resolution resulting in an enhanced user experience.

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

Session interactivity is constantly measured to determine whether any data streams within the ICA session adversely affect interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

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

Touch and mobility support

June 11, 2026

Mobility support

To enable the auto-soft keyboard popup

To enable this feature, configure the automatic keyboard policy to display the soft keyboard when clicking any editable area:

1. On the DDC machine, open **Citrix Studio**.
2. Select **Policies**.
3. Click **Create Policy**.
4. Search for **Automatic Keyboard Display** and select **Allowed**.

> **Note:**
>
> You can enable the auto-soft keyboard popup when no physical keyboard is connected.

Combo box support on mobile platforms

Starting with the 2303 version, selecting UI elements within a combo box on small screens is smoother. An administrator can enable the policy **Remote the combo box** to make the user experience of selecting checkboxes, drop-down list options, radio buttons, and more a smooth experience on iOS and Android mobiles.

For more information, see the Remote combo box section in the Citrix Virtual Apps and Desktops documentation.

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

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

How to configure

You can configure the enhanced touch experience in one of the following ways:

- Configuration.js
- Global App Configuration service

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the enhanced touch experience feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To disable the enhanced touch experience feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **enablePointerForTouchEvents** attribute and set the attribute to **false**.

   For example,

```
'ui':
    {

        'touch':
          {

              'enableMobileComboBoxRedirection': false
           }

     }
```

3. Save the changes.

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

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

Gesture enhancements on touch devices

Starting with the 2304 version, Citrix Workspace app enhances the end user experience for:

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

- gestures, multi-touch, and soft keyboard functionality on mobile devices.
- soft keyboard functionality on Tablet mode.

In your Citrix Workspace app sessions, you can use all the familiar multi-touch gestures, including the tap, swipe, drag, pinch, and zoom.

The following is the gesture guide:

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

Automatic display of virtual keyboard

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

Reference article

- Keyboard

Multi-touch mode

Citrix Workspace app for HTML5 allows you to set **Multi-touch** as the default mode through configuration.js. Multi-touch mode controls whether to enable multi-touch gestures.
Starting with the 2509 release, **Multi-touch** mode is set as the default touch mode for desktop form factors, while Panning mode is the default for mobile form factors.
You can toggle between Panning mode and Multi-touch mode using toolbar option in the desktop session. Administrators can also change the default option by editing the configuration.js and set the value of **defaultMode** to '**multitouch**'/'**panning**'.

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

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"
                                     }

                                }

                             }

                         }

                     }

                 }
```

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is in the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to configure the enhanced touch experience feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To set the default:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **defaultMode** attribute and set the attribute to **multitouch** or **panning**.
   For example,

```
'ui':
    {
```

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

```
3
4          'touch':
5            {
6
7              "defaultMode" : "multitouch"
8             }
9
10       }
```

3. Save the changes.

Printing

September 7, 2025

PDF printing

Enhanced PDF printing experience

The Citrix PDF Universal Printer driver enables users to print documents that are opened with hosted applications. Many a time it can be apps that run on virtual desktops delivered by Citrix Virtual Apps and Desktops. When a user selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. To print the document, the **Print** dialog box appears within your Citrix Workspace app session.

> **Note:**
>
> This enhancement is fully supported and enabled by default in the Google Chrome and Mozilla Firefox browsers.

To disable it in the Google Chrome and Mozilla Firefox browsers, set the value of **supportedBrowsers** to **false** in the **configuration.js** file. The **configuration.js** file is located under `C:\program Files\Citrix\<actual path>\HTML5Client`.

```
1     'pdfPrinting' : {
2
3         'directPrint' : {
4
5            'supportedBrowsers':false,
6                  }
7
8             }
```

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

Optimized resolution In earlier versions, content in a document appeared blurry when you attempted to print the document using the Citrix PDF printer.

We now introduce optimizations to improve the user experience. The `printResolution` value defaults to 150. Also, for crisper content, you can change the value in the `configuration.js` file to 300 or 600 depending on your requirement:

```
    'pdfPrinting' : {

        'directPrint' : {

            'printResolution' :150  }

     }
```

Known limitations in the feature

This enhancement isn't supported for sessions that are launched through the HTML5 HDX™ SDK.

To suppress the Continue print dialog When the enhanced printing experience feature is disabled, you can print a PDF by suppressing the appearance of the **Continue** print dialog.

By default, the **printDialog** property of the **hide** object is set to **false.**

The **configuration.js** file is located under `C:\program Files\Citrix\<actual path>\HTML5Client`.

To print, set the **printDialog** property of the **hide** object to **true**.

> **Note:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Citrix recommends using this method only if Citrix Workspace app for HTML5 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.

```
    {

       'ui' : {

         'hide':{

            'printDialog': true
          }

        }
```

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

```
11
12          }
```

Blocking PDF printing

As an administrator, you can now block PDF printing on the following browsers across platforms: Google Chrome, Mozilla Firefox, Apple Safari, and Microsoft Edge (including Microsoft Edge Chromium).

By default, PDF printing is allowed across all browsers. To prohibit PDF printing, follow these steps:

1. Navigate to the **configuration.js** file, available at `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client`.
2. Edit that file and set the value of disableForBrowsers to **'ALL'**.
    - To disable PDF printing on specific browsers, set the value of **disableForBrowsers** to **'Chrome'**, **'FIREFOX'**, **'SAFARI'**, **'CHROMIUMEDGE'**, or **'MSEDGE'**.

```
1       'pdfPrinting' : {
2
3           'disableForBrowsers' : ['All']
4        }
```

Or

```
1       'pdfPrinting' : {
2
3           'disableForBrowsers' : ['Chrome', 'CHROMIUMEDGE', 'MSEDGE']
4                           }
```

The following describes each of the values in detail:

- 'MSEDGE': All the versions of Microsoft Edge
- 'CHROMIUMEDGE': All the versions of Microsoft Edge Chromium
- 'Chrome': All the versions of Google Chrome
- 'FIREFOX: All the versions of Firefox
- 'SAFARI': All the versions of Safari

To configure PDF printing

> **Note:**
>
> The following section explains the old behavior about how to configure PDF printing.

The Citrix PDF Universal Printer driver enables users to print documents that are opened with hosted applications. Many a time it can be apps that run on virtual desktops delivered by Citrix Virtual Apps

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

and Desktops. When a user selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. You can now open the PDF in a new browser tab to view and print from a locally attached printer.

If you want to **Auto-create PDF Universal Printer** users to print documents that are opened with hosted applications or applications that run on virtual desktops delivered by Citrix Virtual Apps and Desktops, do the following:

1. 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.
2. Set the **Auto-create PDF Universal Printer** policy setting to **Enabled**.

> **Note:**
>
> When you use a Citrix PDF printer in a session launched from Citrix Workspace app for HTML5, set the **Client printer names** setting as default or select **Standard printer names**. Select **Legacy printer names** to use old-style client printer names and to preserve backward compatibility with legacy printer names as present in the Citrix Virtual Apps and Desktops of the product. You can use this option with the current Citrix Virtual Apps and Desktops and Citrix DaaS versions of the product.

To configure with the CSP header added

PDF printing works, unless a Content-Security-Policy (CSP) header is added for users.

The CSP response header is a combination of policies that a browser uses to avoid Cross-site scripting attacks.

If the CSP *header* is added to Citrix Gateway *Rewrite Policies*, PDF printing doesn't work.

Configure as follows:

```
img-src \'self\' data: blob:
```

(**blob:** This parameter allows print preview to load and continue with printing functionality)

deviceTRUST

September 21, 2026

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

Integration of deviceTRUST with Citrix Workspace app for Html5

Starting with version 2607, Citrix Workspace app for HTML5 supports deviceTRUST integration, enhancing security through continuous device posture checks within sessions.

> **Note:**
>
> The minimum Citrix Virtual Apps and Desktops version required for deviceTRUST is 2607.

About the feature

deviceTRUST provides continuous device posture monitoring and assessment capabilities for browsers accessing Citrix environments. The integration uses web-based APIs to collect device information and enforce security policies based on device compliance status.

> **Note:**
>
> For more information about deviceTRUST, see deviceTRUST Platform.

Supported device properties The following device properties (signals) are available for Html5 platform configuration in the deviceTRUST console:

Html5

- **Browser:** Details of Browser
- **Platform:** Details of the platform (Windows/ Mac and so on) on which the browser is running
- **UserAgent:** userAgent details of browser
- **Version:** Browser version

Display

- **Count:** No of display units connected to device
- **BPP:** Color detail per pixel (color depth)
- **DPI:** Pixel density; sharpness of the display
- **Height:** Vertical pixel or physical size of the screen
- **Width:** Horizontal pixel or physical size of the screen
- **Monitor External:** Any external monitor connected to device

Location

- **Position:** The reported geographic location (latitude, longitude)
- **Accuracy:** Value indicating how precise the position

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

> **Note:**
>
> This is a real-time property that is updated whenever there is any change in the location.

Input

- **Keyboard:** Indicates whether the keyboard is connected in the device
- **Mouse:** Indicates whether the mouse is connected to the device
- **Pen:** Indicates whether the device has pen connected
- **Touch:** Indicates whether the device supports touch functionality

Power

- **AC:** Indicates whether power adapter is connected to device
- **Battery:** Indicates battery level (Critical/ High/ Medium/ Low)

Region

- **Locale:** Regional settings that define formats for language
- **Language:** The language used for text and UI Timezone Offset

Name

- **Name:** Device host name

Operating system properties

- **Type:** Client device type

Session properties

- **Idle Period:** Indicates the time interval for which there is no user interaction with Citrix session. The interval span is set by admins through device trust console

Benefits This integration provides:

- **Continuous security monitoring** - Real-time device posture assessment during active sessions
- **Policy enforcement** - Automated responses based on device compliance status
- **Enhanced visibility** - Comprehensive device information for security administrators
- **Seamless user experience** - Transparent security checks without user intervention

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

Troubleshoot

May 7, 2026

HTML5 logs

Citrix Workspace app for HTML5 provides timestamps for the logs generated by the user device.

> **Note:**
>
> - To assist with troubleshooting issues, you can view Citrix Workspace app for HTML5 session logs.

The log page allows users to:

- **Enable Logging:** Enable logging to view the HMTL5 logs.
- **Disable Logging:** Disable logging to stop logging in a session.
- **View logs:** View the logs generated for a session.
- **Clear logs:** Delete the log file generated in a session.
- **Download log file:** Download the log file to a desired location.

Citrix Workspace app supports log collection for ongoing virtual desktop and app sessions. Previously, you collected logs only for sessions launched after selecting **Start Logging** during an ongoing session. Now, the logs are collected for the ongoing and next sessions until you select **Stop Logging**.

Troubleshooting enhancement for mobile devices

You can get quick access to the session log file by tapping the **Get Logs** option. The logging option is renamed from **Logging** to **Get Logs**. When you select **Get Logs** from the secondary menu, the log file downloads on your device, unlike on a new browser tab.

> **Note:**
>
> You can collect logs for the ongoing session and a maximum of the previous five sessions.

How to collect logs

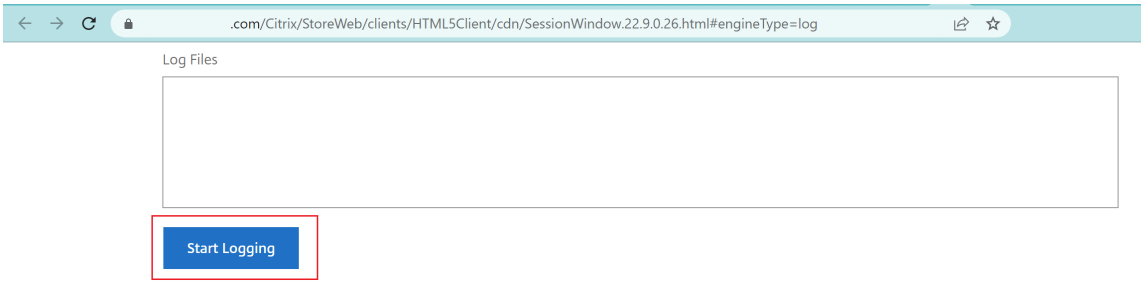
To collect Citrix Workspace app for HTML5 client logs, do the following:

1. Sign in to Citrix Workspace app for HTML5.
2. Access the Log files page as follows:

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

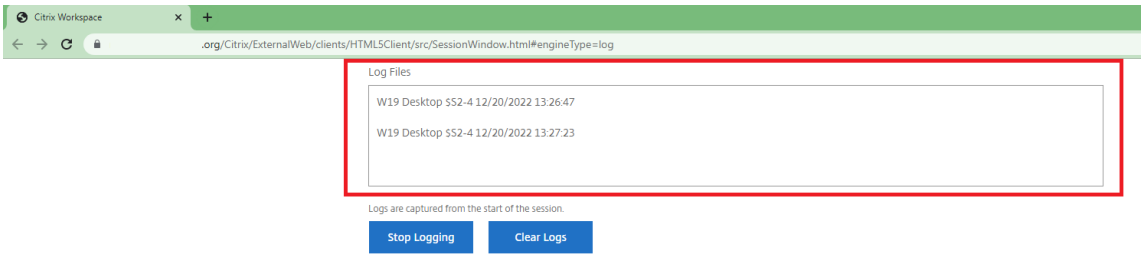
- For Citrix Workspace app versions 1908 and later, open a new tab and navigate to siteurl/-Clients/HTML5Client/src/SessionWindow.html#engineType=log, where **siteurl** is the URL of the Workspace for Web site, for example, `https://server.domain/Citrix/StoreWeb`.
- For Citrix Workspace app versions 1907 and earlier, open a new tab and navigate to siteurl/-Clients/HTML5Client/src/ViewLog.html, where **siteurl** is the URL of the Citrix Workspace for Web site, for example, `https://server.domain/Citrix/StoreWeb`.

3. On the **Log files** page, click **Start Logging**.

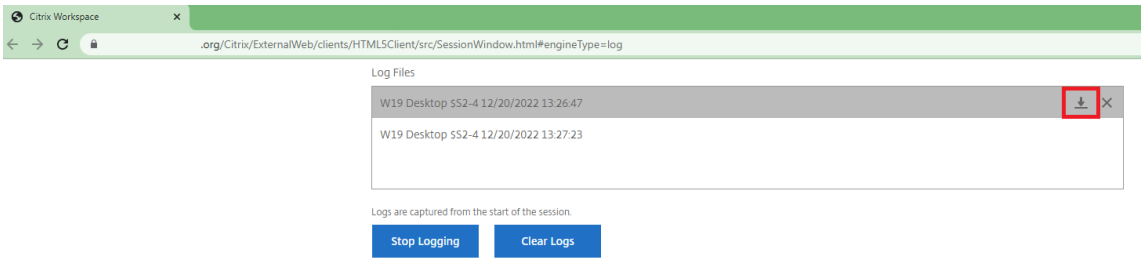


Logging is enabled for the next session launch, and not for the current active session (if any).

4. Sign in to the Citrix Workspace app and start your virtual app session and reproduce the issue to collect logs. Continue to work on the session to reproduce the issue.
5. Close the session once the problem is reproduced.
6. The log files generated for the Citrix Workspace app for HTML5 session are shown in the logging page.



7. Click the arrow button to download and save the Log file.



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

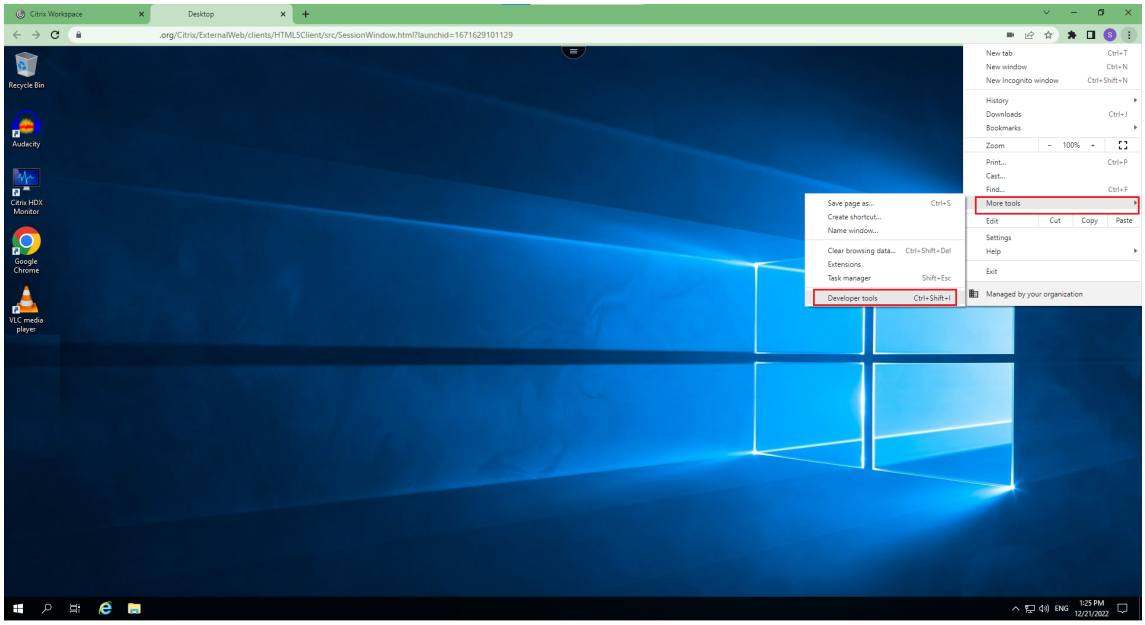
> **Note:**
>
> - To enable and view Citrix Workspace app for HTML5 logs, you can use the option **Logging** from the session toolbar menu.



How to collect console logs

To collect Citrix Workspace app for HTML5 console logs, do the following:

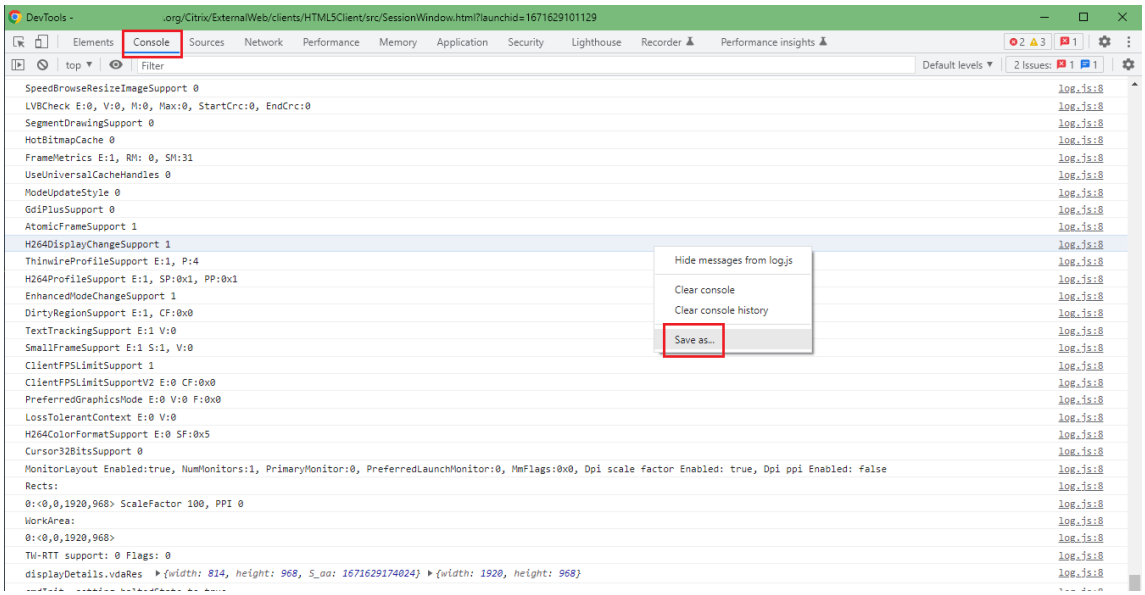
1. Open the Developer tools on the browser tab where the session is running. For example, on the Google Chrome browser, Developer tools can be found under the **More Tools** option.



2. Click **Console** in the opened developer tool.

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

3. Right-click and select the **Save as** option to save all the logs.



How to collect USB redirection logs

To enable logging and to collect logs for USB redirection-related issues, do the following:

Enable logs

1. Edit the `configuration.js` file and navigate to the HTML5_CONFIG section.
2. Add the value **moreLogs{'usb': true}**. This setting is relevant to the StoreFront.
   The `configuration.js` file is at `C:\program Files\Citrix <actual path>\HTML5Client`.

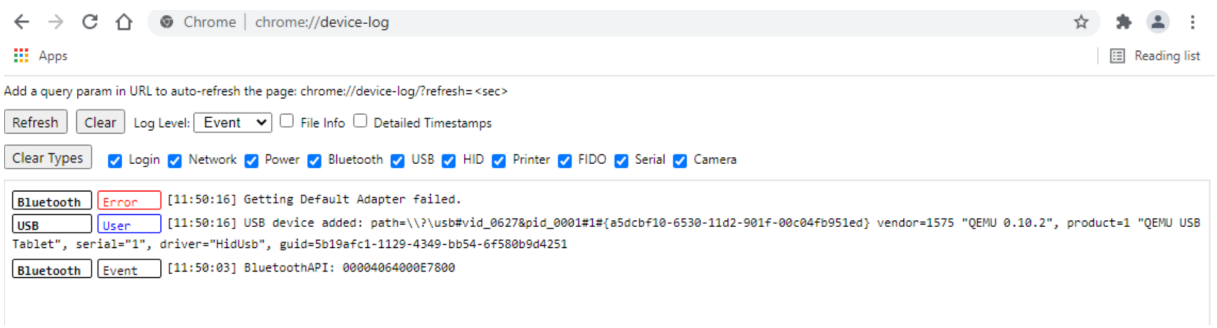
Collect logs

To collect logs, see How to collect logs.

Device logs

To collect device logs, open a new tab in the Google Chrome browser and enter **chrome://device-log** and share the logs.

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



How to collect Microsoft Teams optimization logs

Microsoft Teams optimization supports the latest shim library version 1.10.0.0.

To know the current shim version that you use:

1. Open the Microsoft Teams application and start a call with one of the users.
2. Maximize the Microsoft Teams window after the call is established.
3. Open the **On-screen keyboard** inside the session and click the **Ctrl + Alt + Shift + 1** keys.

   You can now view the log files under the downloads folder in the VDA.
4. Open the **MSTeams_Diagnostics Log <date><time>.txt** file and search for the shim version under **type_script**. For example, “version”:{“type_script”:”1.10.0.0”}.

Enhanced log collection

Starting with version 2411, users can download Citrix Workspace™ app logs in a zip file, simplifying log retrieval and analysis for better troubleshooting and an improved user experience.

The following are the benefits of the feature:

- Users no longer need to manually gather individual log files.
- The streamlined process makes accessing logs more efficient.
- Easy access to comprehensive logs aids in faster and more effective debugging.

Always On Tracing (AOT)

Citrix Workspace app for HTML5 now supports Always On Tracing (AOT), a modern diagnostic framework from Citrix that continuously captures relevant log data across the Citrix Virtual Apps and Desktops environment. This feature simplifies troubleshooting for IT administrators and Citrix support teams by automatically capturing log data for user sessions and system events, eliminating the need to reproduce issues.

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

AOT makes logs easily accessible and readable without engineering-level expertise, enabling self-service diagnostics to reduce dependency on Citrix Support and improve mean-time-to-resolution.

Benefits

AOT provides significant value to customers by:

- **Automatically capturing log data** for user sessions and system events without manual intervention
- **Eliminating the need to reproduce issues** since logs are continuously collected during normal operations
- **Making logs easily accessible and readable** without requiring engineering-level expertise
- **Enabling self-service diagnostics** to reduce dependency on Citrix Support
- **Improving mean-time-to-resolution** for troubleshooting scenarios

Use cases

AOT fits into your overall experience in the following scenarios:

- **Proactive monitoring:** Continuously monitor user sessions and system events to identify potential issues before they impact users
- **Rapid troubleshooting:** Access comprehensive log data immediately when issues occur, without waiting for log reproduction
- **Self-service support:** Enable IT administrators to diagnose and resolve common issues independently using accessible log data

Upload AOT logs to Centralized AOT Log Server

The AOT Log Server acts as a centralized destination for collecting and storing Always On Tracing (AOT) logs from various Citrix® components. It is containerized using Docker technology and is preferably deployed on Linux, though it also supports Windows environments via Docker Desktop.

> **Note:**
>
> Citrix Workspace app for HTML5 2603 now supports AOT log uploads to centralized log servers for on-premises setups that include a gateway in the path.

Starting with Citrix Workspace app for HTML5 2603, you can disable the AOT feature by adding the following configuration:

```
1 {
2
```

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

```
  "aot": {

    "enabled": false
   }

}
```

Prerequisites

This feature is available only when you open a session using:

- Citrix Virtual Apps and Desktops™ version 2507 CU1 or later
- Citrix Virtual Apps and Desktops™ version 2511 or later

Limitations

AOT logs cannot be uploaded if the log server uses HTTP when using Mozilla Firefox and Apple Safari browsers.

How to configure

To configure, you must first install and configure the log server. For detailed installation and configuration steps, see Install and configure log server.

After you install the log server, the system generates a StartLogServer script in the same location. The file name is `StartLogServer.bat` on Windows or `StartLogServer.sh` on Linux.

To enable communication between Citrix Workspace app for HTML5 and the log server, you must configure the log server to accept the StoreFront FQDN URL by enabling Cross-Origin Resource Sharing (CORS) in the log server.

To enable CORS:

1. If the log server is running, stop it using the following command:

```
    docker stop logserver
```

1. Add the following environment arguments to `StartLogServer.bat` (or `StartLogServer.sh` on Linux) by editing the CORS_ORIGINS parameter:

```
    -e CORS_ORIGINS=""
```

Example for single URL:

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

```
    -e CORS_ORIGINS="https://xyz.bvt.local;"
```

Example for multiple URLs:

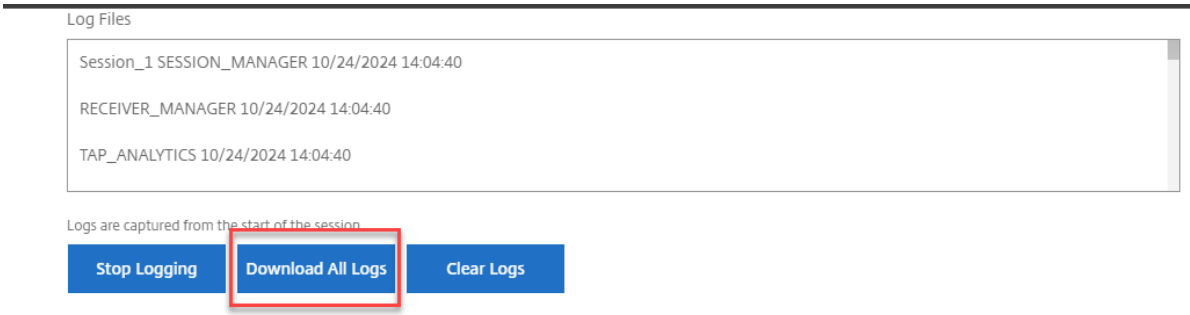
```
    -e CORS_ORIGINS="url1;url2;url3"
```

Use semicolons (;) to separate multiple URLs.

1. Restart the log server using `StartLogServer.bat` (or `StartLogServer.sh` on Linux).

End user experience

On the **Log files** screen, click **Download All Logs**. The app gathers all relevant log files and compresses them into a zip archive. The downloaded file uses a standardized naming convention, such as `CWA_HTML5_LOGS_[timestamp].zip`, ensuring clarity and easy identification.



For more information, see How to collect logs.

View endpoint telemetry in Citrix Director

This feature enhances the ability of admins to view endpoint telemetry data directly in Citrix Director.

Prerequisites

- Citrix Workspace app for HTML5 2411 and later
- VDA version 2411 and later
- Citrix Director

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

Session launch diagnostics

Starting with the 2502 version, we've implemented an improved support process for session failures. Help desk administrators are now equipped with comprehensive insights into failure paths, allowing them to effectively triage and significantly reduce the number of support cases related to session failures.

For more information, see Session launch diagnostics in the Citrix Monitor documentation.

Disable downloading of Citrix Workspace app logs in error dialogs

Starting with the version 2505, admins can hide the **Download Log** button in all error dialogs for both app and desktop sessions in Citrix Workspace app for HTML5 (cloud and on-prem).

> **Note:**
>
> This feature is disabled by default. In other words, the user has an option to download logs from the error dialog.

For more information, see Disable downloading of Citrix Workspace app logs in error dialogs.

Logs to troubleshoot Entra ID single sign-on support for VDA with Azure AD credentials setup

This article describes the logs that you can collect when SSO fails and users receive unexpected credential prompts after the session launches.

To collect logs:

1. Collect the basic Citrix Workspace app logs. For more information, see How to collect logs.
2. Collect the network traces for Microsoft Authentication Library (MSAL) token fetch status:

   i. Install Charles or Fiddler on the endpoint.
   ii. Log in to the Microsoft Entra ID Store in the browser where the issue is occurring.
   iii. Start the Charles or Fiddler app.
   iv. Start Citrix Workspace app for HTML5 session. After you reproduce the issue, export the fiddler traces by clicking **File** > **Save** > **All sessions**. This downloads the traces that you share with Citrix. For more information, see the following screenshot:
3. Collect Citrix Diagnostic Facility (CDF) traces from the VDA for all modules and startup tracing. Follow the steps to collect a CDF trace at system startup because SSO can fail even with successful capability negotiation from Citrix Workspace app.

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

FAQs

Where can I find the latest information about the newly added features or enhancements?

You can find the latest information about the Citrix Workspace app for HTML5 in the product documentation.

How to access technical preview features?

To know about the features that are in technical preview, see Features in Technical Preview.

How to provide feedback on EAR?

To provide feedback on the EAR version, click https://forms.gle/ef3eFFKBk7gvTi1b6.

How to customize the toolbar inside Citrix Workspace app session?

Administrators can customize the toolbar, by choosing which options are visible to end users. Administrators can customize it using the Global App Configuration service. For more information see Toolbar customization in the product documentation.

How to configure cipher suits for the SSL-enabled VDA with Citrix Workspace app for HTML5?

To configure the cipher suites, see cipher suite article within the Citrix Workspace app for HTML5 documentation.

Secure

July 10, 2026

Secure HDX™

Starting with version 2408, Secure HDX is supported. Secure HDX is an Application Level Encryption (ALE) solution that prevents any network elements in the traffic path from being able to inspect the HDX traffic. It does this function by providing true End-to-End Encryption (E2EE) at the application level between the Citrix Workspace™ app (client) and the VDA (session host) using AES-256-GCM encryption.

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

Prerequisites

The minimum VDA version must be 2503 for this feature to function.

Configurations

Secure HDX is disabled by default. You can configure this feature using the **Secure HDX** setting in the Citrix policy:

- **Secure HDX:** Defines whether to enable the feature for all sessions, only for direct connections, or disable it.

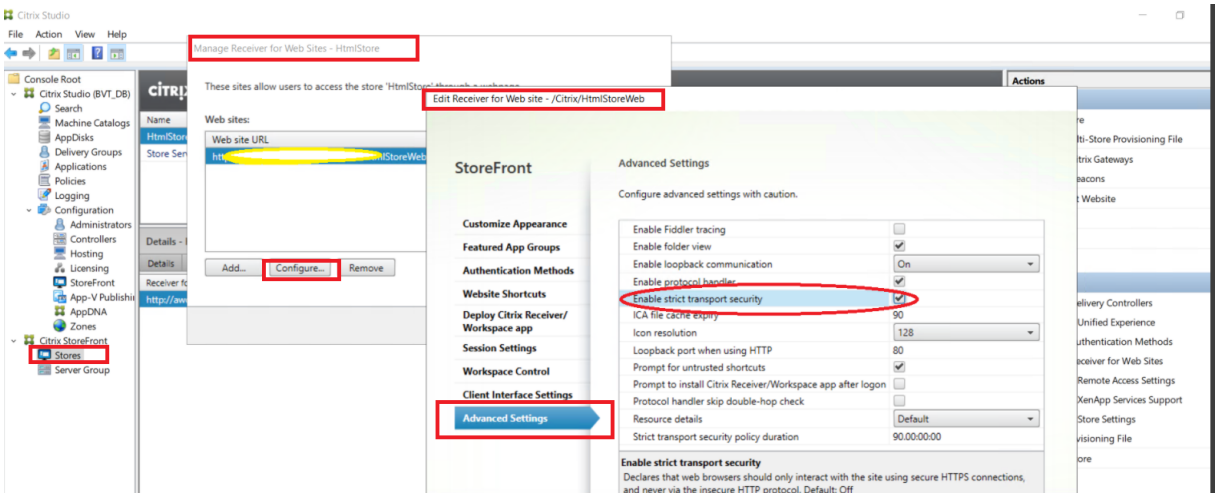
For more information, see Secure HDX in the Citrix DaaS documentation.

Security settings

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**.



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

Authenticate

June 17, 2026

Support for Microsoft Entra ID single sign-on

Starting with version 2511, Citrix Workspace app for HTML5 supports Microsoft Entra ID single sign-on to achieve single sign-on when using Microsoft Entra ID credentials to access virtual applications and desktops on Microsoft Entra joined or Microsoft Entra hybrid joined session hosts.

With this feature, users with Entra ID-joined VDAs get seamless authentication and do not need to enter credentials each time they launch a VDA. For seamless single sign-on (SSO) to Entra VDAs, enable pop-ups in your browser settings because blocked pop-ups can prevent successful SSO.

For details on system requirements and configuration, see Microsoft Entra ID single sign-on for DaaS.

Known issues

- A pop-up window opens during session launch. The pop-up behavior varies depending on your browser and browsing mode (normal or incognito).

Logs to troubleshoot Entra ID single sign-on support for VDA with Azure AD credentials setup

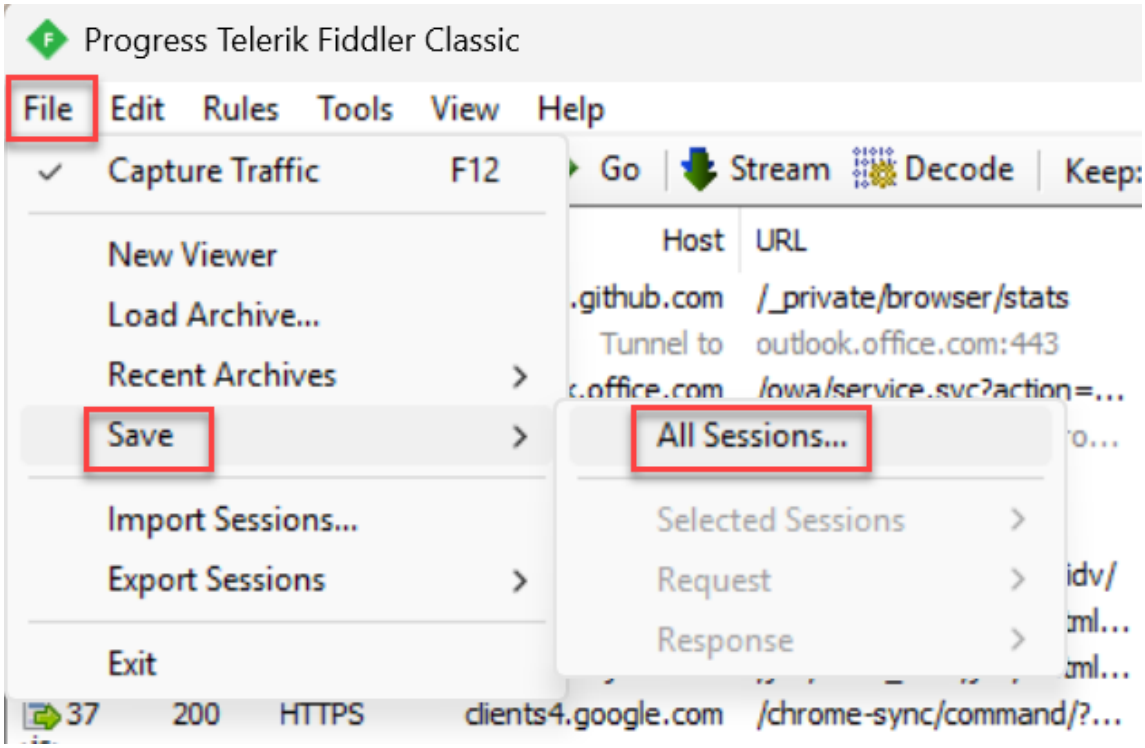
This article describes the logs that you can collect when SSO fails and users receive unexpected credential prompts after the session launches.

To collect logs:

1. Collect the basic Citrix Workspace app logs. For more information, see How to collect logs.
2. Collect the network traces for Microsoft Authentication Library (MSAL) token fetch status:

   i. Install Charles or Fiddler on the endpoint.
   ii. Log in to the Microsoft Entra ID Store in the browser where the issue is occurring.
   iii. Start the Charles or Fiddler app.
   iv. Start Citrix Workspace app for HTML5 session. After you reproduce the issue, export the Fiddler traces by clicking **File** > **Save** > **All sessions**. This downloads the traces that you share with Citrix. For more information, see the following screenshot:

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



3. Collect Citrix Diagnostic Facility (CDF) traces from the VDA for all modules and startup tracing. Follow the steps to collect a CDF trace at system startup because SSO can fail even with successful capability negotiation from Citrix Workspace app.

Support for single-tenant Microsoft Entra ID

This feature lets you use single sign-on (SSO) with Microsoft Entra ID credentials to access virtual apps and desktops on Microsoft Entra hybrid-joined session hosts. To configure VDA SSO, use your customer-specific single-tenant Entra ID client app. For more information, see Microsoft Entra single sign-on.

SDK

September 18, 2026

HDX™ SDK

Citrix Workspace app enhances support for HDX and SDK sessions by enabling you to customize your delivery model for Citrix hosted apps and desktops through your website.

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

This feature is useful for building a rich app experience in your Enterprise portals, and for users as a service. You can provide the experience when you host Citrix Workspace app for HTML5 on your web server while launching Citrix hosted apps and desktops from your website.

For the HDX SDK for Citrix Workspace app for HTML5 documentation, see HDX SDK for HTML5.

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

Autoupdate support for Citrix Workspace app for HTML5 using HDX SDK for HTML5

Citrix HDX SDK for HTML5 enhances the `setPath` API to consume the latest build of Citrix Workspace app for HTML5 from the CDN. This enhancement allows Citrix Workspace app for HTML5 to run on the latest version seamlessly. For existing HDX SDK for HTML5 users, change `citrix.receiver.setPath` in the customer code to use the latest from the CDN. For new users, the `setPath` API provides the option by default.

CDN is provided as the default. If there are any issues with the CDN, the hosted location provides the fallback path. For more information, see HDX SDK for HTML5.

Latest version of Citrix HDX SDK for HTML5

Verify that you use the latest version of the Citrix HDX SDK for HTML5 to start the sessions. Else, the session might fail to start.

For more information, see Citrix Workspace app for HTML5 HDX SDK.

Virtual Channel SDK support

The Citrix Virtual Channel (VC) SDK supports writing server-side applications and client-side drivers using the ICA protocol. The server-side virtual channel applications are on the Citrix Virtual Apps and Desktops server.

VC SDK supports writing new virtual channels and Citrix Workspace app for HTML5 can support up to 20 custom-virtual channels.

Known limitations in the feature

- If the configuration of the virtual channels is incorrect, you can observe a lag of 30 seconds.
- When you create a custom VC, start the 'streamName'with anything other than 'CTX'.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for HTML5.

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

Enhancements to Virtual Channel SDK

Starting with the 2305 release, Citrix Workspace app for HTML5 supports Window Management APIs in the Virtual Channel SDK. Web APIs enable IT administrators to create interactive applications and customize them for their end users.

Support for Unified Communications (UC) SDK

The Citrix Unified Communications SDK allows Unified Communications vendors, Cloud contact center providers, Communications Platform as a Service (CPaaS) providers, or any WebRTC-based communications vendors to integrate seamlessly with electron-based desktop or browser-based applications.

For more information, see Unified Communications (UC) SDK, which is a tech zone article.

Redirection of WebHID APIs

Unified Communications SDK for Citrix Workspace™ app for HTML5 implements the redirection of WebHID APIs as defined in Citrix-WebRTC, with certain known limitations. They are:

- If multiple HID devices of the same type exist, the user can't select a specific device for testing.
- On Mac machines, when you use Citrix Workspace app for HTML5, the app might fail to retrieve the custom 'compositeId'before a newly connected media device is ready.
- On both Windows and Mac systems, when using Citrix Workspace app for HTML5, users might need to re-grant access permissions for reconnected devices. This process includes devices using a wireless keyboard or mouse USB receiver. The need to re-grant permissions is due to the absence of a connection event.

> **Note:**
>
> - This feature is disabled by default.
> - When the Microsoft Teams optimized secondary ringtone is enabled, the ringtone does not play in the Citrix Workspace app for HTML5 client. Citrix Workspace app for HTML5 SDK must be updated to utilize the new Microsoft assets URL. To enable media loading from the Microsoft Content Delivery Network (CDN), add https://*.onecdn.static.microsoft to the `media-src` directive within the Content Security Policy (CSP) meta tag in `HDXEngine.html`.

How to configure

You can enable the feature by using:

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

- Configuration.js
- Global App Configuration service

Configuration.js In Citrix Workspace app for HTML5, the **configuration.js** file is located under the `C:\Program Files\Citrix\Receiver StoreFront\HTML5Client` folder. Edit this file to enableee the feature.

> **Notes:**
>
> - Citrix recommends that you back up the **configuration.js** file before modifying it.
> - Administrator-level credentials are required to edit the **configuration.js** file.

To enable the feature:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Make sure you set the attribute `webHID` to **`true`**. The following is an example of JSON data:

```
'features' : {

    'msTeamsOptimization' : {

        'webHID' : true
         }

         }
```

3. Set the attribute **hidDeviceBlockList** with the correct format. If you want to block some HID devices, the following is an example of JSON data:

```
'features' : {

'msTeamsOptimization' : {

    // The format of the blocklist is ["VID:PID", "VID:PID", "VID:
       PID", ...]
    // Each VID and PID is an up to 4-digit hexadecimal number
       with an optional "0x" prefix.
    // The VID is a required field. The PID is optional, so the
       colon and PID can be omitted.
    // example ["35ab:21ff", "45ac", "0x567:123a", "0x1234:0x5678
       "]
    'hidDeviceBlockList' : []
     }

 }
```

4. Save the changes.

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

Global App Configuration service Administrators can enable the feature by navigating to **Workspace Configuration** > **App Configuration** > **HDX and Multimedia** > **MS Teams** > **Enable webHID redirection** and **HID Device Blocklist**. Select the checkbox and respective toggle button to enable the feature.

Deprecation

September 7, 2025

The announcements in this article give you advanced notice of platforms, Citrix® products, and features that are being phased out. Using these announcements, you can make timely business decisions.

Citrix monitors customer use and feedback to determine when they're withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

Deprecated items aren't removed immediately. Citrix continues to support them in this release but they'll be removed in the future.

Item	Deprecation announced in	Removed in	Alternative
Internet Explorer 11	-	2206	Use the other supported web browsers
Legacy browsers	-	2206	Use the latest version of the browsers

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.