Citrix Workspace™ app for Mac

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

Contents

Citrix Workspace™ app for Mac 3

About this release 5

Features in Technical Preview 134

Citrix Workspace app for Mac 2611 - Preview 148

System requirements and compatibility 148

Install, uninstall, and upgrade 155

Updates and plugins management 161

Update 162

Plug-ins management 179

Configure Citrix Workspace app 188

Mobile Device Management 192

Store configuration 204

Security and Authentication 209

Authenticate 209

Security 221

Secure communications 225

App experience 234

Application delivery 234

Enhanced virtual apps and desktops launch experience for Workspace 236

App preferences 238

Data collection and monitoring 255

HDX™ and multimedia 257

Browser Content Redirection 258

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

Bidirectional content redirection **262**

Graphics and display **264**

Optimized Microsoft Teams **274**

Virtual channel plugin manager **283**

HDX™ transport **284**

HDX™ direct **285**

Devices **285**

Audio and Microphone **286**

Client drive mapping **290**

Keyboard **291**

Printing **312**

USB **315**

Webcam **321**

Session experience **323**

Troubleshooting **349**

Deprecation **355**

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

Citrix Workspace™ app for Mac

Citrix Workspace app for Mac is an easy-to-install app that provides access to your applications and desktops using Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) from a remote client device. Citrix Workspace app for Mac combines ease of deployment and use, and offers quick, secure access to hosted applications and desktops.

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

For information about deprecated items, see the Deprecation page.

You can use Citrix Workspace app on various devices running macOS. For information about the features available in Citrix Workspace app for Mac, see Citrix Workspace app Feature Matrix.

Language support

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

Earlier versions

Citrix Workspace app 2607 for Mac (PDF Download)

Citrix Workspace app 2603.11 for Mac (PDF Download)

Citrix Workspace app 2603 for Mac (PDF Download)

Citrix Workspace app 2511.1 for Mac (PDF Download)

Citrix Workspace app 2508.10 for Mac (PDF Download)

Citrix Workspace app 2508 for Mac (PDF Download)

Citrix Workspace app 2505.10 for Mac (PDF Download)

Citrix Workspace app 2505 for Mac (PDF Download)

Citrix Workspace app 2503.10 for Mac (PDF Download)

Citrix Workspace app 2503 for Mac (PDF Download)

Citrix Workspace app 2411.10 for Mac (PDF Download)

Citrix Workspace app 2411 for Mac (PDF Download)

Citrix Workspace app 2409.10 for Mac (PDF Download)

Citrix Workspace app 2409 for Mac (PDF Download)

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

Citrix Workspace app 2405.11 for Mac (PDF Download)

Citrix Workspace app 2405 for Mac (PDF Download)

Citrix Workspace app 2402.10 for Mac (PDF Download)

Citrix Workspace app 2402 for Mac (PDF Download)

Citrix Workspace app 2311 for Mac (PDF Download)

Citrix Workspace app 2309 for Mac (PDF Download)

Citrix Workspace app 2308 for Mac (PDF Download)

Citrix Workspace app 2307 for Mac (PDF Download)

Citrix Workspace app 2306 for Mac (PDF Download)

Citrix Workspace app 2305 for Mac (PDF Download)

Citrix Workspace app 2304 for Mac (PDF Download)

Citrix Workspace app 2301.1 for Mac (PDF Download)

Citrix Workspace app 2301 for Mac (PDF Download)

Citrix Workspace app 2211 for Mac (PDF Download)

Citrix Workspace app 2210 for Mac (PDF Download)

Citrix Workspace app 2209 for Mac (PDF Download)

Citrix Workspace app 2208.1 for Mac (PDF Download)

Citrix Workspace app 2206.1 for Mac (PDF Download)

Citrix Workspace app 2204 for Mac (PDF Download)

Citrix Workspace app 2203.1 for Mac (PDF Download)

Citrix Workspace app 2201 for Mac (PDF Download)

Citrix Workspace app 2112 for Mac (PDF Download)

Citrix Workspace app 2111 for Mac (PDF Download)

Citrix Workspace app 2110 for Mac (PDF Download)

Citrix Workspace app 2107 for Mac (PDF Download)

Citrix Workspace app 2104 for Mac (PDF Download)

Citrix Workspace app 2102 for Mac (PDF Download)

Citrix Workspace app 2101 for Mac (PDF Download)

Documentation for these product versions is provided as PDFs because they are not the latest versions. For the most recently updated content, see Citrix Workspace app for Mac current release documentation. That documentation includes instructions for upgrading from earlier versions.

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

> **NOTE:**
>
> Links to external websites found in these PDFs take you to the correct pages, but links to other sections within the PDF are no longer usable.

Reference articles

- Tech Brief: Citrix Workspace
- Developer Documentation
- Global App Configuration service
- App Protection
- Workspace user interface (UI)
- Microsoft Teams optimization in Citrix Virtual Apps and Desktops environments
- Citrix Workspace app for iOS
- Citrix Workspace app release timelines

What's new in related products

- Citrix Enterprise Browser: About this release
- Citrix Workspace: What's new
- Citrix DaaS: What's new
- StoreFront: What's new
- Secure Private Access: What's new

Legacy documentation

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

About this release

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

A list of features in Technical Preview is maintained in the Features in Technical Preview section, so you can find them in one place. Explore our preview features and share your feedback using the attached form link.

> **Note:**
>
> Issues have been identified in macOS, including macOS 27 (Golden Gate), macOS 26.7 (Tahoe),

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

> and macOS 15.8 (Sequoia), that affect the manual installation of Citrix Workspace app using the .dmg file. These issues prevent the **Add-ons** section from appearing during installation. Because the issue originates in macOS, it can affect all Citrix Workspace app versions.
>
> *For more information, see the Known Issues section in the Citrix Workspace app for macOS 2609 release notes.*

What's new in 2609

The following is a list of features that are available in Citrix Workspace app 2609 for Mac:

- Support for macOS 27 Golden Gate
- HDX Direct support for direct connections

Support for macOS 27 Golden Gate

Starting with version 2609 of Citrix Workspace app for Mac, the app supports devices running on macOS 27 Golden Gate.

HDX Direct support for direct connections

Starting with version 2609, Citrix Workspace app for Mac secures direct connections with HDX Direct right from launch. In deployments where the client connects straight to the session host without a Gateway, such as StoreFront, Workspace with Direct Workload Connection, or Workspace set to internal-only connectivity, the app now uses HDX Direct certificates to establish a secure connection at launch, instead of starting an unencrypted session and then switching it to a secure one.

For more information, see HDX Direct.

Fixed issues in 2609

- When trying to reset the Citrix Workspace app, users might have experienced the **Reset** dialog rendering larger than intended, with overlapping text and buttons and a misaligned layout. [RFMAC-19464]
- Users might have experienced some mapped client drives not appearing inside published desktops and applications. For example, only the C: drive was accessible, while the home (H:) drive was missing. [CVADHELP-34868]

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

Known issues in 2609

- On macOS 27 (Golden Gate), macOS 26.7 (Tahoe), and macOS 15.8 (Sequoia), installing Citrix Workspace app using the `.dmg` file might not display the **Add-Ons** and **Add Account** setup screens. As a result, add-ons such as the Microsoft Teams Optimization pack cannot be manually selected during installation. This issue affects all supported versions of Citrix Workspace app, including version 2609.

  As a workaround, install the package using the following Terminal command:

  ```
  sudo installer -pkg /Volumes/Citrix\ Workspace/Install\ Citrix\
     Workspace.pkg -target /
  ```

  For more details, see Installation using the terminal command.

- On macOS 27, to open web apps or SaaS apps from Citrix Workspace in Chrome Enterprise Premium, you must grant data access when prompted on the first launch. If you miss or decline this prompt, you can restore access under **System Settings > Privacy & Security > Files & Folders > Citrix Workspace**.

Earlier releases

This section lists features in previous releases along with their fixed and known issues. Releases reach End of Life (EOL) 18 months after the release date. For details about lifecycle dates for the supported versions, see Lifecycle Milestones for Citrix Workspace app and Citrix Receiver.

2607

What's new in 2607

The following is a list of features that are available in Citrix Workspace app 2607 for Mac:

- Microsoft Teams VDI Plugin —generally available and installed by default
- Version rollback support for auto update
- Faster and less disruptive automatic updates (side-by-side silent update)
- Session Pre-Launch support
- Improved Point of Presence (PoP) selection
- DNS caching for improved session resilience (Technical Preview)
- EDT MTU Rediscovery (Technical Preview)
- Streaming read and write for Client Drive Mapping (CDM) (Technical Preview)
- HDX Direct for Service Continuity for connectorless workloads (Technical Preview)
- HDX graphics super resolution (Technical Preview)

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

- Location redirection for virtual sessions (Technical Preview)
- Enhanced call connect times with Unified Communications SDK
- Optimized Overlay Clipping for multimedia sessions
- Resilient and secure third-party plugin execution (Technical Preview)
- OAuth redirection support for Bidirectional content redirection
- Adaptive Webcam Bitrate
- PDF printing enhancements
- Health checker tool for CAM and MDM Policy

Microsoft Teams VDI Plugin —generally available and installed by default

Starting with Citrix Workspace app for Mac 2607, the new VDI optimization for Microsoft Teams is generally available and the Microsoft Teams VDI plug-in is installed by default. The plug-in checkbox in the installer Add-ons step is now checked by default, and the plug-in is also installed automatically during Citrix Workspace app for Mac auto-update.

For more information, see Microsoft Teams VDI Plugin —generally available and installed by default.

Version rollback support for auto update

Starting with version 2607, Citrix Workspace app for Mac supports administrator-initiated version rollback through the automatic update mechanism. When an administrator needs to reverse a problematic update, Citrix Workspace app can move the device back to an earlier, stable version using the same quiet, side-by-side mechanism as a normal automatic update.

For more information, see Version rollback support for auto update.

Faster and less disruptive automatic updates (side-by-side silent update)

Starting with version 2607, Citrix Workspace app for Mac delivers a faster and less disruptive update experience. Updates install silently in the background while you continue working, with no interruption to your running apps or active sessions, and once completed, the previous version is removed automatically to free up disk space.

For more information, see Faster and less disruptive automatic updates (side-by-side silent update).

Session Pre-Launch support

Starting with version 2607, Citrix Workspace app for Mac supports Session Pre-Launch for virtual applications, establishing application sessions in the background before the user explicitly launches an

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

app. When the user clicks an app, the pre-established session is reused immediately, significantly reducing the perceived launch time.

For more information, see Session Pre-Launch support.

Improved Point of Presence (PoP) selection

Starting with version 2607, Citrix Workspace app for Mac improves Gateway Service PoP selection for eligible Citrix Gateway Service sessions. When configured and session latency exceeds the defined threshold, the Citrix Workspace app for Mac can evaluate candidate PoPs associated with the Gateway Service FQDN and reconnect through a better-performing PoP. This enhancement helps improve session responsiveness when applicable.

Enhanced call connect times with Unified Communications SDK

Starting with version 2607, the Unified Communications SDK (UCSDK) 5.0.0 introduces a Smart Sync feature that reduces call connection times by streamlining communication between the VDA and the client endpoint.

For more information, see Enhanced call connect times with Unified Communications SDK.

Optimized Overlay Clipping for multimedia sessions

Starting with version 2607, Citrix Workspace app for Mac introduces Optimized Overlay Clipping, improving both performance and visual accuracy during multimedia sessions that use HDX Microsoft Teams Optimization and UCSDK Optimization.

For more information, see Optimized Overlay Clipping for multimedia sessions.

OAuth redirection support for Bidirectional content redirection

Starting with Citrix Workspace app for Mac 2607, bidirectional content redirection supports OAuth authentication flows. When a user opens an OAuth-protected URL from a VDA session, the bidirectional content redirection policy intercepts the URL and redirects the authentication request to the local Mac endpoint.

For more information, see OAuth redirection support for Bidirectional content redirection.

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

Adaptive Webcam Bitrate

Starting with version 2607, Citrix Workspace app for Mac automatically adjusts webcam video quality to match available network bandwidth in real time. The client continuously monitors network conditions and adapts the webcam stream accordingly —reducing bitrate when the network is constrained and restoring quality as bandwidth recovers.

For more information, see Adaptive Webcam Bitrate.

PDF printing enhancements

Starting with version 2607, Citrix Workspace app for Mac queries connected printers for their capabilities and presents printer-specific settings in the VDA print dialog when using the PDF Universal Print Driver (UPD). Print jobs are routed directly to the auto-created client printer, and print ticket settings such as duplex, orientation, color mode, and stapling are passed through to the client printer and honored.

For more information, see PDF printing enhancements.

Health checker tool for CAM and MDM Policy

When Citrix Client app management (CAM) policies do not take effect on Mac endpoints, diagnosing the cause has historically required collecting logs, running manual network tests, and comparing configuration files by hand —a process that requires intense effort and analysis.

For more information, see Health checker tool for CAM and MDM Policy.

Technical Preview in 2607

- DNS caching for improved session resilience
- EDT MTU Rediscovery
- Streaming read and write for Client Drive Mapping (CDM)
- HDX Direct for Service Continuity for connectorless workloads
- HDX graphics super resolution
- Location redirection for virtual sessions
- Resilient and secure third-party plugin execution

Fixed issues in 2607

- Users might have experienced session launch failures when starting a resource directly from Citrix Workspace app for Mac, even if the same resource opened successfully from the Applications

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

folder. [CVADHELP-33601]

Known issues in 2607

There are no new known issues in the release.

2603.11

What's new in 2603.11

The following is a list of features that are available in Citrix Workspace app 2603.11 for Mac:

- Support for Citrix Snipping Tool integration (Technical Preview)
- Deprecation of Datagram Transport Layer Security (DTLS) 1.0

Deprecation of Datagram Transport Layer Security (DTLS) 1.0

Starting with version 2603.11, Citrix Workspace app for Mac no longer supports DTLS 1.0 due to its known security vulnerabilities and to align with industry standards.

> **Note:**
>
> Citrix Workspace app for Mac uses DTLS 1.2 encryption by default.

Technical Preview in 2603.11

- Support for Citrix Snipping Tool integration

Fixed issues in 2603.11

- Users might experience connection failures when launching virtual apps or desktops on which the SecureICA encryption policy was enabled. [CVADHELP-33330]
- After upgrading to macOS 26.4 or later, launching apps and desktops from a browser using Citrix Workspace Launcher might require manually opening the `.ica` file instead of launching automatically. [RFMAC-18816]
- Sessions might disconnect unexpectedly over Transmission Control Protocol (TCP) because of a decryption failure. [CVADHELP-31790]
- Sessions might disconnect unexpectedly after a network interruption. [CCVADHELP-4930]

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

Known issues in 2603.11

There are no new known issues in the release.

2603

What's new in 2603

The following is a list of features that are available in Citrix Workspace app 2603 for Mac:

- Gesture support for remote Mac sessions
- Bidirectional Content Redirection
- Deprecation of macOS 13.0 Ventura
- Always On Tracing (AOT) support for Citrix Workspace app for Mac
- Microphone troubleshooting
- Shield V2 service continuity
- Support for Microsoft Teams VDI Plugin installation
- Virtual channel plugin manager
- Support for PassKey (FIDO2) authentication
- Seamless application accessibility mirroring
- Improved session reconnection experience

Gesture support for remote Mac sessions

Starting with the 2603 version, Citrix Workspace app for Mac supports macOS gestures in ICA sessions when connected to Remote Mac (macOS VDA) 2603 or later. Gestures behave the same as on the local Mac. Whether they apply locally or in the session follows the keyboard setting **System shortcuts take effect on**. To temporarily apply a gesture on the local Mac during a session, press and hold the **Fn** key while performing it.

Bidirectional Content Redirection

Starting with the 2603 version, Citrix Workspace app for Mac supports Bidirectional Content Redirection (Host-to-Client and Client-to-Host). Administrators can configure specific URLs to redirect from the Citrix session to the local endpoint (Host-to-Client) or from the local endpoint into the Citrix session (Client-to-Host). This optimization ensures URLs launch in the most appropriate environment-preserving server resources for media-heavy sites or ensuring security compliance for internal links. Citrix recommends using Bidirectional Content Redirection over Host-to-Client redirection and Local App Access for most use cases on supported platforms.

For more details, see Bidirectional content redirection.

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

Deprecation announcement of macOS 13.0 Ventura

Starting with the 2603 version, support for macOS Ventura 13.0 is deprecated. As an alternative, you can upgrade to the latest available version of Mac. For more information, see Deprecation.

Always On Tracings (AOT) support for Citrix Workspace app for Mac

Starting with the 2603 version, Citrix Workspace app for Mac introduces support for Always On Tracing (AOT). With this enhancement, log collection is automatic and continuous, enabling Workspace app components to generate structured AOT logs that are centrally collected by the AOT Log Server. This approach removes the need for manual log capture or issue reproduction on end-user devices.

AOT logs from the Workspace app are integrated with Citrix Virtual Apps and Desktops (CVAD) AOT data. This integration provides end-to-end visibility into connection, launch, and session workflows, allowing IT teams to correlate client-side and backend events, troubleshoot issues more efficiently, and reduce the time required to collect diagnostic information.

This feature further enhances observability at the Workspace app layer and supports continuous tracing across the Citrix environment. For more information and guidance on getting started, see Always On Tracing.

Microphone troubleshooting

Starting with the 2603 version, Citrix Workspace app for Mac includes microphone troubleshooting to help you quickly identify privacy-related blocks. If your endpoint system settings or session toolbar preferences deny microphone access, the app does not redirect the microphone device to a virtual session. The **Citrix Assistant** app or `ctxaudiosession` running in the virtual session detects this and displays a clear warning to guide you.

Windows Virtual Desktops: For Windows Virtual Desktops, use the **Citrix Assistant** app to diagnose microphone privacy issues. For more information, see Citrix Virtual Desktop Assistant application.

Linux and macOS Virtual Desktops: For Linux and macOS Virtual Desktops, use the `ctxaudiosession` tool to check microphone privacy status. For details, see:

- Linux: Audio Diagnostic Command Line Tool.
- macOS: Audio Diagnostic Command Line Tool.

Virtual channel plugin manager

Starting with the 2603 version, Citrix Workspace app for Mac enables virtual channel plugin manager for Microsoft Teams. Virtual channel plugin manager helps deploy plug-ins across client endpoints

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

for specified applications. It detects supported applications running on the VDA and prompts users to install the required plug-in on the endpoint for the best in-session experience. Users can choose to install the plug-in, skip the installation, or deny it. This feature provides flexibility to manage plug-ins across both managed and unmanaged endpoints.

For more information, see Virtual channel plugin manager.

Support for PassKey (FIDO2) authentication

Starting with version 2603, Citrix Workspace app for Mac supports **PassKey (FIDO2)** authentication using **TouchID** or password, in addition to external Security Keys. The **PassKey** is specific to the local macOS user profile and stored in the Secure Enclave, accessible only by Citrix Viewer. This feature is supported on Macs with the Secure Enclave.

For more information, see Support for PassKey (FIDO2) authentication.

Seamless application accessibility mirroring

Starting with version 2603, Citrix Workspace app for Mac captures accessibility settings from the client and applies them to seamless applications. This enhancement automatically synchronizes accessibility configurations, providing consistent support across virtual application sessions and eliminating manual reconfiguration.

For more information, see Seamless application accessibility mirroring.

Improved session reconnection experience

Starting with version 2603, this feature enhances the end-user experience during session timeouts caused by inactivity or network interruptions. The solution provides users with an option to reconnect directly from the timeout screen for desktop and app sessions. Users can also reconnect directly during the Auto-Client-Reconnect (ACR) phase.

For more information, see Improved session reconnection experience.

Technical Preview

- Shield V2 service continuity
- Support for Microsoft Teams VDI Plugin installation

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

Fixed issues in 2603

- Users might have experienced redirected web content appearing outside the desktop session window during full-screen sessions when Browser Content Redirection was enabled. [HDX-92827]
- Users might have experienced Browser Content Redirection (BCR) redirected web content appearing outside the desktop session window when the session was not in full-screen mode, especially when moving the browser to the edge of the screen. [HDX-92836]
- While a session automatically reconnects through Auto Client Reconnect (ACR), Browser Content Redirection might not resume, causing redirected pages to fall back to server-side rendering. [HDX-97357]
- While the desktop session is running in windowed mode with Browser Content Redirection, drop-down menus on redirected webpages might fail to open or appear outside the session window. [HDX-96637]
- When you cut and paste a file to a different folder on your network drive within your Citrix session, you might notice that deleting the file appears successful, but it reappears after you refresh and is only permanently deleted after you disconnect or log off. [CVADHELP-30231]
- Users might have experienced the Bomgar and SQL Server Management Studio (SSMS) apps failing to launch from the browser after updating to Citrix Workspace app for Mac 2511. [CVADHELP-31110]
- While upgrading from Mac CWA version 2508 to 2511, the USB keyboard might be recognized as "Generic"instead of "Policy Restricted,"causing it to be automatically redirected to the VDA and unavailable for use on the client. [CVADHELP-31414]

Known issues in 2603

- On MacBook Pro devices (especially Apple silicon) connected to an external display, users might experience screen flickering, half-screen black borders or black areas, or a macOS system crash (kernel panic) when closing the MacBook lid while a Citrix session is in full-screen mode on the external display. This issue is more likely to occur on macOS Tahoe 26.1, 26.2, and 26.3.1 when certain Metal layer optimizations are active. [HDX-102101]

  As a workaround, implement the following:

- **Enable V-Sync**

  - Run the following command in Terminal:

```
defaults write com.citrix.receiver.nomas EnableVSync -bool YES
```

  - Restart Citrix Workspace app for Mac for the change to take effect.

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

2511.1

What's new in 2511.1

The following is a list of features that are available in Citrix Workspace app 2511.1 for Mac:

- Bidirectional Content Redirection support on Mac endpoints
- Modular Browser Content Redirection
- Support for Global App Configuration service in hybrid launches
- uberAgent add-on support for managed devices
- Citrix Enterprise Browser
- Improved session failure reporting
- Enhanced USB diagnostic tool for VDA
- Endpoint Analysis Plugin updates
- Enhanced seamless app experience

Bidirectional Content Redirection support on Mac endpoints

Starting with version 2511.1, Citrix Workspace app for Mac supports Bidirectional Content Redirection on Mac endpoints in the Host-to-Client direction only. This allows URLs from Citrix session browsers to open in the client's default browser. The feature is disabled by default and will be enabled in a future release when Client-to-Host direction is available.

To enable this feature, use the following command:

```
defaults write com.citrix.receiver.nomas EnableBidirURLRedirection -
    bool true
```

For more information, see Bidirectional content redirection.

Modular Browser Content Redirection

Starting with the Citrix Workspace app 2511.1 for Mac, the Modular BCR component is installed by default but not packaged with Citrix Workspace App. The modular and evergreen model allows the Browser Content Redirection component to be updated independently and uninstalled independently. This feature provides the following key benefits:

- **Enhanced security**: The BCR NW.js component can receive security patches and updates when they are available, without waiting for a full Citrix Workspace app for Mac release.
- **Simplified management**: Customers no longer must update entire Citrix Workspace app to receive the latest Browser content redirection features.

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

- **Accelerated innovation**: Faster deployment of new BCR features, enhancements, and bug fixes is now possible, delivering continuous value to customers.

The BCR component is downloaded from Citrix CDN and installed post Citrix Workspace app Mac installation.

For more information, see Modular Browser Content Redirection.

Support for Global App Configuration service in hybrid launches

Starting with version 2511.1, Citrix Workspace app for Mac supports Global App Configuration service for hybrid launches. Previously, Global App Configuration service settings were not applied when users launched HDX sessions from a browser that invoked the client engine. With this enhancement, Global App Configuration service configurations are now enforced for all launch methods—browser-initiated sessions, browser extension launches, and native Citrix Workspace app launches.

uberAgent add-on support for managed devices

Starting with version 2511.1, Citrix Workspace app for Mac supports the uberAgent add-on for managed devices. The uberAgent add-on provides advanced monitoring and diagnostics, delivering detailed insights into user experience and application performance. This integration is available exclusively on managed devices, streamlining deployment and reducing administrative overhead.

To enable uberAgent installation with Citrix Workspace app for Mac on managed devices, use the following MDM setting:

```
<key>UberAgentInstallationEnabled</key>
<true/>
```

Citrix Enterprise Browser

Starting with version 2511.1, the Citrix Enterprise Browser (CEB) is no longer integrated into the Workspace app installation package. If necessary, users and administrators can now install CEB independently by downloading it directly from the Citrix Downloads page, located under the **Citrix Enterprise Browser** section.

Improved session failure reporting

Starting with version 2511.1, Citrix Workspace app for Mac improves session failure reporting in Citrix Director by distinguishing user-canceled session launches from actual connection failures. The app

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

detects user cancellations and notifies StoreFront through a postevent endpoint, excluding these cancellations from the User Connection Failures count. This provides administrators with clearer visibility into genuine connection issues for more efficient troubleshooting.

Enhanced USB diagnostic tool for VDA

Starting with version 2511.1, Citrix Workspace app for MAC enhances the USB diagnostic tool deployed with the VDA to support customers with self-service diagnosis of configuration and runtime issues related to USB redirection.

Endpoint Analysis (EPA) Plugin updates

Starting with version 2511.1, the Endpoint Analysis (EPA) plugin now updates automatically using the Citrix Workspace app's built-in auto-update capability. It no longer depends on **GACS** or **MDM** policies to start the update process.

Enhanced seamless app experience

Starting with version 2511.1, Citrix Workspace app for Mac improves the experience of seamless app sessions connected to Virtual Delivery Agents (VDAs) with Citrix Virtual Apps and Desktops release 2411 or later on Windows Server 2022 or 2025.

For more information, see Enhanced seamless app experience.

Technical Preview

- Support for PassKey (FIDO2) authentication
- Improved session reconnection experience

Fixed issues in 2511.1

- Citrix Workspace app for Mac 2511 might download .ica files instead of launching sessions automatically from the web browser.[RFMAC-18373]
- Users might have experienced unexpected Citrix Workspace app window pop-ups when launching sessions through ICA files. [CVADHELP-30390]

Known issues in 2511.1

There are no new known issues in the release.

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

2508.10

What's new in 2508.10

This release addresses areas that improve overall performance and stability.

Citrix Enterprise Browser™

This release includes Citrix Enterprise Browser version 139.1.1.27, based on Chromium version 139. For more information, see Citrix Enterprise Browser documentation.

Fixed issues in 2508.10

- Users might be unable to launch sessions using Chrome Web Extension. [RFMAC-18097]
- Users might have experienced high CPU usage and performance issues when using Citrix Workspace Widgets due to constant data refreshing by the **QuickAccessWidgetExtension process**. [RFMAC-18118]
- Users might experience high CPU usage in Workspace app when attempting to switch the **FileAccess** permission in Workspace Preferences after installing Citrix Workspace app for Mac 2508 on macOS 26 Tahoe. [HDX-93460]

Known issues in 2508.10

There are no new known issues in the release.

2508

What's new in 2508

The following is a list of features that are available in Citrix Workspace app 2508 for Mac:

- Support for macOS 26 Tahoe
- Support for regional GACS discovery endpoints for US Government customers
- Support for Virtual Channel plug-in Manager for Microsoft Teams on Mac
- Enhanced self-service troubleshooting and user experience
- MDM policy for blocking Global AppConfig Service (GACS) requests
- Enhanced keyboard settings configuration
- Enlightened Data Transport (EDT) connection timeout configuration
- Enhanced session toolbar notch size

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

- Seamless mode API enhancement for Virtual Channel Software Development Kit (VCSDK)
- Audio Quality Enhancer for EDT loss tolerant mode

Support for macOS 26 Tahoe

Starting with version 2508 of Citrix Workspace app for Mac, the app supports devices running on macOS 26 Tahoe.

Support for regional GACS discovery endpoints for US Government customers

Starting with version 2508, Citrix Workspace app for Mac transitions from using a single global GACS discovery endpoint to support regional compliance requirements for US Government customers. Administrators can configure government or regional customer settings through Mobile Device Management (MDM), enabling the app to either directly access regional settings endpoints or connect to region-specific discovery endpoints for US Government environments.

For more information, see Support for regional GACS discovery endpoints for US Government customers.

Support for Virtual Channel plug-in Manager for Microsoft Teams on Mac

Starting with version 2508, Citrix Workspace app for Mac introduces virtual channel plugin manager that automatically detects applications like Microsoft Teams on the VDA and prompts users to install endpoint plug-ins for optimal performance. Users can install, skip, or deny plug-in installation, with flexible management across all endpoints. This enables deployment of the Teams plug-in required for Microsoft Teams SlimCore Optimization on Mac.

For more information, see Virtual channel plugin manager.

> **Note:**
>
> Microsoft SlimCore Optimization for Mac is not yet generally available. This feature is currently inactive. Once it becomes generally available, customers will be able to use the Virtual Channel Plugin Manager with Citrix Workspace App 2508.

Enhanced self-service troubleshooting and user experience

Starting with version 2508, users now receive intelligent, contextual error recommendations that:

- Provide specific, actionable guidance based on the precise error condition
- Enable self-service resolution for common connection issues

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

- Reduce dependency on administrator intervention
- Improve the overall connectivity experience, particularly in persistent VDA environments

These enhancements help address session connectivity issues that can be difficult to diagnose and resolve, empowering users to troubleshoot launch failures independently.

MDM policy for blocking Global AppConfig Service (GACS) requests

Starting with version 2508, administrators can block Global AppConfig Service (GACS) requests using the MDM policy, `DisableClientAppManagement`. When this policy is set to **true**, Citrix Workspace app will not connect to any GACS endpoints.

Example:

```
<key>DisableClientAppManagement</key>
<true/>
```

Enhanced keyboard settings configuration

Citrix Workspace app for Mac provides enhanced keyboard settings that allow users to customize keyboard behavior between the client device and remote sessions. Starting with version 2508, these settings enable real-time configuration during active HDX sessions and provide comprehensive control over keyboard input handling.
All keyboard setting changes made by users are applied in real time across all active sessions, without requiring a session reconnect.

Enlightened Data Transport (EDT) connection timeout configuration

Starting with version 2508, Citrix Workspace app for Mac supports configurable Enlightened Data Transport (EDT) connection timeout values to provide better out-of-box experience and enable fine-tuning for specific network environments. Citrix Workspace app for Mac retrieves the `edtConnectionTimeout` value from the ICA file's WFClient section. If the parameter is not present, the application uses a default timeout of 10 seconds.

Enhanced Native macOS Gesture support

Starting with CWA 2508 for Mac, Citrix Viewer provides enhanced gesture support specifically designed for Citrix VDA for macOS environments.

For more information, see Enhanced Native macOS Gesture support.

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

Enhanced session toolbar notch size

Starting with version 2508 of Citrix Workspace app for Mac, the session window features a redesigned, smaller notch that can be dragged to any window edge. 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:**
>
> This feature is automatically enabled for desktop sessions launched through CWA Mac 2508 and requires no client side configuration.

Seamless mode API enhancement for Virtual Channel Software Development Kit (VCSDK)

Starting with version 2508, Citrix Virtual Channel Software Development Kit (VCSDK) supports seamless mode API for Unified Communication Apps. The sample server application uses the new WF API `WFIsAppShareAvailable()` to automatically disable app sharing in seamless mode, giving developers better control over sharing features based on the session type.

Audio Quality Enhancer for EDT loss tolerant mode

Starting with version 2508, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

For more information, see Audio Quality Enhancer for EDT loss tolerant mode.

Citrix Enterprise Browser™

This release includes Citrix Enterprise Browser version 139.1.1.27, based on Chromium version 139. For more information, see Citrix Enterprise Browser documentation.

Technical Preview

- Seamless application accessibility mirroring
- Audio Quality Enhancer for reliable transport

Fixed issues in 2508

- Users might be unable to use keyboard shortcuts involving Command or Control modifiers in App Protection-enabled Citrix VDI sessions on Mac. [APPP-4425]

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

- Users might have needed to click multiple times to interact with windows within the session when keyboard navigation was enabled and the Citrix Viewer window was not active. [HDX-91545]

Known issues in 2508

- Multi-monitor support with High DPI enabled and different resolutions for Browser Content Redirection (BCR) might fail on Mac when multimedia overlay tracking experiences issues while moving application or browser windows containing video overlays or media controls in full screen sessions. [HDX-90071]
- On macOS Tahoe, Citrix Workspace app logo might be missing from sign-out and account/profile removal confirmation pop-ups. [RFMAC-18091]
- When you install Workspace App for Mac on macOS 26 and set **Automatically hide and show the menu bar** to **On Desktop Only**, you might experience mouse pointer offset issues. As a workaround, select any menu bar option other than **On Desktop Only** to resolve the issue. [HDX-92963]
- When you use Citrix Workspace Widgets, you might face High CPU usage and performance issues caused by constant data refreshing by process **QuickAccessWidgetExtension**. As a workaround, disable the Citrix Workspace widget from system settings and restart the system to resolve the issue. [RFMAC-18118]

2505.10

What's new in 2505.10

Enhanced Option + Mouse Click Behavior

Starting with version 2505.10, the mapping of **Option + mouse click** to right-click behavior has been disabled to restore native Mac functionality. This change enables critical use cases for professional applications that require the **Option/Alt** key modifier during mouse interactions.

For more information, see Enhancement to Option + Mouse Click Behavior.

Citrix Workspace app for Mac on macOS 26.0 Beta 4

Citrix Workspace app 2505.10 for Mac has been tested on macOS 26.0 beta 4 (Public Beta 1) 25A5316i. Use this setup in a test environment and provide your feedback.

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

Citrix Enterprise Browser™

This release includes Citrix Enterprise Browser version 137.1.1.25, based on Chromium version 137. For more information, see Citrix Enterprise Browser documentation.

Fixed issues in 2505.10

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

Known issues in 2505.10

- Multi-monitor support with High DPI enabled and different resolutions for Browser Content Redirection (BCR) might fail on Mac when multimedia overlay tracking experiences issues while moving application or browser windows containing video overlays or media controls in full screen sessions.[HDX-90071]

2505

What's new in 2505

- Citrix Workspace app for Mac on macOS Tahoe Beta2
- Simplified authentication into on-premises store
- Support for voice dictation
- Troubleshoot launch failure self service
- Prevent launching of ICA files from disk
- Monitoring Zoom plug-in metrics on Director
- Auto-Update enhancements for active users in Citrix Workspace app for Mac
- Keyboard accessibility support for the toolbar on the Virtual Desktop
- Enhancement to Connection Strength Indicator on Citrix Viewer toolbar
- Support for macOS window tiling in Citrix Workspace app for Mac
- Platform-specific toolbar update: Ctrl+Alt+Del button hidden for macOS VDA sessions
- Enhanced user interface and experience
- Default audio device selection

Citrix Workspace app for Mac on macOS Tahoe Beta2

Citrix Workspace app 2505 for Mac has been tested on macos tahoe beta 2 Version 25A5295e. Use this setup in a test environment and provide your feedback.

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

Simplified authentication into on-premises store

Starting with the 2505 version, administrators can control the **Remember password** checkbox behavior in Citrix Workspace app for Mac.

Administrators can configure this feature using an MDM-based key-value pair:

```
key: SaveCredentials
value type: Boolean
```

For more information, see Simplified authentication into on-premises store.

Support for voice dictation

Starting with version 2505, Citrix Workspace app for Mac supports dictation. This feature allows users to:

- Voice Navigation
- Voice Dictation
- Text Editing

For more information, see Support for voice dictation.

Troubleshoot launch failure self service

Starting with version 2505, Citrix Workspace app for Mac gives users contextual error recommendations that offer specific guidance, enable self-service resolution, reduce administrator dependency, and improve connectivity, especially in persistent VDA environments.

Prevent launching of ICA® files from disk

Starting with version 2505, admins can control session launches from downloaded ICA files using the new GACS/MDM policy. This feature helps prevent unauthorized access and reduces security risks associated with file-based session initiations.

For more information, see Prevent launching of ICA files from disk.

Monitoring Zoom plug-in metrics on Director

Starting with version 2505 of Citrix Workspace app for Mac, and version 2507 of Citrix Virtual Apps and Desktops for both Delivery Controller (DDC) and Virtual Delivery Agent (VDA), you can monitor optimized Zoom environments for Mac endpoints with enhanced visibility.

For more information, see Monitoring Zoom plug-in metrics on Director.

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

Auto-Update enhancements for active users in Citrix Workspace app for Mac

Starting with version 2411 of Citrix Workspace app for Mac, the auto-update feature was enhanced to trigger only for active users, ensuring that updates are available only for users with Global App Configuration service (GACS) or Mobile Device Management (MDM) policies, or those actively using the app. Building on this, version 2505 further refines the auto-update feature by introducing additional conditions for defining an **active user**. This enhancement provides more precise and controlled updates by applying the auto-update feature only to users who meet the updated activity criteria, offering greater flexibility and control over the update process.

For more information, see Auto-Update enhancements for active users in Citrix Workspace app for Mac.

Keyboard accessibility support for the toolbar on the Virtual Desktop

Starting with version 2505, the **Virtual Desktop** toolbar supports keyboard accessibility for all levels. Users can navigate the entire toolbar using keyboard shortcuts.

For more information, see Keyboard accessibility support for the toolbar on the Virtual Desktop.

Enhancement to Connection Strength Indicator on Citrix Viewer toolbar

Starting with version 2505, Citrix Workspace app for Mac introduces an enhanced Connection Strength Indicator designed for a more intuitive and user-friendly experience.

For more information, see Enhancement to Connection Strength Indicator on Citrix Viewer toolbar.

Support for macOS window tiling in Citrix Workspace app for Mac

Starting with version 2505, Citrix Workspace app for Mac supports macOS window tiling, enabling users to easily organize multiple virtual Apps and Desktops running concurrently. Window tiling is integrated with Citrix Workspace app for a seamless experience, allowing users to arrange Citrix sessions efficiently and improve multitasking. This feature is supported on macOS 15 Sequoia.

Platform-specific toolbar update: Ctrl+Alt+Del button hidden for macOS VDA sessions

Starting with version 2505 of Citrix Workspace app for Mac, the Ctrl+Alt+Del button is no longer displayed in the toolbar for macOS VDA sessions. This update introduces platform-specific logic to hide

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

the Windows-centric keyboard shortcut when connecting to macOS virtual desktops, aligning the toolbar with macOS Human Interface guidelines and reducing end-user confusion. The Ctrl+Alt+Del button remains available for Windows and Linux VDA sessions, ensuring full functionality where applicable. This enhancement improves user experience consistency and addresses customer feedback by removing non-functional shortcuts from macOS sessions.

Enhanced user interface and experience

Starting with version 2505 of Citrix Workspace app for Mac, several UI enhancements have been introduced to improve the overall user experience.

This update includes:

- Enhanced button hover states with updated colors and styling
- Refreshed visual styles for menu buttons
- New intuitive icons for better discoverability
- Optimized interactive elements for improved usability

These changes address usability feedback and provide a more consistent and refined experience for users.

Default audio device selection

Starting with 2505 version, you can now select your preferred audio devices directly in the Desktop Viewer toolbar. This feature offers a more customized audio experience with the following key features when connected to a virtual desktop. For more information, see Default audio device selection.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 137.1.1.25, based on Chromium version 137. For more information, see Citrix Enterprise Browser documentation.

Technical Preview

- Enhanced seamless app experience
- Improved session reconnection experience

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

Fixed issues in 2505

- Users might be unable to use the Windows 10 or 11 “Snap Windows”feature, such as dragging the window to the top of the display to maximize it.[CVADHELP-28268]
- Citrix Workspace app for Mac might fail to add certain stores due to incorrect handling of URL redirection and authentication cookies during the store addition process.[CVADHELP -28057]

Known issues in 2505

- Multi-monitor support with High DPI enabled and different resolutions for Browser Content Redirection (BCR) might fail on Mac when multimedia overlay tracking experiences issues while moving application or browser windows containing video overlays or media controls in full screen sessions.[HDX-90071]

2503.10

What’s new in 2503.10

This release addresses areas that improve overall performance and stability.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 134.1.1.24, based on Chromium version 134. For more information, see Citrix Enterprise Browser documentation.

Fixed issues in 2503.10

- Epic Hyperspace might freeze when using it on macOS devices.[CVADHELP-27670]
- Certain HTTPS URLs can’t be redirected to the client when using the Server File Type Association (SFTA) feature.[CVADHELP-27810]
- Users might experience session launch failures with the error message “No Citrix SSL Server configured on the specified address”when the **Session Reliability Connections** policy is set to **Prohibited** and the **HDX adaptive transport** policy is set to **Preferred**.[CVADHELP-28279]

Known issues in 2503.10

- USB Mass Storage devices might fail to redirect using the Generic USB virtual channel on macOS 15.4 and later. As a workaround, use Dynamic Client Drive Mapping (DCDM) to access the USB Mass Storage. [HDX-87197]

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

2503

What's new in 2503

- Support for automatic installation of deviceTRUST® plug-in with Citrix Workspace app
- Quit background processes with Quick Access menu
- Managing display of app shortcuts on Mac Launchpad
- Enhanced desktop launch experience
- Enhanced structure for Help menu
- Improved session timeout experience (Technical Preview)
- Enhanced keyboard settings for VDA OS and session type
- Optimized graphics performance for Selective Thinwire
- UCSDK deviceID enhancement
- Clipboard support for copying files and folders
- Enhanced Multi-Monitor Management for desktop sessions
- Loss tolerant mode for graphics
- USB Redirection of mass storage devices
- HDX direct support
- Enable Audio Quality Enhancer to improve audio performance
- Hybrid launch support using GACS for on-premises stores
- Enhancing hybrid mode support with GACS for cloud stores (Technical Preview)
- Deprecation announcement of macOS Monterey 12
- Support for sharing system audio on Microsoft teams

Support for automatic installation of deviceTRUST plug-in with Citrix Workspace app

Starting with version 2503, Citrix Workspace app for Mac includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management. For more information, see Support for automatic installation of deviceTRUST plug-in with Citrix Workspace app.

Quit background processes with Quick Access menu

Starting with version 2503, Citrix Workspace app for Mac ensures that all background processes, including the Citrix Workspace Helper, quit when user exits the main application through the **Quick Access** menu. This enhancement addresses common concerns where certain apps, like Citrix Workspace Helper, remained active after users closed the main workspace application. For more information, see Quit background processes with Quick Access menu.

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

Managing display of app shortcuts on Mac Launchpad

Starting with version 2503, admins now have greater control over the visibility of favorite app shortcuts on the Mac Launchpad. For more information, see Managing display of app shortcuts on Mac Launchpad.

Enhanced desktop launch experience

Starting with version 2503, Citrix Workspace app for Mac enhances the desktop launch experience by removing the retry timeout setting and improving status messaging. This enhancement is enabled by default. For more information, see Enhanced desktop launch experience.

Enhanced structure for Help menu

Starting with version 2503, Citrix Workspace app for Mac introduces a restructured **Help** menu to improve usability. Troubleshooting options, such as **Open Log Settings** and **Reset Citrix Workspace**, have been moved to a dedicated **Troubleshoot** submenu. For more information, see Enhanced structure for Help menu.

Improved session timeout experience (Technical Preview)

Starting with version 2503, this initiative improves the end-user experience during session timeouts caused by inactivity or network interruptions. The solution provides users with an option to reconnect directly from the timeout screen, eliminating the need to relaunch sessions from the client UI. For more information, see Improved session timeout experience.

Enhanced keyboard settings for VDA OS and session type

Starting with version 2503, Citrix Workspace app for Mac provides default keyboard settings tailored to the Virtual Desktop Agent (VDA) OS, ensuring an optimal input experience and simplifying configuration for end users. This feature is enabled by default. For more information, see Enhanced keyboard settings for VDA OS and session type.

Optimized graphics performance for selective Thinwire

Starting with version 2503, these enhancements optimize text display performance, providing a smoother and more efficient user experience. Graphic performance improvements for Thinwire with Selective H.264 significantly reduce CPU and Graphics Processing Unit (GPU) usage in scenarios such

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

as rapidly scrolling through text scenes. Users also benefit from improved frame rates and reduced memory usage. This feature is enabled by default. For more information, see Optimized graphics performance for selective Thinwire.

UCSDK deviceID enhancement

The Unified Communications SDK (UCSDK) extends support to WebRTC-based applications, enabling Contact Center and Unified Communications providers to optimize real-time voice and video calls in Citrix Virtual Desktop Infrastructure (VDI) environments by offloading media processing to the user's device. This feature is enabled by default. For more information, see UCSDK deviceID enhancement.

Clipboard support for copying files and folders

Starting with version 2503, this enhancement enables clipboard support for seamless copying of files and folders between HDX sessions. Users can copy files and folders as permitted by their Citrix administrators, enhancing flexibility and productivity. For more information, see Clipboard support for copying files and folders.

Enhanced Multi-Monitor Management for desktop sessions

Starting with version 2503, the Multi-Monitor Selector (MMS) enables users to select which displays to use in full-screen mode for desktop sessions exclusively, not for seamless sessions. A new Multi-Monitor button appears in the toolbar only when multiple screens are connected, offering a more customized and efficient user experience. This feature is enabled by default. For more information, see Enhanced Multi-Monitor Management for desktop sessions.

Loss tolerant mode for graphics

Starting with Version 2503, this feature enables Citrix Workspace app for Mac to use the loss tolerant mode for graphics in Citrix sessions, improving the video experience, particularly in poor network conditions. For more information, see Loss tolerant mode for graphics.

USB Redirection of mass storage devices

Starting with version 2503, USB redirection enables you to access USB mass storage devices connected to a local computer from your virtual apps and desktops, allowing you to use USB drives seamlessly within virtual sessions. This feature is enabled by default. For more information, see USB Redirection of mass storage devices.

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

HDX direct support

Starting with version 2503, HDX Direct allows direct connections from external client devices to Virtual Delivery Agent (VDA), bypassing the Citrix Gateway service. This feature improves performance and reduces latency for both internal and external users through a direct path to the session host, resulting in fewer network hops and improved in-session performance. Also, the decreased load on the Citrix Gateway service enhances the overall system efficiency. This feature is enabled by default. For more information, see HDX direct support.

Enable Audio Quality Enhancer to improve audio performance

Starting with the 2503 version, Audio Quality Enhancer (v2) is added for Adaptive Audio.

Audio Quality Enhancer effectively manages short periods of packet loss and disruptions by intelligently reconstructing audio from previous samples in real-time, thus preventing noticeable degradation in quality. Furthermore, it intelligently and adaptively recovers lost audio packets, if and only when needed. For more information, see Enable Audio Quality Enhancer to improve audio performance.

Hybrid launch support using GACS for on-premises stores

Starting with version 2503, Citrix Workspace app for Mac supports management using Global App Configuration Service (GACS) for hybrid launch. In a hybrid launch scenario, users access Citrix resources through a web browser. When an application or desktop is selected, Citrix StoreFront generates an ICA file with the necessary launch instructions. The locally installed Citrix Workspace app then reads the ICA file, and establishes a secure connection to the remote application or desktop. For more information, see Hybrid launch support for GACS for on-premises store.

Enhancing hybrid mode support with GACS for cloud stores (Technical Preview)

Starting with version 2503, Citrix Workspace app for Mac supports Global App Configuration service (GACS) in Hybrid mode for Cloud stores, leveraging the Citrix workspace launcher. For more information, see Enhancing hybrid mode support with GACS for cloud.

Deprecation announcement of macOS Monterey 12

Starting with the 2503 version, support for macOS Monterey 12 is deprecated. As an alternative, you can upgrade to the latest available version of Mac. For more information, see Deprecation.

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

Support for sharing system audio on Microsoft teams

Starting with the 2503 version, Citrix Workspace app for Mac supports sharing the system audio during the Microsoft Teams meeting.

For more information, see Support for sharing system audio on Microsoft teams.

Limitations This feature is supported only on published desktops.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 134.1.1.24, based on Chromium version 134. For more information, see Citrix Enterprise Browser documentation.

Fixed issues in 2503

- Citrix Viewer might become unresponsive after the Mac display automatically powers off. [CVADHELP-27606]

Known issues in 2503

- Citrix sessions might fail to launch when using this specific policy combination: **Session Reliability Connections** set to **Prohibited** and **HDX adaptive transport** set to **Preferred**.

  Administrators can resolve this issue by implementing at least one of the following workarounds:

  - **Enable Session Reliability Connections**
    - Set the Citrix policy **Session Reliability Connections** to **Allowed**.
  - **Disable HDX Adaptive Transport**
    - Set the Citrix policy **HDX adaptive transport** to **Off**.
- USB Mass Storage devices might fail to redirect using the Generic USB virtual channel on macOS 15.4 and later. As a workaround, use Dynamic Client Drive Mapping (DCDM) to access the USB Mass Storage. [HDX-87197]

2411.10

What's new

This release addresses areas that improve overall performance and stability.

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

Deprecation announcement of XenApp® Services

Citrix is planning to deprecate the XenApp Services (also known as PNAgent) in future releases. For more information, see Deprecation.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 132.1.1.25, based on Chromium version 132. For more information, see the Citrix Enterprise Browser documentation.

Fixed issues

- Citrix Workspace app for Mac becomes unresponsive when using Microsoft Teams. [HDX-74085]
- When Authentication Domain of Cloud Store changes, Citrix Workspace app might not function properly and requires deletion and addition of Store account. [RFMAC-17025]

2411

What's new

- Enhancing Citrix security with pre-populated user name
- Version control using MDM and GACS
- Auto updates support scheduling
- Auto-update enhancement for active users
- UCSDK HID Implementation
- Enhanced keyboard and IME diagnostics tool
- HDX Direct
- Support for log collection when session launch fails
- Support for plug and play webcam redirection
- Seamless drag and resize improvements
- Support for browser content redirection (Technical Preview)
- Enhanced display control with Multi-Monitor selector (Technical Preview)
- USB Redirection of mass storage devices (Technical Preview)
- HDX Direct for non-shield scenario (Technical Preview)
- Enable Audio Quality Enhancer to improve audio performance (Technical Preview)
- Mandate end users to authenticate and access apps and desktops through native app
- Auto-update support for user groups

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

Enhancing Citrix security with pre-populated user name

Starting with version 2411, administrators can use Mobile Device Management (MDM) to push the user name in a specific format to manage devices. Citrix Workspace app reads this configuration, retrieves the user name, and pre-populates it within the authentication prompt, making it read-only. This ensures that only end users to whom a Mac is registered can authenticate to the Citrix Workspace app on that specific machine. This feature enhances sign-in security and gives administrators greater control over authentication. For more information, see Enhancing Citrix security with pre-populated user name.

Version control using MDM and GACS

Starting with version 2411, administrators can configure Citrix Workspace version control and Client App Management using Mobile Device Management (MDM) and Global App Configuration Service (GACS). This capability enables administrators to configure the start date and end date for auto-update of specific versions of Citrix Workspace app. For more information, see Version control using MDM and GACS.

Support for auto-update scheduling

Starting with version 2411, admins can schedule auto-updates for the Citrix Workspace app during convenient hours. This capability allows them to determine the rollout period, minimizing disruption to end-users, and improving adoption of the auto-update service, which was previously controlled by Citrix. Additionally, admins can specify the time of day for users to receive notifications about available updates. For more information, see Support for auto-update scheduling.

Auto-update enhancement for active users

Starting with version 2411 of Citrix Workspace app for Mac, the auto-update feature has been enhanced to trigger only for active users. This change aims to provide better control by ensuring that auto-update is available only for users with Global App Configuration service (GACS) or Mobile Device Management (MDM) policies, or who are actively using the app. For more information, see Auto-update enhancement for active users.

Support for WebHID API in UCSDK

Starting with the 2411 version, Citrix Workspace app for Mac supports the WebHID API to redirect Human Interface Devices (HIDs) from endpoint to Unified Communication SDK application on the VDI. It complies with the HID standard for bi-directional communication between the application based

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

on UCSDK and the HID devices connected to the endpoint. For more information, see Support for WebHID API in UCSDK.

Enhanced keyboard and IME diagnostics tool

Starting with version 2411, a new self-service command-line tool hosted in **Windows Virtual Delivery Agent (VDA)** is supported by **Citrix Workspace app for Mac** to diagnose keyboard and Input Method Editor (IME) related issues. This tool meets various user requirements, provides platform versatility, and caters to personalized needs. For more information, see Enhanced keyboard and IME diagnostics tool.

HDX Direct

Starting with the 2411 version, Citrix Workspace app for Mac supports HDX Direct transport for the connection between Citrix Workspace app and the VDA server. For more information, see HDX Direct.

Support for log collection when session launch fails

Starting with version 2411, Citrix Workspace app for Mac supports direct log collection when session launch fails, allowing for quicker troubleshooting and easier access to logs. For more information, see Support for log collection when session launch fails.

Support for plug and play webcam redirection

Starting with the 2411 version, Citrix Workspace app for Mac supports plug and play (PnP) webcam redirection for Linux VDA and Windows VDA. With this feature, when you connect a built-in or external camera to your device, it is automatically detected in the virtual sessions. For more information, see Support for plug and play webcam redirection.

Seamless drag and resize improvements

Starting with version 2411, the seamless drag and resize enhancement feature is automatically enabled when Citrix Workspace app for Mac connects to a Windows VDA version 2311 or later. This enhancement provides a smoother drag and resize experience for virtual apps, ensuring seamless interaction. For more information, see Seamless drag and resize improvements.

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

Mandate end users to authenticate and access apps and desktops through native app

Starting with version 2411, admins can mandate users on Mac devices to access Citrix Workspace app exclusively through the native app. When this feature is enabled, users attempting to access the store URL and third-party browsers are automatically redirected to the Citrix Workspace app. This ensures they can take advantage of all the native app's capabilities and enjoy a seamless user experience. For more information, see Enforcing Citrix access using Citrix Workspace app.

Auto-update support for user groups

Starting with version 2411, customers can configure different app versions for different user groups through **Configuration Profile** in Global App Configuration Service (GACS). For more information, see Auto-update support for user groups.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 130.1.1.12, based on Chromium version 130. For more information, see the Citrix Enterprise Browser documentation.

Technical previews

- Support for browser content redirection
- Enhanced display control with Multi-Monitor selector
- USB Redirection of mass storage devices
- HDX Direct for non-shield scenario
- Enable Audio Quality Enhancer to improve audio performance

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

Fixed issues

- You might experience Server File Type Association (SFTA) redirection failure in an Mutual Transport Layer Security (mTLS) workflow when accessing internal URLs from Mac. [CVADHELP-26806]
- The webcam H.264 encoder has a bandwidth limit for resolutions up to 1080p. [HDX-69178]
- You might encounter issues deploying Citrix Workspace app for Mac through Intune. [CVADHELP-27098]

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

2409.10

What's new

This release addresses areas that improve overall performance and stability.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 128.1.1.32, based on Chromium version 128. For more information, see the Citrix Enterprise Browser documentation.

Fixed issues in 2409.10

- Citrix Workspace app for Mac might not function as expected if background elements are disabled. End user is prompted to enable background items. For more information, see Citrix Knowledge Center article - CTX691439. [RFMAC-15942]
- You might encounter issues with multi-monitor support, leaving one screen appearing gray. [HDX-70907]
- Transport Protocol status in the Connection Strength Indicator might incorrectly display a message indicating HTML5. [HDX-71031]
- You might see the session notification pop-up in the lower right corner and remain visible. [CVADHELP-26474]

2409

What's new

- Support for Mac VoiceOver on the virtual desktop and seamless app sessions
- Support for HTML format on the Citrix Workspace app for Mac clipboard
- Support for YUV444 color format
- Customize the Desktop Viewer toolbar
- Sustainability initiative from Citrix Workspace app
- Support for macOS 15 Sequoia
- Client App Management
- Support for restricting users to modify the update channel
- Support for Rapid Scan
- Enhanced virtual desktop screen resizing experience
- Enhanced desktop launch experience
- Enhanced clipboard support for HTML text, files and folders

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

- Support for managing composite USB device redirection using DDC policies
- Enhancements to the smart card reader authentication
- Enhanced Desktop Viewer toolbar
- Connection Strength Indicator
- HDX Direct (Technical Preview)
- Support for multiple webcam resolutions
- Support for Plug and play webcam redirection (Technical Preview)
- Feature flag management

Support for Mac VoiceOver on the virtual desktop and seamless app sessions

Starting with the 2409 version, Citrix Workspace app for Mac supports the Mac VoiceOver feature within a virtual desktop and seamless app sessions. This feature allows users to receive verbal descriptions of UI elements and content within the sessions. These features enhance accessibility and ensure compliance with WCAG requirements.

Support for HTML format on the Citrix Workspace app for Mac clipboard

Starting with version 2409, Citrix Workspace app for Mac supports the seamless copying and pasting of HTML-formatted text between a Mac local app and a virtual app or desktop session running through Citrix Workspace app for Mac. Whether you're working locally or in a virtual session, this functionality ensures that HTML content is accurately retained during the copy-and-paste process. With this feature, you can copy and paste large HTML text between local and virtual sessions without any restrictions. For more information, see Support for HTML format on the Citrix Workspace app for Mac clipboard.

Support for YUV444 color format

Starting with the 2409 version, Citrix Workspace app for Mac introduces support for the YUV444 color format. YUV444 is a color format that provides better color accuracy and image clarity compared to the default YUV420 format. It ensures more vibrant and accurate colors, especially when working with multimedia content. This enhancement improves video playback quality and image fidelity. For more information, see Support for YUV444 color format.

Customize the Desktop Viewer toolbar

Previously, you can completely disable the **Desktop Viewer** toolbar. However, you can't enable or disable a few options on the toolbar. With this release, you can customize the Citrix Workspace app for Mac toolbar by adding and removing options on the toolbar. For more information, see Customize the Desktop Viewer toolbar.

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

Sustainability initiative from Citrix Workspace app

Starting with the 2409 version, Citrix Workspace app for Mac supports the **Sign out** option for the virtual desktop session. This feature might help conserve energy if you sign out from virtual machines when not in use. For more information, see Sustainability initiative from Citrix Workspace app.

Support for macOS 15 Sequoia

Citrix Workspace app for Mac is supported on macOS 15 Sequoia.

Client App Management

Starting with version 2409, Citrix Workspace app for Mac offers Client App Management capability that makes the Citrix Workspace app a single client app required on the end point to install and manage agents such as Citrix EndPoint Analysis (EPA) and Zoom VDI plug-ins. With this feature, administrators can easily deploy and manage required agents from a single management console. You can configure this feature using the Global App Configuration service (GACS). For more information, see Client App Management.

Support for restricting users to modify the update channel

Starting with the 2409 version, the Citrix Workspace app for Mac allows the admin to manage the **Select the update channel** option. With this feature, you have control over the update channel preference, ensuring that end users cannot modify it. This ensures that the update channel remains consistent and secure, as per your administrative settings. For more information, see Support for restricting users to modify the update channel update.

Support for Rapid Scan

Starting with the 2409 version, Citrix Workspace app for Mac supports the Rapid scan feature. You can use this feature to scan multiple documents with an iOS device, and then transfer those scanned documents to a Mac device using the Citrix Workspace app for Mac and iOS. For more information, see Support for Rapid Scan.

Enhanced virtual desktop screen resizing experience

Starting with the 2409 version, Citrix Workspace app for Mac ensures a smooth transition and prevents dark screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

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

Enhanced desktop launch experience

Starting with version 2409, Citrix Workspace app for Mac ensures an enhanced desktop launch experience. You'll 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.

Support for multiple webcam resolutions

Previously, only the VGA resolution (640 x 480 pixels) was supported for webcam redirection. Starting with the 2409 version, high-definition webcam streaming supports all webcam resolutions up to 720p are available on the client side. If media type negotiation fails, HDX now defaults back to VGA resolution. For more information, see High-definition webcam streaming.

Enhanced clipboard support for HTML text, files, and folders

Starting with version 2409, Citrix Workspace app for Mac supports the seamless copying and pasting of HTML-formatted text, files, and folders between a Mac local app and a virtual app or desktop session running through Citrix Workspace app for Mac. For more information, see Enhanced clipboard support for HTML text, files, and folders.

Support for managing composite USB device redirection using DDC policies

Starting with the 2409 version, you can manage the composite USB device redirection using the DDC policies. For more information, see Support for managing composite USB device redirection using DDC policies.

Enhancements to the smart card reader authentication

Starting with the version 2409, Citrix Workspace app supports the Fast smart card feature. Fast Smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance significantly when smart cards are used in high-latency WAN environments. For more information, see Enhancements to the smart card reader authentication

Enhanced Desktop Viewer toolbar

Starting with the 2409 version, the virtual **Desktop Viewer** toolbar is enhanced to be more intuitive, modern, and user-friendly. With this feature, you can now customize the Citrix Workspace app toolbar

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

by adding and removing options on the toolbar. For more information, see Enhanced Desktop Viewer toolbar

Connection Strength Indicator

Starting with version 2409, Citrix Workspace app for Mac supports the Connection Strength Indicator (CSI) on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. By clicking the icon, you can view real-time connection statistics for the client, gateway, and VDA, and copy diagnostic information to share with IT for advanced troubleshooting. For more information, see Connection Strength Indicator

Feature flag management

Citrix is changing the way it manages feature flags, allowing access to preview features and enabling dynamic management of features in production. To ensure optimal functioning of features which are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`. For more information, see Feature flag management.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 128.1.1.32, based on Chromium version 128. For more information, see the Citrix Enterprise Browser documentation.

Fixed issues in 2409

- You might notice that the settings configured for Citrix Workspace app using the Global App Configuration Service are not applied on the Mac device. [CVADHELP-25674]
- When you customize the themes for Citrix Workspace app for Mac on StoreFront™ deployment, you might notice that the menus or text on the UI become invisible based on the themes applied. [CVADHELP-25427]
- When using the built-in camera in the virtual desktop session, you might notice that the video is stretched in the output. [HDX-66510]
- You might experience URL redirection failures for URLs containing "%2f". [CVADHELP-26067]
- When using Citrix Workspace app for macOS to run the new Teams in optimized mode, you might notice that the peer user cannot take control. [CVADHELP-26227]
- When Plug and Play (PnP) is enabled, you might fail to switch webcam from the apps that shows only one camera with a generic name 'Citrix HDX Web Camera'. [HDX-69729]

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

2405.11

What's new

Citrix Workspace app for Mac 2405.10 has been rolled back due to a bug. The bug has been fixed in Citrix Workspace app for Mac 2405.11.

Citrix Workspace app for Mac 2405.11 release addresses a few issues that help to improve overall performance and stability.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 126.1.1.22, based on Chromium version 126. For more information, see the Citrix Enterprise Browser documentation.

Fixed issues in 2405.11

- When you open the Citrix Workspace app for Mac through the custom web portal, you might notice that the links on the landing page direct you to blank pages. [CVADHELP-25665]
- You might have noticed that the newly added apps are not visible to the end user on the automatic refresh of Citrix Workspace app. [CVADHELP-25189]
- When the Citrix Viewer is moved to an external monitor, you might notice that the Citrix Viewer disappears if you unplug the external monitor. [HDX-68620]

2405

What's new

Enhanced the High DPI option Previously, Citrix Workspace app supported the **High DPI** option for virtual desktop sessions only.

Starting with the 2405 release, enabling the **High DPI** option can also support for seamless app sessions. Also, you can now enable the High DPI option on three 4k monitors. These features are disabled by default. For more information, see Enhanced the High DPI option.

Store-based configuration of file access

Starting with the 2405 release, the per-store file access is included as part of the client-selective trust feature. This enhancement allows you to provide access to files on a per store basis. For more information, see Store-based configuration of file access.

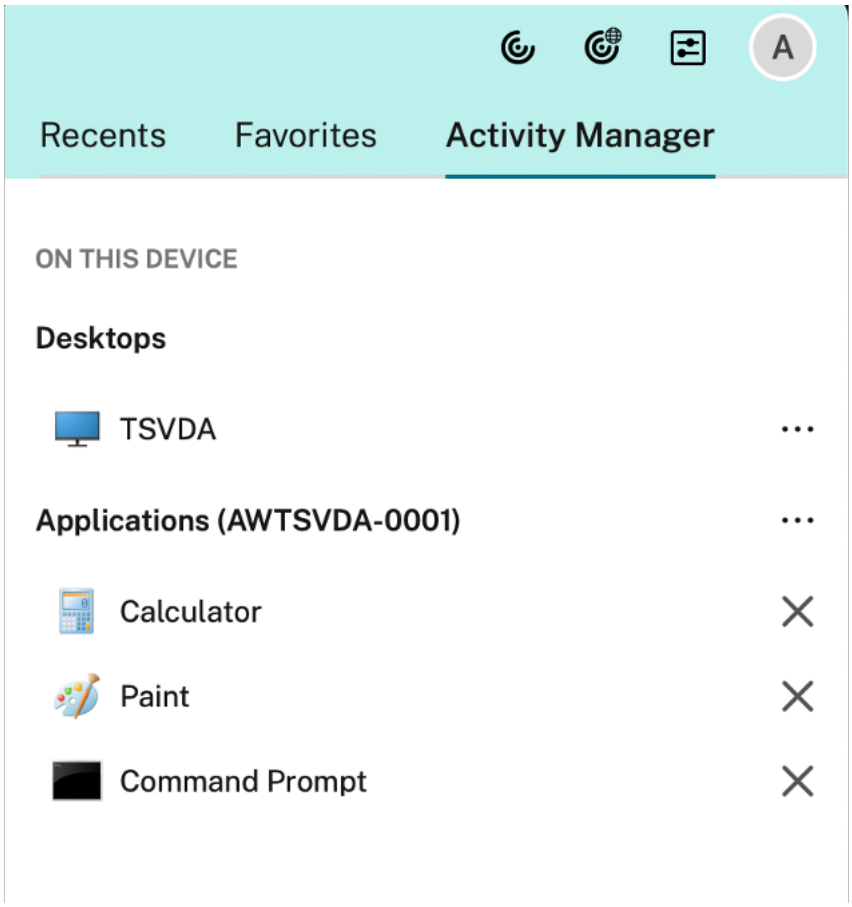
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for unified build for both Apple silicon and Intel-based Mac devices Previously, Citrix Workspace app for Mac provided separate build to support natively on Apple silicon and Intel-based Mac devices.

Starting with the 2405 version, Citrix Workspace app for Mac supports a single unified build that is compatible natively on both Apple silicon and Intel-based Macs.

Support for Mac with M3 chips Starting with the 2405 version, Citrix Workspace app for Mac supports the Mac with M3 series along with the M1 and M2 series that was previously supported.

Support for Activity Manager on the quick access menu for cloud stores Starting with the 2405 version, Citrix Workspace app for Mac supports the Activity Manager feature. This feature lets end users view and interact with all their active apps and desktop sessions at one place. You can disconnect or terminate the active sessions directly from the Activity Manager. For more information, see Support for Activity Manager on the quick access menu for cloud stores and Activity manager.



Support for resetting Citrix Workspace app Starting with the 2405 version, Citrix Workspace app for Mac supports the **Reset App Data** option. This feature allows users to quickly resolve issues result-

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

ing from conflicts caused by cache or settings by resetting the app and get unblocked without external assistance.

When you reset the Citrix Workspace app:

- The app is reverted to its default state (similar to just after fresh installation).
- All caches are cleared.
- Any added stores are removed.
- Preference settings are returned to their default state.

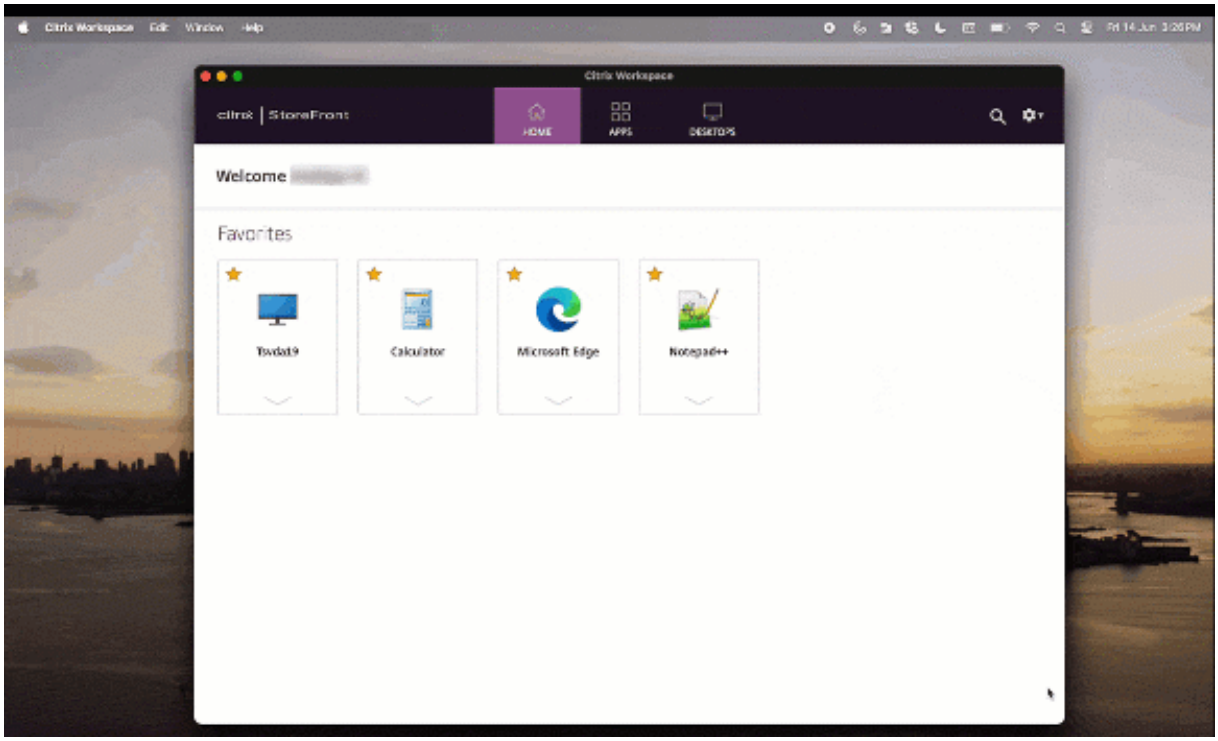
For more information, see Support for resetting Citrix Workspace app.

Support for device touch ID for FIDO2 password-less authentication Previously, Citrix Workspace app supported FIDO2 password-less authentication through the roaming authenticators (USB only) with PIN code and touch.

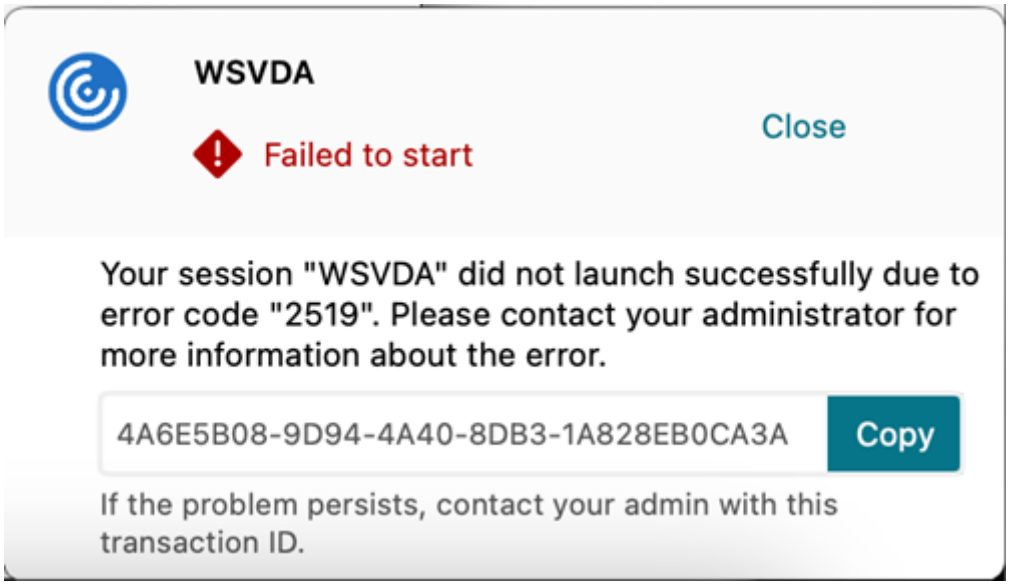
Starting with the 2405 version, Citrix Workspace app now supports device touch ID for FIDO2 password-less authentication, enhancing the sign-in experience for users. With this feature, users can securely sign in to the store configured on the Citrix Workspace app using the device touch ID, eliminating the need for passcodes or passwords. This feature enhances both the usability and security of Citrix Workspace app for macOS users. This feature is enabled by default. For more information, see Support for device touch ID for FIDO2 password-less authentication.

Enhanced virtual apps and desktops launch experience for on-premises stores and custom web portals Starting with the 2405 version, the enhanced virtual apps and desktops launch experience is now supported for on-premises stores and custom web portals. This feature enhances the opening experience of Citrix resources to be more intuitive, informative, and user-friendly.

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



The launch progress notification now appears at the lower-right corner of your screen. A progress status of the resources, which are in the process of being opened is shown. You cannot retrieve the notification once you dismiss it. The notification stays for a few seconds from the time you start the session. If the session fails to start, then the notification shows the failure message.



For more information, see Enhanced virtual apps and desktops launch experience.

Support for automatic installation of the End-Point Analysis (EPA) plug-in with Citrix Workspace app Previously, users were required to manually download and install the End-Point Analysis (EPA)

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

plug-in during the Citrix Workspace app login.

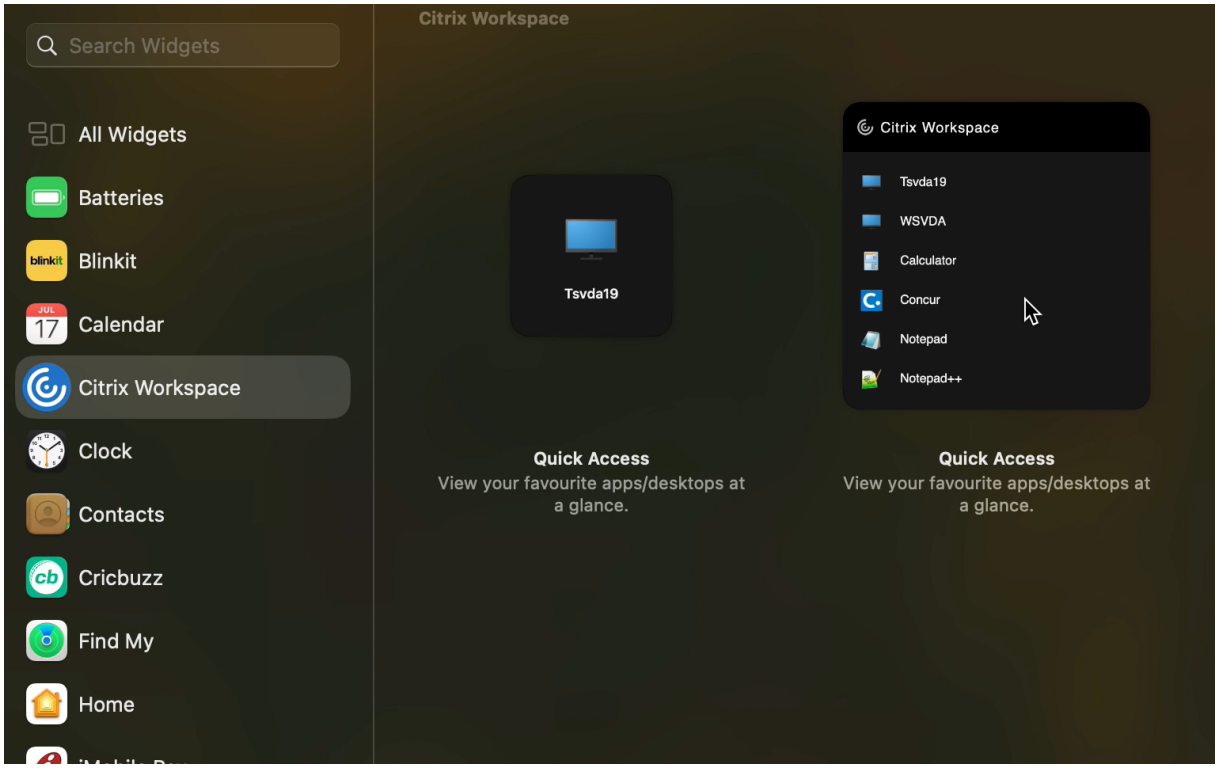
Starting from 2405 version, Citrix Workspace app supports the automatic installation of the EPA plug-in during installation or updates. When you install or update Citrix Workspace app, the EPA plug-in is included by default. This enhancement eliminates the need for separately installing the EPA plug-in, resulting in a smoother experience during Citrix Workspace app setup. For more information, see Support for automatic installation of the End-Point Analysis (EPA) plug-in with Citrix Workspace app.

Support for optionally installing Citrix Enterprise Browser Starting with 2405 version, you have the flexibility to choose whether to install Citrix Enterprise Browser during the installation of the Citrix Workspace app for Mac. Also, if you've already installed Citrix Enterprise Browser with Citrix Workspace app, you can uninstall Citrix Enterprise Browser using the Global App Configuration service and Mobile Device Management (MDM). This feature allows administrators to maintain compliance by controlling whether Citrix Enterprise Browser is allowed for use on their managed devices. For more information, see Support for optionally installing Citrix Enterprise Browser.

Support for Citrix Workspace widgets Starting with the 2405 version, Citrix Workspace app for Mac supports widgets for quick access to its virtual apps and desktops. With this feature, you can easily access your favorite virtual apps and desktops from the widget that is added to your desktop or Notification center.

Citrix Workspace supports two types of widgets, small and large widgets. The small widget can hold either one virtual app or desktop. The large widget can hold six favorite virtual apps and desktops with desktop listed at first. For more information, see Support for Citrix Workspace widgets.

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



Provision to manage multiple proxy servers using PAC files Starting with the 2405 version, you can use multiple proxy servers that allow the HDX sessions to select appropriate proxy servers for accessing specific resources. This selection is based on the proxy rules configured in the Proxy Auto-Configuration (PAC) file. Using this file, you can manage the network by mentioning which network traffic must be sent through a proxy server and which must be sent directly. Also, the PAC URL supports both **http://** and **file://** protocols. For more information, see Provision to manage multiple proxy servers using PAC files

Upgraded version of WebRTC for the optimized Microsoft Teams The version of WebRTC that is used for the optimized Microsoft Teams is upgraded to version M117. For more information, see Upgraded version of WebRTC for the optimized Microsoft Teams.

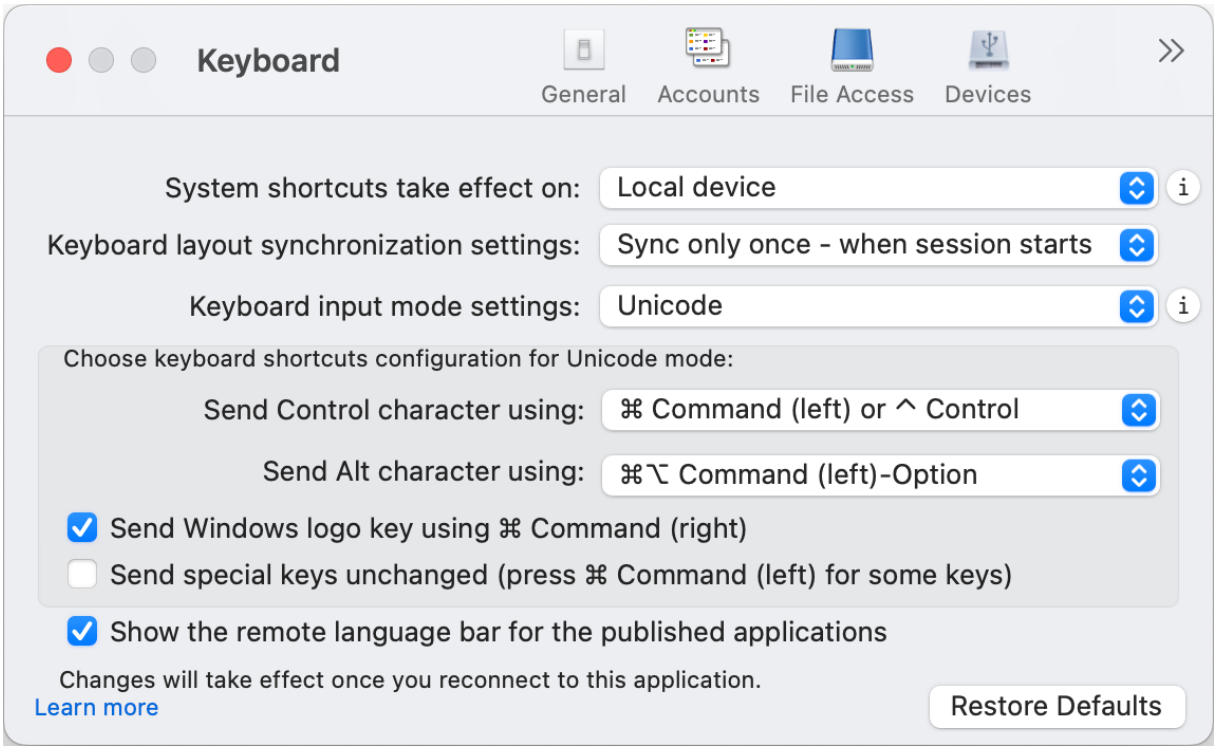
Support for printing PDF documents with selected orientation Starting with the 2405 version, you can now print PDF documents with the correct orientation whether it's portrait or landscape. This feature ensures that the printed output aligns perfectly with the intended layout. This feature is enabled by default. For more information, see Support for printing PDF documents with selected orientation.

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

Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac Starting with the 2405 version, the Citrix Virtual Channel Software Development Kit (VCSDK) supports the desktop and screen sharing VCSDK API and gbuffer sharing.

For more information, see Virtual driver screen sharing and app-sharing functions.

Enhancement to the keyboard Settings Starting with the 2405 version, Citrix Workspace app now provides an improved keyboard settings user interface (UI) by categorizing setting options and adding helpful tip icons. Enhancement to the keyboard Settings.



Support for extending the desktop session to external monitors automatically Starting with the 2405 version, Citrix Workspace app supports the extension of desktop sessions to external monitors automatically. With this feature, when you launch the desktop session on the endpoint, if the external monitors are already connected to the endpoint, then the session is extended to external monitors automatically. When you disconnect the external monitor, the session can automatically adjust to extend only to the connected monitors. For more information, see Support for extending the desktop session to external monitors automatically.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 126.1.1.20, based on Chromium version 126. For more information, see the Citrix Enterprise Browser documentation.

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

Modify the user-agent of Citrix Enterprise Browser Administrators can now modify the Citrix Enterprise Browser's user-agent for any internal web or SaaS apps. You can configure this setting through the Global App Configuration service. This feature provides the flexibility to create different variations of the user-agent for Citrix Enterprise Browser, which you can use for various uses.

One such use-case is the ability to restrict the internal web or SaaS apps to open only in Citrix Enterprise Browser. In addition to modifying the user-agent, you need to configure the Identity Provider (IdP) to perform a conditional check that verifies whether the end user is trying to open the app using Citrix Enterprise Browser or a native browser. The IdP opens the app only if the end user tries to access it using Citrix Enterprise Browser. This restriction prevents users from accessing sensitive information in these apps from other browsers.

For more information, see Use Case 3c - Restrict apps to Citrix Enterprise Browser by modifying its user-agent

Additional security restrictions for the Citrix Enterprise Browser Citrix introduces additional access restrictions to enhance the security and user experience of Citrix Enterprise Browser with Secure Private Access and Global App Configuration service (GACS).

Restrictions managed through Secure Private Access Copy

Administrators can enable or disable copying of data from a SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. The default value is Enabled.

For more information, see the Copy restriction in the Secure Private Access product documentation.

Paste

Administrators can enable or disable pasting of copied data into the SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. The default value is Enabled.

For more information, see the Paste restriction in the Secure Private Access product documentation.

Personal data masking

Administrators can use the **Personal data masking** restriction to mask various types of sensitive information such as credit card numbers, social security numbers, and dates. Also, you have the flexibility to define custom rules for detecting specific types of sensitive information and masking it accordingly. The **Personal data masking** restriction has the option to fully or partially mask the information.

For more information, see Personal data masking.

Upload restriction by file type

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

Administrators can restrict file uploads based on MIME (multi-purpose internet mail extensions) types. Unlike the **Uploads** policy, which allows you to enable or disable all file uploads, the **Upload restriction by file type** restriction allows you to enable or disable file uploads for specific MIME types.

For more information, see Upload restriction by file type.

Download restriction by file type

Administrators can restrict file downloads based on MIME (multi-purpose internet mail extensions) types. Unlike the **Downloads** policy, which allows you to enable or disable all file downloads, the **Download restriction by file type** restriction allows you to enable or disable file downloads for specific MIME types.

For more information, see Download restriction by file type.

Printer management

Enterprises can now prevent the printing of confidential documents and unauthorized data sharing. Admins can configure this policy through Secure Private Access. Admins can configure the behavior for network printers, local printers, and prints using the **Save as PDF** option.

The following options are available for administrators to control access to printers for the end users:

- **Network printers:** A network printer is a printer that can be connected to a network and used by multiple users.
    - **Disabled:** Printing from any network printers in the network is disabled.
    - **Enabled:** Printing from all network printers is enabled. If printer hostnames are specified, then all other network printers apart from the ones specified are blocked.

    > **Note:**
    >
    > Printers are identified by their hostnames.

- **Local printers:** A local printer is a device directly connected to an individual computer. This connection is typically facilitated through Bluetooth, USB, parallel ports, or other direct interfaces.
    - **Disabled:** Printing from all local printers is disabled.
    - **Enabled:** Printing from all local printers is enabled.
- **Print using Save as PDF**
    - **Disabled:** The Save as PDF option for saving the content in PDF format is disabled.
    - **Enabled:** The Save as PDF option for saving the content in PDF format is enabled.

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

> **Note:**
>
> - If the admin has disabled certain printing options, then those options appear grayed out to the end users.
> - End users can't use the network printer if it is renamed on their device.

Clipboard restriction for Security groups

In Secure Private Access, administrators can restrict clipboard access to any designated group of apps. These designated groups of apps are created as **Security groups** in Secure Private Access, so that the end users are permitted to copy and paste contents only within that Security groups. There is also an Advanced option to enable copy and paste contents between Security groups and other local apps on the machines or unpublished web apps.

For more information, see Clipboard restriction for Security groups.

Restrictions managed through Global App Configuration service Clipboard restriction

In GACS, administrators can use the **Enabled Sandboxed Clipboard** option to manage clipboard access. When you restrict clipboard access through GACS, all content copied from any website accessed within the Citrix Enterprise Browser can't be pasted outside the Enterprise Browser. Similarly, any content copied from native apps can't be pasted into any website accessed within the Enterprise Browser.

For more information, see Clipboard restriction.

Audio Capture Allowed

Administrators can use this setting to enable or disable audio capture access. When an administrator enables this setting, or leaves it unset, users are prompted to allow audio capture access. When an administrator disables this setting, these prompts are turned off, and audio capture is blocked.

For more information, see Audio Capture Allowed.

Video Capture Allowed

Administrators can use this setting to enable or disable video capture access. When an administrator enables this setting, or leaves it unset, users are prompted to allow video capture access. When an administrator disables this setting, these prompts are turned off, and video capture is blocked.

For more information, see Video Capture Allowed.

Technical Preview

- Support for Plug and play webcam redirection
- Support for managing composite USB device redirection using DDC policies

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

- Support for sharing system audio on Microsoft teams
- Enhancements to the smart card reader authentication
- Support for fast smart card
- Support for browser content redirection

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

Fixed issues in 2405

- When using the optimized Microsoft Teams in the virtual session, you might notice that the echo cancellation feature is not working in the virtual session. [HDX-65123]
- When using Citrix Workspace app on the macOS Sonoma, you might notice that the USB devices such as mouse and keyboard are not accessible locally once connected to the virtual session. [CVADHELP-2413]
- When using the optimized Microsoft Teams 2.1 in the virtual session, you might notice that the sender and receiver sees the video stretched with an incorrect aspect ratio during the call. [HDX-66354]
- After upgrading from Citrix Workspace app version 2402 or 2402.10 to 2405, you might rarely notice that the resource icons are not displayed correctly on Citrix Workspace app for the on-premises stores. For more information, see Citrix Knowledge Center article - CTX677048. [RFMAC-16042]

2402.10

What's new

This 2402.10 release addresses a few issues that help to improve overall performance and stability.

Enhancements to quit functionality of Citrix Workspace app Starting with the 2402.10 version, the quit functionality of Citrix Workspace app is improved and matches Apple's Quit menu behavior. When you exit the Citrix Workspace app using one of the following options, the app closes and no longer runs in the background.

- **Quit Citrix Workspace** from the menu bar,
- **Quit** from the dock,
- **Quit** from the Quick Access menu, or
- Press the **Command-Q** keys.

Fixed issues in 2402.10

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

- The security vulnerability that allowed local authenticated users to elevate their privileges to root users has been fixed. For more information, see CTX675851. [CVE-2024-5027]

2402

What's new

Improved loading experience of virtual apps and desktops for on-premises deployments Citrix Workspace app for Mac has improved the first-time user experience for on-premises deployments. After successful authentication, the enumeration of virtual apps and desktops is faster than before.

Support for H.265 video decoding Starting with the 2402 version, Citrix Workspace app for Mac supports the use of the H.265 video codec (HEVC) for hardware acceleration of remote graphics and videos. The h.265 video codec (HEVC) supports YUV 4:2:0 color space by default. H.265 video codec must be supported and enabled on both the VDA and Citrix Workspace app. If your Mac device doesn't support H.265 decoding using the VideoToolbox interface, then the H.265 decoding for graphics policy setting is ignored and the session falls back to the H.264 video codec. For more information, see Support for H.265 video decoding.

Support for system shortcuts on HDX desktop sessions Previously, the system keyboard shortcuts such as **Option-Command-ESC, Command-Space bar, Command-Tab, Control-Command-Q, Shift-Command-Q, Control Up/Down/Left/Right** took effect only on macOS locally since they were consumed by macOS at first.

Starting with the 2402 version, Citrix Workspace app for Mac supports passing the macOS system keyboard shortcuts to the VDA (HDX session) in window mode and full-screen mode. This feature allows you to set preferences on how the system shortcut must take effect on macOS locally or the HDX desktop session in window or full-screen mode.

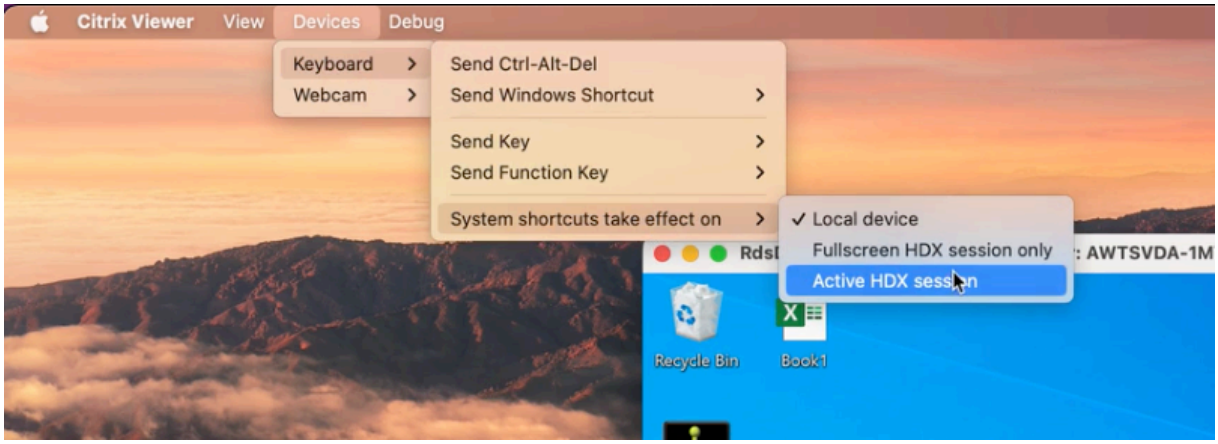
The following options in the keyboard settings allow you to control the system shortcuts:

- **Local device:** The system shortcuts can take effect only on macOS locally. It does not affect the HDX session. The **Local device** option is the default option.
- **Fullscreen HDX session only:** The system shortcuts take effect on HDX sessions when the session is in full-screen mode. If the session is in window mode or there are no active sessions, then the system shortcuts have no effect on HDX sessions.
- **Active HDX session:** The system shortcuts take effect on HDX sessions when the session is in window mode and full-screen mode. If there is no active HDX session or the active session window on the front, then the system shortcuts can take effect only on the macOS locally.

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

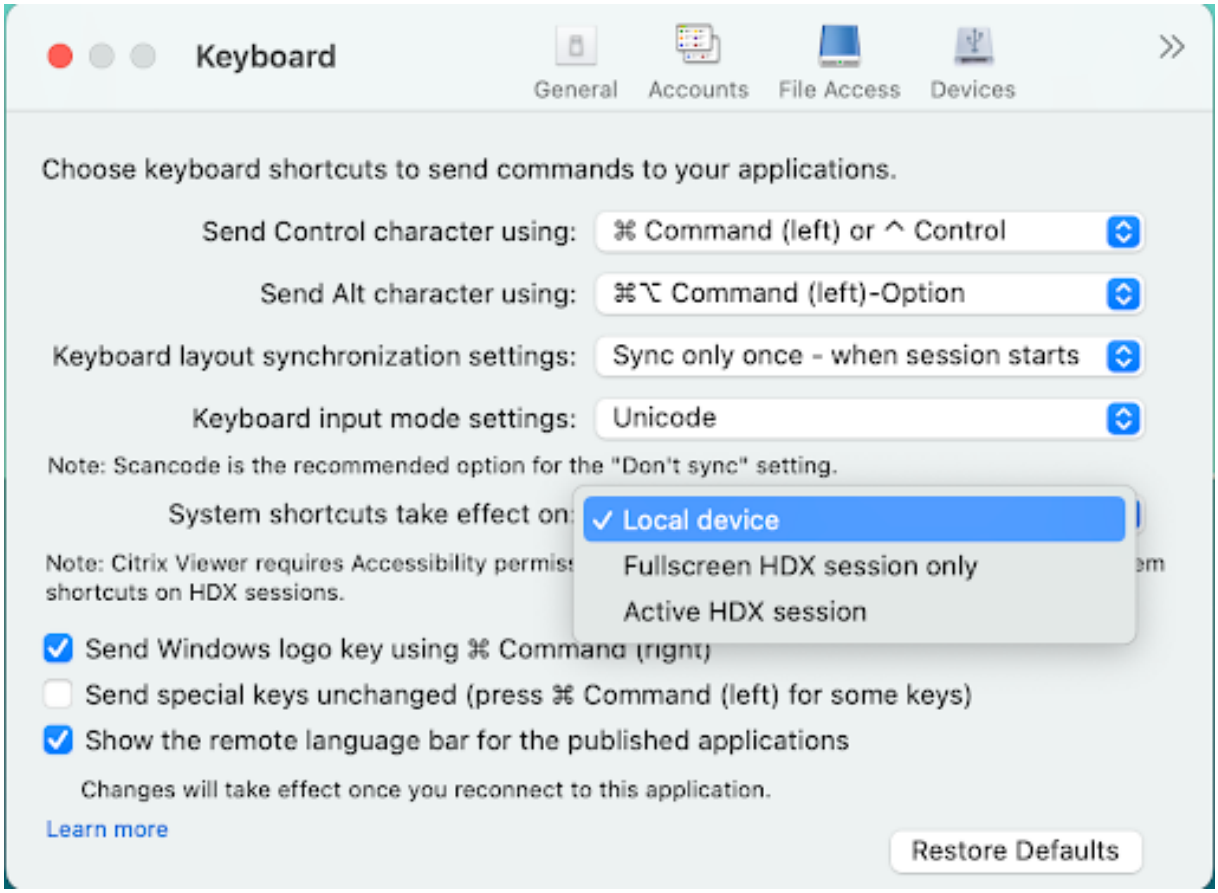
To enable the system shortcuts to take effect on the HDX session, open the HDX session. In the **Citrix Viewer** menu bar, navigate to **Devices > Keyboard > System shortcuts take effect on** and select **Fullscreen HDX session only** or **Active HDX session**.

> **Note:**
>
> When enabling system shortcuts for HDX sessions, you are prompted to provide accessibility access to Citrix Viewer to use this feature. To provide accessibility access to **Citrix Viewer**, click **Open System Settings** in the dialog box and enable accessibility access to **Citrix Viewer**. For more information, see Allow accessibility apps to access your Mac in the Apple support article.



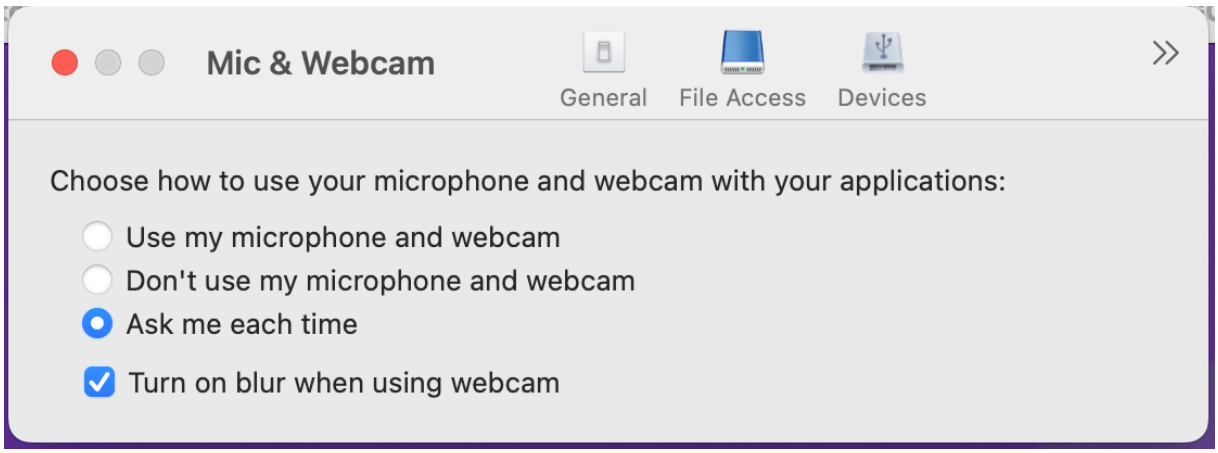
Alternatively, you can enable the system shortcuts to take effect on HDX sessions in full-screen or window mode by navigating to **Preferences > Keyboard**. Select **Fullscreen HDX session only** or **Active HDX session** options from the **System shortcuts take effect on** drop-down menu.

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



For more information, see Support for system shortcuts on HDX desktop sessions.

Support for background blur for webcam Starting with the 2402 version, Citrix Workspace app for Mac supports background blur when using a webcam. You can enable the background blurring feature by navigating to **Preferences > Mic & Webcam** and select **Turn on blur when using webcam**. For more information, see Support for background blur for webcam.



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

Support for audio volume synchronization Previously, audio volume control is independent between the Virtual Delivery Agent (VDA) and your device. You've to adjust the volume on both sides to maintain the desired volume. Also, if you've muted the volume in your device, then it restricts to unmute the volume in the VDA.

Starting with the 2402 version, Citrix Workspace app for Mac supports synchronization of audio volume between the VDA and your audio devices. You can now tune the volume using the VDA audio volume slider and have the same volume on your device and the other way around. By default, this feature is enabled. For more information, see Support for audio volume synchronization.

Loss tolerant mode for audio Starting with the 2402 version, Citrix Workspace app supports loss tolerant mode (EDT lossy) for audio redirection. This feature improves the user experience for real-time streaming when users are connecting through networks with high latency and packet loss. By default, this feature is enabled. For more information, see Loss tolerant mode for audio.

Upgraded HDX Reducer to Version 4 Previously, Citrix Workspace app for Mac supported HDX Reducer V3. Starting with the 2402 version, Citrix Workspace app for Mac supports HDX Reducer V4. This feature reduces the network bandwidth required for a typical session and improves response time. For more information, see Upgraded HDX Reducer to Version 4.

Support for screen sharing when App Protection is enabled Starting with the 2402 version, you can share content through Microsoft Teams with HDX optimization, even when App Protection is enabled. With this feature, you can share a screen in the virtual desktop session to its full potential. For more information, see Compatibility with HDX optimization for Microsoft Teams.

Enhanced Global App Configuration service Starting with the 2402 version, the enhanced Global App Configuration service (GACS) for Citrix Workspace now supports the following features:

- Settings are secured with user authentication
- Enhanced the discovery workflow
- Support for full StoreFront URL

For more information, see Global App Configuration service.

Support for administrator to restrict the user from changing the store name Previously, users were able to change the store name by using the **Edit Account** option.

Starting with the 2402 version, Citrix Workspace app for Mac provides administrators an option to restrict the user from changing the store name. With this feature, administrators can easily identify

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

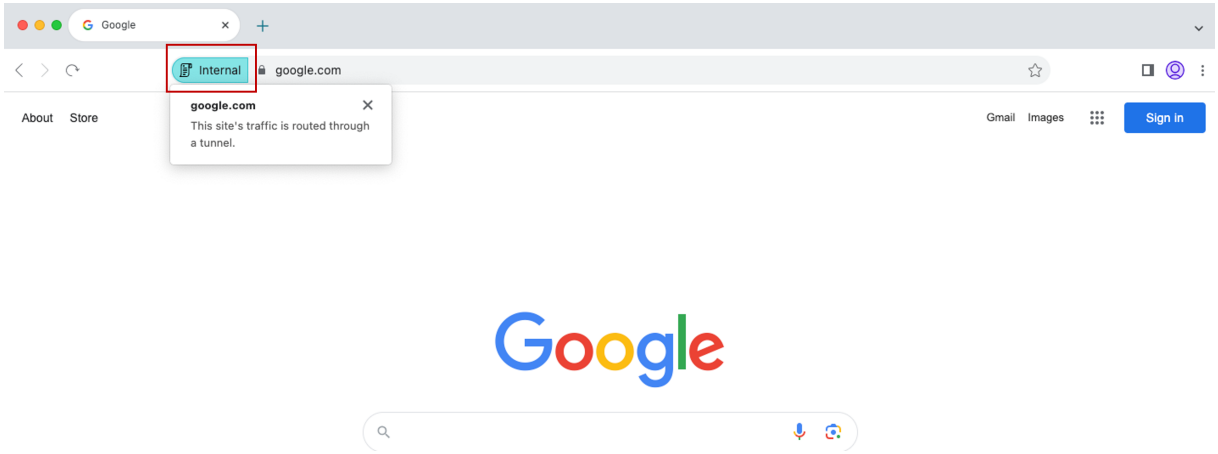
and maintain consistency in the store names. For more information, see Support for administrator to restrict the user from changing the store name.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 121.1.1.26, based on Chromium version 121. For more information, see the Citrix Enterprise Browser documentation.

Security indicator when visiting websites Citrix Enterprise Browser now displays a security indicator on the address bar when users visit any websites. The indicator aims to inform users about the security aspects of the websites, such as whether it is an internal site or if there are any potential security restrictions. The indicator provides more information when you click it. The indicator appears on the Enterprise browser by default, and it enhances the user experience.



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



Simplified single sign-on for Web and SaaS apps through the Global App Configuration service

> **NOTE:**
>
> For the Mac operating system, this feature was previously available only for StoreFront starting with the release 119.1.1.115. Now, with the release of 121.1.1.26, it is also available for Workspace.

Previously, single sign-on (SSO) was configured in Citrix Enterprise Browser using the PowerShell module. From this version, you can configure the simplified SSO feature in Citrix Enterprise Browser by using a newly introduced setting in the Global App Configuration service (GACS). Administrators can use this new setting to enable SSO for all web and SaaS apps in Citrix Enterprise Browser. This method eliminates the need for the complex PowerShell module.

For more information on how to manage SSO through GACS, see Manage single sign-on for Web and SaaS apps through the Global App Configuration service.

Citrix Enterprise Browser introduces additional settings in the Global App Configuration service

The following additional settings have been added into the Global App Configuration service (GACS) for configuring Citrix Enterprise Browser:

- "Enable autofill address"- Allows administrators to enable or disable the autofill suggestions for addresses.
- "Enable autofill credit card"- Allows administrators to enable or disable the autofill suggestions for credit card information.
- "Auto launch protocols from origins"- Allows administrators to specify a list of protocols that can launch an external app from the listed origins without prompting the user.
- "Enable command-line flag security warnings"- Allows administrators to display or hide security warnings, which appear when potentially dangerous command-line flags try to launch the Enterprise Browser.

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

- "Manage default cookies setting"- Allows administrators to manage cookies for a website.
- "Manage default pop-ups setting"- Allows administrators to manage pop-ups from a website.
- "Extension install sources"- Allows administrators to specify valid sources for users to install extensions, apps, and themes.
- "Disable lookalike warning pages"- Allows administrators to specify the preferred domains where lookalike warning pages don't display when the user visits pages on that domain.
- "Enable payment method query"- Allows administrators to enable websites to check whether the users have saved payment methods.
- "Manage saving browser history"- Allows administrators to manage the saving of Enterprise browser history.
- "Manage search suggestion"- Allows administrators to enable or disable search suggestions in the Enterprise browser's address bar.
- "Enable export bookmark"- Allows administrators to enable an option to export the bookmarks in the Enterprise Browser.
- "Force ephemeral profiles"- Allows administrators to clear or persist user profile data when users close the Enterprise Browser.

For more information, see Manage Citrix Enterprise Browser through Global App Configuration service.

Technical Preview

- Support for single sign-on to Citrix Secure Access automatically through Citrix Workspace app
- Client App Management for Zoom VDI plug-in
- Enhanced the Desktop Viewer toolbar
- Support for extending the desktop session to external monitors automatically

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

Fixed issues

- When connecting to Citrix Workspace app for Mac version 2311, you might get the following error message:

  Http/1.1 Internal Server Error 43524
  [CVADHELP-24631]

- You might notice that the Global App Configuration service policies are not applied on some older Mac devices. [CVADHELP-24863]

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

2311

What's new

Support for authentication using FIDO2 when connecting to on-premises store Previously, FIDO2 based password-less authentication was supported for connecting to cloud stores. For more information, see FIDO2 based authentication when connecting to cloud store.

With this version, users can also connect to on-premises stores using FIDO2 authentication. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. This feature currently supports roaming authenticators (USB only) with PIN code and touchID. This feature is supported on macOS 12 and later versions. For more information, see FIDO2-based authentication when connecting to on-premises store.

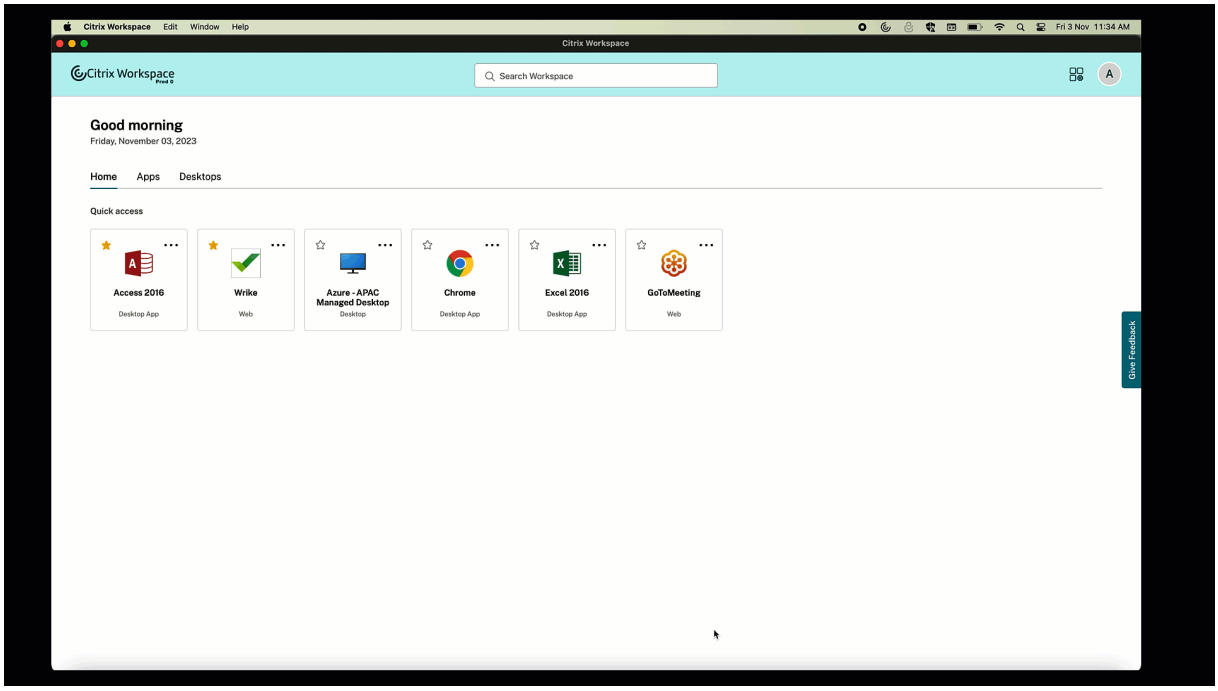
Enhanced Universal Architecture builds for virtual apps and desktops session Starting with the 2311 version, the Universal Architecture build can now automatically choose to run the virtual sessions in the native Apple Silicon mode or Intel mode on Macs with the Apple Silicon chipset. It uses the Rosetta emulation to launch the virtual session in Intel mode. The virtual session launches in the native Apple Silicon mode, if the virtual channel SDK is built based on the native Apple Silicon architecture or there's no virtual channel SDK. However, the virtual session launches in the Intel mode using the Rosetta emulation, if the virtual channel SDK is built based on the x86_64 Intel-based architecture.

This enhancement to the Universal Architecture build improves the launch experience on Macs with the Apple Silicon chipset. For users on Macs with the Intel-based chipset, there is no change, and the Universal Architecture build continues to run the virtual sessions natively.

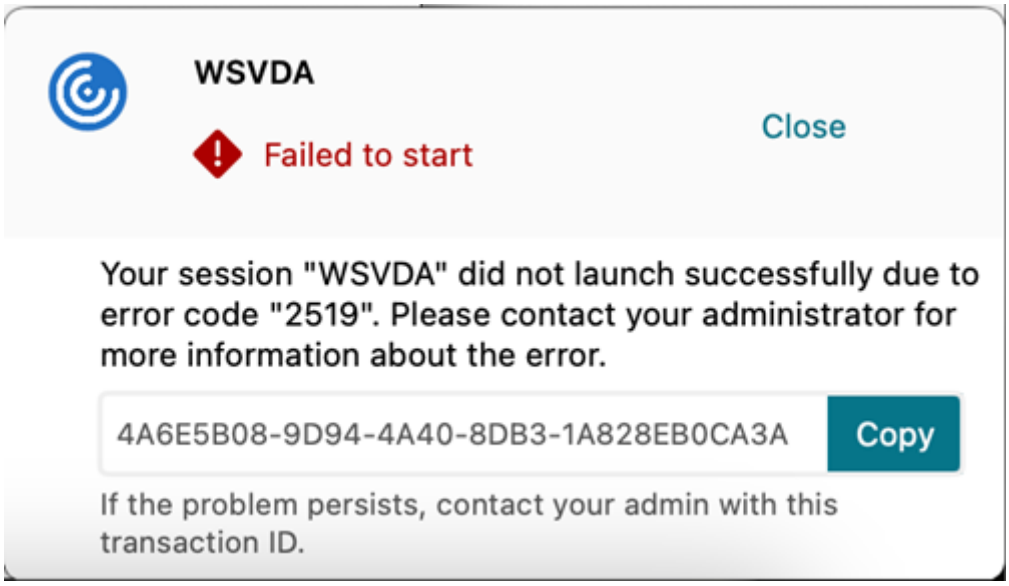
For more information, see Enhanced Universal Architecture builds for virtual apps and desktops session.

Enhanced virtual apps and desktops launch experience for Workspace (Cloud users only) The opening experience of Citrix resources has been enhanced to be more intuitive, informative, and user-friendly. From the 2311 version, this feature is supported for custom web stores and hybrid launch.

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



The launch progress notification now appears at the lower-right corner of your screen. A progress status of the resources, which are in the process of being opened is shown. You cannot retrieve the notification once you dismiss it. The notification stays for a few seconds from the time you start the session. If the session fails to start, then the notification shows the failure message. For more information, see Enhanced virtual apps and desktops launch experience for Workspace (Cloud users only).



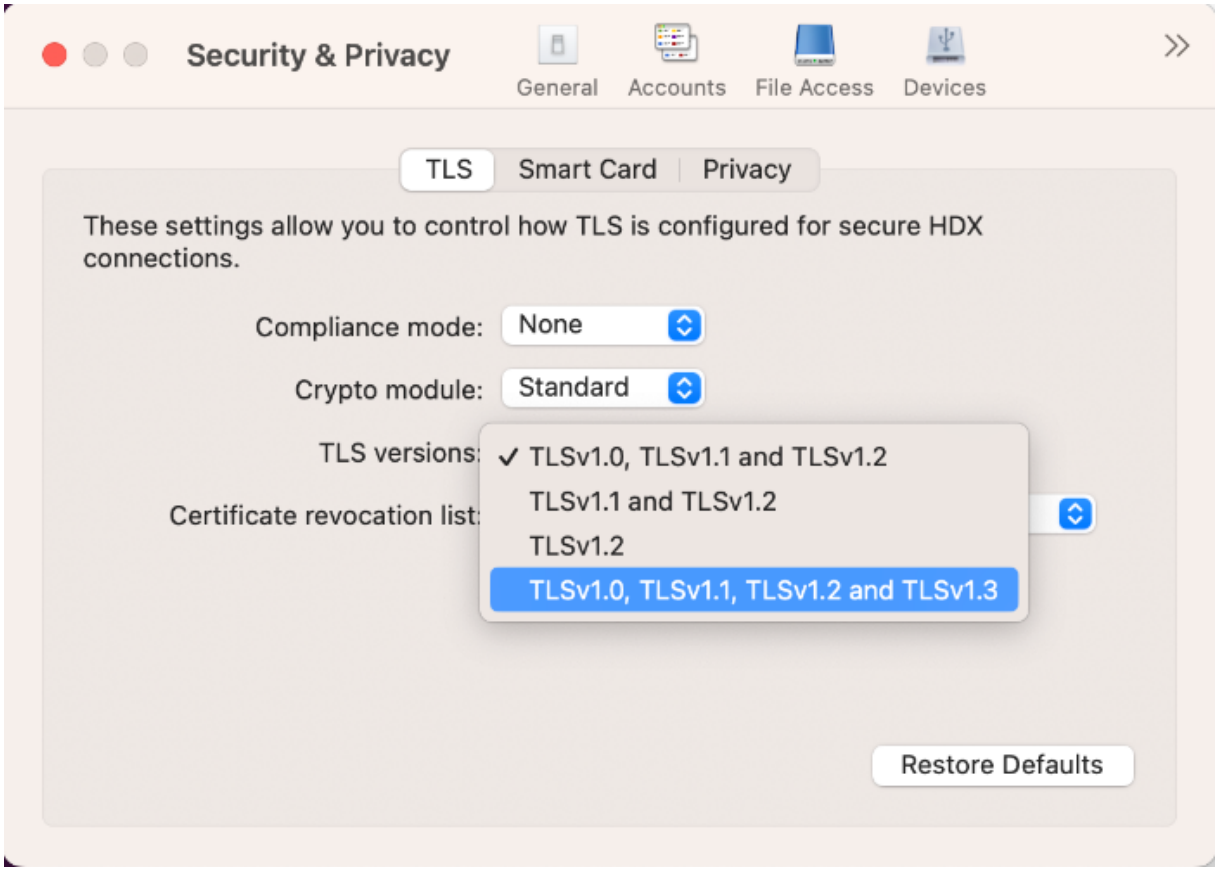
> **Note:**
>
> This feature is available for both Workspace (cloud) and StoreFront sessions.

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

Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac Starting with the 2311 version, the Citrix Virtual Channel Software Development Kit (VCSDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers. This version of the SDK supports writing new virtual channels and screen sharing for Citrix Workspace app for Mac.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Mac in the Developer documentation and Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac.

Support for TLS protocol version 1.3 Starting with the 2311 version, Citrix Workspace app for Mac supports the latest Transport Layer Security (TLS) version 1.3. To enable the TLS version 1.3, navigate to **Preferences > Security and Privacy > TLS** and select the **TLSv1.0, TLSv1.1, TLSv1.2 and TLSv1.3** option from the **TLS versions** drop-down menu.



For more information, see TLS.

Support for multiple audio devices Starting with the 2311 release, Citrix Workspace app for Mac displays all available local audio devices in a session with their names. In addition, plug-and-play is also supported. For more information, see Support for multiple audio devices.

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

Support for extending multiple monitors in full-screen mode on up to five monitors Previously, Citrix supported a maximum of three monitors in full-screen mode, including the primary monitor.

Starting with the 2311 version, you can now use full-screen mode on up to five monitors, including the primary monitor, at the same time. For more information, see Support for extending multiple monitors in full-screen mode on up to five monitors.

Deprecation of International menu from the keyboard settings Previously, you can enable or disable the **Use Client IME, Use Composing Mark and Use Client keyboard layout** features in the Citrix viewer by navigating to **Devices > Keyboard>International**.

From the 2311 version, the **International** menu for the keyboard settings in the Citrix Viewer is deprecated. From this version, the client-side IME is enabled by default. For more information, see Deprecation of International menu from the Keyboard settings.

Deprecation announcement of the SDP format (Plan B) from WebRTC Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use a version of Citrix Workspace app that supports the Unified Plan to continue using certain optimized Microsoft Teams functionalities. For more information, see Deprecation announcement of the SDP format (Plan B) from WebRTC.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 119.1.1.115, based on Chromium version 119. For more information, see the Citrix Enterprise Browser documentation.

Improved user experience Previously, Citrix Enterprise Browser displayed a reconnection modal when you attempted to perform an action after your session expired. Starting with Citrix Workspace app for Mac version 2311 (which corresponds to the Chromium version 119.1.1.115), there is no longer a reconnection modal. Instead, a loading icon now appears on the browser tab when you attempt to perform any action after your session expires.

Improved watermark design Citrix Enterprise Browser now has a new watermark design that is less intrusive and provides a better user experience.

Support for custom browser extension Citrix Enterprise Browser has expanded its extension capabilities. Previously, only extensions from the Chrome Web Store were permitted. Citrix Enterprise Browser now allows you to add custom extensions securely. Administrators can configure custom extensions as part of the mandatory list. End users can access and use these extensions either via

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

`citrixbrowser://extensions` or by clicking the **Extensions** option under **More** button as needed. For more information on how to configure the custom extensions, see Mandatory custom browser extension in the Citrix Enterprise Browser documentation.

Simplified SSO for Web and SaaS apps through the Global App Configuration service

> **Note:**
>
> This feature is available only for StoreFront.

Previously, SSO was configured in Citrix Enterprise Browser using the PowerShell module. From this version, this simplified SSO feature allows you to configure SSO in Citrix Enterprise Browser by using a newly introduced setting in the Global App Configuration service (GACS). Administrators can use this new setting to enable SSO for all web and SaaS apps in Citrix Enterprise Browser. This method eliminates the need for the complex PowerShell module. For more information on how to manage SSO through GACS, see the Manage single sign-on for Web and SaaS apps through the Global App Configuration service.

Enhanced capabilities on monitoring end user activities Previously, administrators were unable to monitor end user activities such as App accessed and Traffic type. Starting with Citrix Workspace app for Windows 2311 and Mac 2311 versions (corresponding to Chromium version 119.1.1.115), you can now monitor these details as well.

- **App accessed**: Enterprise Browser provides information about all the apps accessed by the end user, provided the app is listed in the policy document.
- **Traffic type**: Enterprise Browser provides information about whether data is sent directly or through Secure Private Access authentication.

To monitor the end user activities from the Enterprise Browser, use the Citrix Analytics service using your Citrix Cloud account. After signing in to Citrix Cloud, navigate to **Analytics > Security > Search**. There, you can refer to **Apps and Desktops** under the **Self-Service Search** section. For more information on Citrix Analytics, see Getting started.

App Protection

Support to configure App Protection for Authentication and Self-Service plug-in for on-premises stores Previously, Citrix Workspace app for Mac supported configuring App Protection for Authentication and Self-Service plug-in using the Global App Configuration service UI for customers on cloud stores only.

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

Starting with the 2311 release, this feature is supported for customers on both cloud and on-premises stores. For more information, see Configuration using the Global App Configuration service UI in the App Protection documentation.

Technical Preview

- Loss Tolerant mode for Audio
- Support for Audio volume synchronization
- Support for H.265 video decoding
- Upgraded HDX Reducer to Version 4

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

Fixed issues in 2311

- When the first time users add the Store URL, they might not see the FIDO2 authentication browser window. [RFMAC-14518]
- When using Citrix Workspace app for Mac to access virtual sessions, the mouse scrolling speed might be too fast or too slow in the virtual sessions. [CVADHELP-23514]
- When using Citrix Workspace app for Mac, you might not be able to switch between recent apps inside the virtual app session by clicking `Options + tab` keys after upgrading to VDA 2212 or later. [CVADHELP-23464]
- You might notice that the macOS dock is blocking the windows taskbar of the Remote Desktop Protocol app session launched from Citrix Workspace app for Mac. [CVADHELP-23681]
- When using Citrix Workspace app for Mac, you might experience issue with authentication when persistent session is used for on-premises store. [CVADHELP-24062]

2309

What's new

Support for macOS 14 Sonoma Citrix Workspace app for Mac is supported on macOS 14 Sonoma.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 115.1.1.103, based on Chromium version 115. For more information, see Citrix Enterprise Browser documentation.

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

Citrix will now release independent upgrades for Citrix Enterprise Browser. Starting with Citrix Workspace app 2309 for Mac, you can upgrade Citrix Enterprise Browser independently to compatible versions through the auto-update feature or install manually when the upgrades are available at Downloads. The independent upgrades of Citrix Enterprise Browser are supported only on the latest version of Citrix Workspace app for Mac at any given time.

Technical Preview

- Support for Citrix Secure Private Access™ for On-premises stores

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

Fixed issues

- In optimized Microsoft Teams, you might hear the ringtone sound randomly if you answer the call before it rings. [HDX-55799]
- The **USB** settings to connect devices automatically, which is available on the **Devices** tab of the **Preferences** window, might not work as expected in Citrix Workspace app 2308 for Mac. [RFMAC-14658]
- On macOS Sonoma devices, when you copy an image (.jpeg/.png format) from your Mac to the virtual session, the copied image in the virtual session might get corrupted. [HDX-55307]

Known issues

- No new issues have been observed in this release.

2308

What's new

Citrix Workspace app for Mac on macOS Sonoma Beta Citrix Workspace app 2308 for Mac has been tested on macOS Sonoma Public Beta 7 Version 23A5337a. Use this setup in a test environment and provide your feedback.

Improved graphics performance Starting with the 2308 version, the performance of graphics is improved for seamless app sessions. This feature also optimizes the load on CPU usage. For more information, see Improved graphics performance.

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

Improved network congestion control Starting with the 2308 version, the Citrix-proprietary transport protocol called Enlightened Data Transport (EDT) is improved to efficiently control network congestion. This feature improves data throughput and reduces latency. For more information, see Improved network congestion control.

Increase in the number of supported virtual channels Previously, Citrix Workspace app for Mac supported up to 32 virtual channels. Starting with the 2308 version, you can use up to 64 virtual channels in a session. For more information, see Increase in the number of supported virtual channels.

App Protection

Support for Policy tampering detection Policy tampering detection feature prevents the user from accessing the virtual app or desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered. If policy tampering is detected, then the virtual app or desktop session is terminated. For more information about the policy tampering detection feature, see Policy tampering detection.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 115.1.1.103, based on Chromium version 115. For more information, see Citrix Enterprise Browser documentation.

Technical Preview

- Support for Activity Manager on cloud stores
- Support for screen sharing when App Protection is enabled
- Support for authentication using FIDO2 when connecting to on-premises store

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

Fixed issues

- When using Citrix Workspace app for Mac to access the virtual desktop, the size of the mouse pointer in the virtual desktop might fluctuate irregularly. [CVADHELP-23158]
- You might not see the icons of active apps in the activity manager. [WSUI-8011]
- Citrix Workspace app might consume a lot of application memories after a few minutes of usage. [CVADHELP-23528]

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

2307

What's new

Native support for Macs with M2 chips Starting with the 2307 version, Citrix Workspace app for macOS supports M2 series (along with M1 series that was previously supported) of Apple silicon natively. For more information, see Native support Apple silicon.

Citrix Workspace app for Mac on macOS Sonoma Beta Citrix Workspace app 2307 for Mac has been tested on macOS Sonoma Public Beta 1 Version 23A5286i. Use this setup in a test environment and provide your feedback.

> **Caution:**
>
> Do not use Citrix Workspace app for Mac on macOS Sonoma Beta versions in production environments.

Deprecating support for macOS version Catalina As announced in the 2304 version, support for macOS version Catalina (10.15) is deprecated in the 2307 release and will be removed for future releases. For more information, see Deprecation.

Support for authentication using FIDO2 when connecting to a cloud store Starting with the 2307 version, users can authenticate using FIDO2 based password-less authentication when connecting to a cloud store. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. This feature currently supports roaming authenticators (USB only) with PIN code and touchID. This feature is supported on macOS 12 and later versions. For more information, see FIDO2-based authentication when connecting to cloud store.

Support for authentication using FIDO2 within an HDX session Starting with the 2307 version, users can authenticate using FIDO2 based password-less authentication within an HDX session. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or websites that support FIDO2 without entering a user name or password. This feature currently supports roaming authenticators (USB only) with PIN code. This feature is supported on macOS 12 and later versions. For more information, see FIDO2-based authentication within an HDX session.

> **Note:**
>
> This release supports only one passkey in a FIDO2 supported device. If your FIDO2 supported device has multiple passkeys then the first passkey is used to authenticate the HDX session.

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

Auto-update version control Administrators can now manage the auto-updated version of Citrix Workspace app for the devices in the organization.
Administrators can control the version by setting the range for `maximumAllowedVersion` and `minimumAllowedVersion` properties in the Global App Configuration service.

Example JSON file in Global App Configuration service:

```
{

  "serviceURL": {

    "url": "https://serviceURL:443"
   }
 ,
  "settings": {

    "name": "Version Control for Citrix Workspace",
    "description": "Provides admin ability to Version Control for
       Citrix Workspace",
    "useForAppConfig": true,
    "appSettings": {

      "macos": [
        {

          "category": "AutoUpdate",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [
            {

              "name": "Auto update plugins settings",
              "value": [
                {

                  "pluginName": "Citrix Workspace",
                  "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
                  "pluginSettings": {

                    "deploymentMode": "Update",
                    "upgradeToLatest": false,
                    "minimumAllowedVersion": "23.07.0.63",
                    "maximumAllowedVersion": "23.07.0.63",
                    "delayGroup": "Medium",
                    "detectRule": ""
                   }

                 }

               ]
             }
```

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

```
46
47                ]
48              }
49
50           ]
51         }
52
53      }
54
55   }
```

When the range is set, Citrix Workspace app on the user device is automatically updated to the highest available version that falls between the mentioned range.

If you want to auto-update Citrix Workspace app to a specific version, enter the same version in the maximumAllowedVersion and minimumAllowedVersion properties in the Global App Configuration service. For more information, see Auto-update version control.

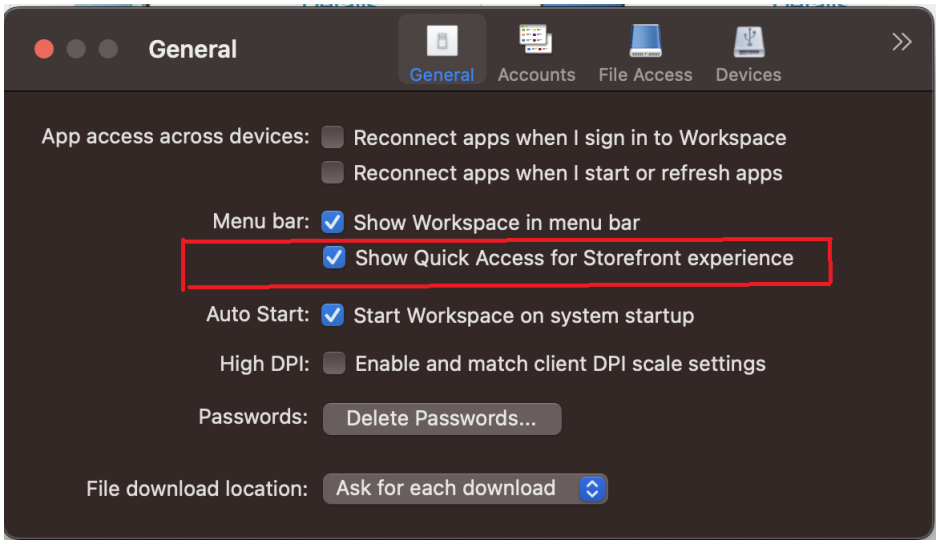
> **Note:**
>
> - To achieve auto-update version control, set the upgradeToLatest setting to false in the Global App Configuration service. If the upgradeToLatest setting is true, maximumAllowed-Version and minimumAllowedVersion is ignored.
> - Do not modify the pluginId. The pluginId is mapped to Citrix Workspace app.
> - If the administrator hasn't configured the version in the Global App Configuration service, Citrix Workspace app is updated to the latest available version by default.
> - You can only use the version ranges that are set to update Citrix Workspace app. However, a downgrade isn't supported.
> - This feature is supported from release 2307 onwards.

Quick access menu for StoreFront Starting with the 2307 version, you can navigate to your favorite apps and desktops quickly and easily using the quick access feature for on-premises stores. To enable quick access, right-click **Citrix Workspace** in the toolbar, navigate to **Preferences > General**, and then select **Show Quick Access for Storefront experience**. This feature allows you to see your favorite data directly from the Mac menu bar.



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

You can enable the quick access feature by using **Preferences**.



Administrators can enable or disable the quick access feature by using the Mobile Device Management (MDM) or Global App Configuration service (GACS) methods. For more information, see the Quick access menu for StoreFront.

Enabling or disabling quick access using MDM To enable quick access through MDM, administrators must use the following settings:

```
<key>ShowQuickAccessForStoreFront</key>
<false/>
```

Enabling or disabling quick access using GACS To enable quick access through GACS, administrators must use the following settings:

```
enableQuickAccessForStoreFront
```

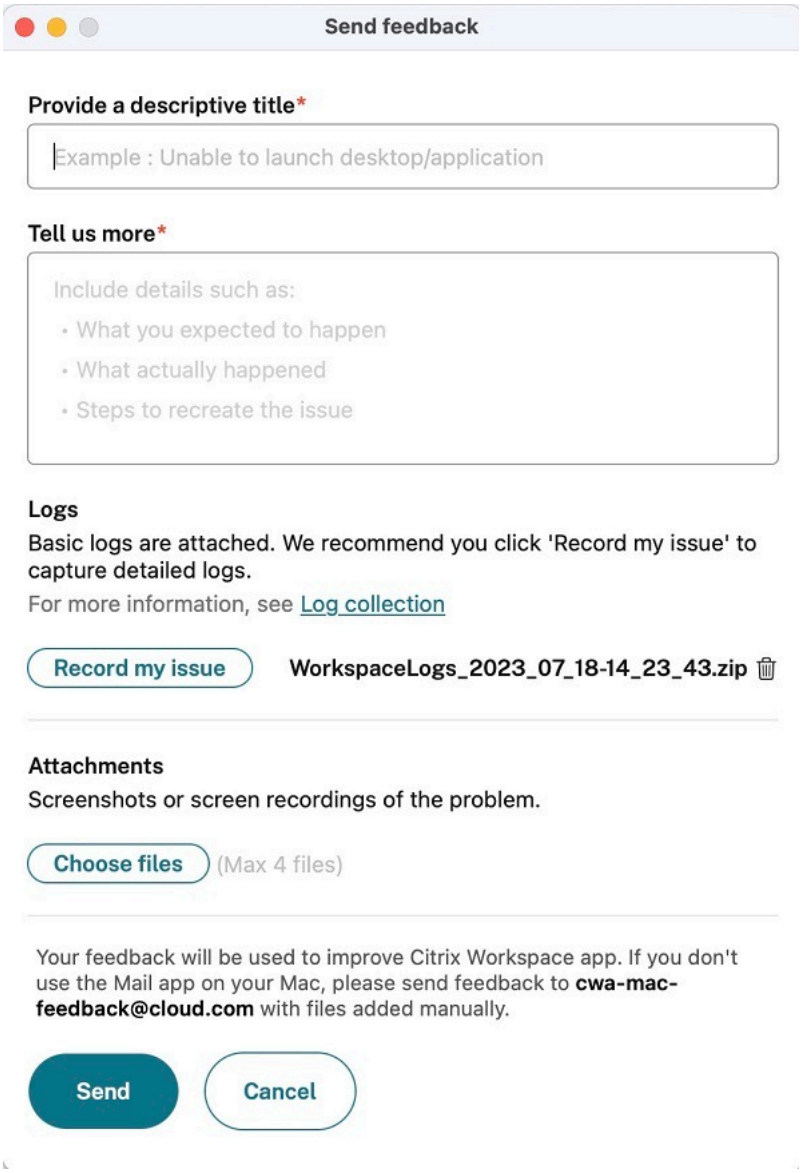
Store-based configuration of microphone and webcam access Starting with the 2307 version, the per-store microphone and webcam access are included as part of the client-selective trust feature. This enhancement allows you to provide access to a microphone and webcam on a per-store basis.

To enable microphone and webcam access for a store, you must select **Preferences > Mic & Webcam**. In the **Mic & Webcam** tab, select the store and the type of access required for that store. For more information, see Store-based configuration of microphone and webcam access.

Send feedback on Citrix Workspace app The Send feedback option allows you to inform Citrix about any issues you might encounter while using the Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

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

You must select **Help > Send feedback** to view and fill the issue details in the Send feedback form. You can add details like the examples provided in the form.



You can attach the existing log files or generate new log files. To generate log files, click **Record my issue > Start Recording** and then reproduce the issue. After the issue is reproduced, click **Stop Recording**. The log file is saved automatically and replaces the existing logs with the reproduced logs.

> **Note:**
>
> Citrix does not collect any Personally Identifiable Information (PII) from the logs.

You can attach screenshots or screen recordings describing the issue to help us understand what you're experiencing. Click **Choose files** and add the attachments such as screenshots or screen recordings. You can attach a maximum of four files.

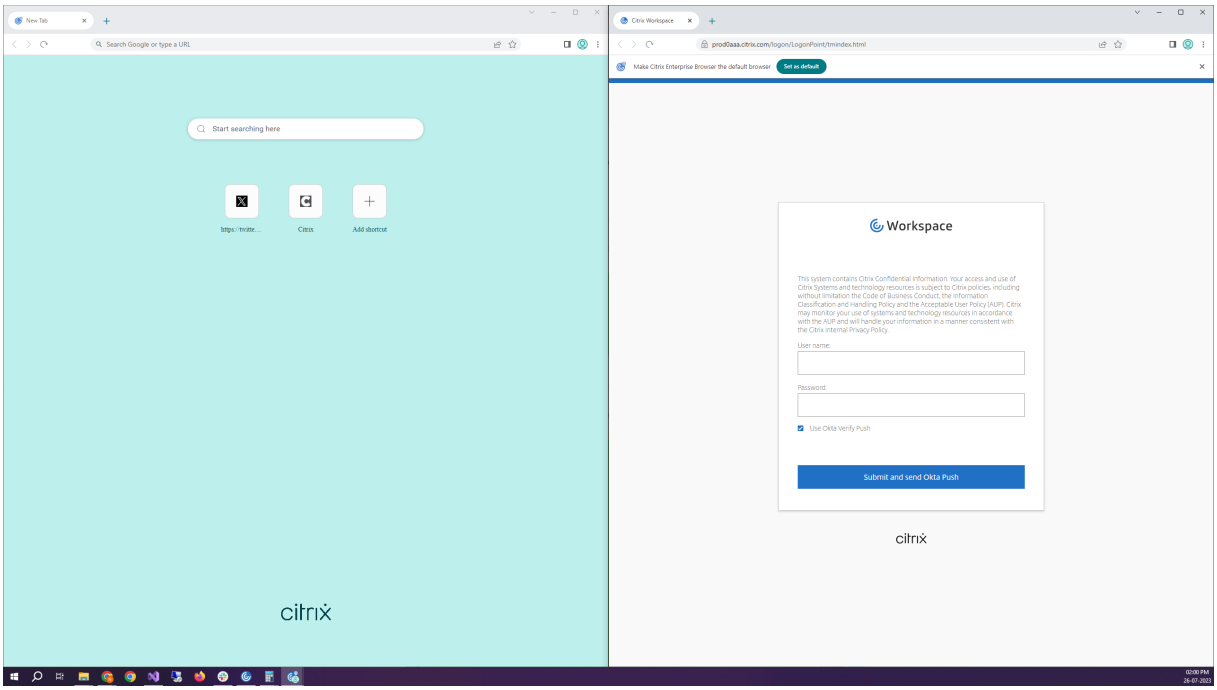
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once you've entered the necessary information, click **Send** to have a new email automatically created in your Mail app with the information you added. From there, click the **Send button** to share the feedback with Citrix. For more information, see Send feedback on Citrix Workspace app.

> **Note**
>
> If you aren't using the default Mail app, then send feedback to cwa-mac-feedback@cloud.com from your mail client. Add the issue details, log files, screenshots, or screen recordings to the email manually.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 113.1.1.34, based on Chromium version 113. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Split view support Citrix Enterprise Browser on macOS supports split view for ease of multitasking. With split view, you can use Citrix Enterprise Browser and another window next to each other, without having to manually move and resize windows. For more information, see Apple's support article.



Citrix Enterprise Browser shortcut Starting with Citrix Workspace app for Mac 2307 version, an administrator can configure and control the presence of the Citrix Enterprise Browser shortcut on the launch pad.

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

> **Note:**
>
> By default, this feature isn't configured.

Configuration

An IT administrator can configure the presence of the Citrix Enterprise Browser shortcut in one of the following ways:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)
- web.config file.

> **Note:**
>
> - All the configuration methods have equal priority. Enabling any one of them enables the shortcut.
> - If you haven't configured the shortcut but have one or more Workspace stores, the shortcut gets automatically enabled.
> - For end users, the Citrix Enterprise Browser shortcut appears if the user makes it as a favorite app irrespective of the configuration.
> - To disable this feature for Workspace stores, administrators must apply one of the following settings:
>
> - Set the **CEBShortcutEnabled** attribute to false in the MDM or web.config file.
> - Disable the Enable Citrix Enterprise Browser shortcut property in GACS.

Mobile Device Management (MDM)

Administrators can push the settings **CEBShortcutEnabled** set as **true** to the user's device.

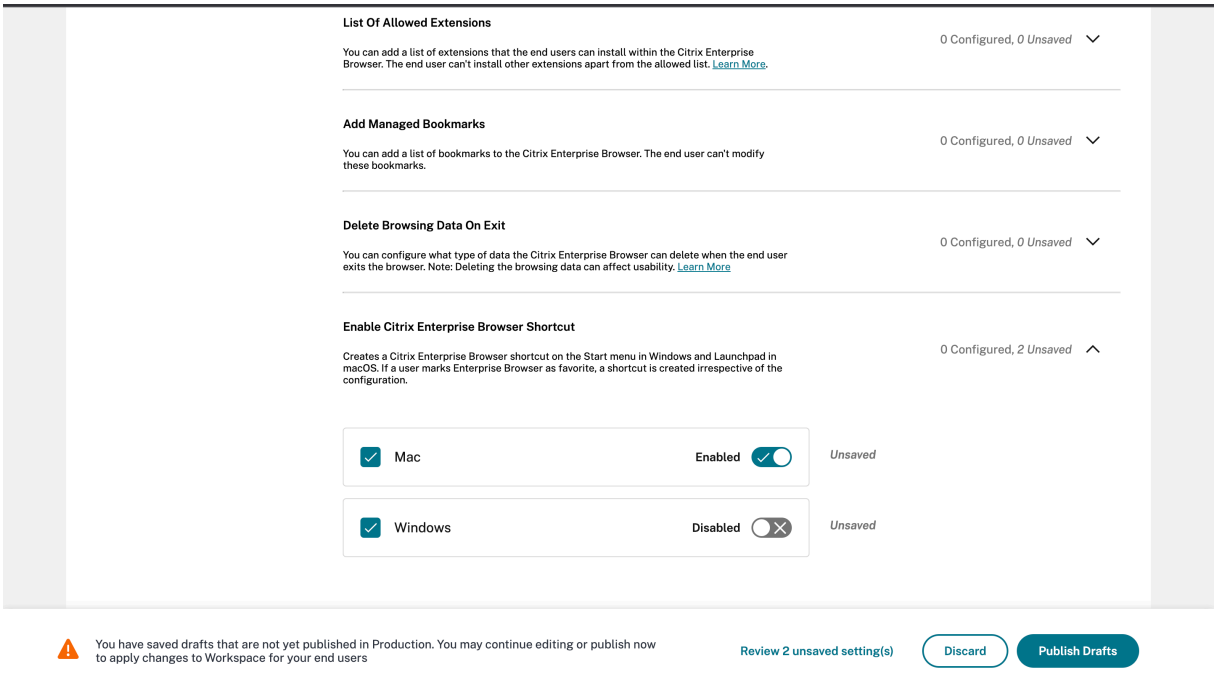
For more information on how to use MDM, see Mobile Device Management (MDM).

> **Note:**
>
> This way of configuration is applicable on Workspace and StoreFront.

Global App Configuration service (GACS)

Navigate to **Workspace Configuration > App Configuration > Citrix Enterprise Browser** and enable **Enable Citrix Enterprise Browser shortcut** property.

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



For more information about how to use the GACS UI, see the User interface article in the Citrix Enterprise Browser documentation.

> **Note:**
>
> This way of configuration is applicable on Workspace and StoreFront.

web.config file

Enable the attribute **CEBShortcutEnabled** under the properties.

```
<properties>
    <property name="CEBShortcutEnabled" value="
       True" />
</properties>
```

> **Note:**
>
> This way of configuration is applicable on StoreFront.

Using web.config

To enable the Citrix Enterprise Browser shortcut, do the following:

1. Use a text editor to open the web.config file, which is typically at `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Locate the user account element in the file (Store is the account name of your deployment).

   For example: `<account id=... name="Store">`

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

3. Before the </account> tag, navigate to the properties of that user account and add the following:

```
                    <properties>
                        <property name="CEBShortcutEnabled" value=
                            "True" />
                    </properties>
```

The following is an example of the web.config file:

```
<account>
    <clear />
    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
      description="" published="true" updaterType="Citrix"
          remoteAccessType="None">
      <annotatedServices>
        <clear />
        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
          <metadata>
            <plugins>
              <clear />
            </plugins>
            <trustSettings>
              <clear />
            </trustSettings>
            <properties>
                  <property name="CEBShortcutEnabled" value="True" />
            </properties>
          </metadata>
        </annotatedServiceRecord>
      </annotatedServices>
      <metadata>
        <plugins>
          <clear />
        </plugins>
        <trustSettings>
          <clear />
        </trustSettings>
        <properties>
          <clear />
        </properties>
      </metadata>
    </account>
```

How to configure using web.config

1. Use a text editor to open the web.config file, which is typically at C:\inetpub\wwwroot\Citrix\Roaming directory.
2. Locate the user account element in the file (Store is the account name of your deployment).

   For example: `<account id=... name="Store">`
3. Before the </account> tag, navigate to the properties of that user account and add the following:

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

```
<properties>
    <property name="CEBShortcutEnabled" value=
        "True" />
</properties>
```

Technical Preview

- Keyboard accessibility support for the toolbar on the Virtual Desktop

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

Fixed issues

- While launching the published app through the browser, the app does not launch directly but downloads an ICA file. The user might have to open the downloaded ICA file manually to launch the app. [CVADHELP-20835]
- Attempts to start a session might fail if the StoreFront keyword is set to "KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"". [CVADHELP-23170]
- You might not be able to select the required gateway from the list of options provided when using Citrix Workspace app for Mac. [CVADHELP-22777]

Known issues

No new issues have been observed in this release.

2306

What's new

Log traceability and user activity Starting with the 2306 version, when a user reports an issue, the administrators can go through the log files to view the basic information such as macOS version, Citrix Workspace app version, details about the previous upgrade, number of stores added, and other details. Administrators can now view the following activities in Citrix Workspace app for Mac:

- The app launched along with the macOS version, number of stores, and other metadata.
- The store addition and deletion operation and the metadata that is required to add an account.
- The session start time and launch status.
- Auto update activation and status.
- System events such as moving the app to the background, sleep mode, or quitting.

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

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 112.1.1.23, based on Chromium version 112. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Fixed issues

- After upgrading Citrix Workspace app for Mac to version 2305, certain third-party virtual apps that have pop-up dialogs for entering username and password might become unresponsive upon opening. [CVADHELP-23032]

Known issues

No new issues have been observed in this release.

2305

What's new

Support for horizontal scroll Previously, Citrix Workspace app for Mac supported only vertical scroll on a trackpad. Starting with the 2305 version, a horizontal scroll is also supported. For more information, see Support for horizontal scroll.

Improved audio echo cancellation support Citrix Workspace app now supports echo cancellation in adaptive audio and legacy audio codecs. This feature is designed for real-time audio use cases, and it improves the user experience. Citrix recommends using adaptive audio. For more information, see Improved audio echo cancellation support.

Improved graphics performance [Technical Preview] Starting with the 2305 version, the performance of graphics is improved for seamless sessions. This feature also reduces the load on CPU usage.

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

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

Support for Certificate-based authentication Starting with the 2305 version, Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to Citrix Workspace app.

The following methods can be used to enable the authentication using conditional access:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

The flag values read by Citrix Workspace app take precedence in the following order:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

For more information, see Support for Certificate-based authentication.

Channel support for Global App Configuration service 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. Global App Configuration service now allows administrators to test the settings before rolling it out to all users. This feature allows to resolve any issues before applying the global app configurations to the entire user base. For more information, see Channel support for Global App Configuration service.

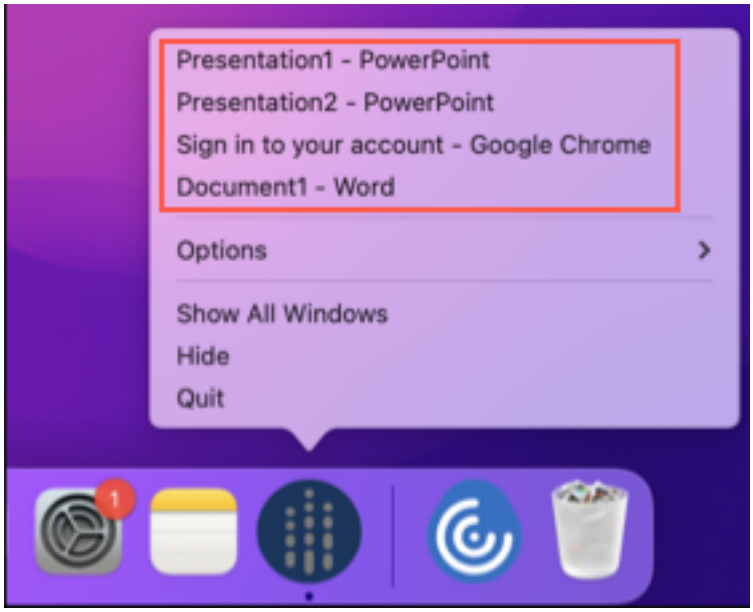
Improved auto-update experience The auto-update feature automatically updates the Citrix Workspace app to the latest version without the need for any user intervention.

Citrix Workspace app periodically checks and downloads the latest available version of the app. Citrix Workspace app determines the best time to install based on user activity not to cause any disruptions.

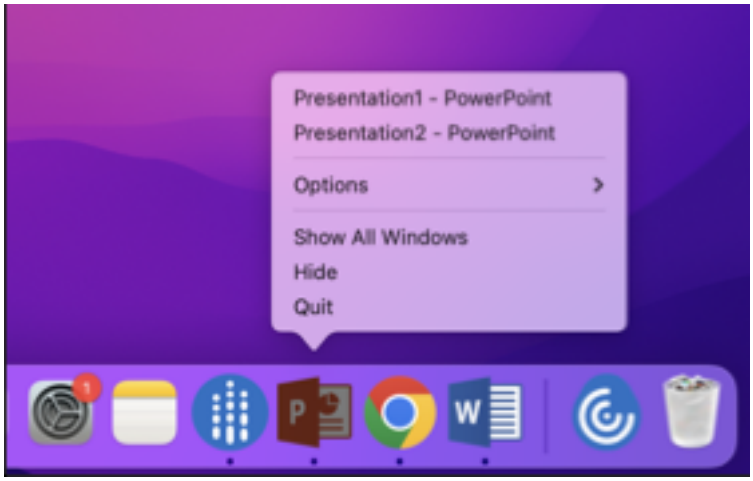
For more information, see Improved auto-update experience.

Opened apps appear in the dock with native app icons Previously, clicking virtual apps in the Citrix Workspace app triggered the **Citrix Viewer** where these apps would be available. If you open many apps, the apps or its instances are opened in the **Citrix Viewer**. You can view the open apps by right-clicking the **Citrix Viewer** icon.

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



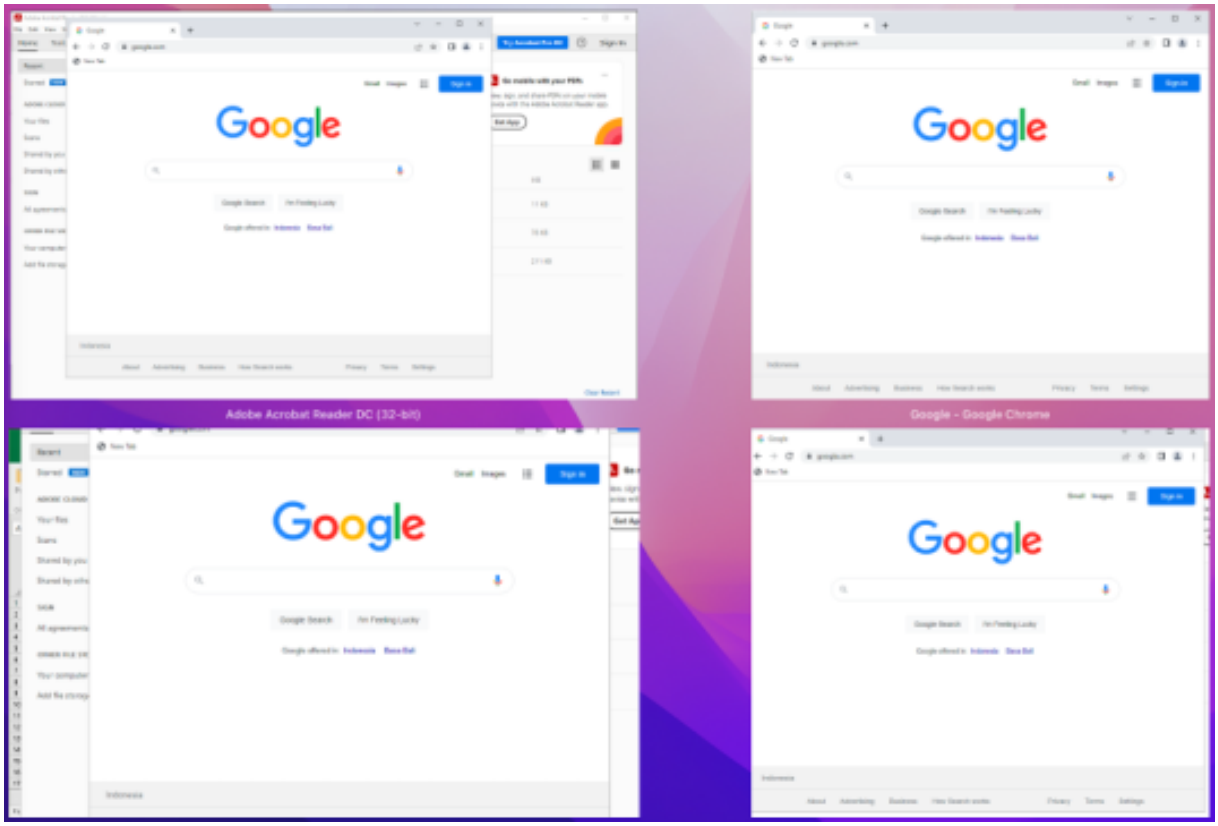
Starting with the 2305 version, when you open virtual apps, they appear in the Dock (bottom-right corner of the screen) with their respective icons and are easily identifiable. You can then access the virtual app from the dock itself. If you open multiple instances of an app, these instances aren't duplicates in the Dock but are grouped within one instance in the Dock.



For more information, see the Opened apps appear in the dock with native app icons page.

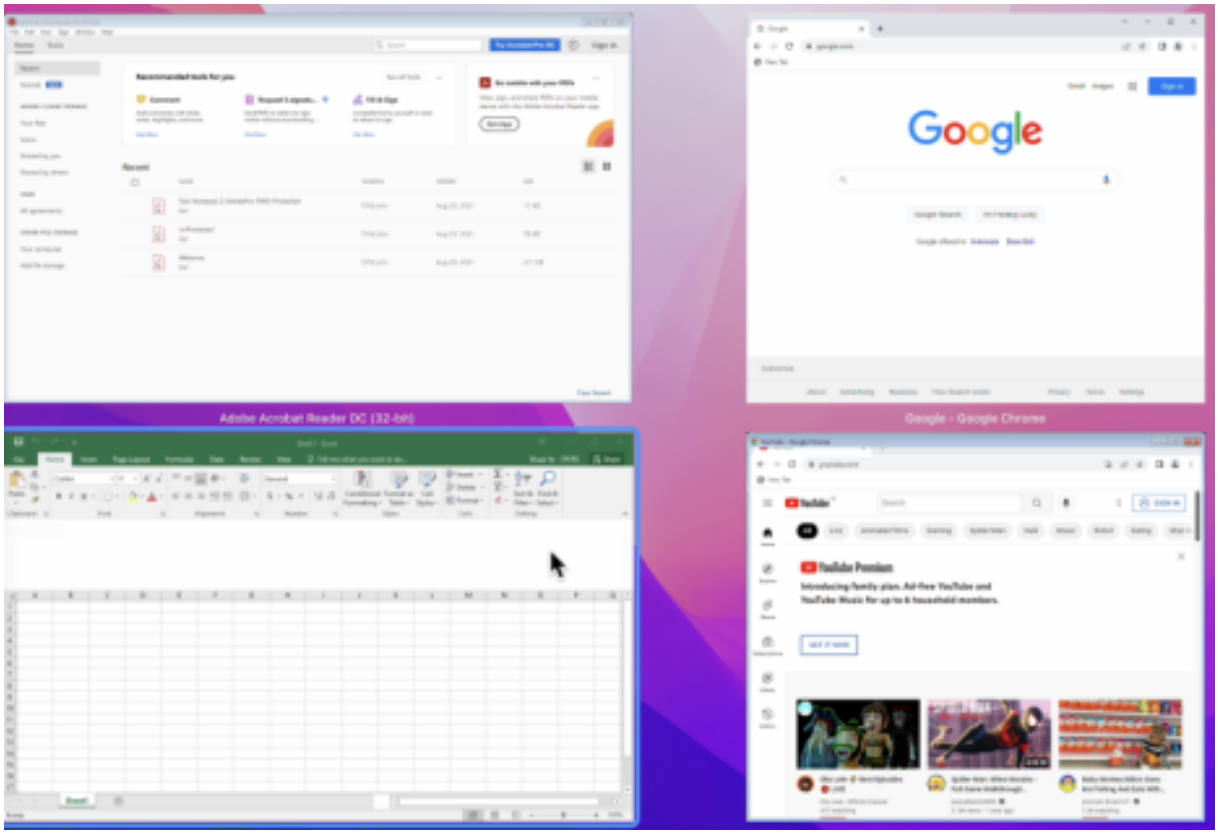
Improved Mission Control and App Expose experience Previously, using the **Mission Control** or **App Expose** feature in a virtual app session resulted in the overlapping of many windows that were opened.

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



Starting with the 2305 version, when you use the **Mission Control** or **App Expose** feature in a virtual app session and open many windows, the windows do not overlap, and you can easily choose from among them.

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



For more information, see Improved Mission Control and App Expose experience.

Enhancement to sleep mode for optimized Microsoft Teams call Previously, when using the optimized Microsoft Teams meeting, if there's no mouse or keyboard interaction, Citrix Workspace app or the optimized Microsoft Teams screen might go to sleep mode.

Starting with the 2305 version, Citrix Workspace app or the optimized Microsoft Teams screen doesn't go to sleep mode even if there's no mouse or keyboard interaction during an optimized Microsoft Teams meeting.

For more information, see Enhancement to sleep mode for optimized Microsoft Teams call.

Support for continuity camera With the Continuity Camera, you can now use the iPhone as your webcam. For a seamless connection, mount your iPhone such that its camera is available to the Mac device. You must select **Webcam > Automatic Camera Selection** for the iPhone to appear automatically on the Mac device as an external camera. You can switch to any other camera manually, for example by selecting **Webcam > FaceTime HD Camera**. The Continuity Camera works wired or wirelessly and provides a high-quality image. For more information, see Support for continuity camera.

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

Increase in the number of supported virtual channels [Technical Preview] In earlier versions of the client, sessions supported up to 32 virtual channels. Starting with the 2305 version, you can use up to 64 virtual channels in a session.

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

Store-based configuration of microphone and webcam access levels [Technical Preview] Starting with the 2305 version, the per-store microphone and webcam access are included as a part of the client-selective trust feature. This enhancement allows you to change the settings based on a per-store basis. You can click a store to enable the required microphone or camera access. The selected setting for microphone or camera access is applied on a per-store basis.

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

Support for authentication using FIDO2 when connecting to cloud stores [Technical Preview] Starting with the 2305 version, users can authenticate using passwordless FIDO2 security keys when connecting to Citrix Workspace app for Mac. Users can sign into the cloud stores using the FIDO2 security keys. The security keys support different types of security inputs such as security pins, biometrics, card swipe, smart card, Public Key Certificates. This feature is supported on macOS 12 and later versions. For more information about FIDO2 see FIDO2 Authentication.

Citrix Workspace app uses the user's default browser for FIDO2 authentication (Webauthn). Administrators can configure the type of browser to authenticate to Citrix Workspace app. The configured setting can be pushed using the Mobile Device Management (MDM), Global App Configuration service (GACS), or the command line interface methods. The FIDO2 feature is not supported for on-premises stores. For more information on the web browser settings, see Global App Configuration service documentation.

The following settings allow you to select the type of browser used for authenticating an end user into Citrix Workspace app:

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

Embedded: Allows you to authenticate within Citrix Workspace app. Citrix Workspace app saves the session data or cookies for single sign-on (for example, SaaS apps) when the enhanced single sign-on feature is enabled. This authentication method does not support passwordless authentications such as FIDO2.

EmbeddedWithPrivateSession: This setting is similar to the **Embedded** setting. Single sign-on isn't supported as session data or cookies aren't present in Citrix Workspace app.

System: Allows you to use the user's default browser for authentication (for example, Safari or Chrome). Authentication occurs outside Citrix Workspace app. Use this setting to support passwordless authentication. This setting tries to use the existing user session from the user's browser.

SystemWithPrivateSession: This setting is like the **System** setting. Citrix Workspace app uses a private session in the browser for authentication. The browser doesn't save authentication cookies or data. Single sign-on isn't supported in this option.

Enabling authentication using MDM To enable authentication through MDM, administrators must use the following settings:

```
<key>WebBrowserForAuthentication</key>
<string>System</string>
```

Enabling authentication using GACS To enable authentication through GACS, administrators must use the following settings:

```
{

    "serviceURL": {

      "url": "https://serviceURL:443"
     }
 ,
    "settings": {

      "name": "Productivity Apps",
      "description": "Provides access to MS Office and other basic apps
          ",
      "useForAppConfig": true,
      "appSettings": {

        "macos": [
          {

            "assignedTo": [
              "AllUsersNoAuthentication"
            ],
```

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

```
            "category": "authentication",
            "settings": [
              {

                "name": "web browser for authentication",
                "value": "SystemWithPrivateSession"
               }

            ],
            "userOverride": false
           }

        ]
       }

    }

  }
```

Enabling authentication using the command-line interface To enable authentication using the command-line interface, administrators must run the following command:

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication
System
```

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

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

Keyboard input mode enhancements Citrix Workspace app for Mac provides UI to configure the keyboard input mode.

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

1. From the Citrix Workspace app icon in the menu bar, click the account icon in the top-right corner and navigate to **Preferences > Keyboard**.

   The Keyboard input mode settings appear

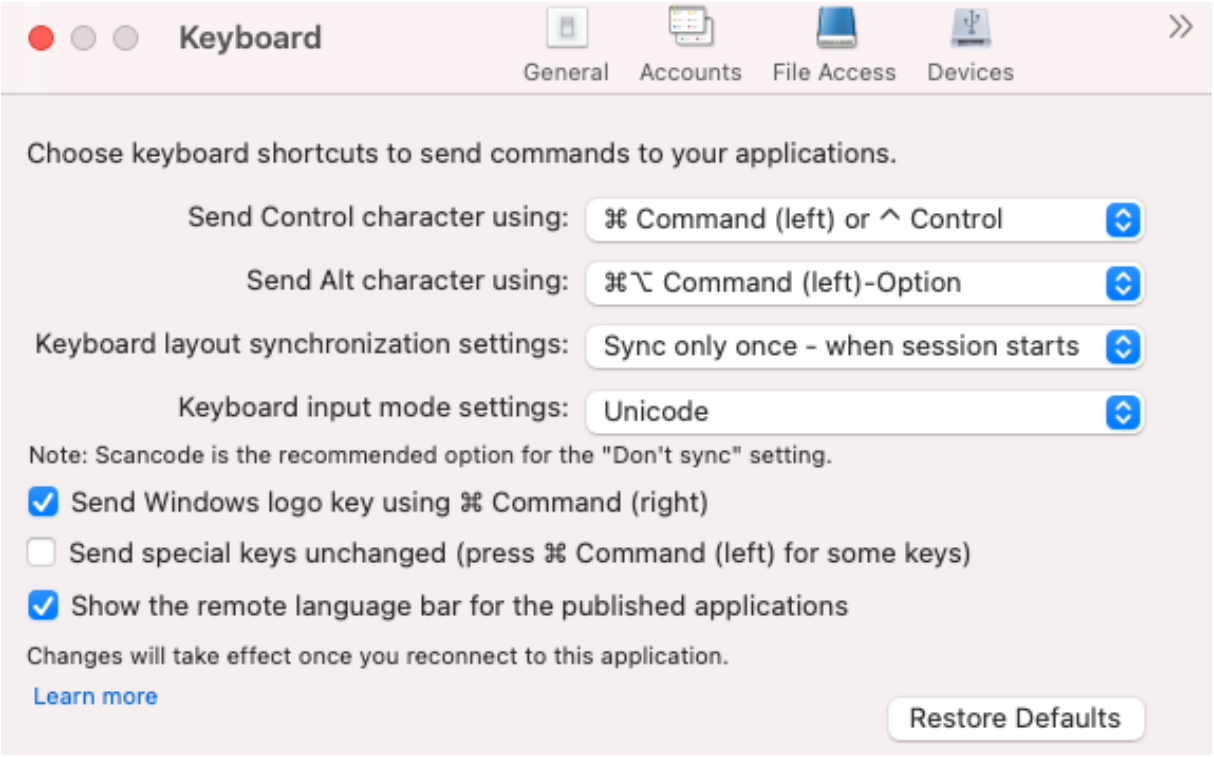
2. Select from one of the following options:

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

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

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

This enhancement is enabled by default.



For example, consider a scenario where you're using a US international keyboard layout and the VDA is using the Russian keyboard layout. When you choose **Scancode** and type the key next to **Caps Lock**, the scancode "1E"is sent to the VDA. The VDA then uses "1E"to display the character "ф". If you choose **Unicode** and type the key next to **Caps Lock**, the character "a"is sent to the VDA. So, even if the VDA uses the Russian keyboard layout, the character "a"appears on the screen.

Citrix recommends the following keyboard input mode for the different keyboard layout sync options:

- Scancode mode for **Don't Sync** option.
- Unicode mode for **Allow dynamic sync** and **Sync only once - when session starts**

> **Note:**
>
> The keyboard configuration changes take effect once you reconnect to the application.

You can change the configuration of Keyboard input mode in the Citrix Workspace app UI. However, for best performance, use the Citrix-recommended modes for different scenarios, physical keyboards, and client devices.

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

For more information on configuration details and limitations, see Keyboard input mode enhancements.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 112.1.1.23, based on Chromium version 112. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Modification in SPA policy implementation on internal Web and SaaS apps This feature enhances the security policies implementation on Web and SaaS apps. When a webpage and iframes within the webpage have different policies, we now have a stricter policy implementation where a union of all policies is applied on the entire webpage, including the iframes. However, the watermark is applied to the webpage only.

Support for browser extensions You can add extensions that are provided by your administrator to the Citrix Enterprise Browser in a secure way. An administrator can deploy, manage, and control the extensions. End users can view and use the extension under citrixbrowser://extensions as required. For more settings, see Global App Configuration service.

For information on how to configure, see the Support for browser extensions documentation.

Use GACS to manage Citrix Enterprise Browser The administrator can use the Global App Configuration service (GACS) for Citrix Workspace to deliver Citrix Enterprise Browser settings through a centrally managed service.

The GACS is designed for administrators to easily configure Citrix Workspace and manage the Citrix Workspace app settings. This feature allows admins to use GACS to apply various settings or system policies to the Citrix Enterprise Browser on a particular store. The administrator can now configure and manage the following Citrix Enterprise Browser settings using APIs or the GACS Admin UI:

- "Enable CEB for all apps"- Makes the Citrix Enterprise Browser the default browser for opening web and SaaS apps from the Citrix Workspace app.
- "Enable save passwords"- Allow or deny end users the ability to save passwords.
- "Enable incognito mode"- Enable or disable incognito mode.
- "Managed Bookmarks"- Allow the administrator to push bookmarks to the Citrix Enterprise Browser.
- "Enable developer tools"- Enable or disable developer tools within the Enterprise Browser.
- "Delete browsing data on exit"- Allow the administrator to configure what data the Citrix Enterprise Browser deletes on exit.
- "Extension Install Force list"- Allow the administrator to install extensions in the Citrix Enterprise Browser.

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

- “Extension Install Allow list”- Allow the administrator to configure an allowed list of extensions that users can add to the Citrix Enterprise Browser. This list uses the Chrome Web Store.

For more information, see Use Global App Configuration service to manage Citrix Enterprise Browser.

> **Notes:**
>
> - The name and value pair are case-sensitive.
> - All the browser settings in Global App Configuration service are under the following category:

```
{

    "category": "browser",
    "userOverride": false,
    "assignedTo": [
    "AllUsersNoAuthentication"
    ]
 }
```

> - The administrator can apply the settings to unmanaged devices as well. For more information, see Global App Configuration service documentation.

User interface

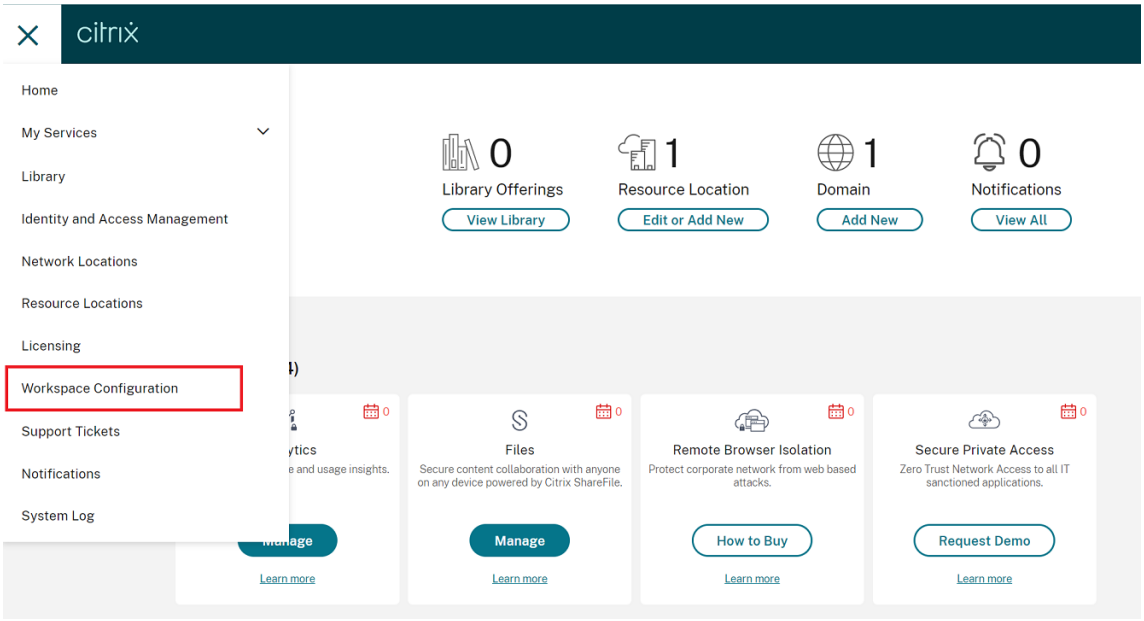
To configure Citrix Enterprise Browser through the GACS Admin UI, do the following:

1. Sign in to citrix.cloud.com with your credentials.

   > **Note:**
   >
   > - Refer to the Sign Up for Citrix Cloud article for step-by-step instructions to create a Citrix Cloud account.

2. Upon authentication, click the menu button in the top left corner and select **Workspace Configuration**.

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



The **Workspace Configuration** screen appears.

3. Click **App Configuration** > **Citrix Enterprise Browser**.

   You can now configure, modify, and publish Citrix Enterprise Browser feature settings.

For more information, see Use Global App Configuration service to manage Citrix Enterprise Browser.

Technical Preview

- Client APP Management

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

Fixed issues

- With this enhancement, the location data can be collected and sent to Microsoft Teams to support the dynamic emergency calling feature. [CVADHELP-21117]
- When you scroll in a MacBook using a touchpad in a user session that is opened through Citrix Workspace app for Mac, the scroll experience might not be smooth. [CVADHELP-21427]
- When using Citrix Workspace app for Mac, external users might get disconnected from the sessions intermittently. [CVADHELP-22191]
- Attempts to add a store URL that contains a query parameter might fail in Citrix Workspace app for Mac with this error message:

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

This store doesn't exist. Please retry or contact support.

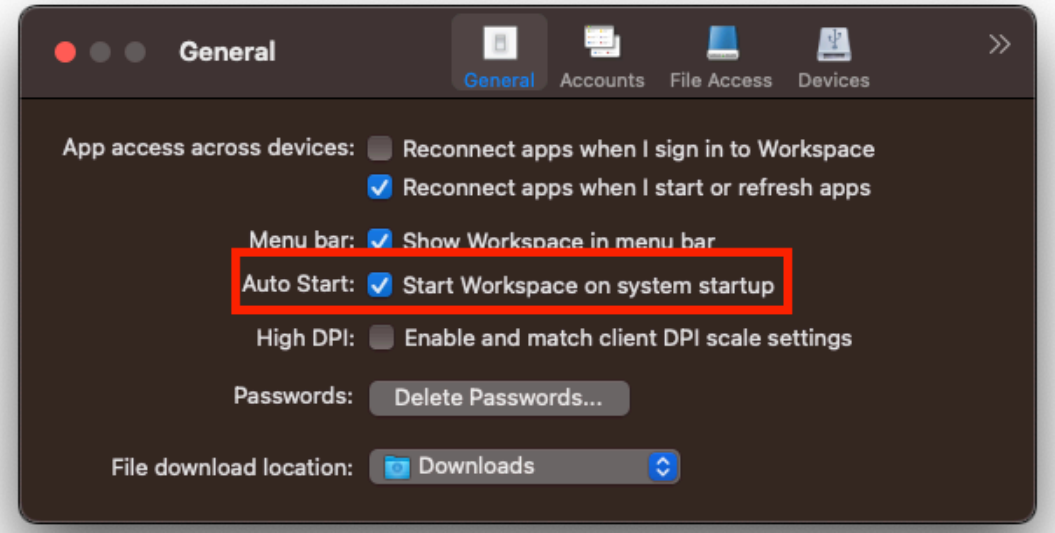
[CVADHELP-22445]

- On an on-premises store, when you attempt to open Citrix Workspace app from the **Menu** bar, you might experience an indefinite wait time. [CVADHELP-22688]

2304

What's new

Enhanced auto start experience Previously, Citrix Workspace app for Mac used to start automatically whenever a computer was turned on. Starting with the 2304 version, you can choose to disable or enable the auto start feature on Citrix Workspace app for Mac by navigating to **Preferences > General > Start Workspace** on system startup. The auto start setting is enabled by default.



For more information, see Enhanced auto start experience.

Improved experience for optimized Microsoft Teams video conference calls Starting with the 2304 version, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved. It is achieved by adapting to the proper resolution for the best call experience for all callers.

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

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

> **Note:**
>
> This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, go to https://www.microsoft.com/ and search for the Microsoft 365 roadmap. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

For more information see,
Improved experience for optimized Microsoft Teams video conference calls.

Support for Certificate-based authentication [Technical Preview] Starting with the 2304 version, Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to Citrix Workspace app.

The following methods can be used to enable the authentication using conditional access:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

The flag values read by Citrix Workspace app take precedence in the following order:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

For more information, see Support for Certificate-based authentication.

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

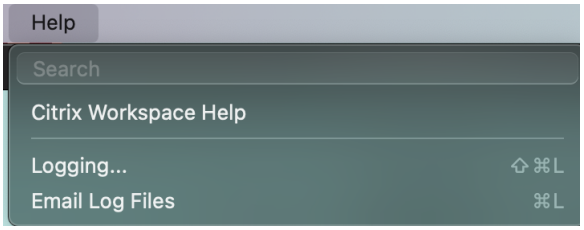
Force login prompt for Federated identity provider Citrix Workspace app now honors the Federated Identity Provider Sessions setting. For more information, see Citrix Knowledge Center article CTX253779.

You no longer need to use the Store authentication tokens policy to force the login prompt. For more information, see Force login prompt for Federated identity provider.

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

Support for non-English-language Input Method Editors (IME) keyboard layouts Support for non-English language IME keyboard layouts continues to work uninterrupted after the Carbon APIs are deprecated with the Cocoa APIs. For more information, see Support for non-English-language Input Method Editors (IME) keyboard layouts.

Log collection Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, facilitate support. Users can now collect logs quickly by using the new option provided in the **Help** menu by navigating to **Help** and selecting the **Logging...** or **Email Log Files** option. This feature improves the user experience during the log collection process.



- **Logging...** - clicking this option directs you to **Preferences > Advanced > Logging**
- **Email Log Files** –clicking this option allows collecting the latest logs.

For more information, see Log collection.

Support synchronization for more keyboard layouts Starting with the 2304 version, Citrix Workspace app for Mac supports keyboard layout synchronization for the following layouts or Input Method Editors (IMEs):

- English ABC
- English ABC - India
- Chinese, Traditional: Zhuyin - Traditional
- Chinese, Traditional: Sucheng - Traditional
- Google Japanese IME
- Sougou Chinese IME

For more information, see Support synchronization for more keyboard layouts.

Microsoft Teams enhancement

Configuring a preferred network interface You can now configure a preferred network interface for media traffic. Run the following command in a terminal:

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

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Select one of the following values as required:

- 1: Ethernet
- 2: Wi-Fi
- 3: Cellular
- 4: VPN
- 5: Loopback
- 6: Any

By default and if no value is set, the WebRTC media engine chooses the best available route.

For more information, see Configuring a preferred network interface.

Limiting video resolutions Administrators with users on lower-performance client endpoints can limit incoming or outgoing video resolutions to reduce the impact of video encoding and decoding on those endpoints. Starting from Citrix Workspace app 2304 for Mac, you can limit these resolutions using client configuration options.

For more information, see Limiting video resolutions.

Support for horizontal scroll [Technical Preview] Previously, Citrix Workspace app for Mac supported only vertical scroll on a trackpad. Starting with the 2304 version, a horizontal scroll is also supported.

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

Keyboard input mode enhancements Citrix Workspace app for Mac provides UI to configure the keyboard input mode.

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

1. From the Citrix Workspace app icon in the menu bar, click the account icon in the top-right corner and navigate to **Preferences > Keyboard**.

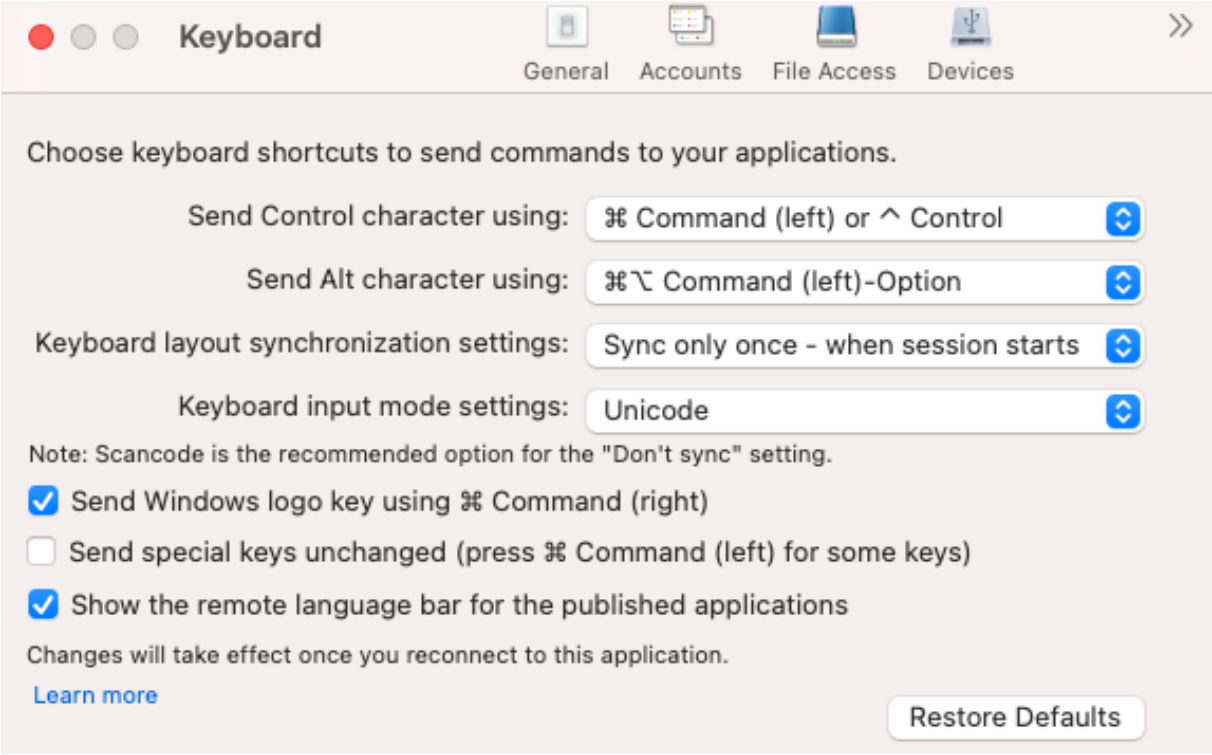
   The Keyboard input mode settings appear

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

2. Select from one of the following options:

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

This enhancement is enabled by default.



For example, consider a scenario where you're using a US international keyboard layout and the VDA is using the Russian keyboard layout. When you choose **Scancode** and type the key next to **Caps Lock**, the scancode "1E"is sent to the VDA. The VDA then uses "1E"to display the character "ф". If you choose **Unicode** and type the key next to **Caps Lock**, the character "a"is sent to the VDA. So, even if the VDA uses the Russian keyboard layout, the character "a"appears on the screen.

Citrix recommends the following keyboard input mode for the different keyboard layout sync options:

- Scancode mode for **Don't Sync** option.
- Unicode mode for **Allow dynamic sync** and **Sync only once - when session starts**

> **Note:**
>
> The keyboard configuration changes take effect once you reconnect to the application.

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

You can change the configuration of Keyboard input mode in the Citrix Workspace app UI. However, for best performance, use the Citrix-recommended modes for different scenarios, physical keyboards, and client devices.

For more information on configuration details and limitations, see Keyboard input mode enhancements.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 109.1.1.31, based on Chromium version 109. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Technical Preview

- Rapid Scan
- Enhanced virtual apps and desktops launch experience
- Support for multiple audio devices

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

Fixed issues

- When you create two XML files on a Mac local client, the VDA might open the incorrect XML file. For example, the VDA opens the Snapshot.xml file instead of opening the SnapshotPopup.xml file. [HDX-45326]
- When you change the active audio devices in the sound settings on the endpoint, Microsoft Teams might not receive any notification about the change. As a result, Microsoft Teams fails to pick the changes. [HDX-47080]
- The Citrix Viewer might quit occasionally when you close a VDA session. [HDX-45668, HDX-47138]
- The responder policy configured using Citrix ADC might fail to work with Citrix Workspace app for Mac. The issue occurs when the policy configured checks if the user agent has sent **CWAWEBVIEW**, **Citrix Receiver**, or **Citrix Workspace** as a substring, which does not match. As a result, users might be redirected to a different Citrix Gateway URL. [CVADHELP-20519]
- When you connect to Citrix Gateway Store and attempt to sign in to Citrix Workspace app for Mac, the sign-in might get stuck or take time with a spinning wheel. [CVADHELP-21323]
- Citrix Workspace app for Mac might fail to start a session if the **File Type Association** is set for an app under **Application Settings** in Citrix Studio. [CVADHELP-21371]

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

- A sign-in window might appear automatically in Citrix Workspace app for Mac when you power on or restart your system. [CVADHELP-21484]
- Citrix Workspace app for Mac might quit unexpectedly when the Universal Windows Platform (UWP) apps within the VDI attempt to authenticate using the FIDO2 authentication. [CVADHELP-21576]
- Attempts to open the web resources might fail with this error message:

  Switch to another store with the necessary permissions. If the issue persists, contact your admin with error details.

  [CVADHELP-21787]
- Citrix Workspace app for Mac might use an incorrect user agent **CitrixReceiver** instead of **Citrix Workspace** as a substring. As a result, the authorization policies aren't honored. [CVADHELP-21969]
- When using the notch screen feature, a part of the text might be cut. [CVADHELP-22134]
- When you open Citrix Enterprise Browser from the dock, instead of a new tab, it shows that the page is loading. As a workaround, enter the URL in the address bar or open another tab to continue browsing. [CTXBR-4706]
- When using the Citrix Secure Private Access enabled store, an infinite loading spinner might appear while launching the published content. The issue occurs when Citrix Enterprise Browser isn't running on the user device. As a result, you can't view the published content. [CTXBR-4813]

2301.1

What's new

This 2301.1 release addresses a few issues that help to improve overall performance and stability.

Fixed issues

- You might face issues when you add or authenticate a store, or start a resource (apps or desktops) using the native Citrix Workspace app. [CVADHELP-22372]
- The incoming video and screen sharing might not work during Microsoft Teams optimized video calls. [HDX-50059]

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

Known issues in 2301.1

- You can't update to Citrix Workspace app for Mac version 2301.1 using the auto-update service. As a workaround, you must manually install the Citrix Workspace app for Mac version 2301.1 by downloading the .dmg file available on the Downloads page.

2301

What's new

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

Auto-update version control [Technical Preview] Administrators can now manage the auto-updated version of Citrix Workspace app for the devices in the organization.
Administrators can control the version by setting the range in the maximumAllowedVersion and minimumAllowedVersion properties in the Global App Configuration service.

Example JSON file in Global App Configuration service:

```
{

  "serviceURL": {

    "url": "https://serviceURL:443"
   }
 ,
  "settings": {

    "name": "Version Control for Citrix Workspace",
    "description": "Provides admin ability to Version Control for
       Citrix Workspace",
    "useForAppConfig": true,
    "appSettings": {

      "macos": [
        {

          "category": "AutoUpdate",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [
            {
```

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

```
25
26                "name": "Auto update plugins settings",
27                "value": [
28                  {
29
30                    "pluginName": "Citrix Workspace",
31                    "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
32                    "pluginSettings": {
33
34                      "deploymentMode": "Update",
35                      "upgradeToLatest": false,
36                      "minimumAllowedVersion": "23.04.0.36",
37                      "maximumAllowedVersion": "23.04.0.36",
38                      "delayGroup": "Medium",
39                      "detectRule": ""
40                     }
41
42                   }
43
44                ]
45               }
46
47            ]
48           }
49
50        ]
51       }
52
53     }
54
55  }
```

When the range is set, Citrix Workspace app on the user's device is automatically updated to the highest available version that falls between the mentioned range.

If you want to auto-update Citrix Workspace app to a specific version, enter the same version in the `maximumAllowedVersion` and `minimumAllowedVersion` properties in the Global App Configuration service.

> **Note:**
>
> - To enable auto-update version control, the `upgradeToLatest` setting in the Global App Configuration service must be set to false. If the upgradeToLatest setting is true, the `maximumAllowedVersion` and `minimumAllowedVersion` is ignored.
> - Do not modify the pluginId. The pluginId is mapped to Citrix Workspace app.
> - If the administrator hasn't configured the version in the Global App Configuration service, Citrix Workspace app is updated to the latest available version by default.
> - You can only use the version ranges that are set to update Citrix Workspace app. However, a downgrade isn't supported.

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

> - This feature is supported from release 2301 onwards.

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

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

Improved auto-update experience [Technical Preview] The automatic update feature automatically updates the Citrix Workspace app to the latest version, without any user intervention. Citrix Workspace app periodically checks for any latest updates and downloads the latest available version of the app. By default, automatic updates are enabled, unless your admin disable the automatic updates.

Installation starts when the Citrix Workspace app or the sessions are idle.

> **Note:**
>
> Citrix Workspace app cannot be accessed during the installation.

When you start the Citrix Workspace app, a notification appears to indicate the status of the installation.

You can disable the auto-update feature by navigating to **Preferences > Advanced > Updates** and unselecting the **Automatically keep Workspace app up to date** option.

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

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

Enhanced notch screen support Starting with the 2301 version, Citrix Workspace app for Mac supports Macs with a notch display. Macs support a native notch screen in full screen mode for retina

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

and multi-monitor displays. The area of the session in the notch screen is now much bigger and provides the customers with more screen space. This enhancement also supports high DPI scaling. The mouse position also appears accurate in all the external monitors connected. For more information, see Enhanced notch screen support.

> **Note:**
>
> Ensure not to select the **Scale to fit below built-in camera** option in the Citrix Viewer. This option isn't selected by default and can be found only on Macs with notch display.

App Protection enhancement Starting with the 2301 version, App Protection is enhanced to protect the Citrix Workspace app. This enhancement includes protecting the authentication screen and the screen that you see after signing into the Workspace app. For more information, see App Protection.

Global App Configuration service channel support [Technical Preview] 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 Global App Configuration service documentation.

Administrators can now use the Global App Configuration service to define settings, which are applicable to specific user-groups. This feature ensures that some features or functionalities can be made available to only certain users as required, and not to others.

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

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

Enhanced menu bar support Starting with the 2301 version, the CWA fully supports the **Automatically hide and show the menu bar in full screen** option in MacOS. For versions earlier than macOS 13, you must navigate to **System Preferences > Dock & Menu Bar** and clear the **Automatically hide and show the menu bar in full screen** option. For macOS 13 and later versions, you must navigate to **System Preferences > Desktop & Dock** and clear the **Automatically hide and show the menu bar in full screen** option. You have the provision to either enable or disable this option. This enhancement

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

also supports high DPI scaling. The mouse position also appears accurate in all the external monitors connected. For more information, see Enhanced menu bar support.

The figure below illustrates a window where the menu bar is hidden



The figure below illustrates a window where the menu bar appears



Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 107.1.1.13, based on Chromium version 107. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Set Citrix Enterprise Browser as the work browser You can now configure Citrix Enterprise Browser as a work browser to open all work links. You can select an alternate browser to open non-work links.

A work link is a link that is associated with the web or SaaS apps that the administrator configures for the end user. When a user clicks any link within a native application, if it's a work link, it's opened through the Enterprise Browser. If not, it's opened through any other browser that the end-user selects.

For more information, see Set Citrix Enterprise Browser as the work browser.

Fixed issues

- HTTP Live Streaming (HLS) protocol with High-Efficiency Advanced Audio Coding (AAC-HE) stream fails to play back audio on Citrix Enterprise Browser. [CTXBR-3899]
- When you click a hyperlink in the custom portal, an error message appears before opening the link. Later, the link opens in a system browser, for example, Google Chrome instead of Citrix Enterprise Browser. [CTXBR-4051]

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

- When using Citrix Workspace app for Mac with a custom web store URL, the versions of the operating system and Citrix Workspace app might not be shown in the user agent string. [CVADHELP-21377]
- With this fix, certain third-party apps such as Epic or Kronos might not freeze when you start them. [HDX-46140]
- When you attempt to start a session using an ICA file from Citrix Workspace app 2301 for Mac Beta build for the first time, the session might quit unexpectedly. [HDX-47361]
- When you add the custom portal site to Citrix Workspace app for Mac, a blank page might appear. [RFMAC-12857]

2211.1

What's new

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

Fixed issues

- You might face issues when you add or authenticate a store, or start a resource (apps or desktops) using the native Citrix Workspace app. [CVADHELP-22372]
- The incoming video and screen sharing might not work during Microsoft Teams optimized video calls. [HDX-50059]

2211

What's new

Workspace apps appear in the Dock with native app icons when opened [Technical Preview] Starting with the 2211 version, this feature is disabled by default.

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

Improved Mission Control and App Expose experience [Technical preview] Starting with the 2211 version, this feature is disabled by default.

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

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

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 105.2.1.40, based on Chromium version 105. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Fixed issues

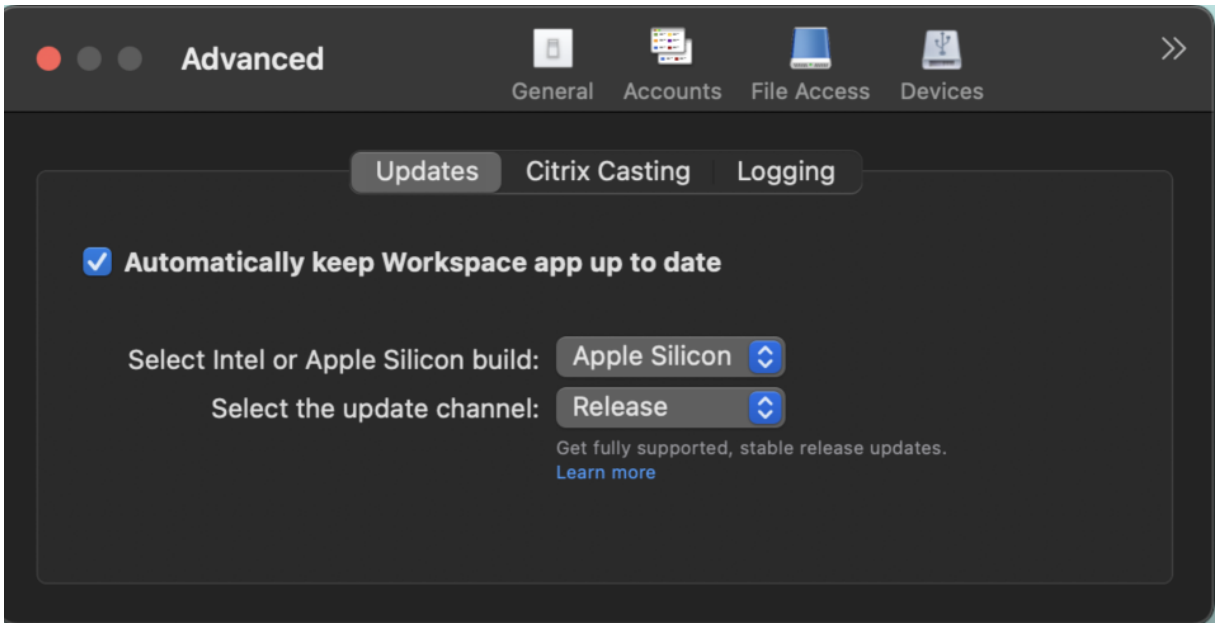
This release also addresses several issues that help to improve overall performance and stability.

2210

What's new

macOS 13 Ventura Support Citrix Workspace app for Mac is supported on macOS 13 Ventura (13.0).

Improved automatic update experience on Mac with Apple Silicon (M1 Series) Starting with this version, when you download the Universal Architecture build, you can choose between the Apple Silicon and Intel builds to support both the Apple Silicon and Intel based Mac machines.



On Apple Silicon machines, the users have the option to automatically update the Intel build even after having downloaded the Apple Silicon build. The option is provided in the **Preferences** tab.

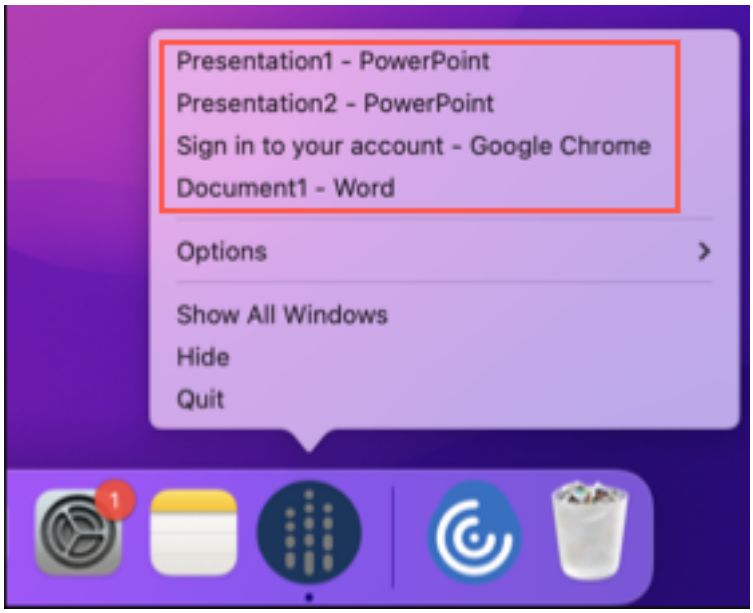
Advanced configuration for automatic updates You can configure Citrix Workspace automatic updates on Mac with Apple silicon (M1 Series) using the following methods:

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

- Graphical user interface
- Global App Configuration service (GACS)
- Mobile Device Management (MDM)
- StoreFront

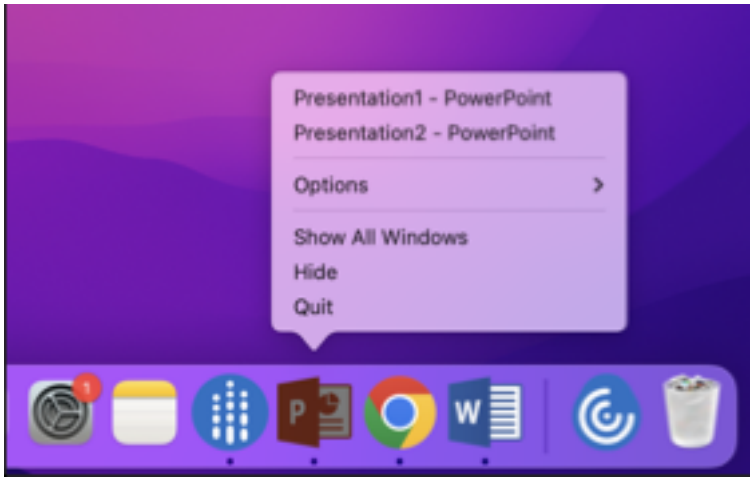
For more information, see Advanced configuration for automatic updates.

Workspace apps appear in the Dock with native app icons when opened [Technical Preview]
Previously, clicking virtual apps in the Citrix Workspace app triggered the Citrix Viewer where these apps would be available. If you open many apps, the apps or its instances opened in the Citrix Viewer. You can view the open apps by right-clicking the Citrix Viewer icon.



Starting with this version, when you open virtual apps, they appear in the Dock with their respective icons and are easily identifiable. You can then access the virtual app from the dock itself. If you open multiple instances of an app, these instances aren't duplicates in the Dock but are grouped within one instance in the Dock.

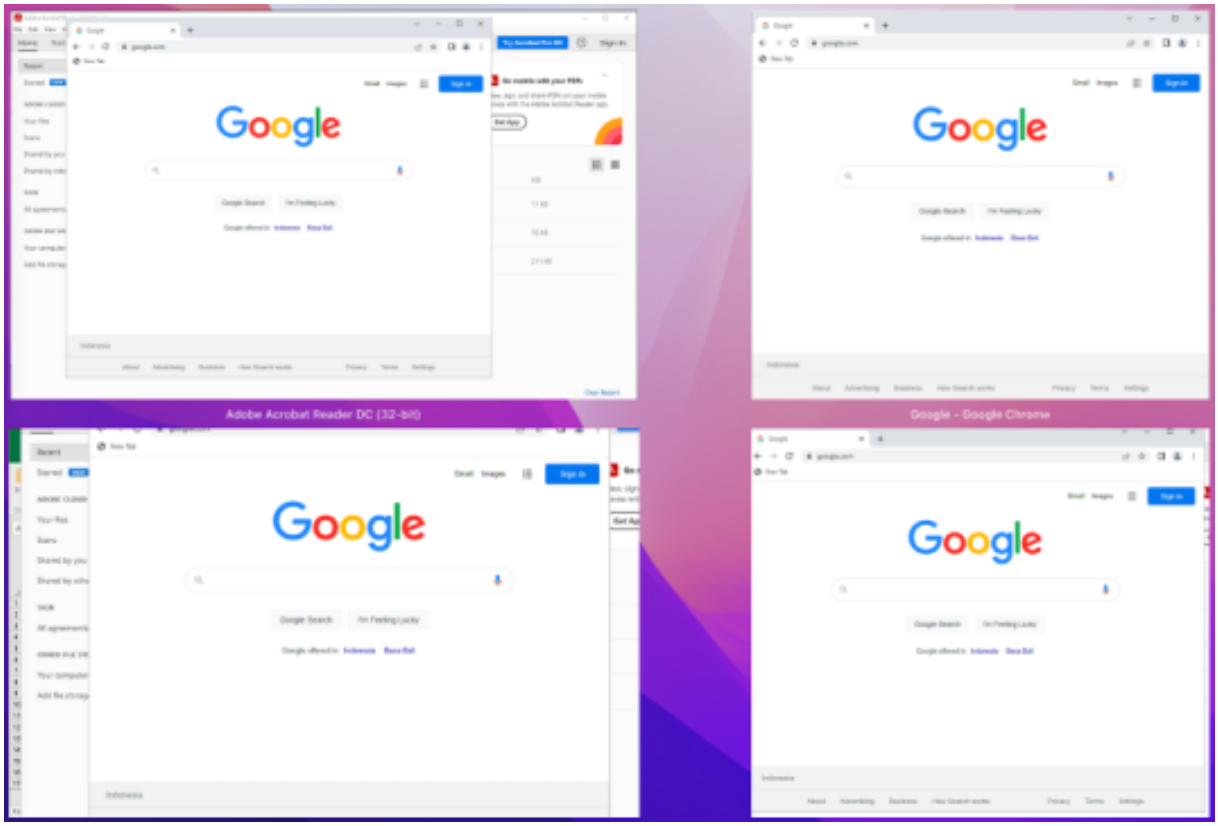
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

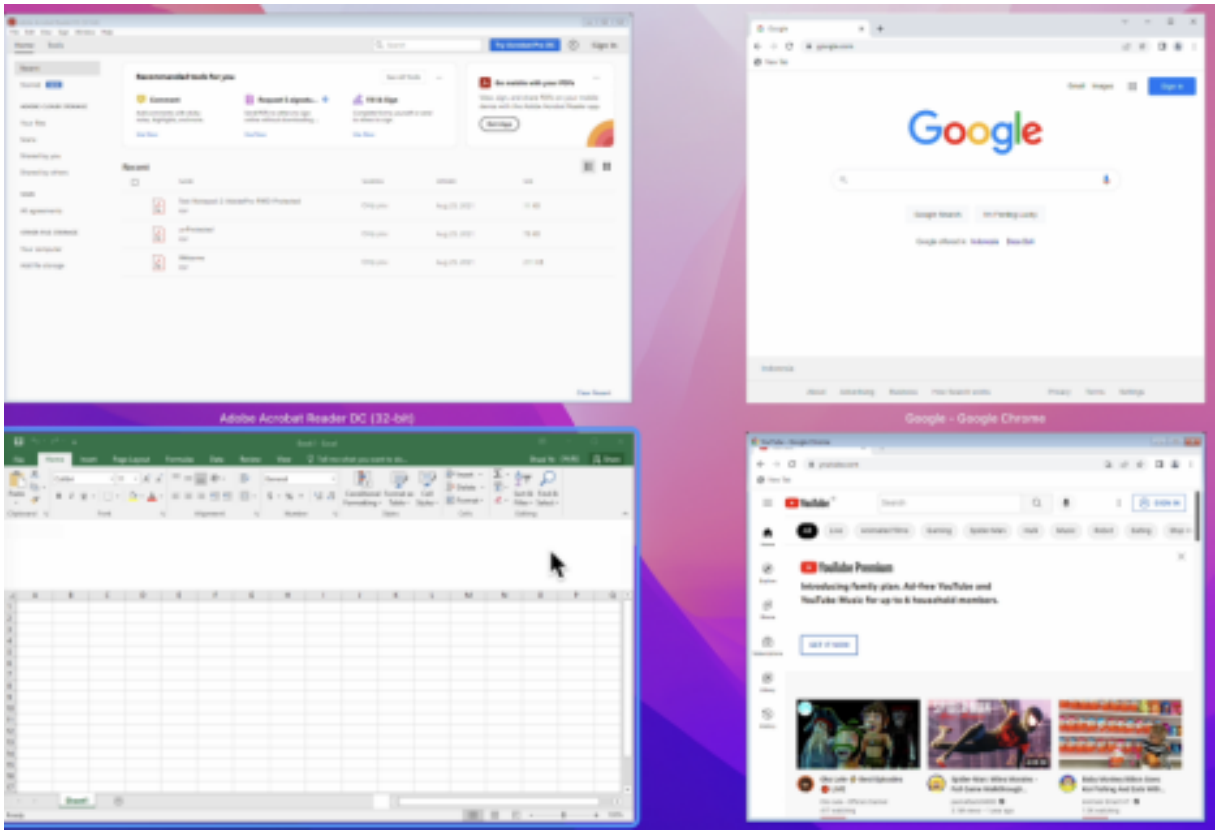
Improved Mission Control and App Expose experience [Technical preview] Previously, using the **Mission Control** or **App Expose** feature in a virtual app session resulted in the overlapping of many windows that were opened.

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



Starting with this version, when you use the **Mission Control** or **App Expose** feature in a virtual app session and open many windows, the windows do not overlap, and you can easily choose from among them.

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



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

Improved graphics performance [Technical preview] With this version, the performance of graphics is improved for desktop sessions.

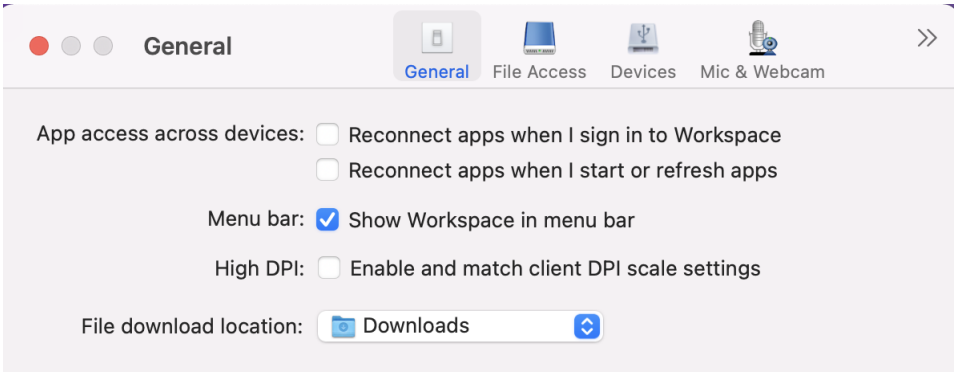
> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on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

Support for high DPI Citrix Workspace app for Mac is now compatible with one high DPI monitor with 4K or 5K resolution. With this feature, the text, images, and other graphical elements on virtual

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

desktop or app sessions appear in a size that can be viewed comfortably on these high-resolution monitors. For more information, see Support for high DPI.

To enable this feature, navigate to **Preferences > General > High DPI**.



> **Note:**
>
> The number of external monitors you can use with your mac is always limited by the Mac model, as well as the resolution and refresh rate of each display. Refer to the technical specifications of your Mac to find out the supported number of external monitors. For more information, see Connect one or more external displays with your Mac in the Apple support article.

Support for admin configuration of user devices through MDM tool Admins can now configure the following settings while deploying Citrix Workspace app through any MDM deployment tool such as Citrix Endpoint Management:

- **StoreURLs** –Configure store details so it's automatically added when the user opens the Citrix Workspace app, simplifying the sign-on experience.
  To add a store, provide the details for the **StoreURLs** setting. For example, `<string>https://myorg.com/?storename</string>`.
- **BlockStoreAddition** –Prevent the user from adding stores.

  To block the user from adding a store, set the value of the **BlockStoreAddition** setting to **True**.

For more information, see Support for store configuration of user devices through MDM tool.

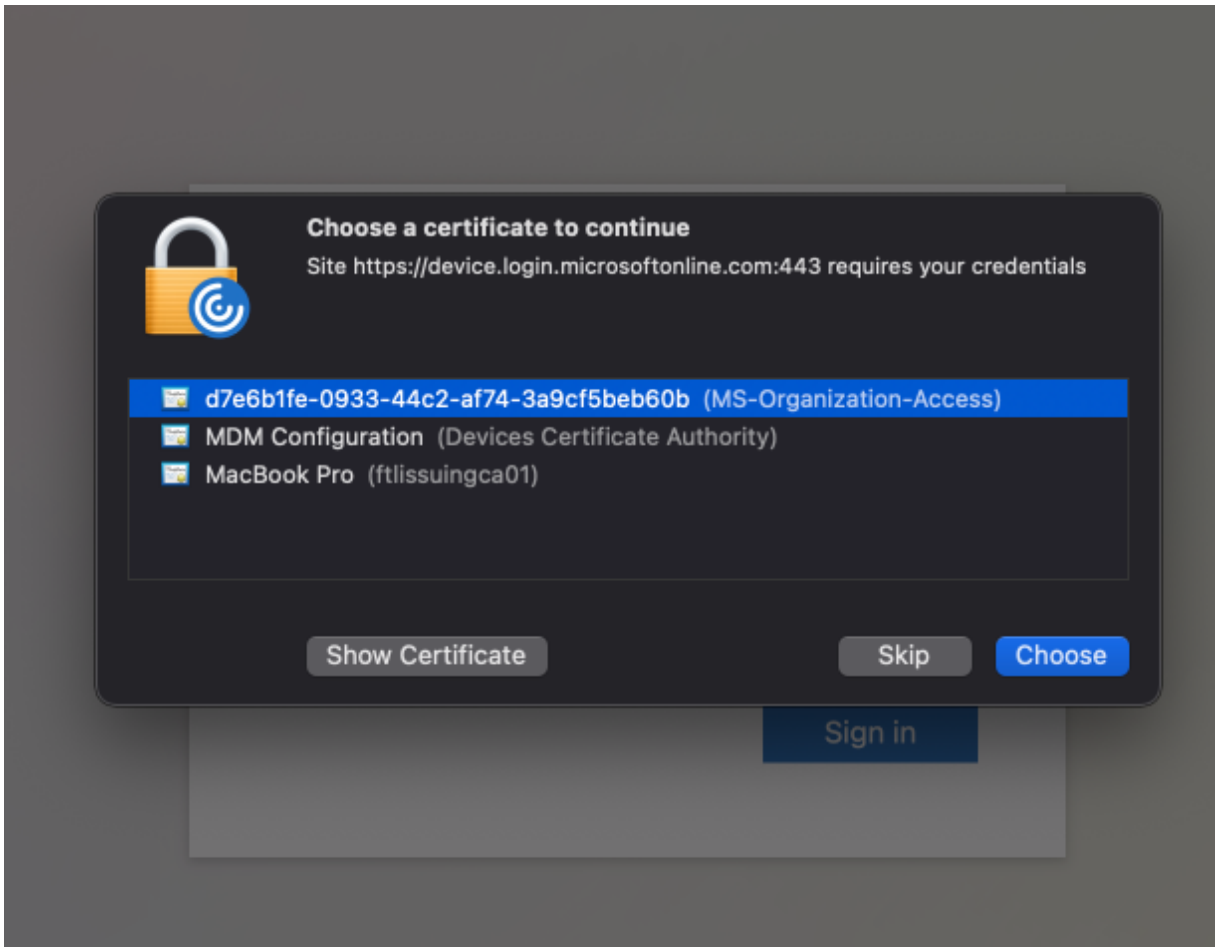
Support for certificate-based authentication [Technical Preview] You can now authenticate to Citrix Workspace app (cloud stores) by using a client certificate.

Previously, Certificate based authentication was supported on on-premises setups and customers on cloud setups were unable to sign in to Citrix Workspace app. This feature is disabled by default and admins must contact the Citrix help desk to enable this feature by filling this request form.

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

If your organization has configured Conditional Access with Azure Active Directory, then the user is prompted to select a Client Certificate for authentication while signing in. Certificate-based authentication adds another layer of security, ensuring that your device is compliant.

Once you add a store and enter valid credentials for that store, Citrix Workspace app displays a list of valid certificates available in your keychain for Client Authentication. If there's only one valid certificate in your keychain, it's selected by default.



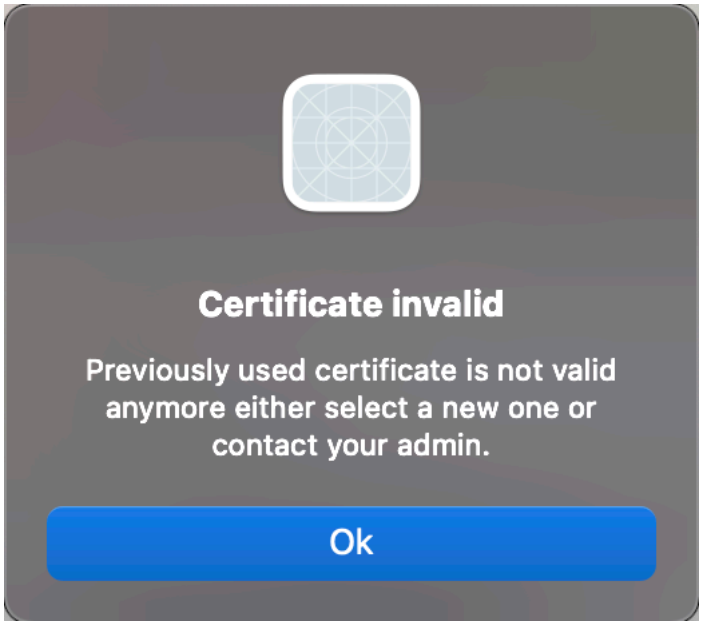
Once you choose a certificate, the identity provider validates it and the Workspace app store appears on successful validation.

> **Note:**
>
> - If there are no valid certificates in your keychain, the Citrix Workspace app performs the default handling for the certificate authentication request from the server.
>   This might prevent the user from logging in.
> - If your organization has configured Conditional Access with Azure Active Directory and valid certificates aren't found in your keychain, you can't log in to Citrix Workspace app.

If a previously selected certificate is no longer valid, an error message appears, prompting you to se-

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

lect a valid certificate or to contact your admin in the absence of one.



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

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

Rebranding Citrix Workspace Browser Citrix Workspace Browser is now Citrix Enterprise Browser. The custom scheme is now changed from citrixworkspace:// to citrixbrowser://.

Implementing this transition in our products and their documentation is an ongoing process. Your patience during this transition is appreciated.

- The product UI, in-product content, and the images and instructions in product documentation will be updated in the coming weeks.
- It's possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 105.1.1.19, based on Chromium version 105. For more information about the Citrix Enterprise Browser, see Citrix Enter-

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

prise Browser documentation. and other resources (such as videos and blog posts) that are linked from this product documentation might still contain former names.

Make Citrix Enterprise Browser the work browser [Technical Preview] You can now configure Citrix Enterprise Browser to open all work or enterprise links and apps configured by your administrator in the Citrix Workspace app. This feature provides a way for you to open only work links or web and SaaS apps in the Citrix Enterprise Browser.
You can select an alternate browser to open any other non-work links or apps.

Open all web and SaaS apps through the Citrix Enterprise Browser From this version, all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Enterprise Browser.

Support for browser extensions [Technical Preview] You can add extensions that are provided by your administrator to the Citrix Enterprise Browser in a secure way. An administrator can deploy, manage, and control the extensions. End users can view and use the extension under citrixbrowser://extensions as required. For more settings, see Global App Configuration service.

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

For information on how to configure, see the Citrix Enterprise Browser documentation.

Use Global App Configuration service to manage Citrix Enterprise Browser [Technical Preview]
The administrator can use the Global App Configuration service for Citrix Workspace to deliver Citrix Enterprise Browser settings through a centrally managed service.

The Global App Configuration service is designed for administrators to easily configure Citrix Workspace and manage the Citrix Workspace app settings. This feature allows admins to use the Global App Configuration service to apply various settings or system policies to the Citrix Enterprise Browser on a particular store. The administrator can now configure and manage the following Citrix Enterprise Browser settings using the Global App Configuration service:

- "Enable CEB for all apps"- Makes the Citrix Enterprise Browser the default browser for opening web and SaaS apps from the Citrix Workspace app.
- "Enable save passwords"- Allow or deny end users the ability to save passwords.
- "Enable incognito mode"- Enable or disable incognito mode.
- "Managed Bookmarks"- Allow the administrator to push bookmarks to the Citrix Enterprise Browser.

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

- “Enable developer tools”- Enable or disable developer tools within the Enterprise Browser.
- “Delete browsing data on exit”- Allow the administrator to configure what data the Citrix Enterprise Browser deletes on exit.
- “Extension Install Force list”- Allow the administrator to install extensions in the Citrix Enterprise Browser.
- “Extension Install Allow list”- Allow the administrator to configure an allowed list of extensions that users can add to the Citrix Enterprise Browser. This list uses the Chrome Web Store.

> **Notes:**
>
> - This feature is a request-only preview. To get it enabled in your environment, fill out the Podio form.
> - Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It’s advised that Beta builds aren’t deployed in production environments.
> - The name and value pair are case-sensitive.
> - All the browser settings in Global App Configuration service are under the following category:

```
{

    "category": "browser",
    "userOverride": false,
    "assignedTo": [
    "AllUsersNoAuthentication"
    ]
 }
```

> - The administrator can apply the settings to unmanaged devices as well. For more information, see Global App Configuration service documentation.

Technical Preview

- Upgraded version of WebRTC for the optimized Microsoft Teams

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

Fixed issues

- Citrix Workspace app might interrupt the restart or shutdown power action of a Mac device. [RFMAC-12530]

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

- The shift key might not work as expected in Citrix Workspace app for Mac version 2206. [CVADHELP-20674]

2209

What's new

Sign out of the custom web store when you close Citrix Workspace app When the **signoutCustomWebstoreOnExit** setting is set to **True**, closing the Citrix Workspace app window signs you out of the custom web store. When you reopen the Citrix Workspace app, the web store URL is loaded again. You can configure the **signoutCustomWebstoreOnExit** setting in the Global App Configuration service. For more information, see Sign out of the custom web store when you close Citrix Workspace app

Citrix Enterprise Browser This release includes Citrix Enterprise Browser (formerly Citrix Workspace Browser) version 103.2.1.10, based on Chromium version 103. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Fixed issues

- Citrix Workspace app for Mac might start automatically when you restart Citrix Workspace app for Mac or install Citrix Workspace app. [RFMAC-12392]
- The screen sharing feature in Optimized Microsoft Teams for certain third-party apps might fail on Citrix Workspace app for Mac. The issue occurs when the Thinwire codec policy is set to **For entire screen**. As a result, the app sharing feature is disabled and no options are available in the sharing panel. [CVADHELP-20853]

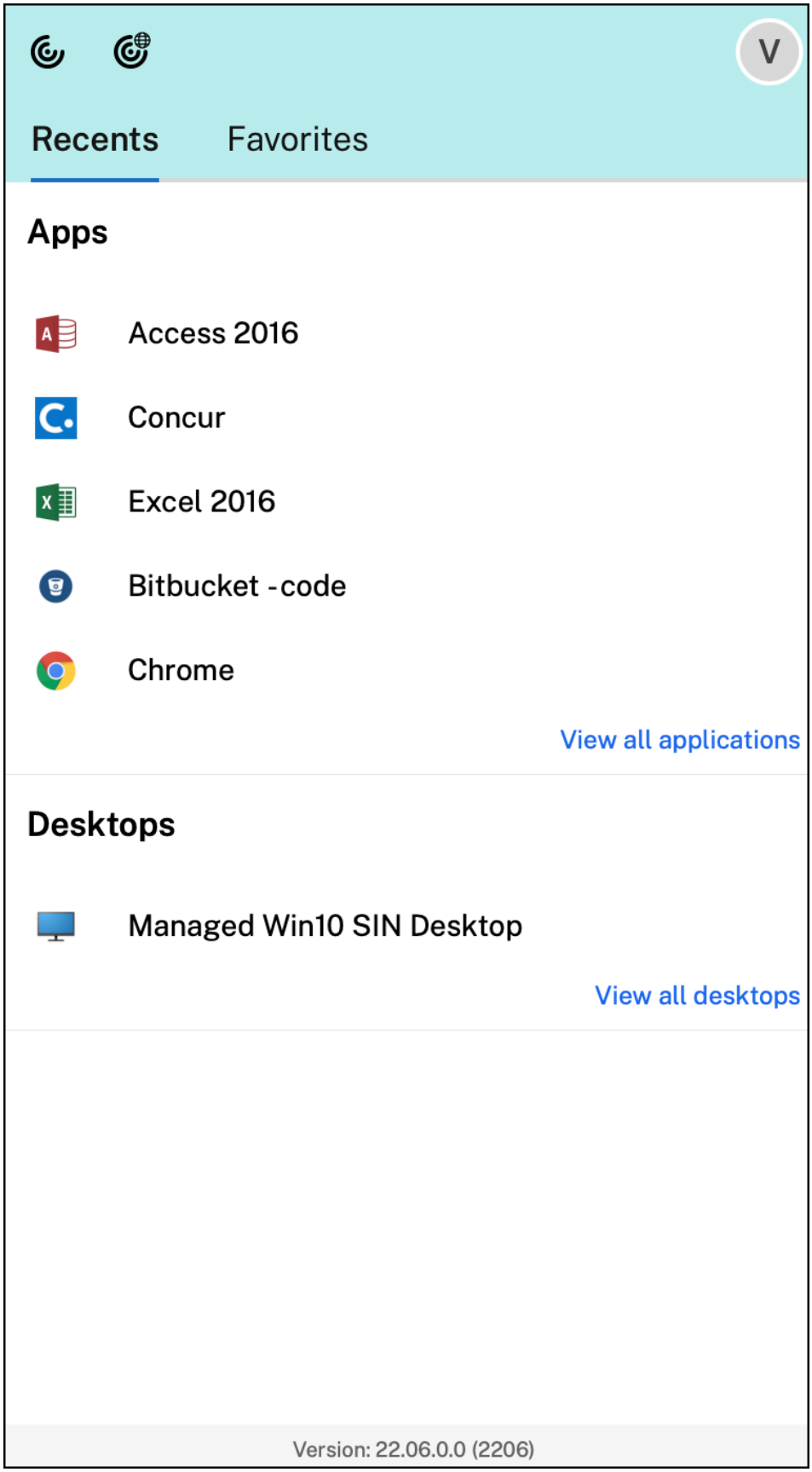
2208.1

What's new

View apps, desktops, and Citrix Enterprise Browser from the menu bar through a quick access menu You can now view your most recently used or favorite apps and desktops or open a Citrix Enterprise Browser window by clicking the Citrix Workspace icon in the menu bar. This feature provides easy access to some of your resources without having to open the Citrix Workspace app.

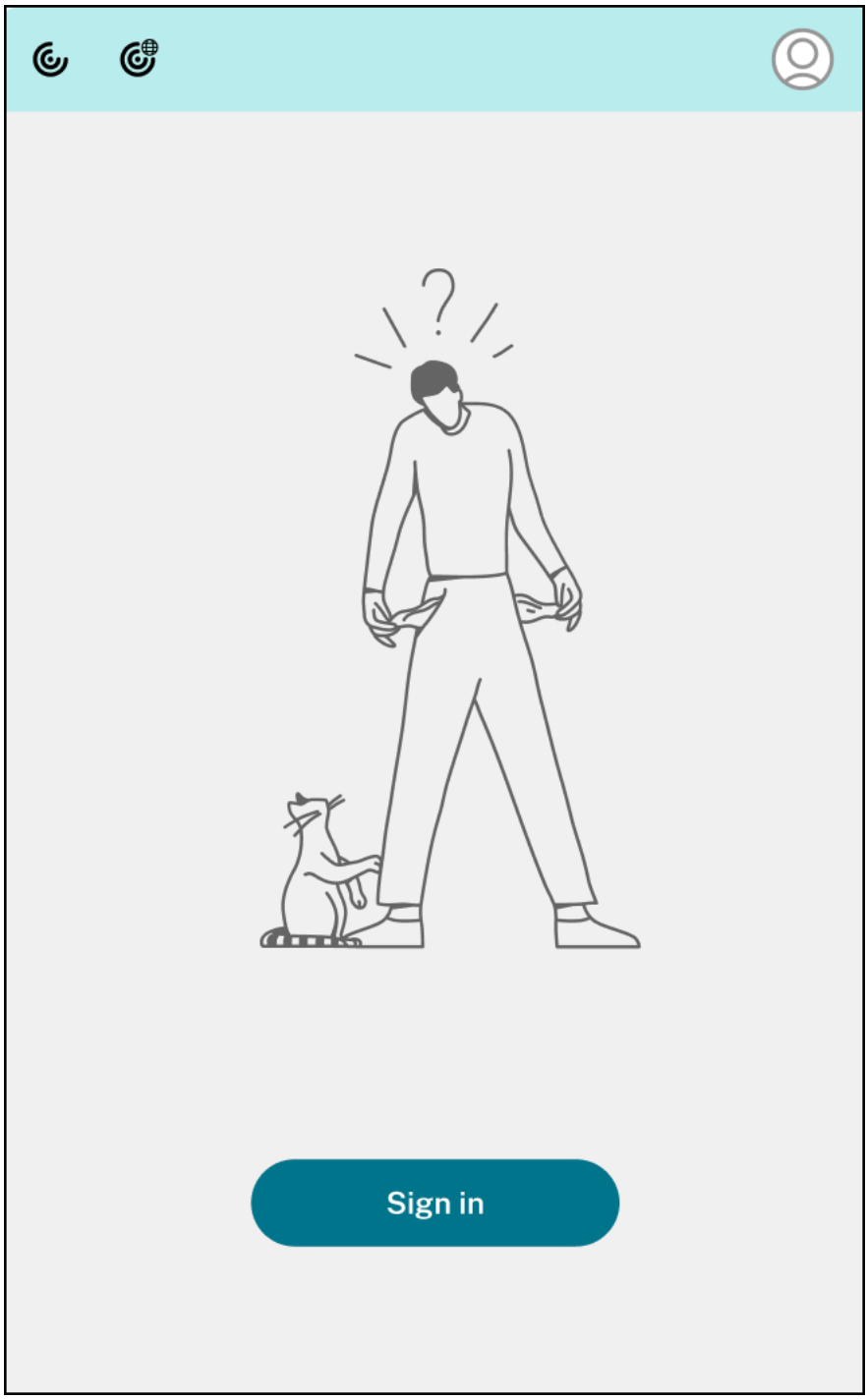
> **Note:**
>
> This feature isn't available on on-premises setups.

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



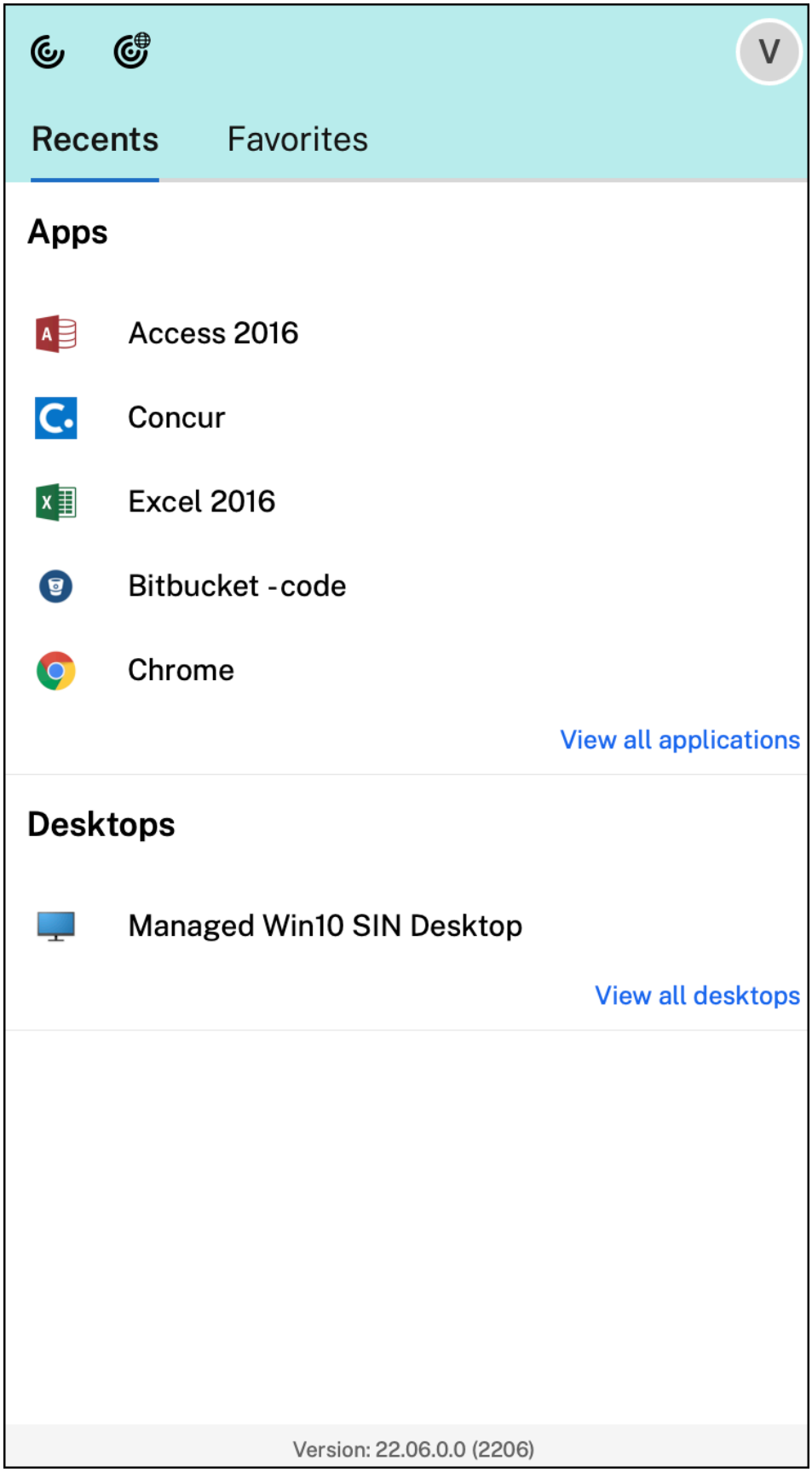
© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you've not configured any accounts, a sign-in prompt appears.



A maximum of 5 of your recently used or favorite apps or desktops appear in the options under the **Recent** and **Favorites** tabs respectively. To view the other apps in the Citrix Workspace app, click **View all applications**. To view the other desktops in the Citrix Workspace app, click **View all desktops**.

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



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

You can open the Citrix Workspace UI by clicking the Citrix Workspace app icon.

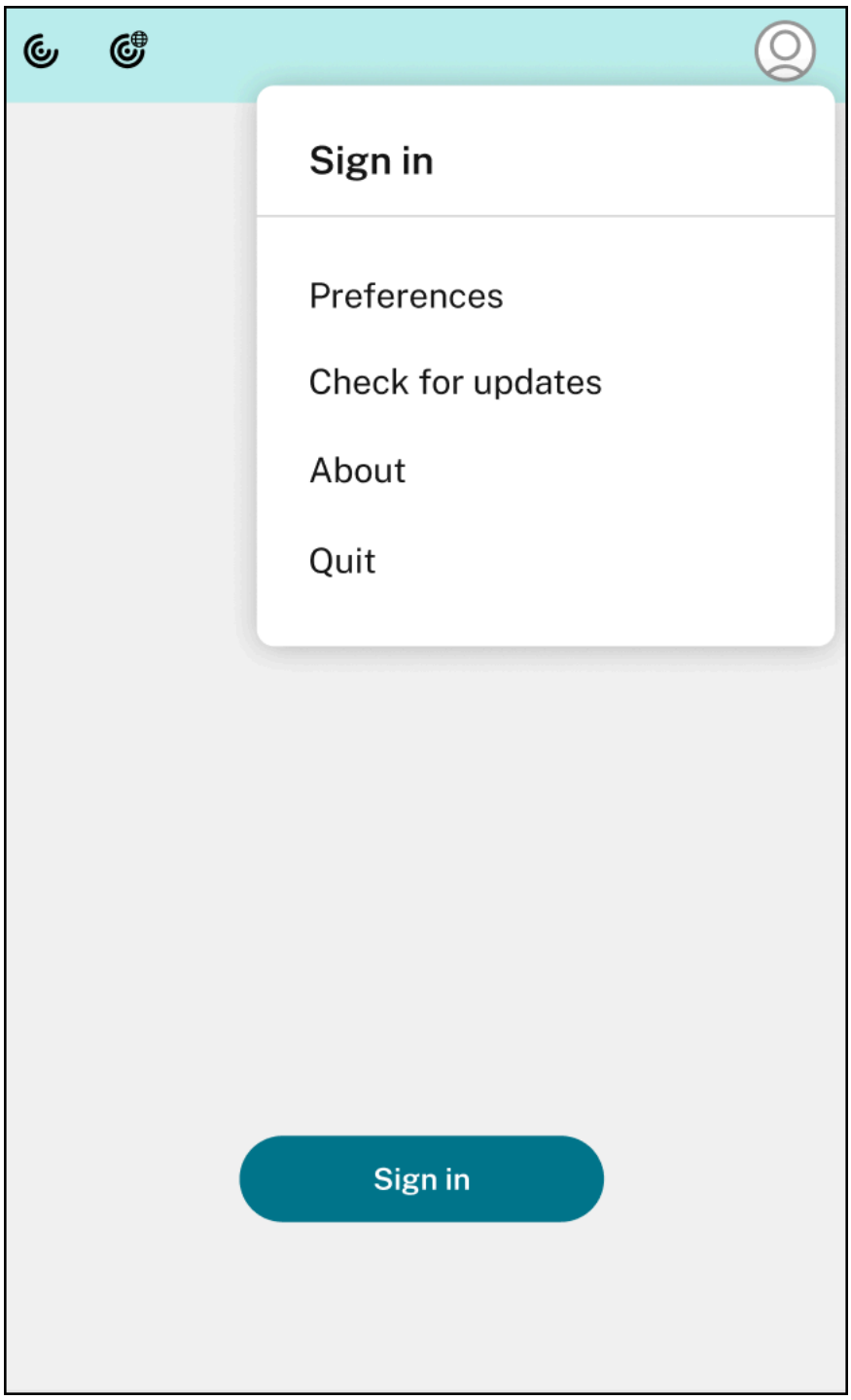


You can open the Citrix Enterprise Browser, without opening a web or SaaS app by clicking the Citrix Enterprise Browser icon.



> **Note:**
>
> The Citrix Enterprise Browser isn't available if the configured store doesn't have any web or SaaS apps. Further, it's available only if your admin has configured Citrix Secure Private Access.

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



You can view the following options when you click the **Account** icon in the top-right corner:

- Preferences
- Check for updates
- About
- Quit

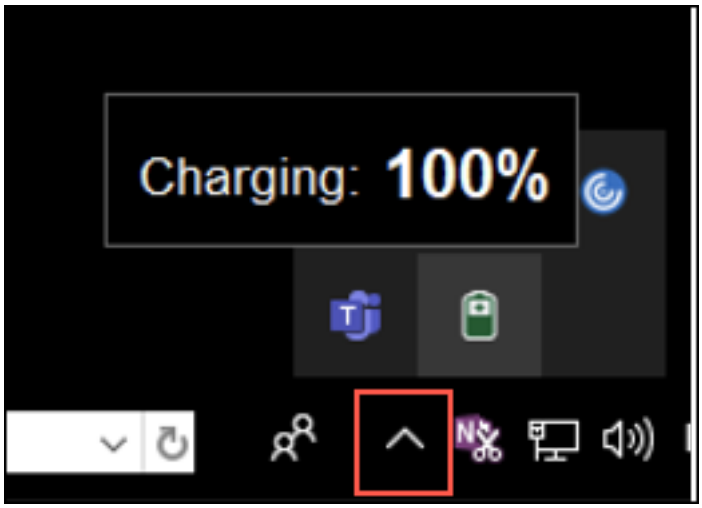
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see View apps, desktops, and Citrix Enterprise Browser from the menu bar through a quick access menu.

Support for authentication using FIDO2 [Technical Preview] With this version, users can authenticate within an HDX session using password-less FIDO2 security keys. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. For more information about FIDO2 see FIDO2 Authentication. This feature currently supports roaming authenticators (USB only) with PIN code and touch capabilities. You can configure FIDO2 Security Keys based authentication. For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.
When you access an app or a website that supports FIDO2, a prompt appears, requesting access to the security key. If you've previously registered your security key with a PIN (a minimum of 4 and a maximum of 64 characters), then you must enter the PIN while signing in.
If you've registered your security key previously without a PIN, simply touch the security key to sign in.

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

Battery status indicator The battery status of the device now appears in the notification area of a Citrix Desktop session. To view the battery status within the desktop session, click the **Show hidden icons** arrow in the taskbar.



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

> **Note:**
>
> The battery status indicator does not appear for server VDAs.

For more information, see Battery status indicator.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 103.1.1.14, based on Chromium version 103. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Citrix Enterprise Browser Profiles Profiles help you keep personal information such as history, bookmarks, passwords, and other settings separate for each of your Citrix Workspace accounts. Based your Workspace store, a profile is created, allowing you to have a unique and personalized browsing experience.

> **Note:**
>
> After you upgrade to version 103.1.1.14 and sign in to the device for the first time, only your previously saved passwords are removed. When you sign in to the device using a different store for the first time, all your previously saved data is lost.

Open all web and SaaS apps through the Citrix Enterprise Browser [Technical Preview] From this version, all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Enterprise Browser. You can register for this technical preview by using this Podio form.

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

Fixed issues

- When the Citrix Workspace login prompt appears, clicking the Cancel button doesn't close the popup and it appears repeatedly. [CVADHELP-19919]
- If you're using Direct Workload Connection in Citrix Cloud to connect to VDAs directly, a black screen appears and you're disconnected from the VDA. This issue occurs when Network Location Service (NLS) is enabled. [HDX-40588]

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

- When you use a multi-touch gesture to swipe between full-screen apps, the Citrix Workspace desktop session window turns black for a moment. This issue occurs on Macs with a notch display. [HDX-42314]

2206.1

What's new

Uninstall the app by dragging the Citrix Workspace app icon to the bin You can now simply drag or move the Citrix Workspace app icon into the bin to completely uninstall the app.

Previously, dragging the Workspace app icon into the bin would remove the app but leave behind certain system files on your Mac. With this version, the Citrix Workspace app and all its associated files are removed from your device when you drag the icon to the bin.

To uninstall the Citrix Workspace app by dragging it to the bin, do the following:

1. Close the Citrix Workspace app, if it's running.
2. Drag the Citrix Workspace app to the bin.
   Alternatively, you can right-click on the Citrix Workspace app and select **Options** > **Move to Bin**.
3. Provide your system credentials when prompted.
4. Close all running apps (Citrix Workspace) and click **Continue** to confirm.
   The Citrix Workspace app and all its system files are deleted from your device.

For more information, see Uninstall

Support for service continuity in the Safari browser The Citrix Workspace service continuity feature is now supported for the Safari browser. Users must install Citrix Workspace app for Mac and the Citrix Workspace web extension. Service continuity removes (or minimizes) the dependency on the availability of the components involved in the connection process. It allows you to connect to your virtual apps and desktops regardless of the cloud services' health status. For more information about the service continuity feature, see section Service continuity.

Improved audio echo cancellation support [Technical Preview] Citrix Workspace app now supports echo cancellation in adaptive audio and legacy audio codecs. This feature is designed for real-time audio use cases, and it improves the user experience.
Citrix recommends using adaptive audio.

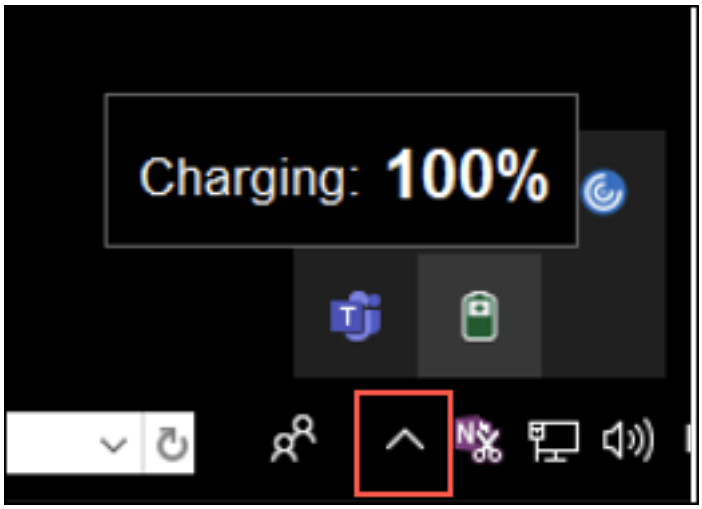
> **Note:**
>
> Technical previews are available for customers to test in their non-production or limited production environments, and share feedback. Citrix does not accept support cases for feature previews

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

> but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It's advised that Beta builds must not be deployed in production environments.

Enhancements to Optimized Microsoft Teams In optimized Microsoft Teams, you can now use the video function when more than one virtual desktop or app session is in use. For more information, see Enhancements to Optimized Microsoft Teams

Battery status indicator [Technical Preview] The battery status of the device now appears in the notification area of a Citrix Desktop session.



> **Note:**
>
> The battery status indicator does not appear for server VDAs.
>
> Technical previews are available for customers to test in their non-production or limited production environments, and share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds are not deployed in production environments.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 101.1.1.14, based on Chromium version 101. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Fixed issues

- The mouse pointer is misaligned on Macs with a notch display. [CVADHELP-19337]

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

- You're not signed out of the Workspace app when the inactivity timeout value lapses. This issue occurs intermittently. [CVADHELP-19812]
- You might get an error when you try to uninstall Citrix Workspace app. [CVADHELP-19121]
- In optimized Microsoft Teams, the video function might not work if you start another virtual desktop or app session. [HDX-40451]
- While sharing the screen or an app during the Microsoft Teams call, your peers might see visual artifacts. This issue occurs due to unstable frame rates, such as incorrect video playback (frozen or transient black frames). This release includes improved frame rates or sampling rates that help to reduce visual artifacts. [HDX-38032]

2204

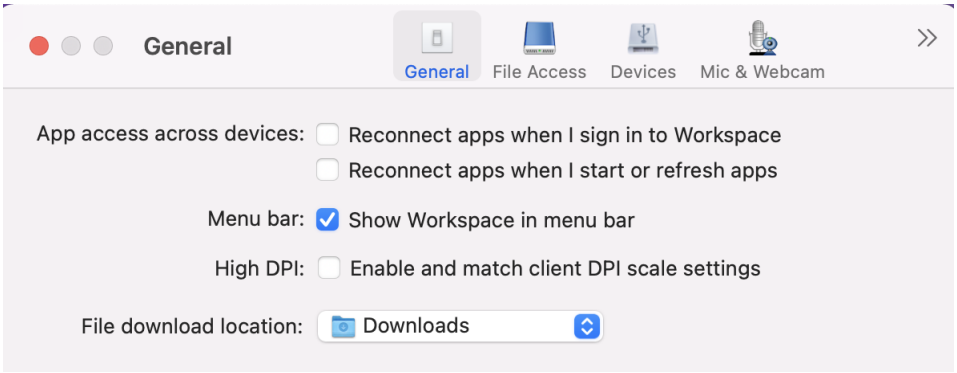
What's new

Global App Configuration service settings for `allowedWebStoreURLs` Admins can now use Global App Configuration service to configure settings of Custom Web Stores. Admins can configure the Custom Web Stores by using the `allowedWebStoreURLs` property. For more information about the Global App Configuration service, see Getting Started.

Support to open Citrix Workspace app in maximized mode Admins can configure the `maximise workspace window` property in the Global App Configuration service to enable the Citrix Workspace app to open in the maximized mode by default. For more information about the Global App Configuration service, see Getting Started.

Support for high DPI monitors [Technical preview] Citrix Workspace app for Mac is now compatible with one high DPI monitor with 4K or 5K resolution. With this feature, the text, images, and graphical elements on virtual desktop or app sessions appear in a size that can be viewed comfortably on these high-resolution monitors.

To enable this feature, navigate to **Preferences > General > High DPI**.



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

Administrators can edit the **Display memory limit** policy, which specifies the maximum video buffer size in kilobytes for a desktop session, to suit the display resolution. The default value for the **Display memory Limit** policy is 65536 KB and is sufficient for one high DPI monitor with 4K resolution.

For virtual app sessions, the default value of **Display memory Limit** is sufficient as the app session doesn't support more than one display.

For virtual desktop sessions, administrators must navigate to **Citrix Studio > Policies > Display memory limit** and use a higher value, for example 393216 KB to use High DPI features for more than one external monitor or 5K resolution monitor.

For more information about the Display memory limit policy, see Display memory limit.

Admins can edit the **Display memory limit** policy, which specifies the maximum video buffer size in kilobytes for a desktop session, to suit the display resolution. The default value for the Display memory Limit policy is 65536 KB and is sufficient for up to 2x4K monitors (2x32400KB). Admins must edit this value by navigating to **Citrix Studio** > **Policies** > **Display memory limit** and use a value of 393216 KB to use this feature.

For more information about the Display memory limit policy, see Display memory limit.

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

Enhancement to Permanent Client Access License (CAL) for Remote Desktop Sessions With this version, if you're running CAL in your environment to access remote desktops, when the client ID is greater than 15 characters, you can launch the remote desktop session with a permanent license.

To enable this feature, admins must configure the **`default.ica`** file by doing the following:

1. In the StoreFront server, navigate to *C:\inetpub\wwwroot\Citrix<StoreName>\App_Data* and open the **`default.ica`** file with any editor.
2. Add the following lines in the **[WFClient]** section:

```
isRDSLicensingEnabled=On
```

Restore default keyboard settings You can now restore the default keyboard settings if you have modified the settings in the keyboard preferences of Citrix Workspace app. To restore the keyboard

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

settings to its default values, open the Citrix Workspace app, navigate to **Preferences** > **Keyboard** and click **Restore Defaults**. Click **Yes** to confirm.

App Protection compatibility with HDX optimization for Microsoft Teams With this version, full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group. When you click **Share content** in Microsoft Teams, the screen picker removes the **Desktop** option. You can only select the Window option to share any open app, if the VDA is 2109 or higher. If you're connected to VDA older than 2019, no content is selectable.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 99.1.1.8, based on Chromium version 99. For more information about the Citrix Enterprise Browser, see Citrix Enterprise Browser documentation.

Make Citrix Enterprise Browser your default browser You can now make Citrix Enterprise Browser your default browser. Once you have made the Citrix Enterprise Browser your default browser, all links and Web and SaaS apps open in the Citrix Enterprise Browser by default.
To make Citrix Enterprise Browser your default browser on macOS, do the following:

1. Open the Citrix Enterprise Browser and click the ellipsis icon and open the **Settings** menu.
2. Click the **Default Browser** option on the left pane.
3. In the Default browser page, click **Make default**. When prompted, click **Use Citrix Enterprise Browser** to confirm your choice and apply the changes.

Fixed issues

- The mouse pointer is misaligned on Macs with a notch display. [CVADHELP-19337]
- You're not signed out of the Workspace app when the inactivity timeout value lapses. This issue occurs intermittently. [CVADHELP-19812]
- You might get an error when you try to uninstall Citrix Workspace app. [CVADHELP-19121]
- In optimized Microsoft Teams, the video function might not work if you start another virtual desktop or app session. [HDX-40451]
- While sharing the screen or an app during the Microsoft Teams call, your peers might see visual artifacts. This issue occurs due to unstable frame rates, such as incorrect video playback (frozen or transient black frames). This release includes improved frame rates or sampling rates that help to reduce visual artifacts. [HDX-38032]

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

Known issues

Known issues in 2411

You might encounter the Citrix Workspace app for Mac stops responding on the loading, authentication screen or closing unexpectedly after an admin updates the Workspace configuration (such as Identity Provider or Device Posture) in the Citrix Cloud™ Console. [RFMAC-17028]

To resolve the issue, users can reconfigure the store by following one of these methods:

Remove and re-add the store:

1. Open the **Workspace app**.
2. Navigate to **Preferences > Accounts**.
3. Select the store and click **Remove**.
4. Add the store again.

Reset Citrix Workspace app(for versions 2409 or later):

1. Open the **Workspace app**.
2. Go to the **Help** menu.
3. Click **Reset Citrix Workspace**.
4. Add the store again.

> **Note:**
>
> Resetting Citrix Workspace app removes all configured stores.

Known issues in 2409.10

There are no new known issues.

Known issues in 2409

There are no new known issues.

Known issues in 2405

- You might have noticed that the newly added apps are not visible to the end user on the automatic refresh of Citrix Workspace app. As a workaround, refresh Citrix Workspace app to view the newly added apps. [CVADHELP-25189]
- When you open the Citrix Workspace app for Mac through the custom web portal, you might notice that the links on the landing page direct you to blank pages. As a workaround, refresh the page to load the content. [CVADHELP-25665]

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

Known issues in 2311

- The HTML5 Video redirection feature is disabled by default in Citrix Workspace app for Mac from version 2311. [HDX-53015]

Known issues in 2402.10

- If the Force Ephemeral Profiles setting is enabled through the Global App Configuration service for Citrix Enterprise Browser, and the user closes the browser window(s) without quitting the browser, it goes into a state where creating new tabs and typing into the omnibox might not function as expected. As a workaround, the user should quit the browser completely and then reopen it. [CTXBR-8738]

Known issues in 2402

- You might notice that the application screen is hidden at the notch when you enter full screen in the virtual sessions for some Macs. As a workaround, adjust the app window to make it fit below the screen notch. [HDX-63035]

Known issues in 2308

- After upgrading Citrix Workspace app for Mac to version 2308, the preferences window might be unresponsive for any user actions. As a workaround, force quit Citrix Workspace app and restart it. For more information about forcing an app to close on a Mac, see Force an app to close in the Apple support article. [RFMAC-14596]

Known issue in 2307

No new issues have been observed in this release.

Known issue in 2306

No new issues have been observed in this release.

Known issues in 2305

- After upgrading Citrix Workspace app for Mac to version 2305, certain third-party virtual apps that have pop-up dialogs for entering user name and password might become unresponsive upon opening. [CVADHELP-23032]

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

Known issues in 2304

- A user with multiple accounts might see the Citrix Workspace app loading screen for a long time. As a workaround, you must quit Citrix Workspace app and restart it. [RFMAC-13432]

Known issues in 2301.1

- You can't update to Citrix Workspace app for Mac version 2301.1 using the auto-update service. As a workaround, you must manually install the Citrix Workspace app for Mac version 2301.1 by downloading the .dmg file available on the Downloads page.

Known issues in 2301

- On macOS Ventura devices, progressive web apps (PWA) fail to open. The following error message appears:

  App Name is damaged and can't be opened. You should move it to the Bin.

  As a workaround, right-click on the app and select Open. If you're using the keyboard, press the Ctrl key and click the app. Select Open. [CTXBR-3885]
- An infinite loading spinner might appear when users sign in to Citrix Workspace associated with Global App Configuration service. This issue doesn't impact StoreFront and custom web stores. [RFMAC-13086]

Known issue in 2211.1

No new issues have been observed in this release.

Known issues in 2211

- When using Citrix Workspace app for Mac 2209 and later versions, the user sign-in page might not be displayed while using the custom web portal. As a workaround, quit Citrix Workspace app by using the **Quit** option from Citrix Workspace icon in the menu bar. [CVADHELP-21377]

Known issues in 2210

- On macOS 13 Ventura, the seamless app interaction might run into issues when you change the **All at Once default** option to the **One at a Time** option in the **Stage Manager** preference under the **Stage Manager** feature. [HDX-44567]

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

- Attempts to start a desktop session in offline mode might fail. As a workaround, resize the session window. [HDX-45081]
- When resizing a session to full-screen mode on a MacBook, the focal point of a cursor might appear slightly above the actual cursor position. As a workaround, navigate to **System Preferences > Dock & Menu Bar** and enable the **Automatically hide and show the menu bar in full screen** option. [HDX-45585]
- With the 2210 version, using Mission Control or App Expose features in an app session might cause Citrix Workspace app to close unexpectedly. [HDX-46130]
- When launching certain third-party apps such as Epic or Kronos, the sign-in window of the apps might covered by another window. As a result, the entire session freezes. As a workaround, perform one of the following actions:

  - Drag the window that is blocking the sign-in window away from it.
  - Locate the sign-in window using the Mission Control feature.
  - Use the keyboard shortcut **Command+~** to switch windows.

  [HDX-46140]

Known issues in 2209

No new issues have been observed in this release.

Known issue in 2208.1

No new issues have been observed in this release.

Known issue in 2206.1

No new issues have been observed in this release.

Known issue in 2204

- When traffic is tunneled through NGS, Citrix Workspace app might fail to upload or download files that are greater than 64 MB. [CTXBR-3354]

Known issues in 2203.1

- You can't click the **Create** button in the Jira app if the browser window is minimized. [CTXBR-1976]

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

- Web socket connections aren't tunneled through Citrix Secure Private Access. [CTXBR-2439]
- After upgrading the Citrix Workspace app to version 2203, a question mark icon appears on the Citrix Enterprise Browser icon. This issue occurs if the Citrix Enterprise Browser was pinned to the dock before the upgrade. [CTXBR-2864]
- When you click the **Reset settings** option on the **Advanced** settings section of the Citrix Enterprise Browser, the log settings do not reset to default. As a workaround, click the **Reset to default log settings** option available on the **Logs** page. [CTXBR-2929]
- After upgrading Citrix Enterprise Browser from version 2201 to version 2203, you are unable to save new passwords and already saved passwords are lost. [CTXBR-3063]
- Full screen mode isn't available on Macs with a notch. [CVADHELP-19337]
- When you launch a desktop or app session using the browser, the session window launches in the background, behind the browser window. [RFMAC-11362]

Known issues in 2201

- The client name appears with random characters in the Citrix Broker Service and the Citrix Director if you're using the Citrix Workspace app in the offline (intranet) mode. [RFMAC-10842]

Known issues in 2112

- In Citrix Workspace app, you might experience intermittent failures when answering or making a Microsoft Teams call. The following error message appears:
  "Call could not be established."[HDX-38819]

Known issues in 2111

No new issues have been observed in this release.

Known issues in 2109.1

No new issues have been observed in this release.

Known issues in 2109

- If you've configured the Citrix Workspace app using the `.cr` file, and signed in with your credentials, the home page appears after a delay. [RFMAC-9990]

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

- If a Progressive Web App (PWA) that is protected is opened on macOS, the *App Protection* policies aren't enforced. [RFMAC-10128]
- After you add stores in the Citrix Workspace app and change the **Current Reauthentication Period** in **Reauthentication Period for Workspace App** and switch from on-premises to the cloud store after a few minutes, you're signed out of the cloud store and an authentication prompt appears. Once you sign in to the Citrix Workspace app, the spinner appears indefinitely and you're unable to sign in. [RFMAC-10140]

Known issues in 2108.1

No new issues have been observed in this release.

Known issues in 2108

- When you start a subscribed SaaS app after changing the authentication domain in the server console, the session does not start and the following error message appears:

  "AuthDomain has changed. Please sign in again after some time"

  [RFMAC-9616]

Known issues in 2107

- When you change the authentication domain in the server console and sign in with your credentials, the following error message appears:

  Cannot connect to the server

  You can access the store once you click OK.

  [RFMAC-9494]

Known issues in 2106

- A black window appears when you share your screen. [HDX-30083]

Known issues in 2104

No new issues have been observed in this release.

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

Known issues in 2102

No new issues have been observed in this release.

Known issues in 2101

- Attempts to access files under Network Shares from within Citrix Workspace app for Mac might fail even when the option is enabled. [RFMAC-7272]
- On macOS Big Sur, attempts to launch the web SAML single sign-on app on Citrix Workspace app for Mac might fail, displaying the following error message.

  ```
  Page could not load. Please try again later or contact your
  administrator for assistance. Incident ID:-202
  ```

  [RFMAC-7282]

Known issues in 2012

- When you start a video call, Microsoft Teams might become unresponsive, displaying a `Citrix HDX not connected` error. As a workaround, restart Microsoft Teams or the VDA. [RFMAC-6727]
- Video calls on Microsoft Skype for Business aren't supported on macOS Big Sur (11.0.1).
- On macOS Big Sur (11.0.1), attempts to connect USB devices might fail, causing the session to exit unexpectedly. As a workaround, reconnect the USB device. [RFMAC-7079]

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

Citrix Workspace app for Mac Third-Party Notices

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

Features in Technical Preview

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

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	Feedback form (Click the icon)
DNS caching for improved session resilience	2607	
EDT MTU Rediscovery	2607	
Streaming read and write for Client Drive Mapping (CDM)	2607	
HDX Direct for Service Continuity for connectorless workloads	2607	
HDX graphics super resolution	2607	
Location redirection for virtual sessions	2607	
Resilient and secure third-party plugin execution	2607	
Support for Citrix Snipping tool integration	2603.11	
Shield V2 service continuity	2603	
Support for Microsoft Teams VDI Plugin installation	2603	
Audio Quality Enhancer for reliable transport	2508	

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

Title	Available from version	Feedback form (Click the icon)
Enhancing hybrid mode support with GACS for cloud stores	2503	
Support for single sign-on to Citrix Secure Access automatically through Citrix Workspace app	2402	
Support for Citrix Secure Private Access for on-premises deployments	2309	

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

DNS caching for improved session resilience

Technical Preview from 2607 version	Feedback form

Starting with version 2607, Citrix Workspace app for Mac caches the Citrix Gateway Service PoP address after each successful session connection. If DNS is temporarily unavailable when a user tries to launch or reconnect to a session —due to a DNS provider outage or an unstable network —the Workspace app automatically falls back to the cached address, allowing the session to proceed without any user intervention.

Without this, a DNS outage translates directly into session launch failures for end users. With DNS caching enabled, session failures during DNS outages are **reduced drastically**.

> **Note:**
>
> DNS caching improves resilience against DNS service disruptions but does not guarantee suc-

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

> cessful session establishment in all scenarios. If the previously cached gateway service PoP is unavailable due to planned maintenance, service disruption, or network reachability issues, session launches may still fail.
>
> If a user has changed locations since the address was last cached, the Workspace app may connect through a gateway service PoP that is not geographically optimal, resulting in slightly higher latency. This is a deliberate tradeoff —a connected session with higher latency is preferable to a failed launch.

To disable it using the terminal command, run the following:

```
defaults write com.citrix.receiver.nomas EnableDNSCACHE -bool false
```

To disable this feature through MDM, use the following setting:

```
<key>EnableDNSCACHE</key><false/>
```

EDT MTU Rediscovery

Technical Preview from 2607 version Feedback form

Starting with version 2607, Citrix Workspace app for Mac supports EDT MTU Rediscovery. Previously, if the MTU decreased after a session was established, ICA traffic could become fragmented, resulting in performance degradation or disconnects. With EDT MTU Rediscovery, MTU changes can be detected and the session MTU is automatically adjusted, improving reliability and stability for users on networks with asymmetric routing or dynamic path changes, such as load-balanced proxy environments. For more details, see Enlightened Data Transport Documentation.

To disable it using the terminal command, run the following:

```
defaults write com.citrix.receiver.nomas EnableMtuRediscovery -bool
    false
```

To disable this feature through MDM, use the following setting:

```
<key>EnableMtuRediscovery</key><false/>
```

Streaming read and write for Client Drive Mapping (CDM)

Technical Preview from 2607 version Feedback form

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

Starting with version 2607, Citrix Workspace app for Mac supports read and write streaming for Client Drive Mapping, significantly improving file transfer performance over high-latency connections.

- **Read streaming**: Large file reads from the client are delivered as a multi-packet chunked response in a single request, eliminating repeated round-trips.
- **Write streaming**: Large file writes from the host are accumulated in memory and flushed to disk in a single OS write call, reducing round-trips.

Previously, file operations on mapped client drives involved many small synchronous round-trips, causing slow performance for users connecting from remote locations.

To enable it using the terminal command, run the following:

```
defaults write com.citrix.receiver.nomas EnableCDMReadWriteStream -bool
    YES
```

To enable this feature through MDM, use the following setting:

```
<key>EnableCDMReadWriteStream</key><true/>
```

HDX Direct for Service Continuity for connectorless workloads

Technical Preview from 2607 version | Feedback form

Starting with version 2607, Citrix Workspace app for Mac supports HDX Direct for sessions launched using Service Continuity for connectorless workloads, allowing clients to establish direct connections with the session host during a cloud outage.

To configure this feature:

1. Ensure that you have a Service Continuity for connectorless workloads environment.
2. Set the **HDX direct** DDC policy to **Allow**.

To enable this feature using the terminal command, run the following:

```
defaults write com.citrix.receiver.nomas EnableShieldHDXDirect -bool
   YES
```

To enable this feature through MDM, use the following setting:

```
<key>EnableShieldHDXDirect</key><true/>
```

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

HDX graphics super resolution

Technical Preview from 2607 version Feedback form

Starting with version 2607, Citrix Workspace app for Mac supports HDX graphics super resolution. HDX graphics super resolution seamlessly downscales video regions on the Virtual Delivery Agent (VDA) and uses the Mac client's hardware to upscale them back to their original resolution without noticeable quality degradation or performance impact. This reduces the network bandwidth required for high-quality video while preserving visual fidelity.

This feature requires the following:

- macOS 26 (Tahoe) or later
- The H.265/XDecoder graphics path enabled (enabled by default)
- VDA configured for HDX graphics super resolution. HDX graphics super resolution is enabled by default in automatic mode starting with CVAD 2603. Use the **HDX graphics super resolution** Citrix Studio policy to control this behavior.

> **Note:**
>
> This feature is disabled by default on the Mac client.

To enable this feature using the terminal command, run the following:

```
defaults write com.citrix.receiver.nomas EnableSuperResolution -bool
    YES
```

To enable this feature through MDM, use the following setting:

```
<key>EnableSuperResolution</key><true/>
```

Location redirection for virtual sessions

Technical Preview from 2607 version Feedback form

Starting with version 2607, Citrix Workspace app for Mac supports redirecting the client device's geographic location to the virtual session. Server-side applications running in the session, such as Maps, can access the end user's real-world location as if the application were running locally. This feature is also known as **Location Redirection** or **Device Sensor Redirection**.

This feature requires the following:

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

- macOS 11 or later
- A Windows VDA that supports location redirection. For multi-session VDAs, Windows 22H2 or later with Citrix GeoLocSync enabled.

This feature is disabled by default and requires all three components —VDA, DDC, and client —to be enabled. To configure it:

1. **On the VDA**, navigate to **Privacy & security > Location** and enable **Location services** and **Let apps access your location**. Then enable the following based on the VDA type:
   - **Single-session VDA**: **Allow location override**
   - **Multi-session VDA** (Windows 22H2 or later): **Citrix GeoLocSync**
2. **On the DDC**, navigate to **User setting > ICA > Client Sensors > Location** and set the **Allow applications to use the physical location of the client device** policy to **Allowed**. This policy is set to **Prohibited** by default.
3. **On the client**, in **System Settings > Privacy & Security > Location Services**, turn on **Location Services** and enable location access for **Citrix Viewer**. Then run the following command and restart Citrix Workspace app for the change to take effect:

```
defaults write com.citrix.receiver.nomas EnableGEORedirection -
    bool YES
```

To enable this feature through MDM, use the following setting:

```
<key>EnableGEORedirection</key><true/>
```

> **Note:**
>
> On the first location request in a session, the user is prompted to **Allow** or **Don't Allow**. If the user selects **Don't Allow**, the VDA receives an Access-Denied status and no location data is shared for that session.

Resilient and secure third-party plugin execution

Technical Preview from 2607 version — Feedback form

Starting with version 2607, Citrix Workspace app for Mac introduces the plug-in Manager, a general out-of-process host for third-party virtual-channel plugins built against the Citrix Virtual Channel SDK (VCSDK).

Previously, plug-ins ran inside the same process as the Citrix session. This meant that a plugin crash could bring down the entire session, forcing users to reconnect and lose their work. With plug-in Manager, plug-ins run in a dedicated isolated process, separate from the session:

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

- **Sessions survive plugin crashes**: If a plug-in such as Teams VDI encounters an error, it recovers automatically without disrupting the user's session or requiring a reconnect to the VDA.
- **Stronger session security**: The session process runs with full macOS security hardening enabled. Plug-ins are isolated so that a misbehaving or compromised plug-in cannot affect the session or other running applications.
- **No changes required for existing plugins**: The architecture is fully backward compatible. Existing plug-ins work without modification.

> **Note:**
>
> This feature is in Technical Preview and is not recommended for production use. Feedback can be submitted through the Citrix Feedback portal.

To enable this feature through MDM, use the following setting:

```
<key>EnablePluginBroker</key><true/>
```

Support for Citrix Snipping tool integration

Technical Preview from 2603.11 version	Feedback form

Starting with version 2603.11, Citrix Workspace app for Mac supports Citrix Snipping tool integration. This feature allows you to seamlessly capture screenshots of overlay and redirected content within your Citrix Virtual Apps and Desktops sessions.

Requirements

- Virtual Delivery Agent (VDA) version 2603 or later

To enable the feature, run the following command:

```
defaults write com.citrix.receiver.nomas EnableScreenCapture -bool YES
```

For more information, see Citrix snipping tool integration in Assistant.

Shield V2 service continuity

Technical Preview from 2603 version	Feedback form

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

Starting with version 2603 Preview, Citrix Workspace app for Mac supports Shield V2, which removes or minimizes dependency on components involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services.

Shield V2 is connector-less and operates without Cloud Connector involvement in the workflow, as compared to Shield V1.

Shield V2 supports:

- Session launch during DaaS or Workspace outage
- New session launches with Shield

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

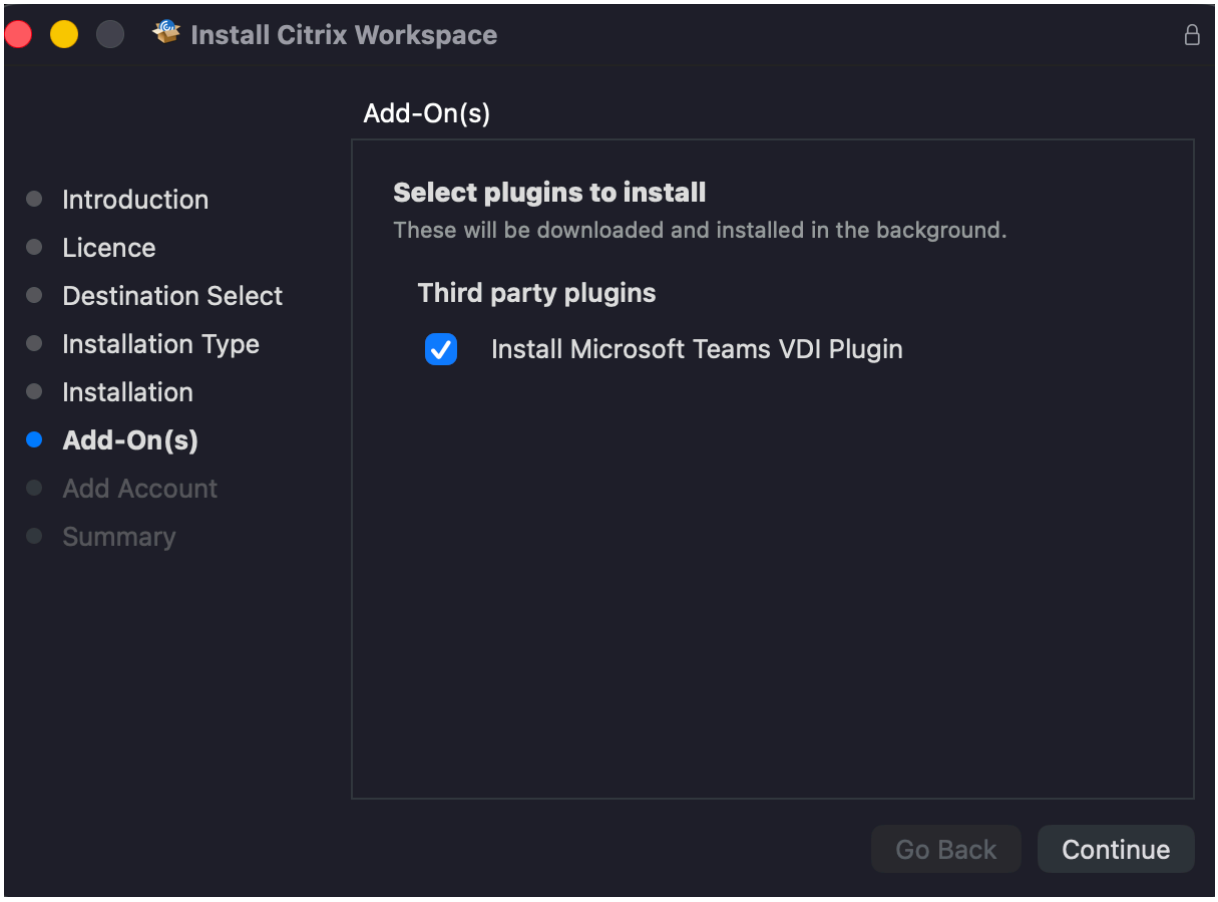
Support for Microsoft Teams VDI Plugin Installation

Technical Preview from 2603 version	Feedback form

Starting with the 2603 version, the Microsoft Teams VDI Plugin is a key client-side component required for Microsoft Teams SlimCore Optimization for Mac. The DMG installer now provides an **Add-On(s)** option, allowing users to select and install the Microsoft Teams VDI Plugin during a fresh Citrix Workspace app installation. The checkbox for the plugin is unchecked by default.

Microsoft Teams VDI Plugin Starting with Citrix Workspace App 2603, the DMG installer provides an **Add-On(s)** option, allowing users to select the option and install the Microsoft Teams VDI Plugin during a fresh CWA Installation.

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



Microsoft Teams SlimCore Optimization for Mac is in Public Preview at the time of writing and administrators may need to enable Teams tenant-side configuration. For more details, see New VDI solution for Teams.

The Microsoft Teams VDI Plugin can also be installed through Client App Management. For more information, see Client App Management.

> **Note:**
>
> - Third-party components are fetched from respective third-party CDNs rather than packaged with Citrix Workspace app. Customers must ensure necessary network access from endpoints for successful component installation on both online and offline Citrix Workspace app packages.
> - Third-party component installation failure does not impact Citrix Workspace app installation.
> - Failed components can be reinstalled by re-running the installer or configuring the installation via Client app management or via Virtual channel plugin manager. It can also be installed during a future upgrade.
> - Citrix Workspace app does not manage uninstall of third-party plugins when uninstalling

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

Citrix Workspace app.

- Citrix Workspace app preserves component selections across updates. For example, the Microsoft Teams plugin cannot be deselected during installation if it was already present on the system as a leftover from manual installation.
- Citrix recommends enabling Citrix Workspace app auto-updates to receive the latest versions of third-party components as they become available in the future.
- *These Plug-in(s) are third party software and are not created, developed or managed by Cloud Software Group. Cloud Software Group has no obligations or liability for any third party services or software. By downloading and/or utilizing such software, YOU HEREBY ACKNOWLEDGE AND AGREE THAT SUCH SOFTWARE IS PROVIDED BY CLOUD SOFTWARE GROUP ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, AS AVAILABLE, AND YOUR ACCESS TO AND/OR USE OF THE SOFTWARE OR ANY RELATED ASSETS IS AT YOUR SOLE RISK. You acknowledge that you are governed by such software's respective third party license(s).*

Audio Quality Enhancer for reliable transport

Technical Preview from 2508 version	Feedback form

Starting with version 2508, audio quality enhancer is also available for connections over reliable transport (i.e. TCP and EDT-Reliable). Under poor network conditions, both audio playback and recording will have a smoother experience with reduced latency.

To enable and disable this feature, see Audio quality enhancer for Mac VDA.

Note:

- Adaptive audio must be enabled for this feature to work.
- This feature is disabled by default in Tech Preview (over reliable transport).
- This feature must be enabled on both VDA and CWA.
- This feature is supported with Mac VDA version 2507 and later.

Enhancing hybrid mode support with GACS for cloud stores

Technical Preview from 2503 version	Feedback form

Starting with version 2503, Citrix Workspace app for Mac supports Global App Configuration service (GACS) in Hybrid mode for Cloud stores, leveraging the Citrix workspace launcher. This allows administrators to configure GACS settings through stores added using the browser, streamlining the management of client experiences. By, default, this feature is disabled. This feature is a request-only preview.

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

To get it enabled in your environment, fill out the Google form.
For more information, see GACS supports hybrid launch.

Support for single sign-on to Citrix Secure Access automatically through Citrix Workspace app

Technical Preview from 2402 version	Feedback form

Citrix Workspace app for Mac now automatically supports single sign-on (SSO) to Citrix Secure Access once your login to Citrix Workspace app. If you have both the Citrix Secure Access agent and the Citrix Workspace app installed on your device, this feature allows you to automatically sign in to Citrix Secure Access through SSO when you login to Citrix Workspace app. For more information, see Automatic single sign-on (SSO) to Citrix Secure Access through Citrix Workspace app - Preview in the NetScaler documentation.

To enable this feature through MDM, the administrator must use the following settings:

`<key>EnableSecureAccessAutoLogin</key><true/>`

> **Note:**
>
> - You need to use Citrix Secure Access version 24.03.1 or later to enable this feature.
> - This feature is supported only on cloud stores and not for on-premises stores.

Customizing the text in the Save Energy screen To use the sustainability feature with a custom message, modify the Delivery Group on the DDC with the following configuration example:

1. Follow the steps in 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`**.
5. Click **OK**.

Default behavior:

- `ICA-LogOffOnClose`: Default is **`false`**, showing the standard disconnect experience.
- `ICA-Title`: Default is `Log out or disconnect?`.
- `ICA-PromptMessage`: Default is `Logging out consumes less energy, but any unsaved changes will be lost. Save your work before logging out`.
- `ICA-Icon`: Default is **`true`**, displaying the green leaf icon when sustainability is enabled.

Customization rules:

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

- **Default Behavior with `ICA-LogOffOnClose=true`**: If no additional keywords are specified, the sustainability feature is enabled with the default title, body text, and green leaf icon.
- **Customization with Keywords**: When `ICA-LogOffOnClose=true` and specific keywords are provided, the sustainability feature is enabled with the specified customizations:
  - `ICA-PromptMessage`: Custom body text (limited to 200 characters).
  - `ICA-Title`: Custom title (limited to 30 characters).
  - `ICA-Icon=false`: Hides the green leaf icon.

Example - Custom configuration:

```
ICA-LogOffOnClose=true
ICA-PromptMessage=`This is a sample custom message.`
ICA-Title="Custom Logout"
ICA-Icon=false
```

The custom message and title is displayed, and the green leaf icon is hidden.

Support for Citrix Secure Private Access for on-premises deployments

Technical Preview from 2309 version	Feedback form

Starting with the 2309 version, Citrix Workspace app for Mac supports Citrix Secure Private Access for on-premises deployments. For more information, see Secure Private Access for on-premises - Preview.

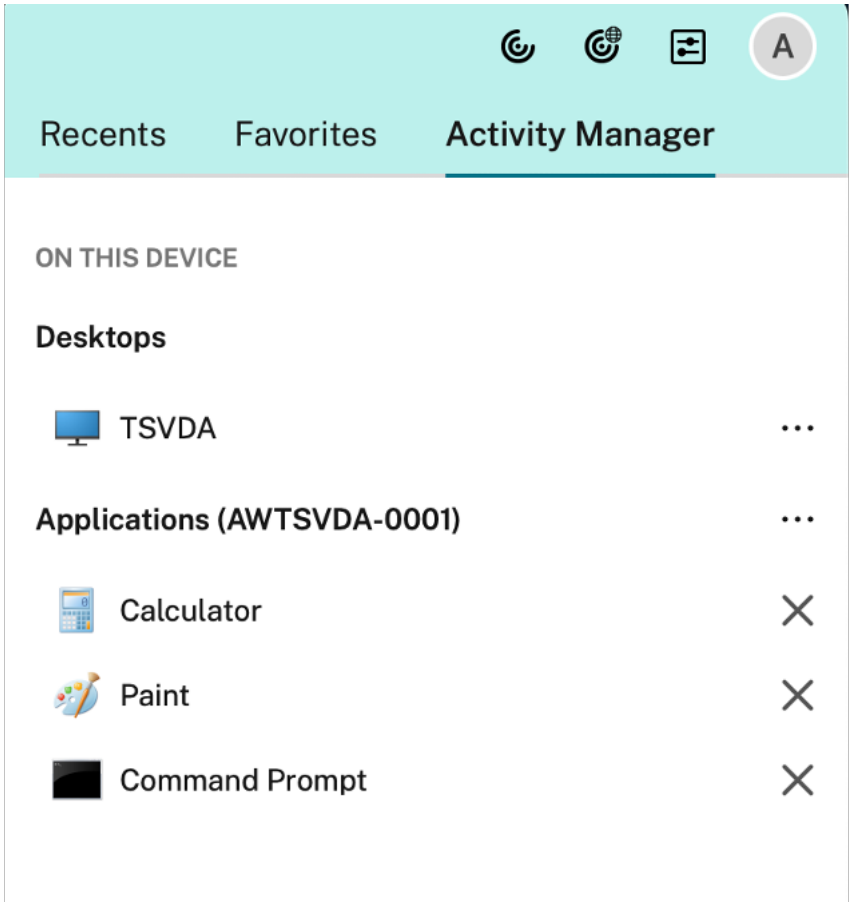
Support for Activity Manager on cloud stores

Technical Preview from 2308 version	Feedback form

Citrix Workspace app for Mac supports the Activity Manager feature. This feature lets end users view and interact with all their active apps and desktop sessions at one place. You can disconnect or terminate the active sessions directly from the Activity Manager.

To view active sessions in the **Activity Manager**, select the Citrix Workspace app icon from the menu bar and then click **Activity Manager**. To disconnect active desktop sessions, select the respective ellipsis **(...)** menu and click **Disconnect**. Click the "X"button to terminate the active app session. For more information, see Activity manager.

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



Single sign-on to Citrix Secure Access using Citrix Workspace app

You can single sign-on to Citrix Secure Access if you have already signed in to Citrix Workspace app. When you sign in to Citrix Workspace app and open Citrix Secure Access, you are not asked to authenticate by entering the credentials. It automatically proceeds with the authentication. This feature provides users with a seamless experience by allowing single sign-on to different Citrix applications. This feature is available only for customers on cloud stores. Along with the latest version of Citrix Workspace app, you must have a compatible version of Citrix Secure Access (22.12.2 and later versions).

Technical Preview to General Availability (GA)

Service or feature	General availability version
Support for PassKey (FIDO2) authentication	2603
Seamless application accessibility mirroring	2603
Improved session reconnection experience	2603

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

Service or feature	General availability version
Enhanced seamless app experience	2511.1
Keyboard accessibility support for the toolbar on the Virtual Desktop	2505
Support for sharing system audio on Microsoft teams	2503
Enhanced Multi-Monitor Management for desktop sessions	2503
USB Redirection of mass storage devices	2503
HDX™ direct V2 for non-shield scenario	2503
Enable Audio Quality Enhancer to improve audio performance	2503
Support for browser content redirection	2411.10
HDX Direct	2411
Support for Plug and play webcam redirection	2411
Client App Management	2409
Support for Rapid Scan client drive mapping	2409
Enhanced Desktop Viewer toolbar	2409
Enhancements to the smart card reader authentication	2409
Support for managing composite USB device redirection using DDC policies	2409
Support for Mac VoiceOver on the virtual desktop and seamless app sessions	2409
Support for HTML format on the Citrix Workspace app for Mac clipboard	2409
Support for YUV444 color format	2409
Customize the Desktop Viewer toolbar	2409
Connection strength indicator	2409
Sustainability initiative from Citrix Workspace app	2409
Support for multiple webcam resolutions	2409
Enhanced the High DPI option	2405
Store-based configuration of file access	2405

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

Service or feature	General availability version
Support for Activity Manager on the quick access menu for cloud stores	2405
Support for extending the desktop session to external monitors automatically	2405
Upgraded HDX Reducer to Version 4	2402
Loss tolerant mode for audio	2402
Support for Audio volume synchronization	2402
Support for background blur for webcam	2402
Support for screen sharing when App protection is enabled	2402
Support for authentication using FIDO2 when connecting to on-premises store	2311
Enhanced virtual apps and desktops launch experience for Workspace (Cloud users only)	2311
Improved graphics performance	2308
Increase in the number of supported virtual channels	2308

Citrix Workspace app for Mac 2611 - Preview

Citrix Workspace app for Mac 2611 - Preview is coming soon. Look forward to the new features and resolved issues in the upcoming release.

The generally available version of Citrix Workspace app for Mac is 2609. For more information on the current release, see About this release.

System requirements and compatibility

Supported operating systems

Citrix Workspace app for Mac supports the following operating systems:

- macOS Golden Gate 27
- macOS Tahoe 26 (up to 26.7)

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

- macOS Sequoia 15
- macOS Sonoma 14

At any point in time, Citrix® supports only the latest and the previous two macOS operating systems (N, N-1, and N-2) only.

Compatible Citrix products

Citrix Workspace app is compatible with all the currently supported versions of Citrix Virtual Apps and Desktops, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), and Citrix Gateway as listed in the Citrix Product Lifecycle Matrix.

Compatible browsers

Citrix Workspace app for Mac is compatible with the following browsers:

- Google Chrome
- Microsoft Edge
- Safari

Hardware requirements

- 2 GB of free disk space
- A working network or Internet connection to connect to servers

Connections, Certificates, and Authentication

Connections

Citrix Workspace app for Mac supports the following connections to Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service):

- HTTPS
- ICA-over-TLS
- ICA-over-DTLS

Citrix Workspace app for Mac supports the following configurations:

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

For LAN connections	For secure remote or local connections
StoreFront using StoreFront services or Citrix Receiver for website;	Citrix Gateway 12.x-13.x, including VPX

Certificates

> **Important:**
>
> If you're running macOS 10.15, ensure that your system is compliant with Apple's requirements for trusted certificates in macOS 10.15. Perform this check before you upgrade to Citrix Workspace app for Mac version 2106.

Private (Self-signed) certificates If a private certificate is installed on the remote gateway, you must install the root certificate for the organization's certificate authority on the user device. Then, you can successfully access Citrix resources using Citrix Workspace app for Mac.

> **Note:**
>
> When the remote gateway's certificate can't be verified upon connection, an untrusted certificate warning appears, as the root certificate isn't included in the local keystore. When a user continues to add a store, the store addition fails. However, on the web browser, the user might be able to authenticate to the store but connections to sessions fail.

Importing root certificates for devices

Obtain the certificate issuer's root certificate and email it to an account configured on your device. When clicking the attachment, you're asked to import the root certificate.

Wildcard certificates Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app for Mac supports wildcard certificates.

Intermediate certificates with Citrix Gateway If your certificate chain includes an intermediate certificate, the intermediate certificate must be mapped to the Citrix Gateway server certificate. For information on this task, see Citrix Gateway documentation. For more information about installing, linking, and updating certificates, see How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway.

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

Server Certificate Validation Policy Citrix Workspace app for Mac has a stricter validation policy for server certificates.

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

When validating a server certificate, Citrix Workspace app for Mac uses **all** the certificates supplied by the server (or gateway). Citrix Workspace app for Mac then checks whether the certificates are trusted. If none of the certificates are trusted, the connection fails.

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

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

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

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

> **Important**
>
> Some certificate authorities have more than one root certificate. If you require this stricter validation, ensure that your configuration uses the appropriate root certificate. For example, there are currently two certificates ("DigiCert/GTE CyberTrust Global Root", and "DigiCert Baltimore Root/Baltimore CyberTrust Root") that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available ("DigiCert Baltimore Root/Baltimore CyberTrust Root"). If you configure "GTE CyberTrust Global Root"at the gateway, Citrix Workspace app for Mac connections on those user devices fail. Consult the certificate authority's documentation to determine which root certificate must be used. Root certificates eventually expire, as do all certificates.
>
> **Note:**

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

> Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

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

- "Example Server Certificate"
- "Example Intermediate Certificate"

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

Now suppose that a gateway is configured with these certificates:

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

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

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

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

> **Important**
>
> Some certificate authorities use a cross-signed intermediate certificate, intended for situations when there's more than one root certificate. An earlier root certificate is still in use at the same time as a later root certificate. In this case, there are at least two intermediate certificates. For example, the earlier root certificate "Class 3 Public Primary Certification Authority"has the corresponding cross-signed intermediate certificate "Verisign Class 3 Public Primary Certification Authority - G5."However, a corresponding later root certificate "Verisign Class 3 Public Primary Certification Authority - G5"is also available, which replaces "Class 3 Public Primary Certification Authority."The later root certificate does not use a cross-signed intermediate certificate.
>
> **Note**
>
> The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By).

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

> This difference in name distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such "Example Intermediate Certificate 2").

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

- "Example Server Certificate"
- "Example Intermediate Certificate"

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

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

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

- "Example Server Certificate"

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

Authentication

For connections to StoreFront, Citrix Workspace app for Mac supports the following authentication methods:

Authentication method	Workspace for Web using browsers	StoreFront Services site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes		
Domain	Yes	Yes	Yes*	Yes*
Domain pass-through				
Security token			Yes*	Yes*
Two-factor authentication (domain with security token)			Yes*	Yes*

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

Authentication method	Workspace for Web using browsers	StoreFront Services site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
SMS			Yes*	Yes*
Smart card	Yes	Yes	Yes*	Yes
User certificate			Yes	Yes (Citrix Gateway Plug-in)

*Available only for deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

Connectivity requirements

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.

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.

Enable traffic for feature flag management

From Citrix Workspace™ app version 2409 onwards:

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

> **Note:**
>
> Adding the preceding URL to the allow list is essential for optimal use of Citrix feature flags and is supported starting with version 2409 of the Citrix Workspace app for Mac.

Provision to disable feature flag management service through MDM tool You can disable the feature flag management service on Citrix Workspace app, irrespective of whether their users are inside or outside the organization's firewall. To disable, set the value for the **DisableFeatureFlag** setting to True.

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

This service is available for admins who manage Mac devices using the MDM tool.

> **Note:**
>
> Disabling the FeatureFlag requires the admin to restart the device for this setting to take effect.

For more information on how to use MDM, see Mobile Device Management.

Install, uninstall, and upgrade

Citrix Workspace app for Mac contains a single installation package and supports remote access through Citrix Gateway, and Secure Web Gateway.

You can install Citrix Workspace app for Mac in any of the following ways:

- From the Citrix® website
- Automatically from Workspace for Web
- Using an Electronic Software Distribution (ESD) tool.

By default, the Citrix Workspace app is installed in the **Applications** directory. The installation paths are as follows:

- Full install - `"/Applications/Citrix\ Workspace.app/"`
- Citrix Workspace app for Mac executable - `"/Applications/Citrix\ Workspace.app/Contents/MacOS/Citrix\ Workspace"`

Manual install

By a user from Citrix.com

As a first-time user, you can download Citrix Workspace app for Mac from Citrix.com or your own download site. You can then set up an account by entering an email address instead of a server URL. Citrix Workspace app for Mac determines the Citrix Gateway or StoreFront server associated with the email address. Then it prompts the user to log on and continue the installation. This feature is referred to as email-based account discovery.

> **Note:**
>
> A first-time user is a user who does not have Citrix Workspace app for Mac installed on their user device.

Email-based account discovery for a first-time user does not apply if you have downloaded from a location other than Citrix.com (such as a Citrix Receiver for website).

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

If your site requires the configuration of Citrix Workspace app for Mac, use an alternate deployment method.

Using an Electronic Software Distribution (ESD) tool

A first-time Citrix Workspace app for Mac user must enter a server URL to set up an account.

From Citrix Downloads page

You can install Citrix Workspace app for Mac from a network share, or directly on to the user device. You can install the app by downloading the file from the Citrix website at Downloads.

To install Citrix Workspace app for Mac:

1. Download the `.dmg` file for the version of Citrix Workspace app for Mac that you want to install from the Citrix website.
2. Open the downloaded file.
3. On the Introduction page, click **Continue**.
4. On the **License** page, click **Continue**.
5. Click **Agree** to accept the terms of the License Agreement.
6. On the **Installation Type** page, click **Install**.
7. On the **Add Account** page, select **Add Account** and then click **Continue**.
8. Enter the user name and password of an administrator on the local device.

Using the terminal command

You can install Citrix Workspace app for Mac using the terminal commands.

To install Citrix Workspace app for Mac:

1. Download the `.dmg` file for the version of Citrix Workspace app for Mac that you want to install from the Downloads page.
2. Open the downloaded `CitrixWorkspaceApp.dmg` file.
3. Drag the `Install Citrix Workspace.pkg` file into the folder.
4. Open the terminal app.
5. Run the following command in the terminal:

```
sudo installer -pkg <path_to_package>/<package_name>.pkg -target /
```

6. Enter the Administrator password, if prompted.
7. After running the command, Citrix Workspace app is successfully installed.

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

Uninstall

Using the bin

You can now simply drag or move the Citrix Workspace app icon into the bin to completely uninstall the Citrix Workspace app for Mac.

To uninstall the Citrix Workspace app, do the following:

1. Close the Citrix Workspace app, if it's running.
   To close the Citrix Workspace app, use one of the following methods:
   - From the menu bar, click **Citrix Workspace™** and then **Quit Citrix Workspace**,
   - From the dock, right click on the Citrix Workspace app and select **Quit** from the options,
   - Press the **Command-Q** keys, or
   - From the Quick Access menu, click the **Account** icon and then **Quit**.

   > **Note:**
   >
   > If you don't close the Citrix Workspace app as per the preceding steps, you might get the following error message after performing the next step:
   >
   > *The item ''Citrix Workspace''can't be moved to the Trash because it's open*.

2. Drag the Citrix Workspace app from the **Application** folder to the bin.
   Alternatively, you can right-click the Citrix Workspace app and select **Options** > **Move to Bin**.
3. Provide your system credentials when prompted.
4. Close all running apps (Citrix Workspace) and click **Continue** to confirm.
   The Citrix Workspace app and all its system files are deleted from your device.

Enhancements on quit menu of Citrix Workspace app Starting with the 2402.10 version, Citrix Workspace app improves quit functionality and matches with Apple's Quit menu behavior. When you exit the Citrix Workspace app using the quit option, the app no longer runs in the background. With this feature, you can conserve battery life and optimize system performance.

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

- Quit from the menu bar,
- Quit from the dock,
- Quit from the Quick Access menu, or
- Press the Command-Q keys.

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

Using the .dmg file

You can also uninstall Citrix Workspace app for Mac manually by opening the .dmg file. Select **Uninstall Citrix Workspace App** and follow the on-screen instructions. The .dmg file is the file that is downloaded from Citrix when installing Citrix Workspace app for Mac for the first time. If the file is no longer on your computer, download the file again from Citrix Downloads to uninstall the application.

Using the terminal command

You can uninstall Citrix Workspace app for Mac using the terminal commands.

To uninstall Citrix Workspace app for Mac:

1. Open the terminal app.
2. Run the following command in the terminal:

```
sudo /Library/Application\ Support/Citrix\ Receiver/Uninstall\
   Citrix\ Workspace.app/Contents/MacOS/Uninstall\ Citrix\
   Workspace --nogui
```

3. After running the command, Citrix Workspace app and all its system files are deleted from your device.

Upgrade

Citrix Workspace app for Mac sends you notifications when there is an update available for an existing version or an upgrade to a newer version. For more information about automatic updates, see Automatic update.

You can upgrade Citrix Workspace app for Mac from any of the previous versions of Citrix Workspace app for Mac. For more information about updating the app manually, see Manual update.

When you upgrade to a newer version of Citrix Workspace app for Mac, the previous version is uninstalled automatically. You don't need to restart your machine.

Support for automatic installation of the End-Point Analysis (EPA) plug-in with Citrix Workspace app

Previously, users were required to manually download and install the End-Point Analysis (EPA) plug-in during the Citrix Workspace app login.

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

Starting from version 2405, Citrix Workspace app supports the automatic installation of the EPA plug-in during installation or updates. When you install or update Citrix Workspace app, the EPA plug-in is included by default. This enhancement eliminates the need for separately installing the EPA plug-in, resulting in a smoother experience during Citrix Workspace app setup.

Support for optionally installing Citrix Enterprise Browser™

Starting with version 2405, you have the flexibility to choose whether to install Citrix Enterprise Browser during the installation of the Citrix Workspace app for Mac. Additionally, if you've already installed Citrix Enterprise Browser with Citrix Workspace app, you can uninstall Citrix Enterprise Browser using the Global App Configuration service and Mobile Device Management (MDM). This feature allows administrators to maintain compliance by controlling whether Citrix Enterprise Browser is allowed for use on their managed devices.

Configuration

You can opt to install the Citrix Enterprise Browser using the Installer GUI and Command Line interface. If Citrix Enterprise Browser is already installed, then you can uninstall by pushing settings through the Global App Configuration service and MDM.

Install using the command line

- **Install Citrix Workspace app with Citrix Enterprise Browser**

To install Citrix Enterprise Browser during the Citrix Workspace app installation using the command line, run the following command:

```
sudo installer -pkg path_to_pkg -target / -verboseR
```

For example:

```
sudo installer -pkg /Volumes/Citrix\ Workspace/Install\ Citrix\
    Workspace.pkg -target / -verboseR
```

- **Install only Citrix Workspace app**

To opt out from installing Citrix Enterprise Browser during the Citrix Workspace installation using the command line, run the following command with the attached citrix_enterprise_browser_optedoutchoices.xml file:

```
sudo installer -applyChoiceChangesXML path_to_ChoiceChangesXML -pkg
    path_to_pkg -target /
```

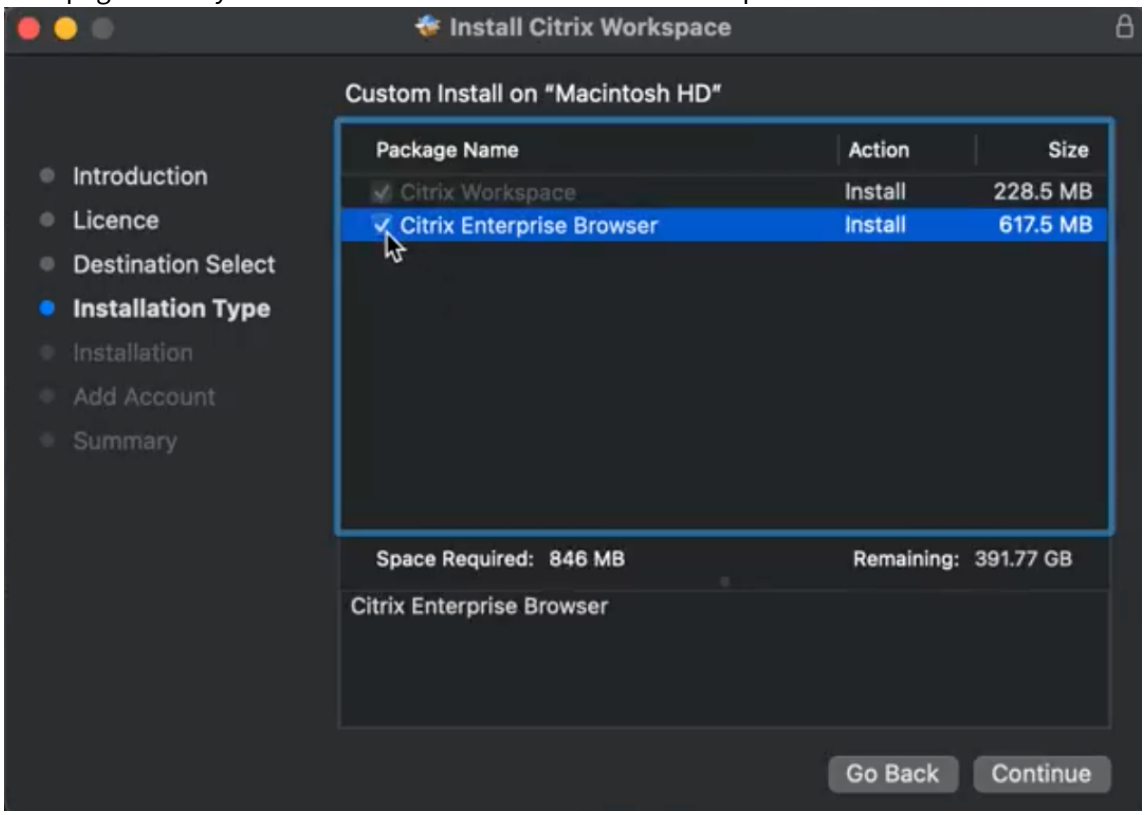
For example:

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

```
sudo installer -applyChoiceChangesXML ./
    citrix_enterprise_browser_optedoutchoices.xml -pkg /Volumes/Citrix\
    Workspace/Install\ Citrix\ Workspace.pkg -target /
```

Install using the installer GUI (Graphical User Interface)

1. During the installation of Install Citrix Workspace.pkg through the installer GUI, the **Custom Install** page allows you to choose whether to install Citrix Enterprise Browser or not.



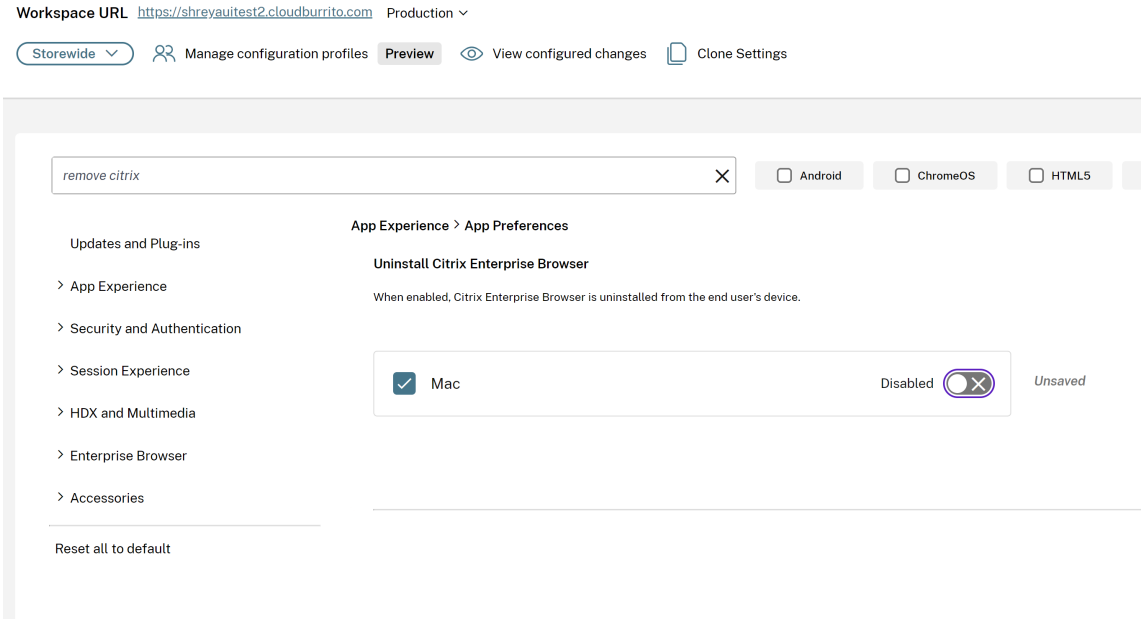
2. In the **Custom Install** page, do one of the following:
   - Select **Citrix Enterprise Browser** checkbox - In this case, both Citrix Workspace app and Citrix Enterprise Browser are installed.
   - Deselect **Citrix Enterprise Browser** checkbox - In this case, only Citrix Workspace app is installed.
3. If you deselect it, only Citrix Workspace app is installed.
4. If you select it, both Citrix Workspace app and Citrix Enterprise Browser are installed.
   For more information about the installation, see Manual install.

Uninstall using the Global App Configuration service

To uninstall the Citrix Enterprise Browser, do the following steps:

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

1. Go to Citrix Cloud and sign in with your Citrix Cloud credentials.
2. Navigate to **Workspace Configuration** > **App Configuration**.
3. From the list of configured store URLs, select the store for which you want to uninstall the Citrix Enterprise Browser and then click **Configure**.
4. Navigate to **App Experience > App Preferences**, select the **Mac** checkbox and toggle the button to **Enabled**. If enabled, then the Citrix Workspace Browser is uninstalled from the end user's device.



5. Click **Publish Drafts** to save the settings.

Uninstall Citrix Enterprise Browser using the Mobile Device Management

To uninstall the Citrix Enterprise Browser, run the following command:

```
<key>RemoveCitrixEnterpriseBrowser</key> <true/>
```

Updates and plugins management

This section describes the following:

- Updates
- Plugins management

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

Update

Version rollback support for auto update

Starting with version 2607, Citrix Workspace app for Mac supports administrator-initiated version rollback through the automatic update mechanism. When an administrator needs to reverse a problematic update, Citrix Workspace app can move the device back to an earlier, stable version using the same quiet, side-by-side mechanism as a normal automatic update.

The earlier version installs in the background while you continue working. If a session is active, you are prompted to **Restart now** or choose **Later**. If you select **Later**, the rollback is applied automatically when you are idle or after a time period configured by your administrator. Your preferences from the earlier version are restored automatically and your store is added back.

> **Note:**
>
> - Because version 2607 is the earliest release that supports rollback, administrators can begin using the rollback capability starting with version 2607.10 and above. As a result, version 2607 will remain the earliest version to which future releases can be rolled back to.
> - If a version newer than the configured rollback source is available, Citrix Workspace app updates forward instead of rolling back, ensuring you are never moved to an older version unnecessarily.

Configuring rollback using MDM

Rollback is delivered through an MDM configuration profile using the macOS preference domain `com.citrix.receiver.nomas`. All values are strings.

MDM key	Type	Required	Default	Description
`AdminRollbackFromVersion`	String	Yes	—	Version to roll back from; evaluated only when the installed version matches this value. For example, `26.07.10.15`.

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

MDM key	Type	Required	Default	Description
AdminRollbackToVersion	String	Yes	—	Target version to roll back to; must exist in the update catalog. For example, 26.07.0.67.
AdminRollbackMaxTimeIntervalHours	String	No	24	Number of hours a rollback can be deferred during an active session before it is applied automatically. Set to 0 to disable forced rollback. For example, 4.

The following is an example of an MDM configuration profile using a Custom Settings payload for the domain com.citrix.receiver.nomas:

```
<key>AdminRollbackFromVersion</key><string>26.07.10.15</string>
<key>AdminRollbackToVersion</key><string>26.07.0.67</string>
<key>AdminRollbackMaxTimeIntervalHours</key><string>4</string>
```

> **Note:**
>
> Delivery of these settings through Global App Configuration Service (GACS) is planned but not yet available. MDM delivery is the only supported method at this time.

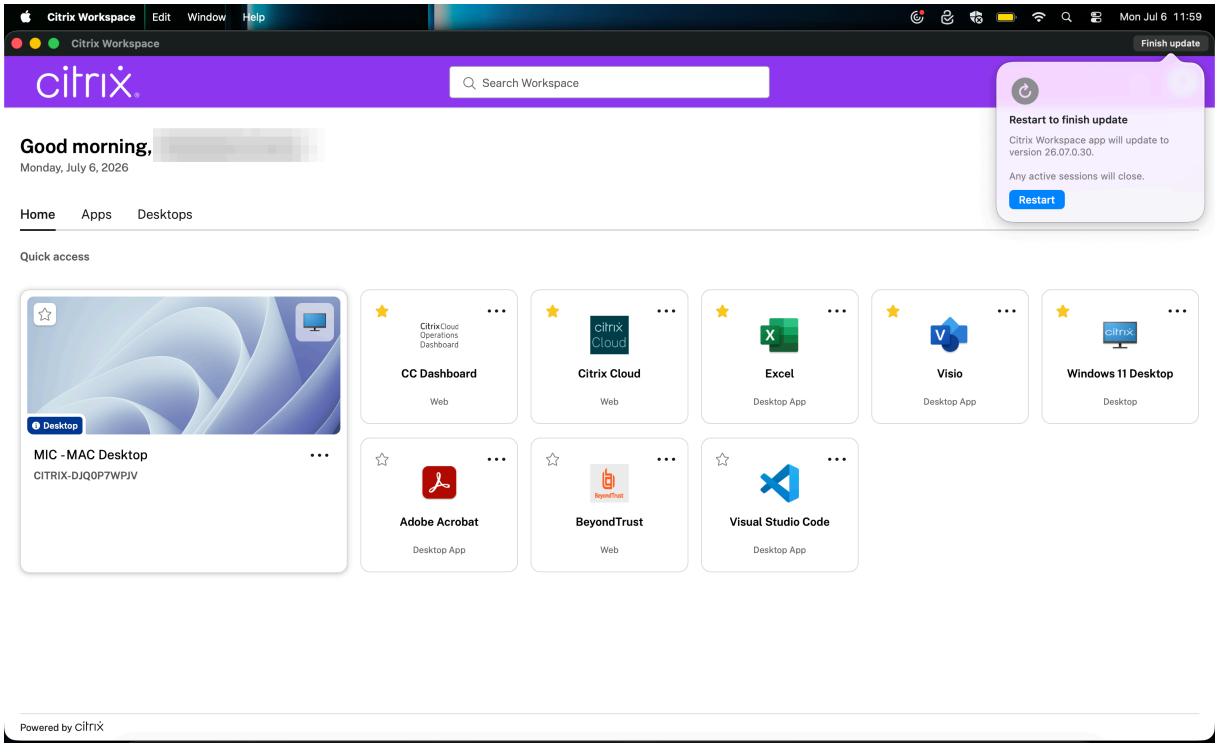
Data handling during rollback

- **User preferences**: The target version's preferences snapshot is restored only when that snapshot is available —that is, when the target version was the version used immediately before the current one. Otherwise, preferences are left unchanged.
- **Store**: The store is kept at its latest state and added back automatically after rollback.
- **Service and cache databases**: These are refreshed rather than reused from the earlier version.

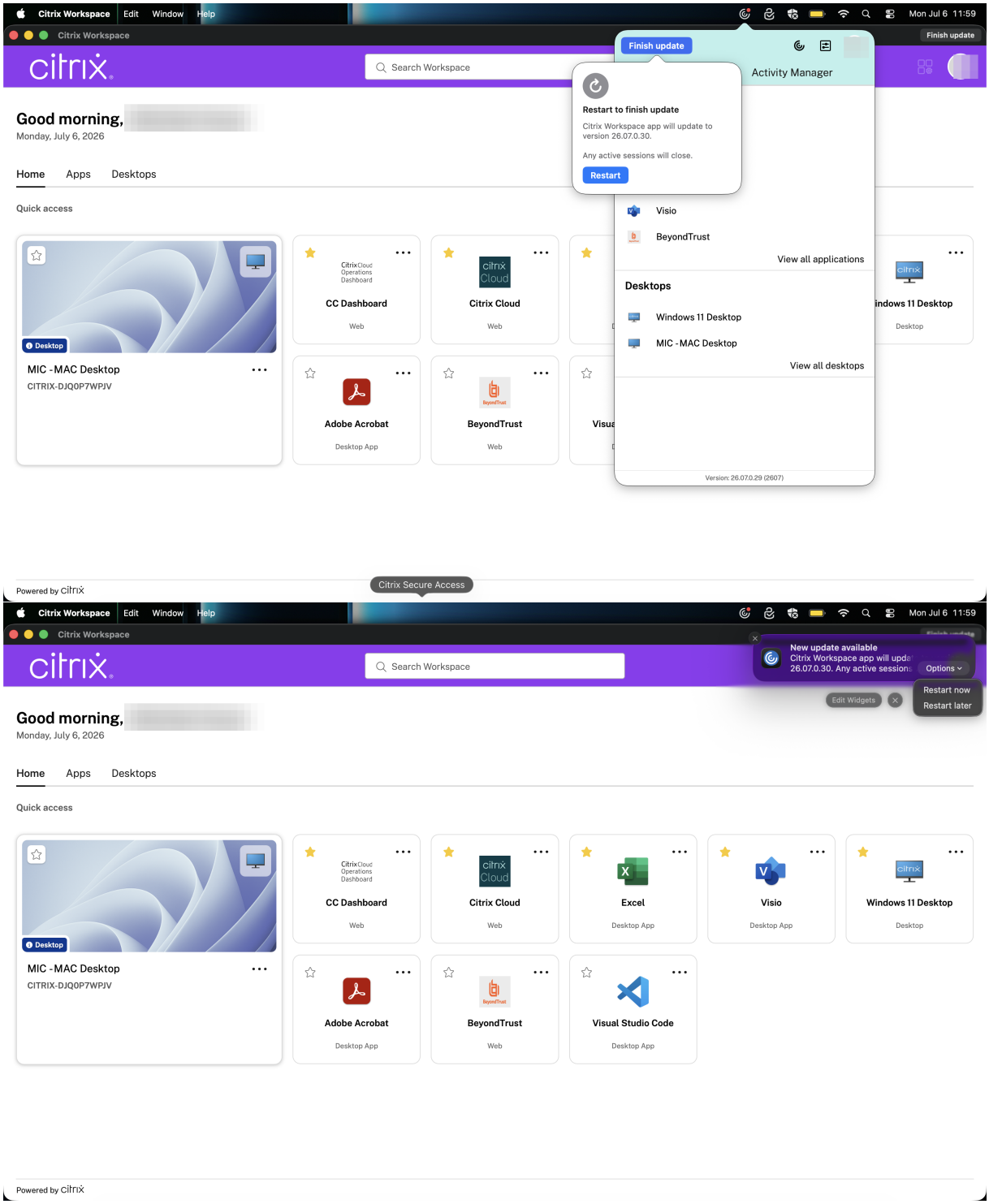
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Faster and less disruptive automatic updates (side-by-side silent update)

Starting with version 2607, Citrix Workspace app for Mac delivers a faster and less disruptive update experience. **This experience takes effect when updating from version 2607 to the next higher version.** Updates install silently in the background while you continue working, with no interruption to your running apps or active sessions. When the app is idle, the update completes automatically in seconds, with no action required. If you prefer to update on your own schedule, you can apply a ready update at any time from the **title bar**, the **Quick Access menu**, or the macOS **Notification Center**. Citrix Workspace app never closes a running app or active session to apply an update, and once completed, the previous version is removed automatically to free up disk space.



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



Support for auto-update scheduling

Starting with version 2411, admins can schedule auto-updates for the Citrix Workspace™ app during convenient hours. This capability allows them to determine the rollout period, minimizing disruption

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

to end-users and improving adoption of the auto-update service, which was previously controlled by Citrix.

End-users receive auto-updates for the Citrix Workspace app at a time scheduled by their admins, ensuring updates happen in a planned manner. Admins can control updates on macOS in the following ways:

- Admins can set the dates and time range for updates of the Citrix Workspace app for macOS.
- Scheduled updates set by customer admins take precedence over any rollout periods defined in the Citrix Catalog.

You can configure this feature using Mobile Device Management (MDM) and Global App Configuration service (GACS).

Using MDM:

```
<array>
 <dict>
  <key>AutoUpdateSchedulerSettings</key>
   <string>
   {

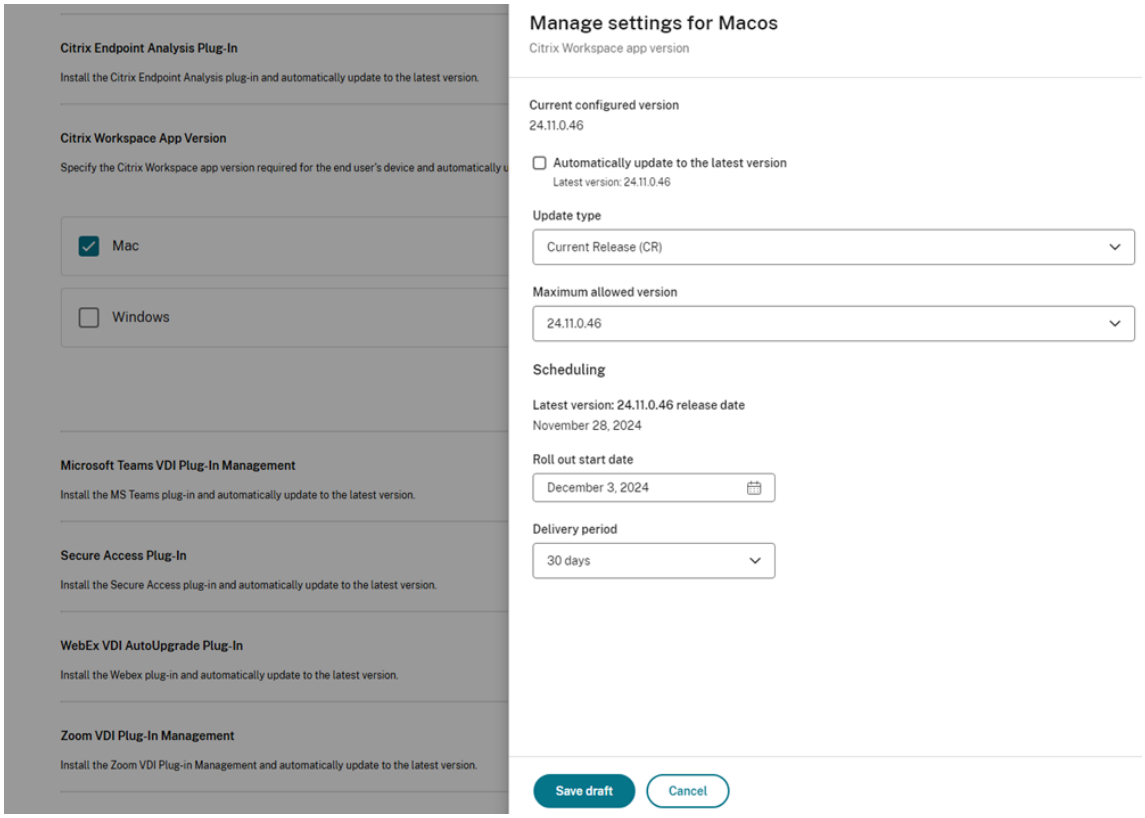
                    "startTime":"20:30",
                    "endTime":"23:30",
                    "deferCount":"4"
    }

   </string>
  <key>PayloadDisplayName</key>
   <string>Citrix Workspace #1</string>
  <key>PayloadIdentifier</key>
   <string>com.citrix.receiver.nomas</string>
  <key>PayloadType</key>
   <string>com.citrix.receiver.nomas</string>
  <key>PayloadUUID</key>
   <string>3BE38AD3-7D95-423F-BD7B-8A4D1F5208EF</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
 </dict>
</array>
```

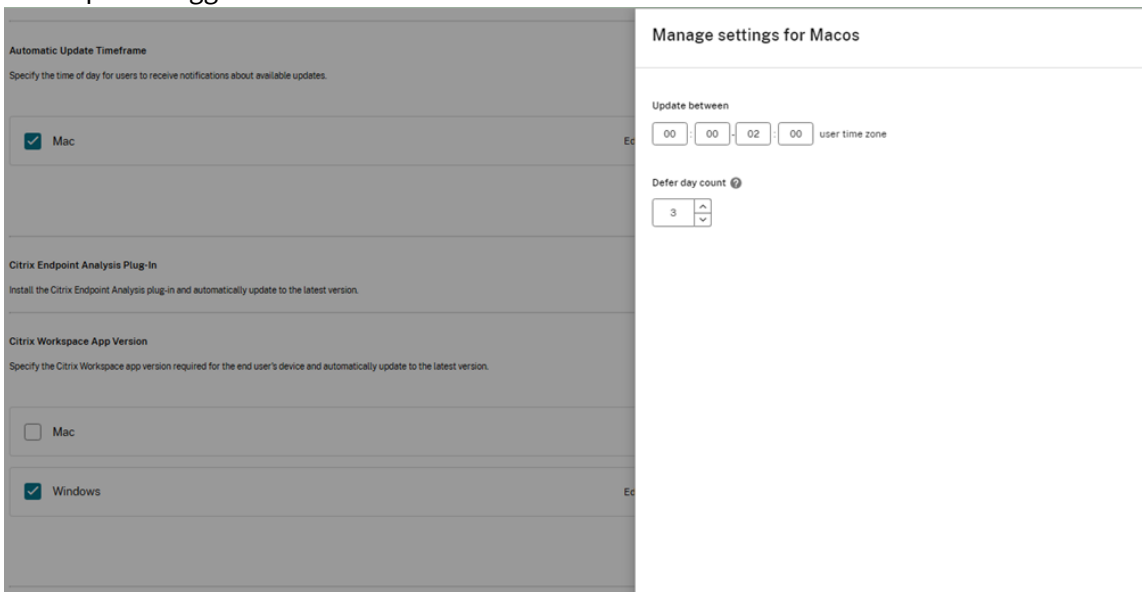
Using GACS:

1. Navigate to **Workspace Configuration** > **App Configuration** > **URL Configuration**.
2. Click **Citrix Workspace app version** and configure the desired settings.

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



3. Next, click **Automatic Update Timeframe** > **Edit** to define the time window within which auto-update trigger occurs.



4. Enter the required values. Defer day count specifies the number of times the end user can defer the auto-update.

For more information, see Automatic update timeframe.

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

Auto-update enhancement for active users

Starting with version 2411 of Citrix Workspace app for Mac, the auto-update feature was enhanced to trigger only for active users, ensuring that updates are available only for users with Global App Configuration service (GACS) or Mobile Device Management (MDM) policies, or those actively using the app. Building on this, version 2505 further refines the auto-update feature by introducing additional conditions for defining an **active user**. This enhancement provides more precise and controlled updates by applying the auto-update feature only to users who meet the updated activity criteria, offering greater flexibility and control over the update process.

A user is considered active if any of the following criteria is met:

- The user has launched at least one session (Desktop, Citrix Virtual app, or SaaS app).
- User is logged into the native Citrix Workspace application, allowing updates to be targeted to those actively engaging with the app.
- A Mobile Device Management (MDM) policy is configured for Auto-update Version Control, ensuring that devices in managed environments with specific update policies receive timely updates.
- The user is a managed user, with their system and profile controlled and maintained by an IT administrator, and has added a store with Global Application Configuration service (GACS) settings.

If none of these conditions are met, the user is considered inactive, and the auto-update feature is not available. When a user transitions from inactive to active status, the application triggers the auto-update feature, if applicable, ensuring the application is up-to-date.

Auto-update support for user groups

Starting with version 2411, customers can configure different app versions for different user groups through **Configuration Profile** in Global App Configuration Service (GACS). For more information, see Automatic update management settings supports configuration profiles.

Manual update

To manually update the Citrix Workspace app for Mac, download and install the latest version of the app from the Citrix Downloads page.

Automatic update

When a new version of the Citrix Workspace app releases, Citrix pushes the update on the system that has the Citrix Workspace app installed. You're notified of the available update.

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

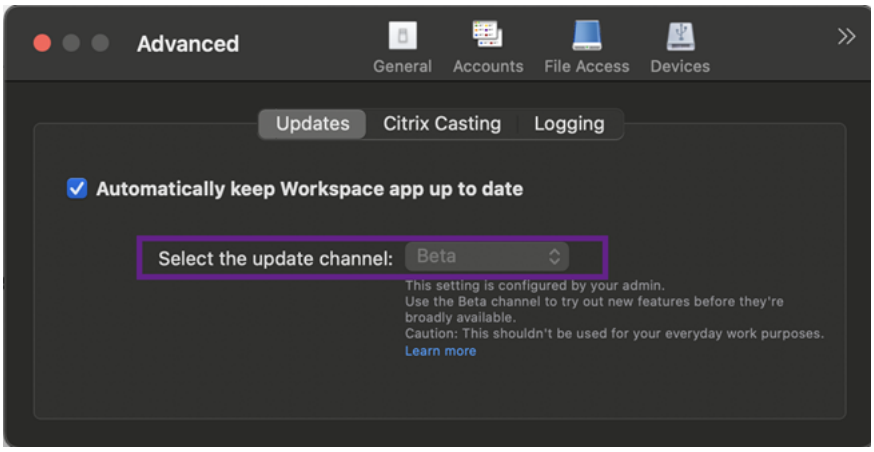
Note:

- If you've configured an SSL intercepting outbound proxy, add an exception to the Workspace auto-update server `https://downloadplugins.citrix.com/` to receive updates from Citrix.
- Auto-update isn't available for Citrix Workspace app versions earlier than 2301.1. For more information, see Knowledge Center article CTX491310.
- Your system must have an internet connection to receive updates.
- Workspace for web users can't download the StoreFront policy automatically.
- Citrix HDX RTME for macOS is included in Citrix Workspace Updates. You're notified of the available HDX RTME update on the Citrix Workspace app.
- Starting with Version 2111, Citrix Workspace updates log paths are modified. The Workspace updates logs are present at `/Library/Logs/Citrix Workspace Updater`. For information about collecting logs, see the Log collection section.

Support for restricting users to modify the update channel

Previously, users can modify the update channel to release or beta using the **Select the update channel** option available on the **Advanced** setting.

Starting with the 2409 version, the Citrix workspace app for Mac allows the admin to manage the **Select the update channel** option. With this feature, you have control over the update channel preference, ensuring that end users cannot modify it. This ensures that the update channel remains consistent and secure, as per your administrative settings.



You can configure this feature through the Global App Configuration service (GACS), Mobile Device Management (MDM), and the web.config file.

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

Using MDM

To push the auto-update for release or beta channels, administrators must use the following settings:

```
<key>AutoUpdateChannel</key><string>release</string>
```

0r

```
<key>AutoUpdateChannel</key><string>beta</string>
```

Using the web.config file

To push the auto-update for release or beta channels, do the following steps:

1. Use a text editor to open the web.config file, which is typically in the `C:\inetpub\ wwwroot \Citrix\Roaming` directory.
2. Locate the user account element in the file (Store is the account name of your deployment). For example: `<account id=... name="Store">`
3. Navigate to the properties of that user account and add the following properties before the </account> tag,:

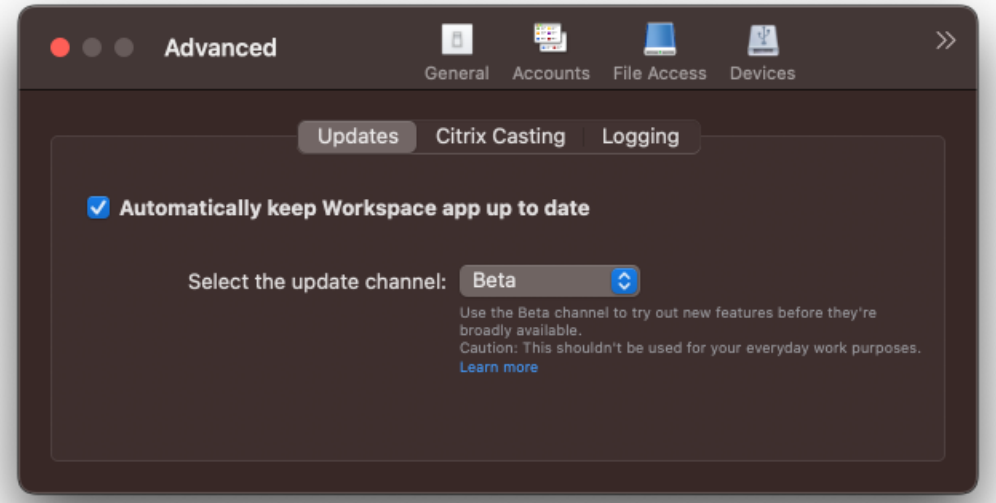
   ```
   <property name="autoUpdateChannel" value="release" />
   <property name="autoUpdateChannel" value="beta" />
   ```

Installing Citrix Workspace app Beta program

You receive an update notification when the Citrix Workspace app is configured for automatic updates. To install the Beta build on your system, perform the following steps:

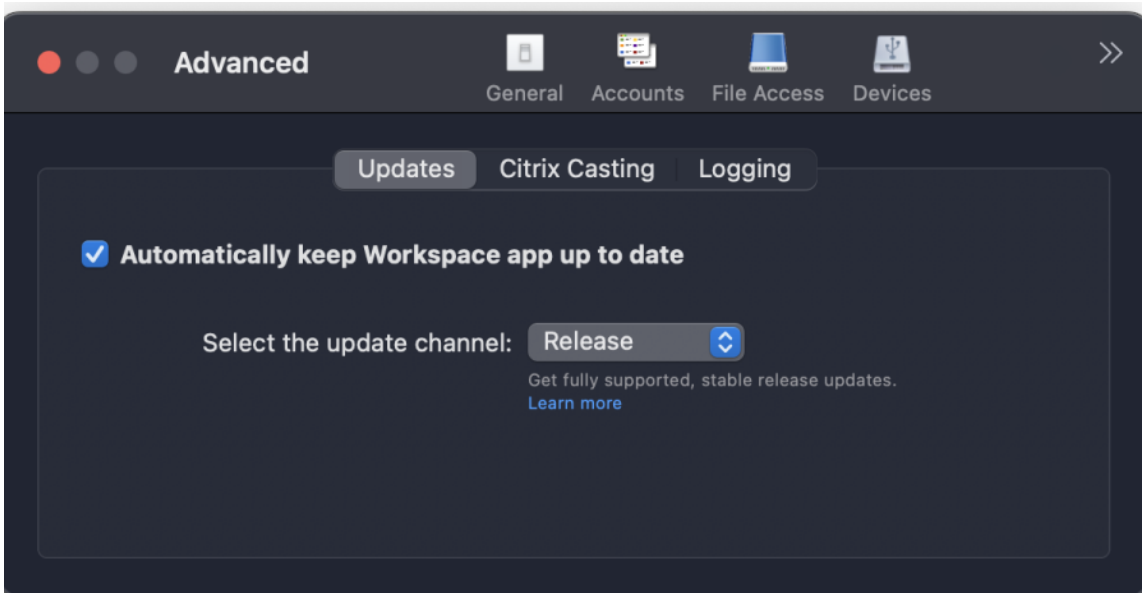
1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Beta** from the drop-down list, when the Beta build is available.

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



To switch from a Beta build to a Release build, perform the following steps:

1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Release** from the **Select the update channel** drop-down list.



> **Note:**
>
> Beta builds are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for beta builds but wel-

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

> comes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It's advised that you do not deploy Beta builds in production environments.

Auto-update version control

Administrators can now manage the auto-updated version of Citrix Workspace app for the devices in the organization.
Administrators can control the version by setting the range for maximumAllowedVersion and minimumAllowedVersion properties in the Global App Configuration service.

Example JSON file in Global App Configuration service:

```
{

  "serviceURL": {

    "url": "https://serviceURL:443"
   }
 ,
  "settings": {

    "name": "Version Control for Citrix Workspace",
    "description": "Provides admin ability to Version Control for
       Citrix Workspace",
    "useForAppConfig": true,
    "appSettings": {

      "macos": [
        {

          "category": "AutoUpdate",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [
            {

              "name": "Auto update plugins settings",
              "value": [
                {

                  "pluginName": "Citrix Workspace",
                  "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
                  "pluginSettings": {

                    "deploymentMode": "Update",
                    "upgradeToLatest": false,
                    "minimumAllowedVersion": "23.07.0.63",
                    "maximumAllowedVersion": "23.07.0.63",
```

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

```
38                      "delayGroup": "Medium",
39                      "detectRule": ""
40                    }
41
42                  }
43
44                ]
45               }
46
47             ]
48           }
49
50         ]
51       }
52
53     }
54
55   }
```

When the range is set, Citrix Workspace app on the user's device is automatically updated to the highest available version that falls between the mentioned range.

If you want to auto-update Citrix Workspace app to a specific version, enter the same version in the maximumAllowedVersion and minimumAllowedVersion properties in the Global App Configuration service.

> **Note:**
>
> - To enable auto-update version control, set the **upgradeToLatest** setting to false in the Global App Configuration service. If the **upgradeToLatest** setting is true, maximumAllowedVersion and minimumAllowedVersion is ignored.
> - Do not modify the pluginId. The pluginID is mapped to Citrix Workspace app.
> - If the administrator hasn't configured the version in the Global App Configuration service, Citrix Workspace app is updated to the latest available version by default.
> - You can only use the version ranges that are set to update Citrix Workspace app. However, a downgrade isn't supported.
> - This feature is supported from release 2307 onwards.

Improved auto-update experience

The auto-update feature automatically updates the Citrix Workspace app to the latest version without the need for any user intervention.

Citrix Workspace app periodically checks and downloads the latest available version of the app. Citrix Workspace app determines the best time to install based on user activity not to cause any disruptions.

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

Advanced configuration for automatic updates (Citrix Workspace Updates)

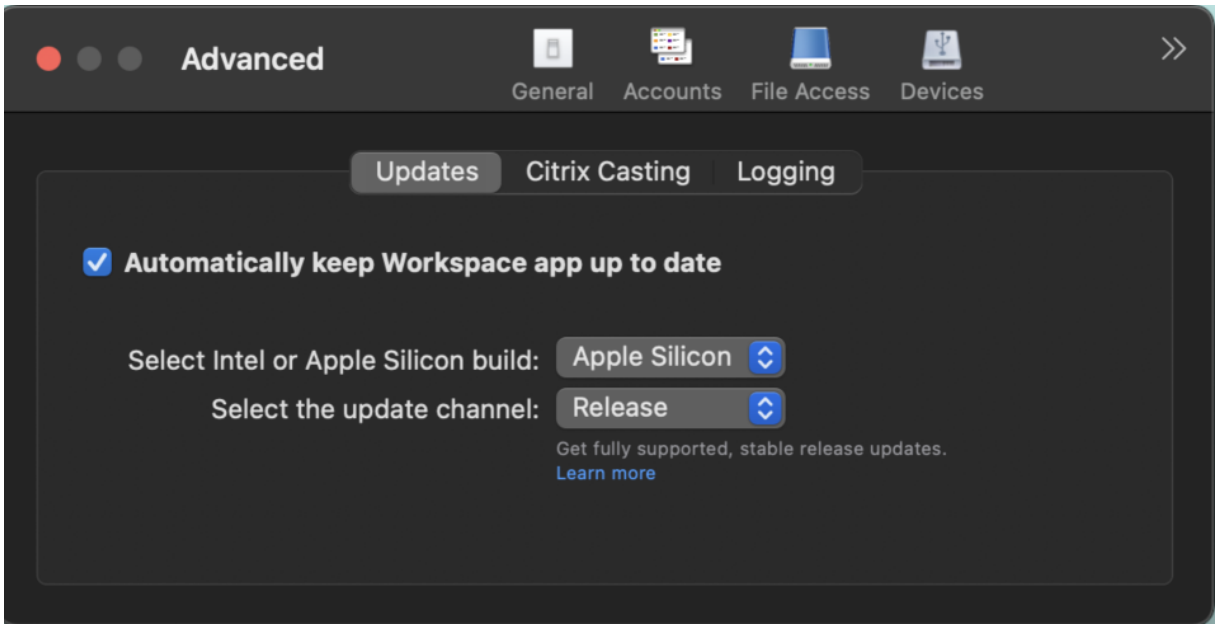
You can configure Citrix Workspace updates using the following methods:

- Graphical user interface (GUI)
- Global App Configuration service (GACS)
- Mobile Device Management (MDM)
- StoreFront

Configure Citrix Workspace automatic updates using the graphical user interface

Individual users can override the Citrix Workspace updates setting using the **Advanced** preferences dialog box, which is a per-user configuration and the settings apply only to the current user. To configure the update using the GUI, perform the following steps:

1. Select the Citrix Workspace app helper icon on your Mac.
2. From the drop-down list, select **Preferences > Advanced > Updates**.
3. Select the build for which you want to install the automatic updates. It can be either the Apple Silicon or Intel build (only applicable for users on Mac with Apple silicon (M1 Series).



Configure Citrix Workspace automatic updates using StoreFront

1. Use a text editor to open the `web.config` file, which is typically in the `C:\inetpub\wwwroot\Citrix\Roaming directory`.

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

2. Locate the user account element in the file (Store is the account name of your deployment).

   For example: <account id=... name="Store">

   Before the </account> tag, navigate to the properties of that user account:

```
<properties>
       <clear/>
 </properties>
```

3. Add the auto-update tag after the *<clear />* tag.

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
       F84Store"

      description="" published="true" updaterType="Citrix"
         remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>

            <properties>

              <property name="Auto-Update-Check" value="Disabled"
                 />

              <property name="Auto-Update-DeferUpdate-Count" value
                 ="1" />

              <property name="Auto-Update-Rollout-Priority" value=
                 "fast" />

              <property name="Auto-Update-Architecture" value="
```

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

```
                    Universal" or "Intel" />
38
39                      </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

The meaning of the properties and their possible values are detailed as follows:

- **Auto-Update-Check:** Indicates that Citrix Workspace app detects an update automatically when available.
  - Auto (default) –Checks and performs updates automatically
  - Manual –updates are only fetched when the user makes a check request from the Citrix Workspace app system tray menu,
  - Disabled –Updates checks aren't performed.
- **Auto-Update-Rollout-Priority:** Indicates the delivery period in which you can receive the update.
  - Fast –updates are rolled-out to the users towards the beginning of the delivery period.
  - Medium –updates are rolled-out towards the middle of the delivery period.
  - Slow–updates are rolled-out towards the end of the delivery period.

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

- **Auto-Update-DeferUpdate-Count:** Indicates the number of counts that you can defer the notifications for the updates.

  > **Note:**
  >
  > This configuration is applicable only for interactive updates and not when the silent auto-update feature is enabled, as the user doesn't get any option to defer the updates.

  - -1: The user can defer the auto-update any number of times.
  - 0: The user can't view the remind me later option.
  - number: The user can view remind later options with the given count.

Configure Citrix Workspace automatic updates using the GACS

Administrators can use GACS to configure the automatic updates to either Apple Silicon or Intel builds by using the following settings:

"name":"autoUpdateArchitecture"

"value":"Universal"or "Intel"

Configure Citrix Workspace automatic updates using the MDM

Administrators can use MDM to configure the automatic updates to either Apple Silicon or Intel builds by using the following settings:

```
<key>AutoUpdateArchitecture</key>
<string>Universal</string> or <string>Intel</string>
<key>AutoUpdateState</key>
<string>Auto</string> or <string>Manual</string> or <string>Disabled
</string>
```

For more information on how to use MDM, see Mobile Device Management.

Log collection

Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, provide support.

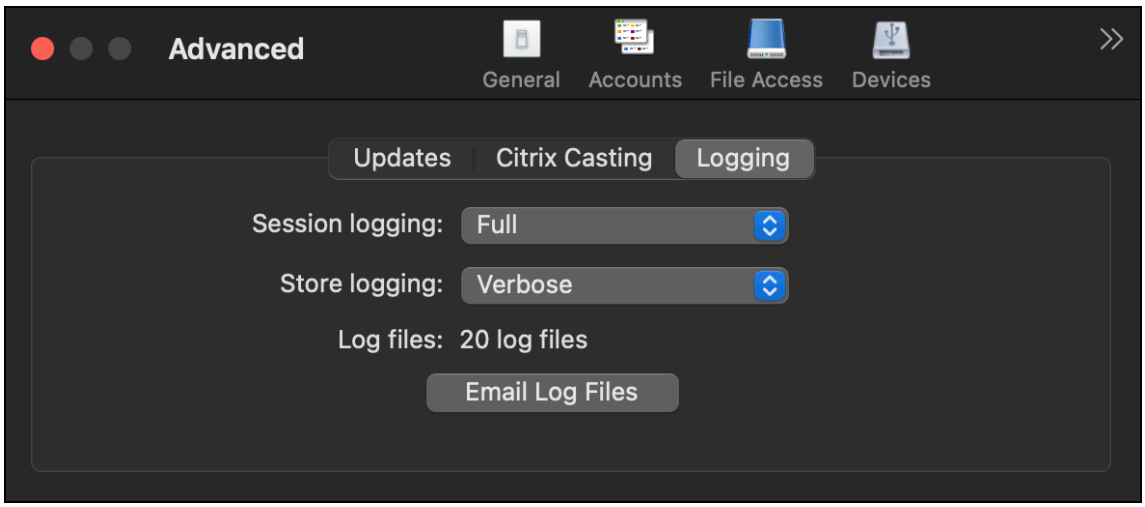
You can collect logs using the GUI.

Collecting logs:

1. Open Citrix Workspace app.

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

2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Logging**.



4. Select one of the following session log levels:

   - **Disabled (Default)**: Minimum logs are collected for basic troubleshooting.
   - **Connection Diagnostics**: Identifies errors while connecting. All logging is enabled up until the point when the session is deemed successful.
   - **Full**: Captures everything including the connection diagnostics. Once enabled, the Citrix Workspace app will store up to 10 session logs after which they're deleted starting with the oldest to maintain 10 logs.

   > **Note:**
   >
   > Selecting the **Full** logging option can impact performance and must be used only while troubleshooting an issue because of the amount of data. Do not enable full logging during normal use. Enabling this level of logging triggers a warning dialog that must be acknowledged for you to continue.

5. Select one of the following store log levels:

   - **Disabled (Default)**: Minimum logs are collected for basic troubleshooting.
   - **Normal**: Only store communication logs are collected.
   - **Verbose**: Detailed authentication and store communication logs are collected.

6. Click **Email Log Files** to collect and share logs as a .zip file.

Enhanced Universal Architecture builds for virtual apps and desktops session

From the 2311 version, the Universal Architecture build can now automatically choose to run the virtual sessions in the native Apple Silicon mode or Intel mode. It uses the Rosetta emulation to launch

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

the virtual session in Intel mode. The virtual session launches in the native Apple Silicon mode, if the virtual channel SDK is built based on the native Apple Silicon architecture or there's no virtual channel SDK. However, the virtual session launches in the Intel mode using the Rosetta emulation, if the virtual channel SDK is built based on the x86_64 Intel-based architecture.

This enhancement to the Universal Architecture build improves the launch experience on Macs with the Apple Silicon chipset. For users on Macs with the Intel-based chipset, there is no change, and the Universal Architecture build continues to run the virtual sessions natively.

Plug-ins management

Health checker tool for CAM and MDM Policy

Starting with version 2607, Citrix Workspace app for Mac includes a Health checker tool for CAM and MDM policy. When Citrix Client app management (CAM) policies do not take effect on Mac endpoints, diagnosing the cause has historically required collecting logs, running manual network tests, and comparing configuration files by hand —a process that requires intense effort and analysis.

The **Config Checker** tool now includes a dedicated **CAM health check**. In a single run, it actively verifies the full CAM delivery chain directly on the device:

- **Endpoint reachability**: Confirms the CAM discovery URL and service endpoint are reachable from the device.
- **Settings fetch**: Verifies whether store settings can be retrieved from the configured endpoint and, if not, identifies where in the chain the failure occurs.
- **Applied settings**: Displays the key-value pairs currently served by CAM for the device's domain.
- **Override detection**: Flags whether local user preferences or MDM profiles are overriding any CAM-delivered values.
- **Config comparison**: Compares the latest settings available from CAM against the settings currently stored on the device and highlights any differences.
- **Fetch timestamp**: Shows when the device last successfully retrieved CAM settings.
- **Report export**: Allows the results to be saved as a file for sharing with support or for auditing across a fleet.

To enable this feature, run the following command:

```
defaults write com.citrix.receiver.nomas EnableConfigChecker -bool YES
```

To enable this feature through GACS, use the following setting:

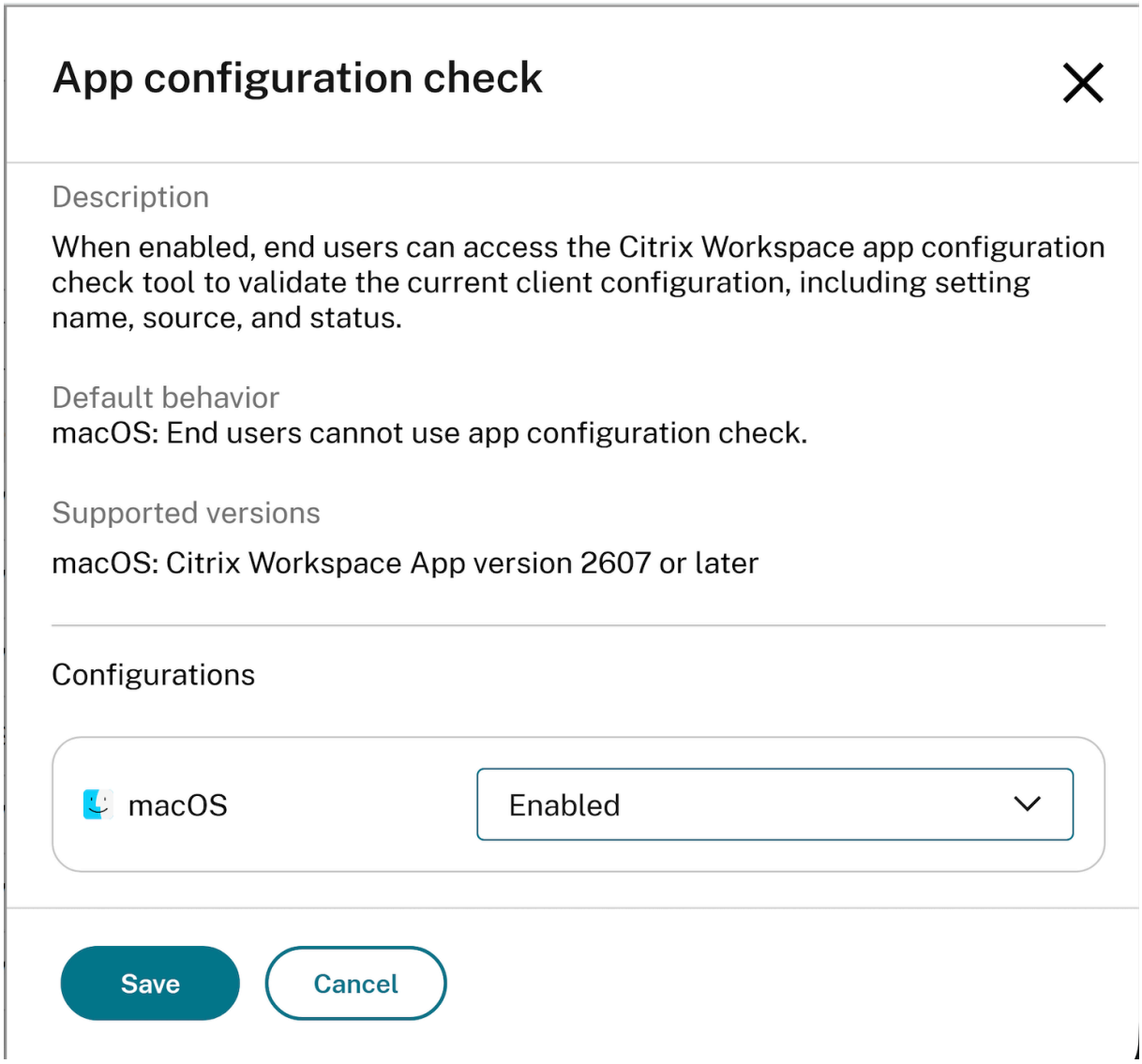
```
      "appSettings": {

        "macos": [
```

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

```
4            {
5
6              "assignedTo": [
7                "AllUsersNoAuthentication"
8              ],
9              "category": "root",
10             "settings": [
11               {
12
13                 "name": "enable config checker",
14                 "value": true
15                }
16
17             ],
18             "userOverride": false
19           }
20
21         ]
22       }
```

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



Support for automatic installation of deviceTRUST® plug-in with Citrix Workspace™ app

Starting with version 2503, Citrix Workspace app for Mac includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management. For more information, see deviceTRUST.

Version control using MDM and GACS

Starting with version 2411, administrators can configure Citrix Workspace version control and Client App Management using Mobile Device Management (MDM). This capability enables administrators

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

to manage the automatic updates of the Citrix Workspace app on devices within their organization. Administrators can control the version by setting the range for `maximumAllowedVersion` and `minimumAllowedVersion` properties in the Global App Configuration service.

For more information, see Auto-update version control.

To enable authentication through MDM, use the following settings:

```
<dict>
   <key>AutoUpdatePluginsSettings</key>
   <string>
       [
       {

         "pluginName": "Citrix Workspace",
         "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
         "pluginSettings": {

           "deploymentMode": "InstallAndUpdate",
           "upgradeToLatest": false,
           "minimumAllowedVersion": "24.02.10.24",
           "maximumAllowedVersion": "24.02.10.24",
           "delayGroup": "Medium"
          }

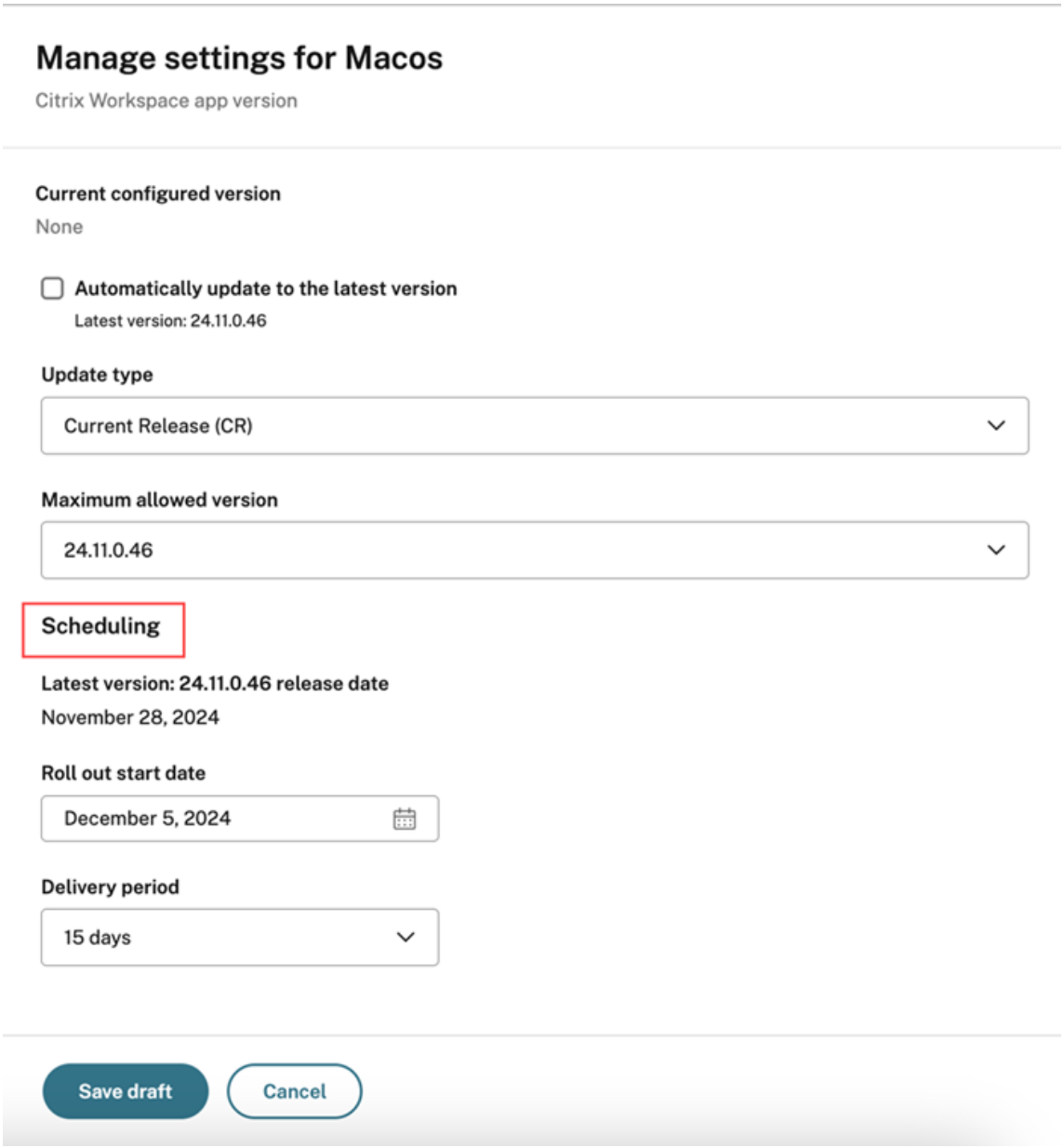
        }

     ]
   </string>
</dict>
```

To enable this feature through GACS, admins must follow these steps:

1. Navigate to **Workspace Configuration** > **App Configuration** > **Configure** in Citrix Cloud.
2. In **Citrix Workspace app** page, click **Citrix Workspace app version** and configure the desired settings.

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



For more information, see Citrix Workspace app version.

Client App Management using MDM

Client App Management allows administrators to install and manage agents like Citrix EndPoint Analysis (EPA) and Zoom VDI plug-ins from a single console.

Client App Management for Zoom VDI auto-update plug-in Administrators can control auto-update settings for Zoom VDI plug-ins on organization devices, ensuring seamless updates and enhanced security.

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

To configure Zoom VDI auto-update plug-in management through MDM, use the following settings:

```
<dict>
   <key>AutoUpdatePluginsSettings</key>
   <string>
   [
       {

           "pluginName": "Zoom VDI AutoUpgrade Plugin",
           "pluginId": "1A4BB471-022C-4C87-BDCD-0B64FB42869C",
           "pluginSettings": {

               "deploymentMode": "InstallAndUpdate",
               "upgradeToLatest": true,
               "ftu": true
            }

        }

   ]
   </string>
</dict>
```

For more information, see Client App Management for Zoom VDI plug-in.

Support for automatic installation of deviceTRUST® plug-in with Citrix Workspace™ app

Starting with version 2503, Citrix Workspace app for Mac includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management. For more information, see deviceTRUST.

Version control using MDM and GACS

Starting with version 2411, administrators can configure Citrix Workspace version control and Client App Management using Mobile Device Management (MDM). This capability enables administrators to manage the automatic updates of the Citrix Workspace app on devices within their organization. Administrators can control the version by setting the range for `maximumAllowedVersion` and `minimumAllowedVersion` properties in the Global App Configuration service.

For more information, see Auto-update version control.

To enable authentication through MDM, use the following settings:

```
<dict>
   <key>AutoUpdatePluginsSettings</key>
```

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

```
    <string>
        [
        {

          "pluginName": "Citrix Workspace",
          "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
          "pluginSettings": {

            "deploymentMode": "InstallAndUpdate",
            "upgradeToLatest": false,
            "minimumAllowedVersion": "24.02.10.24",
            "maximumAllowedVersion": "24.02.10.24",
            "delayGroup": "Medium"
           }

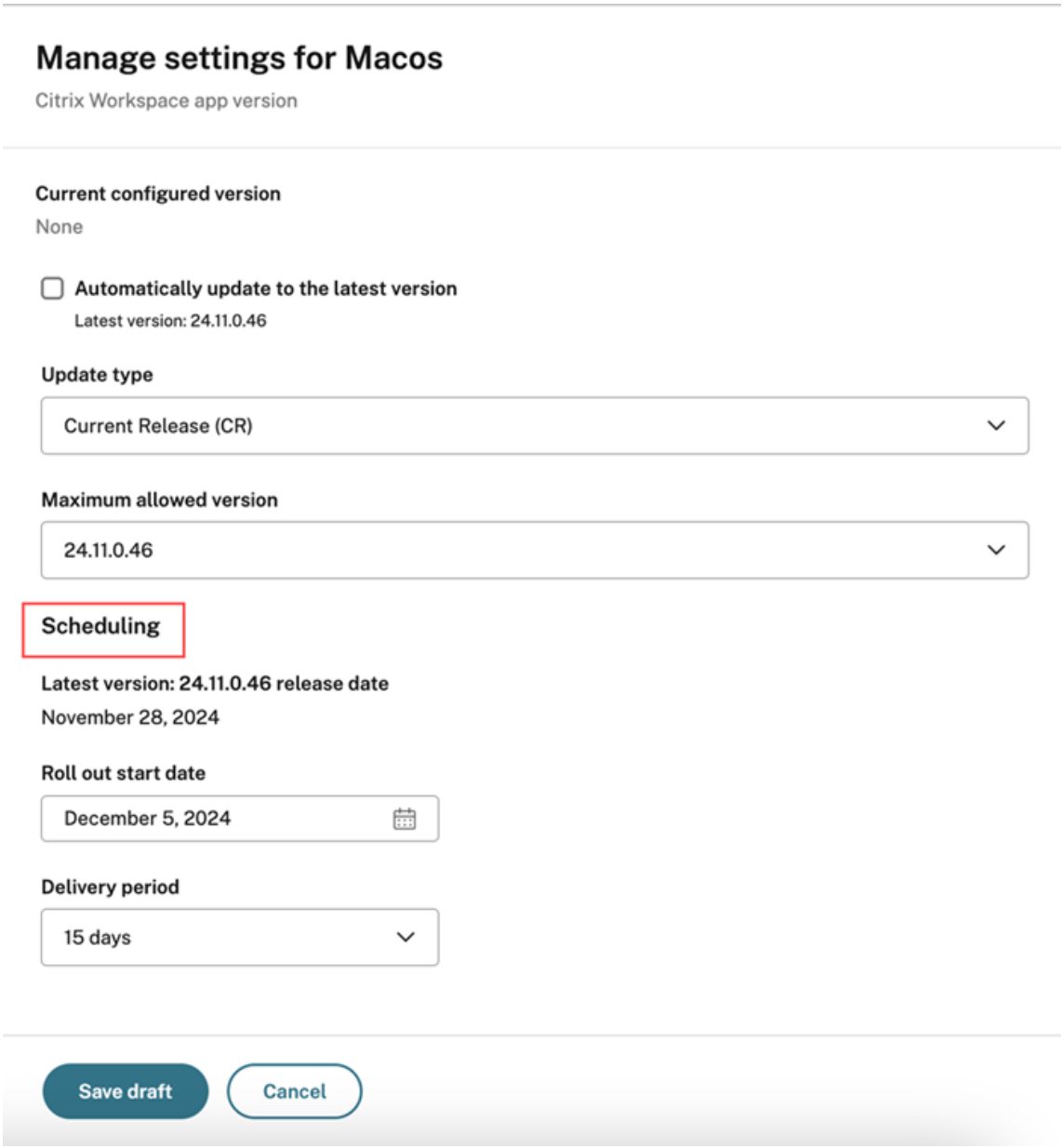
         }

      ]
    </string>
</dict>
```

To enable this feature through GACS, admins must follow these steps:

1. Navigate to **Workspace Configuration** > **App Configuration** > **Configure** in Citrix Cloud.
2. In **Citrix Workspace app** page, click **Citrix Workspace app version** and configure the desired settings.

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



For more information, see Citrix Workspace app version.

Client App Management using MDM

Client App Management allows administrators to install and manage agents like Citrix EndPoint Analysis (EPA) and Zoom VDI plug-ins from a single console.

Client App Management for Zoom VDI auto-update plug-in Administrators can control auto-update settings for Zoom VDI plug-ins on organization devices, ensuring seamless updates and enhanced security.

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

To configure Zoom VDI auto-update plug-in management through MDM, use the following settings:

```
<dict>
   <key>AutoUpdatePluginsSettings</key>
   <string>
   [
       {

           "pluginName": "Zoom VDI AutoUpgrade Plugin",
           "pluginId": "1A4BB471-022C-4C87-BDCD-0B64FB42869C",
           "pluginSettings": {

               "deploymentMode": "InstallAndUpdate",
               "upgradeToLatest": true,
               "ftu": true
            }

        }

   ]
   </string>
</dict>
```

For more information, see Client App Management for Zoom VDI plug-in.

Client App Management

Starting with version 2409, Citrix Workspace app for Mac offers Client App Management capability that makes the Citrix Workspace app a single client app required on the end point to install and manage agents such as Citrix EndPoint Analysis (EPA) and Zoom VDI plug-ins. With this feature, administrators can easily deploy and manage required agents from a single management console. You can configure this feature using the Global App Configuration service (GACS).

To configure Client App Management, do the following:

1. Administrators must specify the agents required on end users'devices in GACS.
2. Citrix Workspace app fetches the list of agents from GACS.
3. Based on the list fetched from GACS, Citrix Workspace app downloads the agent packages through the auto-update service. If the agent isn't previously installed on the end point, Citrix Workspace app triggers the installation of the agent. If the agent is already installed, Citrix Workspace app triggers an update to the agent (if the version of the downloaded agent is higher than the installed version.)

Citrix Workspace app ensures to automatically update the agents whenever an update is available in the future.

For more information about configuration, see Manage plug-ins using Global App Configuration service.

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

Client App Management for Zoom VDI plug-in

Starting with version 2409, you can now manage the Zoom VDI plug-in using the Client App Management capability. With this feature, you can download, install, and auto-update the Zoom VDI plug-in from Citrix Workspace app. For more information about configuration, see Zoom VDI Plug-in Management in the GACS documentation.

Configure Citrix Workspace app

You can configure Citrix Workspace app for Mac using Global App Configuration service User Interface (UI) and Mobile Device Management. Settings can be configured for both cloud (Citrix Workspace) and on-premises (Citrix StoreFront) environments.

For more information, see the following:

- Global App Configuration service
  - Configure settings for cloud stores
  - Configure settings for on-premises stores
- Mobile Device Management

Quit background processes with Quick Access menu

Starting with version 2503, Citrix Workspace™ app for Mac ensures that all background processes, including the Citrix Workspace Helper, quit when user exits the main application through the **Quick Access** menu. This enhancement addresses common concerns where certain apps, like Citrix Workspace Helper, remained active after users closed the main workspace application. To provide a better user experience, this functionality ensures that:

- When users select the **Quit** option from the **Quick Access** menu of the Citrix Workspace app, all associated background processes are closed.
- If the Citrix Workspace app is exited through other methods, such as **Command+Q** or quitting from the dock, the background processes remain running. This behavior ensures that necessary background functionalities remain operational unless explicitly exited.

Keyboard layout synchronization

Keyboard layout synchronization enables you to switch between the preferred keyboard layouts on the client device. For more information, see Keyboard layout synchronization.

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

Channel support for Global App Configuration service

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. Global App Configuration service now allows administrators to test the settings before rolling it out to all users. This feature allows to resolve any issues before applying the global app configurations to the entire user base.

You can achieve the channel support by mapping the settings that you want to test to a channel and then add the channel in the payload. For more information, see Global App Configuration service documentation.

Citrix Virtual Channel SDK

The Citrix Virtual Channel software development kit (VCSDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops™ servers. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) is used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- The Windows Monitoring API, which enhances the visual experience and support for third-party applications integrated with ICA.
- Working source code for virtual channel sample programs to demonstrate programming techniques.

The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

Load Custom Virtual Channels on Macs with Apple Silicon

As an end-user, you can load the Custom Virtual Channel SDK (VCSDK) successfully on a Mac with the M1 and M2 chipset. With universal architecture, you must load the VCSDK by recompiling your Custom Virtual Channels using the latest VCSDK on the M1 and M2 chipset device. You can download the universal architecture build from the **Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture** section at Downloads.

To load the VCSDK, do the following:

1. Download Virtual Channel SDK 2204 for macOS from Downloads.
2. Open your Custom Virtual Channel project in Xcode.

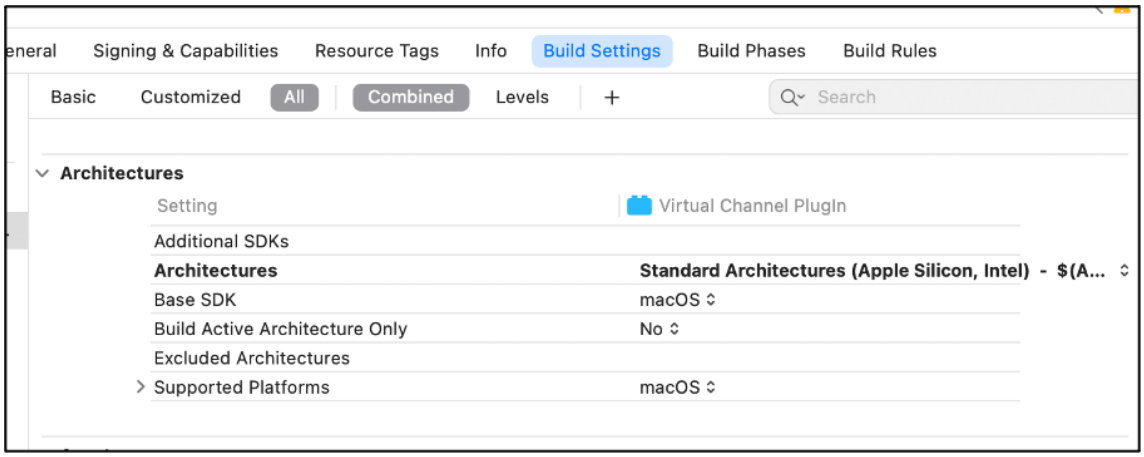
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Change your code.
4. Compile your Custom Virtual Channel to generate the virtual channel bundle.

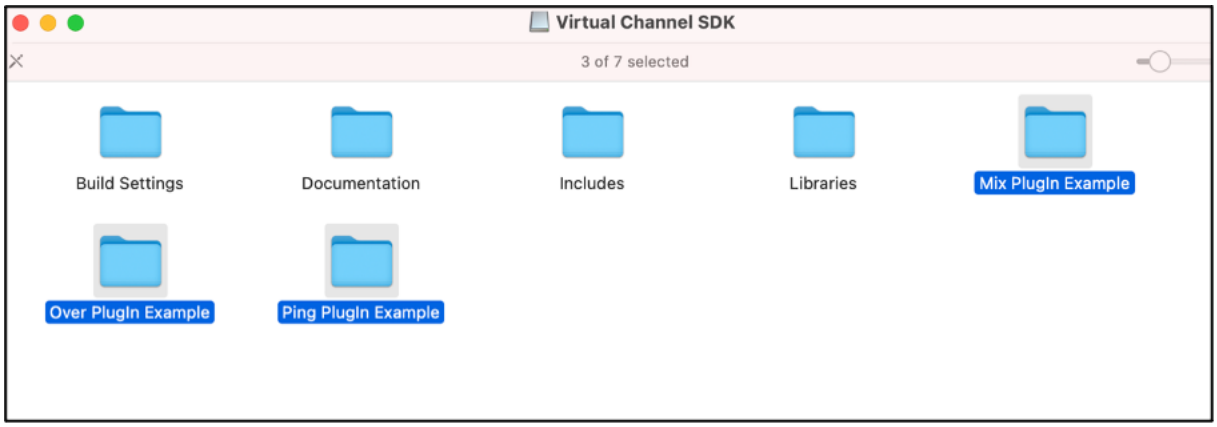
Test your Virtual Channel Software Development Kit (VCSDK)

If you're using the Citrix Virtual Channel Software Development Kit (VCSDK), you must customize so your customized virtual channels run correctly. To test your VCSDKs, do the following:

1. Ensure that all the linked libraries of your customized virtual channels are compiled for Universal Binary.
2. Change the Project file to support Universal Binary:
    - Open **Project** > **Build Settings**.
    - Set **Architectures** to **Standard Architectures**.



Examples for the VCSDK can be found inside *VCSDK.dmg*. These examples support Apple's Universal macOS Binary that runs natively on both Apple silicon and Intel-based Mac computers. Because it contains executable code for both architectures. You can use these examples as a reference.



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

Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac

Starting with the 2311 version, the Citrix Virtual Channel Software Development Kit (VCSDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers. This version of the SDK supports writing new virtual channels and screen sharing for Citrix Workspace app for Mac.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Mac in the Developer documentation.

Increase in the number of supported virtual channels

Previously, Citrix Workspace app for Mac supported up to 32 virtual channels. Starting with the 2308 version, you can use up to 64 virtual channels in a session.

Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac

Starting with the 2405 version, the Citrix Virtual Channel Software Development Kit (VCSDK) supports the desktop and screen sharing VCSDK API and gbuffer sharing.

For more information, see Virtual driver screen sharing and app-sharing functions.

Support for regional GACS discovery endpoints for US Government customers

Starting with version 2508, Citrix Workspace app for Mac transitions from using a single global GACS discovery endpoint to support regional compliance requirements for US Government customers. Administrators can configure government or regional customer settings through Mobile Device Management (MDM), enabling the app to either directly access regional settings endpoints or connect to region-specific discovery endpoints for US Government environments.

Configuration Configure using MDM policy with the following parameters:

Policy Key	Values	Description
GACSDiscoveryRegion	us_gov	Uses United States Government-compliant endpoints
	default	Uses global endpoints (standard behavior)

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

Example:

```
<key>GACSDiscoveryRegion</key>
<string>us_gov</string>
```

Behavior

- **No configuration:** App uses existing global discovery endpoint.
- **us_gov setting:** App connects through US Government-compliant regional endpoints.

Mobile Device Management

Citrix Workspace app now supports Mobile Device Management (MDM) that allows the administrators to configure, secure, and support Citrix Workspace app for Mac by enforcing policies through any MDM tool.

Install and uninstall Citrix Workspace app through the MDM

You can use terminal commands to install and uninstall the Citrix Workspace app through the MDM. For more information about using the terminal commands to install and uninstall, see the Manual install and Uninstall section.

To install Citrix Workspace app for Mac:

1. Download the `.dmg` file for the version of Citrix Workspace app for Mac that you want to install from the Downloads page.
2. Open the downloaded `CitrixWorkspaceApp.dmg` file.
3. Drag the `Install Citrix Workspace.pkg` file into the folder.
4. Use the following terminal command to install the package through MDM:

```
sudo installer -pkg /Volumes/Citrix\ Workspace/Install\ Citrix\
   Workspace.pkg -target /
```

To uninstall Citrix Workspace app:

You can use the following terminal command to uninstall the Citrix Workspace app through MDM:

```
sudo /Library/Application\ Support/Citrix\ Receiver/Uninstall\ Citrix
   \ Workspace.app/Contents/MacOS/Uninstall\ Citrix\ Workspace --
   nogui
```

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

Settings supported on MDM

Setting	Description	Key	Value	Value type	Default Value	Supported version
Session pre-launch	Enable/disable session pre-launch through MDM.	EnablePreLaunch	true/false	Boolean	false	2607
Configurations Checker tool	Enable/disable Citrix Workspace app config-uration check tool.	EnableConfigChecker	true/false	Boolean	false	2607
Block direct ICA file launch	Managing the launch of virtual app and desktop sessions from local ICA files on Mac.	BlockDirectICAFileLaunches	true/false	Boolean	false	2505
Remember password	Managing the behavior of the Remember password checkbox on Mac.	SaveCredential	true/false	Boolean	false	2505
Display of app shortcuts	Managing display of app shortcuts on Mac Launchpad.	AddShortcutsToLaunchPad	True/false	Boolean	True	2503

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Set pre-populated username	Sets the username that will be pre-populated in the authentication prompt.	CitrixUserName	UserNameValue	String	NA	2411
Lock pre-populated username	Locks the pre-populated username field, used with CitrixUserName to prevent edits.	LockUserName	true/false	Boolean	NA	2411
Auto update - AutoUpdateScheduler	Allows administrators to manage the Select the update channel option, preventing end users from modifying it.	AutoUpdateSchedulerSettings	{"startTime":"20:30","endTime":"23:30","deferCount":"4"}	String	NA	2411

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Version Control	Allows administrators to manage version control and auto-updates for Citrix Workspace plugins.	AutoUpdatePluginsSettings	[{ "pluginName": "Citrix Workspace", "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826", "pluginSettings": { "deploymentMode": "InstallAndUpdate", "upgradeToLatest": false, "minimumAllowedVersion": "24.02.10.24", "maximumAllowedVersion": "24.02.10.24", "delayGroup": "Medium"} }	String	NA	2411

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Auto update - Zoom AutoUpdatePlugInsSettings	Settings for managing auto-updates of plugins in Citrix Workspace.	AutoUpdatePlugInsSettings	[{ "pluginName": "Zoom VDI AutoUpgrade Plugin", "pluginId": "1A4BB471-022C-4C87-BDCD-0B64FB42869C", "pluginSettings": { "deploymentMode": "InstallAndUpdate", "upgradeToLatest": true, "ftu": true } }]	String	NA	2411

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Auto update - AutoUpdateChannel	Allows administrators to manage the Select the update channel option, preventing end users from modifying it.	AutoUpdateChannel	release/beta	String	release	2409
Enable/disable to install Citrix Enterprise Browser during Citrix Workspace app installation	Allows administrators to enable or disable the installation of Citrix Enterprise Browser during Citrix Workspace app installation.	RemoveCitrixEnterpriseBrowser	true/false	Boolean	False	2405

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Enable/disable loss tolerant mode for audio redirection	Allows administrators to enable or disable the loss-tolerant mode (EDT lossy) for audio redirection.	EdtUnreliableAllowed	true/false	Boolean	True	2402
Enable/disable audio volume synchronization	Allows administrators to enable or disable the synchronization of audio volume between the VDA and your audio devices.	EnableVolumeSync	true/false	Boolean	True	2402

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Enable/Disable H.265 video decoding	Allows administrators to enable or disable the H.265 video codec (HEVC) for hardware acceleration of remote graphics and videos.	EnableXdecoderForH265	true/false	Boolean	True	2402

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Select browser for FIDO2 web Authentication	Allows administrators to select the type of browser used for authenticating an end user into Citrix Workspace app. For more information about the description of values, see FIDO2 based authentication when connecting to cloud and on-premises store	WebBrowserForAuthenticationWithPrivateSession	System/SystemWithPrivateSession/EmbeddedWebView/EmbeddedWebViewWithPrivateSession	String	Embedded/EmbeddedWebViewWithPrivateSession	2307
Enable/disable FIDO2 authentication for HDX session	Allows administrators to enable or disable FIDO2 authentication within an HDX session.	Fido2Enabled	true/false	Boolean	true	2307

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Quick access menu for StoreFront	Allows administrators to enable or disable the **Quick access** menu for On-prem stores.	ShowQuickAccessForStoreFront	true/false	Boolean	false	2307
Auto update – AutoUpdateState	Updates Citrix Workspace app to the latest version without any user intervention automatically.	AutoUpdateState	Auto/Manual/Disabled	String	Auto	2305
Enable Azure Active Directory	Allows administrators to configure and enforce Azure Active Directory conditional access policies for users authenticating to Citrix Workspace app.	enableAAD	true/false	Boolean	False	2305

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Auto start of Citrix Workspace app	Controls Citrix Workspace app for Mac to start automatically whenever a computer is turned on by an end user.	AutoLaunchApp	true/false	Boolean	True	2304
Pre-configuration of Store URL	Allows administrators to preconfigure and add the store details to the Workspace app so that the end users don't have to do it.	StoreURLs	<Store URL>	String	NA	2210
Block new Store addition by end-user	Prevents the end user from adding a store in the Workspace app on their endpoint devices.	BlockStoreAddition	true/false	Boolean	False	2210

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

Setting	Description	Key	Value	Value type	Default Value	Supported version
Show/Hide menu bar	Shows or hides the Citrix Workspace menu on the Mac menu bar.	ShowHelperInMenuBar	True/False	Boolean	True	2208.1

Schema for reference

```
<array>
    <dict>
      <key>ShowHelperInMenuBar</key>
        <true/>
      <key>AutoLaunchAppOnRestart</key>
        <true/>
      <key>StoreURLs</key>
        <array>
          <string>PROVIDE STORE URL HERE</string>
        </array>
      <key>BlockStoreAddition</key>
        <false/>
      <key>CEIPEnabled</key>
        <true/>
      <key>LockUserName</key>
        <false/>
      <key>CitrixUserName</key>
        <string>PROVIDE USER NAME HERE</string>
      <key>AutoUpdateState</key>
        <string>Auto</string>
      <key>AutoUpdateChannel</key>
        <string>release</string>
      <key>WebBrowserForAuthentication</key>
        <string>Embedded</string>
      <key>Fido2Enabled</key>
        <false/>
      <key>ShowQuickAccessForStoreFront</key>
        <true/>
      <key>EnableXdecoderForH265</key>
        <false/>
      <key>EnableVolumeSync</key>
        <false/>
      <key>EdtUnreliableAllowed</key>
        <false/>
      <key>AddShortcutsToLaunchPad</key>
        <false/>
```

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

```
37        <key>PayloadDisplayName</key>
38          <string>Citrix Workspace</string>
39        <key>PayloadIdentifier</key>
40          <string>com.citrix.receiver.nomas</string>
41        <key>PayloadType</key>
42          <string>com.citrix.receiver.nomas</string>
43        <key>PayloadUUID</key>
44          <string>3BE38AD3-7D95-423F-BD7B-8A4D1F5208EF</string>
45        <key>PayloadVersion</key>
46          <integer>1</integer>
47      </dict>
48  </array>
```

Store configuration

Support for store configuration of user devices through MDM tool

Admins can now configure the following settings while deploying Citrix Workspace app through any MDM deployment tool such as Citrix Endpoint Management:

- **StoreURLs** –Configure store details so it's automatically added when the user opens the Citrix Workspace app, simplifying the sign-on experience.
  To add a store, provide the details for the **StoreURLs** setting. For example:

  ```
  <array>
  <string>https://myorg.com/?storename</string>
  </array>
  ```

  You can also add multiple stores as follows:

  ```
  <array>
  <string>https://myorg.com/?storename1</string>
  <string>https://myorg.com/?storename2</string>
  </array>
  ```

To add the StoreURLs to Citrix Workspace app, the user must quit and relaunch Citrix Workspace app.

- **BlockStoreAddition** –Prevent the user from adding stores.

  To block the user from adding a store, set the value of the **BlockStoreAddition** setting to **True**.

For more information, see Mobile Device Management.

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

StoreFront to Workspace migration

As your organization transitions from on-premises StoreFront to Workspace, users are required to manually add the new Workspace URL to the Citrix Workspace app. This feature enables admins to seamlessly migrate users from a StoreFront store to a Workspace store with minimal user interaction.

Consider, all your end users have a StoreFront store `storefront.com` added to their Workspace app. As an administrator, you can configure a StoreFront URL to Workspace URL Mapping {'storefront.com':'xyz.cloud.com'} in the Global App Configuration service. The Global App Configuration service pushes the setting to all Citrix Workspace app instances, on both managed and unmanaged devices that have the StoreFront URL `storefront.com` added.

Once the setting is detected, Citrix Workspace app adds the mapped Workspace URL `xyz.cloud.com` as another store. When the end user launches the Citrix Workspace app, the Citrix Workspace store opens. The previously added StoreFront store `storefront.com` remains added to the Citrix Workspace app. Users can always switch back to the StoreFront store `storefront.com` using the **Switch Accounts** option in the Citrix Workspace app. Admins can control the removal of the StoreFront store `storefront.com` from the Citrix Workspace app at the users' end points. The removal can be done through the global app config service.

To enable the feature, do the following steps:

1. Configure StoreFront to Workspace mapping using the Global App Configuration service. For more information on the Global App config service, see Global App Configuration service.
2. Edit the payload in the app config service:

```
{
  "serviceURL": Unknown macro: \{
  "url" }

,
"settings":{

"name":"Productivity Apps", [New Store Name]
"description":"Provides access StoreFront to Workspace Migration",
"useForAppConfig":true,
"appSettings":
{
  "macos":[ Unknown macro: \{
  "category" }

]
 }

 }

 }
```

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

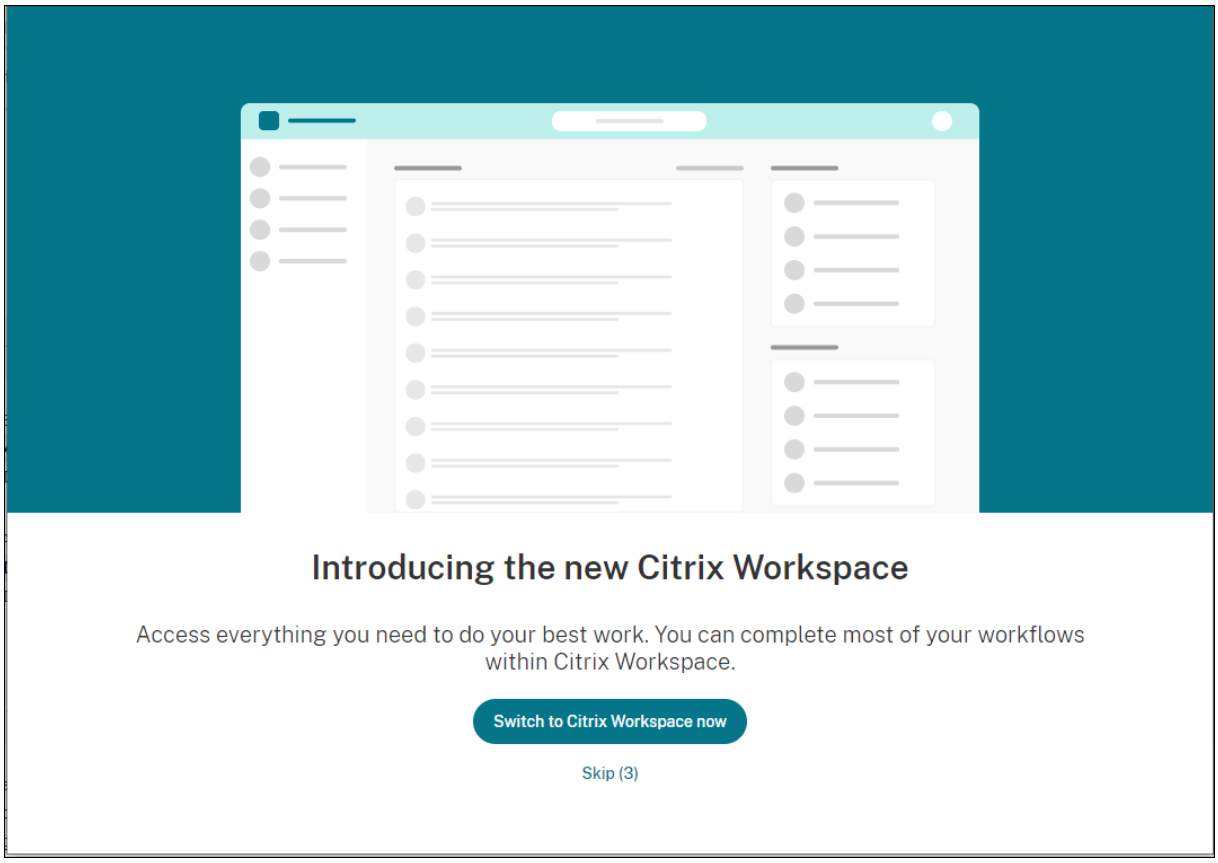
> **Note:**
>
> If you're configuring the payload for the first time, use POST.
> If you're editing the existing payload configuration, use PUT and check that you have the payload that consists of all the supported settings.

3. Specify the StoreFront URL `storefront.com` as the value for **URL** in the **serviceURL** section.
4. Configure the Workspace URL `xyz.cloud.com` inside the section **migrationUrl**.
5. Use **storeFrontValidUntil** to set the timeline for the removal of the StoreFront store from the Citrix Workspace app. This field is optional. You can set the following value based on your requirement:

    - Valid date in the format (YYYY-MM-DD)

    > **Note:**
    >
    > If you've provided a past date, then the StoreFront store is removed immediately upon URL migration. If you've provided a future date, then the StoreFront store is removed on the set date.

Once the app config service settings are pushed, the following screen appears:



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

When the user clicks **Switch to Citrix Workspace now**, the Workspace URL is added to Citrix Workspace app and the authentication prompt appears. Users have a limited option to delay the transition up to three times.

Custom web store

Support for custom web stores

Starting with the 2112 version, you can access your organization's custom web store from the Citrix Workspace app for Mac. Previously, you accessed all customized stores through the browser only. To use this feature, the admin must add the custom web store to the list of allowed URLs in the `allowedWebStoreURLs` property in the Global App Configuration service.

Citrix Workspace app for Mac loads the custom web stores with a browser-like experience and extends App Protection capabilities to custom web stores. Making the custom portal accessible from the native Citrix Workspace App provides comprehensive capabilities and user experience for this feature. For more information about Global App Configuration service, see Getting Started.

To add a custom web store URL, perform the following steps:

1. Open the Citrix Workspace app and navigate to **Accounts**.
2. In the **Accounts** window, click the **+** icon and type the URL.

To delete a custom web store URL, perform the following steps:

1. Open the Citrix Workspace app and navigate to **Accounts**.
2. In the **Accounts** window, select the account you want to delete and click the **-** icon.

Support for customized URLs through 301 redirects

Starting with the 2106 version, you can add URLs that redirect to Citrix Workspace from StoreFront or Citrix Gateway through HTTP 301 redirects.

If you're migrating from StoreFront to Citrix Workspace, you can redirect the StoreFront URL to a Citrix Workspace URL through an HTTP 301 redirect. As a result, when adding an old StoreFront URL, you're automatically redirected to Citrix Workspace.

Example of a redirect:

The StoreFront URL `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` can be redirected to a Citrix Workspace URL: `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`.

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

> **Note:**
>
> - Citrix Workspace app for Mac does not support Dual Tone Multi Frequency (DTMF) with Microsoft Teams due to pending changes from Microsoft.
> - From the 2106 release onward, the Citrix Viewer's version number and the Citrix Workspace app's version number might not match. This change does not affect your experience.

Email-based auto-discovery of store

Starting with the 2109 version, You can provide your email address in Citrix Workspace app for Mac to automatically discover the store associated with the email address. If there are multiple stores associated with a domain, by default the first store returned by the Global App Configuration service is added as the store of choice. Users can always switch to another store if necessary.

Sign out of the custom web store when you close Citrix Workspace app

When the **signoutCustomWebstoreOnExit** setting is set to **True**, closing the Citrix Workspace app window signs you out of the custom web store. When you reopen the Citrix Workspace app, the web store URL is loaded again. You can configure the **signoutCustomWebstoreOnExit** setting in the Global App Configuration service.

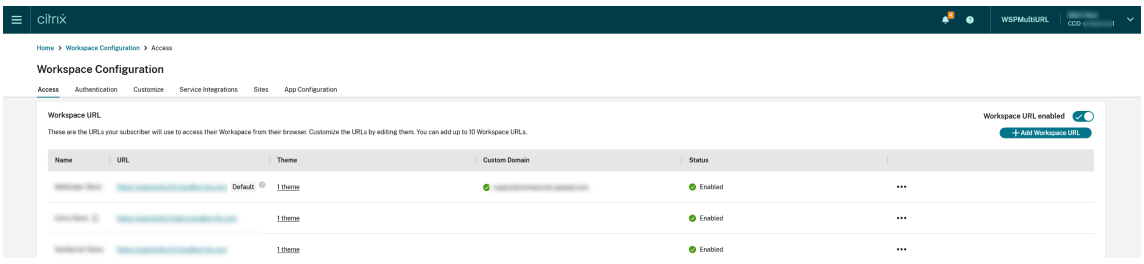
Support for administrator to restrict the user from changing the store name

Previously, users were able to change the store name by using the **Edit Account** option.

Starting with the 2402 version, Citrix Workspace app for Mac provides administrators an option to restrict the user from changing the store name. With this feature, administrators can easily identify and maintain consistency in the store names.

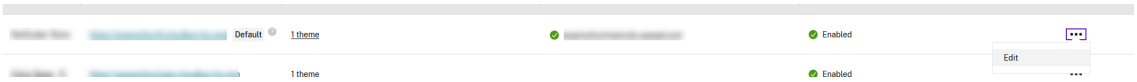
To allow the end-users to change the store name, do the following steps:

1. Sign in to Citrix Cloud with your credentials.
2. Navigate to **Workspace Configuration** >**Access**. Under **Workspace URL**, you can find a list of existing store URLs.

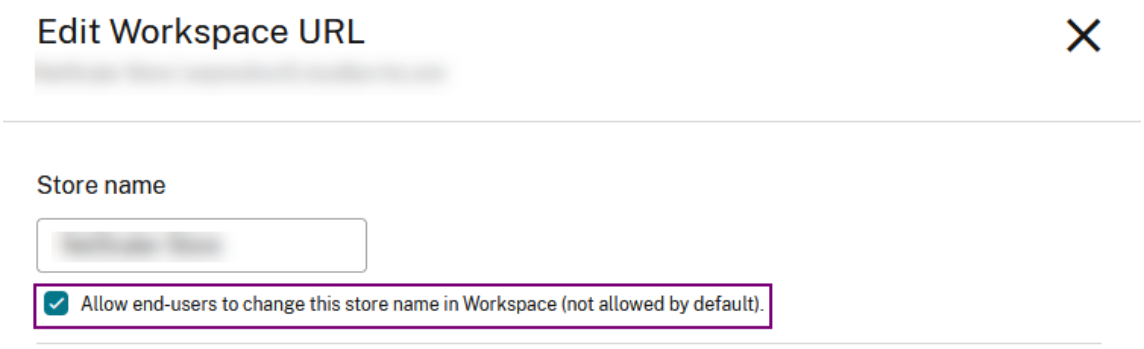


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click the ellipsis menu for the store that you want to allow end-users to change the store name.
4. Select **Edit**.



5. On the **Edit Workspace URL** dialog box, select **Allow end-users to change this store name in Workspace (not allowed by default)**.



6. Click **Save**.

For more information, see Restrict end users to change the store name in the Citrix Workspace documentation.

Security and Authentication

This section describes about the security features and authentication details for Citrix Workspace app for Mac.

- Authentication
- Security
- Secure communications

Authenticate

Enhancing Citrix® security with pre-populated user name

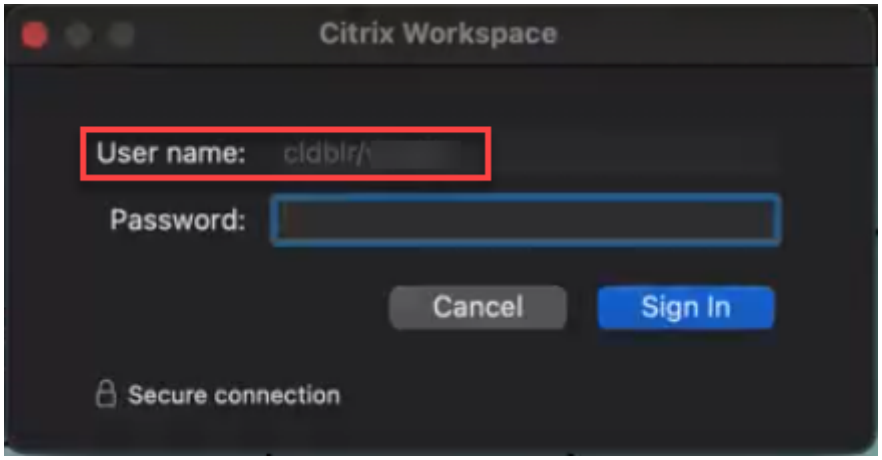
Starting with version 2411, administrators can use Mobile Device Management (MDM) to push the user name in a specific format to manage devices. Citrix Workspace™ app reads this configuration, retrieves the user name, and pre-populates it within the authentication prompt, making it read-only. This ensures that only end users to whom a Mac is registered can authenticate to the Citrix Workspace

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

app on that specific machine. This feature enhances sign-in security and gives administrators greater control over authentication.

You can configure this feature through MDM using the following settings:

```
<array>
   <dict>
       <key>LockUserName</key>
       <true/>
       <key>CitrixUserName</key>
       <string>UserNameValue</string>
   </dict>
</array>
```



Limitations:

- This solution works only with on-premises stores that use basic authentication.
- It is not compatible with SAML (WebView) authentication.
- The scope is limited to the Citrix Workspace app and browser-based logins are not managed.

For more information on how to use MDM, see Mobile Device Management.

Mandate end users to authenticate and access apps and desktops through native app

Starting with version 2411, admins can mandate users on Mac devices to access Citrix Workspace app exclusively through the native app. When this feature is enabled, users attempting to access the store URL and third-party browsers are automatically redirected to the Citrix Workspace app. This ensures they can take advantage of all the native app's capabilities and enjoy a seamless user experience. Also, users connecting through a browser while invoking the HDX™ engine are prompted to add the store to the native client for future access. This feature also gives admins greater control over the user environment and enhances security by keeping the authentication process within the native app, eliminating the need to download ICA files.

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

Admins can enable this feature using their Citrix Cloud account. This feature is currently supported for Cloud stores only. For more information, see Mandate end users to authenticate and access apps and desktops through native app.

Enhancements to the smart card reader authentication

Starting with the version 2409, Citrix Workspace app supports the plug and play functionality for the smart card readers. With this feature, users can conveniently use their smart cards without needing to manually connect the reader before launching an ICA® session. The system automatically detects and initializes the reader once the smart card is inserted.

Also, Citrix Workspace app handles concurrent smart card command requests more efficiently. When multiple processes on the Virtual Delivery Agent (VDA) read the smart card simultaneously, the redirection speed is improved.

These enhancements ensure a smoother user experience while using the smart card reader for authentication.

Support for fast smart card

Starting with the version 2409, Citrix Workspace app supports the Fast smart card feature. Fast Smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance significantly when smart cards are used in high-latency WAN environments.

Enabling the fast smart card logon on Citrix Workspace app

To enable this feature, you need to specify the location of the PKCS#11 library file on the **Smart card** settings in Citrix Workspace app preferences. For more information, see Specifying a PKCS#11 module for smart card authentication.

Disabling the fast smart card logon on Citrix Workspace app

To disable fast smart card logon on Citrix Workspace app, set the “PKCS#11 module”in Citrix Workspace app Preferences to “None Selected”.

> **Note:**
>
> - Fast smart card logon is enabled by default on the VDA and disabled by default on Citrix Workspace app.
> - Earlier versions of Citrix Workspace app for Mac employed the PKCS#11 module to establish SSL connections, rather than relying on smart card redirection and authentication.

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

> Presently, fast smart cards on Citrix Workspace app for Mac exclusively support cards that use the RSA algorithm. Attempting to configure an incompatible PKCS#11 module can lead to authentication failure.

Smart card

Citrix Workspace app for Mac supports smart card authentication in the following configurations:

- Smart card authentication to Workspace for Web or StoreFront 3.12 and later.
- Citrix Virtual Apps and Desktops™ 7 2203 and later.
- XenApp and XenDesktop 7.15 and later.
- Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office that allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.
- Citrix Workspace app for Mac supports using multiple certificates with a single smart card or with multiple smart cards. When your user inserts a smart card into a card reader, the certificates are available to all applications running on the device, including Citrix Workspace app for Mac.
- For double-hop sessions, a further connection is established between Citrix Workspace app for Mac and your user's virtual desktop.

About smart card authentication to Citrix Gateway

There are multiple usable certificates when you use a smart card to authenticate a connection. Citrix Workspace app for Mac prompts you to select a certificate. After you select a certificate, Citrix Workspace app for Mac prompts you to enter the smart card password. Once authenticated, the session launches.

If there's only one suitable certificate on the smart card, Citrix Workspace app for Mac uses that certificate and does not prompt you to select it. However, you must still enter the password associated with the smart card to authenticate the connection and to start the session.

Specifying a PKCS#11 module for smart card authentication

> **Note:**
>
> Installing the PKCS#11 module isn't mandatory. This section only applies to ICA sessions. It does not apply to Citrix Workspace access to Citrix Gateway or StoreFront where a smart card is required.

To specify the PKCS#11 module for smart card authentication:

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

1. In Citrix Workspace app for Mac, select **Preferences**.
2. Click **Security & Privacy**.
3. In the **Security & Privacy** section, click **Smart Card**.
4. In the **PKCS#11** field, select the appropriate module. Click **Other** to browse to the location of the PKCS#11 module if the module you wanted isn't listed.
5. After selecting the appropriate module, click **Add**.

Supported readers, middleware, and smart card profiles

Citrix Workspace app for Mac supports most macOS-compatible smart card readers and cryptographic middleware. Citrix has validated the operation with the following.

Supported readers:

- Common USB connect smart card readers

Supported middleware:

- Clarify
- ActivIdentity client version
- Charismathics client version

Supported smart cards:

- PIV cards
- Common Access Card (CAC)
- Gemalto .NET cards

Follow the instructions provided by your vendor's macOS-compatible smart card reader and cryptographic middleware for configuring user devices.

Restrictions

- Certificates must be stored on a smart card, not on the user device.
- Citrix Workspace app for Mac does not save the user certificate choice.
- Citrix Workspace app for Mac does not store or save the user's smart card PIN. OS handles the PIN acquisitions, which might have its own caching mechanism.
- Citrix Workspace app for Mac does not reconnect sessions when a smart card is inserted.
- To use VPN tunnels with smart card authentication, you must install the Citrix Gateway Plug-in and log on through a webpage. Use your smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway Plug-in isn't available for smart card users.

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

Conditional Access with Azure Active Directory

This authentication method is currently not supported on Citrix Workspace app for Mac.

User-Agent

Citrix Workspace app sends a user agent in network requests that can be used to configure authentication policies including redirection of authentication to other Identity Providers (IdPs).

> **Note:**
>
> Don't mention the version numbers while configuring the policies.

Scenario	Description	User-Agent
Regular HTTP Requests	In general, a network request made by Citrix Workspace app contains a general User-Agent. For example, the following network requests contain a general User-Agent GET /Citrix/Roaming/Accounts GET / AGServices/discover	`CitrixReceiver/23.05.0.36 MacOSX/13.4.0 com.citrix.receiver.nomas X1Class CWACapable`
Cloud Store	When users add a cloud store to Citrix Workspace app, the network requests made by Citrix Workspace app contains a specific User-Agent.	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Citrix Workspace/23.05.0.36 MacOSX/13.4.0 com.citrix.receiver.nomas X1Class CWACapable`
OnPrem Store with Gateway Advanced Auth	When users add an on-premises store with Advanced Auth configured on Gateway to Citrix Workspace app, the network requests made by Citrix Workspace app contains a specific User-Agent. For example, network requests with path /cgi/connect/authorize contains a specific User-Agent.	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko), CWAWEBVIEW/23.05.0.36`
Custom Web Store	When a user adds a custom web store Citrix Workspace app, the network requests made by Citrix Workspace app contains a specific User-Agent. For example, network requests with requests containing GET /nf/auth/doWebview.do GET /logon/LogonPoint/tmindex.html	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Safari CWA/23.05.0.18 MacOSX/13.4.0`

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

FIDO2 for password-less authentication

Citrix Workspace app for Mac supports password-less authentication using FIDO2 security keys when connecting to a cloud store or within an HDX session. FIDO2 security keys provide a seamless way for enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a user name or password. This feature currently supports roaming authenticators (USB only) with PIN code and touchID. This feature is supported on macOS 12 and later versions.

For more information about FIDO2 see FIDO2 Authentication.

For information about the prerequisites and using this feature, see Local authorization and virtual authentication using FIDO2.

FIDO2-based authentication when connecting to cloud and on-premises store

Citrix Workspace app uses the user's default browser for FIDO2 authentication (Web Authentication), when connecting to the cloud and on-premises stores. Administrators can configure the type of browser to authenticate to Citrix Workspace app. For more information on the web browser settings, see Global App Configuration service documentation.

The following settings allow you to select the type of browser that is used for authenticating an end user into Citrix Workspace app:

Settings	Description
System	Allows you to use the user's default browser for authentication (for example, Safari or Chrome). Authentication occurs outside Citrix Workspace app. Use this setting to support passwordless authentication. This setting tries to use the existing user session from the user's browser.
SystemWithPrivateSession	This setting is similar to the **System** setting. Citrix Workspace app uses a private session in the browser for authentication. The browser doesn't save authentication cookies or data. Single sign-on isn't supported in this option.

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

Settings	Description
Embedded	Allows you to authenticate within Citrix Workspace app. Citrix Workspace app saves the session data or cookies for single sign-on (for example, SaaS apps) when the enhanced single sign-on feature is enabled. This authentication method does not support passwordless authentications such as FIDO2.
EmbeddedWithPrivateSession	This setting is similar to the **Embedded** setting. Single sign-on isn't supported as session data or cookies aren't present in Citrix Workspace app.

To push the configured settings, run the following commands using the Mobile Device Management (MDM), Global App Configuration service (GACS), or the command line interface methods:

- **Enable FIDO2 using MDM:** To enable authentication through MDM, administrators must use the following setting:

  ```
  <key>WebBrowserForAuthentication</key><string>System</string>
  ```

For more information on how to use MDM, see Mobile Device Management.

- **Enable FIDO2 using GACS:** To enable authentication through GACS, administrators must use the following setting:

```
{

    "serviceURL": {

      "url": "https://serviceURL:443"
     }
 ,
    "settings": {

      "name": "Web browser for Authenticating into Citrix Workspace",
      "description": "Allows admin to select the type of browser used
         for authenticating an end user into Citrix Workspace app",
      "useForAppConfig": true,
      "appSettings": {

        "macos": [
          {

            "assignedTo": [
              "AllUsersNoAuthentication"
            ],
```

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

```
            "category": "authentication",
            "settings": [
              {

                "name": "web browser for authentication",
                "value": "SystemWithPrivateSession"
               }

            ],
            "userOverride": false
           }

        ]
       }

    }

  }
```

- **Enable FIDO2 using the command-line interface:** To enable authentication using the command-line interface, administrators must run the following command:

  ```
  defaults write com.citrix.receiver.nomas WebBrowserForAuthentication
   System
  ```

FIDO2-based authentication within an HDX session

You can configure FIDO2 Security Keys to authenticate within an HDX session. This feature currently supports roaming authenticators (USB only) with PIN code.

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

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

This feature is enabled by default for Citrix Workspace app for 2307 and future releases. You can disable FIDO2 authentication using the Mobile Device Management (MDM) or command-line interface methods by running the following commands:

- **Disable FIDO2 based authentication using MDM:** To disable this feature through MDM, administrators must use the following setting:

  ```
  <key>Fido2Enabled</key><false/>
  ```

For more information on how to use MDM, see Mobile Device Management.

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

- **Disable FIDO2 based authentication using the command-line interface:** To disable this feature, run the following command in command-line interface methods:

```
defaults write com.citrix.receiver.nomas Fido2Enabled -bool NO
```

Support for device touch ID for FIDO2 password-less authentication

Previously, Citrix Workspace app supported FIDO2 password-less authentication through the roaming authenticators (USB only) with PIN code and touch.

Starting with the version 2405, Citrix Workspace app now supports device touch ID for FIDO2 password-less authentication, enhancing the sign-in experience for users. With this feature, users can securely sign in to the store configured on the Citrix Workspace app using the device touch ID, eliminating the need for passcodes or passwords. This feature enhances both the usability and security of Citrix Workspace app for macOS users. This feature is enabled by default.

Support for Certificate-based authentication

Starting with the 2305 version, Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to Citrix Workspace app.

The following methods can be used to enable the authentication using conditional access:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

The flag values read by Citrix Workspace app take precedence in the following order:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

Enabling authentication using conditional access through MDM

To enable authentication using conditional access with Azure AD through MDM, admins must use the following setting:

```
<key>enableAAD</key>
<true/>
```

This setting supports Boolean values. The value is set to false by default. The default value is considered if the key value isn't available.

For more information on how to use MDM, see Mobile Device Management.

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

Enabling authentication using conditional access through GACS

To enable authentication using conditional access with Azure AD through GACS, admins must use the following setting:

```
enable conditional AAD
```

For more information, see Supported settings and their values per platform for macOS in the GACS documentation.

Simplified authentication into on-premises store

Starting with the 2505 version, administrators can control the **Remember password** checkbox behavior in Citrix Workspace app for Mac.

Administrators can configure this feature using an MDM-based key-value pair:

```
key: SaveCredentials
```

```
value type: Boolean
```

The following logic determines the behavior of the **Remember password** checkbox based on StoreFront™ configuration and the presence of the `SaveCredentials` MDM key:

- If `SaveCredential` is not set in StoreFront:
  - The system displays the **Remember password** checkbox to the user.
  - If the **MDM** key `SaveCredentials` is present:
    - If `SaveCredentials = true`: The system selects the checkbox and disables it, so the user can't change its state.
    - If `SaveCredentials = false`: The system unchecks, disables, and locks the checkbox.
  - If the **MDM** key is not present: The StoreFront configuration solely controls the checkbox behavior.
- If `SaveCredential` is set in StoreFront to False:
  - The system does not display the **Remember password** checkbox to the user.
  - If the **MDM** key is set, the system still saves credentials to disk according to its value, but keeps the checkbox hidden.

> **Note:**
>
> - If the **MDM** key is present, it overrides user interaction with the checkbox.
> - **MDM** policy manages credentials even if the UI element is hidden.

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

Limitations

This solution applies only to on-premises environments where Citrix Workspace app can access StoreFront directly using the user name and password authentication method exclusively.

Support for Entra ID Single Sign-On (SSO)

Starting with version 2508, Citrix Workspace app for MAC supports Single Sign-On (SSO) with Microsoft Entra ID.

Single Sign-On with Microsoft Entra ID

Users can sign in to Citrix Workspace app using their Microsoft Entra ID credentials and seamlessly launch Citrix Virtual Apps and Desktops with SSO, reducing repeated prompts and improving the overall sign-in experience.

For detailed configuration instructions, see Entra ID SSO configuration guide.

Default authentication behavior

With the default authentication flow, users authenticate once during the first session launch. Subsequent sessions automatically use Single Sign-On (SSO).

This authentication method supports both on-premises and cloud deployments.

System browser authentication behavior

When using system browser authentication, macOS displays a modal dialog that indicates:

- The domain being authenticated.
- A prompt to proceed with authentication.

You can enable system browser authentication through **MDM** or **GACS**:

- GACS configuration: In the Authentication category, set Web Browser For Authentication to System. For details, see Supported settings and their values per platform.
- MDM configuration: Use the following setting:

```
<key>WebBrowserForAuthentication</key><string>System</string>
```

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

> **Notes:**
>
> - System browser authentication doesn't support on-premises stores.
> - When using the `SystemWithPrivateSession` option, the browser operates in a private session without saving cookies or data, so SSO isn't supported.

Disable Entra ID support

To disable Entra ID support for Citrix Workspace app for MAC, run the following command:

```
defaults write com.citrix.receiver.nomas UseLegacyTermsrvResourceUri -bool YES
```

Support for PassKey (FIDO2) authentication

Starting with version 2603, Citrix Workspace app for Mac supports **PassKey (FIDO2)** authentication using **TouchID** or password, in addition to external Security Keys. The **PassKey** is specific to the local macOS user profile and stored in the Secure Enclave, accessible only by Citrix Viewer. This feature is supported on Macs with the Secure Enclave.

> **Notes:**
>
> - Citrix Workspace app for Mac creates and manages **PassKeys**, which are valid only within active sessions.
> - Contact your administrator if the organization requires certified authenticators.

Security

App Protection

App Protection feature is an add-on feature that provides enhanced security when using Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). The feature restricts the ability of clients to compromise with keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information on the screen. For more information, see App Protection documentation.

> Disclaimer
>
> App Protection policies filter the access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). App Protection policies

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

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

To configure App Protection on Citrix Workspace app for Mac, see the Citrix Workspace app for Mac section in the Configuration article.

> **Note:**
>
> - App Protection is supported only from Citrix Workspace app 2001 for Mac or later.

App Protection enhancement

Starting with the 2301 version, App Protection is enhanced to protect the Citrix Workspace app. This enhancement includes protecting the authentication screen and the screen that you see after signing into the Workspace app.

Support for screen sharing when App Protection is enabled

Starting with the 2402 version, you can share content through Microsoft Teams with HDX optimization, even when App Protection is enabled. With this feature, you can share a screen in the virtual desktop session to its full potential. For more information, see Compatibility with HDX optimization for Microsoft Teams.

Force login prompt for Federated identity provider

Citrix Workspace app now honors the Federated Identity Provider Sessions setting. For more information, see Citrix Knowledge Center article CTX253779.

You no longer need to use the Store authentication tokens policy to force the login prompt.

Inactivity timeout for Citrix Workspace app

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

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

The inactivity timeout value can be set starting from 1 minute to 1440 minutes. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module. Click here to download the PowerShell modules for Citrix Workspace Configuration.

The end-user experience is as follows:

- A notification appears three minutes before you're signed out, with an option to stay signed in, or sign out. The notification appears if you've enabled Citrix Workspace app notifications in the system preferences of your Mac.
- The notification appears only if the configured inactivity timeout value is greater than 5 minutes. For example, if the configured value is 6 minutes, a notification appears when 3 minutes of inactivity is detected. If the configured inactivity timeout value is less than or equal to 5 minutes, the user is signed out without a notification.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click Sign-out to end the session for the current store.

Prevent launching of ICA® files from disk

Starting with version 2505, admins can control session launches from downloaded ICA files using the new GACS/MDM policy. This feature helps prevent unauthorized access and reduces security risks associated with file-based session initiations.

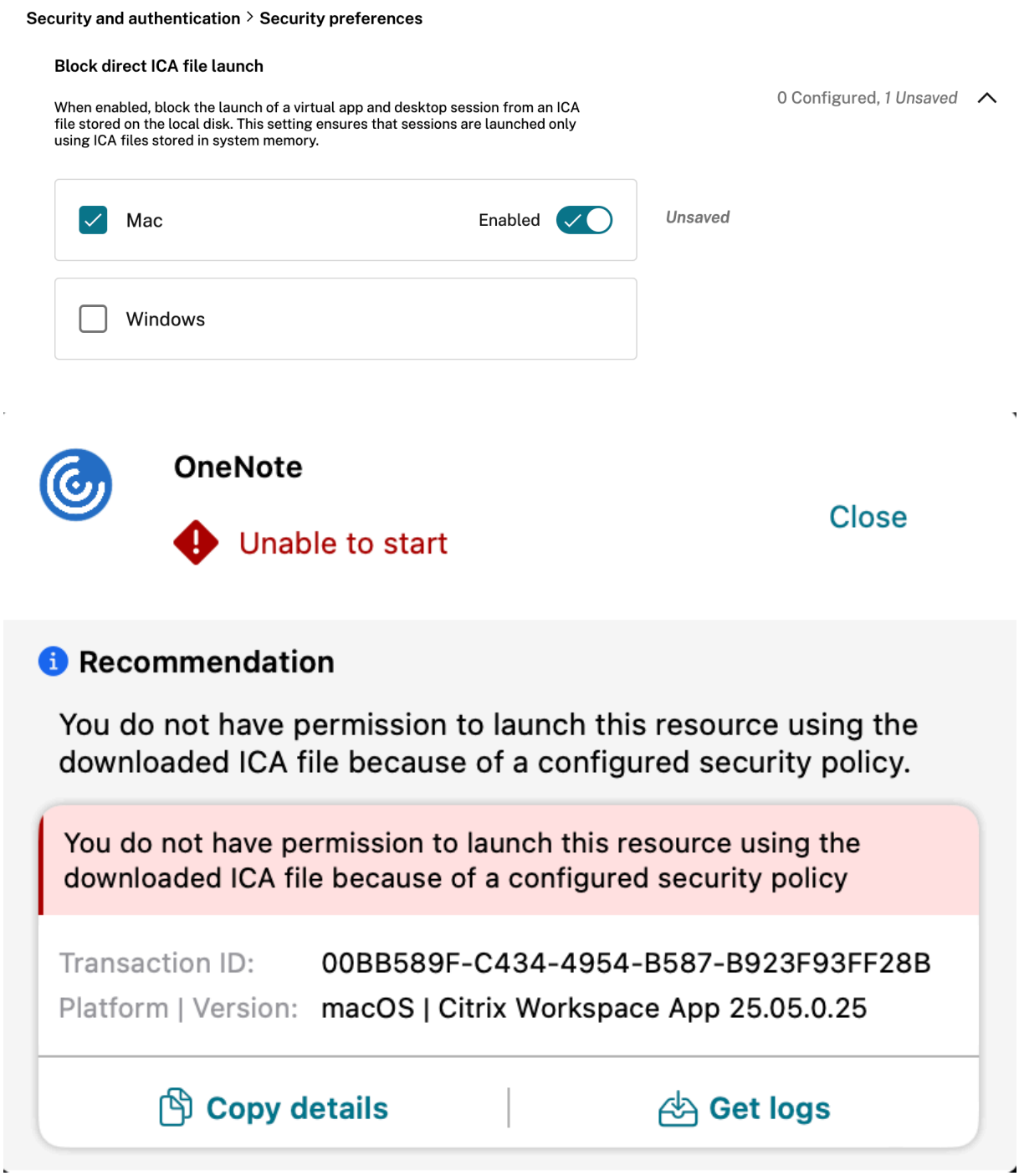
To enable authentication through MDM, use the following settings:

```
<key>BlockDirectICAFileLaunches</key>
<true/>
```

To enable this feature through GACS, admins must follow these steps:

1. In the Block direct ICA file launch page, go to **Security and authentication > Security preferences > Configure**.
2. Select **Mac** and set it to **Enabled** to apply your preferred settings.

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



This policy aims to improve security and prevent unauthorized use by:

- Restricts session launches using downloaded ICA files.
- Prevents unauthorized or unintended access to resources.

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

Functionality

- When the policy is enabled:
  - Users can't launch sessions using downloaded ICA files.
  - The system displays this error message:

    "You do not have permission to launch this resource using the downloaded ICA file because of a configured security policy."
- When the policy is disabled or not configured:
  - Users can launch sessions using downloaded ICA files.

Behavior based on the MDM key `BlockDirectICAFileLaunches`:

- If the MDM key `BlockDirectICAFileLaunches` is present:
  - If `BlockDirectICAFileLaunches` = **`true`**, ICA file launches are blocked and an error popup appears to indicate the block.
  - If `BlockDirectICAFileLaunches` = **`false`**, ICA file launches are allowed and the session proceeds as normal.

Secure communications

To secure the communication between your Site and Citrix Workspace app for Mac, you can integrate your connections with a range of security technologies, including Citrix Gateway. For information about configuring Citrix Gateway with Citrix StoreFront, see StoreFront documentation.

> **Note:**
>
> Citrix recommends using Citrix Gateway to secure communications between StoreFront servers and users' devices.

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace and servers. Citrix Workspace app for Mac supports SOCKS and secure proxy protocols.
- Citrix Secure Web Gateway. You can use Citrix Secure Web Gateway to provide a single, secure, encrypted point of access through the internet to servers on internal corporate networks.
- SSL Relay solutions with Transport Layer Security (TLS) protocols
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you use a firewall that maps the server's internal IP address to an external internet address such as network address translation (NAT), configure the external address.

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

> **Note:**
>
> Starting with macOS Catalina, Apple has enforced extra requirements for root CA certificates and intermediate certificates which administrators must configure. For more information, see Apple Support article HT210176.

Citrix Gateway

To enable remote users to connect to your XenMobile deployment through Citrix Gateway, you can configure Citrix Gateway to support StoreFront. The method for enabling access depends on the edition of XenMobile in your deployment.

If you deploy XenMobile in your network, allow connections from internal or remote users to StoreFront through Citrix Gateway, by integrating Citrix Gateway with StoreFront. This deployment allows users to connect to StoreFront to access published applications from XenApp and virtual desktops from XenDesktop. Users connect through Citrix Workspace app for Mac.

Connecting with the Citrix Secure Web™ Gateway

If the Citrix Secure Web Gateway Proxy is installed on a server in the secure network, you can use the Citrix Secure Web Gateway Proxy in Relay mode. For more information about Relay mode, see XenApp and Citrix Secure Web Gateway documentation.

If you're using Relay mode, the Citrix Secure Web Gateway server functions as a proxy and you must configure Citrix Workspace app for Mac to use:

- The fully qualified domain name (FQDN) of the Citrix Secure Web Gateway server.
- The port number of the Citrix Secure Web Gateway server. Citrix Secure Web Gateway Version 2.0 does not support Relay mode.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example, my_computer.example.com is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (example), and a top-level domain (`com`). The combination of intermediate and top-level domain (`example.com`) is referred to as the domain name.

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

Connecting through a proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app for Mac and servers. Citrix Workspace app for Mac supports both SOCKS and secure proxy protocols.

When the Citrix Workspace app for Mac communicates with the Web server, it uses the proxy server settings configured for the default web browser on the user device. Configure the proxy server settings for the default Web browser on the user device accordingly.

Provision to manage multiple proxy servers using PAC files

Starting with the version 2405, you can use multiple proxy servers that allow the HDX sessions to select appropriate proxy servers for accessing specific resources. This selection is based on the proxy rules configured in the Proxy Auto-Configuration (PAC) file. Using this file, you can manage the network by mentioning which network traffic must be sent through a proxy server and which must be sent directly. Additionally, the PAC URL supports both **http://** and **file://** protocols.

Connecting through a firewall

Network firewalls can allow or block packets based on the destination address and port. Citrix Workspace app for Mac must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 for a secure Web server) for user device to Web server communication. For Citrix Workspace to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

TLS

Transport Layer Security (TLS) is the latest, standardized version of the TLS protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

Citrix Workspace app for Mac supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

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

> **Note:**
>
> Citrix Workspace app for Mac uses platform (OS X) crypto for connections between Citrix Workspace app for Mac and StoreFront.

The following cipher suites are deprecated for enhanced security:

- Cipher suites with prefix "TLS_RSA_*"
- Cipher suites RC4 and 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Citrix Workspace app for Mac supports only the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

For DTLS 1.0 users, Citrix Workspace app for Mac 1910 and later supports only the following cipher suite:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Upgrade your Citrix Gateway version to 12.1 or later if you want to use DTLS 1.0. Otherwise, it falls back to TLS based on the DDC policy.

The following matrices provide details of internal and external network connections:

		Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

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

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

Note:

- Use Citrix Gateway 12.1 or later for EDT to work properly. Older versions do not support ECDHE cipher suites in DTLS mode.
- Citrix Gateway doesn't support DTLS 1.2. So, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` and `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` aren't supported. Citrix Gateway must be configured to use `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` to work properly in DTLS 1.0.

Configuring and enabling Citrix Workspace app for TLS

There are two main steps involved in setting up TLS:

1. Set up SSL Relay on your Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server. Then, obtain and install the necessary server certificate.
2. Install the equivalent root certificate on the user device.

Installing root certificates on user devices

To use TLS to secure communications between TLS-enabled Citrix Workspace app for Mac and the server farm, you need a root certificate on the user device. This root certificate verifies the signature of the Certificate Authority on the server certificate.

macOS X comes with about 100 commercial root certificates already installed. However, if you want to use another certificate, you can obtain one from the Certificate Authority and install it on each user device.

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

Install the root certificate on each device, depending on your organization's policies and procedures, instead of prompting users to install it. The easiest and safest way is to add root certificates to the macOS X keychain.

To add a root certificate to the keychain

1. Double-click the file containing the certificate. This action automatically starts the Keychain Access application.
2. In the Add Certificates dialog box, choose one of the following from the Keychain pop-up menu:
    - login (The certificate applies only to the current user.)
    - System (The certificate applies to all users of a device.)
3. Click OK.
4. Type your password in the Authenticate dialog box and then click OK.

The root certificate is installed and used by TLS-enabled clients and by any other application using TLS.

About TLS policies

This section provides information for configuring security policies for ICA sessions over TLS. You can configure certain TLS settings used for ICA connections in Citrix Workspace app for Mac. These settings are not exposed in the user interface. Changing them requires running a command on the device running Citrix Workspace app for Mac.

> **Note:**
>
> TLS policies are managed in other ways - by devices controlled by an OS X server or another mobile device management solution.

TLS policies include the following settings:

SecurityComplianceMode. Sets the security compliance mode for the policy. If you don't configure SecurityComplianceMode, FIPS is used as the default value. Applicable values for this setting include:

- **None**. No compliance mode is enforced
- **FIPS**. FIPS cryptographic modules are used
- **SP800-52**. NIST SP800-52r1 compliance is enforced

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800
-52
```

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

SecurityAllowedTLSVersions. Specifies the TLS protocol versions that are accepted during protocol negotiation. This information is represented as an array and any combination of the possible values is supported. When this setting isn't configured, the values TLS10, TLS11, and TLS12 are used as the default values. Applicable values for this setting include:

- **TLS10**. Specifies that the TLS 1.0 protocol is allowed.
- **TLS11**. Specifies that the TLS 1.1 protocol is allowed.
- **TLS12**. Specifies that the TLS 1.2 protocol is allowed.
- **TLS13**. Specifies that the TLS 1.3 protocol is allowed.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -
array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. Improves the cryptographic authentication of the Citrix server and improves the overall security of the SSL/TLS connections between a client and a server. This setting governs the handling of a trusted root certificate authority (CA) while opening a remote session through SSL when using the client for OS X.

When you enable this setting, the client checks whether the server's certificate is revoked. There are several levels of certificate revocation list checking. For example, the client can be configured to check only its local certificate list, or to check the local and network certificate lists. In addition, certificate checking can be configured to allow users to log on only if all Certificate Revocation lists are verified.

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows admins to revoke security certificates (invalidated before their expiry date) if there is cryptographic compromise of certificate private keys, or unexpected changes in the DNS name.

Applicable values for this setting include:

- **NoCheck**. No Certificate Revocation List check is performed.
- **CheckWithNoNetworkAccess**. Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate Revocation List isn't critical for verification of the server certificate that presented by the target SSL Relay or Citrix Secure Web Gateway server.
- **FullAccessCheck**. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List isn't critical for verification of the server certificate presented by the target SSL Relay or Citrix Secure Web Gateway server.
- **FullAccessCheckAndCRLRequired**. Certificate Revocation List check is performed, excluding the root Certificate Authority. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.
- **FullAccessCheckAndCRLRequiredAll**. Certificate Revocation List check is performed, including the root certificate authority. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

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

> **Note:**
>
> If you don't set SSLCertificateRevocationCheckPolicy, FullAccessCheck is used as the default value.
>
> ```
> defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy
>  FullAccessCheckAndCRLRequired
> ```

Configuring TLS policies

To configure TLS settings on an unmanaged computer, run the **defaults** command in Terminal.app.

defaults is a command line application that you can use to add, edit, and delete app settings in an OS X preferences list file.

To change settings:

1. Open **Applications > Utilities \ > Terminal**.
2. In Terminal, run the command:

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

Where:

<name>: The name of the setting as described earlier.

<type>: A switch identifying the type of the setting, either -string or -array. If the setting type is a string, this setting can be omitted.

<value>: The value for the setting. If the value is an array and multiple values need to be specified, separate the values with a space.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -
array TLS11 TLS12
```

Reverting to the default configuration

To reset a setting back to its default:

1. Open **Applications > Utilities \ > Terminal**.
2. In Terminal, run the command:

```
defaults delete com.citrix.receiver.nomas <name>
```

Where:

<name>: The name of the setting as described earlier.

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

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Security settings

Security improvements and enhancements were introduced with Citrix Receiver for Mac version 12.3, including the following:

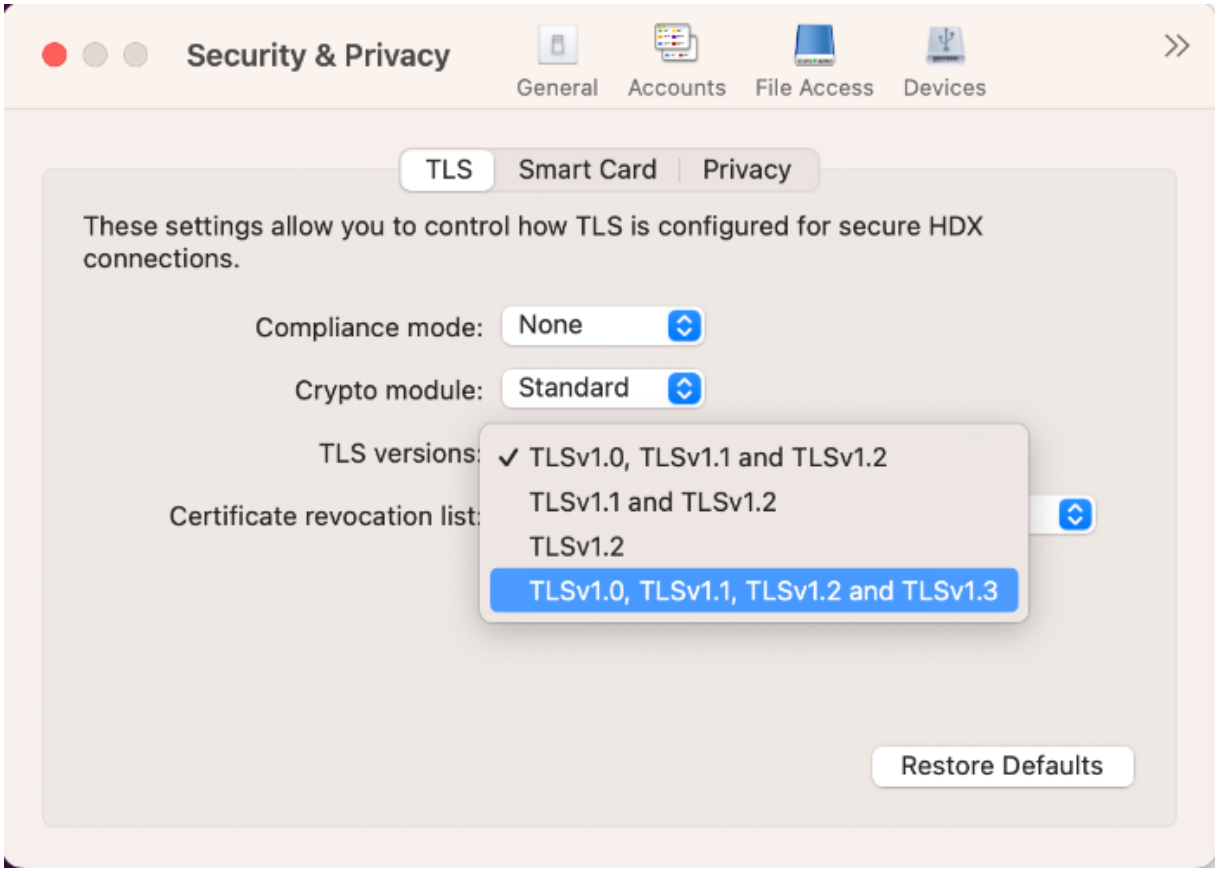
- improved security configuration user interface. In previous releases, the command line was the preferred method to make security-related changes. Configuration settings related to session security are now simple and accessible from the UI. This improvement improves the user experience while creating a seamless method for the adoption of security-related preferences.
- view TLS connections. You can verify connections that use a specific TLS version, encryption algorithms, mode, key size, and SecureICA status. In addition, you can view the server certificate for TLS connections.

The improved **Security and Privacy** screen includes the following new options in the **TLS** tab:

- set the compliance mode
- configure the crypto module
- select the appropriate TLS version
- select the certificate revocation list
- enable settings for all TLS connections

The following image illustrates the **Security and Privacy** settings accessible from the UI:

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



App experience

This section describes the following:

- Application delivery
- Enhanced virtual apps and desktops launch experience for Workspace (Cloud users only)
- App preferences
- Data collection and monitoring

Application delivery

When delivering applications with Citrix Virtual Apps and Desktops™ and Citrix DaaS, consider the following options to enhance the experience for your users when they access their applications:

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

Web access mode

Without any configuration, Citrix Workspace app for Mac provides web access mode: browser-based access to applications and desktops. Users simply open a browser to a Workspace for Web and select and use the applications that they want. In web access mode, no app shortcuts are placed in the App Folder on your user's device.

Self-service mode

Add a StoreFront account to Citrix Workspace app for Mac or configure Citrix Workspace app for Mac to point to a StoreFront site. Then, you can configure the self-service mode, which enables your users to subscribe to applications through Citrix Workspace app for Mac. This enhanced user experience is similar to that of a mobile app store. In self-service mode you can configure mandatory, auto-provisioned, and featured app keyword settings as needed. When one of your users selects an application, a shortcut to that application is placed in the App Folder on the user device.

When they access a StoreFront 3.0 site, your users see the Citrix Workspace app for Mac preview.

When publishing applications on your Citrix Virtual Apps farms, you can enhance the experience for users accessing those applications through StoreFront stores. Ensure that you include meaningful descriptions for the published apps. The descriptions are visible to your users through Citrix Workspace app for Mac.

Configure self-service mode

As mentioned previously, you can add a StoreFront account to Citrix Workspace app for Mac or configure Citrix Workspace app for Mac to point to a StoreFront site. Thus, you can configure the self-service mode, which allows users to subscribe to applications from the Citrix Workspace app for Mac user interface. This enhanced user experience is similar to that of a mobile app store.

In self-service mode, you can configure mandatory, auto-provisioned, and featured app keyword settings as needed.

- Automatically subscribe all store users to an app by appending the string '**KEYWORDS:Auto**'to the app description when publishing it in Citrix Virtual Apps. The app is provisioned automatically without requiring a manual subscription when users log in to the store.
- Advertise applications to users or make commonly used applications easier to find by listing them in the Citrix Workspace app for Mac Featured list. To list apps in the Mac Featured list, append the string `**KEYWORDS:Featured**` to the app description.

For more information, see StoreFront documentation.

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

Managing display of app shortcuts on Mac Launchpad

Starting with version 2503, admins now have greater control over the visibility of favorite app shortcuts on the Mac Launchpad.

Key enhancements:

- Admins can prevent subscribed applications from appearing on the Launchpad of Mac end users.
- Greater flexibility for admins to manage the visibility of app shortcuts on Mac devices.

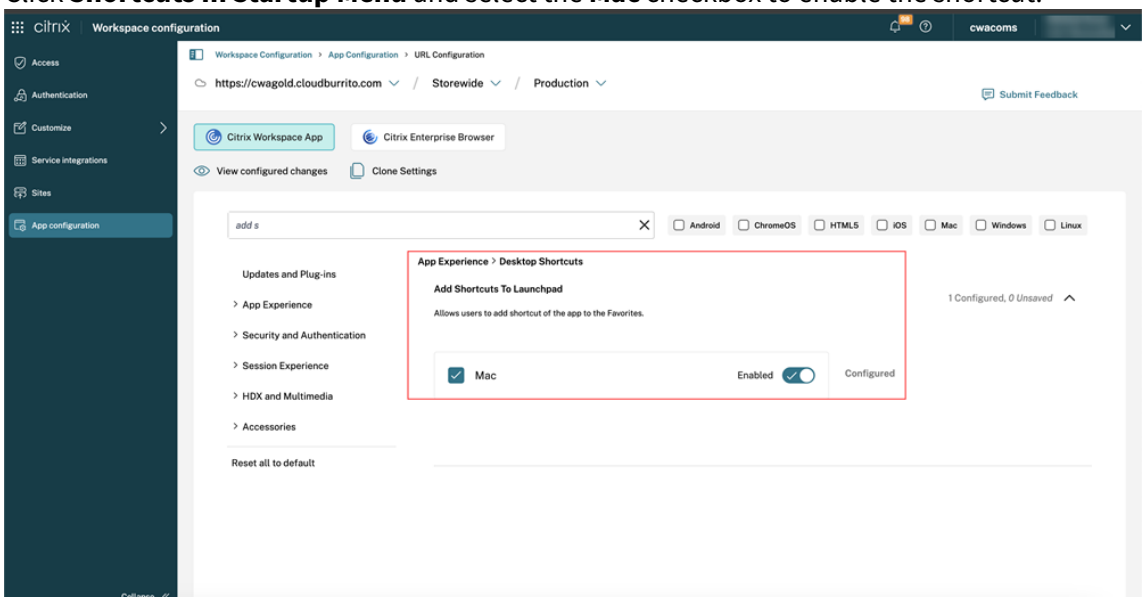
You can configure this feature using Global App Configuration service (GACS) and Mobile Device Management (MDM):

Using MDM:

```
<key>AddShortcutsToLaunchPad</key>
```

Using GACS:

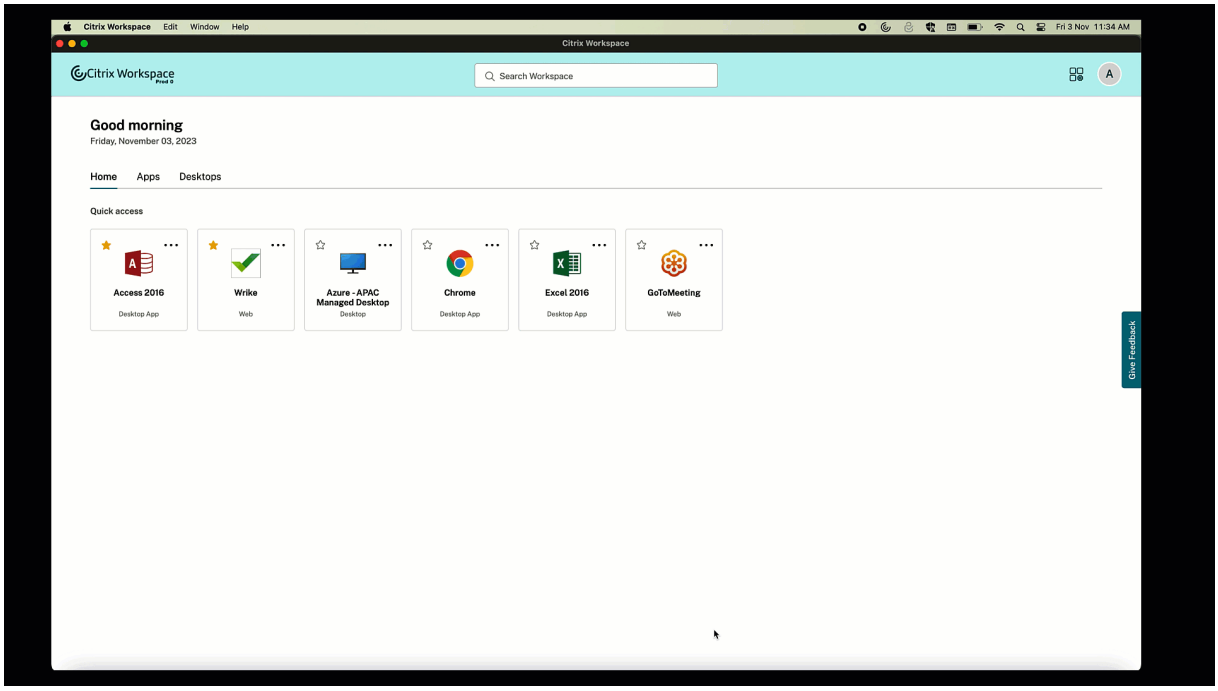
1. Navigate to **Workspace Configuration** > **App Configuration** > **Configure** in Citrix Cloud.
2. In **Citrix Workspace™ app** page, click **App Experience** > **Desktop Shortcuts**.
3. Click **Shortcuts In Startup Menu** and select the **Mac** checkbox to enable the shortcut.



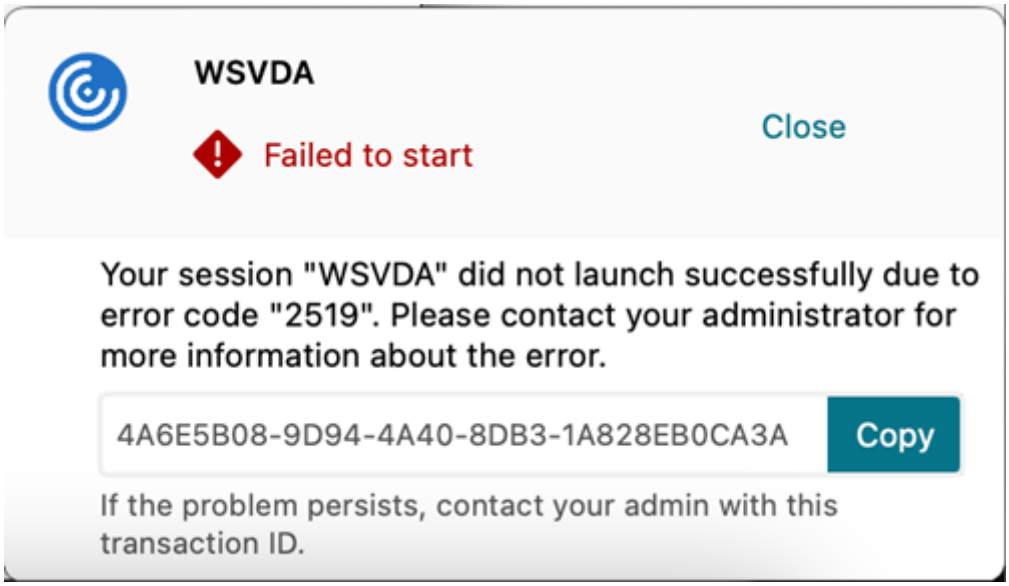
Enhanced virtual apps and desktops launch experience for Workspace

The opening experience of Citrix® resources has been enhanced to be more intuitive, informative, and user-friendly. From the 2311 version, this feature is supported for custom web stores and hybrid launch.

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



The launch progress notification now appears at the lower-right corner of your screen. A progress status of the resources, which are in the process of being opened is shown. You cannot retrieve the notification once you dismiss it. The notification stays for a few seconds from the time you start the session. If the session fails to start, then the notification shows the failure message.



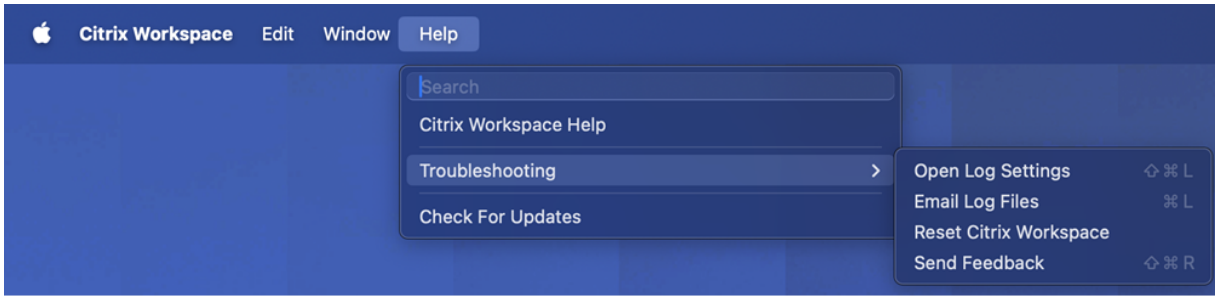
This feature is supported on cloud, on-premises and custom web portals deployments.

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

App preferences

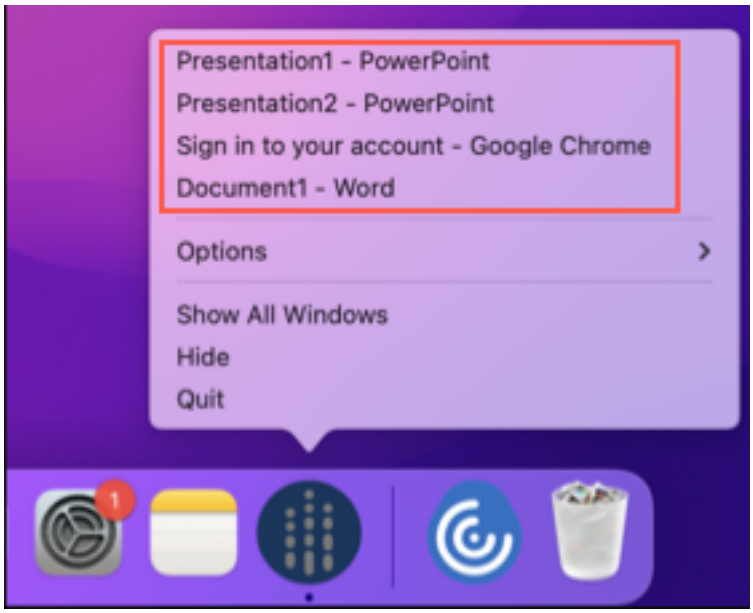
Enhanced structure for Help menu

Starting with version 2503, Citrix Workspace™ app for Mac introduces a restructured **Help** menu to improve usability. Troubleshooting options, such as **Open Log Settings** and **Reset Citrix Workspace**, have been moved to a dedicated **Troubleshoot** submenu. This change makes the **Help** menu cleaner and easier for users to navigate.



Opened apps appear in the dock with native app icons

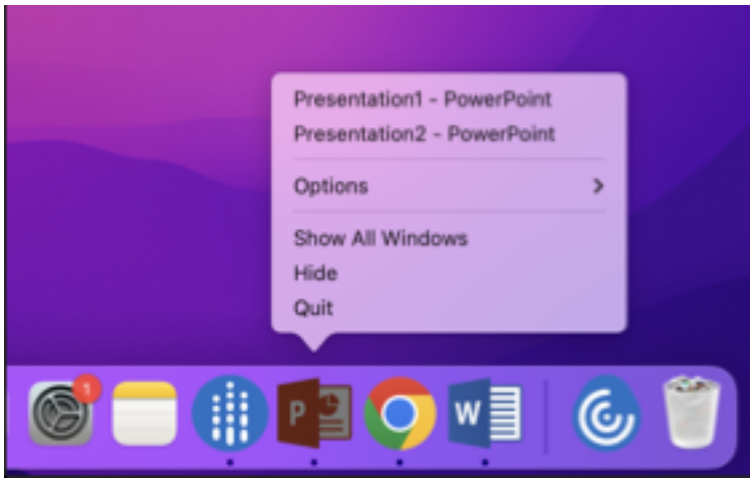
Previously, clicking virtual apps in the Citrix Workspace app triggered the **Citrix Viewer** where these apps would be available. If you open many apps, the apps or its instances are opened in the **Citrix Viewer**. You can view the open apps by right-clicking the **Citrix Viewer** icon.



Starting with the 2305 version, when you open virtual apps, they appear in the Dock (bottom-right corner of the screen) with their respective icons and are easily identifiable. You can then access the

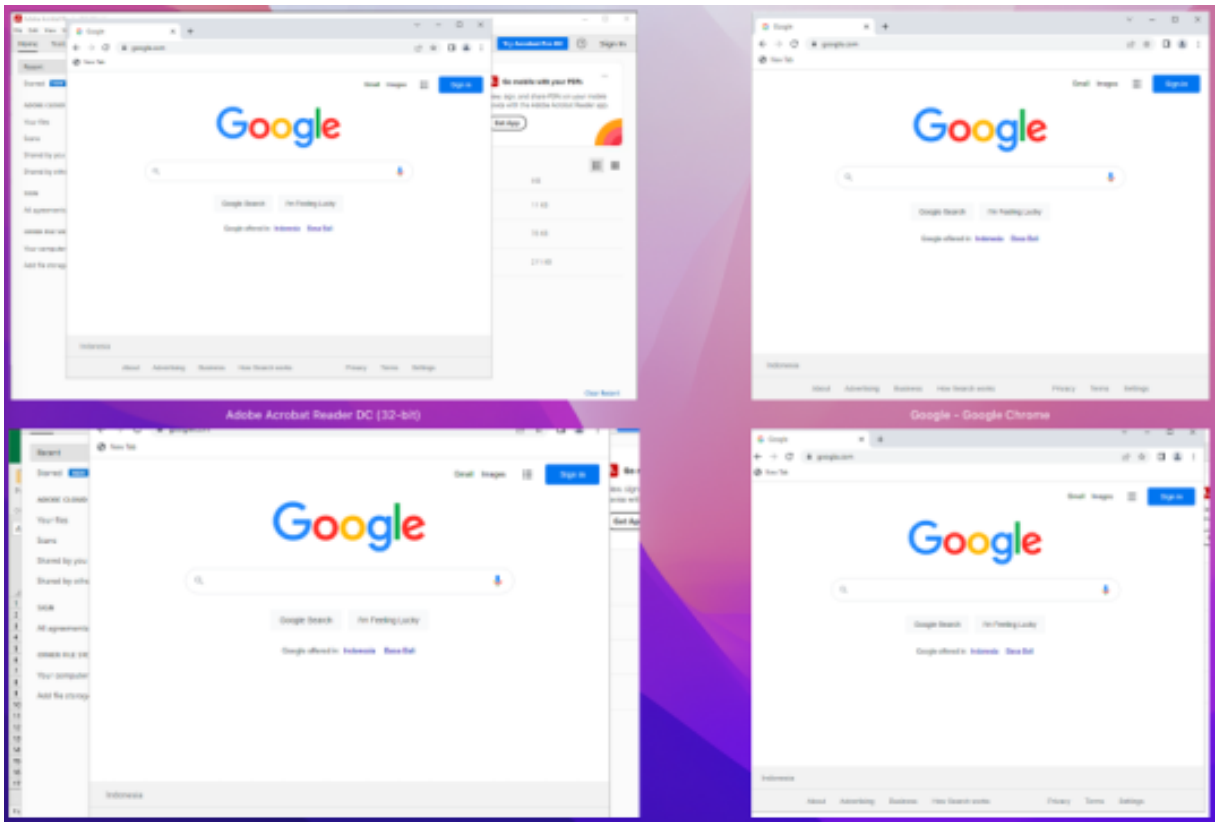
© 1997–2026 Citrix Systems, Inc. All rights reserved.

virtual app from the dock itself. If you open multiple instances of an app, these instances aren't duplicates in the Dock but are grouped within one instance in the Dock.



Improved Mission Control and App Expose experience

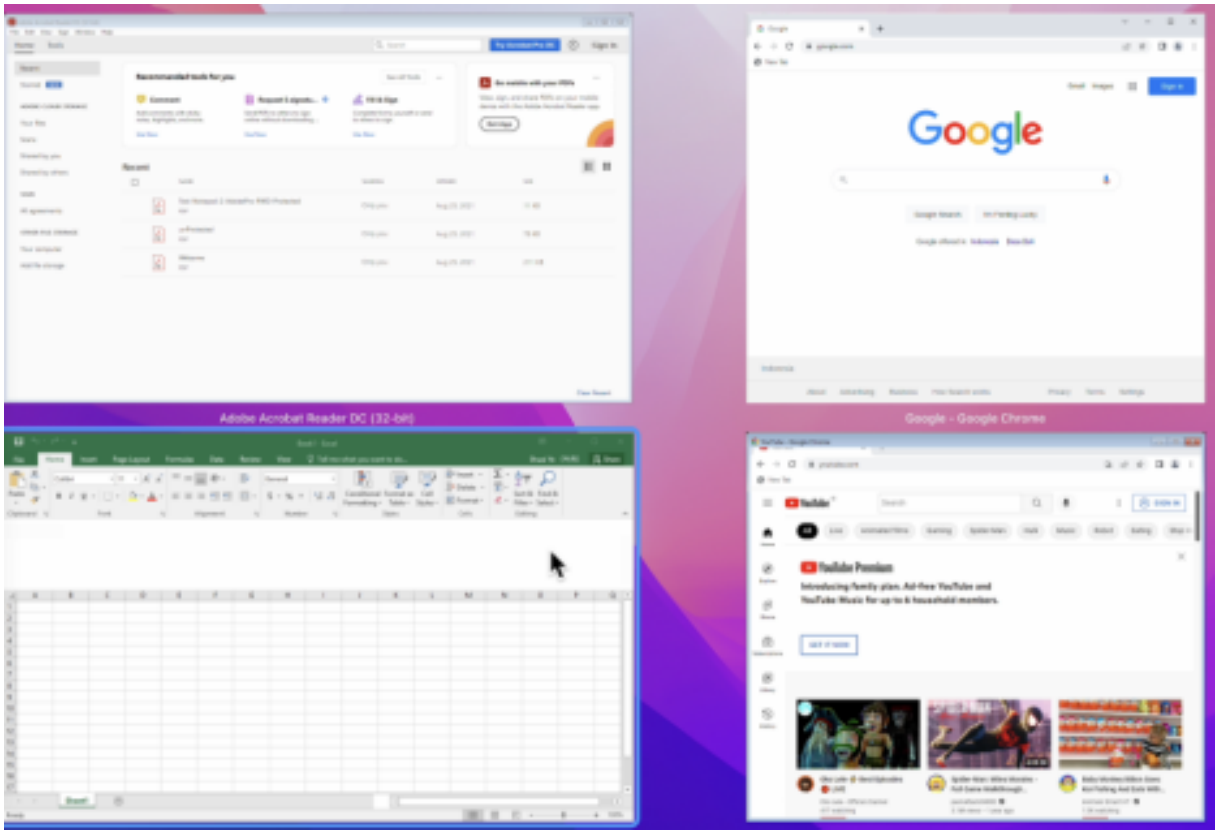
Previously, using the **Mission Control** or **App Expose** feature in a virtual app session resulted in the overlapping of many windows that were opened.



Starting with the 2210 version, when you use the **Mission Control** or **App Expose** feature in a virtual

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

app session and open many windows, the windows do not overlap, and you can easily choose from among them.



Enhanced menu bar support

Starting with the 2301 version, the CWA fully supports the **Automatically hide and show the menu bar in full screen** option in macOS. For versions earlier than macOS 13, you must navigate to **System Preferences > Dock & Menu Bar** and clear the **Automatically hide and show the menu bar in full screen** option. For macOS 13 and later versions, you must navigate to **System Preferences > Desktop & Dock** and clear the **Automatically hide and show the menu bar in full screen** option. You have the provision to either enable or disable this option. This enhancement also supports high DPI scaling. The mouse position also appears accurate in all the external monitors connected.

The following figure illustrates a window where the menu bar is hidden:



The following figure illustrates a window where the menu bar appears:

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

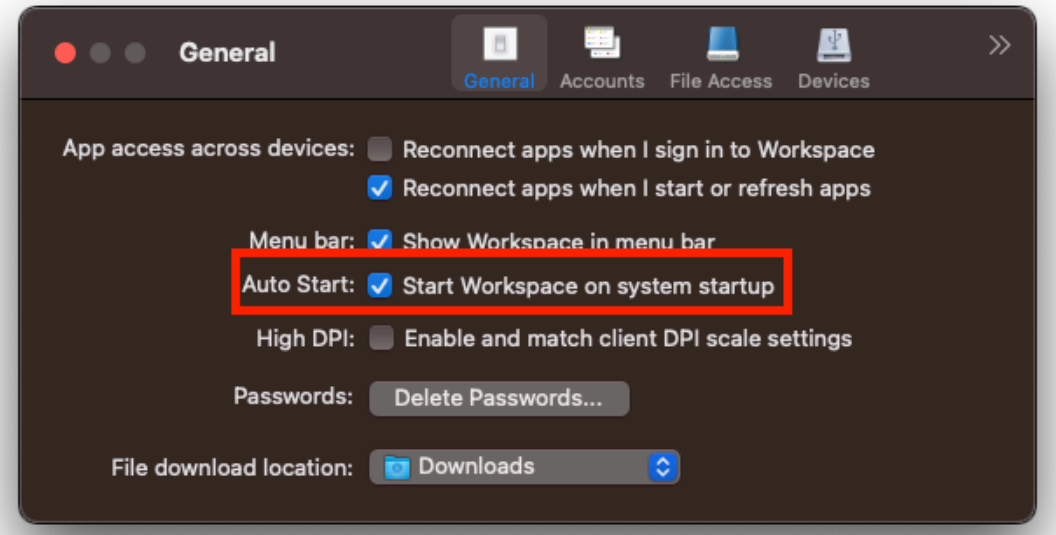


Support for horizontal scroll

Previously, Citrix Workspace app for Mac supported only vertical scroll on a trackpad. Starting with the 2305 version, a horizontal scroll is also supported.

Enhanced auto start experience

Previously, Citrix Workspace app for Mac used to start automatically whenever a computer was turned on. Starting with the 2304 version, you can choose to disable or enable the auto start feature on Citrix Workspace app for Mac by navigating to **Preferences > General > Start Workspace** on system startup. The auto start setting is enabled by default.



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

Workspace Control

Workspace Control lets desktops and applications follow users as they move between devices. For example, clinicians in hospitals to move from workstation to workstation without having to restart their desktops and applications on each device.

Policies and client drive mappings change appropriately when you move to a new user device. Policies and mappings are applied according to the user device where you're currently logged on to the session. For example, a healthcare worker can sign out from a device in the emergency room and sign-in to a workstation in the X-ray laboratory. The policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session in the X-ray laboratory.

To configure workspace Control settings

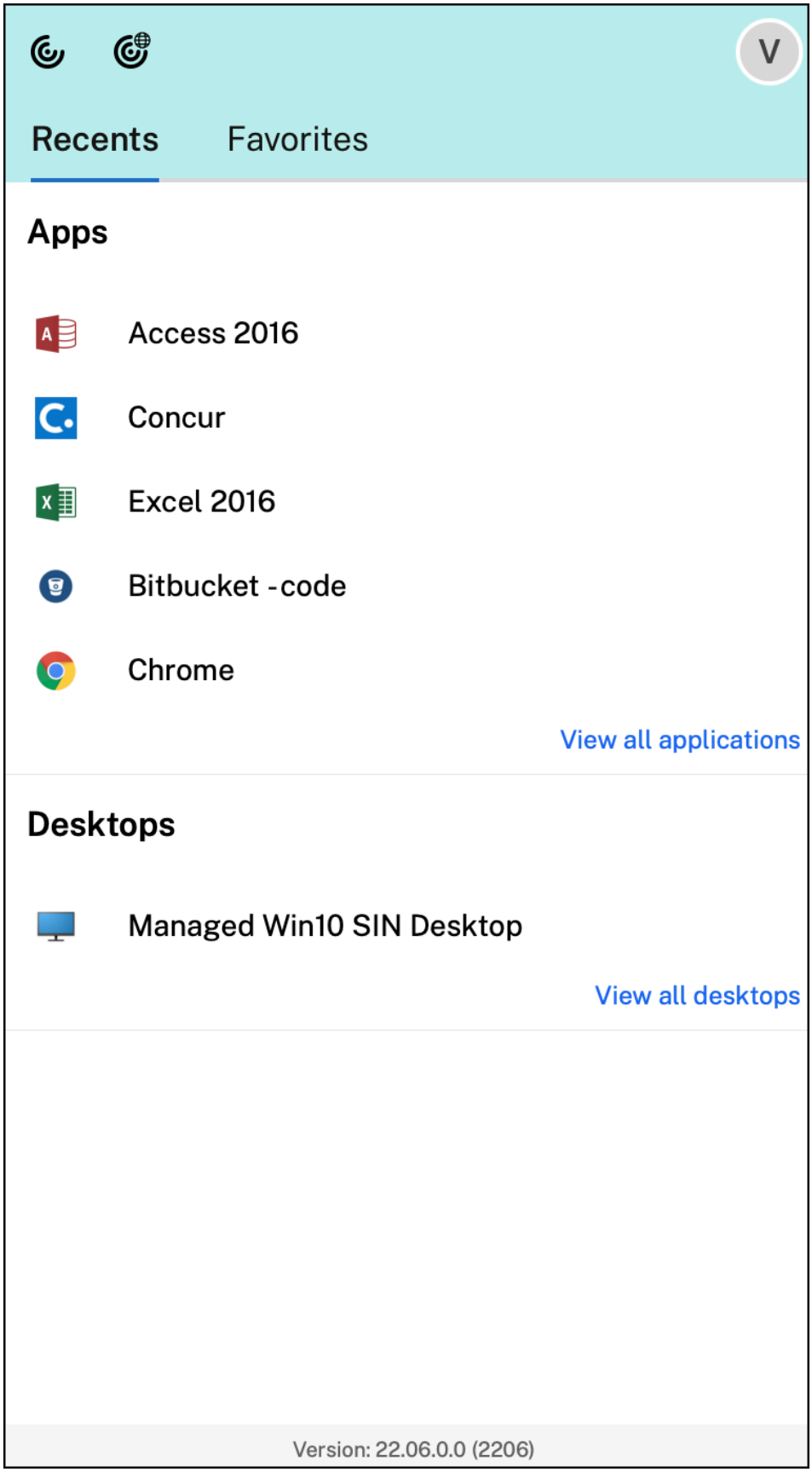
1. Click the down arrow icon in the Citrix Workspace app for Mac window and choose **Preferences**.
2. Click the **General** tab.
3. Choose one of the following:

    - Reconnect apps when I start Citrix Workspace app. Allows users to reconnect to disconnected apps when they start Citrix Workspace app.
    - Reconnect apps when I start or refresh apps. Allows users to reconnect to disconnected apps either when they start apps or when they select Refresh Apps from the Citrix Workspace app for Mac menu.

View apps, desktops, and Citrix Enterprise Browser from the menu bar through a quick access menu

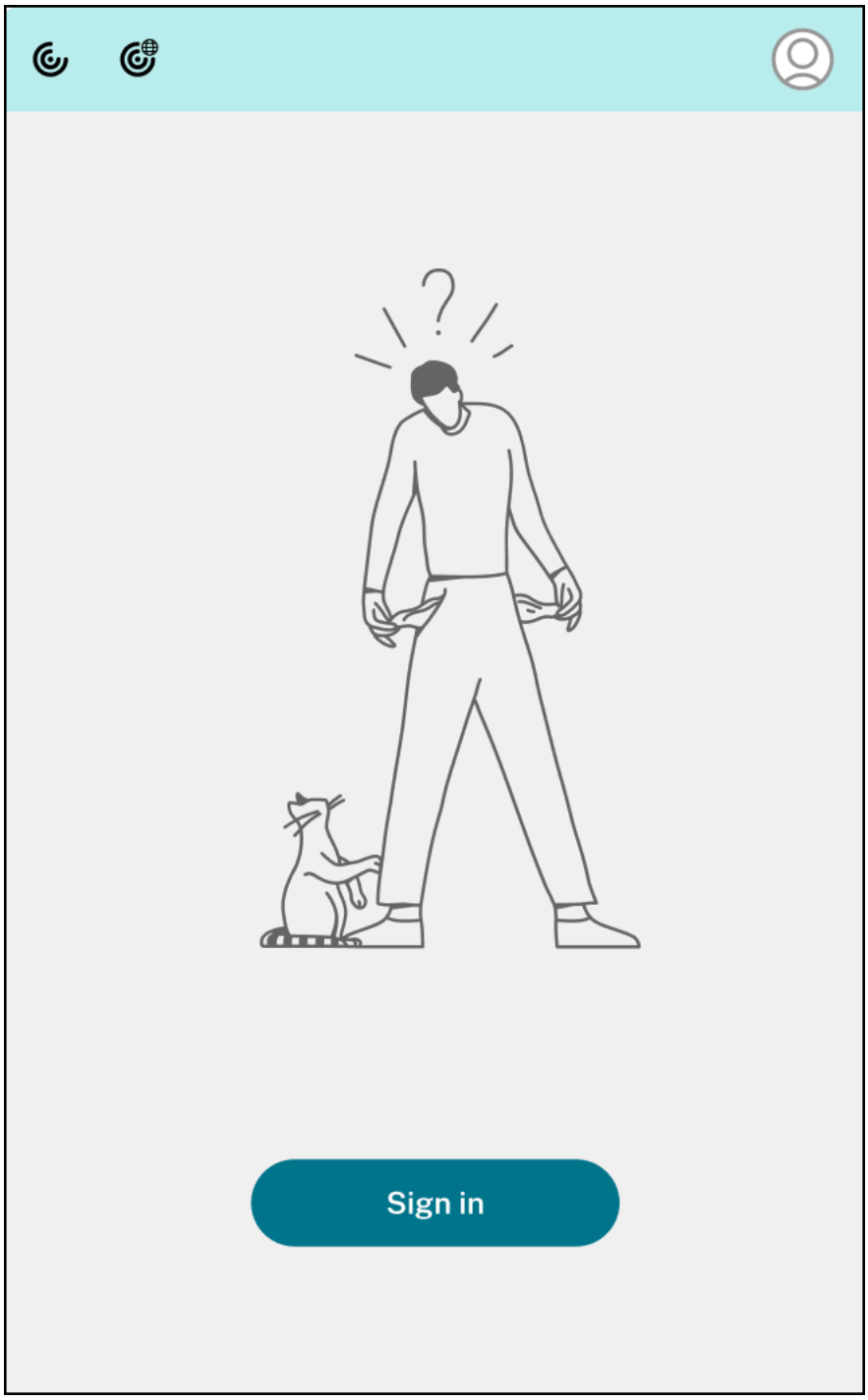
You can now view your most recently used or favorite apps and desktops or open a Citrix Enterprise Browser window by clicking the Citrix Workspace icon in the menu bar. This feature provides easy access to some of your resources without having to open the Citrix Workspace app.

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



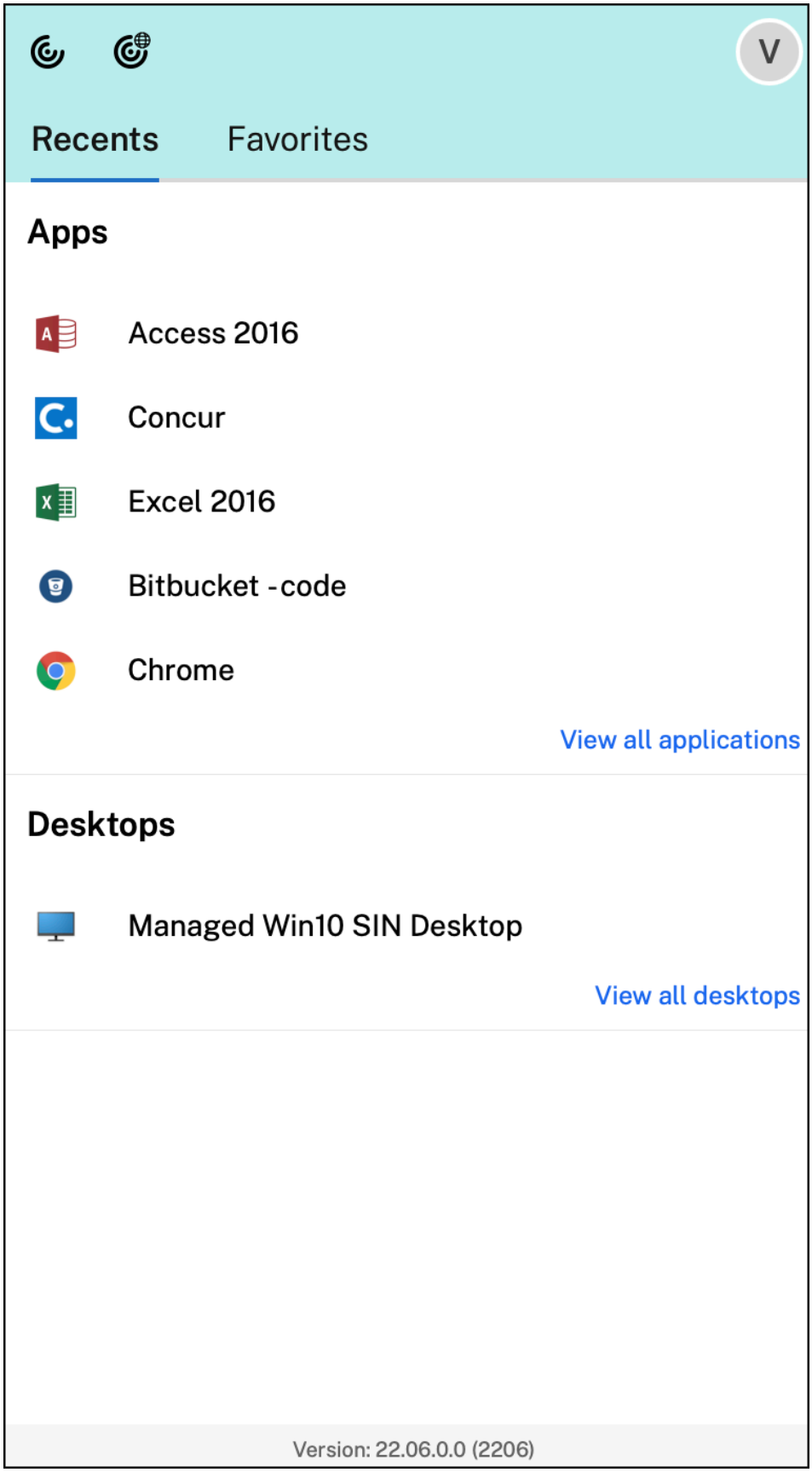
© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you've not configured any accounts, a sign-in prompt appears.



A maximum of 5 of your recently used or favorite apps or desktops appear in the options under the **Recent** and **Favorites** tabs respectively. To view the other apps in the Citrix Workspace app, click **View all applications**. To view the other desktops in the Citrix Workspace app, click **View all desktops**.

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



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

You can open the Citrix Workspace UI by clicking the Citrix Workspace app icon.

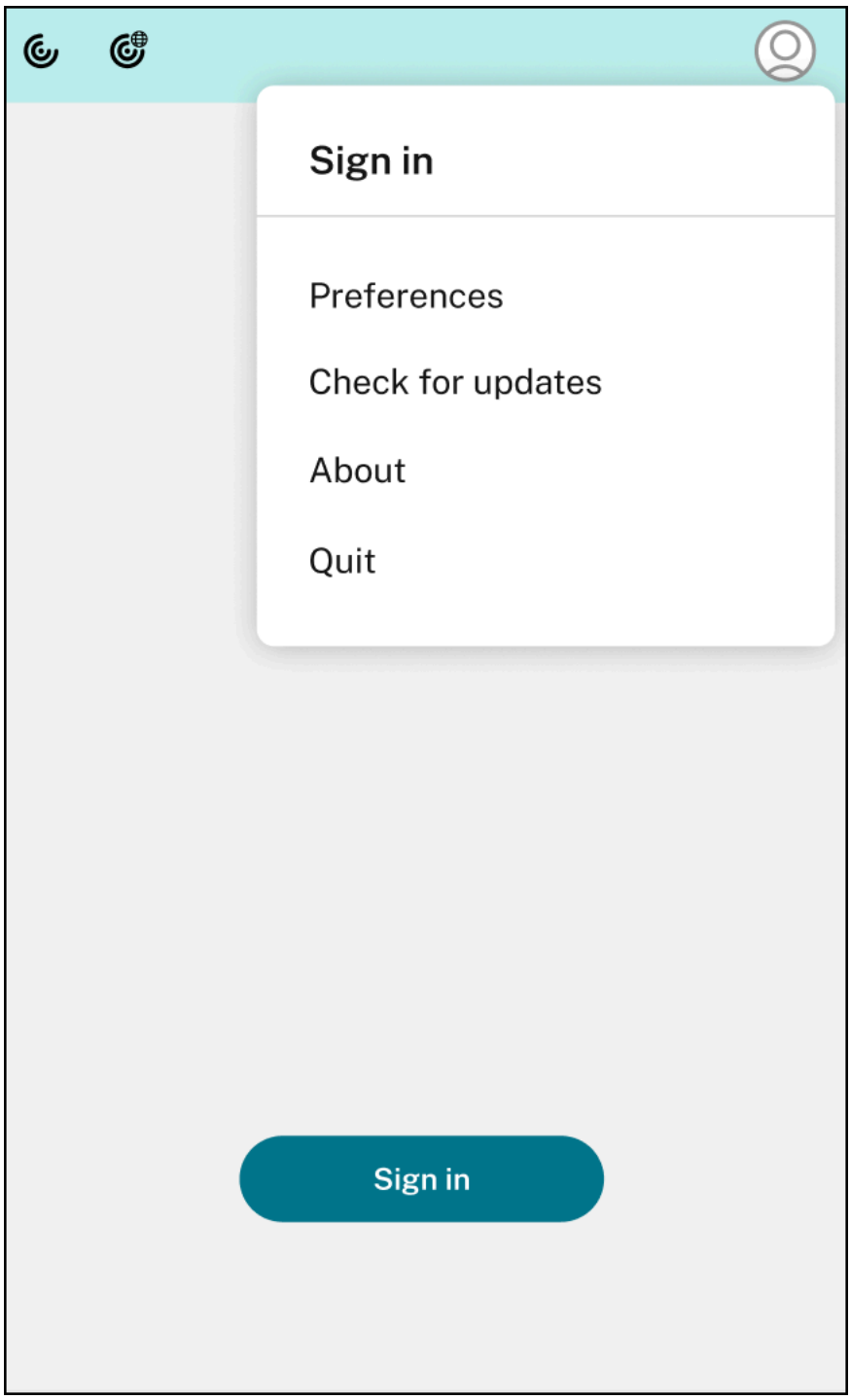


You can open the Citrix Enterprise Browser, without opening a web or SaaS app by clicking the Citrix Enterprise Browser icon.



> **Note:**
>
> The Citrix Enterprise Browser isn't available if the configured store doesn't have any web or SaaS apps. Further, it's available only if your admin has configured Citrix Secure Private Access.

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



You can view the following options when you click the **Account** icon in the top-right corner:

- Preferences
- Check for updates
- About
- Quit

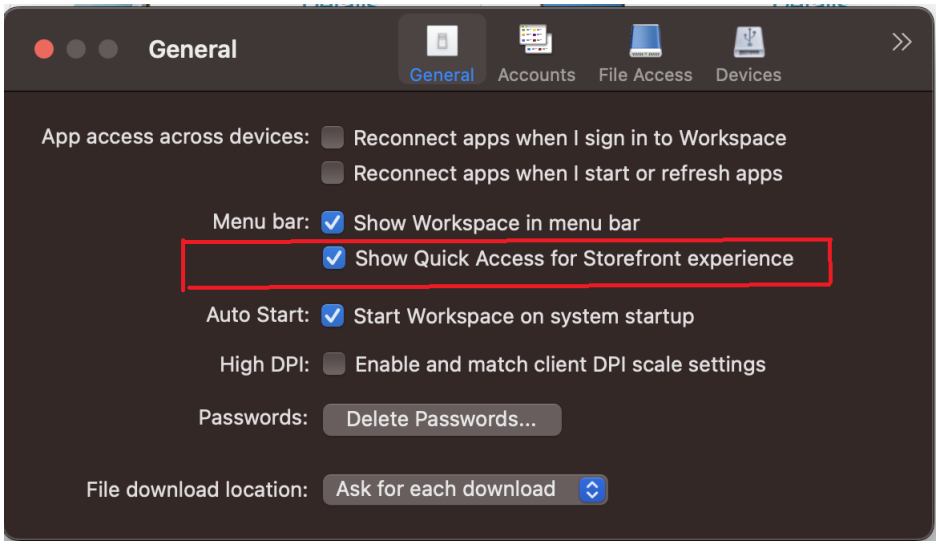
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quick access menu for StoreFront

Starting with the 2307 version, you can navigate to your favorite apps and desktops quickly and easily using the quick access feature for on-premises stores. To enable quick access, right-click **Citrix Workspace** in the toolbar, navigate to **Preferences > General**, and then select **Show Quick Access for Storefront experience**. This feature allows you to see your favorite data directly from the Mac menu bar.



You can enable the quick access feature by using **Preferences**.



Administrators can enable or disable the quick access feature by using the Mobile Device Management (MDM) or Global App Configuration service (GACS) methods.

Enabling or disabling quick access using MDM

To enable quick access through MDM, administrators must use the following settings:

```
<key>ShowQuickAccessForStoreFront</key>
<false/>
```

For more information on how to use MDM, see Mobile Device Management.

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

Enabling or disabling quick access using GACS

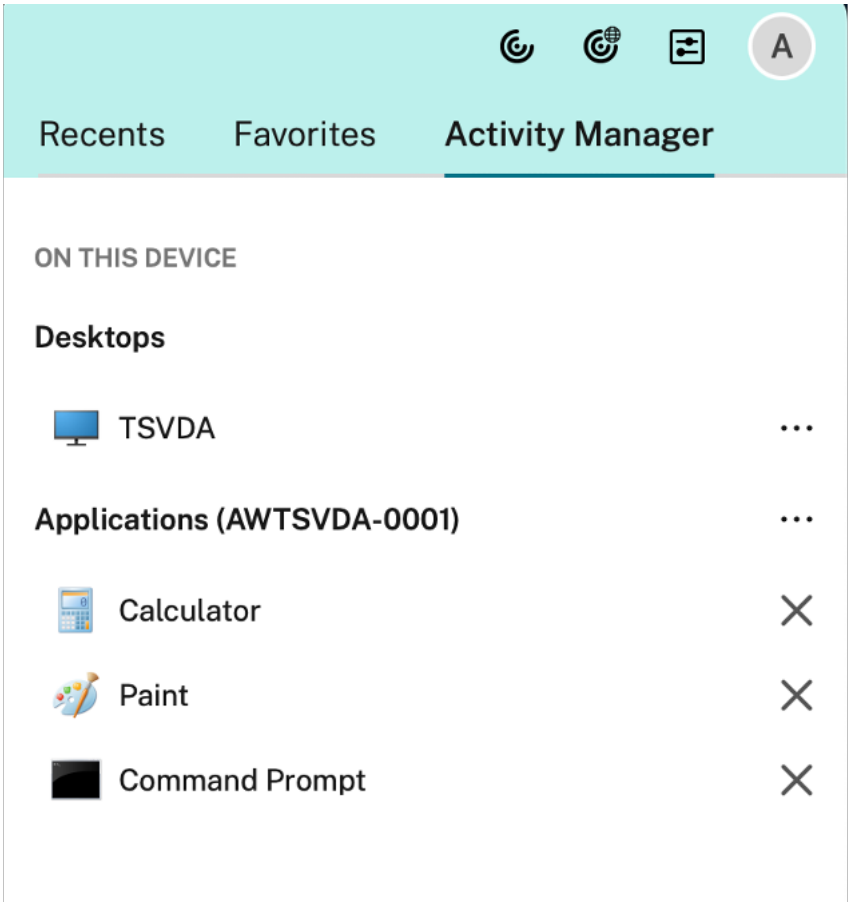
To enable quick access through GACS, administrators must use the following settings:

```
enableQuickAccessForStoreFront
```

Support for Activity Manager on the quick access menu for cloud stores

Starting with the version 2405, Citrix Workspace app for Mac supports the Activity Manager feature. This feature lets end users view and interact with all their active apps and desktop sessions at one place. You can disconnect or terminate the active sessions directly from the Activity Manager.

To view active sessions in the Activity Manager, select the Citrix Workspace app icon from the menu bar and then click **Activity Manager**.



You can perform the following actions on the active desktop sessions by clicking the respective ellipsis(…) button.

- **Disconnect**: The remote session is disconnected, but the apps and desktops are active in the background.

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

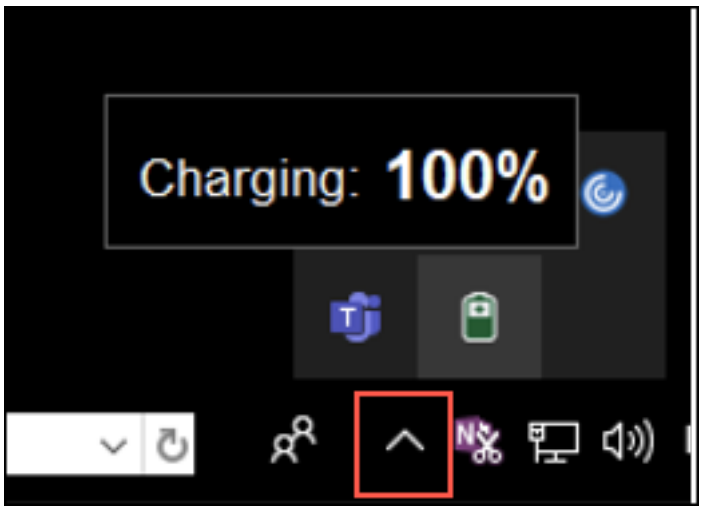
- **Log out**: Logs out from the current session. All the apps in the sessions are closed, and any unsaved files are lost.
- **Shut Down**: Closes your disconnected desktops.
- **Force Quit**: Forcefully powers off your desktop in case of a technical issue.
- **Restart**: Shuts down your desktop and starts it again.

For active seamless app session, you can terminate the app session by clicking the close (X) button.

For more information, see Activity manager.

Battery status indicator

The battery status of the device now appears in the notification area of a Citrix Desktop session. To view the battery status within the desktop session, click the **Show hidden icons** arrow in the taskbar.



> **Note:**
>
> The battery status indicator does not appear for server VDAs.

Citrix Casting™

Citrix Casting is used to cast your Mac screen to nearby Citrix Ready workspace hub devices. Citrix Workspace app for Mac supports Citrix Casting to mirror your Mac screen to workspace hub connected monitors.

For more information, see the Citrix Ready workspace hub documentation.

Prerequisites

- Latest supported version of Citrix Workspace app.

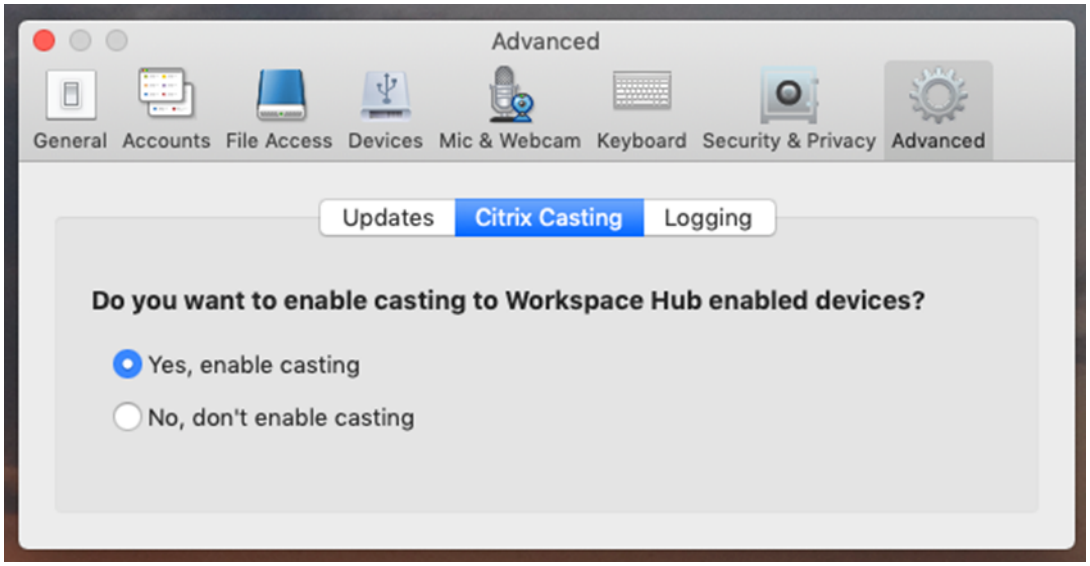
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bluetooth enabled on the device for hub discovery.
- Both Citrix Ready workspace hub and Citrix Workspace app must be on the same network.
- Ensure Port 55555 isn't blocked between the device running Citrix Workspace app and the Citrix Ready workspace hub.
- Port 55556 is the default port for SSL connections between mobile devices and the Citrix Ready® workspace hub. You can configure a different SSL port on the Raspberry Pi's settings page. If the SSL port is blocked, users can't establish SSL connections to the workspace hub.
- For Citrix Casting, ensure port 1494 isn't blocked.

Enable Citrix Casting

Citrix Casting is disabled by default. To enable Citrix Casting using Citrix Workspace app for Mac:

1. Go to **Preferences**.
2. Select **Advanced** in the panel and then choose **Citrix Casting**.
3. Select **Yes, enable casting**.



A notification appears when Citrix Casting is launched and a Citrix Casting icon appears in the menu bar.

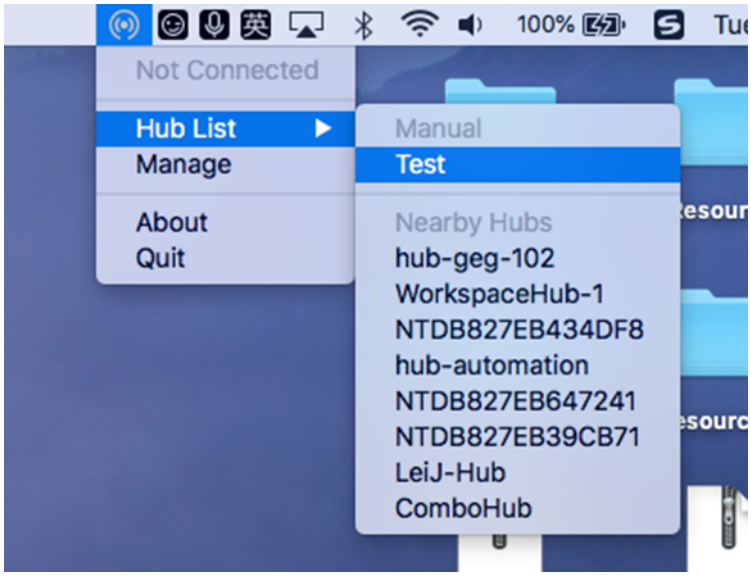
> **Note:**
>
> After enabling, Citrix Casting launches with Citrix Workspace app for Mac automatically every time until you disable it by selecting **No, don't enable casting** in **Preferences > Advanced > Citrix Casting**.

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

Discover workspace hub devices automatically

To connect to workspace hubs automatically:

1. On your Mac, sign in to Citrix Workspace app and ensure that Bluetooth is turned on. Bluetooth is used to discover nearby workspace hubs.
2. Select the **Citrix Casting** icon in the menu bar. All Citrix Casting functions are operated through this menu.
3. The **Hub List** submenu shows all nearby workspace hubs on the same network. Hubs are listed in descending order by their proximity to your Mac and display their workspace hub configured names. All automatically discovered hubs display under **Nearby Hubs**.
4. Choose the hub that you want to connect to by selecting its name.



To cancel selection of a workspace hub during connection, select **Cancel**. You can also use **Cancel** if the network connection is poor and connecting is taking longer than usual.

> **Note:**
>
> Occasionally, your chosen hub might not appear in the menu. Check the **Hub List** menu again after a few moments or add your hub manually. Citrix Casting receives the workspace hub's broadcasting periodically.

Discover workspace hub devices manually

If you can't find the Citrix Ready workspace hub device in the **Hub List** menu, add the workspace hub's IP address to access it manually. To add a workspace hub:

1. On your Mac, sign in to Citrix Workspace app and ensure that Bluetooth is turned on. Bluetooth is used to discover nearby workspace hubs.

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

2. Select the **Citrix Casting** icon in the menu bar.
3. Select **Manage** in the menu. The **Manage hubs** window appears.
4. Click **Add new** to enter the IP address of your hub.
5. After successfully adding the device, the **Hub name** column displays the hub's friendly name. Use this name to identify the hub in the **Manual** section of the **Hub List** submenu.

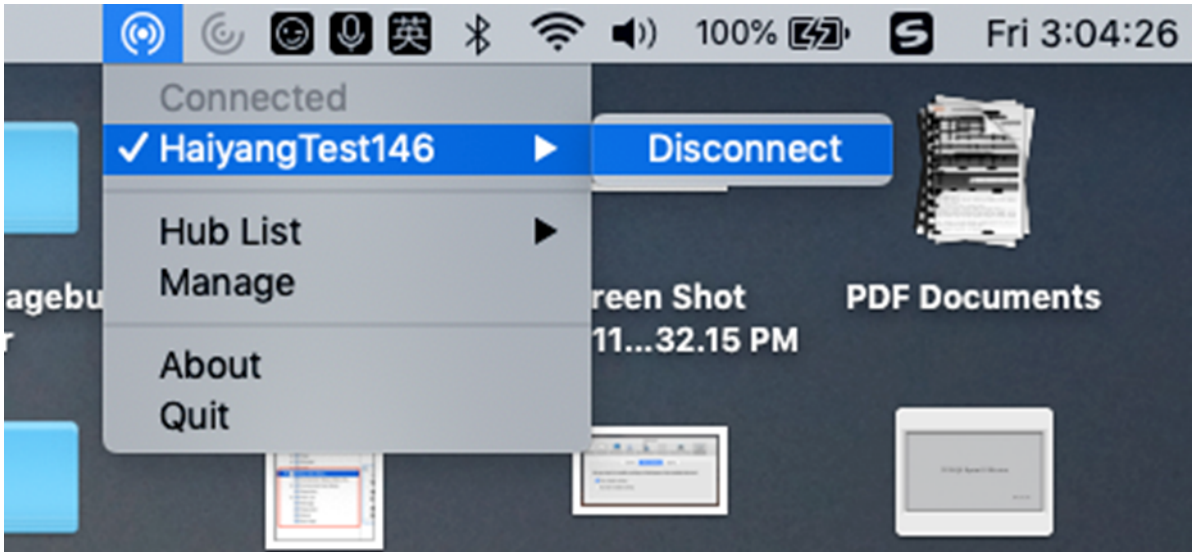
> **Note:**
>
> Currently, only **Mirror** mode is supported. **Mirror** is the only available choice in the **Display Mode** column.

Disconnect the workspace hub device

You can disconnect your current session and exit the Citrix Ready workspace hub automatically or manually.

- To disconnect the screen casting session automatically, close your laptop.
- To disconnect the screen casting session manually:

1. Select the **Citrix Casting** icon.
2. In the list of hubs, select the name of your workspace hub. The **Disconnect** option appears to the right.
3. Select **Disconnect** to exit the hub.



Known issues

- There are small latency issues when viewing the mirrored screen. In poor network conditions, latency might be even longer.

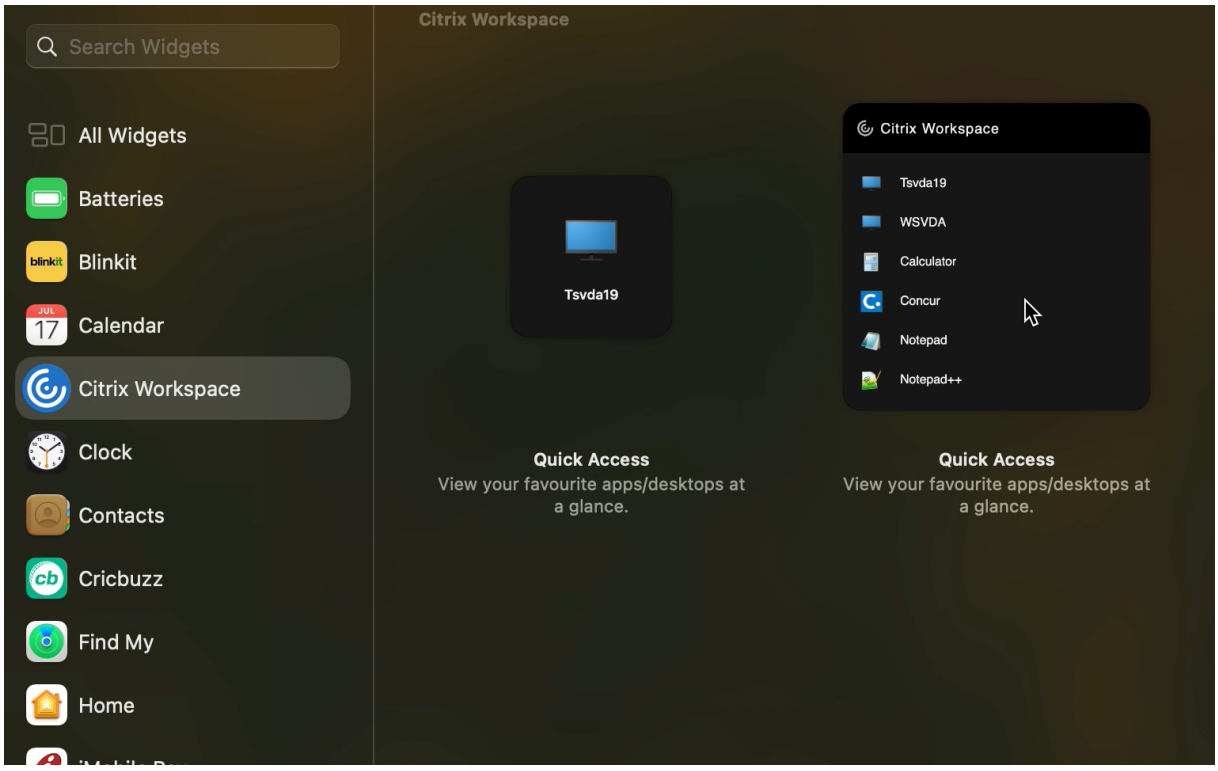
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When SSL is enabled in a Citrix Ready workspace hub and the hub's certificate isn't trusted, an alert window appears. To solve the issue, add the certificate to your trusted certificate list with the Keychain tool.

Support for Citrix Workspace widgets

Starting with the 2405 version, Citrix Workspace app for Mac supports widgets for quick access to its virtual apps and desktops. With this feature, you can easily access your favorite virtual apps and desktops from the widget that is added to your desktop or Notification centre.

Citrix Workspace supports two types of widgets, small and large widgets. The small widget can hold either one virtual app or desktop. The large widget can hold six favorite virtual apps and desktops with desktop listed at first.



For Citrix Workspace app installed on macOS Sonoma, you can add the Citrix Workspace widgets to the desktop screen. For Citrix Workspace app installed on macOS Ventura and earlier versions, you can add the Citrix Workspace widgets to Notification centre.

To add Citrix Workspace widgets, do the following steps:

1. On the macOS Sonoma devices, right-click on the wallpaper, then choose **Edit Widgets**. On the devices running on macOS Ventura or earlier version, open **Notification Centre** and click the **Edit Widgets** at the bottom of **Notification Centre**.

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

2. In the widget gallery, search for **Citrix Workspace**. Or click **Citrix Workspace** from the list to view its available widgets.
3. Drag the small or large widgets onto the desktop or **Notification Centre** as required.

Data collection and monitoring

Citrix Analytics

Citrix Workspace app is instrumented to securely transmit logs to Citrix Analytics. The logs are analyzed and stored on Citrix Analytics servers when enabled. For more information about Citrix Analytics, see Citrix Analytics.

Customer Experience Improvement Program (CEIP)

What is the Citrix Customer Experience Improvement Program (CEIP) for Citrix Workspace app?

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 Mac uses Citrix Analytics to collect the CEIP data.

Data collected

The specific CEIP data elements collected by Citrix Analytics are:

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

Operating System Version*	Citrix Workspace app version*	Generic USB Redirection Usage	Store configuration
Citrix Enterprise Browser Usage	Citrix Virtual Apps and Desktops Session Launch Status	Auto-update preference	Auto-update Status
Session launch method	Uninstall information	Inactivity Timeout Feature Usage	Email Discovery Feature Usage
Custom Web Store Feature Usage	Reconnection preferences	Global App Configuration service Usage	Restore Keyboard Usage
Delete Password Feature Usage	Auto-update channel	Connection Lease Details	USER GUID

> **Note:**
>
> You can stop sending CEIP data except for the operating system and Citrix Workspace™ app versions collected for Citrix Analytics indicated by an * in the preceding table.

Which users is CEIP data collected from?

The Citrix Workspace app collects the CEIP data via Citrix Analytics that is configured to include users from all regions. To ensure that this functionality is in place, update to the most recent version of Citrix Workspace app.

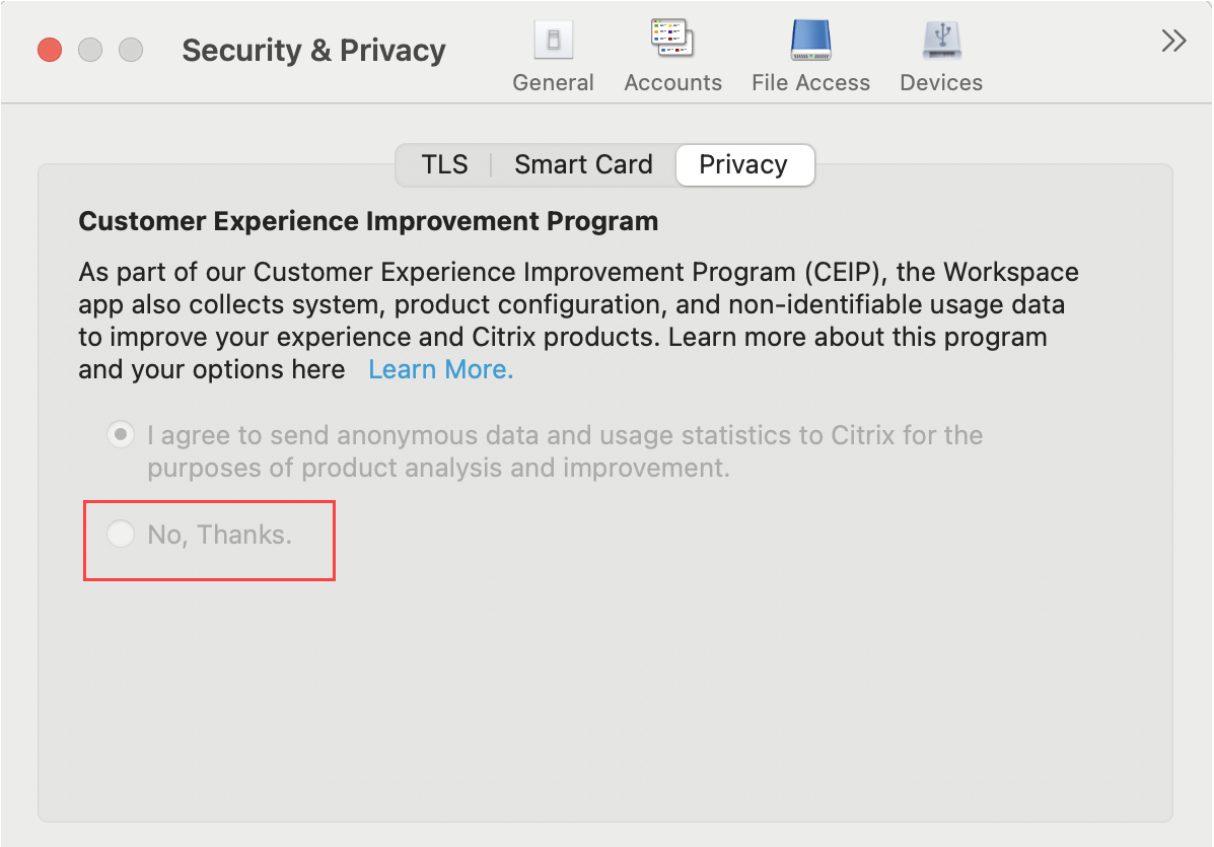
Can users and administrators disable CEIP data collection?

CEIP data collection can be fully disabled in all jurisdictions as per the following configuration.

Starting with version 2205, you can stop sending CEIP data (except for two data elements - Operating System version and Citrix Workspace app version) by using the following steps:

1. On the **Preferences** window, select **Security and Privacy**.
2. Click the **Privacy** tab.
3. Select **No, Thanks** to disable CEIP participation.

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



Alternatively, you can disable CEIP by running the terminal command:

```
defaults write com.citrix.receiver.nomas CEIPEnabled -bool NO
```

To disable CEIP using MDM tools, refer to the schema here and set the following:

```
<key>CEIPEnabled</key> to <false/>
```

Additional Information

Citrix handles your data in accordance with the terms of your contract with Citrix. Your data is protected, according to the Citrix Services Security Exhibit available at the Citrix Trust Center.

HDX™ and multimedia

This section describes about the HDX and multimedia features for the following components:

- Graphics and Display
- Optimized Microsoft Teams
- HDX transport
- HDX Direct V1

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

Browser Content Redirection

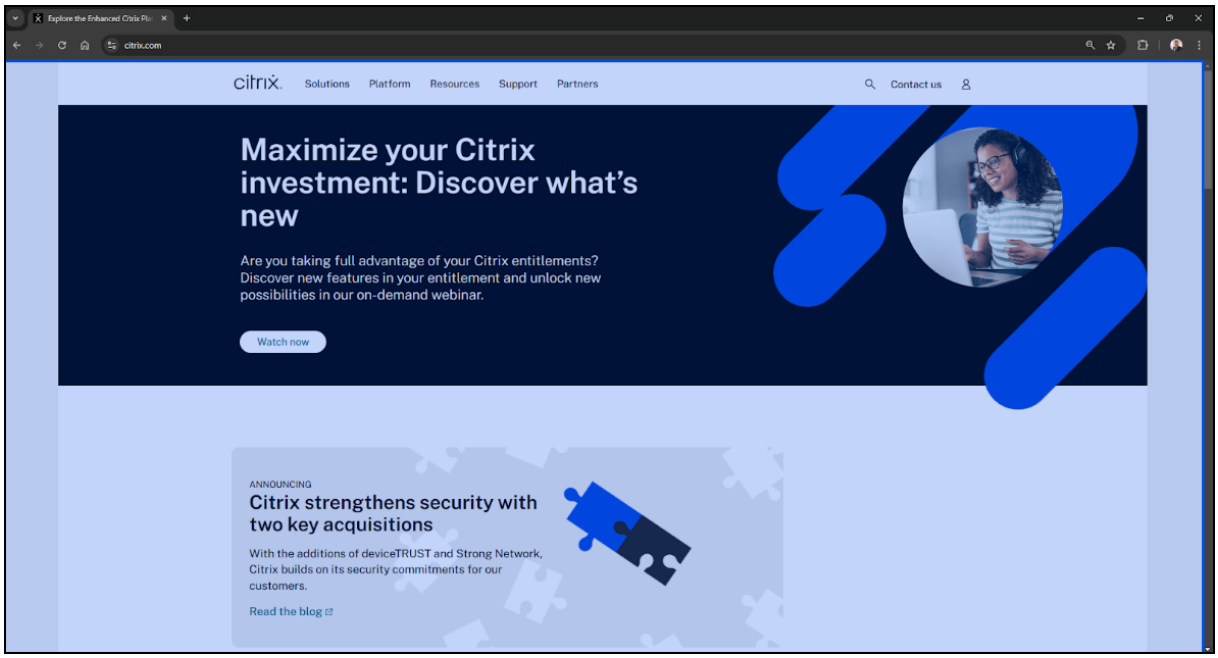
Browser Content Redirection (BCR) enhances the user experience of web browsing within Citrix Virtual Apps and Desktops™ environments. By offloading the rendering of webpages to the user's local machine, BCR reduces server load and improves performance, for complex or resource-intensive websites.

For more information, see Citrix Virtual Apps and Desktops.

How it works

BCR uses the Citrix Workspace™ app to create a secure browsing environment on the user's device. When a user accesses an allowed webpage, the viewport of the browser window is redirected to the client. The client side browser engine then uses the local machine's resources to render the page, resulting in faster loading times and smoother interaction.

> **Note:**
>
> Only the browser viewport is redirected. The viewport is the rectangular area in your browser where the content is displayed. The viewport doesn't include the Address Bar, **Favorites** Toolbar, or **Status** Bar. Those items are in the user interface, which is still running on the browser in the Virtual Delivery Agent.



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

Key benefits

Browser content redirection manages the web traffic, delivering a superior experience for your users while reducing strain on your infrastructure. Your organization can benefit in the following ways:

- **Resource optimization**: Offloading resource-intensive webpages to user devices helps free up server capacity and reduce bandwidth consumption. This leads to improved efficiency and lower hardware and network demands.
- **Enhanced user experience**: Delivers a smoother, more responsive browsing experience, even for graphics-intensive websites. Ensures native-like performance, eliminating lag and boosting productivity.
- **Improved security**: Maintains a secure environment while enabling access to both internal and external resources.
- **Increased flexibility**: Supports diverse use cases, from basic web browsing to complex web applications requiring proxy traversal or SSO authentication. Manages redirection settings effortlessly with granular policy controls in Citrix Web Studio.

System requirements

Server side components

Citrix Virtual Apps and Desktops:

- Long Term Service Release
  - Minimum requirements: Any non end-of-life LTSR Citrix Virtual Apps and Desktops release.
  - Recommended: Citrix Virtual Apps and Desktops 2402 or higher.
- Current Release
  - Minimum requirement: Any non end-of-life CR Citrix Virtual Apps and Desktops release.
  - Recommended: Latest Citrix Virtual Apps and Desktops release.

Browser components:

- Browsers
  - Microsoft Edge
  - Google Chrome
- Browser redirection extension: Published in both Chrome and Edge web stores.
- It is recommended to use the latest version of the browsers for best experience.

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

Client side components

Citrix Workspace app:

Minimum requirement: Version 2411 or higher.

> **Note:**
>
> - For macOS, Browser content redirection package is independent of Citrix Workspace app and is always the latest version. Hence, the package is compatible with multiple Citrix Workspace app versions above the specified minimum version.
> - Since Browser Content Redirection is independent of Citrix Workspace app for Mac, its version numbering no longer aligns with Citrix Workspace app for Mac.
> - Seamless downgrades of BCROverlay while downgrading Citrix Workspace app are not supported. To downgrade BCROverlay, uninstall it first using **Uninstall Citrix BCR Overlay.app** in **/Library/Application Support/Citrix Receiver**, and then downgrade Citrix Workspace app.
> - Client side browser engine is not packaged with Citrix Workspace app Mac. Download and install the client side for Mac on Citrix Downloads.
> - Intel and ARM packages are separate. Hence, you must install the appropriate version that suits the macOS endpoint.

Configuration

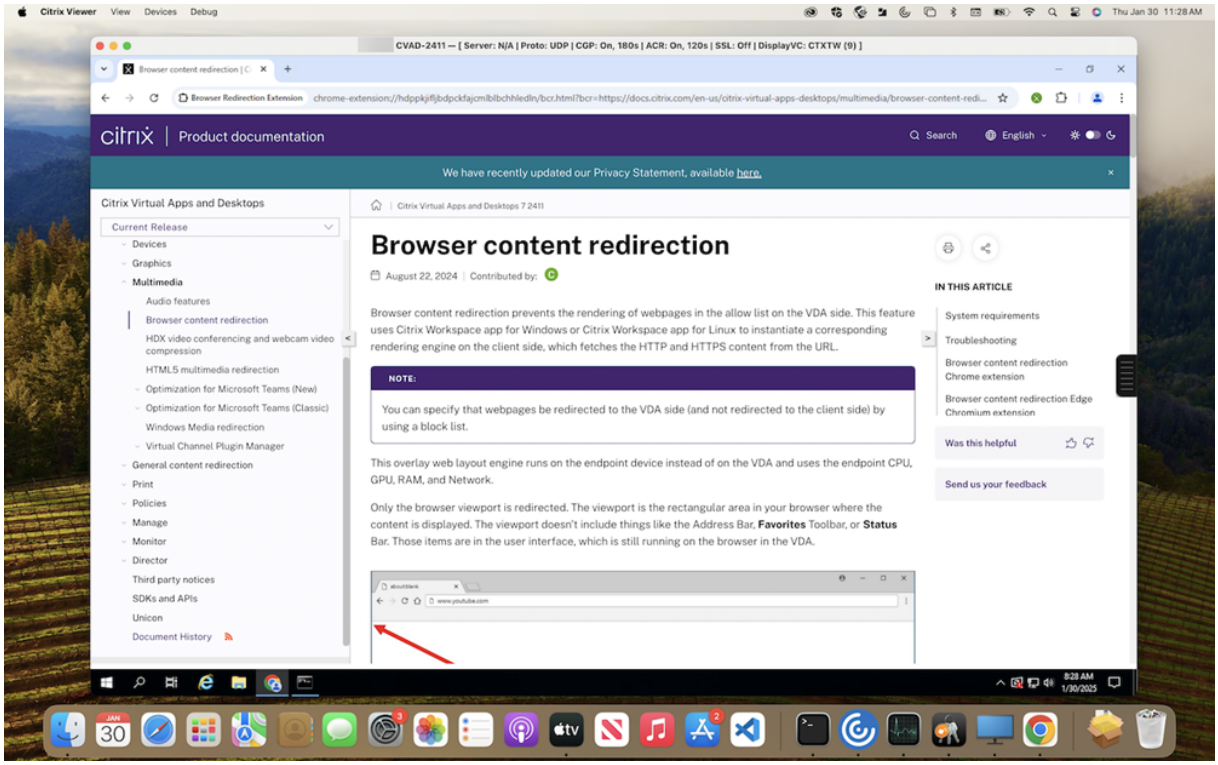
To configure Browser content redirection, follow these steps:

1. Install the client side and server side components according to the system requirements. For information on extension deployment, see Extension deployment.
2. Configure the studio policies.
    - Web studio policies offer a granular way to configure Browser content redirection to suit various use cases.
    - The basic policies allow the administrator to configure URLs that must be allowed or not allowed with Browser content redirection.
    - The URLs can be configured with wild cards.
3. Open a supported web browser and navigate to an allowed URL.
    - If the match is found in the allow list, the website is redirected to the client.
    - Citrix Workspace app blends the viewport onto the VDA side browser for a seamless experience.

The color of the extension logo specifies the status of the content redirection. It is one of these three colors:

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

- Green: Active and connected
- Gray: Not active or idle on the current tab
- Red: Broken or Not Working



For more information, see Browser content redirection policy settings.

> **Note:**
>
> - HTML5 video redirection and browser content redirection are independent features. The HTML5 video redirection policies aren't needed for this feature to work. However, the Citrix HDX™ HTML5 Video Redirection Service is used for browser content redirection.
> - It is recommended to configure all settings through Web Studio rather than using registry keys.

Modular Browser Content Redirection

Starting with the Citrix Workspace app 2511.1 for Mac, the Modular BCR component is installed by default but not packaged with Citrix Workspace App. The modular and evergreen model allows the Browser Content Redirection component to be updated independently and uninstalled independently. This feature provides the following key benefits:

- **Enhanced security**: The BCR NW.js component can receive security patches and updates when they are available, without waiting for a full Citrix Workspace app for Mac release.

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

- **Simplified management**: Customers no longer must update entire Citrix Workspace app to receive the latest Browser content redirection features.
- **Accelerated innovation**: Faster deployment of new BCR features, enhancements, and bug fixes is now possible, delivering continuous value to customers.

The BCR component is downloaded from Citrix CDN and installed post Citrix Workspace app Mac installation.

Installation and management

When you install or upgrade to Citrix Workspace app 2511.1 or later, the installer triggers BCR component and installs it by default. No additional action is needed to install the BCR component.

For environments that do not use Browser Content Redirection, you can prevent its installation using the below **MDM** setting:

```
<key>BCRInstallationEnabled</key>
<false/>
```

- If you exclude the BCR component during initial setup, you can install it anytime by downloading the standalone installer from the Citrix Downloads page.
- The BCR component can be uninstalled separately from Citrix Workspace app anytime by uninstalling the Citrix Browser Content Redirection Plug-in.

Automatic updates

Once the modular and evergreen BCR component is installed, it keeps itself up-to-date automatically. The component periodically checks for new versions and silently installs them in the background. This automatic update ensures that you always have the latest features and security updates without manual upgrades.

Bidirectional content redirection

Bidirectional content redirection allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions. This means:

- A URL entered in a browser running in the Citrix session can be opened using the client's default browser (Host-to-Client).
- Conversely, a URL entered in a browser running on the client can be opened in a Citrix session, either with a published application or desktop (Client-to-Host).

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

Citrix also offers host-to-client redirection and Local App Access redirection. However, it is recommended to use **Bidirectional Content Redirection** for most use cases.

System requirements

- Citrix Virtual Apps and Desktops™ version 2402 or later.
- Citrix Workspace™ app for Mac 2603 or later.
- Browsers: Google Chrome or Microsoft Edge must be installed on both Client and VDA.
- Browser Extension: Browser Redirection Extension on both Client and VDA side browsers.
    - Chrome Extension Browser Redirection Extension- Chrome Web Store
    - Edge Extension Browser Redirection Extension - Microsoft Edge Addons

> **Note:**
>
> To enable Bidirectional Content Redirection, ensure that you have Virtual Delivery Agent (VDA) version 2503 if you intend to use the Browser redirection extension from the Microsoft Edge Add-ons store. For older VDA versions, you can achieve the same functionality by installing the extension from the Chrome Web Store within your Microsoft Edge browser.

Configuration

Starting with modern versions of Citrix Virtual Apps and Desktops, Bidirectional Content Redirection is configured primarily through Citrix Web Studio.

Server-Side:

For server-side configuration, refer to Bidirectional content redirection.

Client-Side:

- Browser Extension: The **Citrix Browser Redirection Extension** must be installed and enabled on the local Mac browser (Google Chrome or Microsoft Edge).
- On macOS, no additional Group Policy configuration is required. The policy settings are pushed from the VDA upon session connection.

For detailed instructions, see the Bidirectional content redirection documentation for Citrix Virtual Apps and Desktops.

OAuth redirection support for Bidirectional content redirection

Starting with Citrix Workspace app for Mac 2607, bidirectional content redirection supports OAuth authentication flows. When a user opens an OAuth-protected URL from a VDA session, the bidirectional

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

content redirection policy intercepts the URL and redirects the authentication request to the local Mac endpoint. The user provides credentials on the Mac. After successful authorization, the OAuth callback URL (containing the authorization code or token) is redirected back to the VDA to complete the flow.

For more information, see Bidirectional content redirection policy settings.

Limitations

- **OAuth Redirection:** Due to macOS security requirements for notarized applications, custom OAuth callback URL schemes must be pre-registered with Citrix and cannot be changed dynamically post-installation. Only `citrix-oauth-redir` is supported by default. Please reach out to the Citrix Product team to register your URL scheme.

Graphics and display

Loss tolerant mode for graphics

Starting with Version 2503, this feature enables Citrix Workspace™ app for Mac to use the loss tolerant mode for graphics in Citrix sessions, improving the video experience, particularly in poor network conditions.

Loss Tolerant Mode for graphics improves performance by allowing Citrix® applications to handle video and graphics better, even when the network connection isn't strong. For users who work remotely or in areas with unreliable networks, this feature ensures that graphics-heavy applications remain usable without major performance issues like lag or pixelation. This feature is enabled by default.

With this feature, you can do the following:

- Access and use applications seamlessly, even in unstable network conditions, without major interruptions.
- Enjoy smoother visuals and quicker response times, leading to a more productive and less frustrating work environment.
- Work from anywhere without sacrificing application quality, regardless of network conditions.

Use the following command to disable the feature:

```
1 defaults write com.citrix.receiver.nomas EnableThinwireLossy NO
```

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

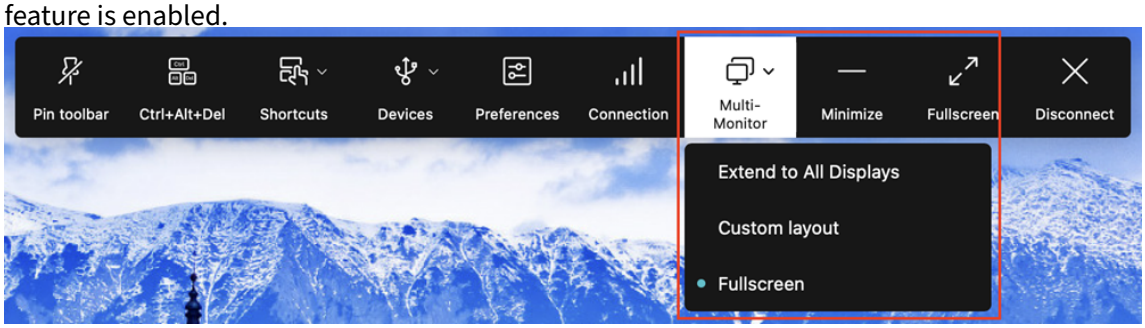
Enhanced Multi-Monitor Management for desktop sessions

Starting with version 2503, the Multi-Monitor Selector (MMS) enables users to select which displays to use in full-screen mode for desktop sessions exclusively, not for seamless sessions. A new Multi-Monitor button appears in the toolbar only when multiple screens are connected, offering a more customized and efficient user experience. This feature is enabled by default.

If the new toolbar is **OFF**, the Multi-Monitor Selector feature is also turned **OFF**.

The toolbar button includes three drop-down menu options for desktop sessions in full-screen mode:

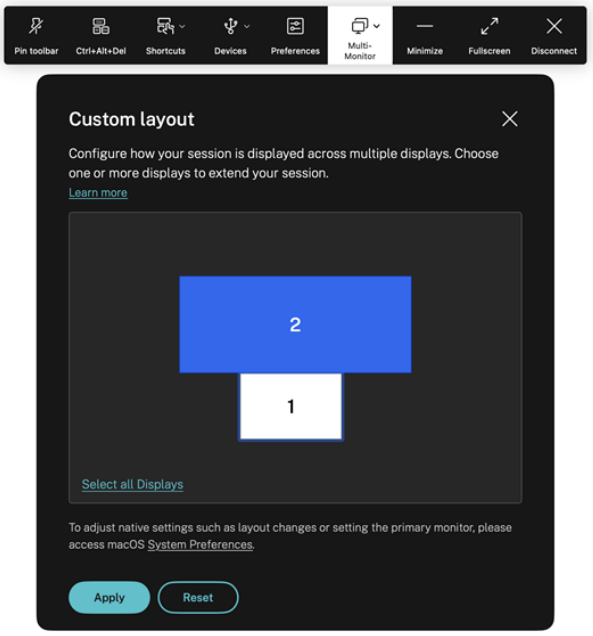
- **Extend to All Displays:** The session switches to full-screen mode on all connected screens. The previous checkbox **Use All Displays In Fullscreen Mode** in the menu bar is removed if this feature is enabled.



- **Custom Layout:** This option opens a custom monitor selector displaying the layout of the macOS system. Users can click on the rectangles in the selector to choose which screens to use and then click **Apply**. The session then uses the selected screens in full-screen mode.
- **Fullscreen:** The session enters full screen following the legacy behavior, using screens that intersect with the session window.

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

1



Use the following command to disable the feature:

```
defaults write com.citrix.receiver.nomas EnableNewCustomMonitorSelector
    NO
```

When a new monitor is plugged in, a notification appears for the user to make a selection. Users can check **Remember my preference** to mute this notification for the current session.

Optimized graphics performance for selective Thinwire

Starting with version 2503, these enhancements optimize text display performance, providing a smoother and more efficient user experience. Graphic performance improvements for Thinwire with Selective H.264, or H.265, significantly reduce CPU and Graphics Processing Unit (GPU) usage in scenarios such as rapidly scrolling through text scenes. Users also benefit from improved frame rates and reduced memory usage. This feature is enabled by default.

Use the following command to disable the feature:

```
defaults write com.citrix.receiver.nomas EnableBitBltOptimization NO
```

Limitation:

The performance enhancement only works when Selective Thinwire is used as the graphic profile.

Multiple monitors

You can set Citrix Workspace app for Mac to work in full-screen mode across multiple monitors.

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

1. Open the Citrix Viewer.
2. From the menu bar, click **View** and select one of the following options, based on your requirement:
    - **Enter Full Screen** - Full screen on the primary monitor only.
    - **Use All Displays In Full Screen** - Full screen on all connected monitors.
3. Drag the Citrix Virtual Desktops™ screen between the monitors.

The screen is now extended to all monitors.

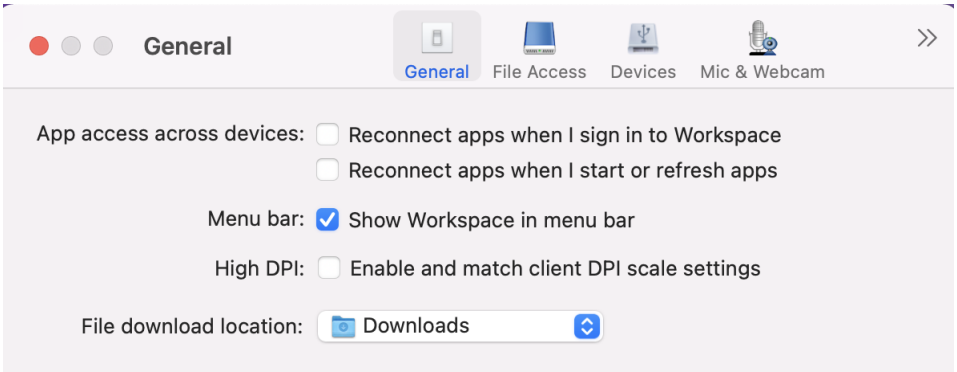
Limitations

- Full-screen mode is only supported on one monitor or all monitors, which are configurable through a menu item.
- Citrix recommends using a maximum of 2 monitors. Using more than 2 monitors might degrade session performance or cause usability issues.
- Full screen mode isn't available on Macs with a notch.

Support for high DPI

Citrix Workspace app for Mac is now compatible with one high DPI monitor with 4K or 5K resolution. With this feature, the text, images, and other graphical elements on virtual desktop or app sessions appear in a size that can be viewed comfortably on these high-resolution monitors.

To enable this feature, navigate to **Preferences > General > High DPI**.



Administrators can edit the **Display memory limit** policy, which specifies the maximum video buffer size in kilobytes for a desktop session, to suit the display resolution. The default value for the **Display memory Limit** policy is 65536 KB and is sufficient for one high DPI monitor with 4K resolution.

For virtual app sessions, the default value of **Display memory Limit** is sufficient as the app session doesn't support more than one display.

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

For virtual desktop sessions, administrators must navigate to **Citrix Studio > Policies > Display memory limit** and use a higher value, for example 393216 KB to use High DPI features for more than one external monitor or 5K resolution monitor.

For more information about the Display memory limit policy, see Display memory limit.

> **Note:**
>
> This feature works with a maximum of two connected monitors.
>
> The number of external monitors you can use with your mac is always limited by the Mac model, as well as the resolution and refresh rate of each display. Refer to the technical specifications of your Mac to find out the supported number of external monitors. For more information, see Connect one or more external displays with your Mac in the Apple support article.

Enhanced notch screen support

Starting with the 2301 version, Citrix Workspace app for Mac supports Macs with a notch display. Macs support a native notch screen in full screen mode for retina and multi-monitor displays. The area of the session in notch screen is now much bigger and provides the customers with more screen space. This enhancement also supports high DPI scaling. The mouse position also appears accurate in all the external monitors connected.

> **Note:**
>
> Ensure not to select the **Scale to fit below built-in camera** option in the Citrix Viewer. This option isn't selected by default and can be found only on Macs with notch display.

Desktop toolbar

Users can now access the **Desktop** Toolbar in both windowed and full-screen mode. Previously, the toolbar was only visible in full-screen mode. Other toolbar changes include:

- The **Home** button has been removed from the toolbar. This function can be run by using the following commands:
  - Cmd-Tab to switch to the previous active application.
  - Ctrl-Left Arrow to switch to the previous Space.
  - Using the built-in trackpad or Magic Mouse gestures to switch to a different Space.
  - Moving the cursor to the edge of the screen while in full-screen mode displays a Dock where you can choose which applications to make active.
- The **Windowed** button has been removed from the toolbar. Follow one of these methods to switch from full-screen mode to windowed mode:

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

- On OS X 10.10, click the green window button on the drop-down menu bar.
- On OS X 10.9, click the blue menu button on the drop-down menu bar.
- On all versions of OS X, select **Exit Full Screen** from the **View** menu of the drop-down menu bar.

- Support to drag between windows in full screen with multiple monitors.

Hide or show the desktop tool bar in the virtual desktop session

You can customize to hide or show the desktop tool bar completely in the virtual desktop session.

For more information about hiding the desktop tool bar completely, see the CTX202450 support article in the knowledge center.

Extend multiple monitors in full-screen mode

Starting with the 2203.1 version, you can enter full-screen mode on two or more monitors simultaneously. To use this feature, perform the following steps:

1. Open the Citrix Viewer.
2. To use full-screen mode on the other connected monitors, drag the window from your primary monitor to span into the connected monitors. From the menu bar, select **View** > **Enter Full Screen**. The window goes into full screen mode on those monitors.

   > **Note:**
   >
   > If you have previously selected the **Use All Displays In Full Screen** option, ensure to unselect it as this selection extends full screen on all connected monitors.

Citrix recommends using a maximum of 3 monitors, including the primary monitor.

Support to open Citrix Workspace app in maximized mode

Starting with the 2204 version, admins can configure the `maximise workspace window` property in the Global App Configuration service to enable the Citrix Workspace app to open in the maximized mode by default. For more information about the Global App Configuration service, see Getting Started.

Support for extending multiple monitors in full-screen mode on up to five monitors

Previously, Citrix supported a maximum of three monitors in full-screen mode, including the primary monitor.

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

Starting with the 2311 version, you can now use full-screen mode on up to five monitors, including the primary monitor, at the same time.

> **Note**
>
> The number of external monitors you can use with your mac is always limited by the Mac model, as well as the resolution and refresh rate of each display. Refer to the technical specifications of your Mac to find out the supported number of external monitors. For more information, see Connect one or more external displays with your Mac in the Apple support article.

You can extend multiple monitors in full-screen mode in the following two ways:

- **Using the menu bar**

1. Open the **Citrix Viewer**.
2. From the menu bar, click **View** and select **Enter Full Screen** to extend full screen.

> **Note:**
>
> You can extend the screen to full-screen mode in all connected displays at once by enabling **Use All Displays In Full Screen** and then selecting **Enter Full Screen** from the **View** menu.

- **Using the green button in the app window**

1. Open the **Citrix Viewer**.
2. Drag or resize the Citrix Viewer window to make it spread on the monitors that you want to use in full-screen mode.
3. Move the pointer to the green button in the upper-left corner of the window, then select **Enter Full Screen** from the menu that appears or click the green button. The screen is now extended to monitors that have an intersection with the window.

Admins can edit the **Display memory limit** policy, which specifies the maximum video buffer size in kilobytes for a desktop session, to suit the display resolution. The default value for the **Display memory Limit** policy is 65536 KB and is sufficient only for up to 2x4K monitors (2x32400KB). Admins must increase this value to use five monitors based on the display resolution. You can edit the **Display memory Limit** by navigating to **Citrix Studio > Policies > Display memory limit**. For more information about the Display memory limit policy, see the Display memory limit section in the XenApp and XenDesktop documentation.

Improved graphics performance

Starting with the 2308 version, the performance of graphics is improved for seamless app sessions. This feature also optimizes the load on CPU usage.

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

Support for H.265 video decoding

Starting with the 2402 version, Citrix Workspace app for Mac supports the use of the H.265 video codec (HEVC) for hardware acceleration of remote graphics and videos. The h.265 video codec (HEVC) supports YUV 4:2:0 color space by default. H.265 video codec must be supported and enabled on both the VDA and Citrix Workspace app. If your Mac device doesn't support H.265 decoding using the VideoToolbox interface, then the H.265 decoding for graphics policy setting is ignored and the session falls back to the H.264 video codec.

Prerequisites

- VDA 7.16 or later using the following GPUs:
  - NVIDIA Maxwell generation GPU or later
  - Intel 6th generation GPU or later
  - AMD Raven generation GPU or later
- Enable the **Optimize for 3D graphics workload policy** on the VDA.
- Enable the **Use hardware encoding for video codec policy** on the VDA.

On Citrix Workspace app for Mac, this feature is set to be enabled by default.

To disable this feature through Mobile Device Management (MDM), administrators must use the following settings:

```
<key>EnableXdecoderForH265</key><false/>
```

Restart the session for the changes to take effect.

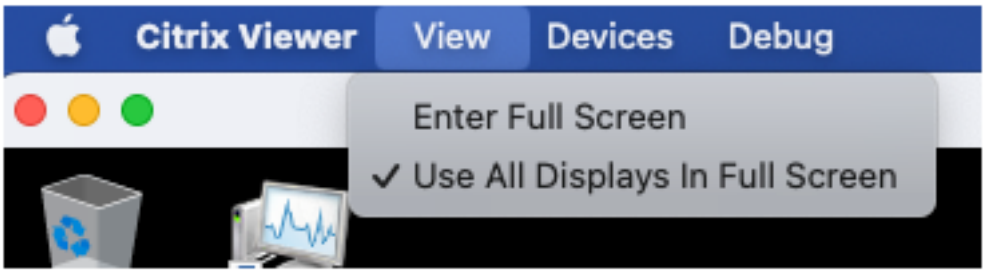
> **Note:**
>
> Run the HDX Monitor 3.x tool to identify if the H.265 video encoder is enabled within the session. For more information about the HDX Monitor 3.x tool, see the Knowledge Center article CTX135817.

Support for extending the desktop session to external monitors automatically

Starting with the 2405 version, Citrix Workspace app supports the extension of desktop sessions to external monitors automatically. With this feature, when you launch the desktop session on the endpoint, if the external monitors are already connected to the endpoint, then the session is extended to external monitors automatically. When you disconnect the external monitor, the session can automatically adjust to extend only to the connected monitors.

To enable this feature, go to the **View** menu in the Citrix Viewer menu bar and select the **Use All Displays in Full Screen** option.

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



Support for YUV444 color format

Starting with the 2409 version, Citrix Workspace app for Mac introduces support for the YUV444 color format. YUV444 is a color format that provides better color accuracy and image clarity compared to the default YUV420 format. It ensures more vibrant and accurate colors, especially when working with multimedia content. This enhancement improves video playback quality and image fidelity.

Mac CPU type	Video codec	Support YUV444 (hardware) decode
Intel	H.264	No
Intel	H.265	Yes
AppleSilicon	H.264	Yes
AppleSilicon	H.265	Yes

> **Note:**
>
> - Macs with Apple silicon support YUV444 using both H.264 and H.265 with hardware acceleration.
> - Macs with Intel architecture do not support H.264 YUV444 decoding with hardware acceleration. In this case, Citrix Workspace app fall back to the supported color format automatically.

Enabling YUV444

For full-screen H.264:

To enable YUV444 for full-screen H.264 video, configure the following policies on the Delivery Controller (DDC):

- Visual Quality: Always lossless / Build to lossless
- Allow visually lossless compression: Enabled

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

- Additional Requirements for full-screen H.265:

If you're using full-screen H.265 video with YUV444, ensure the following:

- Citrix Virtual Apps and Desktops™ version 2209 or newer
- Graphics hardware that meets the requirements:
- NVIDIA Pascal GPU or newer
- Intel 6th generation GPU or later
- AMD Generation GCN3 or later

Recommended Policies

- Use video codec: "Use when Preferred"or "For the Entire Screen"
- Optimize for 3D Graphics: Enabled
- Hardware Encoding: Enabled

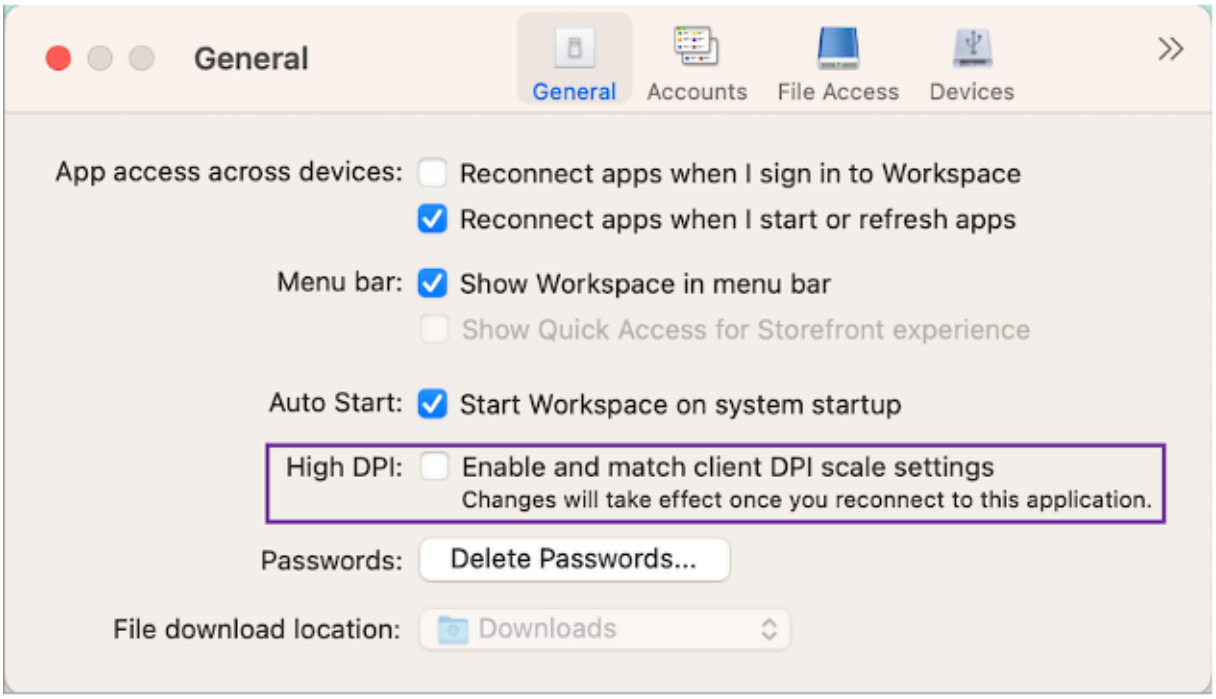
Enhanced the High DPI option

Previously, Citrix Workspace app supported the **High DPI** option for virtual desktop sessions only.

Starting with the 2405 release, enabling the **High DPI** option can also support for seamless app sessions. Also, you can now enable the High DPI option on three 4k monitors. These features are disabled by default.

To enable the **High DPI** option, you must select **Preferences > General**. On the **General** tab, select **Enable and match the client DPI scale settings**. Restart the application for the changes to take effect.

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



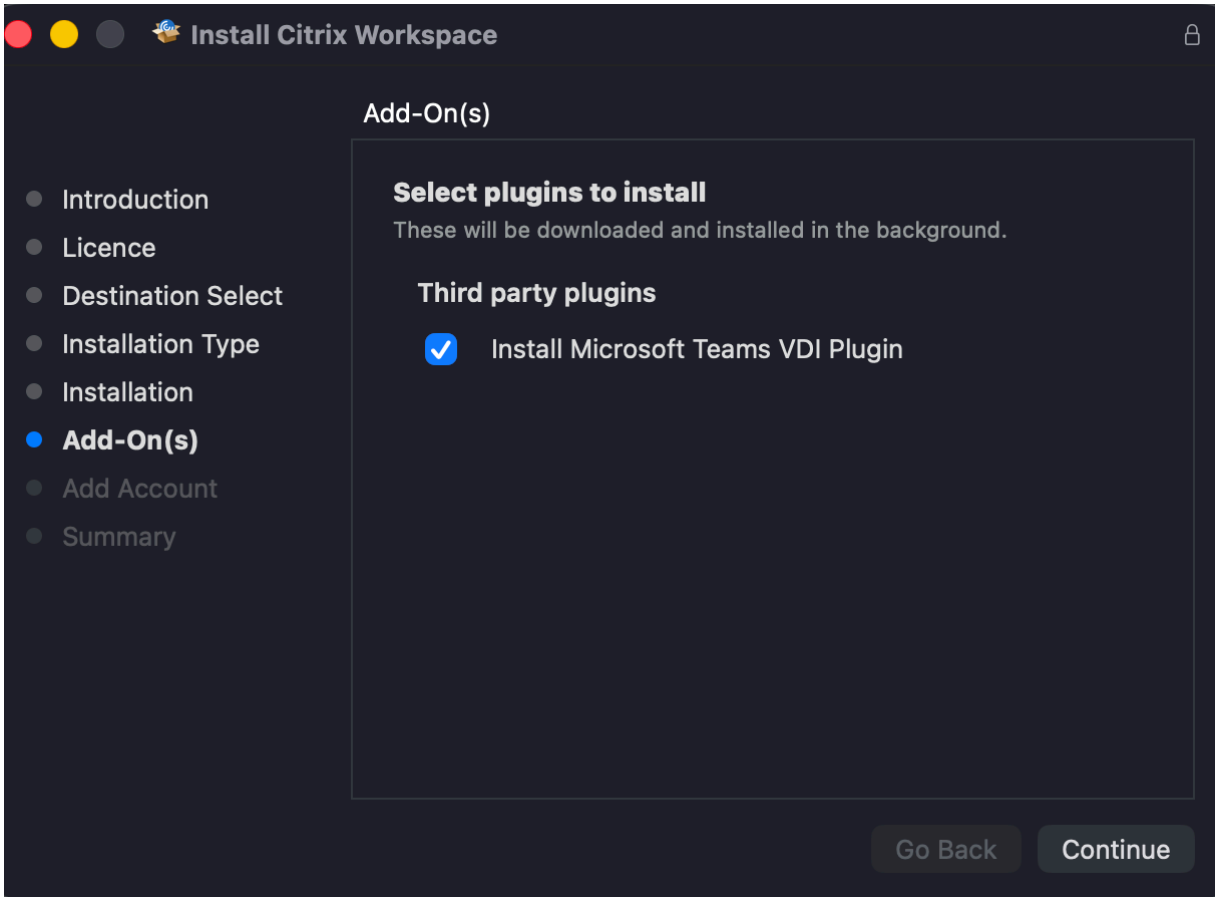
Optimized Microsoft Teams

Microsoft Teams VDI Plugin —generally available and installed by default

Starting with Citrix Workspace app for Mac 2607, the new VDI optimization for Microsoft Teams is generally available and the Microsoft Teams VDI plug-in is installed by default. The plug-in checkbox in the installer Add-ons step is now checked by default, and the plug-in is also installed automatically during Citrix Workspace app for Mac auto-update.

This is a behavior change from the 2603 release, where the plug-in was opt-in and had carried a Technical Preview designation. The New VDI Optimization for Microsoft Teams for Mac is now Generally available. For more information, see Generally available: Microsoft Teams new optimization for VDI on Mac.

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



Enhanced call connect times with Unified Communications SDK

Starting with version 2607, the Unified Communications SDK (UCSDK) 5.0.0 introduces a Smart Sync feature that reduces call connection times by streamlining communication between the VDA and the client endpoint. This delivers faster call setup across all network conditions, with the most significant improvements in high-latency environments.

Citrix recommends that customers work with their UC application vendors to upgrade to UCSDK 5.0.0. For more information, see Unified Communications SDK optimization.

Optimized Overlay Clipping for multimedia sessions

Starting with version 2607, Citrix Workspace app for Mac introduces Optimized Overlay Clipping, improving both performance and visual accuracy during multimedia sessions that use HDX Microsoft Teams Optimization and UCSDK Optimization.

This enhancement provides the following benefits:

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

- **Improved visual accuracy**: Resolves issues where UI elements, such as pop-up menus or notifications, incorrectly appear behind video content, ensuring a more seamless and predictable user experience.
- **Enhanced performance**: Reduces CPU utilization on the VDA by replacing legacy polling methods with a more efficient graphics-based approach, improving scalability and supporting higher user density.

For more information, see Optimized Overlay Clipping for enhanced performance and user experience.

UCSDK deviceID enhancement

The Unified Communications SDK (UCSDK) extends support to WebRTC-based applications, enabling Contact Center and Unified Communications providers to optimize real-time voice and video calls in Citrix Virtual Desktop Infrastructure (VDI) environments by offloading media processing to the user's device. This feature is enabled by default.

With this feature, you can:

- Control calls using Web Human Interface Device (HID) support, allowing mute, unmute, hold, and pickup directly from headsets, with real-time status updates in the application.
- Enable screen recording beyond VDI by configuring policies to record endpoint screens, allowing retrieval and playback of recorded sessions.
- Use UCSDK in browser applications to achieve full feature parity with desktop applications for a seamless experience.

Audio and video device identification and grouping are enhanced, providing more precise control over built-in and peripheral devices. UCSDK partners receive clear, user-friendly information about user devices.

Support for WebHID API in UCSDK

Starting with the 2411 version, Citrix Workspace™ app for Mac supports the WebHID API to redirect Human Interface Devices (HIDs) from endpoint to Unified Communication SDK application on the VDI. It complies with the HID standard for bi-directional communication between the application based on UCSDK and the HID devices connected to the endpoint.

With this feature, your UCSDK application can interpret HID commands such as call accept, reject, mute, or unmute within the HDX™ session for an enhanced user experience. This feature is enabled by default.

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

Configuring a preferred network interface

Starting with the 2304 version, you can configure a preferred network interface for media traffic. Run the following command in the terminal:

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Select one of the following values as required:

- 1: Ethernet
- 2: Wi-Fi
- 3: Cellular
- 4: VPN
- 5: Loopback
- 6: Any

By default and if no value is set, the WebRTC media engine chooses the best available route.

Encoder performance estimator

The `HdxRtcEngine.exe` is the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection. The `HdxRtcEngine.exe` can estimate the best encoding resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 480p, 720p, and 1080p.

The performance estimation process uses macroblock code to determine the best resolution that can be achieved with the particular endpoint. The Codec negotiation includes the highest possible resolution. The Codec negotiation can be between the peers, or between the peer and the conference server.

There are four performance categories for endpoints that have its own **maximum** available resolution:

Endpoint performance	Maximum resolution	Registry key value
Fast	1080p (1920x1080 16:9 @ 30 fps)	3
Medium	720p (1280x720 16:9 @ 30 fps)	2
Slow	360p (640x360 16:9 @ 30 fps or 640x480 4:3 @ 30 fps)	1
Very slow	240p (320x180 16:9 @ 30 fps or 320x240 4:3 @ 30 fps)	0

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

To set the video encoding resolution value to 360p, run the following command from the terminal:

```
defaults write com.citrix.HdxRtcEngine OverridePerformance -int 1
```

For more information about Microsoft Teams optimization, see Optimization for Microsoft Teams.

Improved experience for optimized Microsoft Teams video conference calls

Starting with the 2304 version, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, every call is adjusted to the proper resolution for the optimal call experience. This feature enhances the quality and experience of video conference calls across various endpoints.

With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on). The video resolution 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 and giving all users the optimum video experience.

> **Note:**
>
> This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, go to https://www.microsoft.com/ and search for the Microsoft 365 roadmap. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

Limiting video resolutions

Administrators who have users on lower-performance client endpoints can choose to limit incoming or outgoing video resolutions to decrease the impact of encoding and decoding video on those endpoints. Starting from Citrix Workspace app 2304 for Mac, you can limit these resolutions using client configuration options.

> **Note:**
>
> Users running with restricted resolutions impact the overall video quality of the conference because the Microsoft Teams server is forced to use the lowest-common-denominator resolution for all conference participants.

Call constraints are disabled by default on the client with Citrix Workspace app 2304. To enable, administrators must set the following client-side configurations with the defaults command:

```
defaults write com.citrix.HdxRtcEngine <Name> -<Type> <Value>
```

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

Name	Type	Mandatory	Accepted values
EnableSimulcast	int	YES	1–3 (set it to 1)
MaxOutgoingResolution	int	YES	180, 240, 360, 540, 720, 1080 (Microsoft Teams supported Resolutions)
MaxIncomingResolution	int	YES	180, 240, 360, 540, 720, 1080 (Microsoft Teams supported Resolutions)
MaxIncomingStreams	int	YES	1–8
MaxSimulcastLayers	int	YES	1–3 (set it to 1)
MaxVideoFrameRate	int	NO	1–30
MaxScreenShareFrameRate	int	NO	1–15

Background blurring and replacement for Citrix Optimized Microsoft Teams

Starting with the 2301 version, Citrix Optimized Microsoft Teams in Citrix Workspace app for Mac now supports background blurring and background replacement. You can use this feature by selecting **More > Apply Background Effects** when you are in a meeting or a P2P call.

Enhancement to sleep mode for optimized Microsoft Teams call

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

Starting with the 2305 version, Citrix Workspace app or the optimized Microsoft Teams screen doesn't go to sleep mode even if there's no mouse or keyboard interaction during an optimized Microsoft Teams meeting.

Screen sharing optimization with Microsoft Teams

Starting with the 2012 version, Citrix Workspace app for Mac supports screen sharing optimization with Microsoft Teams. For more information, see the following:

- Optimization for Microsoft Teams
- Microsoft Teams redirection

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

Microsoft Teams optimization support for seamless app sessions

Starting with the 2101 version, Citrix Workspace app for Mac now supports Microsoft Teams optimization for seamless app sessions. As a result, you can launch Microsoft Teams as an application from within the Citrix Workspace app. For more information, see the following:

- Optimization for Microsoft Teams
- Microsoft Teams redirection

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

Starting with the 2101 version, Citrix Workspace app for Mac supports Dual Tone Multi Frequency (DTMF) signaling interaction with telephony systems (for example, PSTN) and conference calls in Microsoft Teams. This feature is enabled by default.

Enhancements in Desktop Viewer

When the **Desktop Viewer** is in full screen mode, the user can select one from all the screens covered by the **Desktop Viewer** to share. In the window mode, the user can share the **Desktop Viewer** window. In the seamless mode, the user can select one screen from the screens connected to the endpoint device.
When the Desktop Viewer changes the window mode (maximize, restore, or minimize), the screen sharing stops.

When the user wants to share the screen, previews for all available screens appear in the screen sharing panel. Making it intuitive for users to select the right one from the previews.

Support for H.264 Advanced Video Coding (MPEG-4 AVC) with Microsoft Teams

Starting with the 2109 version, Citrix Workspace app for Mac supports hardware accelerated H.264 video encoding or decoding. It reduces the load on CPU usage and improves your video conferencing experience. The multimedia engine of Citrix HDX optimized Microsoft Teams (HdxRtcEngine.exe) now uses Apple's Video Toolbox framework for encoding and decoding. This framework compresses and decompresses video faster and in real time. Also, the offloading of encoding and decoding to the GPU is optimized. Hardware-accelerated video decoding and encoding are enabled by default if a device supports it. This enhancement reduces the load on the CPU during multimedia usage when Microsoft Teams is optimized with HDX.

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

Dynamic e911

Starting With the 2112 version, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it allows you to do the following:

- Configure and route emergency calls.
- Notify security personnel.

Notification is provided based on the current location of the Citrix Workspace app running on the endpoint. It is not sent based on the Microsoft Teams client that runs on the VDA. Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112.1 for Windows, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law. For more information about this feature, see Support for dynamic e911 in the section **Microsoft Phone System**.

Request control in Microsoft Teams

Starting with the 2112 version, you can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other modifications to the shared screen.

To take control when a screen is being shared, click **Request control** at the top of the Microsoft Teams screen. The meeting participant who's sharing the screen can either allow or deny your request. When you're done, click **Release control**.

Limitation:

The **Request Control** option isn't available during peer-to-peer calls between an optimized user and a user on the native Microsoft Teams desktop client that is running on the endpoint. As a workaround, users can join a meeting to get the **Request Control** option.

Give or take control in Microsoft Teams

Starting with the 2203.1 version, you can use the **Give control** button to give control of your shared screen to other users participating in the meeting. The other participants can make selections and modify the shared screen through keyboard, mouse, and clipboard input. You both now have the control of the shared screen and you can take back the control anytime.

To take control during screen sharing sessions, any participant can request control access through the **Request control** button. The person sharing the screen can then approve or deny the request. When you have the control, you can control the keyboard and mouse input on the screen shared and release the control to stop sharing control.

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

> **Note:**
>
> This feature is available only after the roll-out of a future update from Microsoft Teams.

Multi-window chat and meetings for Microsoft Teams

Starting with the 2203.1 version, you can use multiple windows for chat and meetings in Microsoft Teams (1.5.00.5967 or higher) when optimized by HDX in Citrix Virtual Apps and Desktops and Citrix DaaS. Users can pop out their conversations or meetings in various ways. For details on the pop-out window feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings on the Microsoft Office 365 site.

If you're running an older version of Citrix Workspace App or VDA, Microsoft can deprecate the single-window code in the future. However, you have a minimum of nine months to upgrade to a version of the VDA/CWA that supports multiple windows (2203 or later).

> **Note:**
>
> This feature is available only after the roll-out of a future update from Microsoft Teams. Got more details, see the Microsoft 365 roadmap.

Share apps using the 'Share content'feature in Microsoft Teams

Starting with the 2203.1 version, you can share individual applications, windows, or full screen using the screen sharing feature in Microsoft Teams. Citrix Virtual Delivery Agent 2109 is a prerequisite for this feature.
To show a specific application, click **Share content** in your meeting controls and select the application of interest. After a red border appears around the app you select, peers on the call can see your app. If you minimize the app, Microsoft Teams displays the last image from the shared app. Maximize the window to resume sharing.

Enhancements to Optimized Microsoft Teams

In optimized Microsoft Teams, you can now use the video function when more than one virtual desktop or app session is in use.

App Protection compatibility with HDX optimization for Microsoft Teams

Starting with the 2204 version, full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group. When you click **Share content** in Microsoft Teams, the screen picker

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

removes the **Desktop** option. You can only select the Window option to share any open app, if the VDA is 2109 or higher. If you're connected to VDA older than 2019, no content is selectable.

Deprecation announcement of the SDP format (Plan B) from WebRTC

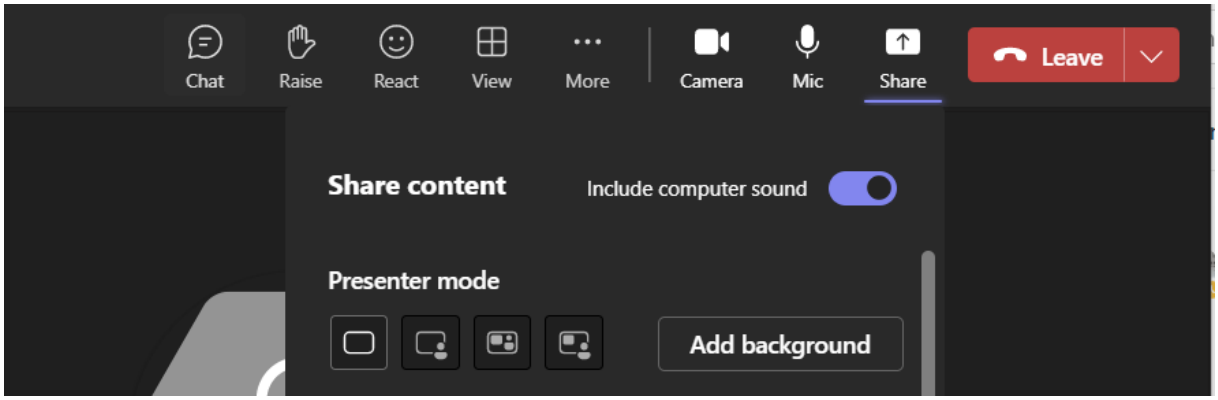
Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use a version of Citrix Workspace app that supports the Unified Plan to continue using certain optimized Microsoft Teams functionalities.

Upgraded version of WebRTC for the optimized Microsoft Teams

Starting with the 2405 version, the version of WebRTC that is used for the optimized Microsoft Teams is upgraded to version M117.

Support for sharing system audio on Microsoft teams

Starting with the 2503 version, Citrix Workspace app for Mac supports sharing the system audio during the Microsoft Teams meeting. With this feature, you can now share the audio playing on your VDA with the participants in a meeting. Select the **Include computer sound** option to allow sharing the system audio to the meeting.



Virtual channel plugin manager

Starting with version 2603, Citrix Workspace app for Mac enables virtual channel plugin manager for Microsoft Teams. Virtual channel plugin manager helps deploy plug-ins across client endpoints for specified applications. It detects supported applications running on the VDA and prompts users to install the required plug-in on the endpoint for the best in-session experience. Users can choose to

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

install the plug-in, skip the installation, or deny it. This feature provides flexibility to manage plug-ins across both managed and unmanaged endpoints.

For more information, see Virtual channel plugin manager.

HDX™ transport

Enlightened Data Transport (EDT)

By default, EDT is enabled in Citrix Workspace app for Mac.

Citrix Workspace app for Mac reads the **EDT** settings as set in the default.ica file and applies it.

To disable EDT, run the following command in a terminal:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT)

Starting with the 2108 version, Citrix Workspace app for Mac supports Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT). It increases the reliability and compatibility of the EDT protocol and provides an improved user experience.

> **Note:**
>
> EDT MTU discovery is supported on macOS Big Sur and later.

Improved network congestion control

Starting with the 2308 version, the Citrix-proprietary transport protocol called Enlightened Data Transport (EDT) is improved to efficiently control network congestion. This feature improves data throughput and reduces latency.

Upgraded HDX Reducer to Version 4

Previously, Citrix Workspace app for Mac supported HDX Reducer V3. Starting with the 2402 version, Citrix Workspace app for Mac supports HDX Reducer V4. This feature reduces the network bandwidth required for a typical session and improves response time.

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

HDX™ direct

HDX direct support

Starting with version 2503, HDX Direct allows direct connections from external client devices to Virtual Delivery Agent (VDA), bypassing the Citrix Gateway service. This feature improves performance and reduces latency for both internal and external users through a direct path to the session host, resulting in fewer network hops and improved in-session performance. Also, the decreased load on the Citrix Gateway service enhances the overall system efficiency. This feature is enabled by default.

Prerequisites:

- Access to the internal network or configuration for direct connections.
- Network infrastructure that supports direct VDA connections.
- Configuration of Session Traversal Utilities for NAT (STUN) and Traversal Using Relay around NAT (TURN) servers.

To disable the feature, use the following commands:

```
defaults write com.citrix.receiver.nomas EnableHDXDirectV2 NO
```

Limitation:

- Requires ownership of STUN and TURN servers.
- This feature does not support service continuity. It only functions without service continuity.

For more information, see HDX Direct.

HDX Direct

Starting with version 2411, Citrix Workspace app for Mac supports HDX Direct transport for the connection between Citrix Workspace app and the Virtual Delivery Agent server. HDX Direct allows client devices to establish a secure, direct connection with the session host if direct communication is feasible. For more information, see HDX Direct.

Devices

This section describes about the features supports for the following devices:

- Audio and Microphone
- Client drive-mapping
- Keyboard

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

- Printing
- USB
- Webcam

Audio and Microphone

Default audio device selection

Starting with 2505 version, you can now select your preferred audio devices directly in the Desktop Viewer toolbar. This feature offers a more customized audio experience with the following key features when connected to a virtual desktop.

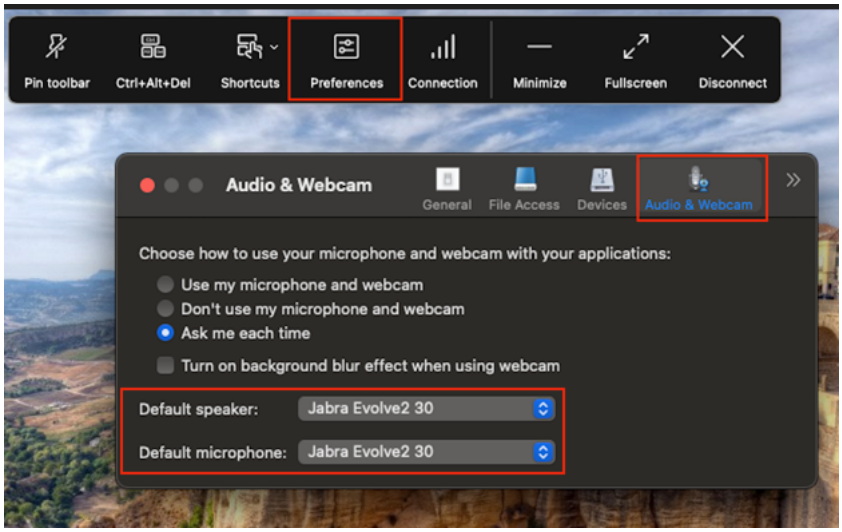
- Device splitting: You can assign different audio devices to different VDAs. For example, you can have two monitors with two different VDAs, each using a separate audio device (one loudspeaker and one headset).
- Specific device selection: The exact audio device can be selected for each active VDA from the **Preferences** section.
- Configuration persistence: The selected configuration is preserved for the next session, ensuring a seamless experience.

> **Note:**
>
> If you don't want the selected configuration to be preserved for the next session, you can adjust the settings accordingly in the Preferences section.
> This feature isn't applicable to a pooled desktop environment because each time a user signs in, they might be connected to a different VDA.

To select the specific audio device, do the following:

1. Navigate to the **Preferences** section on the Desktop Viewer toolbar.
2. Navigate to the **Audio & Webcam** tab.

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



3. Select the device that you want from the **Default speaker** drop-down list.
4. Select the device that you want from the **Default microphone** drop-down list.

> **Note:**
>
> The option to configure default audio devices is not available in Citrix Workspace™ Preferences. To select default audio devices, use the Desktop Viewer toolbar.

Audio Quality Enhancer for EDT loss tolerant mode

Starting with version 2508, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Adaptive audio must be enabled for this feature to work.

Adaptive audio

You don't need to configure the audio quality policies on the VDA with the Adaptive audio feature. Adaptive audio optimizes settings for your environment and replaces legacy audio compression formats to provide an excellent user experience. For more information, see Adaptive Audio.

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

Improved audio echo cancellation support

Citrix Workspace app supports echo cancellation in adaptive audio and legacy audio codecs. This feature is designed for real-time audio use cases, and it improves the user experience. Citrix recommends using adaptive audio.

Client-side microphone input

Citrix Workspace app for Mac supports multiple client-side microphone inputs. You can use locally installed microphones for:

- Live events, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Digital dictation support is available with Citrix Workspace app for Mac.

You can choose how to use your microphone and webcam with the virtual app and desktop sessions. To apply access type to your microphone and webcam, select any of the following access types as per your requirement on the **Mic & Webcam** tab in the **Preferences** settings:

- **Use my microphone and webcam** - Provides access to microphone and webcam when it's connected.
- **Dont use my microphone and webcam** - No access to microphone and webcam.
- **Ask me each time** - Request permission each time when microphone and webcam access is required.

To apply a background blur effect when using the webcam, select **Turn on background blur effect when using webcam**.

Support for multiple audio devices

Starting with the 2311 release, Citrix Workspace app for Mac displays all available local audio devices in a session with their names. In addition, plug-and-play is also supported.

Store-based configuration of microphone and webcam access

Starting with the 2307 version, the microphone and webcam access per store are included as part of the client-selective trust feature. This enhancement allows you to provide access to a microphone and webcam on a per store basis.

To enable microphone and webcam access for a store, you must select **Preferences > Mic & Webcam**. In the **Mic & Webcam** tab, select the store and the type of access required for that store.

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

Support for audio volume synchronization

Previously, audio volume control is independent between the Virtual Delivery Agent (VDA) and your device. You've to adjust the volume on both sides to maintain the desired volume. Also, if you've muted the volume in your device, then it restricts to unmute the volume in the VDA.

Starting with the 2402 version, Citrix Workspace app for Mac supports synchronization of audio volume between the VDA and your audio devices. You can now tune the volume using the VDA audio volume slider and have the same volume on your device and the other way around. By default, this feature is enabled.

To enable this feature, you need to use VDA version 2308 or later. For more information, see audio volume synchronization in the Citrix Virtual Apps and Desktops documentation.

To enable audio volume synchronization on the VDA, configure the following registry value and restart the machine:

For Server OS VDA:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Value name: EnableVolumeSync
- Value type: DWORD
- Value data: 1

For Desktop OS VDA:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- Value name: EnableVolumeSync
- Value type: DWORD
- Value data: 1

To disable this feature through Mobile Device Management (MDM), administrators must use the following settings:

```
<key>EnableVolumeSync</key><false/>
```

Restart the session for the changes to take effect.

Loss tolerant mode for audio

Starting with the 2402 version, Citrix Workspace app supports loss tolerant mode (EDT lossy) for audio redirection. This feature improves the user experience for real-time streaming when users are connecting through networks with high latency and packet loss. By default, this feature is enabled.

To enable this feature, you need to use VDA version 2311 or later. For more information, see Support for audio over loss-tolerant mode (Preview) in the Citrix Virtual Apps and Desktops documentation.

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

To disable this feature through Mobile Device Management (MDM), administrators must use the following settings:

```
<key>EdtUnreliableAllowed</key><false/>
```

Restart the session for the changes to take effect.

Client drive mapping

During the session, Client drive mapping allows you to access local drives on the user hardware device. The user hardware devices can be CD-ROM drives, DVDs, and USB memory sticks. When a server configuration allows client drive mapping, you can access locally stored files and work on them during sessions. You can also save them either on a local drive or on a drive on the server.

Citrix Workspace app for Mac monitors the directories in which user hardware devices are typically mounted on the user device. It can automatically map any new ones that appear during a session to the next available drive letter on the server.

You can configure the level of read and write access for mapped drives using the Citrix Workspace app for Mac preferences.

To configure read and write access for mapped drives

1. On the Citrix Workspace app for Mac home page, click the down arrow icon, and then click **Preferences**.
2. Click **File Access**.
3. Select the level of read and write access for mapped drives from the following options:
    - Read and Write
    - Read only
    - No access
    - Ask me each time
4. Log off from any open sessions and reconnect to apply the changes.

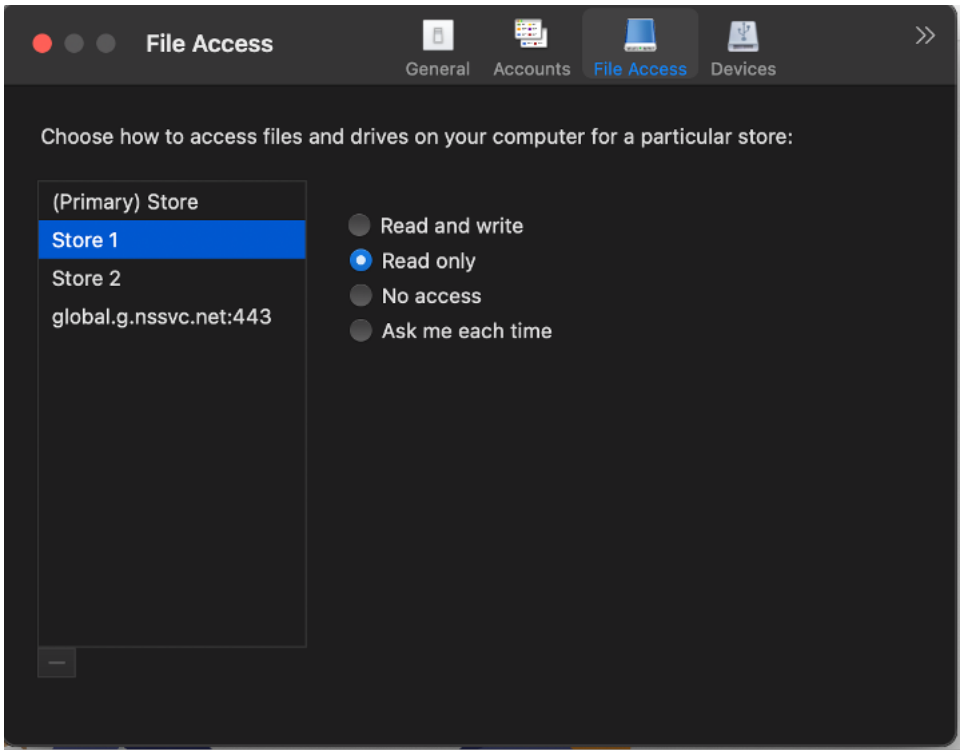
Store-based configuration of file access

Starting with the 2405 release, the per-store file access is included as part of the client-selective trust feature. This enhancement allows you to provide access to files on a per store basis.

To enable file access for a store, you must select **Preferences > File Access**. On the **File Access** tab, select the store and the type of access required for that store. You can choose any of the following types of access for files and drives on your computer:

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

- **Read and write:** Provides read and write access to files and drives for the selected store.
- **Read only:** Provides read only access to files and drives for the selected store.
- **No access:** Restrict access to files and drives for the selected store.
- **Ask me each time:** Request permission to access files and drives each time when read or write access is required for the selected store.



Keyboard

Enhanced keyboard settings for VDA OS and session type

Starting with version 2503, Citrix Workspace™ app for Mac provides default keyboard settings tailored to the Virtual Desktop Agent (VDA) OS, ensuring an optimal input experience and simplifying configuration for end users. This feature is enabled by default.

Key features and updates:

- Dynamic sync enhancements:
  - Application sessions: The default setting is now **Dynamic Sync**, allowing seamless input synchronization and simplifying the configuration process.
  - Desktop sessions: The default is also set to **Dynamic Sync** to ensure consistency and balance flexibility with stability.

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

- Automatic Keyboard Input Mode: A new option **Automatic** is added as the default for the Keyboard Input Mode. This feature ensures:
  - **Scancode** is automatically selected for Mac VDAs.
  - **Unicode** is automatically selected for Windows and Linux VDAs.
  - Users can manually select either **Scancode** or **Unicode** for all sessions, depending on their needs.

Limitation:

When upgrading from earlier versions of Citrix Workspace app for Mac with pre-defined local configuration files for the preceding settings, your previous configurations are retained. To use different options, you must manually select them.

Enhanced keyboard and IME diagnostics tool

Starting with version 2411, a new self-service command-line tool hosted in **Windows Virtual Delivery Agent (VDA)** is supported by **Citrix Workspace app for Mac** 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 VDAs 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.

- **Checks for consistency** between VDA policy and client keyboard layout sync mode.
- **Checks for client keyboard layout** and VDA keyboard layout, and provides best practices.
- **Checks the remote language bar setting** and provides best practices.
- **Checks system shortcut pass-through configurations, accessibility permissions, and full screen mode status** to suggest best practices.

Prerequisites:

- Citrix Workspace app for Mac 2411 or higher.
- Virtual Delivery Agent 2411 or higher.

The command line tool is hosted in Windows VDA as `CtxKbImeDiagnostics.exe`. The interfaces are as follows:

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

Interface	Description	Note
`CtxKbimeDiagnostics`	Shows diagnostic results for current user's ICA® sessions.	If the user has admin privilege, it shows diagnostics for all active ICA sessions. If the user has no admin privilege, it shows diagnostics for the current user's ICA sessions.
`CtxKbimeDiagnostics [-v]`	Shows setting information and diagnostic results for current users ICA sessions.	Admin privilege shows diagnostics for all active ICA sessions.
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	Shows setting information and diagnostic results for this session.	Admin privilege can query other ICA sessions. Normal users can query their own sessions.
`CtxKbimeDiagnostics [-s Session_Id]`	Shows diagnostic results for a specific session.	Admin privilege can query other ICA sessions. Normal users can query their own sessions.
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	Shows all setting information and diagnostic results for a specific session.	Admin privilege can query other ICA sessions. Normal users can query their own sessions.
`CtxKbimeDiagnostics [-h]`	Shows supported arguments, parameters, and examples.	Help interface.
`CtxKbimeDiagnostics [-V]`	Shows current tool version.	

Keyboard layout synchronization

Keyboard layout synchronization enables you to switch between the preferred keyboard layouts on the client device.

To enable keyboard layout synchronization, go to **Preferences > Keyboard** and select the required options.

> **Note:**
>
> Using the local keyboard layout option activates the client Input Method Editor (IME). Users working in Japanese, Chinese, or Korean can also use the server IME by choosing the option **"Don't**

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

> **sync.**" The session will revert to the keyboard layout provided by the remote server when they connect to the next session.

Starting with version 2210, Citrix Workspace app for Mac supports three different keyboard layout synchronization modes:

- **Sync only once - when session starts** –Based on the CTXIME value in the `Config` file, the client keyboard layout is synchronized to the server when the session launches. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, sign out and sign in to the app. The Sync only once - when session starts mode is the default keyboard layout for the Citrix Workspace app on Mac.
- **Allow dynamic sync** - This option synchronizes the client keyboard layout to the server when you change the client keyboard layout.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

Prerequisites

- Enable the Unicode Keyboard Layout Mapping feature on the Windows VDA. For more information, see Knowledge Center article CTX226335.
- Enable the Dynamic Keyboard layout sync feature on the Linux VDA. For more information, see Dynamic keyboard layout synchronization.
- When using Windows Server 2016 or Windows Server 2019, navigate to the **HKEY_LOCAL_MACHINE\Softwar** registry path and add a **DWORD** value with the key name **DisableKeyboardSync** and set the value to **0**.

Configure keyboard layout

Citrix Workspace app for Mac provides the UI to configure the three different keyboard layout synchronization modes.

To configure keyboard layout synchronization using the GUI:

1. From the Citrix Workspace app icon in the menu bar, click the account icon in the top-right corner and navigate to **Preferences > Keyboard**.

   The Keyboard layout synchronization settings appear.

2. Select from one of the following options:

   - **Sync only once** - when session starts - Indicates that the keyboard layout is synced to the VDA only once at the session launch. Unicode keyboard input mode is the recommended option for the Sync only once –when the session starts

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

- **Allow dynamic sync** - Indicates that the keyboard layout is synced dynamically to the VDA when the client keyboard is changed in a session. Unicode keyboard input mode is the recommended option for the Allow dynamic sync mode.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server, irrespective of the keyboard layout that is selected in the client. Scancode keyboard input mode is the recommended option for **Don't sync**. You must make sure that the client keyboard layout is the same as the keyboard layout on the VDA if you select Unicode for the **Don't Sync** option.

Limitations

- Using the keyboard layouts listed in "**Supported Keyboard Layouts in Mac**"works while using this feature. When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality can't be confirmed.
- Remote apps that run with elevated privileges can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.
- When a user is working within an RDP session, it's not possible to change the keyboard layout using the `Alt + Shift` shortcuts when RDP is deployed as an app. As a workaround, you can use the language bar in the RDP session to switch the keyboard layout.

Keyboard layout support for Windows VDA

Language on Mac	Input Source on Mac	Applicable Mac OS version
English	ABC	All
English	ABC - India	All
English	U.S.	All
English	U.S. International - PC	All
English	Dvorak	All
English	Dvorak - Left-Handed	All
English	Dvorak - Right-Handed	All
English	British	All
English	British - PC	All
English	Canadian English	All

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
English	Australian	All
English	Irish	All
French	French	All
French	French - Numerical	All
French	Canadian French - CSA	11, 12
French	Canadian –CSA	13
French	Swiss French	All
French	French - PC	All
German	German	All
German	Austrian	All
German	Swiss German	All
Spanish	Spanish	All
Spanish	Spanish - ISO	10,11
Spanish	Spanish –Legacy	12,13
Spanish	Latin American	All
Swedish	Swedish	All
Swedish	Swedish –Legacy	12,13
Swedish	Swedish - Pro	10, 11
Czech	Czech	All
Danish	Danish	All
Finnish	Finnish	All
Hungarian	Hungarian	All
Italian	Italian	All
Italian	Italian - Typewriter	10,11
Italian	Italian –QZERTY	12,13
Greek	Greek	All
Dutch	Belgian	All
Dutch	Dutch	All
Russian	Russian	All

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
Russian	Russian - PC	All
Croatian	Croatian - PC	All
Slovak	Slovak	All
Slovak	Slovak - QWERTY	All
Turkish	Turkish F	All
Turkish	Turkish Q	All
Portuguese	Brazilian	All
Portuguese	Brazilian - ABNT2	All
Portuguese	Brazilian –Legacy	12,13
Portuguese	Brazilian - Pro	10,11
Portuguese	Portuguese	All
Ukrainian	Ukrainian - PC	10,11
Ukrainian	Ukrainian	12,13
Belarusian	Belarusian	All
Slovenian	Slovenian	All
Estonian	Estonian	All
Latvian	Latvian	All
Polish	Polish - Pro	10,11
Polish	Polish	12,13
Icelandic	Icelandic	All
Norwegian	Norwegian	All
Japanese	Katakana	All
Japanese	Half-width Katakana	All
Japanese	Romaji	All
Japanese	Full-width Romaji	All
Japanese	Hiragana	All
Japanese	Alphanumeric (Google)	All
Japanese	Hiragana (Google)	All
Japanese	Katakana (Google)	All

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
Japanese	Half-width Katakana (Google)	All
Japanese	Full-width Alphanumeric (Google)	All
Korean	2-Set Korean	All
Chinese, Simplified	Pinyin - Simplified	All
Chinese, Simplified	Sogou pinyin	All
Chinese, Traditional	Pinyin - Traditional	All
Chinese, Traditional	Cangjie - Traditional	All
Chinese, Traditional	Zhuyin - Traditional	All
Chinese, Traditional	Sucheng - Traditional	All

Keyboard layout support for Linux VDA, Swiss French

Language on Mac	Input Source on Mac	Applicable Mac OS version
English	ABC	All
English	ABC - India	All
English	U.S.	All
English	U.S. International - PC	All
English	Dvorak	All
English	Dvorak - Left-Handed	All
English	Dvorak - Right-Handed	All
English	British	All
English	British - PC	All
English	Canadian English	All
English	Australian	All
English	Irish	All
French	French	All
French	French - Numerical	All
French	Canadian French - CSA	11, 12

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
French	Canadian –CSA	13
French	Swiss French	All
French	French - PC	All
German	German	All
German	Austrian	All
German	Swiss German	All
Spanish	Spanish	All
Spanish	Spanish - ISO	10,11
Spanish	Spanish –Legacy	12,13
Spanish	Latin American	All
Bulgarian	Bulgarian	10,11,12
Bulgarian	Bulgarian –Standard	13
Swedish	Swedish	All
Swedish	Swedish –Legacy	12,13
Swedish	Swedish - Pro	10, 11
Czech	Czech	All
Danish	Danish	All
Finnish	Finnish	All
Hungarian	Hungarian	All
Italian	Italian	All
Italian	Italian - Typewriter	10,11
Italian	Italian –QZERTY	12,13
Greek	Greek	All
Belgian	Belgian	All
Dutch	Dutch	All
Romanian	Romanian - Standard	All
Russian	Russian	All
Russian	Russian - PC	All
Croatian	Croatian - PC	All

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
Slovak	Slovak	All
Slovak	Slovak - QWERTY	All
Turkish	Turkish F	All
Turkish	Turkish Q	All
Portuguese	Brazilian	All
Portuguese	Brazilian - ABNT2	All
Portuguese	Brazilian –Legacy	12,13
Portuguese	Brazilian - Pro	10,11
Portuguese	Portuguese	All
Ukrainian	Ukrainian - PC	10,11
Ukrainian	Ukrainian	12,13
Belarusian	Belarusian	All
Slovenian	Slovenian	All
Estonian	Estonian	All
Polish	Polish - Pro	10,11
Polish	Polish	12,13
Icelandic	Icelandic	All
Norwegian	Norwegian	All
Japanese	Katakana	All
Japanese	Half-width Katakana	All
Japanese	Romaji	All
Japanese	Full-width Romaji	All
Japanese	Hiragana	All
Japanese	Alphanumeric (Google)	All
Japanese	Hiragana (Google)	All
Japanese	Katakana (Google)	All
Japanese	Half-width Katakana (Google)	All
Japanese	Full-width Alphanumeric (Google)	All

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

Language on Mac	Input Source on Mac	Applicable Mac OS version
Korean	2-Set Korean	All
Chinese, Simplified	Pinyin - Simplified	All
Chinese, Simplified	Sogou pinyin	All
Chinese, Traditional	Pinyin - Traditional	All
Chinese, Traditional	Cangjie - Traditional	All
Chinese, Traditional	Zhuyin - Traditional	All
Chinese, Traditional	Sucheng - Traditional	All

By default, the keyboard layout synchronization feature is turned on. To control this feature alone, open the **Config** file in the ~/**Library**/**Application Support**/**Citrix Receiver**/ folder, locate the "**EnableIMEEnhancement**"setting and turn the feature on or off by setting the value to "true"or "false," respectively.

> **Note:**
>
> The setting change takes effect after restarting the session.

Keyboard input mode enhancements

Citrix Workspace app for Mac provides the UI to configure the keyboard input mode.

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

1. From the Citrix Workspace app icon in the menu bar, click the account icon in the top-right corner and navigate to **Preferences > Keyboard**.

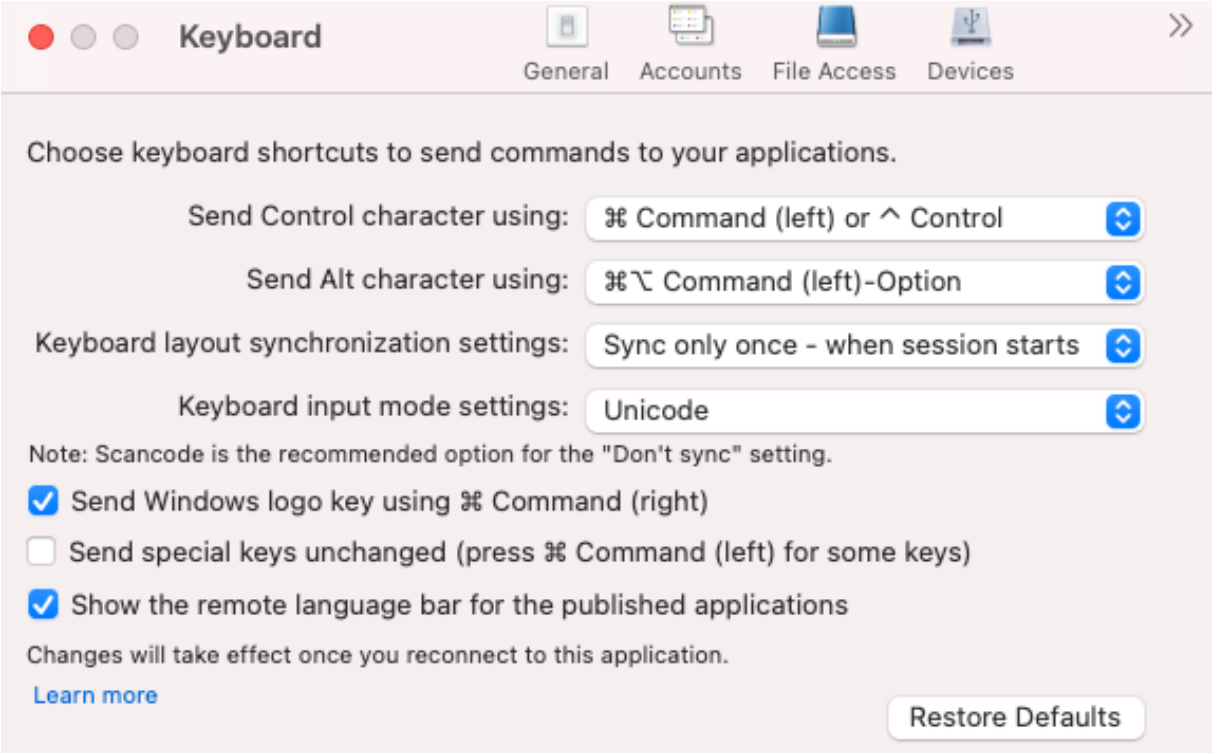
   The Keyboard input mode settings appear

2. Select from one of the following options:

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

This enhancement is enabled by default.

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



For example, consider a scenario where you're using a US international keyboard layout and the VDA is using the Russian keyboard layout. When you choose **Scancode** and type the key next to **Caps Lock**, the scancode "1E"is sent to the VDA. The VDA then uses "1E"to display the character "ф". If you choose **Unicode** and type the key next to **Caps Lock**, the character "a"is sent to the VDA. So, even if the VDA uses the Russian keyboard layout, the character "a"appears on the screen.

Citrix® recommends the following keyboard input mode for the different keyboard layout sync options:

- Scancode mode for **Don't Sync** option.
- Unicode mode for **Allow dynamic sync** and **Sync only once - when session starts**

> **Note:**
>
> The keyboard configuration changes take effect once you reconnect to the application.

You can change the configuration of Keyboard input mode in the Citrix Workspace app UI. However, for best performance, use the Citrix-recommended modes for different scenarios, physical keyboards, and client devices.

Language bar

You can choose to show or hide the remote language bar in an application session using the GUI. The language bar displays the preferred input language in a session. In earlier releases, you might change

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

this setting using only the registry keys on the VDA. Starting with Citrix Workspace for Mac version 1808, you can change the settings using the **Preferences** dialog. The language bar appears in a session by default.

> **Note:**
>
> This feature is available in sessions running on VDA 7.17 and later.

Configure showing or hiding the remote language bar

1. Open Preferences.
2. Click Keyboard.
3. Click or unclick Show the remote language bar for the published applications.

> **Note:**
>
> The setting changes take effect immediately. You can change the settings in an active session. The remote language bar does not appear in a session if there's only one input language.

Support synchronization for more keyboard layouts

Starting with the 2304 version, Citrix Workspace app for Mac supports keyboard layout synchronization for the following layouts or Input Method Editors (IMEs):

- English ABC
- English ABC - India
- Chinese, Traditional: Zhuyin - Traditional
- Chinese, Traditional: Sucheng - Traditional
- Google Japanese IME
- Sougou Chinese IME

Support for non-English-language Input Method Editors (IME) keyboard layouts

Support for non-English language IME keyboard layouts continues to work uninterrupted after the Carbon APIs are deprecated with the Cocoa APIs.

Windows special keys

Citrix Workspace app for Mac provides several options and easier ways to substitute special keys such as function keys in Windows applications with Mac keys. Use the **Keyboard** tab to configure the options you want to use, as follows:

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

- **Send Control character using**: Lets you choose whether to send Command-character keystroke combinations as Ctrl+character key combinations in a session. Select "Command or Control" from the pop-up menu to send familiar Command-character or Ctrl-character keystroke combinations on the Mac as Ctrl+character key combinations to the PC. If you select Control, you must use Ctrl-character keystroke combinations.
- **Send Alt character using**: Lets you choose how to replicate the Alt key within a session. If you select Command-Option, you can send Command-Option and keystroke combinations as Alt+ key combinations within a session. Alternatively, if you select Command, you can use the Command key as the Alt key.
- **Send Windows logo key using Command (right)**: Lets you send the Windows logo key to your remote desktops and applications when you press the Command key on the right side of the keyboard. If this option is disabled, the right Command key has the same behavior as the left Command key according to the above two settings in the preferences panel. However, you can still send the Windows logo key using the Keyboard menu; choose **Keyboard > Send Windows Shortcut >** Start.
- **Send special keys unchanged**: Lets you disable the conversion of special keys. For example, the combination Option-1 (on the numeric keypad) is equivalent to the special key F1. You can change this behavior and set this special key to represent 1 (the number one on the keypad) in the session. To do this, select the "Send special keys unchanged" checkbox. By default, this checkbox isn't selected so Option-1 is sent to the session as F1.

You send the function and other special keys to a session using the **Keyboard** menu.

If your keyboard includes a numeric keypad, you can also use the following keystrokes:

PC key or action	Mac options
INSERT	0 (the number zero) on the numeric keypad. Num Lock must be off; you can turn this on and off using the **Clear** key; Option-Help
DELETE	Decimal point on the numeric keypad. Num Lock must be off; you can turn this on and off using the **Clear** key; Clear
F1 to F9	Option-1 to -9 (the numbers one to nine) on the numeric keypad
F10	Option-0 (the number zero) on the numeric keypad
F11	Option-Minus Sign on the numeric keypad
F12	Option-Plus Sign on the numeric keypad

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

Windows shortcuts and key combinations

Remote sessions recognize most Mac keyboard combinations for text input, such as Option-G to input the copyright symbol ©. Some keystrokes you make during a session, however, do not appear on the remote application or desktop. The Mac operating system interprets them. This can result in keys triggering Mac responses instead.

You might also want to use certain Windows keys, such as Insert, that many Mac keyboards do not have. Similarly, some Windows 8 keyboard shortcuts display charms and app commands, and snap and switch apps. Mac keyboards do not mimic these shortcuts. However, these can be sent to the remote desktop or application using the **Keyboard** menu.

Keyboards and the ways keys are configured can differ widely between machines. Citrix Workspace app for Mac therefore offers several choices to ensure that keystrokes can be forwarded correctly to hosted applications and desktops. These keystrokes are listed in the table. The default behavior is described. If you adjust the defaults (using the Citrix Workspace app or other preferences), different keystroke combinations might be forwarded and other behavior might be observed on the Remote PC Access.

> **Important**
>
> Certain key combinations listed in the table aren't available when using newer Mac keyboards. In most of these cases, keyboard input can be sent to the session using the Keyboard menu.

Conventions used in the table:

- Letter keys are capitalized and do not imply that the Shift key must be pressed simultaneously.
- Hyphens between keystrokes indicate that keys must be pressed together (for example, Control-C).
- Character keys create text input and include all letters, numbers, and punctuation marks. Special keys do not create input by themselves but act as modifiers or Controllers. Special keys include Control, Alt, Shift, Command, Option, arrow keys, and function keys.
- Menu instructions relate to the menus in the session.
- Depending on the configuration of the user device, some key combinations might not work as expected, and alternative combinations are listed.
- Fn refers to the Fn (Function) key on a Mac keyboard. The function key refers to F1 to F12 on either a PC or Mac keyboard.

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

Windows key or key combination	Mac equivalents
Alt+character key	Command–Option–character key (for example, to send Alt-C, use Command-Option-C)
Alt+special key	Option–special key (for example, Option-Tab); Command–Option–special key (for example, Command-Option-Tab)
Ctrl+character key	Command–character key (for example, Command-C); Control–character key (for example, Control-C)
Ctrl+special key	Control–special key (for example, Control-F4); Command–special key (for example, Command-F4)
Ctrl/Alt/Shift/Windows logo + function key	**Choose Keyboard > Send Function** key > Control/Alt/Shift/Command-Function key
Ctrl+Alt	Control-Option-Command
Ctrl+Alt+Delete	Control-Option-Fn-Command-Delete; Choose **Keyboard > Send Ctrl-Alt-Del**
Delete	Delete; Choose **Keyboard > Send Key > Delete**; Fn-Backspace (Fn-Delete on some US keyboards)
End	End; Fn-Right Arrow
Esc	Escape; Choose **Keyboard > Send Key > Escape**
F1 to F12	F1 to F12; Choose **Keyboard > Send Function Key > F1 to F12**
Home	Home; Fn-Left Arrow
Insert	Choose **Keyboard > Send Key > Insert**
Num Lock	Clear
Page Down	Page Down; Fn-Down Arrow
Page Up	Page Up; Fn-Up Arrow
Spacebar	Choose **Keyboard > Send Key > Space**

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

Windows key or key combination	Mac equivalents
Tab	Choose **Keyboard > Send Key > Tab**
Windows logo	Command (Right) key (a keyboard preference, enabled by default); Choose **Keyboard > Send Windows Shortcut > Start**
Key combination to display charms	Choose **Keyboard > Send Windows Shortcut > Charms**
Key combination to display app commands	Choose **Keyboard > Send Windows Shortcut > App Commands**
Key combination to snap apps	Choose **Keyboard > Send Windows Shortcut > Snap**
Key combination to switch apps	Choose **Keyboard > Send Windows Shortcut > Switch Apps**

Use Input Method Editors (IME) and international keyboard layouts

Citrix Workspace app for Mac allows you to use an Input Method Editor (IME) on either the user device or on the server.

When client-side IME is enabled, users can compose text at the insertion point rather than in a separate window.

Citrix Workspace app for Mac also allows users to specify the keyboard layout they want to use.

To enable client-side IME

1. From the Citrix Viewer menu bar, choose **Keyboard > International > Use Client IME**.
2. Ensure that the server-side IME is set to direct input or alphanumeric mode.
3. Use the Mac IME to compose text.

To indicate explicitly the starting point when composing text

- From the Citrix Viewer menu bar, choose **Keyboard > International > Use Composing Mark**.

To use server-side IME

- Ensure that the client-side IME is set to alphanumeric mode.

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

Mapped server-side IME input mode keys

Citrix Workspace app for Mac provides keyboard mappings for server-side Windows IME input mode keys that aren't available on Mac keyboards. On Mac keyboards, the **Option** key is mapped to the following server-side IME input mode keys, depending on the server-side locale:

Server-side system locale	Server-side IME input mode key
Japanese	Kanji key (Alt + Hankaku/Zenkaku in Japanese keyboard)
Korean	Right-Alt key (Hangul/English toggle on Korean keyboard)

To use international keyboard layouts

- Ensure both client-side and server-side keyboard layouts are set to the same locale as the default server-side input language.

Restore default keyboard settings

If you had previously modified the keyboard preferences in the Citrix Workspace app, you can now restore the default keyboard settings. To restore the keyboard settings to its default values, open the Citrix Workspace app and navigate to **Preferences** > **Keyboard**. Then, click **Restore Defaults** and click **Yes** to confirm.

Deprecation of International menu from the keyboard settings

Previously, you can enable or disable the **Use Client IME, Use Composing Mark and Use Client keyboard layout** features in the Citrix viewer by navigating to **Devices > Keyboard>International**.

From the 2311 version, the **International** menu for the keyboard settings in the Citrix Viewer is deprecated. From this version, the client-side IME is enabled by default.

Support for system shortcuts on HDX™ desktop sessions

Previously, the system keyboard shortcuts such as **Option-Command-ESC, Command-Space bar, Command-Tab, Control-Command-Q, Shift-Command-Q, Control Up/Down/Left/Right** took effect only on macOS locally since they were consumed by macOS at first.

Starting with the 2402 version, Citrix Workspace app for Mac supports passing the macOS system keyboard shortcuts to the VDA (HDX session) in window mode and full-screen mode. This feature allows

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

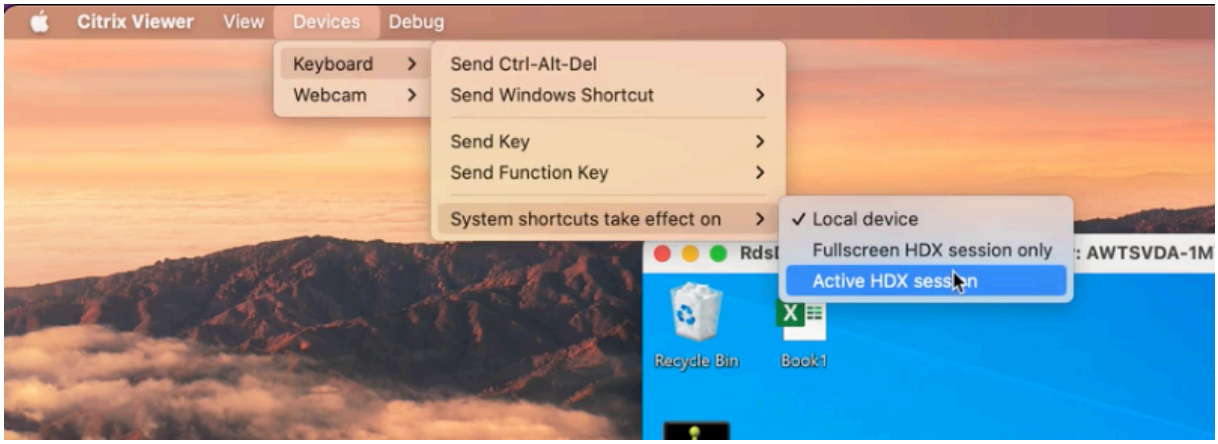
you to set preferences on how the system shortcut must take effect on macOS locally or the HDX desktop session in window or full-screen mode.

The following options in the keyboard settings allow you to control the system shortcuts:

- **Local device:** The system shortcuts can take effect only on macOS locally. It does not affect the HDX session. The **Local device** option is the default option.
- **Fullscreen HDX session only:** The system shortcuts take effect on HDX sessions when the session is in full-screen mode. If the session is in window mode or there are no active sessions, then the system shortcuts have no effect on HDX sessions.
- **Active HDX session:** The system shortcuts take effect on HDX sessions when the session is in window mode and full-screen mode. If there is no active HDX session or the active session window on the front, then the system shortcuts can take effect only on the macOS locally.

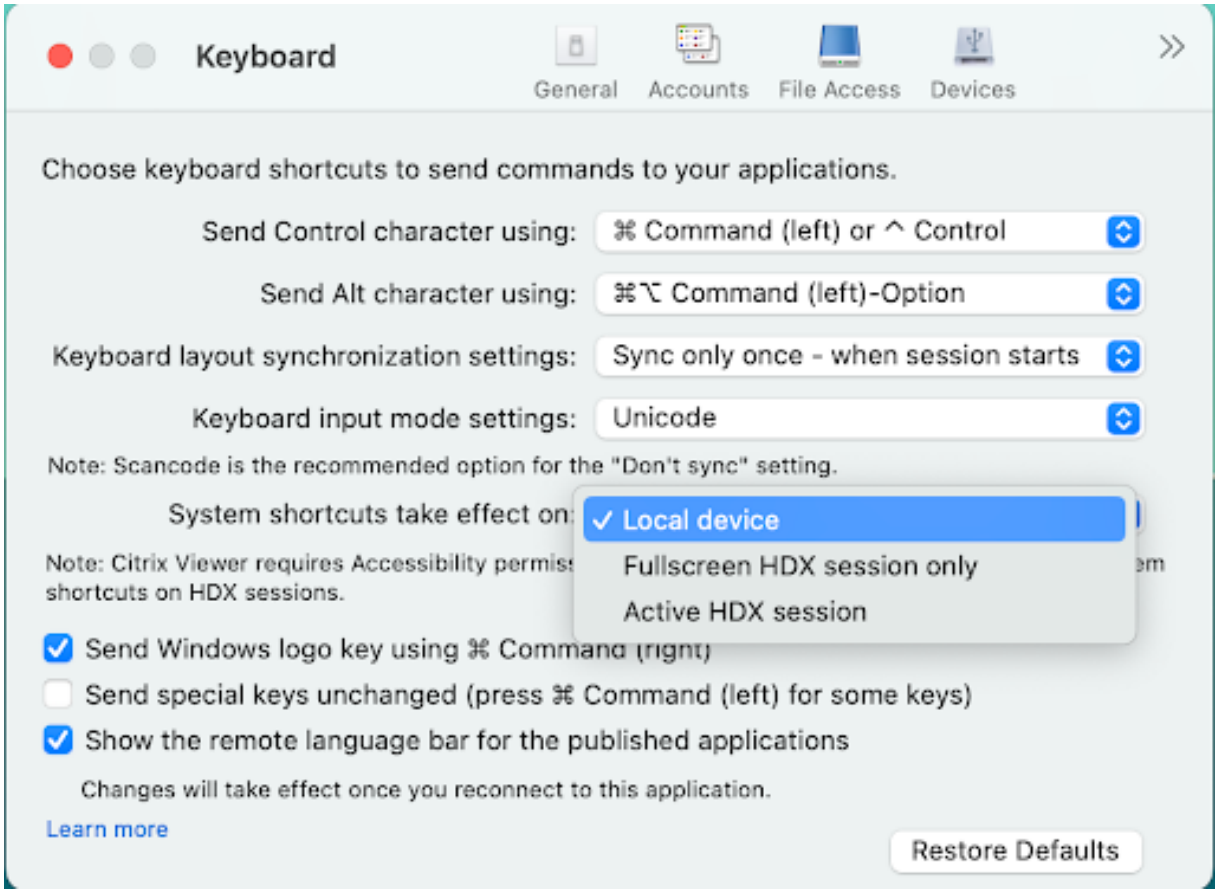
To enable the system shortcuts to take effect on the HDX session, open the HDX session. In the **Citrix Viewer** menu bar, navigate to **Devices > Keyboard > System shortcuts take effect on** and select **Fullscreen HDX session only** or **Active HDX session**.

> **Note:**
>
> When enabling system shortcuts for HDX sessions, you are prompted to provide accessibility access to Citrix Viewer to use this feature. To provide accessibility access to **Citrix Viewer**, click **Open System Settings** in the dialog box and enable accessibility access to **Citrix Viewer**. For more information, see Allow accessibility apps to access your Mac in the Apple support article.



Alternatively, you can enable the system shortcuts to take effect on HDX sessions in full-screen or window mode by navigating to **Preferences > Keyboard**. Select **Fullscreen HDX session only** or **Active HDX session** options from the **System shortcuts take effect on** drop-down menu.

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



Enhancement to the keyboard Settings

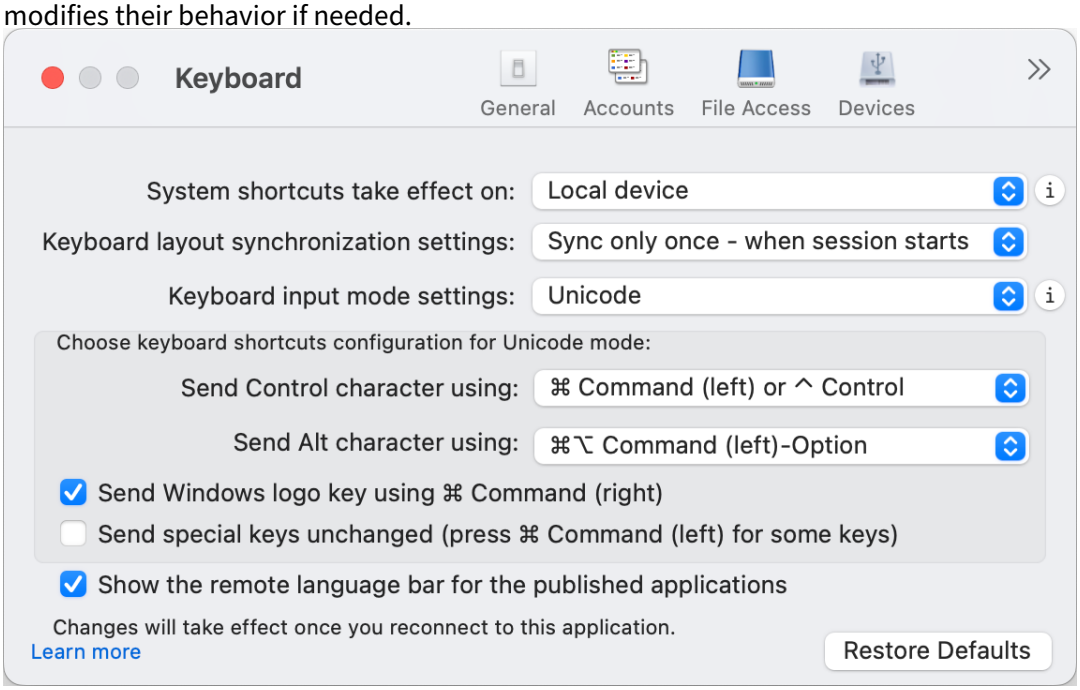
Starting with the 2405 version, Citrix Workspace app now provides an improved keyboard settings user interface (UI) by categorizing setting options and adding helpful tip icons.

The following settings are now available as secondary options under the **Unicode input mode** setting:

- Send Control character using
  - This setting specifies an alternative key to act as the Control key (often used for shortcuts like Ctrl+C for copy) within the virtual session. On different keyboards or operating systems, the Control key might be in different locations, so this setting allows customization to maintain consistency for a better user experience.
- Send Alt character using
  - This setting specifies which key can act as the Alt key (used for accessing alternate functions of keys, like Alt+Tab for switching windows).
- Send Windows logo key using Command (right)

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

    - This setting specifies the right Command key on a Mac keyboard to function as the Windows logo key. This setting is particularly useful for macOS users who use the Command key frequently but need the functionality of the Windows logo key when using Windows or applications that recognize it.
- Send special keys unchanged (press Command (left) for some keys)
    - This setting keeps certain special keys (like function keys, escape, etc.) unchanged in their function, except when the left Command key is pressed. It allows for a hybrid approach where the default behavior of special keys is retained, but pressing the left Command key modifies their behavior if needed.



Enhancement to Option + Mouse Click Behavior

Starting with version 2505.10, the mapping of **Option + mouse click** to right-click behavior has been disabled to restore native Mac functionality. This change enables critical use cases for professional applications that require the **Option/Alt** key modifier during mouse interactions.

Key benefits

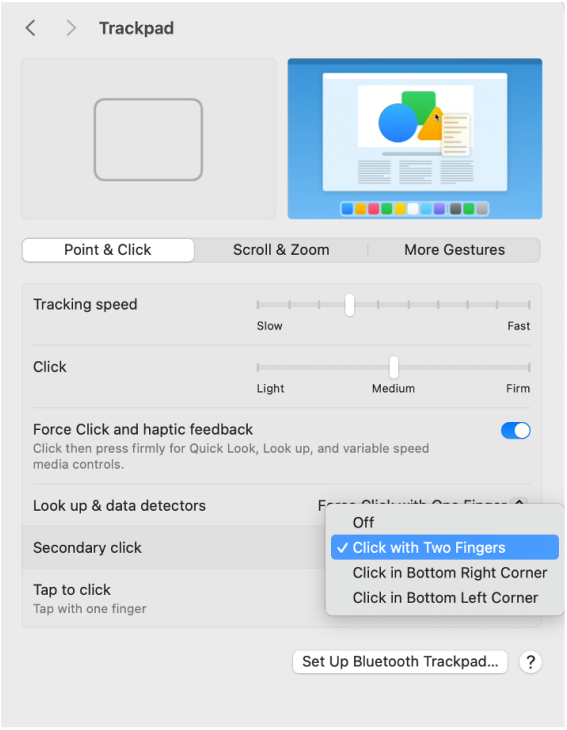
- **Adobe Photoshop on Mac VDA:** Users can hold the **Option** key to change tool behavior before clicking, enabling proper tool functionality.
- **Windows VDA applications: Alt + mouse** click works correctly for specific actions such as:
    - Vertical editing in Notepad++
    - Option + mouse drag to copy objects in Figma

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

Right-click access

Mac users can still access right-click functionality through their preferred input method:

- **For trackpad users:** Secondary Click is configured as **Click with Two Fingers** (Mac system default).
- **For Apple magic mouse users:** Secondary Click is configured as **Click right side** (Mac system default) or can be performed using **Control+Click**.





This enhancement ensures that Mac users can access right-click functionality through their native input methods while preserving the **Option/Alt** key behavior required for professional applications.

Printing

Starting with the 2203.1 release, you can use PDF universal printing when printing from a Mac device. If you choose to use PDF Universal Printing, you no longer need to install the HP Color LaserJet 2800 Series PS driver when auto-creating printers with Universal Print Driver.

PostScript Printing

By default, the auto-redirected client printers are created with the Citrix UPD with PostScript support. For more information, see support article CTX296662.

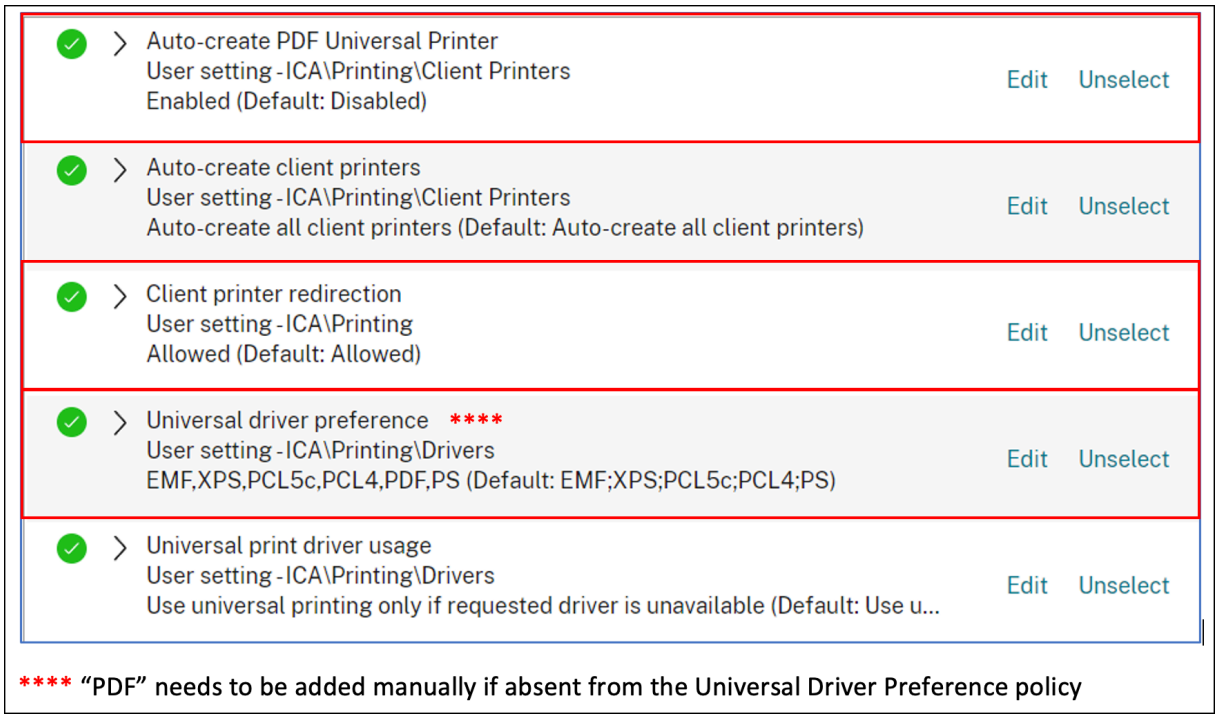
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify the settings for the Universal Print Driver Priority, Universal Print Driver Usage, and Client Printer Redirection are all set to default. Also ensure that you've installed the HP Color LaserJet 2800 Series PS driver on the VDA.
For more information about installing the driver, see support article CTX140208.

PDF Universal Printing

Prerequisites:

- Citrix Workspace app for Mac version 2112 or later - Enables consumption of PDF print streams for Citrix Workspace app for Mac.
- Citrix Virtual Apps and Desktops™ version 2112 or later - Enables PDF universal printing for auto-created client printers.
- Enable the Client printer redirection policy in the Citrix Studio or web console.



**** "PDF" needs to be added manually if absent from the Universal Driver Preference policy

You can print via PDF once you configure either or both of the following options:

1. Provide a single PDF Universal Printer created in each session.
2. Use the UPD for regular auto-created printers.

Provide a single PDF Universal Printer created in each session

To enable creation of the **PDF Universal Printer** in sessions from a Mac client or any other PDF enabled client endpoint, go to Citrix Studio or the web console and enable the **Auto-Create PDF uni-**

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

versal printer policy.
Once the policy is enabled, the PDF universal printer is created in the session. The printer is called **Citrix PDF Printer**.

Use this printer in a session to generate a PDF output that delivers to the client. Also, send the pdf output to the default PDF handling application on the endpoint. For the macOS client, this PDF handling application is typically the built-in **Preview** application, but it could be any registered PDF handling application such as Adobe Acrobat Reader.

Use the UPD for regular auto-created printers

To enable PDF universal printing for all redirected client printers in a session, visit Citrix Studio or a web console from a Mac client. Then, configure the Universal print driver priority policy to place the PDF metafile format in before PS within the priority list.

After this configuration, the Citrix PDF Universal Driver replaces the HP Color LaserJet 2800 Series PS driver on the host for automatically created printers. The automatically created printers use a universal driver with a Mac client that can print PDFs.
When using one of the auto-created printers in a session, PDF is used as the intermediate format of the print job. But the print output flows directly to the selected client-attached printer.

Support for printing PDF documents with selected orientation

Starting with the 2405 version, you can now print PDF documents with the correct orientation whether it's portrait or landscape. This feature ensures that the printed output aligns perfectly with the intended layout. This feature is enabled by default.

> **Note:**
>
> For printing diagnostics on macOS endpoints, administrators may enable additional Citrix Workspace app settings in the `config` file. Certain diagnostic-level options can expose **personally identifiable information (PII)**, such as user names, device identifiers, or session details.
>
> Ensure you handle, store, and share configuration files and logs in accordance with your organization's data-protection and privacy policies, and share diagnostic output only through approved channels.

PDF printing enhancements

Starting with version 2607, Citrix Workspace app for Mac queries connected printers for their capabilities and presents printer-specific settings in the VDA print dialog when using the PDF Universal Print Driver (UPD). With enhanced PDF printing, print jobs are routed directly to the auto-created client

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

printer, and print ticket settings selected in the VDA print dialog—such as duplex, orientation, color mode, and stapling—are passed through to the client printer and honored.

USB

USB Redirection of mass storage devices

Starting with version 2503, USB redirection enables you to access USB mass storage devices connected to a local computer from your virtual apps and desktops, allowing you to use USB drives seamlessly within virtual sessions. This feature is enabled by default.

Prerequisites:

- USB mass storage devices must be connected to the local device.
- The USB redirection policy must be enable in store.

> **Note:**
>
> The system triggers a **Disk Not Ejected Properly** message for users. This is a controlled behavior, designed to gain control of the device when existing drivers do not respond to seize requests.

Use the following command to disable the feature:

```
1 defaults write com.citrix.receiver.nomas EnableUSBMassStorage NO
```

Limitations:

Users cannot redirect two USB mass storage devices that share the same Product ID and Vendor ID simultaneously.

Support for managing composite USB device redirection using DDC policies

Starting with the 2409 version, you can manage the composite USB device redirection using the DDC policies.

With this release, Citrix Workspace™ app for Mac supports the following policies which help you to manage the usage of the composite USB device redirection:

- Client USB device redirection
- Client USB device redirection rules
- Client USB device redirection rules (Version 2)
- Allow existing USB devices to be automatically connected
- Allow newly arrived USB devices to be automatically connected

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

Note:
For more information about configuring the preceding policies, see Client USB device redirection in the Citrix Virtual Apps and Desktops document.

Desktop Viewer's updates according to the polices:

- If the **Client USB device redirection** policy is set to **Prohibited** on DDC, the **Devices** on the toolbar is set to insensible and the **Devices** option on the **Citrix Workspace app - Preferences** screen won't be visible.
- Based on the values set for **Allow existing USB devices to be automatically connected** and **Allow newly arrived USB devices to be automatically connected** policies, the following checkboxes might be enabled or disabled on the **Devices** option on the **Citrix Workspace app - Preferences** screen:
    - When a session starts, connect devices automatically.
    - When a new device is connected while a session is running, connect devices automatically.

Limitation:

If the users only redirect one interface of a composite USB device for an application, then the other interfaces can't be used by other applications.

USB redirection

HDX™ USB device redirection enables redirection of USB devices to and from a user device. A user can connect a flash drive to a local computer and access it remotely from a virtual desktop or a desktop hosted application.

During a session, users can plug and play devices, including Picture Transfer Protocol (PTP) devices. For example:

- Digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players
- Point-of-sale (POS) devices, and other devices such as 3D Space Mice, Scanners, Signature Pads and so on.

> **Note:**
>
> Double-hop USB is not supported for desktop-hosted application sessions.

USB redirection is available for the following:

- Windows
- Linux
- Mac

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

By default, USB redirection is allowed for certain classes of USB devices, and denied for others. To restrict the types of USB devices made available to a virtual desktop, update the list of USB devices supported for redirection. More information is provided later in this section.

> **Tip**
>
> Where security separation between the user device and server is needed, ensure that you inform users about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide superior performance and bandwidth efficiency over a WAN. Optimized virtual channels are usually the best option, especially in high latency environments.

> **Note:**
>
> For USB redirection purposes, Citrix Workspace app for Mac handles a SMART board the same as a mouse.

The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports. For example, a CDM virtual channel is used to view files on a camera or to provide audio to a headset. The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

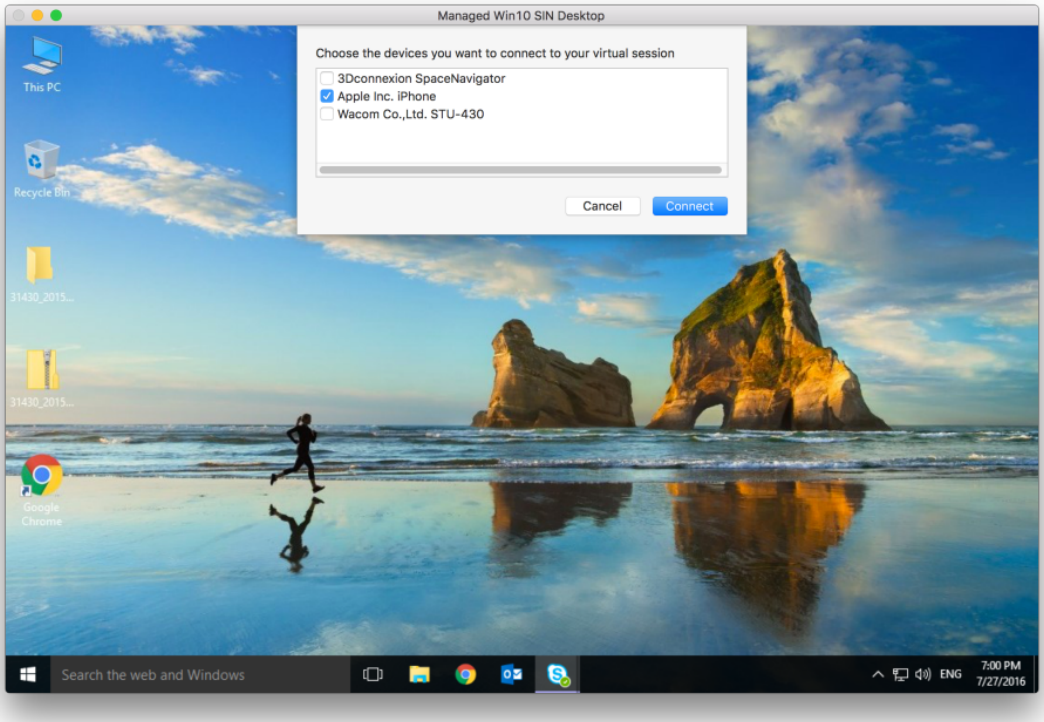
Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, might not work as expected with the optimized virtual channel. Use the Generic USB virtual channel as an alternative.

Certain devices are not redirected by default, and are only available to the local session. For example, it would not be appropriate to redirect a NIC that is directly attached via internal USB.

To use USB redirection:

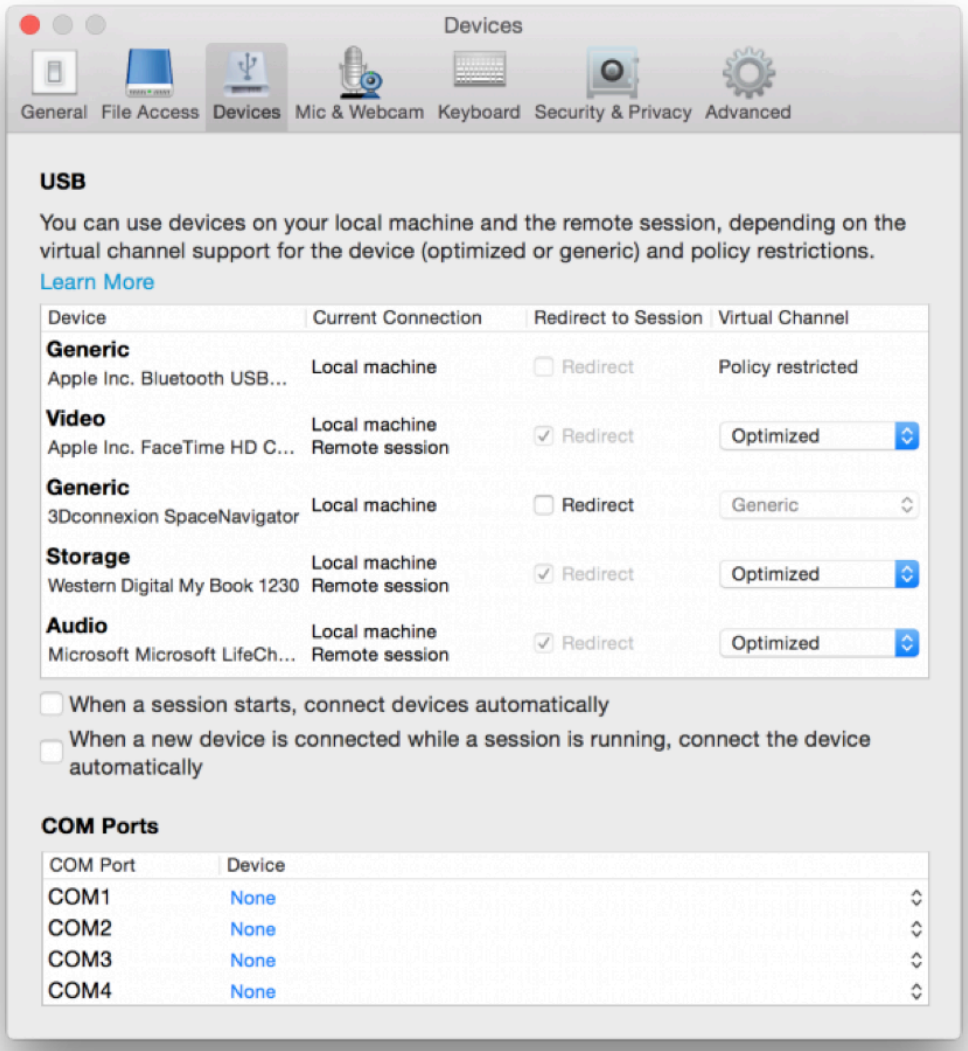
1. Connect the USB device to the device where Citrix Workspace app for Mac is installed.
2. You are prompted to select the available USB devices on your local system.

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

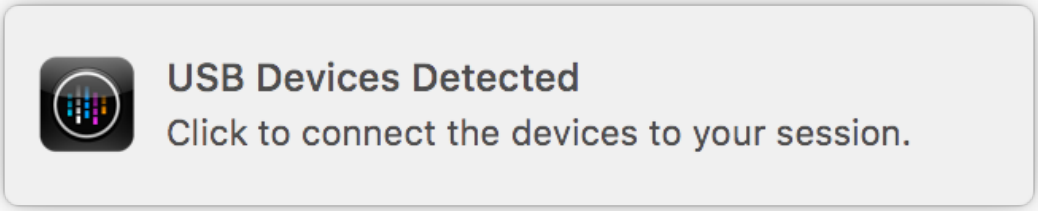


3. Select the device you want to connect and click **Connect**. If the connection fails, an error message appears.
4. In the **Preferences** window **Devices** tab, the connected USB device is listed in the USB panel:

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



5. Select the type of virtual channel (Generic or Optimized) for the USB device.
6. A message is displayed. Click to connect the USB device to your session:



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

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session. When using Citrix Workspace app for Mac, the following applies:

- Devices connected after a session starts immediately appear in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, sometimes you can resolve the problem by waiting to connect the device until after the virtual session has started.
- To avoid data loss, use the **Windows Safe** removal menu before removing the USB device.

Supported USB devices

With Apple announcing the deprecation of Kernel Extensions (KEXT), Citrix Workspace app for Mac migrated to the new user mode USB framework `IOUSBHost` provided by Apple. This article lists the supported USB devices.

USB devices that are compatible with USB redirection The following USB devices work seamlessly with USB redirection:

- 3DConnexion SpaceMouse
- Mass Storage Devices
- Kingston DataTraveler USB Flash Drive
- Seagate external HDD
- Kingston/Transcend Flash drive 32 GB/64 GB
- NIST PIV smartcard /reader
- YubiKey

USB devices that fail with USB redirection The **Transcend SSD external Hard disk** device is not compatible with USB redirection:

Unverified USB Devices There are plenty of devices, unverified by Citrix, for successful USB redirection with Citrix Workspace app for Mac. Here are some of these devices:

- Other Hard Disks
- Special Keys on the keyboard and headsets that use a custom HID protocol

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

Support for Mass Storage devices

We have seen that not all types of Mass Storage devices can be redirected successfully. For the devices which fail to redirect, there is an optimized virtual channel called Client Drive mapping. Using the Client Drive mapping, access to the mass storage devices can be controlled through the policies on the delivery controller.

Support for Isochronous devices Generic USB redirection doesn't support the Isochronous class of USB devices in Citrix Workspace app for Mac. The isochronous mode of data transfer in a USB specification indicates devices that stream the timestamped data at a constant rate. For example: WebCams, USB Headphones, and so on

Support for Composite devices A USB composite device is a single gadget that can perform more than one function. For example: multi-function printers, iPhone, and so on. Currently, Citrix Workspace app for Mac does not support redirection of composite devices to the Citrix Virtual Apps and Desktops and Citrix DaaS session.

Alternatives for unsupported USB devices There are optimized virtual channels that can handle devices that are not supported with generic USB redirection. These virtual channels are optimized for speed when compared to generic USB redirection. Some examples are as follows:

- **Webcam redirection:** Optimized for raw webcam traffic. Microsoft Teams Optimization Pack has its own method of webcam redirection. Hence, it does not fall under the Webcam redirection virtual channel.
- **Audio redirection:** Optimized to transfer Audio streams.
- **Client Drive Mapping:** Optimized for redirecting mass storage devices to the Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session. For example: Flash Drives, Hard Disks, DVD ROM/RW, and so on.

Webcam

Adaptive Webcam Bitrate

Starting with version 2607, Citrix Workspace app for Mac automatically adjusts webcam video quality to match available network bandwidth in real time. The client continuously monitors network conditions and adapts the webcam stream accordingly —reducing bitrate when the network is constrained and restoring quality as bandwidth recovers.

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

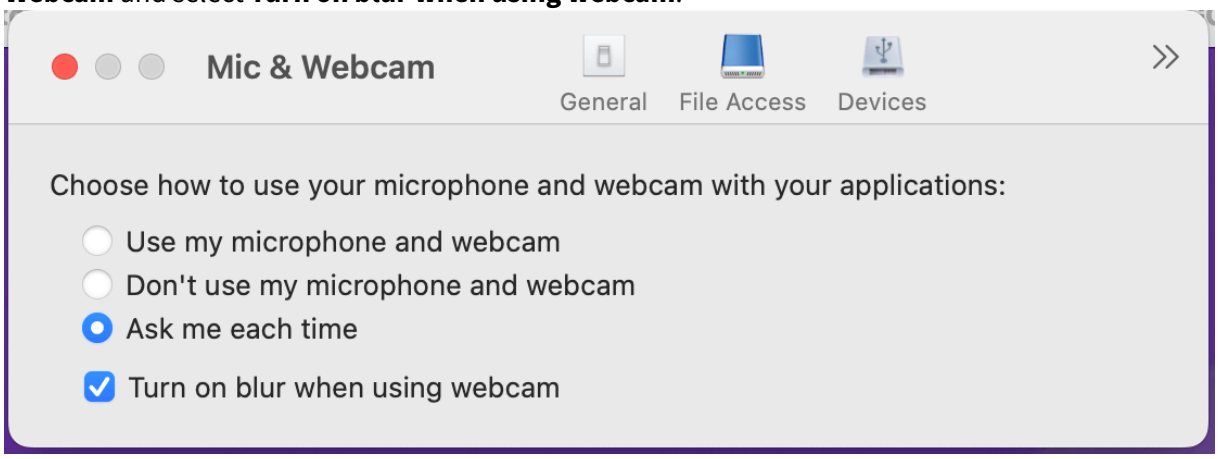
This feature requires no configuration, reduces video freezing, and maintains video continuity, providing an optimal webcam stream and ensures that meetings and calls remain usable on variable networks.

Support for plug and play webcam redirection

Starting with the 2411 version, Citrix Workspace™ app for Mac supports plug and play (PnP) webcam redirection for Linux VDA and Windows VDA. With this feature, when you connect a built-in or external camera to your device, it is automatically detected in the virtual sessions. If you unplug a camera form the device, Citrix Workspace app for Mac can promptly detect the change and remove the disconnected cameras from your selection options in the virtual sessions.

Support for background blur for webcam

Starting with the 2402 version, Citrix Workspace app for Mac supports background blur when using a webcam. You can enable the background blurring feature by navigating to **Preferences > Mic & Webcam** and select **Turn on blur when using webcam**.



Support for continuity camera

Starting with the 2305 version, you can use the iPhone as your webcam with the continuity camera. For a seamless connection, mount your iPhone such that its camera is available to the Mac device. You must select **Webcam > Automatic Camera Selection** for the iPhone to appear automatically on the Mac device as an external camera. You can switch to any other camera manually, for example by selecting **Webcam > FaceTime HD Camera**. The Continuity Camera works wired or wirelessly and provides a high-quality image.

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

Prerequisites

- This feature is supported on a Mac device running on macOS version 13.
- This feature is supported on an iOS device running on iOS version 16.
- You must be signed into the same Apple account in the Citrix Workspace app on both your iOS device and Mac device.
- For a wired connection, the iPhone must be connected to the Mac device through a USB.
- For a wireless connection, the iPhone and Mac devices must be in proximity and have Bluetooth and Wi-Fi turned on.

Some of the advantages are:

- **Center Stage** - Keeps the image within the frame as you move around.
- **Portrait** mode - Blurs the background of the image.
- **Studio Light** - Provides a bright effect on the image. It dims the background and illuminates the image.
- **Desk View** –The iPhone splits the Ultra Wide camera feed into two. It shows the desk and faces both at the same time.
- **Share Windows** - The iPhone splits the Ultra Wide camera feed into two. It shows the desk and faces both at the same time. The share windows function available in the video conferencing apps can be used to share the Desk View feed.

Session experience

Session Pre-Launch support

Starting with version 2607, Citrix Workspace app for Mac supports Session Pre-Launch for virtual applications, establishing application sessions in the background before the user explicitly launches an app. When the user clicks an app, the pre-established session is reused immediately, significantly reducing the perceived launch time. This brings Session Pre-Launch for virtual applications to parity with Citrix Workspace app for Windows.

Pre-launch sessions are initiated automatically on login, store connect, settings refresh, and system wake. The app icon appears in the Dock only after the user launches an app. Virtual desktops are not currently supported for Session Pre-Launch.

Session Pre-Launch is triggered only when all of the following conditions are met:

- Pre-Launch is enforced through MDM (`EnablePreLaunchFromMDM`).
- Session Pre-Launch policy is enabled on Studio. For more information, see Configure session prelaunch and session linger in a delivery group.

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

Pre-Launch runs only in the native Citrix Workspace app for Mac flow. The browser extension and Workspace for Web do not trigger it, but they can reuse an existing prelaunch session.

The session prelaunch and session linger features help specified users access applications quickly, by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger).

Configuring session pre-launch using MDM

Session pre-launch is delivered through an MDM configuration profile using the macOS preference domain `com.citrix.receiver.nomas`. The value is a Boolean.

MDM key	Type	Required	Default	Description
`EnablePreLaunchFromMDM`	Boolean	Yes	**`false`**	Enables session pre-launch, enforced through MDM. When set to **`true`**, Citrix Workspace app pre-launches a session so that subsequent app or desktop launches start faster. When the key is absent, pre-launch is disabled.

The following is an example of an MDM configuration profile using a Custom Settings payload for the domain `com.citrix.receiver.nomas`:

```
1  <key>EnablePreLaunchFromMDM</key><true/>
```

Clipboard support for copying files and folders

Starting with version 2503, this enhancement enables clipboard support for seamless copying of files and folders between HDX™ sessions. Users can copy files and folders as permitted by their Citrix® administrators, enhancing flexibility and productivity.

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

With this feature, you can do the following:

- Copy files and folders between the HDX sessions seamlessly.
- Ensure files, folders, and content remain intact with no corruption during transfer.
- Admins can define and enforce policies to regulate and secure copy-paste operations, tailoring functionality to organizational needs.

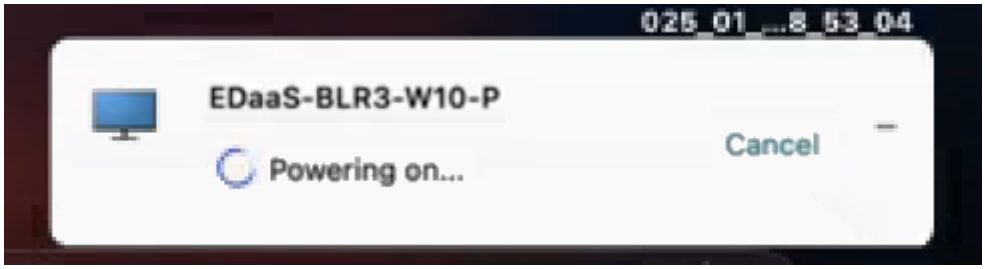
This feature is enabled by default through the clipboard redirection policy, allowing seamless copy and paste of files and folders. For more information, see Client clipboard redirection.

Enhanced desktop launch experience

Starting with version 2503, Citrix Workspace™ app for Mac enhances the desktop launch experience by removing the retry timeout setting and improving status messaging. This enhancement is enabled by default.

This update ensures that:

- Users no longer experience premature failures during the launch process, even if it takes a longer time to complete.
- Retry messages, such as **Powering On** and **Waiting for registration**, are now displayed, making it more intuitive for end users to check the status of the Virtual Delivery Agent.



Hybrid launch support for GACS for on-premises store

Starting with version 2503, Citrix Workspace app for Mac supports management using Global App Configuration Service (GACS) for on-premises store in hybrid launch. In a hybrid launch scenario, users access Citrix resources through a web browser. When an application or desktop is selected, Citrix StoreFront™ generates an ICA file with the necessary launch instructions. The locally installed Citrix Workspace app then reads the ICA file, and establishes a secure connection to the remote application or desktop.

Key Behavior:

- When a user launches a session, in-session settings apply from the next launch.

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

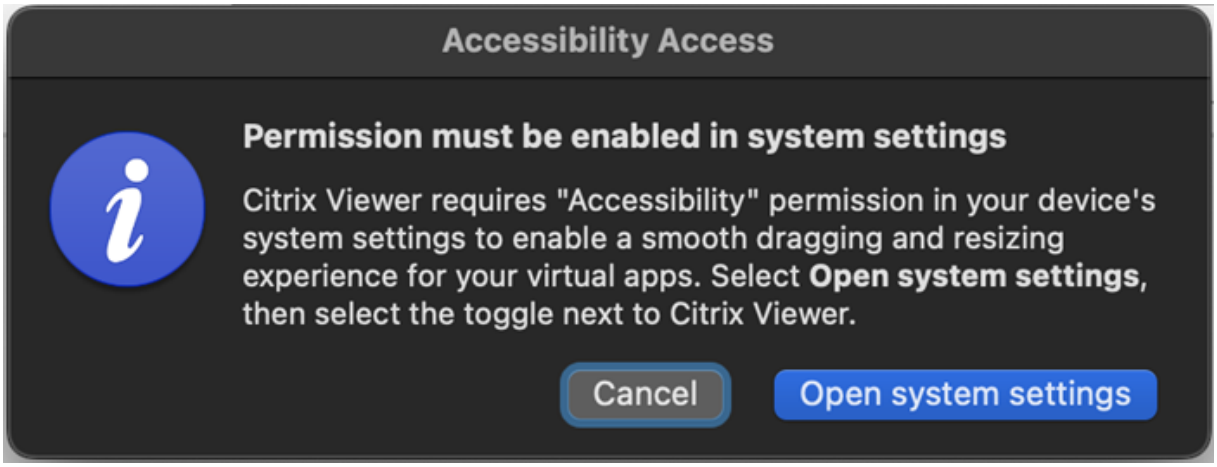
- If a store is added in the app and later accessed via a browser, settings are retrieved from the client app.
- Only the most recently accessed store applies its settings to the native app.

For example:

If a user first launches a session from one store, the app fetches and applies its GACS policies. Later, if the user switches to another store and launches a session, the app updates and applies the new store's GACS policies. For more information, see GACS supports hybrid launch.

Seamless drag and resize improvements

Starting with version 2411, the seamless drag and resize enhancement feature is automatically enabled when Citrix Workspace app for Mac connects to a Windows VDA version 2311 or later. This enhancement provides a smoother drag and resize experience for virtual apps, ensuring seamless interaction. This feature requires user-provided Accessibility permissions. If Citrix Viewer does not have the necessary permissions, a prompt appears requesting Accessibility permission.



Support for Rapid Scan

Starting with the 2409 version, Citrix Workspace app for Mac supports the Rapid scan feature. You can use this feature to scan multiple documents with an iOS device, and then transfer those scanned documents to a Mac device using the Citrix Workspace app for Mac and iOS.

If you're signed into Citrix Workspace on both your Mac and iOS device, you can use Rapid Scan to scan documents with your iPhone or iPad. The scanned files are saved on your Mac, and you can also access them remotely from a virtual desktop using Client Drive Mapping. This feature works for both cloud and on-premise stores.

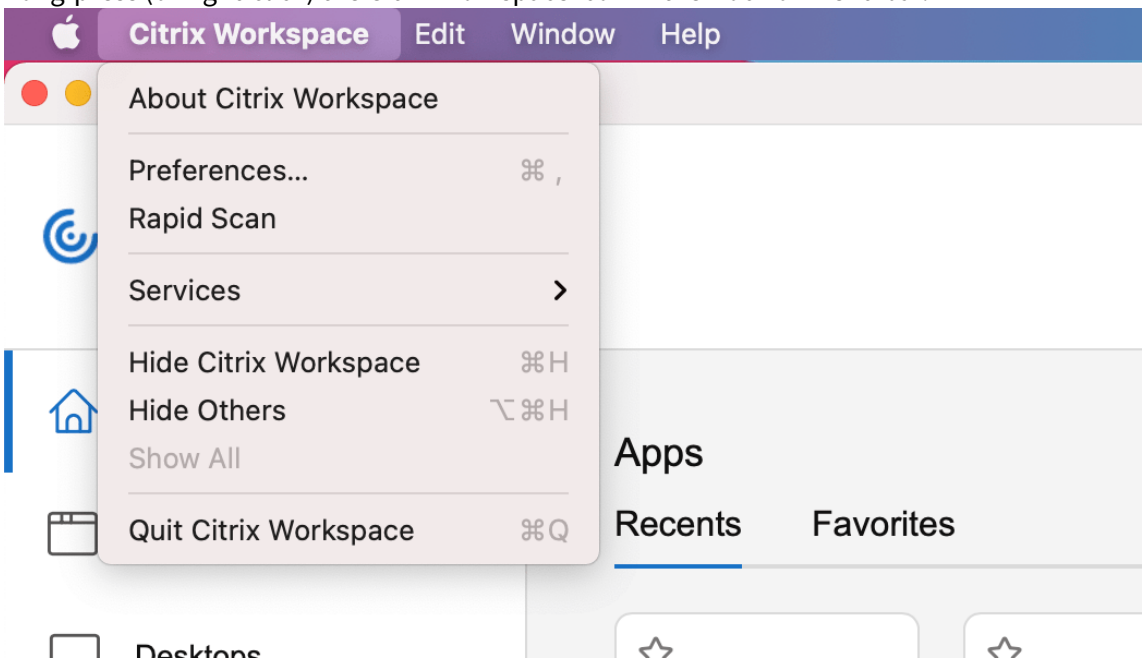
Prerequisites:

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

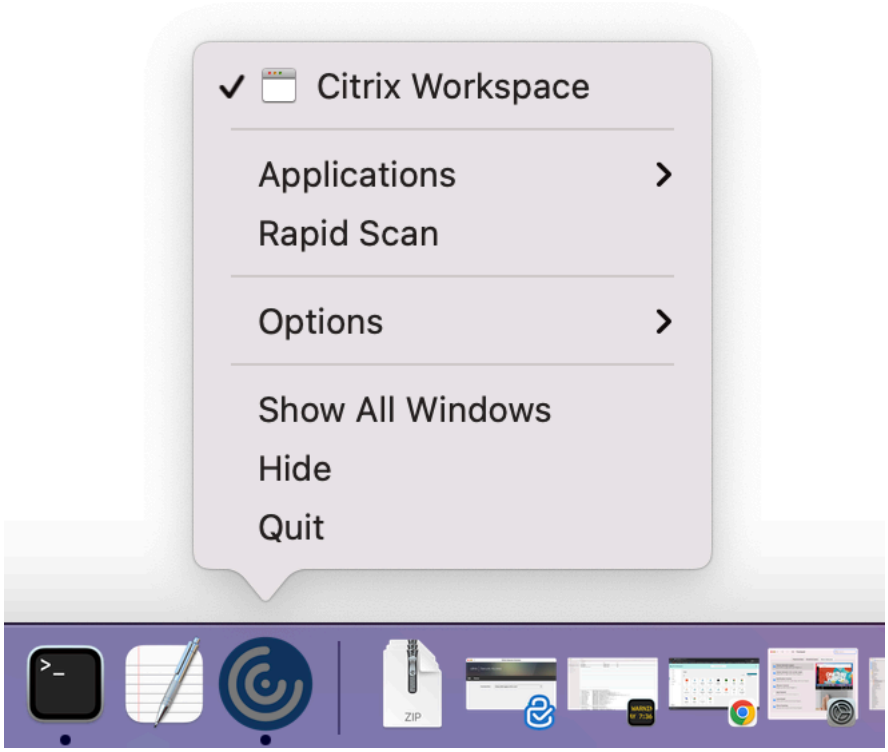
- Ensure that both devices are logged into the same Citrix Workspace account.
- Both devices must be connected to the same Wi-Fi network.
- The Citrix Workspace app for Mac must be version 2409 or higher.

How to Use Rapid Scan:

1. Open the Citrix Workspace app on your Mac.
2. Long-press (or right-click) the Citrix Workspace icon in the Dock or menu bar.



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



3. Select **Rapid Scan** from the menu. A QR code appears on your Mac screen.
4. On your iOS device, go to **Settings** and tap **Rapid Scan**.
5. Scan the QR code displayed on your Mac using your iOS device.
6. When the confirmation window appears on your Mac, click **Yes** to establish the connection. You can now use your iOS device to scan documents.
7. Choose to save the scanned files in PDF or JPEG format.
8. By default, the scanned documents are saved to the **Downloads** folder on your Mac.
9. After the download is complete, click **Open in Finder** on your Mac to locate the scanned documents.

Access scanned documents from a Virtual Desktop:

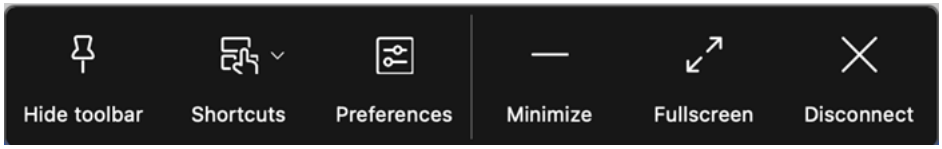
1. Client Drive Mapping (CDM) must be enabled to access your Mac's storage drives inside the Virtual Desktop. This allows you to transfer files between your Mac and the Virtual Desktop. Please contact your administrator to enable this feature.
2. Once CDM is enabled, your local drives is visible in the Virtual Desktop.
3. When prompted, allow **Read & Write** permissions to access your local disk from the Virtual Desktop.

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

4. Navigate to the folder where the scanned documents are stored (the **Downloads** folder by default) and copy the files to the Virtual Desktop's storage.

Enhanced Desktop Viewer toolbar

Starting with the 2409 version, the virtual **Desktop Viewer** toolbar is enhanced to be more intuitive, modern, and user-friendly. With this feature, you can now customize the Citrix Workspace app toolbar by adding and removing options on the toolbar.



The new toolbar provides the following options:

Show or hide toolbar	Click this button to show or hide the Desktop Viewer toolbar. A notch appears when the toolbar is hidden.
Shortcuts	Click this button to access the shortcuts.
Devices	Click this button to access the options in the **Devices** section.
Preferences	Click this button to access the options in the **Preferences** section.
Minimize	Click this button to minimize the virtual session. This option is hidden in the full-screen mode.
Fullscreen	Click this button to access the virtual session in full screen.
Restore	Click this button to restore the virtual session from the full-screen mode.
Disconnect	Click this button to sign out or to disconnect from a virtual session.

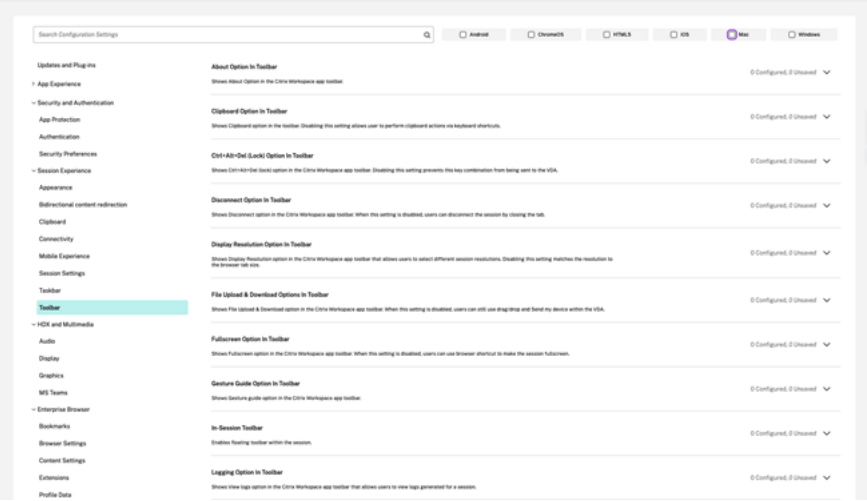
You can click and drag the toolbar across all screens in the virtual session. When you drag the toolbar, it can rotate automatically based on its placement on the screen. Once you release the drag, it gets positioned to the nearest edge of the screen.

You can configure this feature using the Global App configuration service (GACS) and Mobile Device Management (MDM).

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

Using GACS

1. Sign in to your Citrix Cloud™ account and navigate to **Workspace Configuration > App Configuration**.
2. From the list of configured URLs, select the one for which you want to map settings, and click **Configure**.



3. Under the **Toolbar** section, navigate to the required option in the toolbar and click the expand icon.
4. Select the Mac checkbox and then click **Edit**.
5. You can now customize the toolbar option to hide or show.
6. Click **Publish Drafts** to save the settings.

Using MDM

To hide the toolbar, administrators must use the following setting:

```
<key>EnableInSessionToolbar</key>
```

```
<false/>
```

To hide specific buttons in the toolbar, administrators must use the following setting:

```
<key>HiddenToolbarButtons</key>
```

```
<array>
```

```
`<string>preferences</string>`

`<string>minimize</string>`

`<string>fullscreen</string>`
```

```
</array>
```

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

The supported values include `ctrlAltDel`, `connectionStrength`, `device`, `shortcuts`, `preferences`, `minimize`, `fullscreen`, and `close`.

> **Note:**
>
> If no configuration is made, the session toolbar is displayed by default with all buttons.

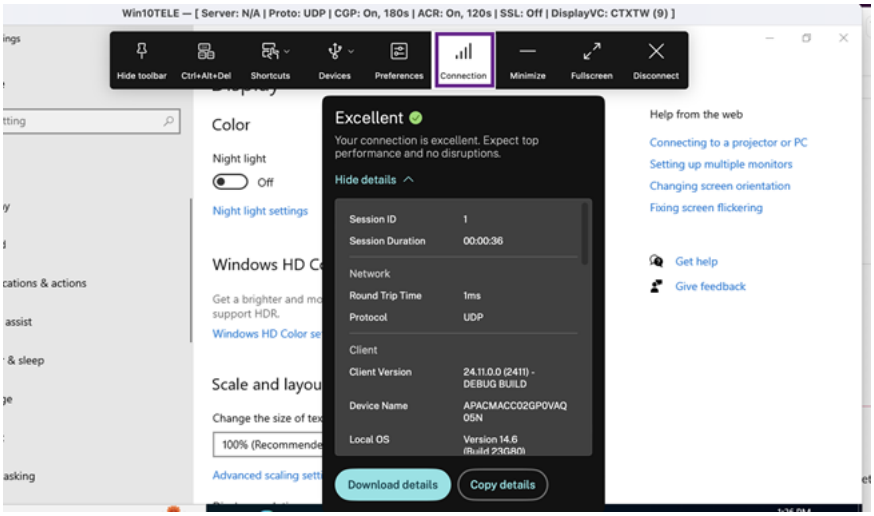
Connection Strength Indicator

Starting with version 2409, Citrix Workspace app for Mac supports the Connection Strength Indicator (CSI) on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. By clicking the icon, you can view real-time connection statistics for the client, gateway, and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

Prerequisites

- macOS version must be at least Monterey or above.
- Telemetry service must be supported on Windows VDA (enabled by default from VDA 2405 and 2402 CU1).
- Telemetry service must be enabled on Linux VDA from version 2311.
- Telemetry service must be enabled on Mac VDA from Phase I Public TP.

> **Note:**
>
> To use this feature, the new Toolbar feature needs to be enabled. For more information, see Enhanced Desktop Viewer toolbar.



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

Enhanced virtual desktop screen resizing experience

Starting with the 2409 version, Citrix Workspace app for MAC ensures a smooth transition and prevents black screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

Enhanced desktop launch experience

Starting with version 2409, Citrix Workspace App for Mac ensures an enhanced desktop launch experience. You'll experience a seamless, flicker-free transition to your desktop without intermediate screens. The app also eliminates black screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

Enhanced clipboard support for HTML text, files, and folders

Starting with version 2409, Citrix Workspace app for Mac supports the seamless copying and pasting of HTML-formatted text, files, and folders between a Mac local app and a virtual app or desktop session running through Citrix Workspace app for Mac.

HTML text

Whether you're working locally or in a virtual session, this functionality ensures that HTML content is accurately retained during the copy-and-paste process. With this feature, you can copy and paste large HTML text between local and virtual sessions without any restrictions.

To enable the HTML format for clipboard, you need to add an entry for CF_HTML and any other in "Client clipboard write allowed formats"and "Session clipboard write allowed formats"in the ICA® policy settings.

> **Note:**
>
> - **Client clipboard write allowed formats** does not apply if the Client clipboard redirection policy is set to **Prohibited** or **Restrict client clipboard write policy** is disabled.
> - **Session clipboard write allowed formats** does not apply if the Client clipboard redirection policy is set to **Prohibited** or Restrict session clipboard write policy is disabled.

Files and folders

With this feature, you can do the following:

- Users can copy files and folders between the native Mac client and virtual desktops.

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

- Users can copy HTML content between the native Mac client and HDX sessions, and between HDX sessions.
- Admins can set policies to control the scope of copy-paste capabilities.
- Ensures no corruption in copied files, folders, and content.

The copy and paste of files and folders is enabled by default in the clipboard redirection policy. For more information, see Client clipboard redirection.

Session reliability and auto client reconnect

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application that they're using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes until connectivity resumes on the other side of the tunnel. Session reliability reconnects users without reauthentication prompts.

> **Important**
>
> - Citrix Workspace app for Mac users can't override the server setting.
> - With Session reliability enabled, the default port used for session communication switches from 1494 to 2598.

You can use session reliability with Transport Layer Security (TLS).

> **Note:**
>
> TLS encrypts only the data sent between the user device and Citrix Gateway.

Using session reliability policies

The **session reliability connections** policy setting allows or prevents session reliability.

The **session reliability timeout** policy setting has a default 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 for reauthentication.

> **Tip**
>
> 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.

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

You can configure the **Auto client reconnect authentication policy** setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes, or disconnects, the user session after the amount of time you specify in the **Session reliability timeout policy** setting. After that, the auto client reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

> **Note:**
>
> Session reliability is enabled by default at the server. To disable this feature, configure the policy managed by the server.

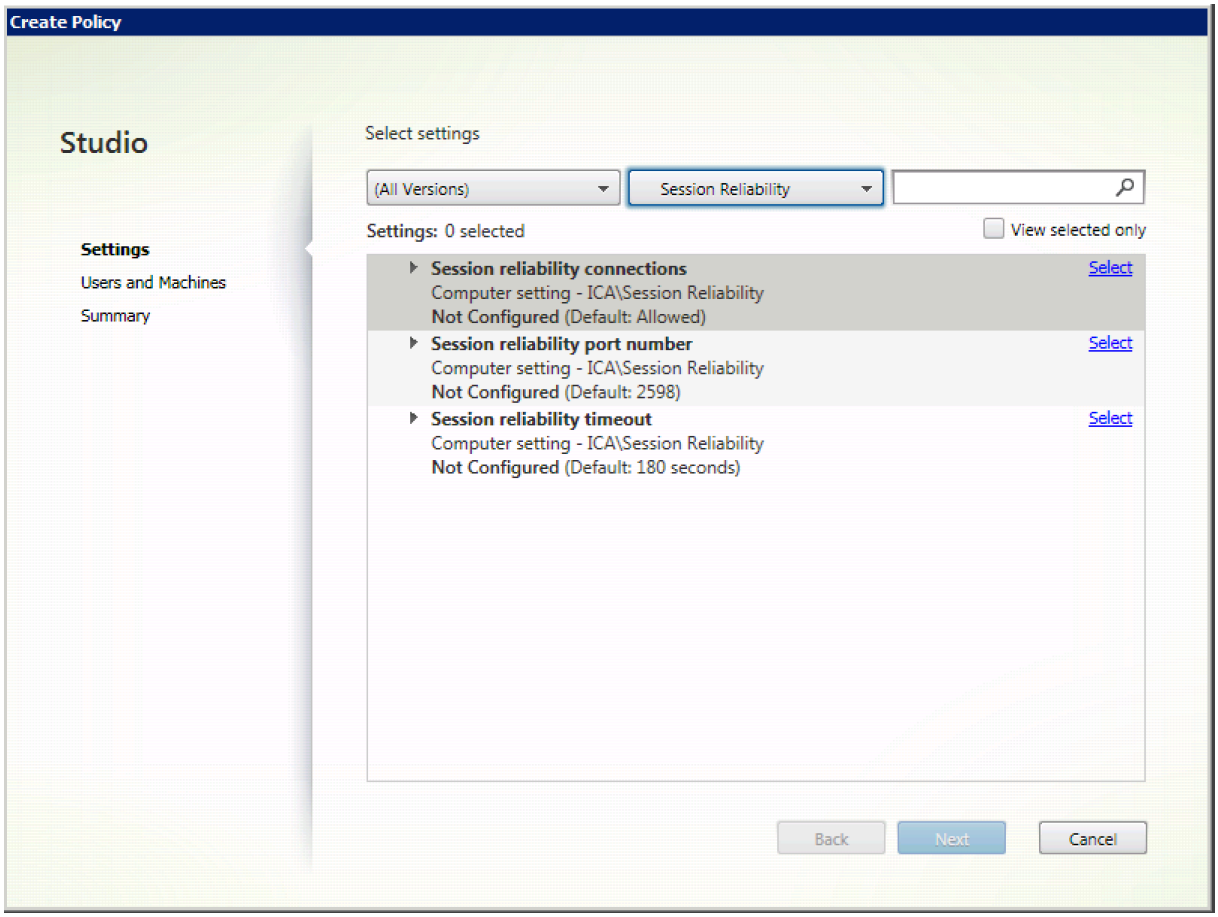
Configuring session reliability from Citrix Studio

By default, session reliability is enabled.

To disable session reliability:

1. Launch Citrix Studio.
2. Open the **Session Reliability connections** policy.
3. Set the policy to **Prohibited**.

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



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**.

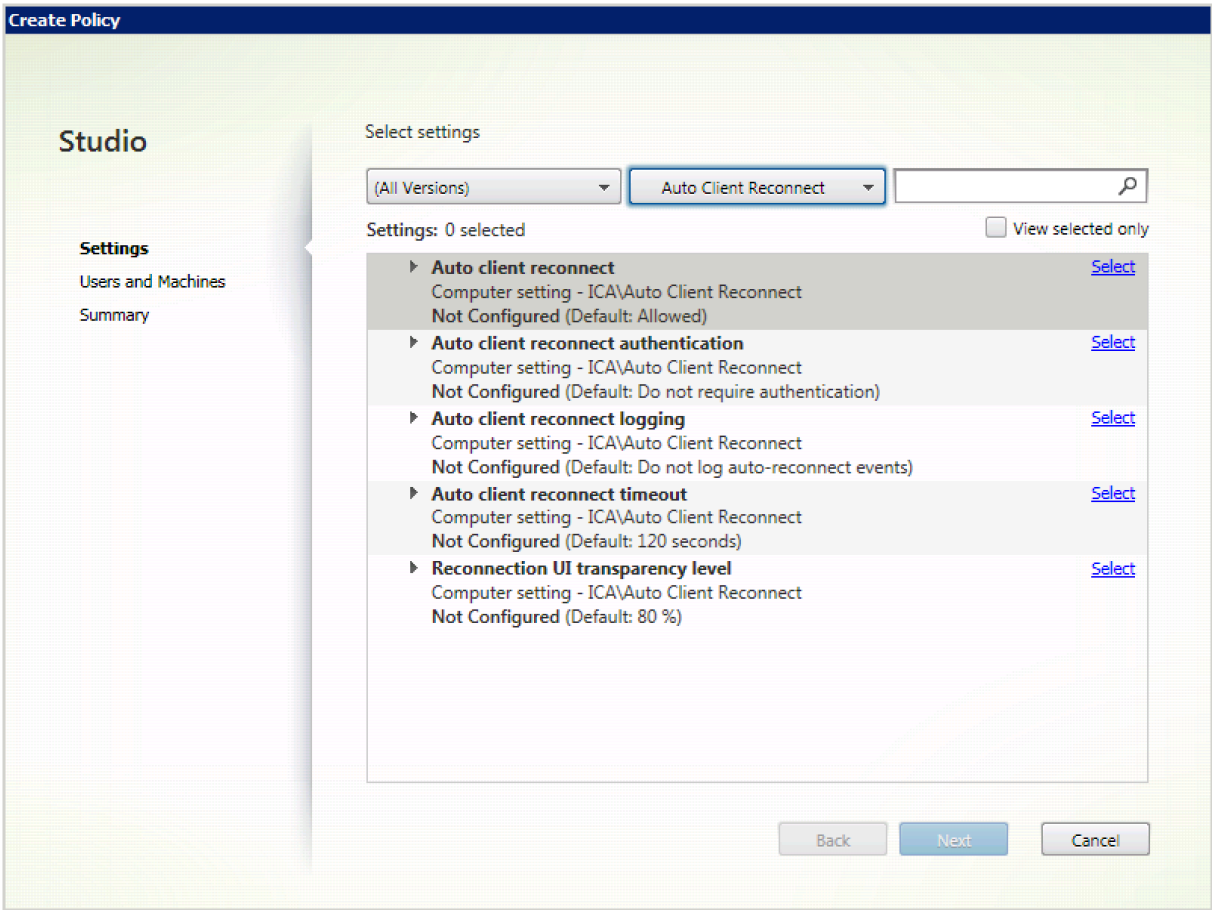
Configuring auto client reconnection using Citrix Studio

By default, auto client reconnection is enabled.

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

To disable auto client reconnection:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect policy**.
3. Set the policy to **Prohibited**.



Configuring Auto client reconnection timeout

By default, the Auto client reconnection timeout is set to 120 seconds.

> **Note:**
>
> Auto client reconnect timeout policy can be configured only with XenApp and XenDesktop 7.11 and later.

To modify auto client, reconnect timeout:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect** policy.
3. Edit the timeout value.

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

4. Click **OK**.

> **Limitations:**
>
> On a Terminal Server VDA, Citrix Workspace app for Mac uses 120 seconds as the timeout value irrespective of the user settings.

Configuring the Reconnect user interface Transparency

The Session User Interface is displayed during a session reliability and auto client reconnect attempts. The Transparency level of the user interface can be modified using Studio policy.

By default, Reconnect UI Transparency is set to 80%.

To modify Reconnect user interface Transparency level:

1. Launch Citrix Studio.
2. Open the **Reconnect UI Transparency level** policy.
3. Edit the value.
4. Click **OK**.

Auto client reconnect and session reliability interaction

There are mobility challenges associated with switching between various access points, network disruptions, and display timeouts related to latency. These create challenging environments when trying to maintain link integrity for active Citrix Workspace app for Mac sessions. Citrix enhanced session reliability and auto reconnection technologies resolve this issue.

This feature allows users to reconnect to sessions automatically after recovery from network disruptions. These features, enabled by policies in Citrix Studio, can be used to improve the user experience.

> **Note:**
>
> Auto client reconnection and session reliability timeout values can be modified using the **default.ica** file in StoreFront.

Auto client reconnection

Auto client reconnection can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled. For information about modifying this policy, see the auto client reconnection section earlier in this article.

Use the default.ica file in StoreFront to modify the connection timeout for AutoClienreconnect. By default, this timeout is set to 120 seconds (or two minutes).

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

Setting	Example	Default
TransportReconnectRetryMaxTSeconds	TransportReconnectRetryMaxTSeconds=60	120

Session reliability

Session reliability can be enabled or disabled using Citrix Studio policies. By default this feature is enabled.

Use the **default.ica** file in StoreFront to modify the connection timeout for session reliability. By default this timeout is set to 180 seconds (or three minutes).

Setting	Example	Default
SessionReliabilityTTL	SessionReliabilityTTL=120	180

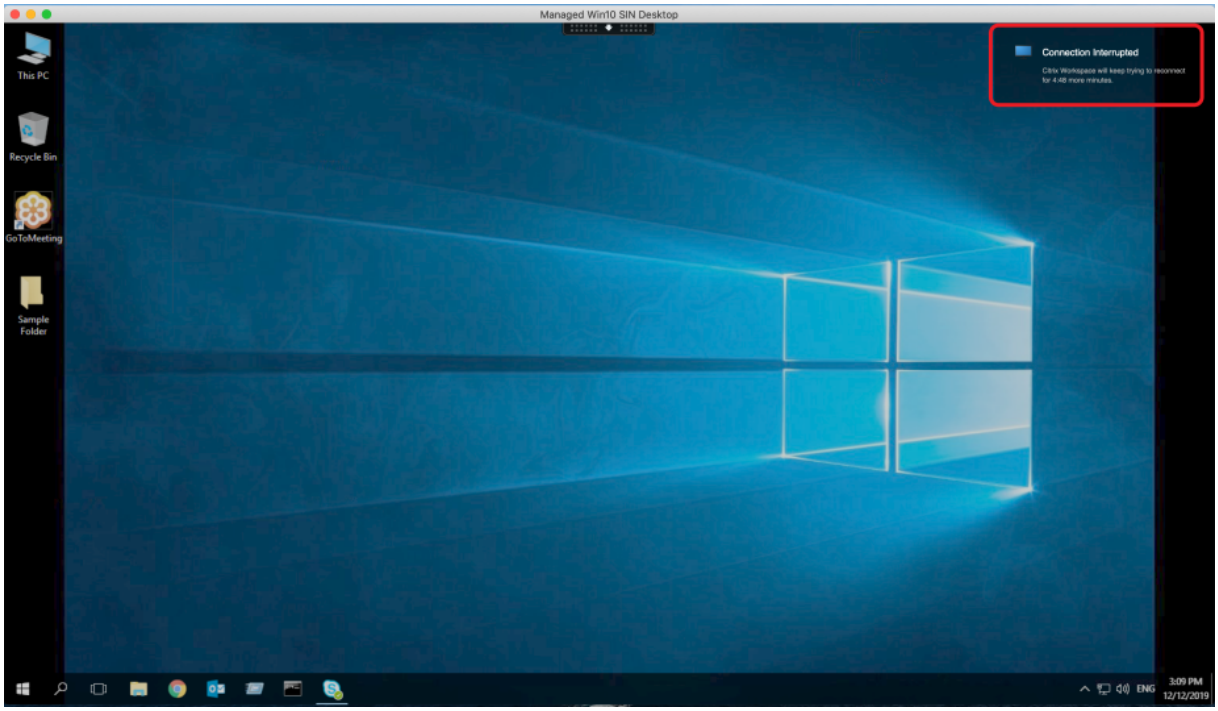
How auto client reconnection and session reliability work

When auto client reconnection and session reliability are enabled for a Citrix Workspace app for Mac, consider the following:

- A session window is grayed out when a reconnection is in progress. A countdown timer displays the amount of time remaining before the session is reconnected. Once a session is timed out, it's disconnected.

By default, the reconnect countdown notification starts at 5 minutes. This timer value represents the combined default values for each of the timers (auto client reconnection and session reliability), 2 and 3 minutes respectively. The following image illustrates the countdown notification which appears in the upper right portion of the session interface:

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

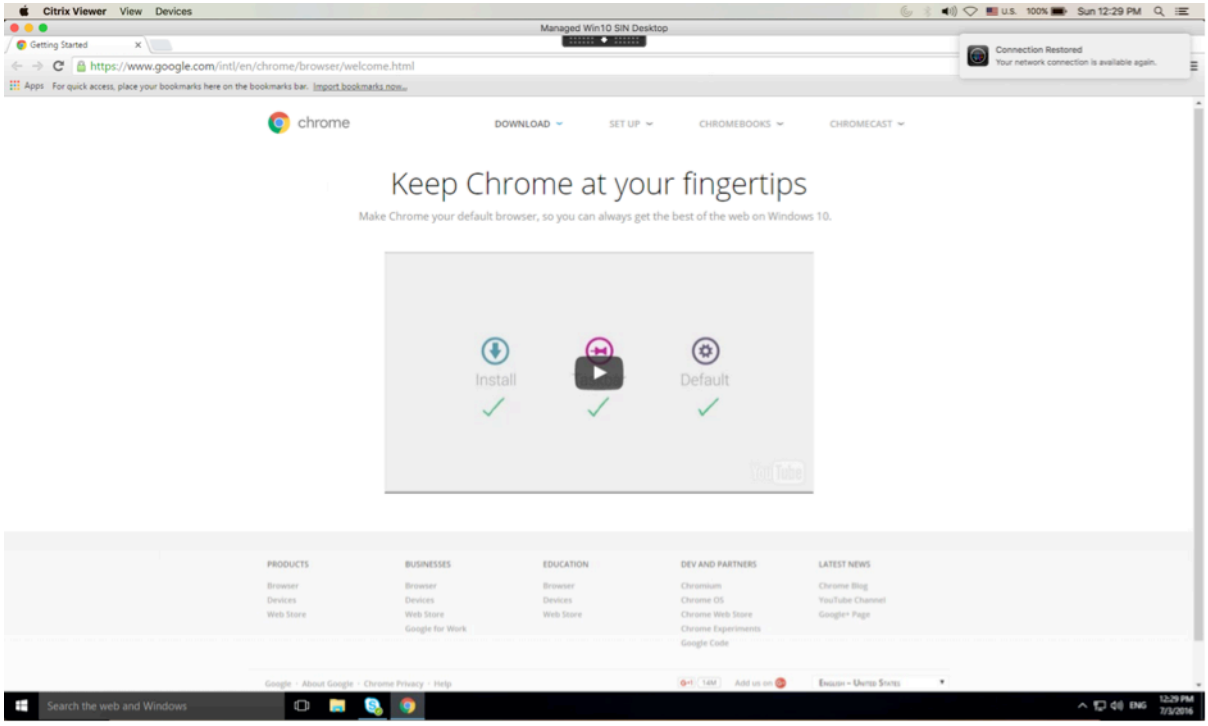


Tip

You can alter the grayscale brightness used for an inactive session using a command prompt. For example, `defaults write com.citrix.receiver.nomas NetDisruptBrightness 80`. By default, this value is set to 80. The maximum value can't exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

- Users are notified when a session successfully reconnects (or when a session is disconnected). This notification appears in the upper right portion of the session interface:

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



- A session window which is under auto client reconnect and session reliability control provides an informational message indicating the state of the session connection. Click **Cancel Reconnection** to move back to an active session.

Service continuity

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services.

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

Support for service continuity in the Safari browser

Starting with the 2206.1 version, the Citrix Workspace service continuity feature is supported for the Safari browser. Users must install Citrix Workspace app for Mac and the Citrix Workspace web extension. Service continuity removes (or minimizes) the dependency on the availability of the components involved in the connection process. It allows you to connect to your virtual apps and desktops regardless of the cloud services' health status. For more information about the service continuity feature, see section Service continuity.

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

Enhancement to Permanent Client Access License (CAL) for Remote Desktop Sessions

Starting with the 2204 version, if you're running CAL in your environment to access remote desktops, when the client ID is greater than 15 characters, you can launch the remote desktop session with a permanent license.

To enable this feature, admins must configure the **default.ica** file by doing the following:

1. In the StoreFront server, navigate to *C:\inetpub\wwwroot\Citrix<StoreName>\App_Data* and open the **default.ica** file with any editor.
2. Add the following lines in the **[WFClient]** section:

```
isRDSLicensingEnabled=On
```

Support for HTML format on the Citrix Workspace app for Mac clipboard

Starting with version 2409, Citrix Workspace app for Mac supports the seamless copying and pasting of HTML-formatted text between a Mac local app and a virtual app or desktop session running through Citrix Workspace app for Mac. Whether you're working locally or in a virtual session, this functionality ensures that HTML content is accurately retained during the copy-and-paste process. With this feature, you can copy and paste large HTML text between local and virtual sessions without any restrictions.

This feature is disabled by default in the clipboard redirection policy.

To enable the HTML format for clipboard, you need to add an entry for CF_HTML (and any other in "Client clipboard write allowed formats"and "Session clipboard write allowed formats") in the **ICA policy** settings. For more information, see Client clipboard redirection.

> **Note:**
>
> - Client clipboard write allowed formats does not apply if the Client clipboard redirection policy is set to **Prohibited** or **Restrict client clipboard write policy** is disabled.
> - Session clipboard write allowed formats does not apply if the Client clipboard redirection policy is set to **Prohibited** or **Restrict session clipboard write** policy is disabled.

Customize the Desktop Viewer toolbar

Previously, you can completely disable the **Desktop Viewer** toolbar. However, you can't enable or disable a few options on the toolbar. With this release, you can customize the Citrix Workspace app for Mac toolbar by adding and removing options on the toolbar. For more information, see Hide or show the desktop tool bar in the virtual desktop session.

You can configure the toolbar through the Mobile Device Management (MDM) settings. The following settings can hide the Device, Preferences, Minimize, and Full screen button:

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

```
<key>HiddenToolbarButtons</key>
<array>
  <string>device</string>
  <string>preferences</string>
  <string>minimize</string>
  <string>fullscreen</string>
</array>
```

> **Note:**
>
> You cannot hide the **Pin** button from the toolbar.

Sustainability initiative from Citrix Workspace app

Starting with the 2409 version, Citrix Workspace app for Mac supports the **Sign out** option for the virtual desktop session. This feature might help conserve energy if you sign out from virtual machines when not in use.

When the user clicks **Disconnect** or **Log out**, or closes a virtual desktop, then the following prompt is displayed, recommending the user to use the **Log out** option to save energy.

To enable this feature on Terminal Server Virtual Delivery Agent (TSVDA), follow these steps:

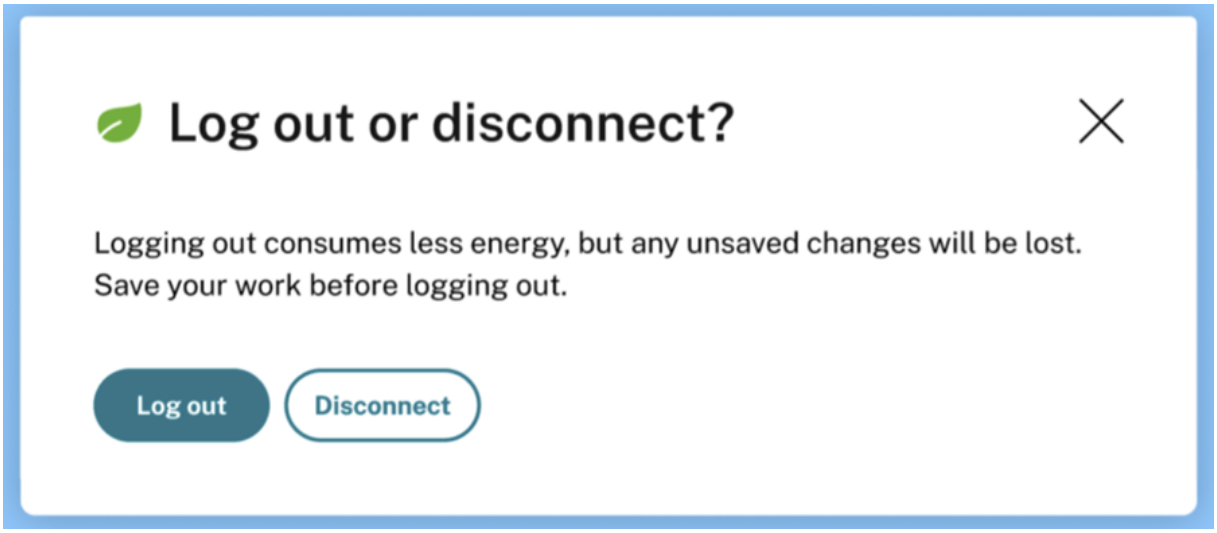
1. Navigate to Citrix Studio.
2. Click **Delivery Groups** in the left navigation pane.
3. Select the required VDA from the **Delivery Group** section.
4. Click the **Edit** icon to open the **Edit Delivery Group** page.
5. Click **Desktops** from the left navigation pane.
6. Choose the VDA where the keyword must be added and click **Edit**.
7. In the **Edit Desktop** page, set the `ICA-LogOffOnClose` keyword to **`true`** in the **Description** field.
8. Click **OK** to save the changes.

To enable this feature on Windows Desktop Virtual Delivery Agent (WVDA), follow these steps:

1. Navigate to Citrix Studio.
2. Click **Delivery Groups** in the left navigation pane.
3. Select the required VDA from the **Delivery Group** section.
4. Click the **Edit** icon to open the **Edit Delivery Group** page.
5. Click **User Settings** from the left navigation pane.
6. Set the `ICA-LogOffOnClose` keyword to **`true`** in the **Description** field.
7. Click **OK** to save the changes.

The following dialog box appears when you close the virtual desktop.

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



Support for voice dictation

Starting with version 2505, Citrix Workspace app for Mac supports dictation. This feature allows users to:

- **Voice Navigation:** Interact with the Citrix Viewer toolbar using voice commands for easier access to toolbar functions.

  > **Note:**
  >
  > Voice navigation is limited to the toolbar and does not support navigation within applications inside the session.

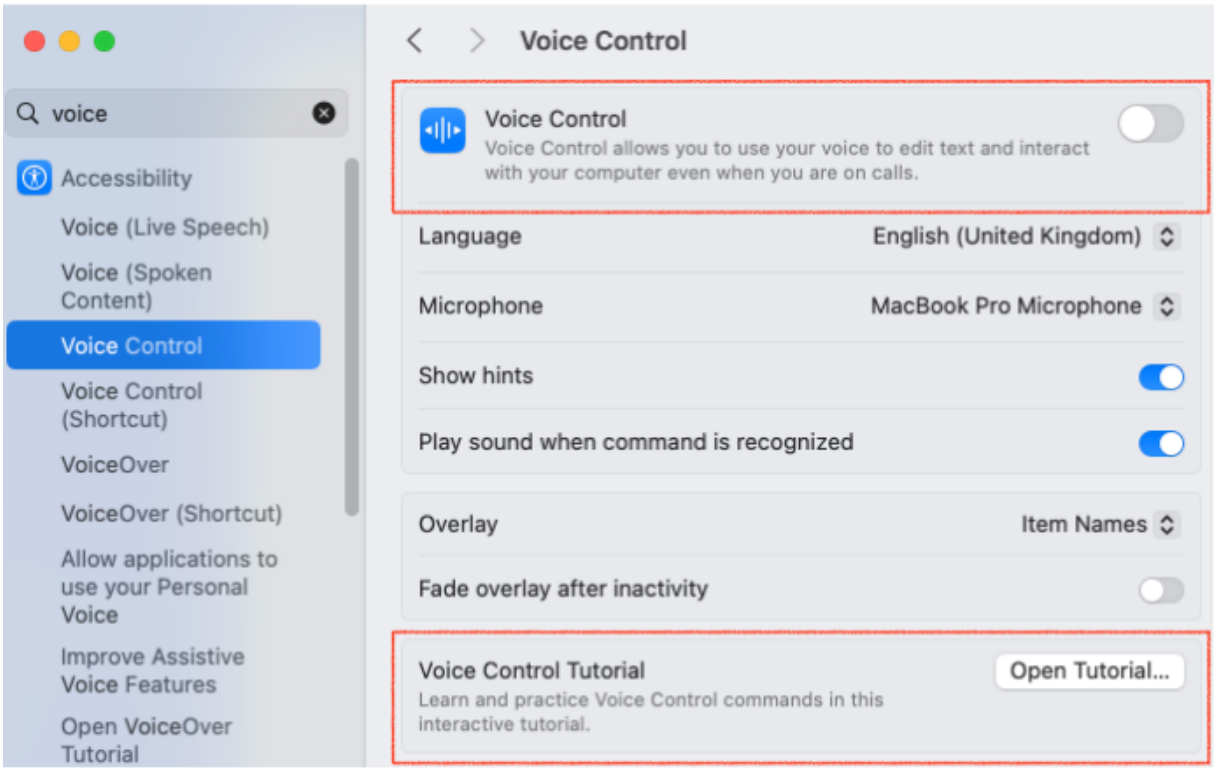
- **Voice Dictation:** Enter text by speaking, with your words automatically transcribed into any text field within your Citrix session.
- **Text Editing:** Edit and format text using voice commands while in session, available on macOS only.

This feature improves accessibility and productivity by allowing users to interact with virtual desktops hands-free.

Tips

To enable this feature, open **System Settings** on your macOS device and turn on Voice Control. To learn how to use Voice Control, select **Open Tutorial** in the **Voice Control** settings.

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



Monitoring Zoom plug-in metrics on Director

Starting with version 2505 of Citrix Workspace app for Mac, and version 2507 of Citrix Virtual Apps and Desktops for both Delivery Controller (DDC) and Virtual Delivery Agent (VDA), you can monitor optimized Zoom environments for Mac endpoints with enhanced visibility.

To track the Zoom plug-in management status directly in the Director UI, follow these steps:

1. Access the **Director UI** by navigating to http://[DDC_IP]/Director.
2. Click **Filters**.
3. Select the desired **VDI session**.
4. Click **Session Performance**.
5. Under Real-time Communications, check **Zoom**.
6. Click **View Details**.
7. Review the **Zoom metrics**.

Keyboard accessibility support for the toolbar on the Virtual Desktop

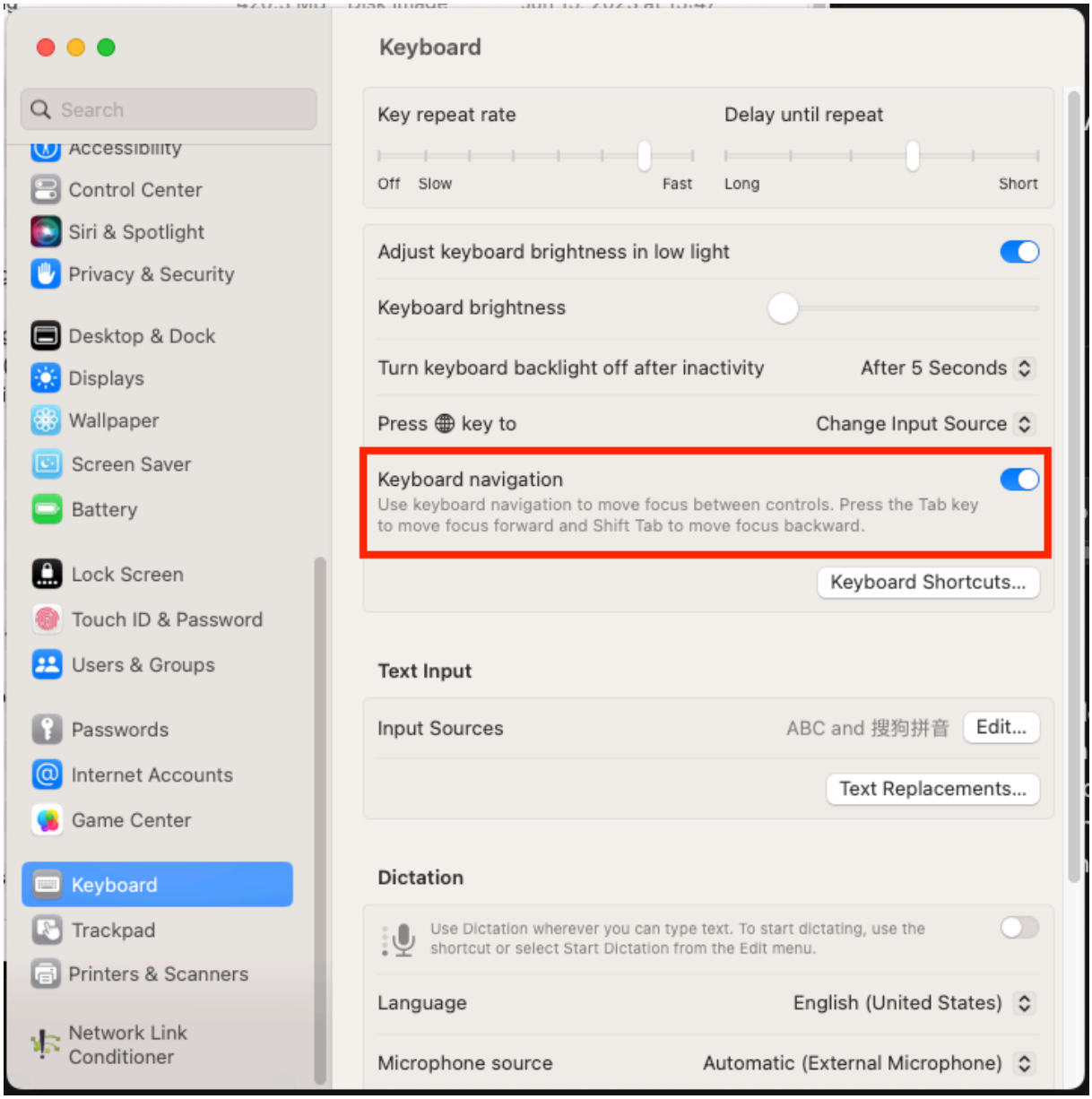
Starting with version 2505, the **Virtual Desktop** toolbar supports keyboard accessibility for all levels. Users can navigate the entire toolbar using keyboard shortcuts.

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

You can use the following keyboard shortcuts to access the **VDI** toolbar using the keyboard:

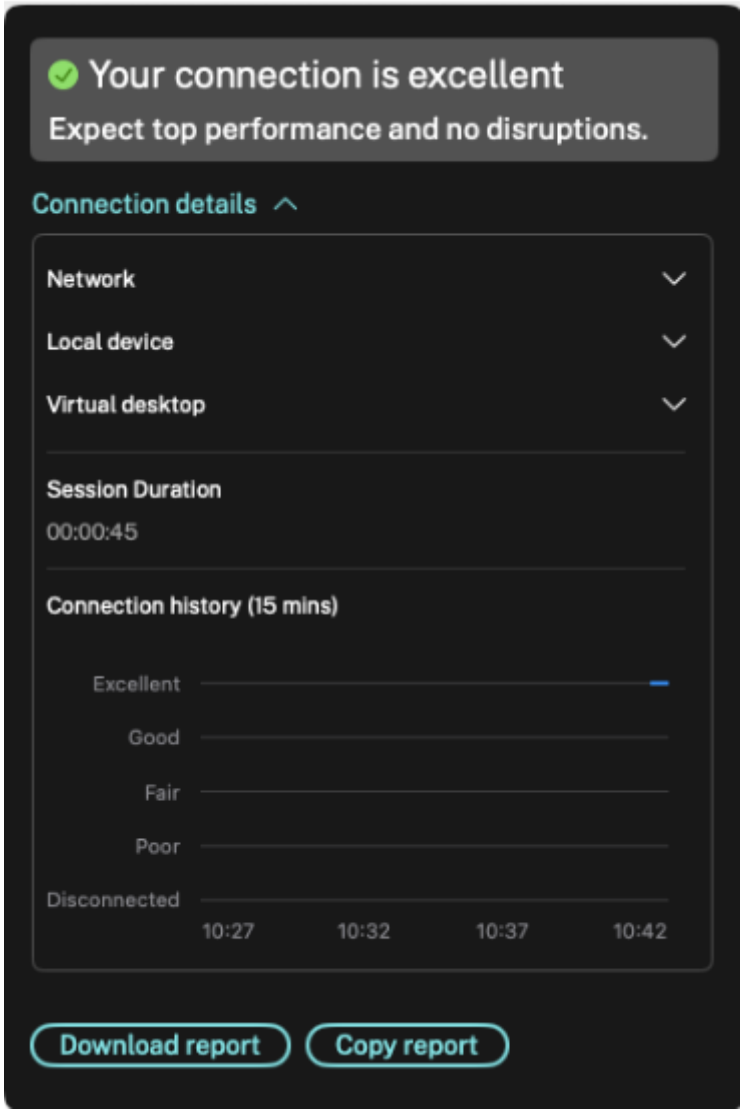
- **Shift + Command + T**: To activate the VDI toolbar.
- **Tab**: To navigate across the VDI Toolbar in the clockwise direction.
- **Shift + Tab**: To navigate across the VDI toolbar in the anti-clockwise direction.
- **Space**: To select an option on the VDI Toolbar.
- **Escape**: To close a modal in focus, the user can't simply interact with the toolbar. Instead, they must either switch to another application or click the session area outside the modal.

The toolbar now supports **Keyboard navigation**, allowing users to navigate and highlight UI elements within it.



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

Enhancement to Connection Strength Indicator on Citrix Viewer toolbar



Starting with version 2505, Citrix Workspace app for Mac introduces an enhanced Connection Strength Indicator designed for a more intuitive and user-friendly experience.

The key improvements include:

- **Real-time Wi-Fi strength**: Instantly view your current Wi-Fi signal quality for better connectivity awareness.
- **Expanded device details**: Access information such as CPU, memory, and disk usage directly from the indicator.
- **Proactive notifications with snooze options**: Receive alerts when your connection strength drops, with the ability to temporarily snooze notifications.
- **Actionable recommendations**: Get clear suggestions to resolve connectivity issues when your connection strength falls below optimal levels.

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

- **15-minute connection history**: Review a visual history of your connection strength over the past 15 minutes to assist with troubleshooting and analysis.

Enhanced Native macOS Gesture support

Starting with CWA 2508 for Mac, Citrix Viewer provides enhanced gesture support specifically designed for Citrix VDA for macOS environments.

Native macOS Gesture shortcuts

Citrix Viewer now provides the following native macOS gesture shortcuts:

- **Mission Control** - Access Mission Control functionality.
- **App Expose** - View all windows for the current application.
- **LaunchPad** - Open LaunchPad to access applications.
- **Show Desktop** - Display the desktop by minimizing all windows.

Debugging Shortcuts

Two debugging shortcuts are available for Mac VDA environments:

- **Restart Citrix Service** - Restart the Citrix service for troubleshooting.
- **Restart macOS** - Restart the macOS system (Mac VDA only).

Configuration

The native macOS gesture shortcuts include the following configuration details:

- **Access Location:** You can access all shortcuts from the Citrix Viewer toolbar.
- **Auto-Configuration:** The system automatically enables this feature without requiring client side configuration.

Requirements

Make sure that you have the following:

- Citrix Workspace App 2508 or later for Mac
- Mac VDA 2507 or later
- Mac VDA environment

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

Enhanced seamless app experience

Starting with version 2511.1, Citrix Workspace app for Mac improves the experience of seamless app sessions connected to Virtual Delivery Agents (VDAs) with Citrix Virtual Apps and Desktops release 2411 or later on Windows Server 2022 or 2025. When users enter **Mission Control or App Expose**, windows are arranged without overlap and animations are rendered smoothly, offering a more polished and visually appealing experience.

Seamless application accessibility mirroring

Starting with version 2603, Citrix Workspace app for Mac captures accessibility settings from the client and applies them to seamless applications. This enhancement automatically synchronizes accessibility configurations, providing consistent support across virtual application sessions and eliminating manual reconfiguration.

Prerequisites

To use seamless application accessibility mirroring, ensure that you have the following requirements:

- **Citrix Virtual Apps and Desktops™:** 2503 or later
- **VDA operating systems:**
  - Windows Server 2022
  - Windows Server 2025
  - Windows 10 Multi-session
  - Windows 11 Single-session & Multi-session
- **Citrix Workspace app for Mac:** 2508 or later

Configuration

To enable seamless application accessibility mirroring, you must configure settings on both the VDA and the client side.

VDA configuration Set the following key on the VDA to enable the accessibility mirroring feature:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\AccessibilityMirroring`

Set a DWORD type with value **1** to enable the feature.

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

> **Note:**
>
> The VDA configuration must be completed for the accessibility mirroring feature to function properly.

Improved session reconnection experience

Starting with version 2603, this feature enhances the end-user experience during session timeouts caused by inactivity or network interruptions. The solution provides users with an option to reconnect directly from the timeout screen for desktop and app sessions. Users can also reconnect directly during the Auto-Client-Reconnect (ACR) phase.

Prerequisites

- Citrix Virtual Apps and Desktops™: Version 2411 or later
- Citrix Workspace™ app: Version 2511 or higher

The key features are as follows:

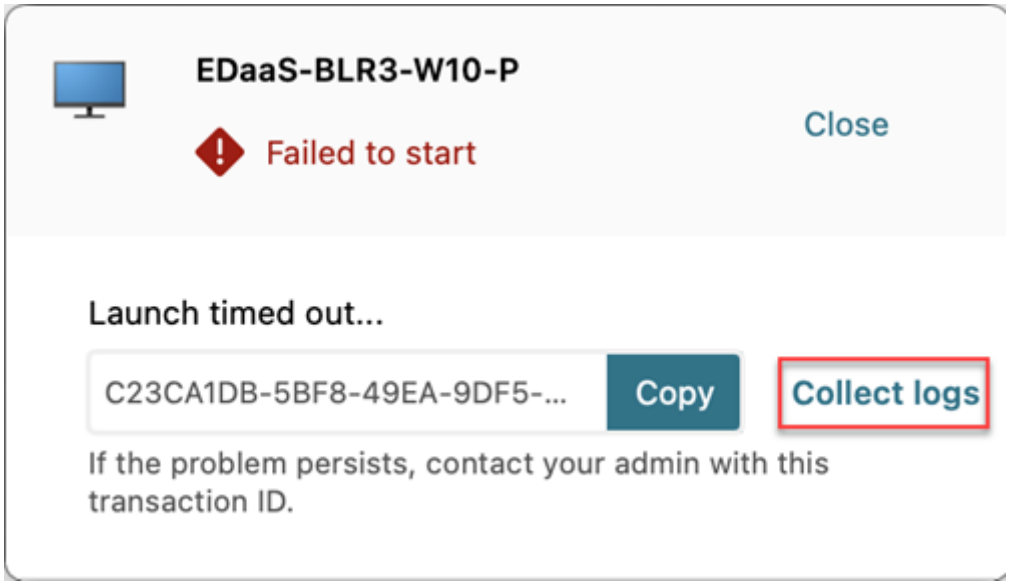
- Displaying specific reasons for session timeouts, such as **Device went to sleep**, or **Network disruption**.
- Allowing seamless reconnection to the session, whether it's a new or persisting session, based on the administrator's configuration.
- Supporting scenarios where auto reconnect might fail, such as network switches (for example Wi-Fi to LAN).
- Supporting directly reconnect during the auto-client-reconnect phase.
- Enabling seamless reconnection to hybrid-launched sessions, requiring user authentication only when the store is not configured in CWA.

Troubleshooting

Support for log collection when session launch fails

Starting with version 2411, Citrix Workspace™ app for Mac supports direct log collection when session launch fails, allowing for quicker troubleshooting and easier access to logs.

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

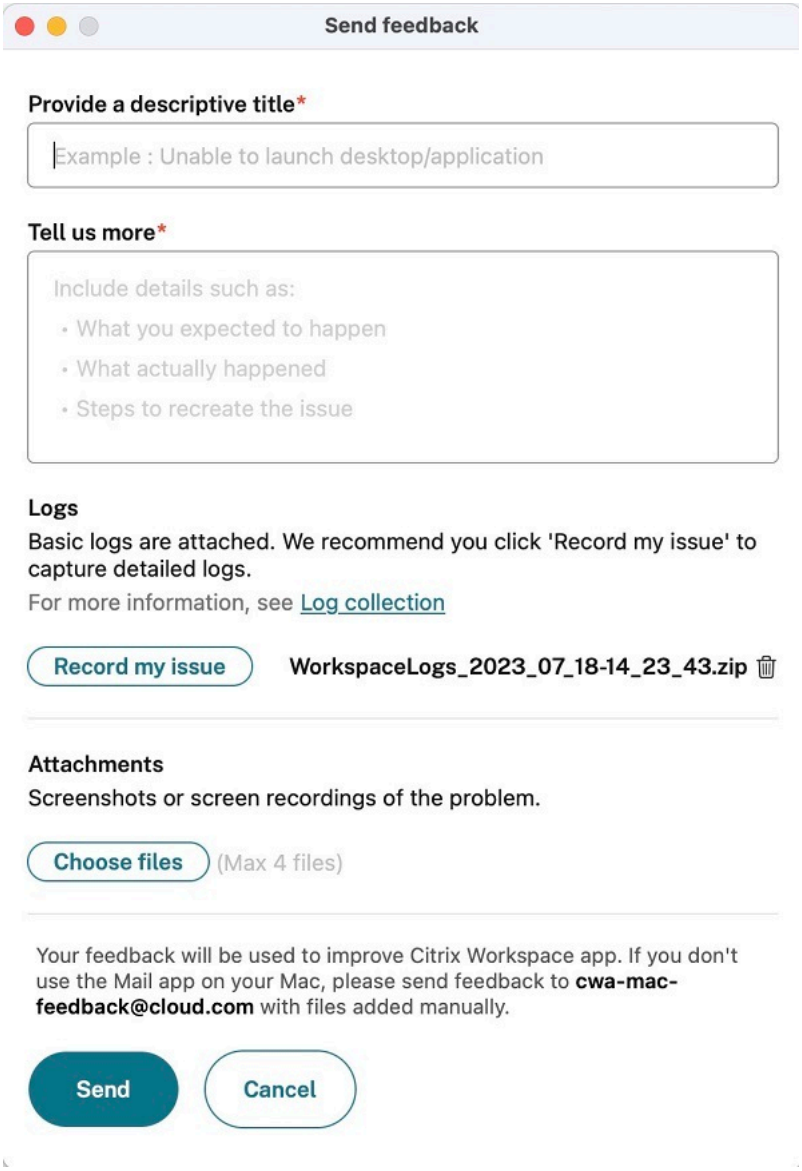


Send feedback on Citrix Workspace app

Starting with the 2307 version, Citrix Workspace app for Mac supports the **Send feedback** feature. The Send feedback option allows you to inform Citrix about any issues you might encounter while using the Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

You must select **Help > Send feedback** to view and fill the issue details in the Send feedback form. You can add details like the examples provided in the form.

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



You can attach the existing log files or generate new log files. To generate log files, click **Record my issue > Start Recording** and then reproduce the issue. After the issue is reproduced, click **Stop Recording**. The log file is saved automatically and replaces the existing logs with the reproduced logs.

> **Note:**
>
> Citrix® does not collect any Personally Identifiable Information (PII) from the logs.

You can attach screenshots or screen recordings describing the issue to help us understand what you're experiencing. Click **Choose files** and add the attachments describing your issues, such as screenshots or screen recordings. You can attach a maximum of four files.

Once you've entered the necessary information, click **Send** to have a new email automatically created in your Mail app with the information you added. From there, click the **Send button** to share the

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

feedback with Citrix.

> **Note:**
>
> If you aren't using the default Mail app, then send feedback to cwa-mac-feedback@cloud.com from your mail client. Add the issue details, log files, screenshots, or screen recordings to the email manually.

Log collection

Starting with the 2304 version, Citrix Workspace app for Mac supports the **Log collection** feature. Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, provide support.

Starting with the 2402 version, the log collection feature is enhanced to collect and email additional log data. With this feature, you can easily collect all the required log information at once.

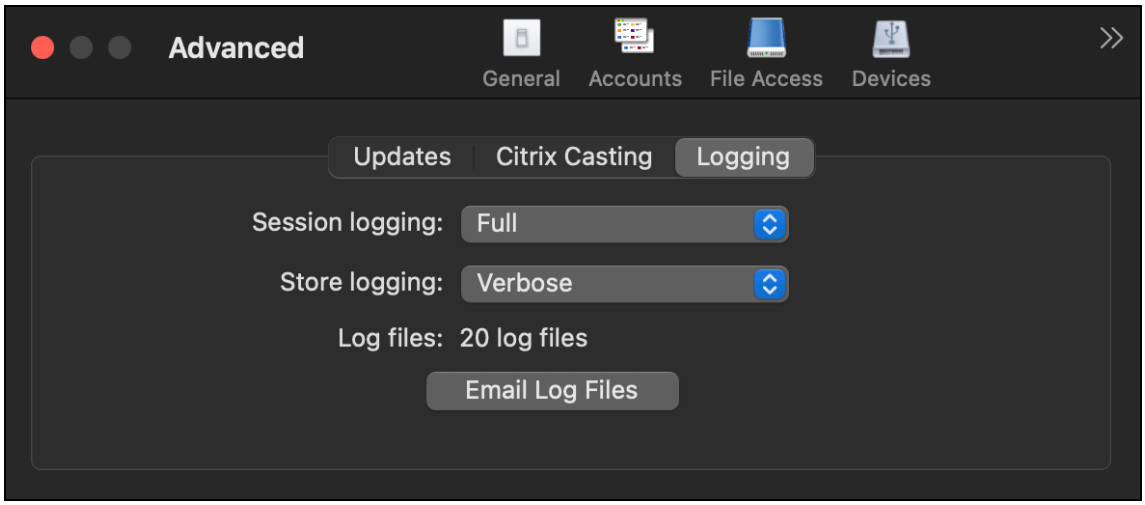
The following additional log data are collected using this feature:

- Crash report for Citrix Process
- Citrix related files under preferences
- Citrix related files `launchagents` and `launchdaemons`
- Citrix related files under application or Citrix receiver™

You can collect logs using the GUI.

Collecting logs:

1. Open Citrix Workspace app.
2. Right-click on Citrix Workspace in the toolbar and click **Preferences** > **Advanced**.
3. Select **Logging**.



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

4. Select one of the following session log levels:

    - **Basic (Default)**: Minimum logs are collected for basic troubleshooting.
    - **Connection Diagnostics**: Identifies errors while connecting. All logging is enabled up until the point when the session is deemed successful.
    - **Verbose**: Captures everything including the connection diagnostics. Once enabled, the Citrix Workspace app will store up to 10 session logs after which they're deleted starting with the oldest to maintain 10 logs.

    > **Note:**
    >
    > Selecting the **Full** logging option can impact performance and must be used only while troubleshooting an issue because of the amount of data. Do not enable full logging during normal use. Enabling this level of logging triggers a warning dialog that must be acknowledged for you to continue.

5. Select one of the following store log levels:

    - **Disabled (Default)**: Minimum logs are collected for basic troubleshooting.
    - **Normal**: Only store communication logs are collected.
    - **Verbose**: Detailed authentication and store communication logs are collected.

6. Click **Email Log Files** to collect and share logs as a .zip file.

Sentry

Sentry is used to collect app logs to analyze issues and crashes to improve product quality. Citrix does not collect or store any other personal user information or use Sentry for feature analytics data. For more information about Sentry, go to [https://sentry.io/welcome/].

Support for resetting Citrix Workspace app

Starting with the 2405 version, Citrix Workspace app for Mac supports the **Reset App Data** option. This features allows users to quickly resolve issues resulting from conflicts caused by cache or settings by resetting the app and get unblocked without external assistance.

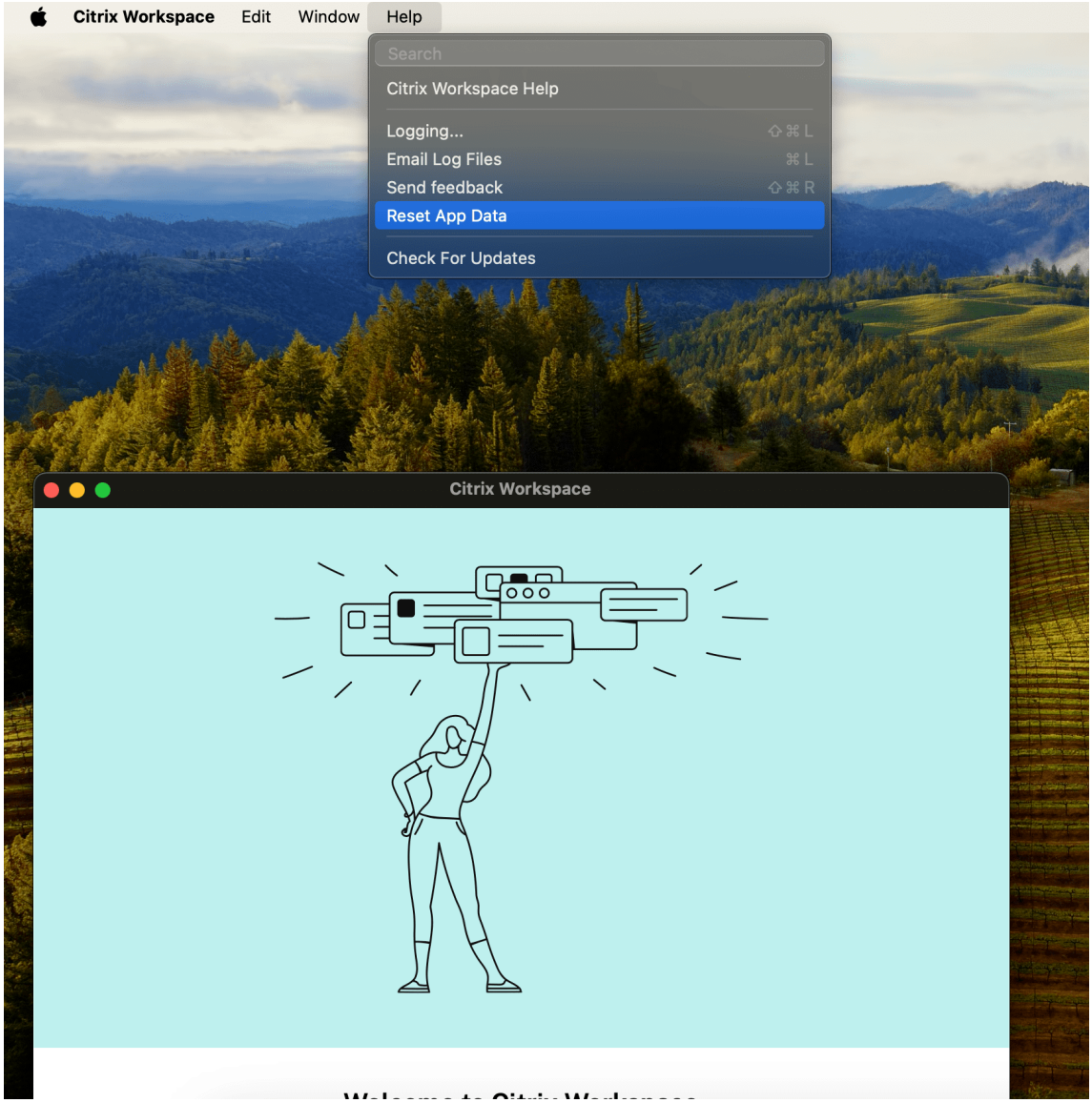
When you reset the Citrix Workspace app:

- The app is reverted to its default state (similar to just after fresh installation).
- All cache is cleared.
- Any added stores are removed.
- Preference settings are return to their default state.

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

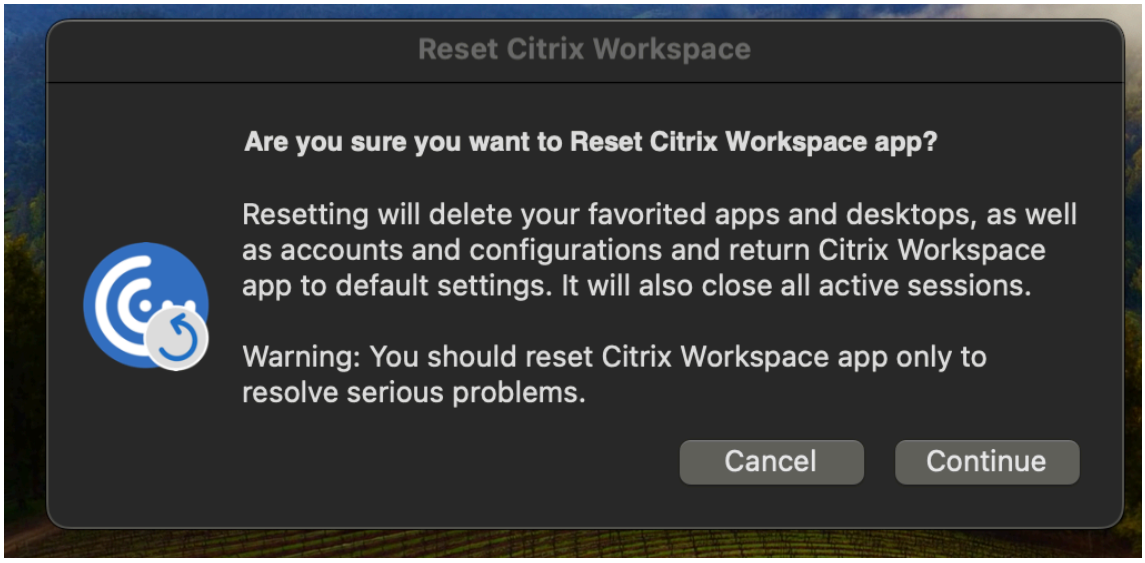
How to Reset Citrix Workspace app

1. Open the Citrix Workspace app.
2. On the menu bar, navigate to **Help > Reset App Data**.

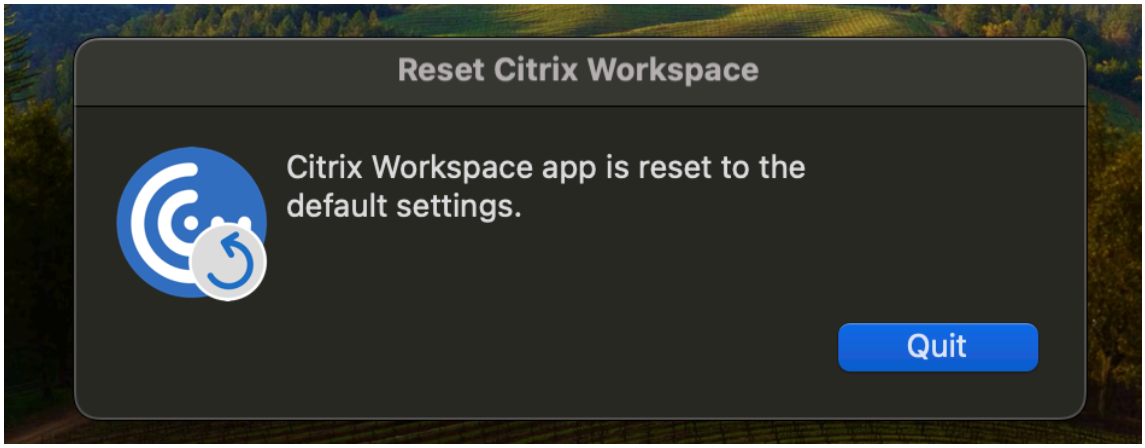


3. Click **Continue**.

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



4. Click **Quit**



Deprecation

This article gives you advance notice of the phase-out of platforms, Citrix® products, and features so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

Deprecated items are not removed immediately. Citrix continues to support them in this release but they will be removed in the future.

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

Item	Removed/To be removed in	Deprecation announced in	Alternative
macOS Sonoma 14	Citrix Workspace™ app for Mac version 26Q4	Citrix Workspace app for Mac version 2603.11	Upgrade to the latest available version of Mac.
Legacy Desktop Viewer Toolbar	Citrix Workspace™ app for Mac version 2511.1	Citrix Workspace app for Mac version 2508	New Desktop Viewer toolbar.
macOS Ventura 13	Citrix Workspace™ app for Mac version 26Q1	Citrix Workspace app for Mac version 2508	Upgrade to the latest available version of Mac.
Citrix Casting	Citrix Workspace app for Mac version 26Q1	Citrix Workspace app for Mac version 2508	None.
macOS Monterey 12	Citrix Workspace app for Mac version 2409	Citrix Workspace app for Mac 2503	Upgrade to the latest available version of Mac.
XenApp® Services (also known as PNAgent)	To be removed in July 2025	February 2025 (2411)	Within Citrix Workspace app, connect to stores using the store URL rather than the XenApp Services URL
macOS version Monterey (12)	To be removed in January 2025	September 2024 (2409)	Use the supported operating system as given in the Supported operating systems section.
Support for WebRTC SDP format (Plan B)	Removed in February 2024	2311	Upgrade Citrix Workspace app to a supported version.
macOS version Big Sur (11)	Removed in July 2024 (2405)	September 2023 (2308)	Use the supported operating system as given in the Supported operating systems section.
Citrix Workspace apps for macOS (Intel (x86) build)	Removed in April 2024	April 2022 (2204)	Citrix Workspace app for MacOS that uses Universal Architecture.

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

Item	Removed/To be removed in	Deprecation announced in	Alternative
macOS version Catalina (10.15)	Removed in July 2023 (2307)	April 2023 (2304)	Use the supported operating system as given in the Supported operating systems section.
macOS versions High Sierra (10.13) and Mojave (10.14)	Removed in September 2020 (2009)	August 2020 (2008)	Use the supported operating system as given in the Supported operating systems section.

© 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.