Citrix Enterprise Browser™

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

Contents

Citrix Enterprise Browser™ 2

About this release 3

System requirements and compatibility 61

Install Citrix Enterprise Browser 61

Get started 63

Configure 65

Browser restrictions through Secure Private Access for Workspace 65

Browser restrictions through Secure Private Access for StoreFront™ 75

Manage Citrix Enterprise Browser™ through Global App Configuration service 85

Manage single sign-on for Web and SaaS apps through the Global App Configuration service 126

Citrix Enterprise Browser™ shortcut 129

Independent update of Citrix Enterprise Browser™ 134

Browser Data Encryption 140

System requirements and compatibility 141

Configure Browser Data Encryption 142

Troubleshooting 147

Disable the address bar of the browser 148

Features 149

End user settings 152

Troubleshoot 165

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

Citrix Enterprise Browser™

September 6, 2025

Citrix Enterprise Browser (formerly Citrix Workspace™ Browser) is a native browser running on the client machine. It enables users to open web or SaaS apps from the Citrix Workspace app in a secure manner. It ensures a consistent user interface while accessing various web or SaaS apps while improving your productivity and giving you a great performance in rendering those apps.

The Enterprise Browser is Chromium-based, secure, and protects your device and your organization's network from unintended user behavior. The Enterprise Browser is available as part of Citrix Workspace app for Windows and Mac. When you open web or SaaS apps in the Workspace app, the Enterprise Browser is invoked and the apps open in a new window. You can open the following types of web and SaaS apps that have the enhanced security feature enabled:

- Internal web apps that would otherwise require a VPN to access outside of the Citrix Workspace app framework, open in the Enterprise Browser.
- External SaaS apps open in the Enterprise Browser if **Secure Private Access** policies are applied while deploying the app. If the **Secure Private Access** policies aren't applied to the external SaaS app, they open in your native browser.

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

> **Important:**
>
> This documentation describes features and configurations in the Current Release (CR) of Citrix Workspace app for Windows.
>
> For more information about the lifecycles of CRs and LTSRs, see Lifecycle Milestones for Citrix Workspace app.

Keyboard support

Citrix Enterprise Browser supports non-English language keyboards and Input Method Editors (IMEs).

Supported languages

The Enterprise Browser is available in the following languages:

- English

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

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian
- Spanish

Reference articles

- Introducing the all-new Citrix Enterprise Browser
- Delivering enterprise web apps with Citrix Enterprise Browser
- Citrix Workspace app
- Citrix Secure Private Access

About this release

December 5, 2025

This section lists new features and fixed issues for Citrix Enterprise Browser™ (formerly Citrix Workspace™ Browser) for Mac and Windows operating systems.

What's new in 140.1.1.33

This release includes an independent update for Citrix Enterprise Browser version 140.1.1.33, which is based on Chromium version 140. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU4), Windows 2508 (Current Release), and Mac 2508. It is available for both auto update and manual update. The installer for a manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues in 140.1.1.33

This release includes some security fixes.

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

Known issue in 140.1.1.33

There are no known issues in this release.

Earlier releases

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

140.1.1.29

What's new

This release includes an independent update for Citrix Enterprise Browser version 140.1.1.29, which is based on Chromium version 140. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU4), Windows 2508 (Current Release), and Mac 2508. It is available for both auto update and manual update. The installer for a manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

- Browser notification defaults can now be controlled through Global Apps Configuration service (GACS). A new **DefaultNotificationsSetting** toggle has been added to provide enterprise-level policy management for notification settings.

  The default notification settings support the following values:

  - 1 = Allow sites to show desktop notifications
  - 2 = Do not allow any site to show desktop notifications
  - 3 = Ask every time a site wants to show desktop notifications [CTXBR-13422]

Known issue in 140.1.1.29

There are no known issues in this release.

139.1.1.25

This release includes an independent update for Citrix Enterprise Browser version 139.1.1.25, which is based on Chromium version 139. This version is compatible with Citrix Workspace app for Windows

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

LTSR 2402 (CU4), Windows 2503.10 (Current Release), and Mac 2505.10. It is available for both auto update and manual update. The installer for a manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

There are no fixed issues in this release.

Known issue

There are no known issues in this release.

137.1.1.32

What's new

This release includes an independent update for Citrix Enterprise Browser version 137.1.1.32, which is based on Chromium version 137. This version is compatible with Citrix Workspace app for Windows LTSR 2402 Cumulative Update 4.

137.1.1.25

What's new

This release includes an independent update for Citrix Enterprise Browser version 137.1.1.25, which is based on Chromium version 137. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU3), Windows 2503 (Current Release), and Mac 2503. It is available for both auto update and manual update. The installer for a manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues in 137.1.1.25

There are no fixed issues in this release.

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

136.1.1.47

What's new

This release includes an independent update for Citrix Enterprise Browser version 136.1.1.47, which is based on Chromium version 136. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU3), Windows 2503 (Current Release), and Mac 2503. It is available for both auto update and manual update. The installer for a manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

- In Citrix Enterprise Browser, when the *copy* functionality is disabled in the Secure Private Access (SPA) settings, users are still able to press `Ctrl + s` to save the entire webpage in HTML format to their local machine. [CTXBR-13009]
- The **Save As...** option in the context menu is enabled when the Download V1 policy restricts downloads. [CTXBR-12986]

135.1.1.22

What's new

This release includes an independent update for Citrix Enterprise Browser version 135.1.1.22, which is based on Chromium version 135. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU3), Windows 2503 (Current Release), and Mac 2503. It is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

- The search bar (CTRL+F) doesn't function when the Download, Upload, Watermark, or Print Policy is enabled. [CTXBR-12675]
- [AAC Codec] Audio and video playback is not functional in Citrix Enterprise Browser on macOS. [CTXBR-12686]

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

134.1.1.24

What's new

This release includes an independent update for Citrix Enterprise Browser version 134.1.1.24, which is based on Chromium version 134. This version is compatible with Citrix Workspace app for Windows LTSR 2402 (CU2 and CU3), Windows 2409.10 (Current Release), and Mac 2411.10. It is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

There are no fixed issues in this release.

133.1.1.5

What's new

This release includes an independent update for Citrix Enterprise Browser version 133.1.1.5, which is based on Chromium version 133. This version is compatible with Citrix Workspace app for Windows LTSR 2402 Cumulative Update 3.

133.1.1.16

What's new

This release includes an independent update for Citrix Enterprise Browser version 133.1.1.16, which is based on Chromium version 133. This update is compatible with Citrix Workspace app for Windows 2409.10 and Mac 2411.10. It is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

132.1.1.25

What's new

This release includes an independent update for Citrix Enterprise Browser version 132.1.1.25, which is based on Chromium version 132. This update is compatible with Citrix Workspace app for Windows

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

2409.10 and Mac 2411. It is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

There are no fixed issues in this release.

131.1.1.32

What's new

This release includes an independent update for Citrix Enterprise Browser version 131.1.1.32, which is based on Chromium version 131. This update is compatible with Citrix Workspace app for Windows 2402 LTSR (Initial release and CU1), Windows 2409, and Mac 2409.10, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

- When you access any web or SaaS app through Citrix Workspace app for Windows version 2405 or later, the accessed app might display an additional authentication page instead of opening directly. [CTXBR-11941]
- When you use Citrix Workspace app for Windows on a Microsoft Entra ID-joined device, the simplified single sign-on (SSO) feature doesn't work in Citrix Enterprise Browser. [CTXBR-11939]

130.1.1.12

What's new

This release includes an independent update for Citrix Enterprise Browser version 130.1.1.12, which is based on Chromium version 130. This update is compatible with Citrix Workspace app for Windows 2402 LTSR (Initial release and CU1), Windows 2405.11, and Mac 2409, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

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

Fixed issues

- Some web apps mightn't function as expected and display an error screen when accessed through Citrix Enterprise Browser. [CTXBR-11829]
- Citrix Enterprise Browser closes automatically when you close a tab that is still loading in the browser. [CTXBR-11828]
- When you use Citrix Enterprise Browser version 126.1.1.23 in Windows devices, the browser might close automatically when you open a new tab and type some texts in the search engine available on the homepage. [CTXBR-11827]
- When you sign in to Citrix Workspace app with a cloud store that doesn't have Secure Private Access entitlement, and if you open Citrix Enterprise Browser, an incorrect error message appears. [CTXBR-5838]

128.1.1.32

This release includes an independent update for Citrix Enterprise Browser version 128.1.1.32, which is based on Chromium version 128. This update is compatible with Citrix Workspace app for Windows 2402 LTSR (Initial release and CU1), Windows 2405.10 and Mac 2405.11, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

127.1.1.41

This release includes an independent update for Citrix Enterprise Browser version 127.1.1.41, which is based on Chromium version 127. This update is compatible with Citrix Workspace app for Windows 2402 LTSR, Windows 2405, and Mac 2405, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Disable the address bar of the browser

Starting with the release of Citrix Enterprise Browser version 127.1.1.41 for Windows and Mac, the administrators can disable the address bar of the Enterprise Browser on their users'device through Global App Configuration service (GACS).

Disabling the address bar prevents the users from web browsing and restricts them to access only the pre-approved web and SaaS apps within the Enterprise Browser, which includes all hyperlinks within

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

those webpages. When disabled, the address bar looks grayed out and uneditable, preventing users from entering URLs.

For more information, see Disable the address bar of the browser.

Browser Data Encryption

Browser Data Encryption (formerly App Data Protection) is a feature that provides enhanced security when using the Citrix Enterprise Browser.

When you're using the Citrix Enterprise Browser with the Browser Data Encryption feature enabled, the feature focuses on encrypting browser-generated data, including the following:

- Auto-fill data
- Bookmarks
- Browser cache
- Browser storage folders
- Cookies
- History
- Network cache
- Password vault
- Settings

For more information, see Browser Data Encryption.

Fixed issues

There are no fixed issues in this release.

126.1.1.23

This release includes an independent update for Citrix Enterprise Browser version 126.1.1.23, which is based on Chromium version 126. This update is compatible with Citrix Workspace app for Windows 2405.10 and is available for auto update. For more information on auto update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

There are no fixed issues in this release.

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

126.1.1.22

This release includes an independent update for Citrix Enterprise Browser version 126.1.1.22, which is based on Chromium version 126. This update is compatible with Citrix Workspace app for Windows 2402 LTSR (Initial release and CU1), Windows 2405 and Mac 2405, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

Fixed issues

Citrix Enterprise Browser stops responding when you download a file through a blob URL, where the blob URL is a special type of URL used to represent files directly within a web page's code. [CTXBR-9799]

126.1.1.20

This release includes an independent update for Citrix Enterprise Browser version 126.1.1.20, which is based on Chromium version 126. This update is compatible with Citrix Workspace app for Windows 2402 LTSR, Windows 2405 and Mac 2405, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser.

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 through 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 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.

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

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 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 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. Additionally, 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 Administrators can restrict file uploads based on MIME (multipurpose 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 (multipurpose 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.

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

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 print 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.

> **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 group 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.

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

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.

Fixed issues

Citrix Enterprise Browser takes more time to load Google Chat and Google Docs. [CTXBR-9083]

125.1.1.15

This release includes an independent update for Citrix Enterprise Browser version 125.1.1.15, which is based on Chromium version 125. This update is compatible with Citrix Workspace app for Windows 2402 LTSR, Windows 2403.1 and Mac 2402.10, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser

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

Fixed issue

When Citrix Enterprise Browser is opened on the Mac operating system, it might enter a state where creating new tabs is not allowed, and typing into the omnibox might not function as expected. [CTXBR-8738]

124.2.1.19

This release includes an independent update for Citrix Enterprise Browser version 124.2.1.19, which is based on Chromium version 124. This update is compatible with Citrix Workspace app for Windows 2402 LTSR, Windows 2403 and Mac 2402, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of the independent installer, see Independent update of Citrix Enterprise Browser

Fixed issue

There are no fixed issues in this release.

123.2.1.22

This release includes an independent update for Citrix Enterprise Browser version 123.2.1.22, which is based on Chromium version 123. This update is compatible with Citrix Workspace app for Mac 2402 and Windows 2402. For the Mac operating system, the update is available for both auto update and manual update. For the Windows operating system, the update is available only for manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of independent installer, see Independent update of Citrix Enterprise Browser.

123.1.1.9

This release of Citrix Enterprise Browser is installed with Citrix Workspace app for Windows 2403, and it is based on the Chromium version 123.

Fixed issue

After upgrading to version 122.1.1.2, end users might encounter an issue with the bookmark bar functionality. Specifically, when clicking the bookmark folder, users might receive a prompt to open all

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

the bookmarks within that folder instead of expanding the folder to display the individual bookmarks. [CTXBR-7488]

121.1.1.26

This release of Citrix Enterprise Browser is installed with Citrix Workspace app for Windows 2402 and Mac 2402, and it is based on the Chromium version 121.

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.
> - For the Windows operating system, this feature has been available for both Workspace and StoreFront since the 119.1.1.115 release.

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.

Fixed issues

There are no fixed issues in this release.

122.1.1.2

This release includes an independent update for Citrix Enterprise Browser version 122.1.1.2, which is based on Chromium version 122. This update is compatible with Citrix Workspace app for Windows 2311.1 and Mac 2311, and is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of independent installer, see Independent update of Citrix Enterprise Browser.

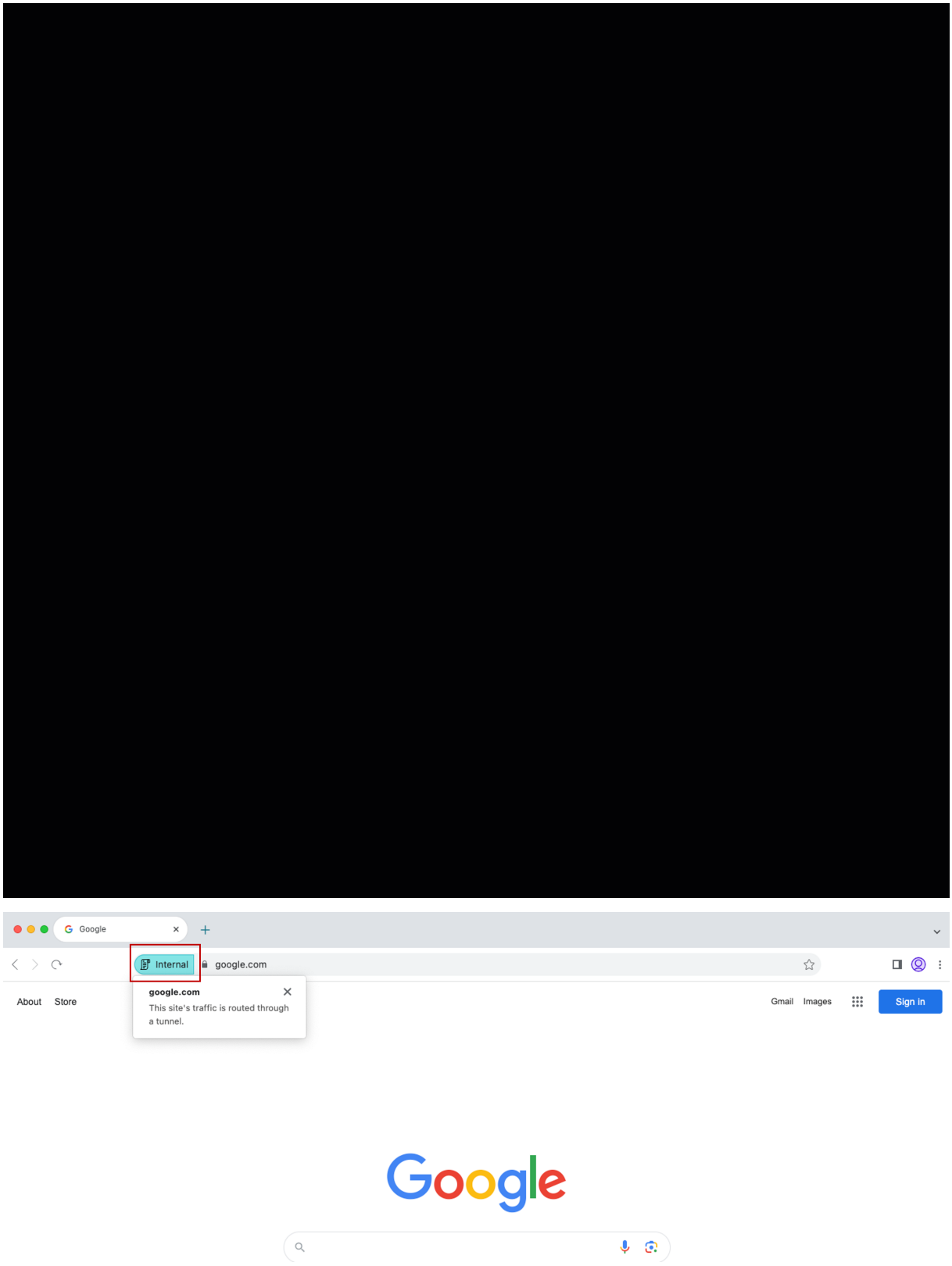
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Starting with this release, Citrix Enterprise Browser now automatically upgrades all `http://` navigations to `https://` for enhanced security. This means that even when you click on a link explicitly declaring `http://`, it will be automatically redirected to `https://`. Consequently, apps published as `http://` in Citrix Workspace app no longer open in the Enterprise Browser. As a solution, we highly recommend upgrading your apps to `https://` for seamless compatibility.

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's 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.



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

Additional settings for Citrix Enterprise Browser in the Global App Configuration service

Additional settings have been added into Global App Configuration service (GACS) for configuring Citrix Enterprise Browser. For more information, see Manage Citrix Enterprise Browser through Global App Configuration service.

Fixed issues

There are no fixed issues in this release.

121.1.1.9

This release includes an independent update for Citrix Enterprise Browser version 121.1.1.9, which is based on Chromium version 121. This update is compatible with Citrix Workspace app for Mac 2311 and Windows 2311.1. The update is available for both auto update and manual update. The installer for manual update is available on the Downloads page. For more information on auto update and manual update of independent installer, see Independent update of Citrix Enterprise Browser.

Supports auto update of independent installer on Windows

Starting with this release, Citrix Enterprise Browser supports auto update of independent installer on Windows. For more information on auto update, see Auto update.

Fixed issues

Citrix Enterprise Browser might stop responding when you apply security policies to the apps with lengthy URLs. [SPAHELP-247]

120.1.1.13

This release of the Enterprise Browser is compatible with Citrix Workspace app for Mac 2311 and Windows 2311. Enterprise Browser is based on Chromium version 120.

Citrix Enterprise Browser update to version 120 for Mac and Windows

This release includes an independent update for Citrix Enterprise Browser version 120.1.1.13, which is based on Chromium version 120. This update is compatible with Citrix Workspace app for Mac 2311 and Windows 2311 respectively. The update is available on the Downloads page.

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

Fixed issue

There are no fixed issues in this release.

119.1.1.115

This release of Citrix Enterprise Browser is compatible with the Citrix Workspace app for Mac 2311 and Windows 2311. Citrix Enterprise Browser is based on Chromium version 119.

Improved user experience and session reload time

Previously, Citrix Enterprise Browser displayed a reconnection modal when you attempt to perform an action after your session expired. Starting with Citrix Workspace app for Mac 2311 and Windows 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 `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 extension.

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

> **Note:**
>
> For Mac operating system, this feature is available only for StoreFront.

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

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

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.

Extending simplified single sign-on functionality to StoreFront

> **Note:**
>
> The feature is available only for the Windows operating system.

The single sign-on (SSO) feature is now available for StoreFront, which assures a unified SSO experience. This new capability eliminates the need for users to authenticate separately when accessing apps through StoreFront. To facilitate this SSO feature, use the same Identity Provider (IdP) for both Web and SaaS apps, and for StoreFront. 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.

Manage pass-through authentication in Citrix Enterprise Browser

> **Note:**
>
> The feature is available only for the Windows operating system.

Pass-through authentication (PTA) is a feature of Azure AD Connect. PTA is an authentication method where the user credentials are passed from the client machine to the server. You never see it as it happens on the back end. In this method, the client machine directly communicates with the authentication server to validate the user's credentials. PTA is typically used when your client machine and the authentication server trust each other, and your client machine is considered to be secure. For more information on Microsoft Azure AD pass-through authentication, see the Microsoft Entra seamless single sign-on.

To facilitate pass-through authentication, you need the Windows Accounts extension to interact with applications that require Azure AD based access within the Enterprise Browser. Administrator can configure this Windows Accounts extension as part of the mandatory list under **ExtensionInstallForcelist**. For more information on the configuration of mandatory extensions, see the Mandatory extension.

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 Mac 2311 versions (corresponding to Chromium version 119.1.1.115), you can now monitor these details as well.

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

- **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.

To monitor the end user activities from 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 the Citrix Analytics documentation.

Fixed issues

There are no fixed issues in this release.

119.1.1.4

This release of Citrix Enterprise Browser is compatible with Citrix Workspace app for Mac 2309, Windows 2309, and Windows 2309.1. Also it's based on Chromium version 119.

Citrix Enterprise Browser update to version 119 for Mac and Windows

This release includes an independent update for Citrix Enterprise Browser version 119.1.1.4, which is based on Chromium version 119. This update is compatible with Citrix Workspace app for Mac 2309, Windows 2309, and Windows 2309.1 respectively. The update is available on the Downloads page.

Fixed issue

There are no fixed issues in this release.

118.1.1.7

This release of Citrix Enterprise Browser is compatible with the Citrix Workspace app for Mac 2309 and it's based on Chromium version 118.

Citrix Enterprise Browser update to version 118 for Mac

This release includes the independent update for Citrix Enterprise Browser version 118.1.1.7, which is based on Chromium version 118. The update is compatible with Citrix Workspace app for Mac 2309. The update is available on the Downloads page.

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

Citrix Enterprise Browser user agent has changed

Earlier, the Citrix Enterprise Browser was using a custom user-agent. Starting with the Citrix Enterprise Browser version 118, the user-agent is as follows:

user-agent: `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)AppleWebKit/537.36 (KHTML, like Gecko)Chrome/118.0.0.0 Safari/537.36`

x-citrix-client: `CWABrowser CWACapable`

brand: `Citrix Enterprise Browser`

> **Note:**
>
> Depending on the version, the numbers in the user agent are subject to change.

The user-agent header, `Citrix Enterprise Browser`, helps to differentiate Citrix Enterprise Browser from other native browsers. To enhance the security, you can restrict the SaaS apps to open only in the Enterprise Browser. To do so, you must modify the sign-in page of your company's Identity Provider (IdP) to leverage the user-agent header to specify the browser brand. Then, enable the IdP to check the header during the authentication process. As a result, users can open SaaS apps only in the Enterprise Browser, not in other browsers.

For more information, see the Controlled access to SaaS applications. In this article, you can see how to restrict SaaS app access to the Enterprise Browser using either Okta or NetScaler as an IdP.

Fixed issues

There are no fixed issues in this release.

117.1.1.13

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2309.1 and it's based on Chromium version 117.

Fixed issue

The anti-screen capture feature doesn't function as intended on Citrix Enterprise Browser version 117.1.1.9, when running on Windows 11. [CTXBR-6181]

117.1.1.11

This release of Citrix Enterprise Browser is compatible with the Citrix Workspace app for Mac 2309 and it's based on Chromium version 117.

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

Support for independent update of Citrix Enterprise Browser for Mac

Citrix Enterprise Browser now supports independent update of Citrix Enterprise Browser using the independent installer. The new stand-alone installer updates Citrix Enterprise Browser independently without a need to update Citrix Workspace app. For more information, see Independent update of Citrix Enterprise Browser.

Fixed issues

There are no fixed issues in this release.

117.1.1.9

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2309 and it's based on Chromium version 117.

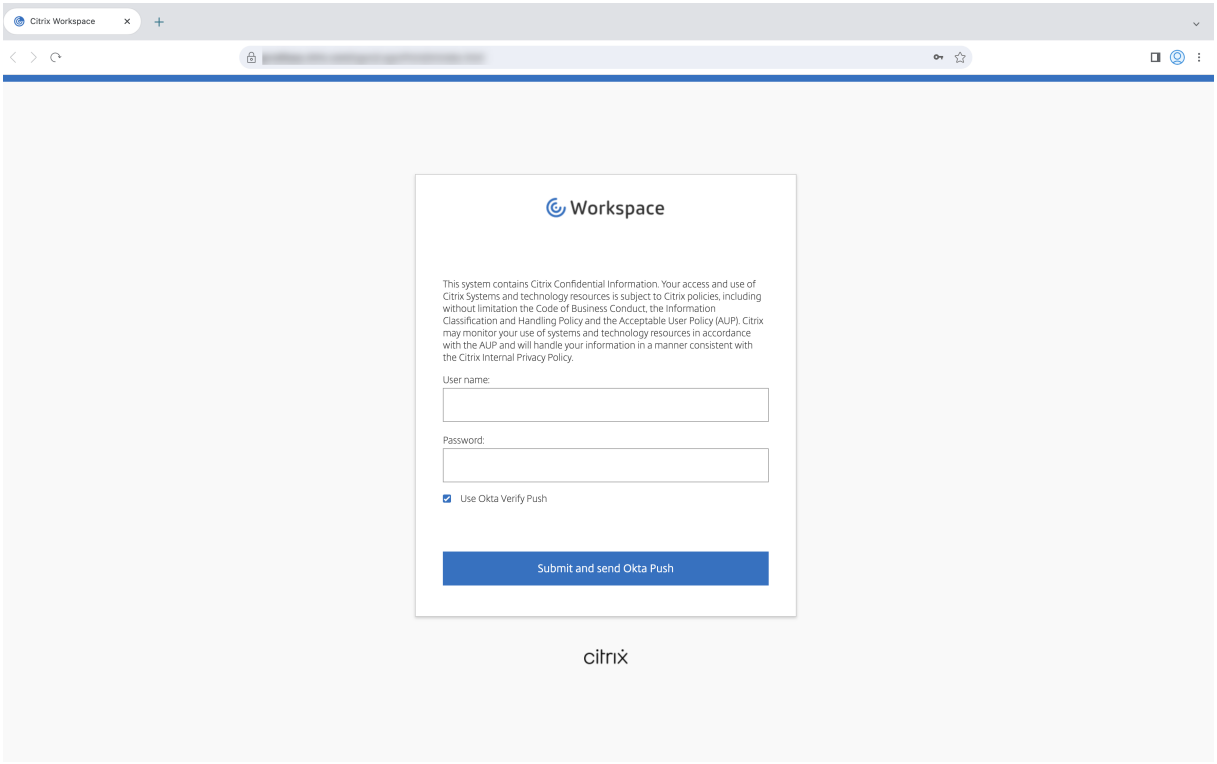
Authentication through Citrix Enterprise Browser for Windows

Previously, if the authentication token for Citrix Workspace app expired, you weren't able to use Citrix Enterprise Browser. You had to switch to Citrix Workspace app and reauthenticate to continue using Citrix Enterprise Browser.

From Citrix Workspace app for Windows 2309 version (which corresponds to the Chromium version 117.1.1.9), you can authenticate within Citrix Enterprise Browser only when the store remains the same. It ensures authentication to Citrix Workspace app as well. In addition, this feature provides a seamless sign-in experience.

> **Note:**
>
> - This feature applies to Workspace stores.

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



Fixed issues

There are no fixed issues in this release.

115.1.1.103

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2308 and it's based on Chromium version 115.

113.1.1.34

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2307 and it's based on Chromium version 113.

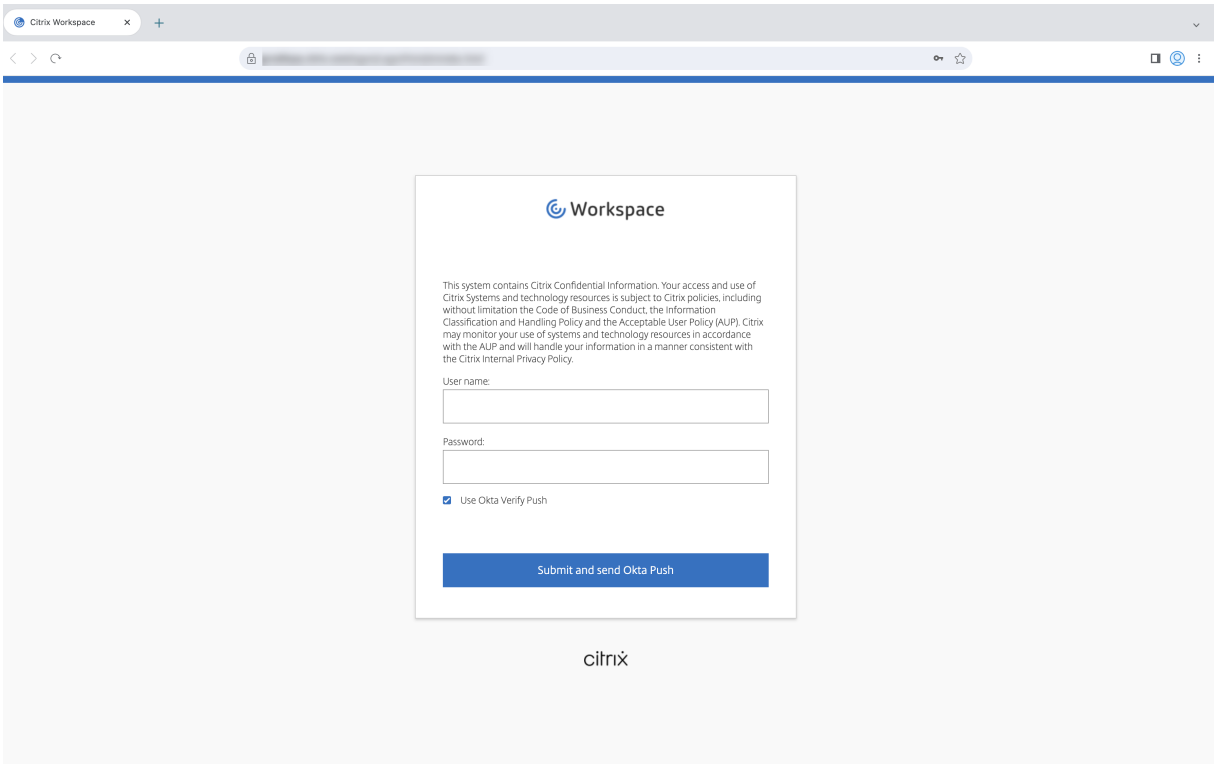
Authentication through Citrix Enterprise Browser for Mac

Previously, if the authentication token for Citrix Workspace app expired, you weren't able to use Citrix Enterprise Browser. You had to switch to Citrix Workspace app and reauthenticate to continue using Citrix Enterprise Browser.

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

From Citrix Workspace app for Mac 2307 version (which corresponds to the Chromium version 113.1.1.34), you can authenticate within Citrix Enterprise Browser only when the store remains the same. It ensures authentication to Citrix Workspace app as well. In addition, this feature provides a seamless sign-in experience.

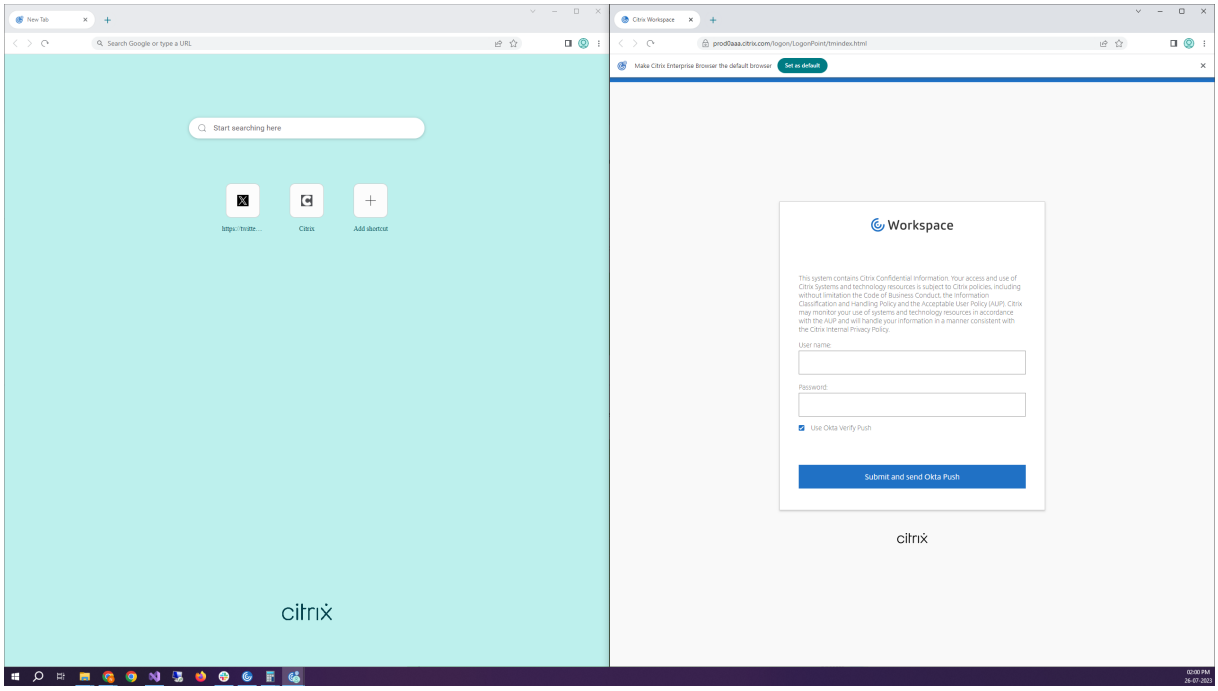
> **Note:**
>
> - This feature applies to Workspace stores.



Split view support

Citrix Enterprise Browser on Mac 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.

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



Citrix Enterprise Browser shortcut

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

> **Note:**
>
> By default, this setting is enabled for Workspace stores.

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 fa-

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

> vorite app regardless 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) Administrators can enable **Enable Citrix Enterprise Browser shortcut** as follows:

Configuration through API

To configure, here's an example JSON file to enable **Enable Citrix Enterprise Browser shortcut**:

```
"settings" : [
    {

        "name": "enable citrix enterprise browser shortcut",
        "value": true
     }

]
```

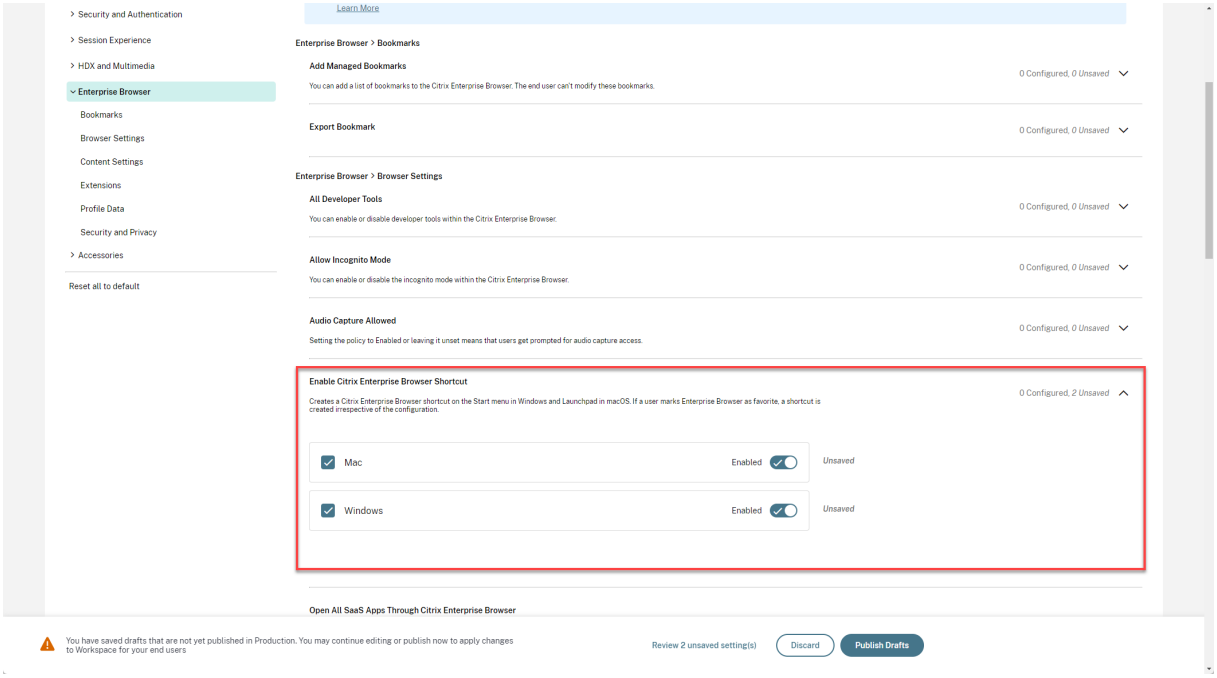
> **Note:**
>
> - The default value is **Null**.

Configuration through UI

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

Select the appropriate checkbox from the UI:

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



For more information on 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 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">`
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>
```

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:

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

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

```
    </properties>
```

Fixed issues

There are no fixed issues in this release.

112.1.1.24

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2305 and it's based on Chromium version 112.

What's new

Citrix Enterprise Browser shortcut Starting with the Citrix Workspace app for Windows 2309 version, an administrator can configure and control the presence of the Citrix Enterprise Browser shortcut on the **Start** menu.

> **Note:**
>
> - By default, this setting is enabled for Workspace stores.

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

- Group Policy Object (GPO)
- Global App Configuration service (GACS)
- web.config.file.

> **Notes:**
>
> - 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 regardless of the configuration.
> - To disable this feature for Workspace stores, administrators must apply the following settings in any one of the following:

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

```
1  - set the **CEBShortcutEnabled** attribute to **false** in the `web.
     config` file.
2  - disable the **Enable Citrix Enterprise Browser shortcut** property
     in GPO and GACS.
```

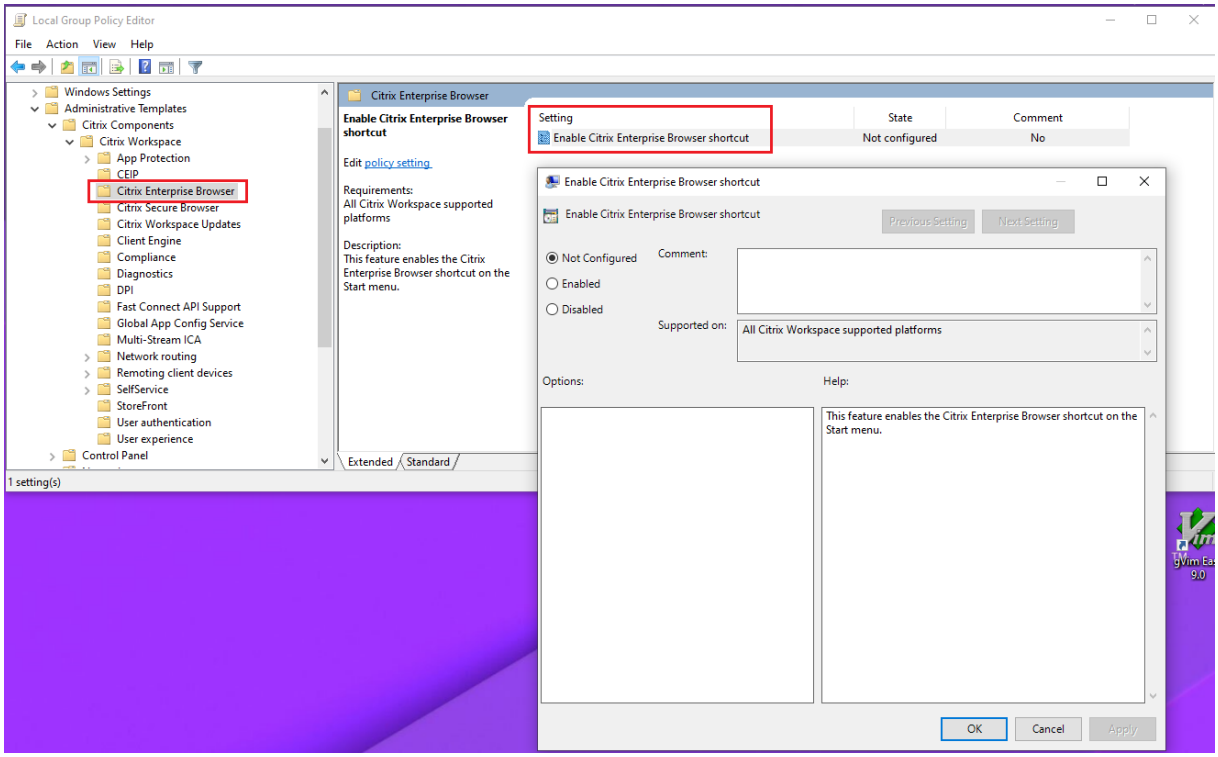
Using Group Policy Object

Administrators can use the **Enable Citrix Enterprise Browser shortcut** property to control the display of the Citrix Enterprise Browser shortcut on the Start menu.

> **Note:**
>
> Configuration through GPO is applicable on Workspace and StoreFront.

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

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Citrix Enterprise Browser**.
3. Select the **Enable Citrix Enterprise Browser** shortcut option.



For more information on how to use the GPO, see Group Policy Object administrative template in Citrix Workspace app for Windows documentation.

Global App Configuration service (GACS)

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

Administrators can enable **Enable Citrix Enterprise Browser shortcut** as follows:

Configuration through API To configure, here's an example JSON file to enable **Enable Citrix Enterprise Browser shortcut**:

```
"settings" : [
    {

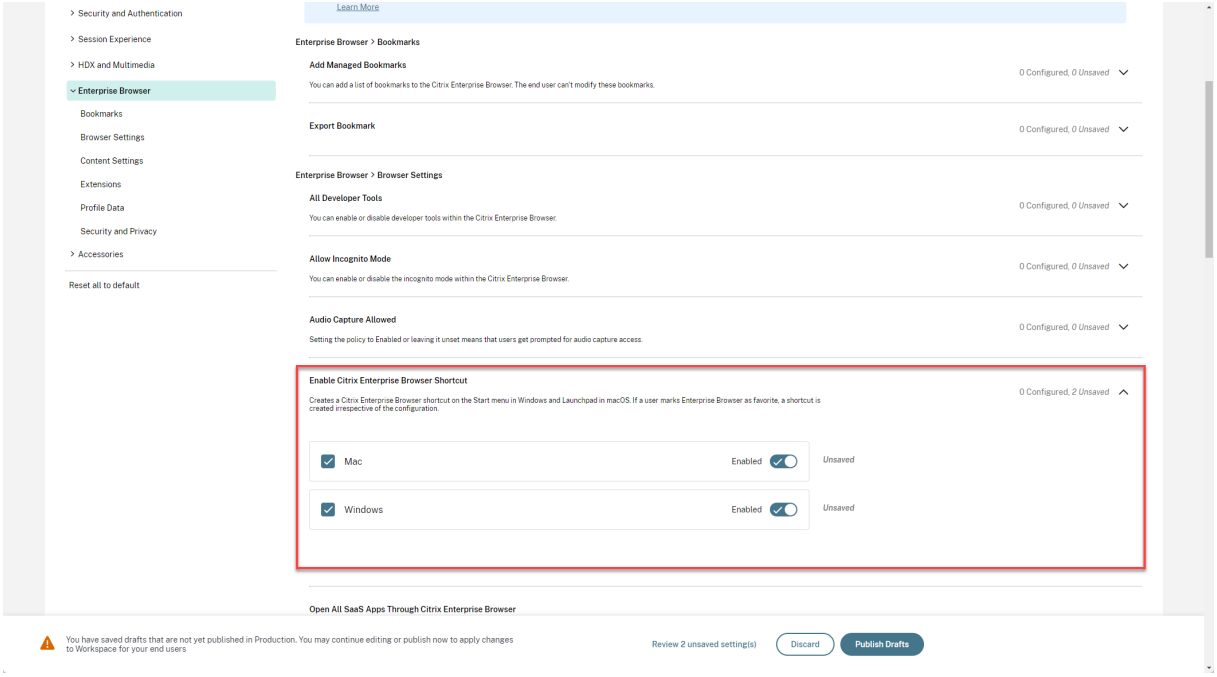
        "name": "enable citrix enterprise browser shortcut",
        "value": true
    }

]
```

> **Note:**
>
> - The default value is **Null**.

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

Select the appropriate checkbox from the UI:



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

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

> **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:**
>
> Configuration through `web.config` 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">`
3. Before the `</account>` tag, navigate to the properties of that user account and add the following:

```
<properties>

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

</properties>
```

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>
```

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

```
                        <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>
```

Modification in Secure Private Access policy implementation on internal Web and SaaS apps
This feature enhances the security policies implementation on the Web and SaaS apps. When a webpage and its iframes have different policies, we follow a stricter policy implementation. You can apply a union of all policies on the entire webpage, including the iframes. However, the watermark is applied to the webpage only.

Support for browser extensions Citrix Enterprise Browser allows you to add browser extensions 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 the Global App Configuration service.

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

Use the Global App Config service 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 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 APIs or the GACS Admin UI:

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

- “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 an administrator to push bookmarks to the Citrix Enterprise Browser.
- “Enable developer tools”- Enable or disable developer tools within Citrix 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.

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

> **Notes:**
>
> - The name and value pair are case-sensitive.
> - All the browser settings in GACS are under the following categories:

```
```
        {

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

```
```

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

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

> **Note:**
>
> The minimum version required is:
>
> - Citrix Workspace app for Mac 2305, and the corresponding Citrix Enterprise Browser version is 112.1.1.23.

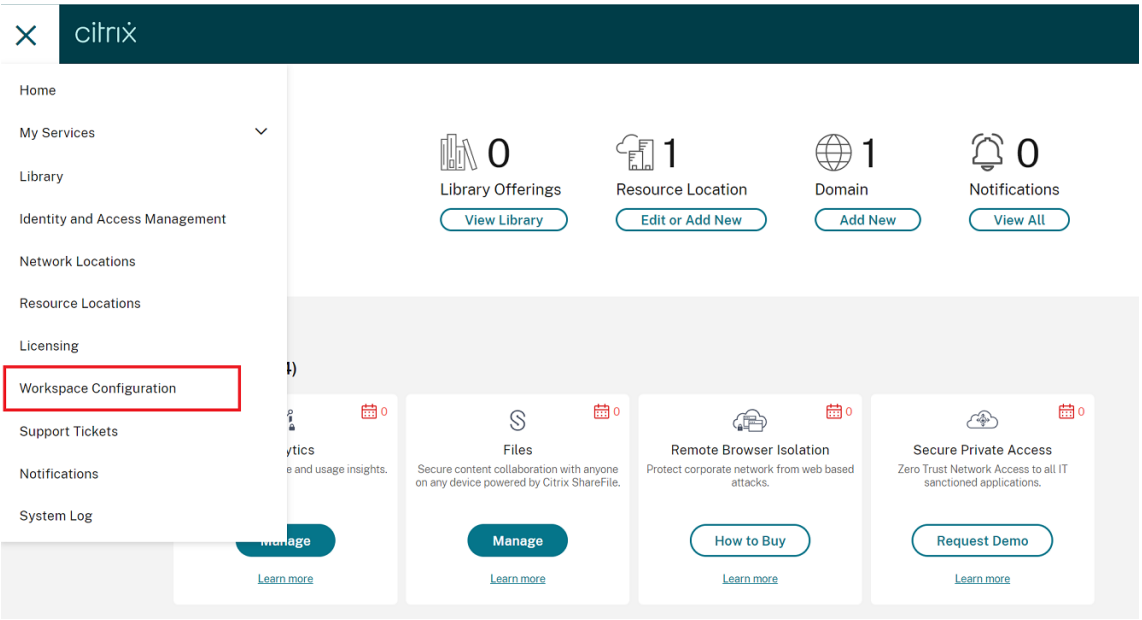
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - Citrix Workspace app for Windows 2305, and the corresponding Citrix Enterprise Browser version is 112.1.1.24.

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**.



   The **Workspace Configuration** screen appears.

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

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

Fixed issues

There are no fixed issues in this release.

112.1.1.23

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2305 and it's based on Chromium version 112.

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

What's new

Modification in Secure Private Access policy implementation on internal Web and SaaS apps
This feature enhances the security policies implementation on the Web and SaaS apps. When a webpage and its iframes have different policies, we follow a stricter policy implementation. You can apply a union of all policies on the entire webpage, including the iframes. However, the watermark is applied to the webpage only.

Support for browser extensions Citrix Enterprise Browser allows you to add browser extensions 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 the Global App Configuration service.

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

Use the Global App Config service 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 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 APIs or the GACS Admin UI:

- "Enable CWB 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 an administrator to push bookmarks to the Citrix Enterprise Browser.
- "Enable developer tools"- Enable or disable developer tools within Citrix 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.

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

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

> **Notes:**
>
> - The name and value pair are case-sensitive.
> - All the browser settings in GACS are under the following categories:

```
```
        {

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

```
```

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

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

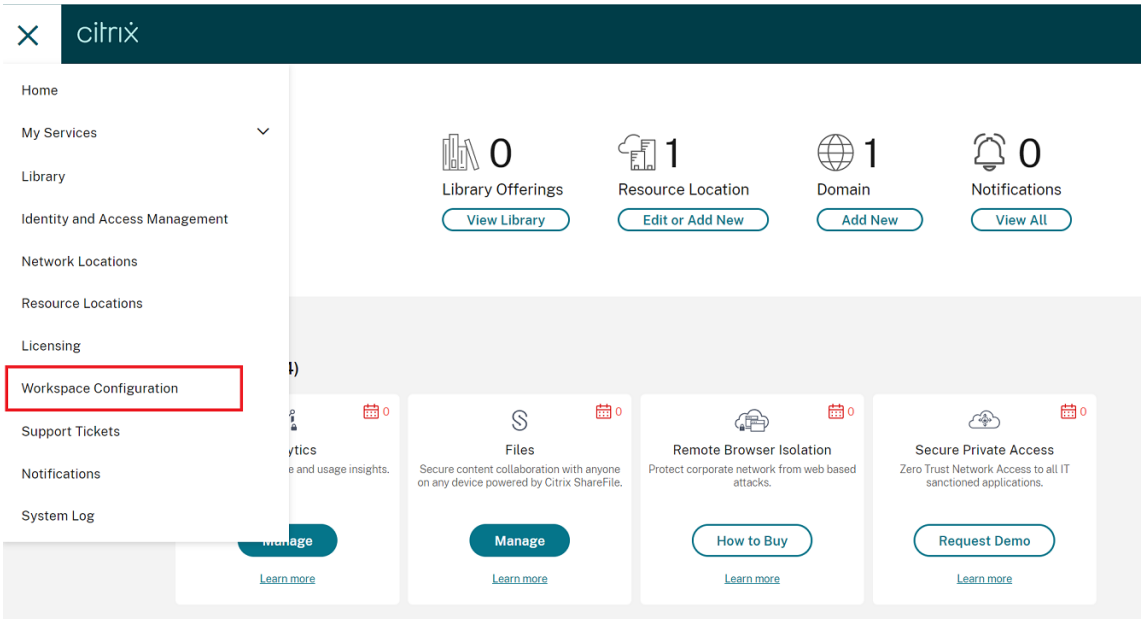
> **Note:**
>
> The minimum version that is required is:
>
> - Citrix Workspace app for Mac 2305, and the corresponding Citrix Enterprise Browser version is 112.1.1.23.
> - Citrix Workspace app for Windows 2305, and the corresponding Citrix Enterprise Browser version is 112.1.1.24.

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.

Fixed issues

There are no fixed issues in this release.

109.1.1.29

What's new

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2303 and it's based on Chromium version 109.

Secure Private Access support for StoreFront As an administrator, you can now configure Web and SaaS apps in StoreFront using a Secure Private Access solution. After the administrator configures the app, end users can open web and SaaS apps using Citrix Enterprise Browser with enhanced security.

For more information, see Secure Private Access for on-premises in the Citrix Secure Private Access documentation.

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

Fixed issues

- The published URLs open through the Citrix Enterprise Browser instead of the device's default browser. [CTXBR-4718]

108.1.1.97

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2302 and it's based on Chromium version 108.

What's new

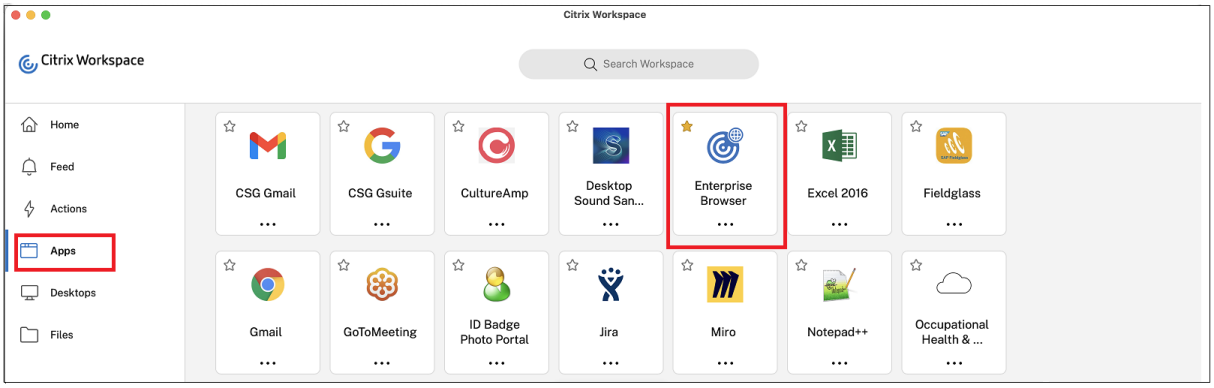
Open all web and SaaS apps through the Citrix Enterprise Browser In this release of Enterprise Browser (in Citrix Workspace app for Windows), all internal web apps and external SaaS apps available in Citrix Workspace app open in Citrix Enterprise Browser.

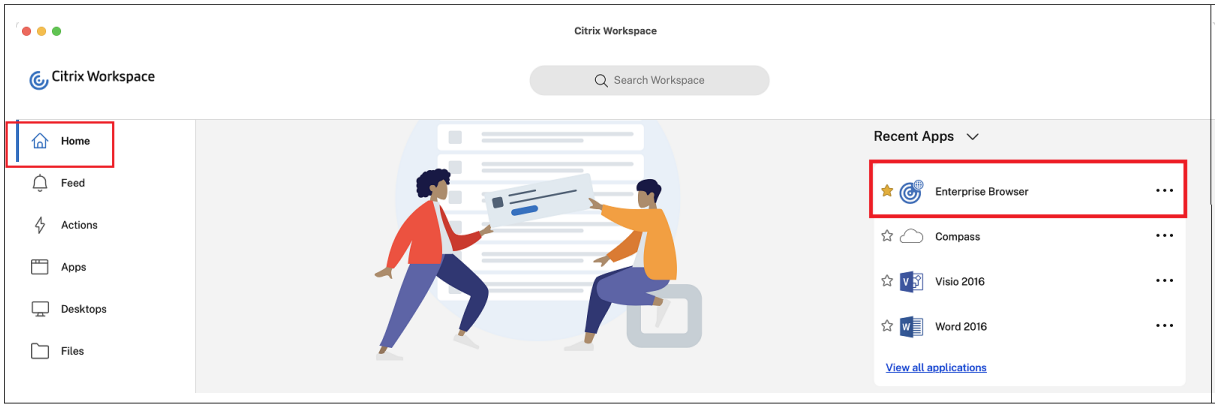
Option to start Citrix Enterprise Browser from within Citrix Workspace app Previously, you opened Citrix Enterprise Browser from Citrix Workspace app after opening a web or SaaS app.

Starting with this release, you can open the Citrix Enterprise Browser directly from the Citrix Workspace app without requiring you to open a web or SaaS app. This feature provides easy access to Citrix Enterprise Browser and doesn't require any configurations from administrators. This feature is available by default.

> **Note:**
>
> This feature is available for Cloud customers only, and the end user must have entitlement to at least one web or SaaS app through Secure Private Access.

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





Fixed issues

- Some SaaS apps which have enhanced security set to OFF fail to open in Citrix Enterprise Browser if Citrix Enterprise Browser is the default browser. [CTXBR-4106] [CTXBR-4405]

107.1.1.13

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2301 and it's based on Chromium version 107.

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 are configured by the administrator for the end user. When a user clicks any link within a native application, if it's a work link, it's opened through Citrix Enterprise Browser. If not, it's opened through the alternate browser that the end-user selects.

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

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]

107.1.1.13

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2212 and it's based on Chromium version 107.

> **Note:**
>
> - From release 2210 (105.1.1.27), the **Open all web and SaaS apps through the Citrix Enterprise Browser** feature is disabled.

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 are configured by the administrator for the end user. When a user clicks any link within a native application, if it's a work link, it's opened through Citrix Enterprise Browser. If not, it's opened through the alternate browser that the end-user selects.

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

Fixed issues

There are no fixed issues in this release.

105.2.1.40

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2210.5 and it's based on Chromium version 105. This release addresses issues that help to improve performance and stability.

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

Fixed issues

There are no fixed issues in this release.

105.2.1.40

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2211 and it's based on Chromium version 105. This release addresses issues that help to improve performance and stability.

Fixed issues

There are no fixed issues in this release.

105.1.1.36

This release of Citrix Enterprise Browser (in Citrix Workspace app for Mac) is based on Chromium version 105.

This release addresses issues that help to improve overall performance and stability. For more information about what's new in 105.1.1.36, see what's new in 105.1.1.27 section. The list of features is common in both releases.

Fixed issues

- When you open a Web or SaaS app with upload restrictions, the app opens in Secure Browser Service (SBS) instead of Citrix Enterprise Browser. [CTXBR-3686]

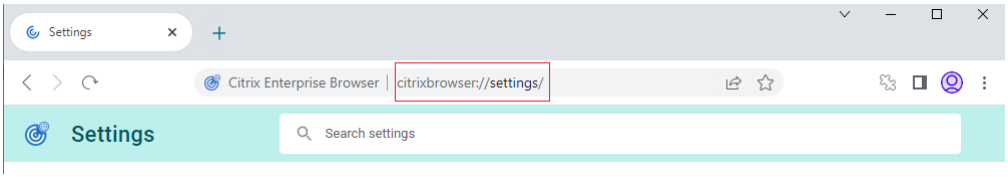
105.1.1.27

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Windows 2210 and it's based on Chromium version 105.

Rebranding Citrix Workspace Browser

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

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



> **Note:**
>
> If you've pinned the Citrix Workspace Browser icon to the docker, you must remove it manually.

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 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.

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.

Open all web and SaaS apps through the Citrix Enterprise Browser

In this release of Citrix Enterprise Browser (in Citrix Workspace app for Windows), all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Enterprise Browser.

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

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 the Global App Configuration service.

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

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.

Use the Global App Config 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 CWB 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 Citrix 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 Config service to manage 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

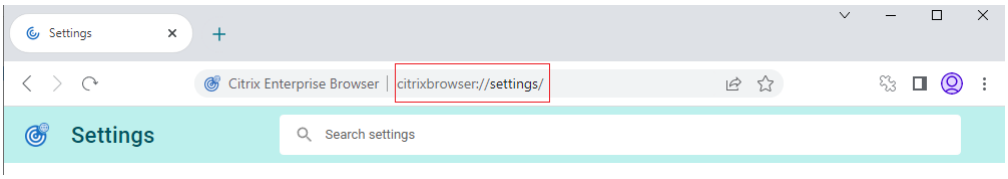
There are no fixed issues in this release.

105.1.1.19

This release of Citrix Enterprise Browser is installed with the Citrix Workspace app for Mac 2210 and it's based on Chromium version 105.

Rebranding Citrix Workspace Browser

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



> **Note:**
>
> If you've pinned the Citrix Workspace Browser icon to the docker, you must remove it manually.

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 the product documentation are being updated in the coming weeks.

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

- It's possible that some items (such as commands and MSIs) might continue to keep their former names to prevent breaking existing customer scripts.
- Related product 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.

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.

Open all web and SaaS apps through the Citrix Enterprise Browser

In this release of Citrix Enterprise Browser (in Citrix Workspace app for Windows), 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 the Global App Configuration service.

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

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 ac-

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

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

Use the Global App Config 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 CWB 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 administrator to push bookmarks to the Citrix Enterprise Browser.
- "Enable developer tools"- Enable or disable developer tools within Citrix 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.

For more information, see Use Global App Config service to manage 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.

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

Fixed issues

There are no fixed issues in this release.

103.2.1.10

This release of Citrix Enterprise Browser (in Citrix Workspace app for Mac 2209) is based on Chromium version 103.

Fixed issues

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

103.1.1.14

This release of Citrix Enterprise Browser (in Citrix Workspace app for Mac 2208.1) is based on Chromium version 103.

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 update 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 release, 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 ac-

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

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

Fixed issues

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

102.1.1.14

This release of Citrix Enterprise Browser (in Citrix Workspace app for Windows 2207) is based on Chromium version 102.

Open all web and SaaS apps through the Citrix Enterprise Browser [Technical Preview]

From this release, 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

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

101.1.1.14

- This release of Citrix Enterprise Browser (in Citrix Workspace app for Mac) is based on Chromium version 101.
- Citrix Workspace app now alerts you about closing active browser windows, when you do any of the following in the Citrix Workspace app:
  - Sign out from a store
  - Switch to a different store

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

- Add a new store
- Delete the current store

Fixed issues

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

101.1.1.12

This release of Citrix Enterprise Browser (in Citrix Workspace app for Windows) is based on Chromium version 101.

Fixed issues

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

101.1.1.9

This release of Citrix Enterprise Browser (in Citrix Workspace app for Windows) is based on Chromium version 101.

Fixed issues

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

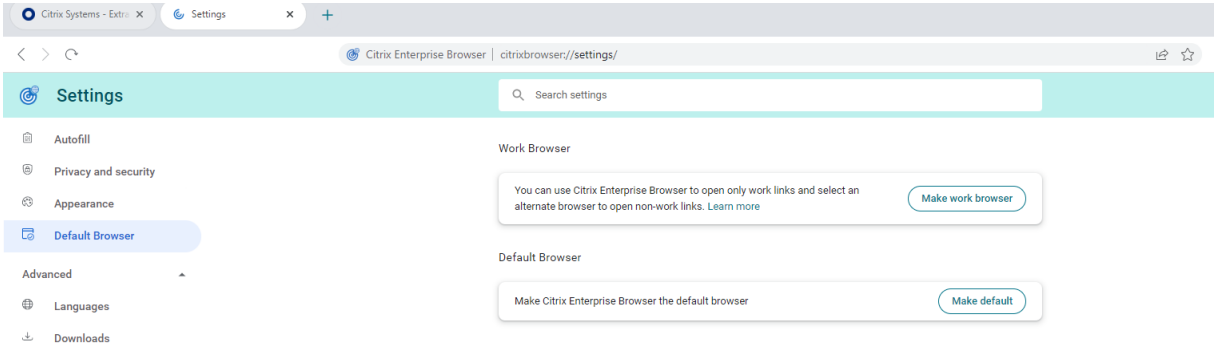
99.1.1.8

This release of Citrix Enterprise Browser (on Mac) is based on Chromium version 99.

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.

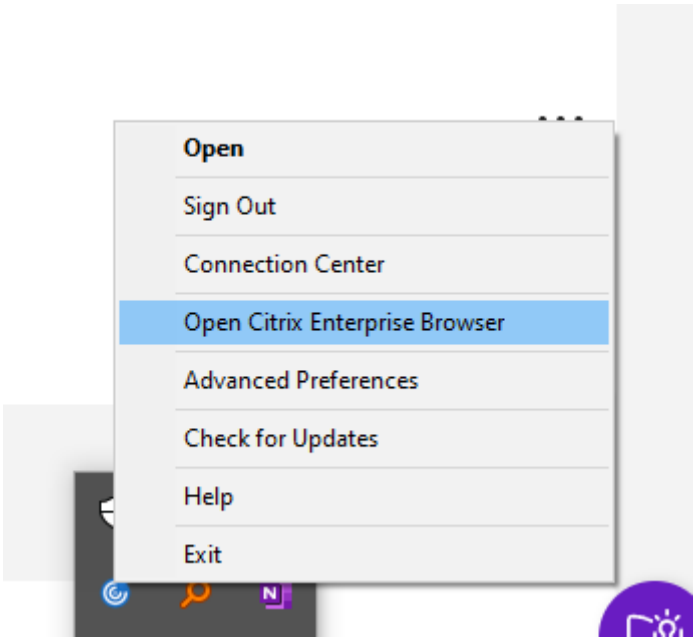
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about making Citrix Enterprise Browser your default browser, see Set Citrix Enterprise Browser as the default browser.

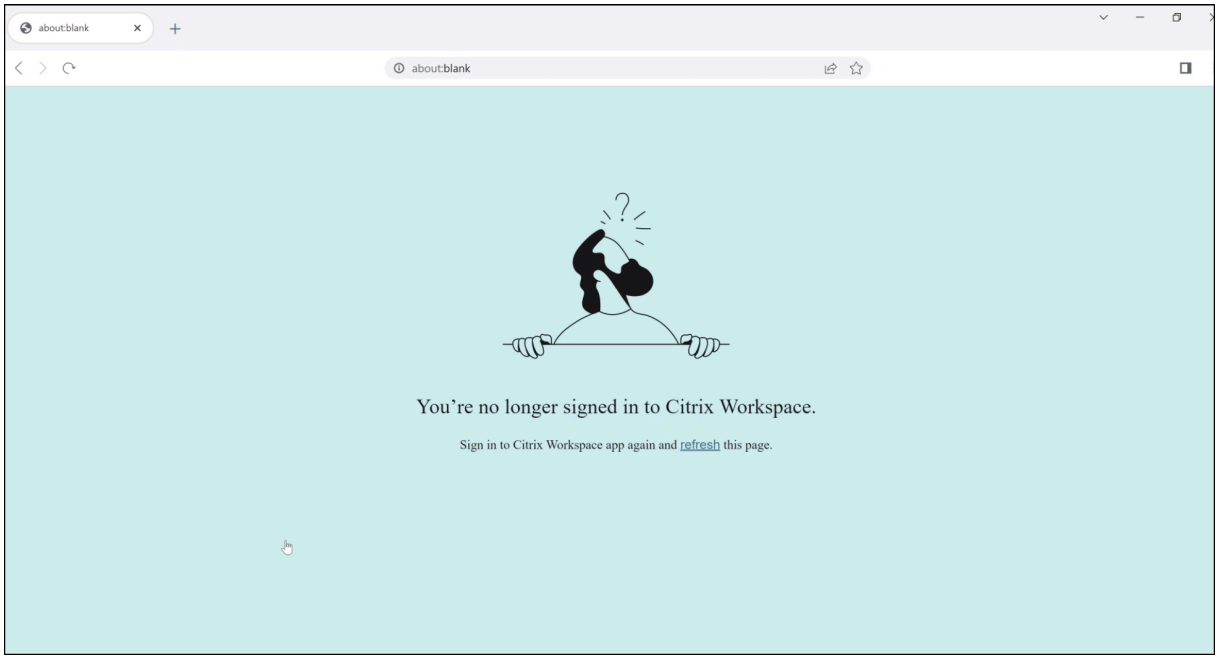
Open Citrix Enterprise Browser from the Workspace icon in the system tray

You can now open **Citrix Enterprise Browser** from the Workspace app icon on Windows OS. To open the **Citrix Enterprise Browser** from the Workspace app icon in the system tray, right-click the Workspace app icon and click **Open Citrix Enterprise Browser**.



If you have not already signed in to the Workspace app, you must provide your credentials and refresh the page when prompted.

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



> **Note:**
>
> The **Open Citrix Enterprise Browser** option isn't available if your system administrator hasn't added any web or SaaS apps in the Workspace app.

Fixed issues

- On devices running Mac, the **Look Up** option is grayed out when the **Restrict clipboard access** policy is enabled. [CTXBR-1812]
- The **Save link as** option is enabled for SaaS apps when the **Restrict clipboard access** policy is enabled. [CTXBR-1827]
- When the **Restrict clipboard access** is enabled, you cannot drag selections from a webpage to the text editor although the webpage supports it. [CTXBR-1829]
- On devices running Mac, Advanced Audio Coding (AAC) isn't supported. [CTXBR-1844]

98.1.2.20

This release of Citrix Enterprise Browser is based on Chromium version 98.

Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps [Technical Preview]

This feature simplifies the configuration of SSO for internal web apps and SaaS apps while using third-party identity providers (IdPs) in the Workspace app for Windows. The enhanced SSO experience re-

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

duces the entire process to a few commands. It eliminates the mandatory prerequisite to configure Citrix Secure Private Access™ in the IdP chain to set up SSO. It also improves the user experience, provided the same IdP is used for authentication to both the Workspace app and the particular web or SaaS app being launched.

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

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

98.1.2.17

This release of Citrix Enterprise Browser is based on Chromium version 98.

Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps [Technical Preview]

This feature simplifies the configuration of SSO for internal web apps and SaaS apps while using third-party identity providers (IdPs) in the Workspace app for Mac. The enhanced SSO experience reduces the entire process to a few commands. It eliminates the mandatory prerequisite to configure Citrix Secure Private Access in the IdP chain to set up SSO. It also improves the user experience, provided the same IdP is used for authentication to both the Workspace app and the particular web or SaaS app being launched.

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.

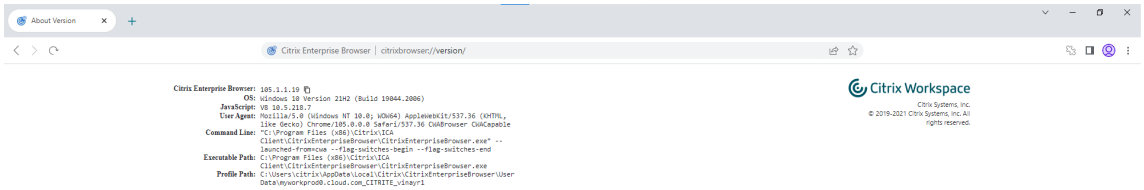
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

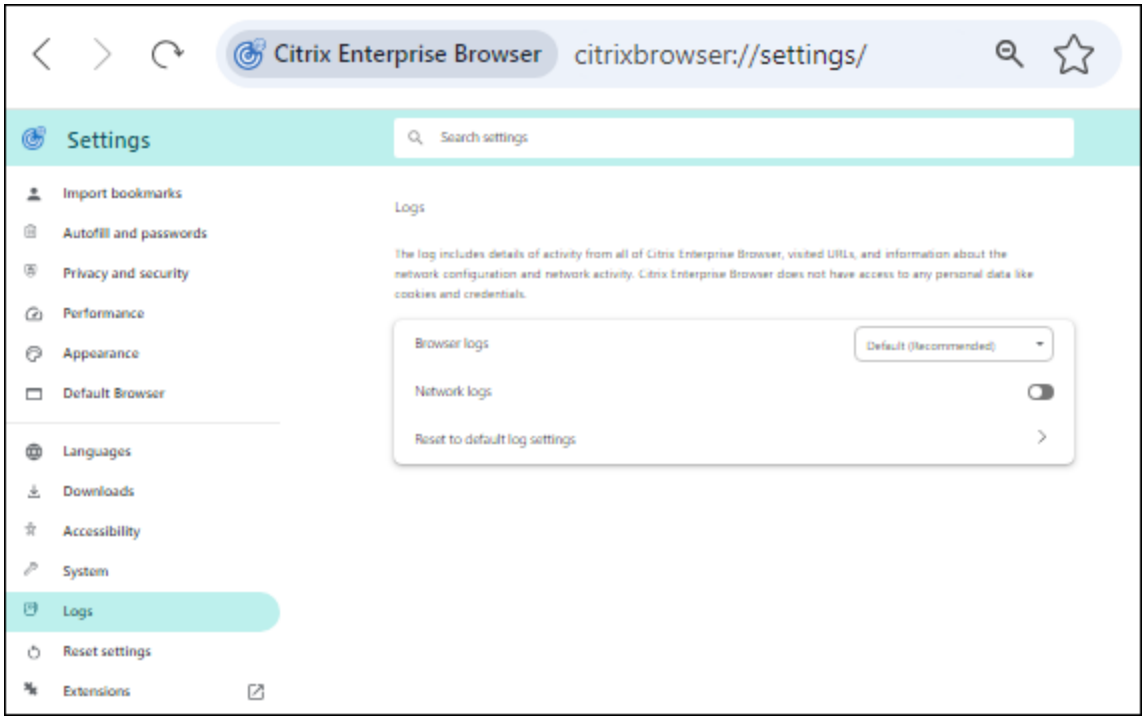
This release addresses several issues that help to improve overall performance and stability.

97.1.2.22

- This release of Citrix Enterprise Browser is based on Chromium version 97.
- As part of the branding update, the browser is renamed as Citrix Enterprise Browser in the UI and system files.
- **View Enterprise Browser version details.**: you can now view the complete version details of the Citrix Enterprise Browser by typing the following URL in the address bar:`citrixbrowser://version/`.



- **Collect Citrix Enterprise Browser logs.**: you can collect details about browser activity and network configuration by navigating to **Settings** > **Advanced** > **Logs**. By default, the log collection level is set to **Error**, which is the recommended value.



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

You can customize the log collection level by selecting one of the following values from the drop-down list:

- **Verbose**
- **Info**
- **Warning**
- **Error (Recommended)**
- **Fatal**

For more information about collecting logs, see Log collection.

Fixed issues

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

95.1.1.19

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

Fixed issues

- If a Progressive Web App (PWA) that is protected is opened on Mac, the **App Protection** policies aren't enforced. [RFMAC-10128]

92.2.1.10

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

Fixed issues

- On devices running Mac, the Advanced Audio Coding (AAC) isn't supported. [CTXBR-1844]
- In Citrix Enterprise Browser, you're unable to capture screenshots of browser windows that aren't protected. This issue occurs when protected browser windows are minimized. This issue occurs intermittently. [CTXBR-1925]
- Open a protected SaaS app, open a new tab, and separate the new tab into a new window by dragging it out of the tab bar. Now arrange two windows next to each other and open a new tab in the second window and take a screenshot. You can capture the screenshot for the protected SaaS app as well. This issue occurs on Mac. [RFMAC-10060]

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

92.1.1.31

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

Fixed issues

- The browser crashes when you switch from the protected desktop session window to the unprotected SaaS app. This issue occurs on Mac when you've opened a protected app, an unprotected SaaS app, and a protected desktop session. [CTXBR-2087]
- If your administrator has installed external extensions in Google Chrome, the Citrix Enterprise Browser crashes when you open it. [CTXBR-2135]

Known issues

Known issues in 133.1.1.16 for Windows and Mac

After updating Citrix Enterprise Browser to version 132.1.1.25, users are unable to use the Enterprise Browser when Browser Data Encryption is enabled. The following error message is displayed:

"You're no longer signed in to Citrix Workspace"[CTXBR-12287]

Known issues in 131.1.1.32 for Mac

Uninstalling Citrix Workspace app for macOS 15 or later doesn't clean up the Launch Service Database. As a result, when you reinstall the Citrix Workspace app, users can't manage the **Work Browser** feature in Citrix Enterprise Browser under **Settings** > **Default Browser**. As a workaround, you can run the following command in Terminal and then restart the device.

```
/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks
/LaunchServices.framework/Versions/A/Support/lsregister -kill -r -v -
apps u,s,l
```

[CTXBR-11967]

Known issues in 122.1.1.2 for Mac

After upgrading to version 122.1.1.2, end users might encounter an issue with the bookmark bar functionality. Specifically, when clicking the bookmark folder, users might receive a prompt to open all the bookmarks within that folder instead of expanding the folder to display the individual bookmarks. [CTXBR-7488]

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

Known issues in 115.1.1.103 for Mac

- When you sign in to Citrix Workspace app with a cloud store that doesn't have Secure Private Access entitlement, and if you open Citrix Enterprise Browser, an incorrect error message appears:

  Sign in to Citrix Workspace app again and refresh this page.

  The expected error message is:

  Secure Private Access entitlements aren't available for your store.

  [CTXBR-5838]

Known issues in 109.1.1.29 for Windows

- When the end user doesn't have Citrix Enterprise Browser installed, the published URLs with the **SPAEnabled** tag open through the device's default browser instead of Citrix Enterprise Browser. In such a case, the security policies don't apply. The issue occurs on the StoreFront deployments only. [CTXBR-4753]

Known issues in 107.1.1.13 for Mac

- On Mac 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]

Known issues in 107.1.1.13 for Windows

- Some SaaS apps which have enhanced security set to **OFF** fail to open in Citrix Enterprise Browser if Citrix Enterprise Browser is the default browser. [CTXBR-4106]

Known issues in 99.1.1.9

- When traffic is tunneled through NGS, Citrix Workspace app might fail to upload or download files that are greater than 64 MB. [CTXBR-3354]

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

Known issues in 98.1.2.17

- After upgrading from Citrix Enterprise Browser version 2201 to version 2203, previously saved passwords are lost and you're unable to save new passwords. This issue occurs in the Citrix Workspace app for Mac version 2203. [CTXBR-3063]

Known issues in 92.1.1.31

- On devices running Mac, the **Look Up** option is grayed out and not available when the **Restrict clipboard access** policy is enabled. [CTXBR-1812]
- The **Save link as** option still is enabled for SaaS apps when the **Restrict clipboard access** policy is enabled. [CTXBR-1827]
- When the **Restrict clipboard access** is enabled, you can't drag selections from a webpage to the text editor although the webpage supports it. [CTXBR-1829]
- If you open Citrix Enterprise Browser as a standalone app by clicking the icon when you aren't signed in to the Workspace app, an authentication prompt appears. When you sign in to the Workspace app and click the refresh icon continuously on the browser window, a blank page appears. [CTXBR-1834]
- On devices running Mac, Advanced Audio Coding (AAC) isn't supported. [CTXBR-1844]
- While you're logged into the Workspace app for Mac and the network connection is lost and restored again, the following error message appears:

  "You're no longer signed into Citrix Workspace"

  This issue occurs when you open a resource by starting the Citrix Enterprise Browser from the **Library** folder before the network connection is restored. [CTXBR-1888]
- Install a Progressive Web App from both Google Chrome and Enterprise Browser, and then uninstall either one of the apps. This action removes the desktop icon for both the app instances. [CTXBR-1893]
- Active Citrix Enterprise Browser windows don't close when the Citrix Workspace app is reset from the system tray. [CTXBR-1899]
- In Citrix Enterprise Browser, you're unable to capture screenshots of browser windows that aren't protected. This issue occurs when protected browser windows are minimized. This issue occurs intermittently. [CTXBR-1925]
- If Google Chrome has managed extensions, then Citrix Enterprise Browser crashes on launch. [CTXBR-2135]

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

- Open a protected SaaS app, open a new tab, and separate the new tab into a new window by dragging it out of the tab bar. Now arrange two windows next to each other and open a new tab in the second window and take a screenshot. You can capture the screenshot for the protected SaaS app as well. This issue occurs on Mac. [RFMAC-10060]
- If a Progressive Web App (PWA) that is protected is opened on Mac, the **App Protection** policies aren't enforced. [RFMAC-10128]

Third-party notices

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

Third Party Libraries for Citrix Enterprise Browser

System requirements and compatibility

September 6, 2025

Citrix Enterprise Browser™ (formerly Citrix Workspace™ Browser) is available starting from:

- Citrix Workspace app Windows 2309 version. For more information about requirements and compatibility, see System requirements and compatibility.
- Citrix Workspace app for Mac 2309 version. For more information about requirements and compatibility, see System requirements and compatibility.

Prerequisite

End users can use the Citrix Enterprise Browser for secure web access, only if you configure at least one web or SaaS app through Secure Private Access. For more information on configuring apps through Secure Private Access, see Apps configuration and management.

Install Citrix Enterprise Browser

February 6, 2026

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

> **Note:**
>
> Citrix Enterprise Browser can only be installed along with Citrix Workspace app for Windows and Mac version 2508.10 or earlier.

Step 1: Check your current Citrix Workspace app version

First, verify your **Citrix Workspace app** version to determine the appropriate installation method:

1. If you have Citrix Workspace app version 2508.10 or earlier with Citrix Enterprise Browser included - continue to step 2.
2. If you have a version 2511 and later - jump to step 3.

Step 2: Verify auto-update settings

Check your auto-update configuration:

1. **If auto-update is enabled** and you've previously used Citrix Enterprise Browser:
    - The latest version installs automatically through the auto-update process.
2. **If auto-update is disabled**:
    - Apps continue using the older Citrix Enterprise Browser version.
    - To get the latest version, you must upgrade it manually.

Important note

First-time users: Citrix Enterprise Browser does not update automatically if it has never been used before, even with auto-update enabled.

Step 3: Install Citrix Enterprise Browser on newer Citrix Workspace app versions

If your device has **Citrix Workspace app for Windows or Mac version 2511 or later**, follow these steps:

Begin by installing Citrix Enterprise Browser

The Citrix Workspace app for Windows and Mac versions 2511 or later don't include Citrix Enterprise Browser. You must first install a compatible version.

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

1. Install Citrix Workspace app version 2508.10 or earlier (which includes Citrix Enterprise Browser) from Citrix Downloads page.
2. To get the latest version of Citrix Workspace app for Windows or Mac, upgrade the Citrix Workspace app that was installed in step 1 without uninstalling it. Web and SaaS apps continue to launch in Citrix Enterprise Browser that is installed in step 1.

After you complete these steps, the latest Citrix Enterprise Browser is installed and ready for use.

Get started

September 6, 2025

The Citrix Enterprise Browser™ (formerly Citrix Workspace™ Browser) is released with the Citrix Workspace app for Windows and Mac. Web and SaaS apps open in the Enterprise Browser by default.

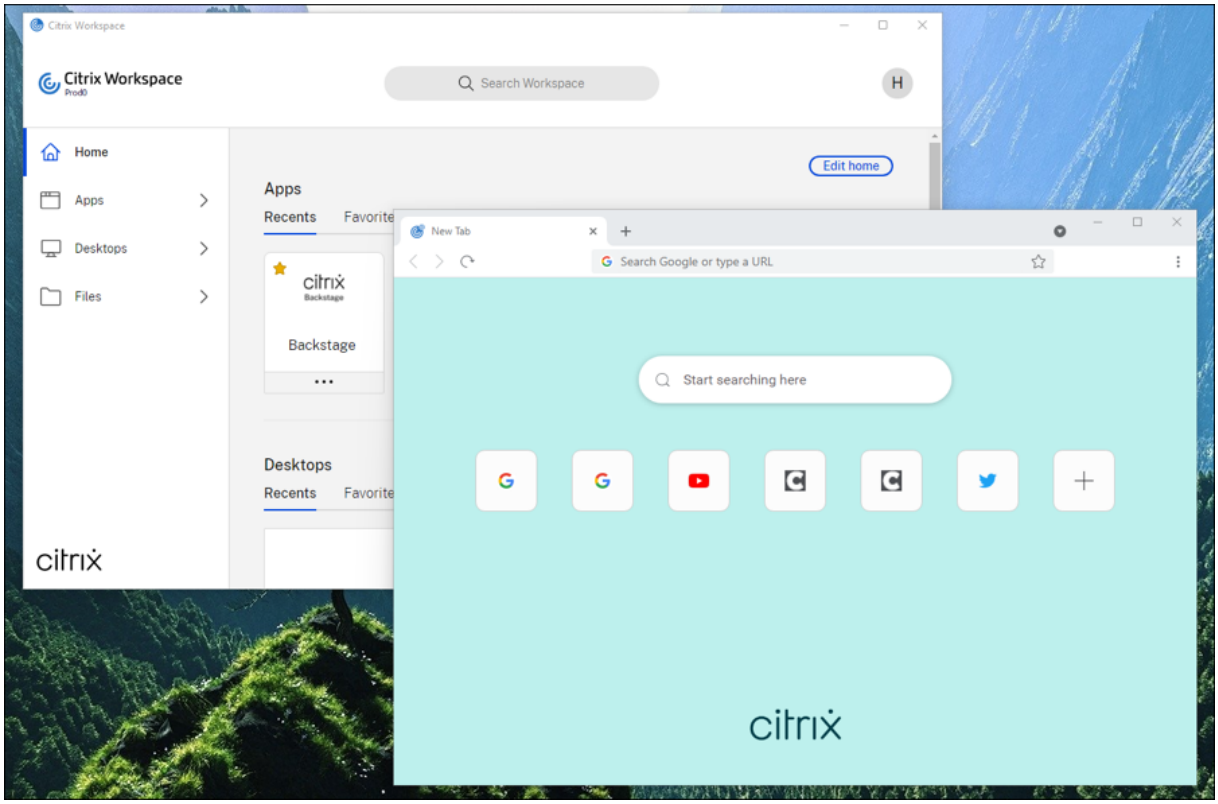
When you open a web or SaaS app in Citrix Workspace app for the first time, the app opens in Citrix Enterprise Browser. You can identify the browser windows by the following icon:



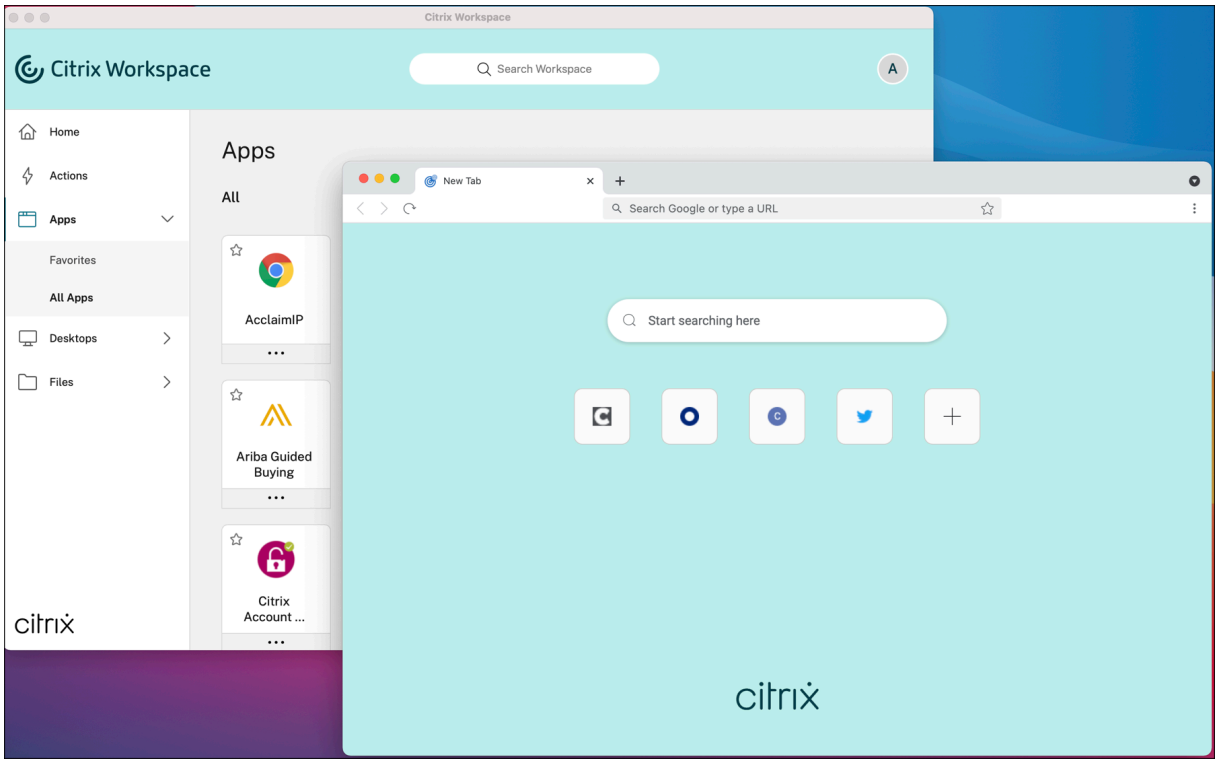
The app opens in the Citrix Enterprise Browser and the following screen appears along with a search bar:

On Windows:

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



On macOS:



All subsequent apps open in new tabs. You can log out of the Citrix Workspace app and continue to

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

use the Enterprise Browser until the session cookies time out.

Configure

September 6, 2025

You can enforce enhanced access security policies for secure access to Web or SaaS apps. You can restrict actions such as restricting printing, uploads, downloads, and clipboard access (copy-paste), and so on.

When a webpage and its iframes have different policies, we enforce a stricter policy that applies a union of all policies to the entire page, including the iframes. However, the watermark is applied to the webpage only.

For more information, see Get started with Citrix Secure Private Access. The policies are applied on a per-app and per-URL basis.

You must specify the content access settings in the Citrix Secure Private Access™ to control the policies.

The following articles help you configure Citrix Enterprise Browser™:

- Browser restrictions through Secure Private Access for Workspace
- Browser restrictions through Secure Private Access for StoreFront
- Manage Citrix Enterprise Browser through Global App Configuration service
- Manage single sign-on for Web and SaaS apps through Global App Configuration service
- Citrix Enterprise Browser shortcut
- Independent update of Citrix Enterprise Browser
- Disable the address bar of the browser

Browser restrictions through Secure Private Access for Workspace

September 6, 2025

You can now configure web and SaaS apps in Citrix Workspace™ using the Secure Private Access solution. Once you configure the apps, end users can open the web and SaaS apps using Citrix Enterprise Browser™ with enhanced security.

For more information on Secure Private Access support for Workspace, see:

- Get started with Citrix Secure Private Access in the Citrix Secure Private Access documentation.

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

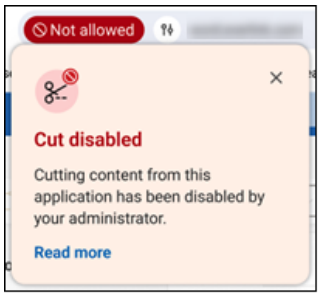
- Admin-guided workflow for easy onboarding and set up in the Citrix Secure Private Access documentation.

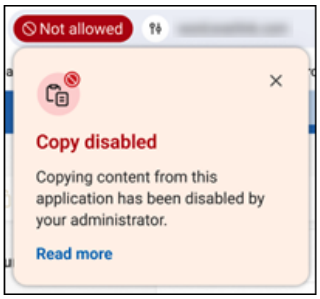
Restrict end user access on Citrix Enterprise Browser

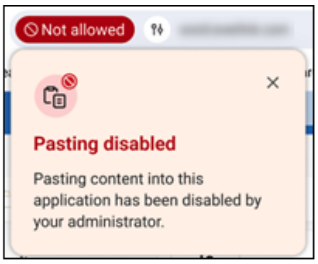
An administrator can apply the following access restrictions to Citrix Enterprise Browser for end users by using the Secure Private Access solution.

Restrict clipboard access

Disables cut, copy, and paste operations between the app and the endpoint's clipboard.



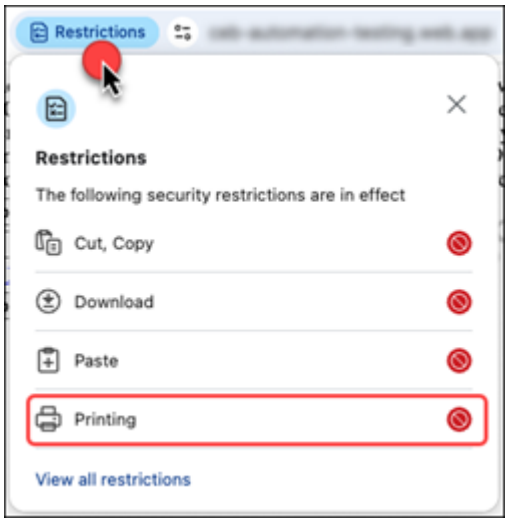




For more information, see Clipboard in Citrix Secure Private Access product documentation.

Restrict printing

Disables the ability to print from within the app.

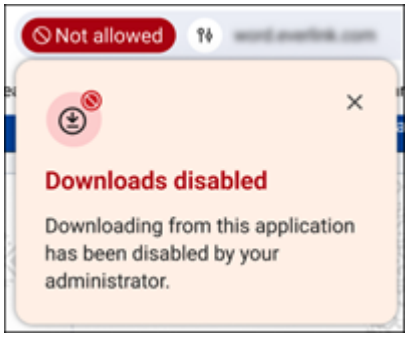


For more information, see Printing in Citrix Secure Private Access product documentation.

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

Restrict downloads

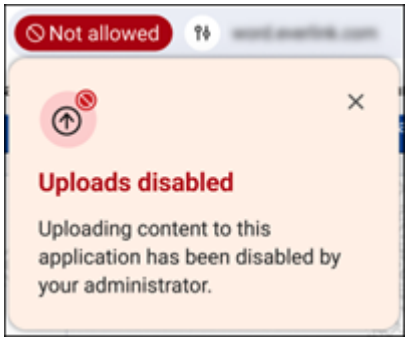
Disables the ability to download from within web and SaaS apps or copy files from the browser.



For more information, see Downloads in Citrix Secure Private Access product documentation.

Restrict upload

Disables the ability to upload files.



> **Note:**
>
> The restrict upload feature is available on:
>
> - Windows 105.1.1.27 and later
> - Mac 105.1.1.36 and later

For more information, see Uploads in Citrix Secure Private Access product documentation.

Display watermark

Overlays a screen-based watermark that shows the user name and public IP address of the endpoint.

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

> **Note:**
>
> The **Restrict navigation** option isn't supported.

For more information, see Watermark in Citrix Secure Private Access product documentation.

App protection policies

Restrict keylogging Protects users from keyloggers.

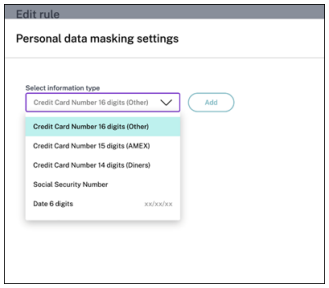
For more information, see Keylogging protection in Citrix Secure Private Access product documentation.

Restrict screen capturing Disables capturing screenshots or screen recording for the app that this policy is applied to. This policy is applied as long as a protected tab is visible (not minimized) in your browser window.

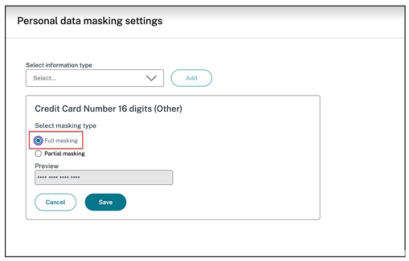
For more information, see Screen capture in Citrix Secure Private Access product documentation.

Personal data masking

Administrators can use the **Personal data masking** restriction to mask various types of Personal Identifiable Information (PII) such as credit card numbers, social security numbers, and dates. The masked contents remain secured even when copied or printed, ensuring comprehensive safeguarding of sensitive information.

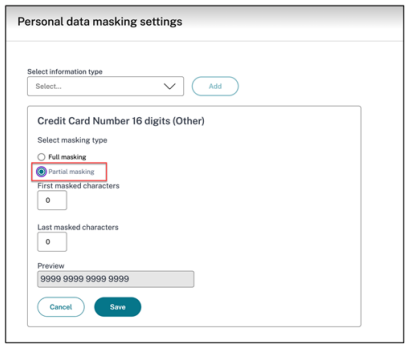


The **Personal data masking** restriction has the option to fully or partially mask the information. The **Full masking** option masks the information completely. The **Partial masking** option can be used to masks relevant areas of the information.



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

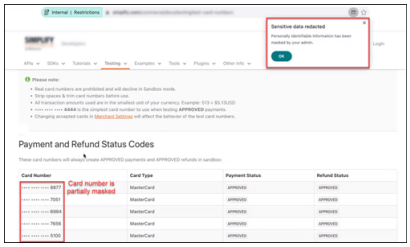
In the **Partial masking** option, administrators can choose how many characters to mask from the information, either from the beginning or the end. Respective text boxes are available to enter the character count.



Additionally, as an administrator, you have the flexibility to define the custom PII detection rules according to your requirements using regular expressions. This capability allows you to detect and mask specific information from the web page.

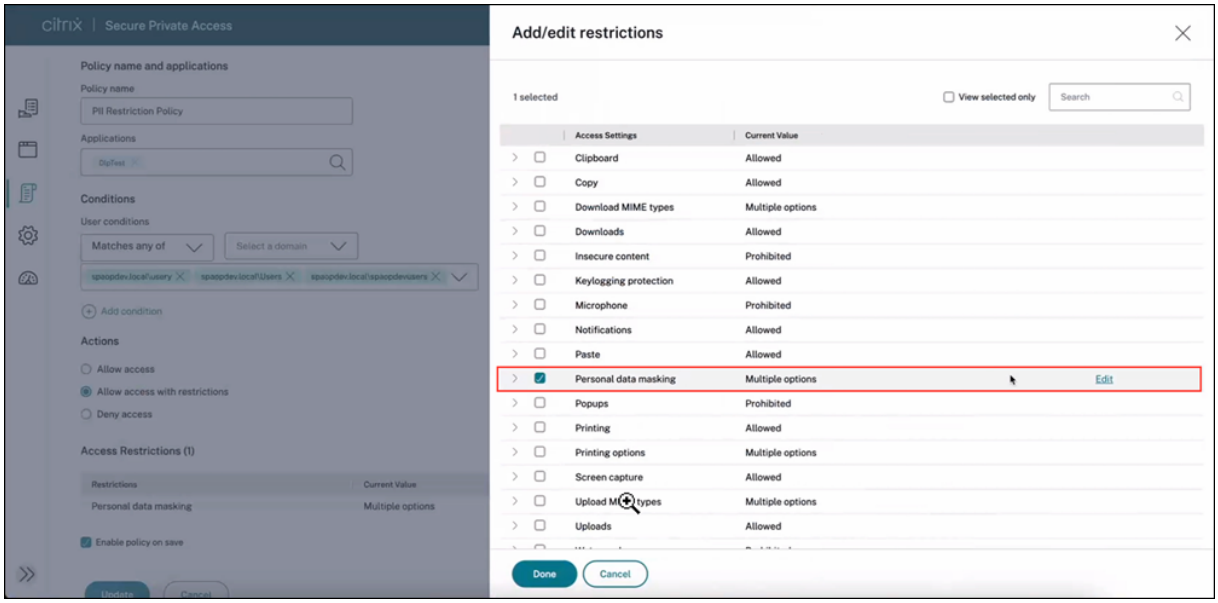
> **Note:**
>
> This feature supports only Regular expression 2 (RE2). For more information, see WhyRE2 and RE2 Syntax.

When you enable this restriction, Citrix Enterprise Browser detects the PII you choose to mask, then masks it, and displays a notification to end users.



Configuration To know more information about configuring this restriction, see Personal data masking in the Citrix Secure Private Access documentation.

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



> **Note:**
>
> - When defining PII detection rules, we recommend you to test the regular expressions before deploying them.
> - PII masking isn't applicable to PDF files, images, and web pages with editable content.

For more information, see Personal data masking in Citrix Secure Private Access product documentation.

Clipboard restriction for Security groups

Administrators can manage clipboard restrictions either through Global App Configuration service (GACS) or Secure Private Access or a combination of the two. This minimizes the risk of unauthorized data transfers and data leakage, making it an essential feature for organizations with stringent security requirements.

> **Note:**
>
> For more information on managing clipboard restrictions through Global App Configuration service (GACS), see Clipboard restriction

Restrict clipboard access through Secure Private Access When you manage the clipboard restriction through Secure Private Access, the restriction gets applied only to those apps'URLs that are added for restriction.

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

Clipboard restriction using Security groups To restrict clipboard access to specific apps that are configured in Citrix Secure Private Access™ and are opened in Citrix Enterprise Browser, administrators must create a Security groups and add those specific apps to it. This allows end users to copy and paste content only among the apps within that Security groups. For example, let's assume you create a Security groups adding the apps Wikipedia, Pinterest, and Dribble. So, when users open these apps from Citrix Workspace, they can copy and paste content only among these three apps.

To create a Security groups and add any designated group of apps, see Create Security groups in the Citrix Secure Private Access product documentation.

If administrators need to enable copy and paste content between Security groups' app and other local apps on their machines or unpublished apps, see Enable copy and paste between Security groups and other unpublished apps.

> **Note:**
>
> If administrators want to impose stricter restrictions on the specific apps within a Security groups, such as enabling or disabling copy and paste functionalities for a particular app within a Security groups, you can manage it by creating an access policy for that particular app. There are two access settings options, **Copy** and **Paste**, available inside an access policy rule security settings. For more information on this feature, see Enable granular level copy or paste in the Citrix Secure Private Access product documentation.

Enable copy and paste between Security groups and other unpublished apps Administrators can even allow end users to perform copy and paste functionalities between the apps in the Security groups and the other unpublished apps opened in the Enterprise browser, or with other native apps present within the system. To manage that, you can use the **Advanced clipboard settings** option in the Security groups. You can choose any of the following options to manage the settings as per your requirements.

Allow copying of data from the security group to unpublished domains: Enable copying of data from apps in the Security groups to websites that are not published in Secure Private Access.

Allow copying of data from the security group to native apps: Enable copying of data from the apps in the Security groups to local apps on the machine.

Allow copying of data from the unpublished domains to the security group: Enable copying of data from the apps not published through Secure Private Access to websites in the Security groups.

Allow copying of data from native apps operating system the security group: Enable copying of data from local apps on the machine to the apps in the Security groups.

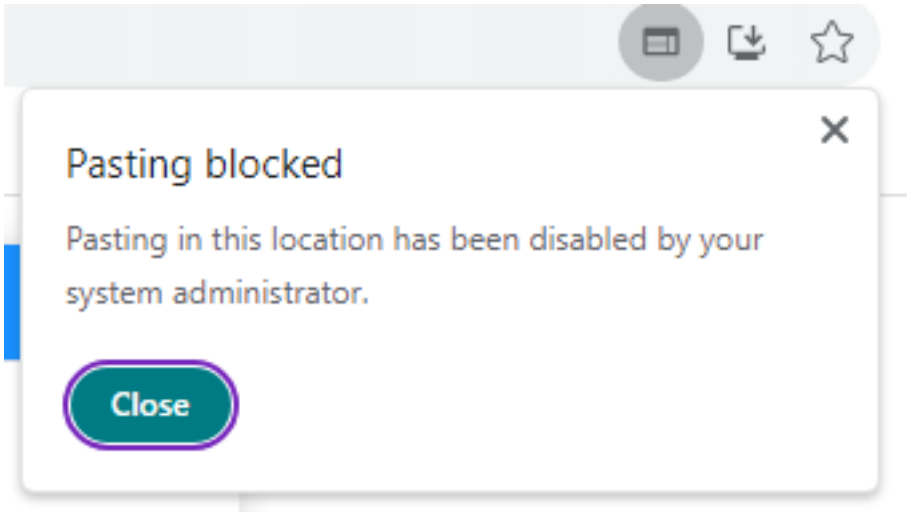
For more information, see the Advanced clipboard settings in the Citrix Secure Private Access product documentation.

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

> **Note:**
>
> - When you apply clipboard restriction through both GACS and Secure Private Access, the restriction applied through Secure Private Access takes precedence over GACS.
> - The individual restrictions such as **Copy**, **Paste**, and **Clipboard** supersede the **Clipboard restriction for Security groups**.

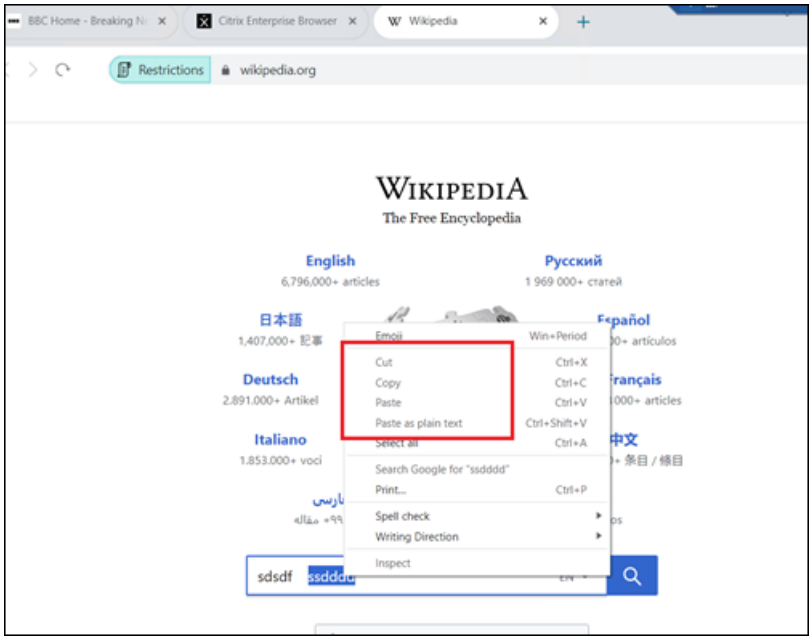
For more information, see Clipboard restriction for security groups in Citrix Secure Private Access product documentation.

End-user experience When the clipboard restrictions are enabled on any web pages, the following notification appears when users try to paste any contents to a restricted web page.



When the clipboard restriction is enabled, the **Cut**, **Copy** and **Paste** functionalities appear disabled on the right-click menu list. Alternatively, users have to use either keyboard shortcuts or access the **Cut**, **Copy and** Paste options from **More** (⊠) > **Find and edit**.

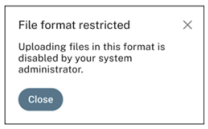
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Upload restriction by file type

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** policy allows you to enable or disable file uploads for specific MIME types.

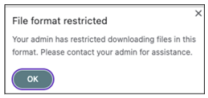
When an end user tries to upload a restricted file type, Citrix Enterprise Browser displays a warning message.



For more information on configuring this restriction, see Upload restriction by file type in Citrix Secure Private Access documentation.

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** policy allows you to enable or disable file downloads for specific MIME types.



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

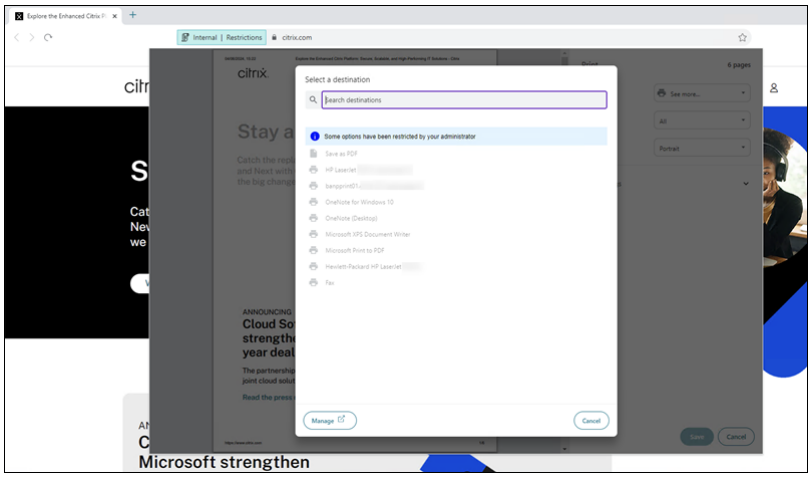
For more information on configuring this restriction, see Download restriction by file type in Citrix Secure Private Access documentation.

> **Note:**
>
> When both **Uploads** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the other. Similarly, when both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the other.

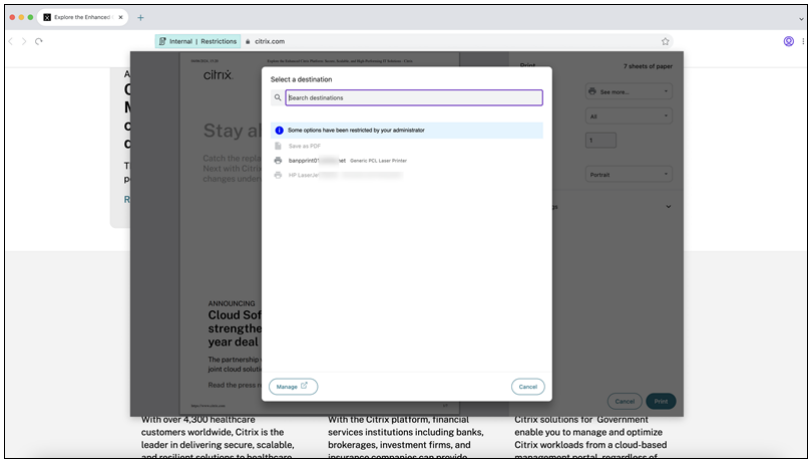
Printer management

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 print using the **Save as PDF** option.

In Windows:



In Mac:



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

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

- **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.

> **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.

For more information, see Printer management in Citrix Secure Private Access product documentation.

Browser restrictions through Secure Private Access for StoreFront™

September 6, 2025

You can now configure web and SaaS apps in StoreFront using the Secure Private Access solution. Once after you configure the apps, end users can open the web and SaaS apps using Citrix Enterprise Browser™ with enhanced security.

For more information on Secure Private Access support for StoreFront, see:

- Secure Private Access Overview in the Citrix Secure Private Access documentation.
- Deployment Guide: Citrix Secure Private Access On-Premises.

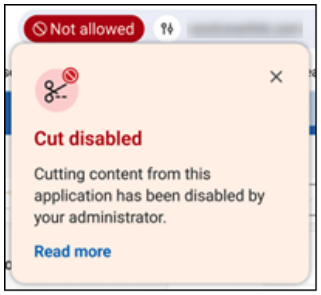
© 1997–2026 Citrix Systems, Inc. All rights reserved.

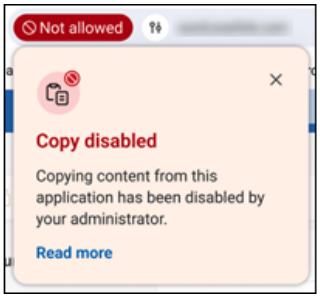
Restrict end user access on Citrix Enterprise Browser

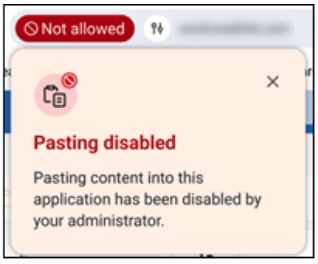
An administrator can apply the following access restrictions to Citrix Enterprise Browser for end users by using the Secure Private Access solution.

Restrict clipboard access

Disables cut, copy, and paste operations between the app and the endpoint's clipboard.



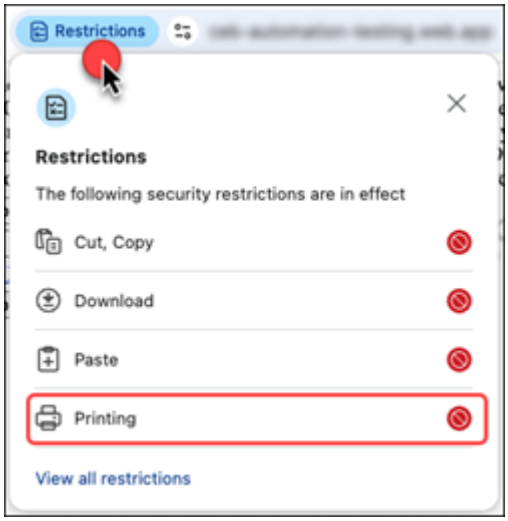




For more information, see Clipboard in Citrix Secure Private Access product documentation.

Restrict printing

Disables the ability to print from within the app.

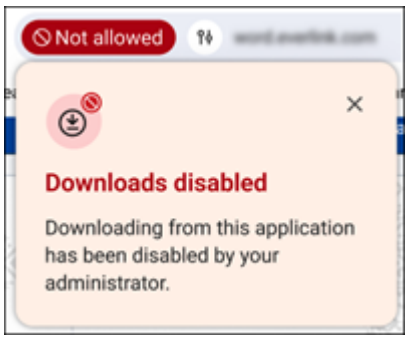


For more information, see Printing in Citrix Secure Private Access product documentation.

Restrict downloads

Disables the ability to download from within web and SaaS apps or copy files from the browser.

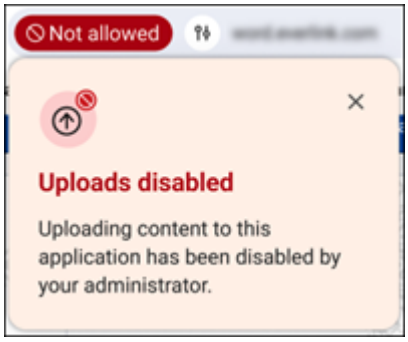
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see Downloads in Citrix Secure Private Access product documentation.

Restrict upload

Disables the ability to upload files.



> **Note:**
>
> The restrict upload feature is available on:
>
> - Windows 105.1.1.27 and later
> - Mac 105.1.1.36 and later

For more information, see Uploads in Citrix Secure Private Access product documentation.

Display watermark

Overlays a screen-based watermark that shows the user name and public IP address of the endpoint.

> **Note:**
>
> The **Restrict navigation** option isn't supported.

For more information, see Watermark in Citrix Secure Private Access product documentation.

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

App protection policies

Restrict keylogging Protects users from keyloggers.

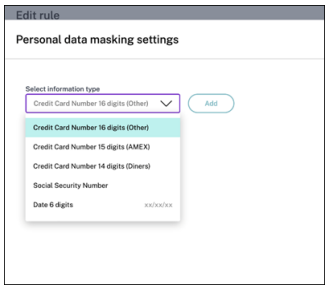
For more information, see Keylogging protection in Citrix Secure Private Access product documentation.

Restrict screen capturing Disables capturing screenshots or screen recording for the app that this policy is applied to. This policy is applied as long as a protected tab is visible (not minimized) in your browser window.

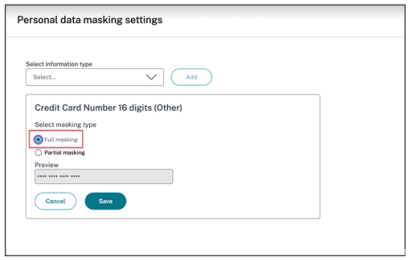
For more information, see Screen capture in Citrix Secure Private Access product documentation.

Personal data masking

Administrators can use the **Personal data masking** restriction to mask various types of Personal Identifiable Information (PII) such as credit card numbers, social security numbers, and dates. The masked contents remain secured even when copied or printed, ensuring comprehensive safeguarding of sensitive information.

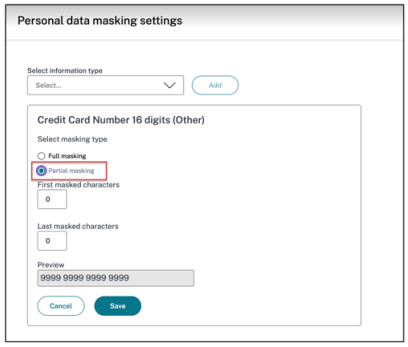


The **Personal data masking** restriction has the option to fully or partially mask the information. The **Full masking** option masks the information completely. The **Partial masking** option can be used to masks relevant areas of the information.



In the **Partial masking** option, administrators can choose how many characters to mask from the information, either from the beginning or the end. Respective text boxes are available to enter the character count.

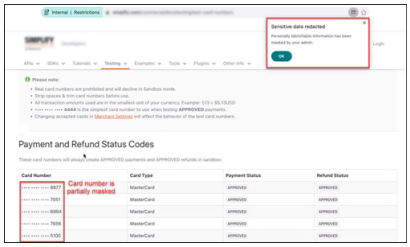
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Additionally, as an administrator, you have the flexibility to define the custom PII detection rules according to your requirements using regular expressions. This capability allows you to detect and mask specific information from the web page.

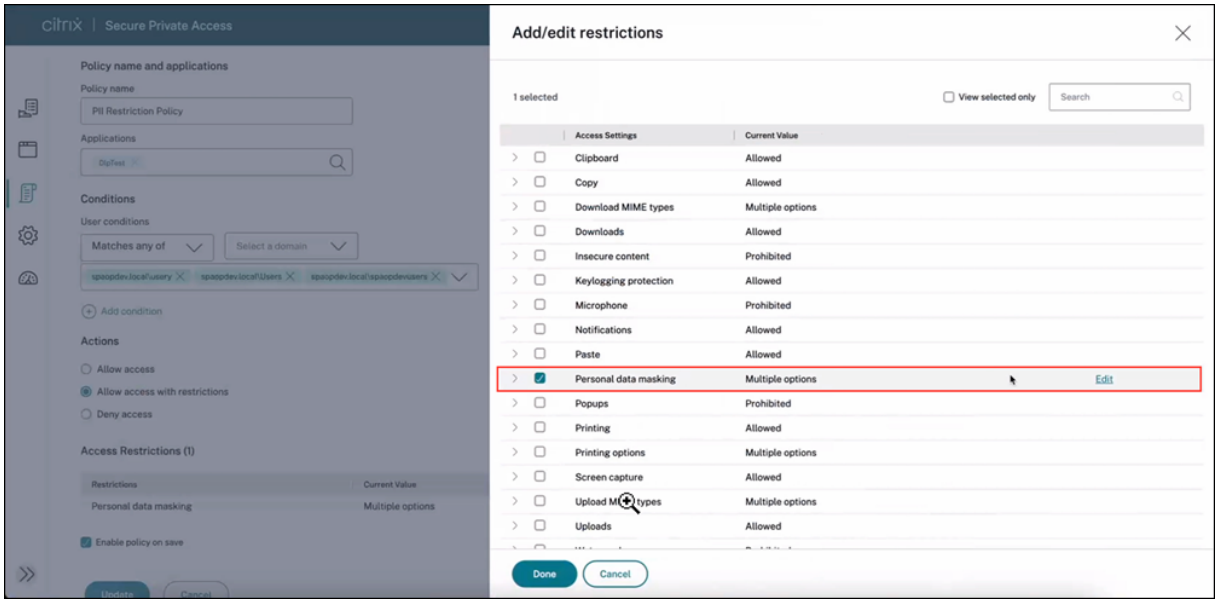
> **Note:**
>
> This feature supports only Regular expression 2 (RE2). For more information, see WhyRE2 and RE2 Syntax.

When you enable this restriction, Citrix Enterprise Browser detects the PII you choose to mask, then masks it, and displays a notification to end users.



Configuration To know more information about configuring this restriction, see Personal data masking in the Citrix Secure Private Access documentation.

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



> **Note:**
>
> - When defining PII detection rules, we recommend you to test the regular expressions before deploying them.
> - PII masking isn't applicable to PDF files, images, and web pages with editable content.

For more information, see Personal data masking in Citrix Secure Private Access product documentation.

Clipboard restriction for Security groups

Administrators can manage clipboard restrictions either through Global App Configuration service (GACS) or Secure Private Access or a combination of the two. This minimizes the risk of unauthorized data transfers and data leakage, making it an essential feature for organizations with stringent security requirements.

> **Note:**
>
> For more information on managing clipboard restrictions through Global App Configuration service (GACS), see Clipboard restriction

Restrict clipboard access through Secure Private Access When you manage the clipboard restriction through Secure Private Access, the restriction gets applied only to those apps'URLs that are added for restriction.

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

Clipboard restriction using Security groups To restrict clipboard access to specific apps that are configured in Citrix Secure Private Access™ and are opened in Citrix Enterprise Browser, administrators must create a Security groups and add those specific apps to it. This allows end users to copy and paste content only among the apps within that Security groups. For example, let's assume you create a Security groups adding the apps Wikipedia, Pinterest, and Dribble. So, when users open these apps from Citrix Workspace™, they can copy and paste content only among these three apps.

To create a Security groups and add any designated group of apps, see Create Security groups in the Citrix Secure Private Access product documentation.

If administrators need to enable copy and paste content between Security groups' app and other local apps on their machines or unpublished apps, see Enable copy and paste between Security groups and other unpublished apps.

> **Note:**
>
> If administrators want to impose stricter restrictions on the specific apps within a Security groups, such as enabling or disabling copy and paste functionalities for a particular app within a Security groups, you can manage it by creating an access policy for that particular app. There are two access settings options, **Copy** and **Paste**, available inside an access policy rule security settings. For more information on this feature, see Enable granular level copy or paste in the Citrix Secure Private Access product documentation.

Enable copy and paste between Security groups and other unpublished apps Administrators can even allow end users to perform copy and paste functionalities between the apps in the Security groups and the other unpublished apps opened in the Enterprise browser, or with other native apps present within the system. To manage that, you can use the **Advanced clipboard settings** option in the Security groups. You can choose any of the following options to manage the settings as per your requirements.

Allow copying of data from the security group to unpublished domains: Enable copying of data from apps in the Security groups to websites that are not published in Secure Private Access.

Allow copying of data from the security group to native apps: Enable copying of data from the apps in the Security groups to local apps on the machine.

Allow copying of data from the unpublished domains to the security group: Enable copying of data from the apps not published through Secure Private Access to websites in the Security groups.

Allow copying of data from native apps operating system the security group: Enable copying of data from local apps on the machine to the apps in the Security groups.

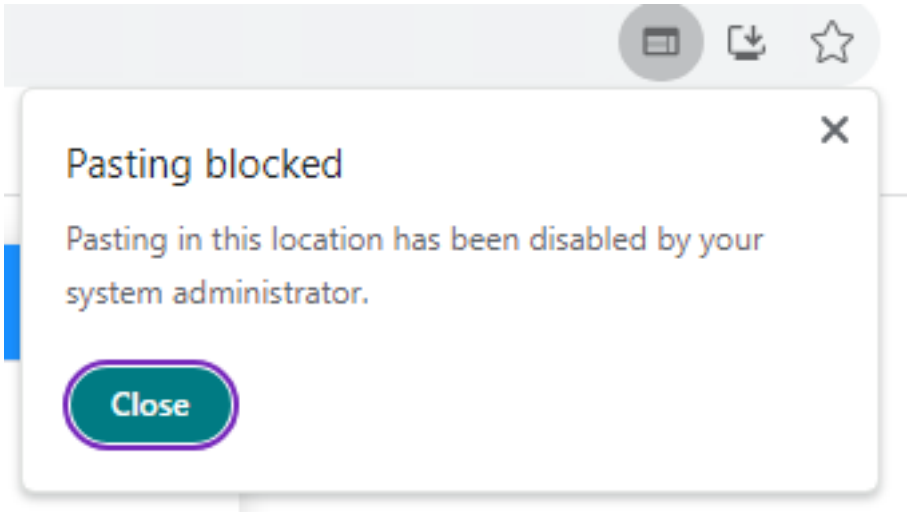
For more information, see the Advanced clipboard settings in the Citrix Secure Private Access product documentation.

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

> **Note:**
>
> - When you apply clipboard restriction through both GACS and Secure Private Access, the restriction applied through Secure Private Access takes precedence over GACS.
> - The individual restrictions such as **Copy**, **Paste**, and **Clipboard** supersede the **Clipboard restriction for Security groups**.

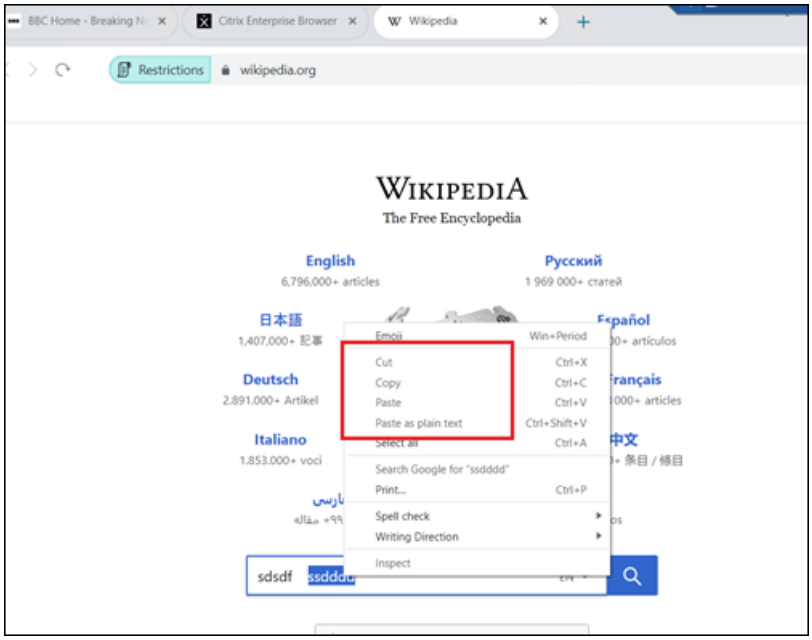
For more information, see Clipboard restriction for security groups in Citrix Secure Private Access product documentation.

End-user experience When the clipboard restrictions are enabled on any web pages, the following notification appears when users try to paste any contents to a restricted web page.



When the clipboard restriction is enabled, the **Cut**, **Copy** and **Paste** functionalities appear disabled on the right-click menu list. Alternatively, users have to use either keyboard shortcuts or access the **Cut**, **Copy and** Paste options from **More** (⊠) > **Find and edit**.

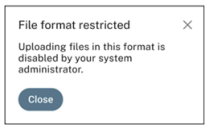
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Upload restriction by file type

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** policy allows you to enable or disable file uploads for specific MIME types.

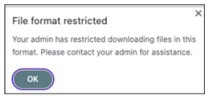
When an end user tries to upload a restricted file type, Citrix Enterprise Browser displays a warning message.



For more information on configuring this restriction, see Upload restriction by file type in Citrix Secure Private Access documentation.

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** policy allows you to enable or disable file downloads for specific MIME types.



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

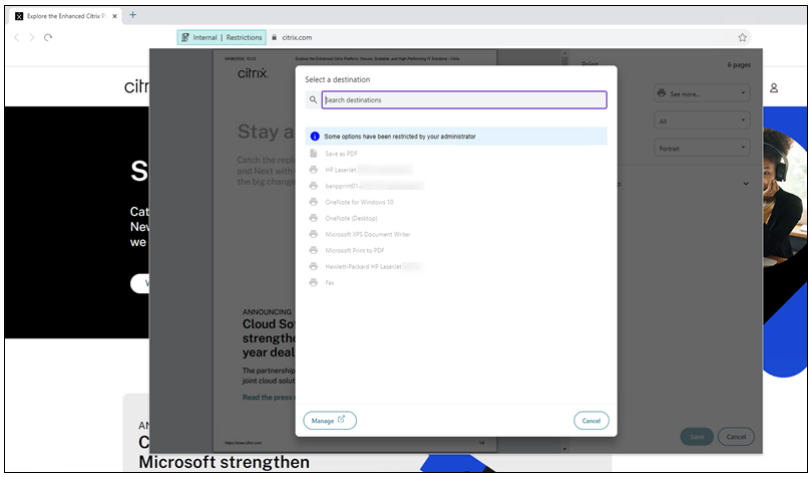
For more information on configuring this restriction, see Download restriction by file type in Citrix Secure Private Access documentation.

> **Note:**
>
> When both **Uploads** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the other. Similarly, when both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the other.

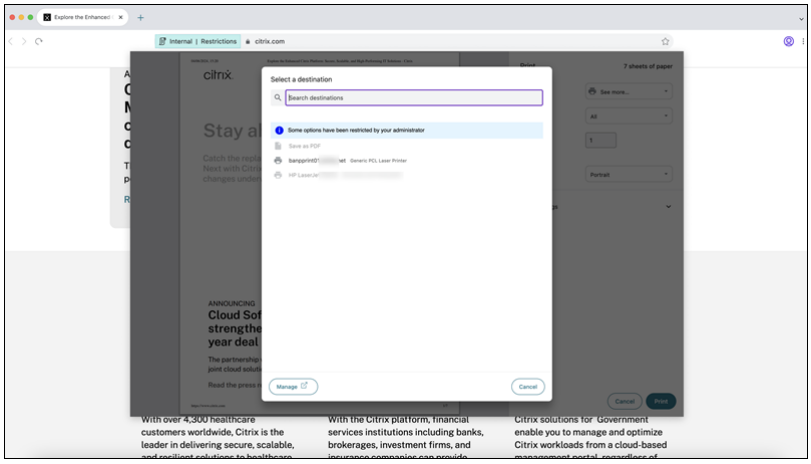
Printer management

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 print using the **Save as PDF** option.

In Windows:



In Mac:



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

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

- **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.

> **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.

For more information, see Printer management in Citrix Secure Private Access product documentation.

Manage Citrix Enterprise Browser™ through Global App Configuration service

September 6, 2025

Administrators can manage the following features using Global App Configuration service (GACS).

> **Note:**
>
> We recommend you to restart Citrix Workspace™ app when you modify the Citrix Enterprise Browser settings in GACS. However, you can also wait for the automatic refresh to complete. For more information on the sync duration of policies fetched from GACS, refer Frequency of

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

> settings update.

Use GACS to manage Citrix Enterprise Browser

The administrator can use Global App Configuration service (GACS) for Citrix Workspace to deliver the Citrix Enterprise Browser settings through a centrally managed service. GACS is designed for administrators to easily configure Citrix Workspace and manage the Citrix Workspace app settings. This feature allows admins to use the 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 Citrix Enterprise Browser 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 an 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.
- 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.
- 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.
- 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.

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

- 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.
- Disable the address bar of the Enterprise browser - Allows administrators to disable the address bar of the Enterprise Browser, restricting users to open only the pre-approved web and SaaS apps.
- Change user agent for Enterprise Browser - Allows administrators to modify the Enterprise Browser's user-agent for any internal web or SaaS apps.

> **Notes:**
>
> - The name and value pair are case-sensitive.
> - All the browser settings in GACS are under the following categories:

```
{

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

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

User interface

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

> **Note:**
>
> The minimum version that is required is:
>
> - Citrix Workspace app for Mac 2305, and the corresponding Citrix Enterprise Browser version is 112.1.1.23.
> - Citrix Workspace app for Windows 2305, and the corresponding Citrix Enterprise Browser

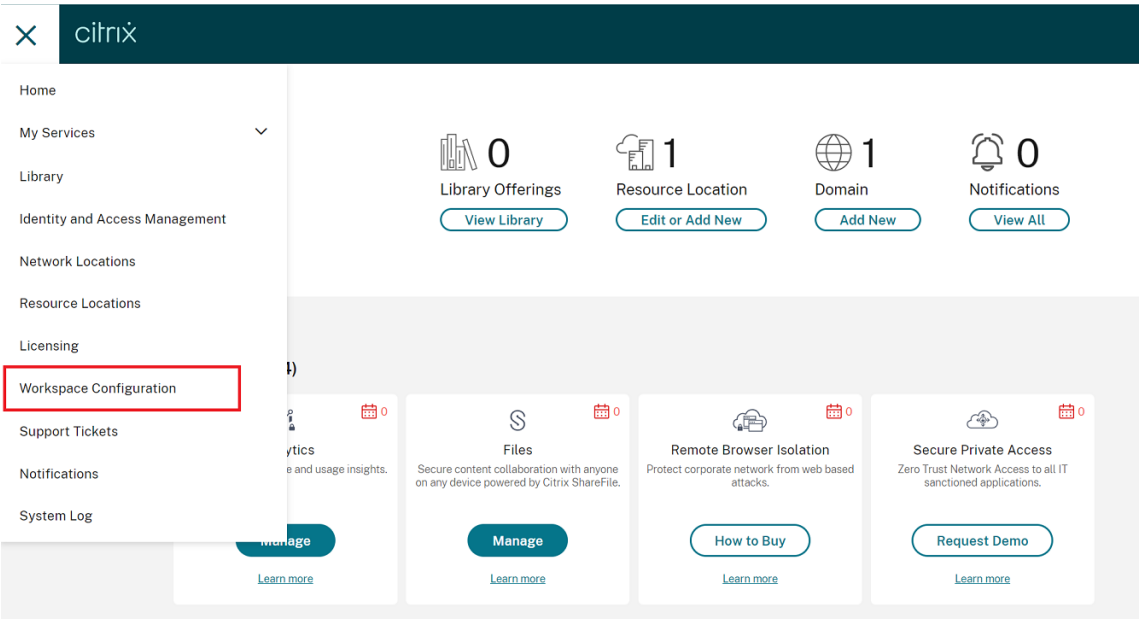
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> version is 112.1.1.24.

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**.



   The **Workspace Configuration** screen appears.

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

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

Enable Citrix Enterprise Browser for all apps

Administrators can configure Citrix Enterprise Browser as the default browser to start web and SaaS apps from the Citrix Workspace app.

Configuration through API

To configure, here is an example JSON file for **Citrix Enterprise Browser for all apps as default**:

```
"settings": [
                {
```

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

```
3
4                       "name": "open all apps in ceb",
5                       "value": "true"
6                     }
7
8                    ]
```

> **Note:**
>
> - The default value is **true**.

Configuration through UI

Select the appropriate checkbox from the UI:

Enable save passwords

Administrators can allow or deny the saving of user passwords.

Configuration through API

To configure, here is an example JSON file to **save passwords**:

```
1 "settings": [
2                   {
3
4                     "name": "enable password save",
5                     "value": "true"
6                   }
7
8                   ]
```

> **Note:**
>
> - The default value is **true**.

Configuration through UI

Select the appropriate checkbox from the UI:

Enable incognito mode

Administrators can enable or disable incognito mode.

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

Configuration through API

To configure, here is an example JSON file to **enable incognito mode**:

```
"settings": [
                  {

                   "name": "Incognito mode availability",
                   "value": "Incognito mode available"
                   }

                  ]
```

The other possible values are:

- Incognito mode available
- Incognito mode disabled

> **Note:**
>
> - The default value is **false**.

Configuration through UI

Select the appropriate checkbox from the UI, and then select an option from the drop-down list:

Manage bookmarks

Administrators can configure a list of bookmarks with a nested folder structure. The end user can access the preloaded bookmarks but can't modify them. For more settings, see the Global App Configuration service.

> **Note:**
>
> - By default, the Bookmarks bar isn't enabled in Citrix Enterprise Browser. The end user has to navigate to citrixbrowser://settings/appearance and enable the **Show bookmarks bar** option.

Configuration through API

To configure, here is an example JSON file to **manage bookmarks**:

```
        {

        "name": "Managed bookmarks",
```

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

```
        "value": [
             {

                "toplevel_name": "My managed bookmarks folder"
             }
,
            {

                "name": "Citrix",
                "url": "https://www.citrix.com/"
             }
,
            {

                "name": "Citrix Workspace app",
                "url": "https://www.citrix.com/products/receiver.html"
             }
,
            {

                "name": "Citrix Downloads",
                "children": [{

                        "name": "Download page",
                        "url": "https://www.citrix.com/downloads/
                           workspace-app/"
                     }
,
                    {

                        "name": "Product documentation",
                        "url": "https://docs.citrix.com/en-us/citrix-
                           workspace-app.html"
                     }

                ]
             }

        ]
    }
```

> **Note:**
>
> - The default value is an empty list.

Configuration through UI

Select the appropriate checkbox, and click **Manage Settings**. You can configure using the JSON data and save the changes.

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

Enable developer tools

Administrators can enable or disable developer mode.

> **Warning:**
>
> If the **Developer Tools** option is enabled for end users, they can bypass all restriction policies applied to Citrix Enterprise Browser.
>
> Therefore, we recommend that administrators enable **Developer Tools** for selected users only if they need it for debugging purposes.

Configuration through API

To configure, here is an example JSON file to **enable developer tools**:

```
"settings": [
                  {

        "name": "developer tools availability",
        "value": "Allow usage of the Developer Tools"
                  }

                 ]
```

Other possible values:

- Disallow usage of the Developer Tools on extensions installed by enterprise policy
- Disallow usage of the Developer Tools

> **Note:**
>
> - The default value is **Disallow usage of the Developer Tools**.

Configuration through UI

Select the appropriate checkbox from the UI, and then select an option from the drop-down list:

Delete browsing data on exit

Administrators can configure what data the Citrix Enterprise Browser deletes on exit.

Configuration through API

To configure, here is an example JSON file to **delete browsing data** upon exit:

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

```
"settings": [{

        "name": "Delete browsing data on exit",
        "value": [
            "browsing_history",
            "download_history",
            "cookies_and_other_site_data",
            "cached_images_and_files",
            "password_signin",
            "autofill",
            "site_settings",
            "hosted_app_data"
        ]
        }
]
```

> **Notes:**
>
> - You can exclude a value to avoid being deleted.
> - The default value is an empty list.

Configuration through UI

Select the appropriate checkbox from the UI, and then select an option from the drop-down list:

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 the Global App Configuration service.

For more information on how to identify an extension ID, see the How to identify an extension ID article.

How to configure

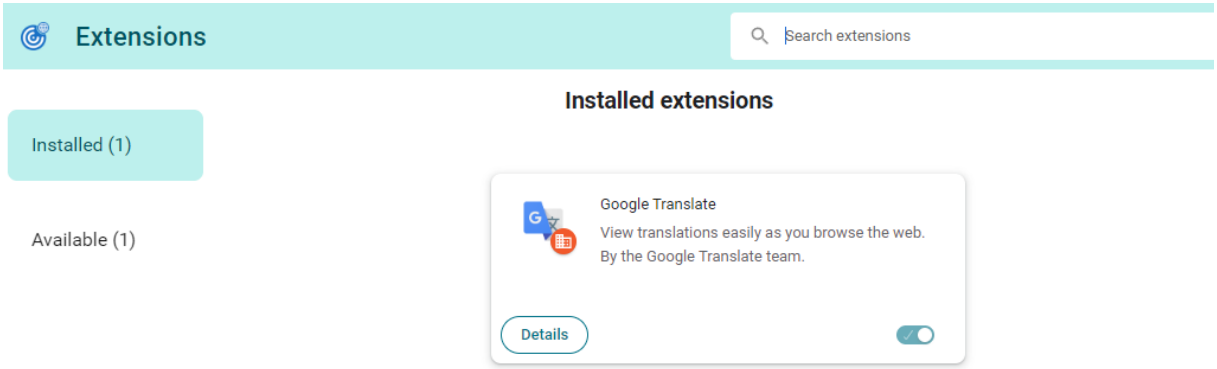
There are two categories of extensions:

- **ExtensionInstallForcelist**: The administrator can configure a list of extensions that are mandatorily added to the end user's browser profile. End users can view these extensions under the **Installed** section in the UI. The user can't uninstall any of the extensions.
- **ExtensionInstallAllowlist**: The administrator can configure a list of extensions as part of the allowed list. End users can view these extensions under the **Available** section in the UI. Users

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

can decide if they want to add a particular extension or not. Users can uninstall an extension if necessary.

> **Note:**
>
> - In case the administrator has no extensions configured under the **Installed** and **Available** sections, the end user might not view the extension manager icon in the address bar.



Mandatory extension

The administrator can configure the list of mandatory extensions in one of the following ways:

Configuration through API To configure, here is an example JSON file for **ExtensionInstallForcelist**:

```
{

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

        "name": "Extension Install Force list",
        "value": [
            "extension_id1",
```

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

```
14              "extension_id2"
15                       ]
16                        }
17
18                       ]
19  }
```

> **Note:**
>
> - The default value is an empty list.

Configuration through UI Select the appropriate checkbox from the UI, and then click **Manage settings**. You can configure using the JSON data and save the changes.

Mandatory custom extension

The administrator can configure the custom extensions as part of the mandatory list in one of the following ways:

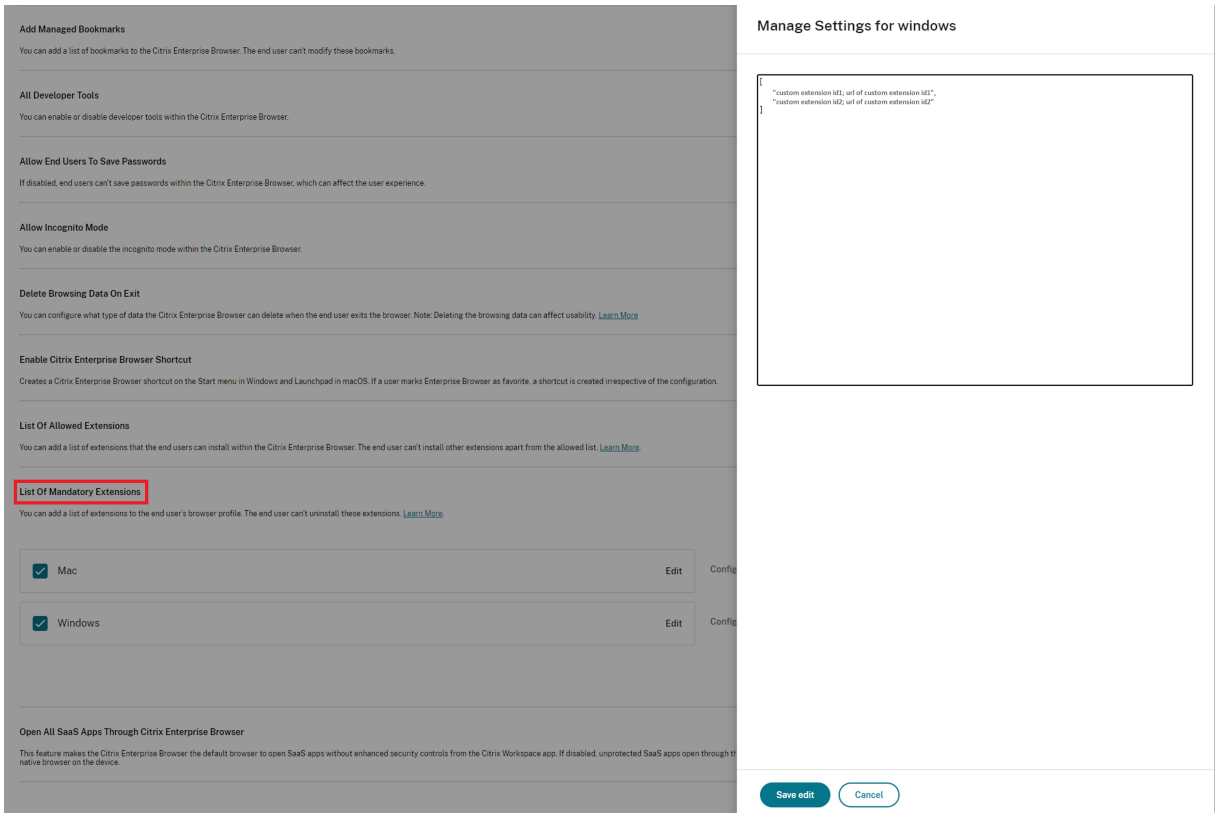
Configuration through API To configure, here is an example JSON file for **ExtensionInstallForcelist**:

```
1  {
2
3  "category": "browser",
4  "userOverride": false,
5  "assignedTo": [
6  "AllUsersNoAuthentication"
7                ],
8  "settings": [
9                      {
10
11      "name": "Extension Install Force list",
12      "value": [
13             "custom extension id1; url of custom extension id1",
14             "custom extension id2; url of custom extension id2"
15                         ]
16                          }
17
18                         ]
19  }
```

> **Note:**
>
> The default value is an empty list.

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

Configuration through UI Select the appropriate checkbox from the UI, and then click **Manage** settings. You can configure using the JSON data and save the changes.



Allowed extensions

The administrator can configure the list of allowed extensions in one of the following ways:

Configuration through API To configure, here is an example JSON file for **ExtensionInstallAllowlist**:

```
{

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

        "name": "Extension Install Allow list",
        "value": [
            {

```

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

```
                "id" : "extension_id1",
                "name" : "Name of extension",
                 "install link" : "chrome store url for the extension"
               }
,
              {

                "id" : "extension_id2",
                "name" : "Name of the extension",
                 "install link" : "chrome store url for the extension"
               }

          ]
      }

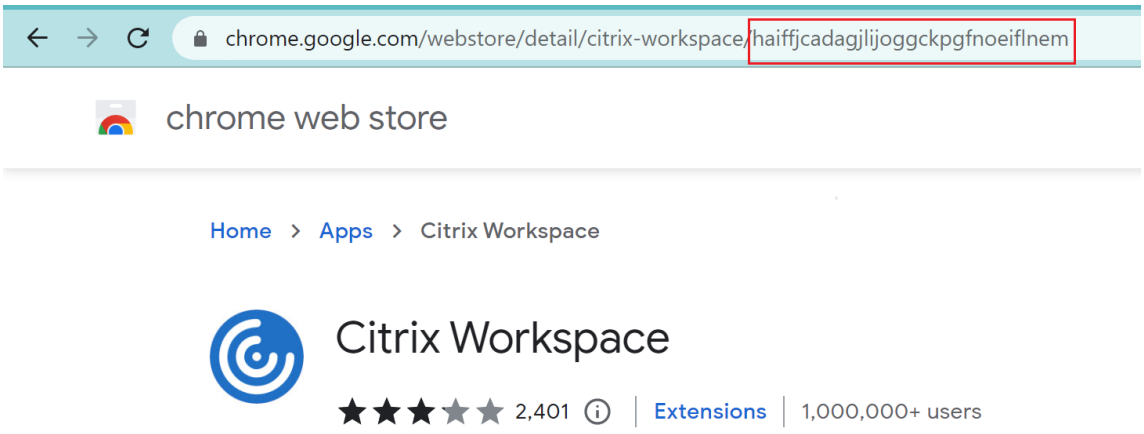
   ]
}
```

> **Note:**
>
> - The default value is an empty list.

Configuration through UI Select the appropriate checkbox from the UI, and then click **Manage settings**. You can configure using the JSON data and save the changes.

How to identify an extension ID

1. Go to the Chrome Web Store.
2. Search for an app and click to open.
   The app page appears.
3. Observe the URL. The ID is the long string of characters at the end of the URL.



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

Enable autofill address

When you enable the autofill address setting, Autofill suggests or fills in address information.

Configuration through API

To configure, here's an example JSON file to enable autofill address. Setting the value to 'true' autofills the address, whereas 'false' disables it.

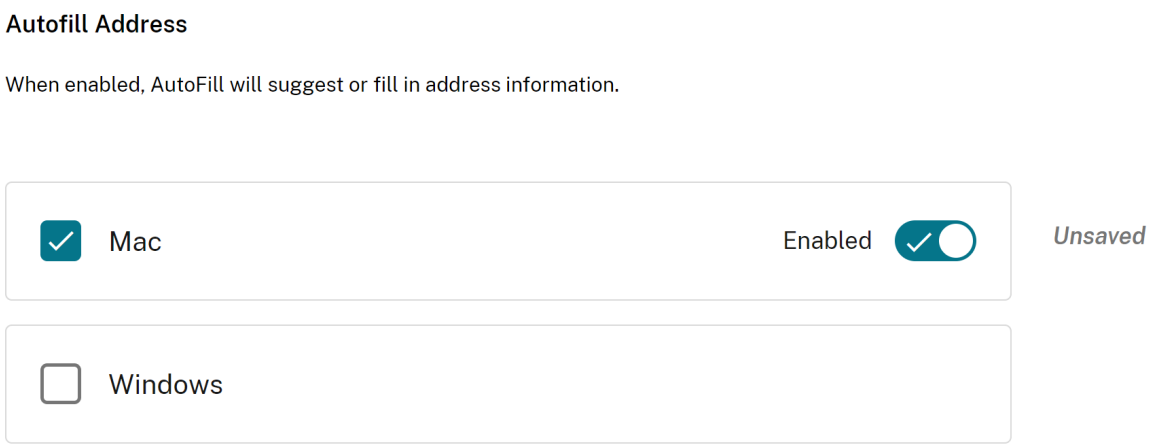
```
"settings": [{

        "name": "auto fill address enabled",
        "value": true
    }
]
```

> **Note:**
>
> The default value is **true**.

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Enable autofill credit card

When you enable the autofill credit card setting, autofill suggests or fills in credit card information.

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

Configuration through API

To configure, here's an example JSON file to enable autofill credit card. Setting the value to 'true' autofills the credit card details, whereas 'false'disables it.

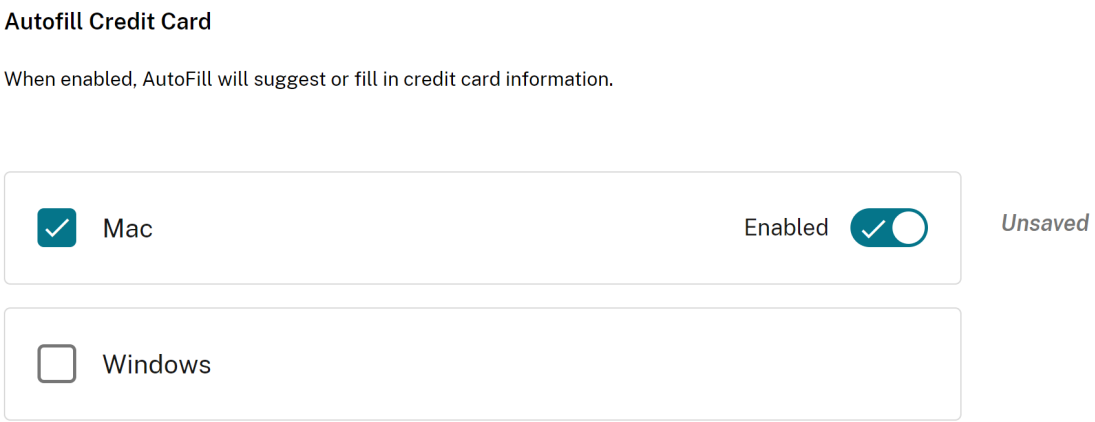
```
"settings": [{

    "name": "auto fill credit card enabled",
    "value": true
  }
]
```

> **Note:**
>
> The default value is **true**.

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click ***Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Auto launch protocols from origins

This setting allows you to launch an external app without prompting the user for authentication. For that, add a protocol that can launch an external app and list the URLs of external apps.

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

Configuration through API

To configure, here's an example JSON file to enable this setting:

```
"settings": [{

     "name": "auto launch protocols from origins",
     "value": [
       {

         "protocol": "teams",
         "allowed_origins": [
           "example.com",
           "http://www.example.com:8080"
         ]
        }

     ]
    }

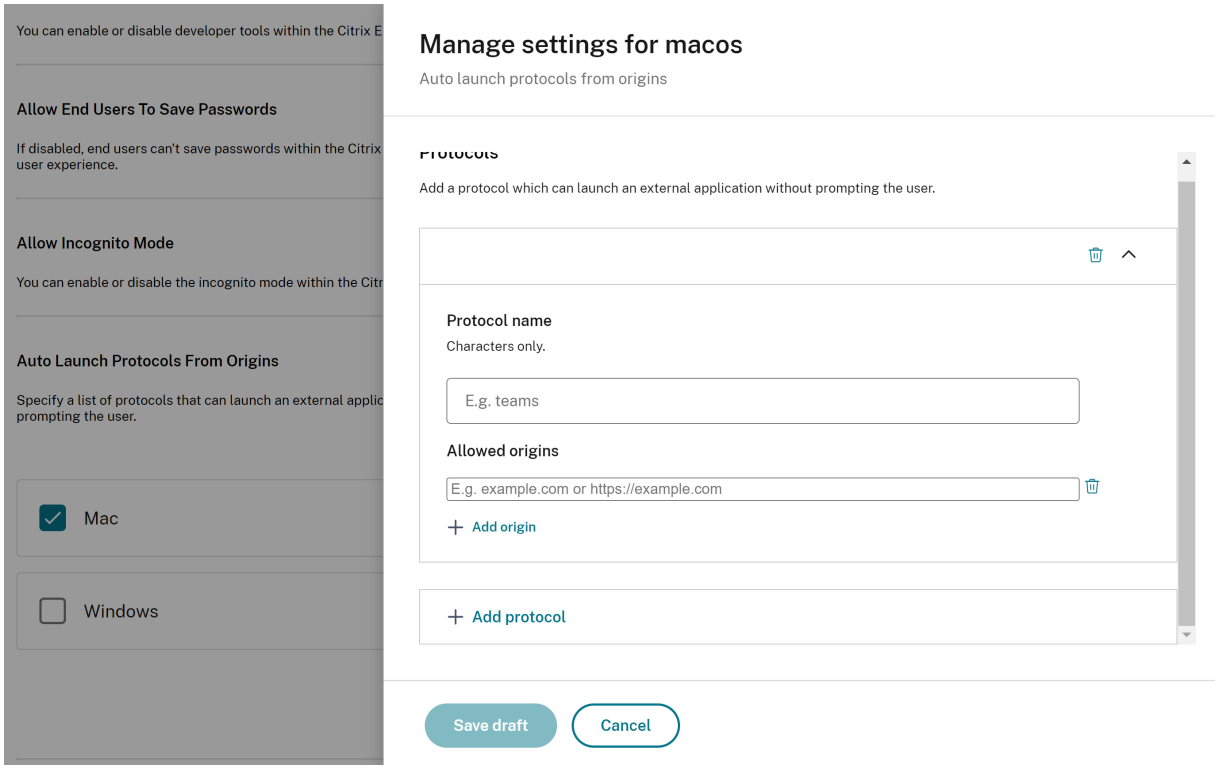
 ]
```

> **Note:**
>
> There's no default value.

Configuration through UI

1. Select the appropriate operating system under the **Auto Launch Protocols From Origins** section.
2. Click **Edit**.
3. On the **Manage setting** screen, enter the protocol name and allowed origins.
4. Click **Save draft**.
5. On the **Save Settings** window, click **Yes** to save the settings.

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



Enable command-line flag security warnings

You can enable this setting to display security warnings when potentially dangerous command-line flags are used to launch the browser.

Configuration through API

To configure, here's an example JSON file to enable command-line flag security warnings. Setting the value to 'true'enables the setting, whereas 'false'disables it.

```
"settings": [{

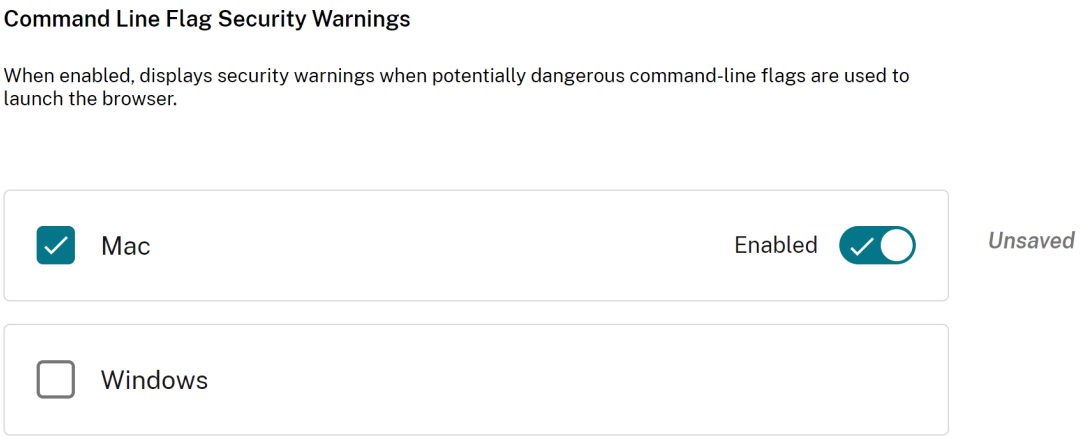
        "name": "command line flag security warnings enabled",
        "value": true
    }
 ]
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.

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

4. Click **Yes** to save the changes for your end users.



Manage default cookies setting

You can enable the default cookies setting to manage how websites can store local data and cookies. Depending on your preference, you can set any of the following options:

- **Allow all sites to set local data:** This is the default setting and allows any website to store cookies and other data on your device without restriction.
- **Do not allow any site to set local data:** This setting blocks all websites from storing any cookies and local data on your device.
- **Keep cookies for the duration of the session:** This setting allows websites to store cookies while you're browsing, but deletes them once you close your browser.

Configuration through API

To configure, here's an example JSON file to enable **Default Cookies**.

```
"settings": [{

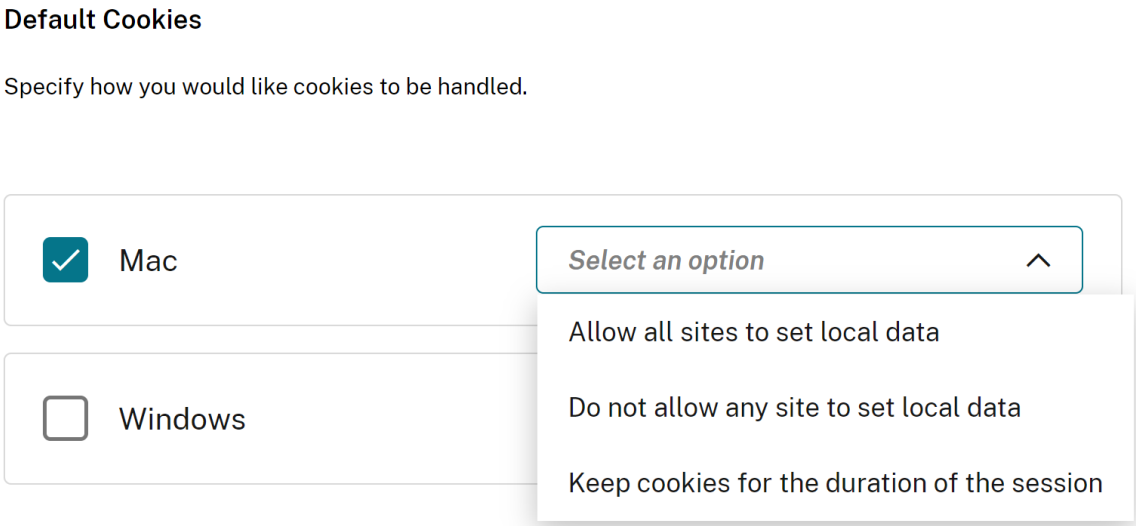
        "name": "default cookies setting",
        "value": "Allow all sites to set local data"
    }
 ]
```

Configuration through UI

1. Select the appropriate operating system.
2. Select an option from the drop-down list.

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

3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage default pop-ups setting

You can enable the default pop-up setting to manage pop-ups from a website. Depending on your preference, you can set any of the following options:

- **Allow all sites to show pop-ups:** This is the default setting where all websites can display pop-ups.
- **BlockPopups applies, but users can change this setting:** No websites can display pop-ups. However, users can manage this setting as per their preference.
- **Do not allow any site to show pop-ups:** This setting blocks pop up from all websites.

Configuration through API

To configure, here's an example JSON file to manage the default pop-up settings.

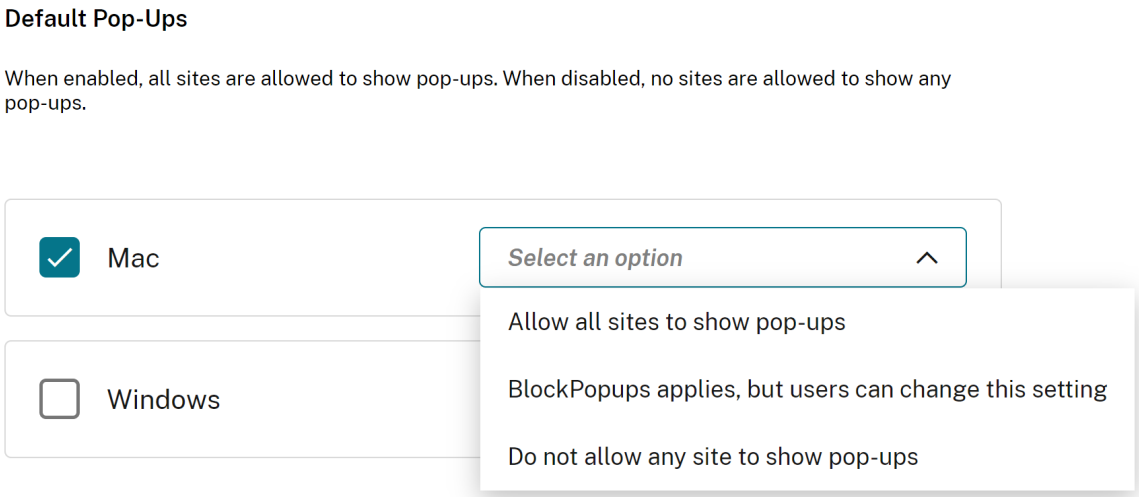
```
"settings": [{

      "name": "default popups setting",
      "value": "Allow all sites to show pop-ups"
   }
 ]
```

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

Configuration through UI

1. Select the appropriate operating system.
2. Select an option from the drop-down list.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Extension install sources

You can specify the source URLs from which users can install extensions, apps, and themes to the browser.

Configuration through API

To configure, here's an example JSON file to manage this setting.

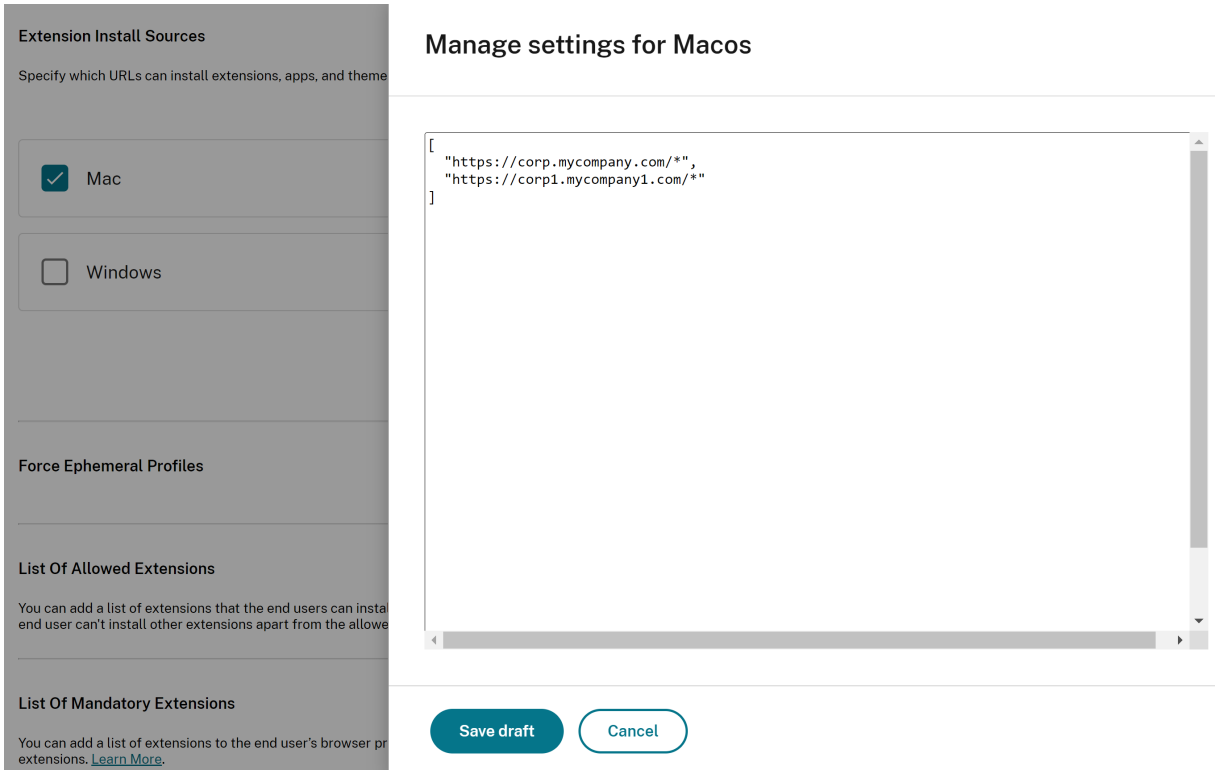
```
"settings": [{

      "name": "extension install sources",
      "value": [
          "https://corp.mycompany.com/*"
          "https://corp1.mycompany1.com/*"
        ]
   }
 ]
```

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

Configuration through UI

1. Select the appropriate operating system under the **Extension Install Sources** section.
2. Click **Edit**.
3. On the **Manage setting** screen, enter the list of source URLs.
4. Click **Save draft**.
5. On the **Save Settings** window, click **Yes** to save the settings.



Disable lookalike warning pages

This setting allows you to prevent the display of lookalike URL warnings. If you enable the setting and specify one or more domains, no lookalike warning pages show when a user visits pages on that domain.

Configuration through API

To configure, here's an example JSON file to enable this setting.

```
"settings": [{

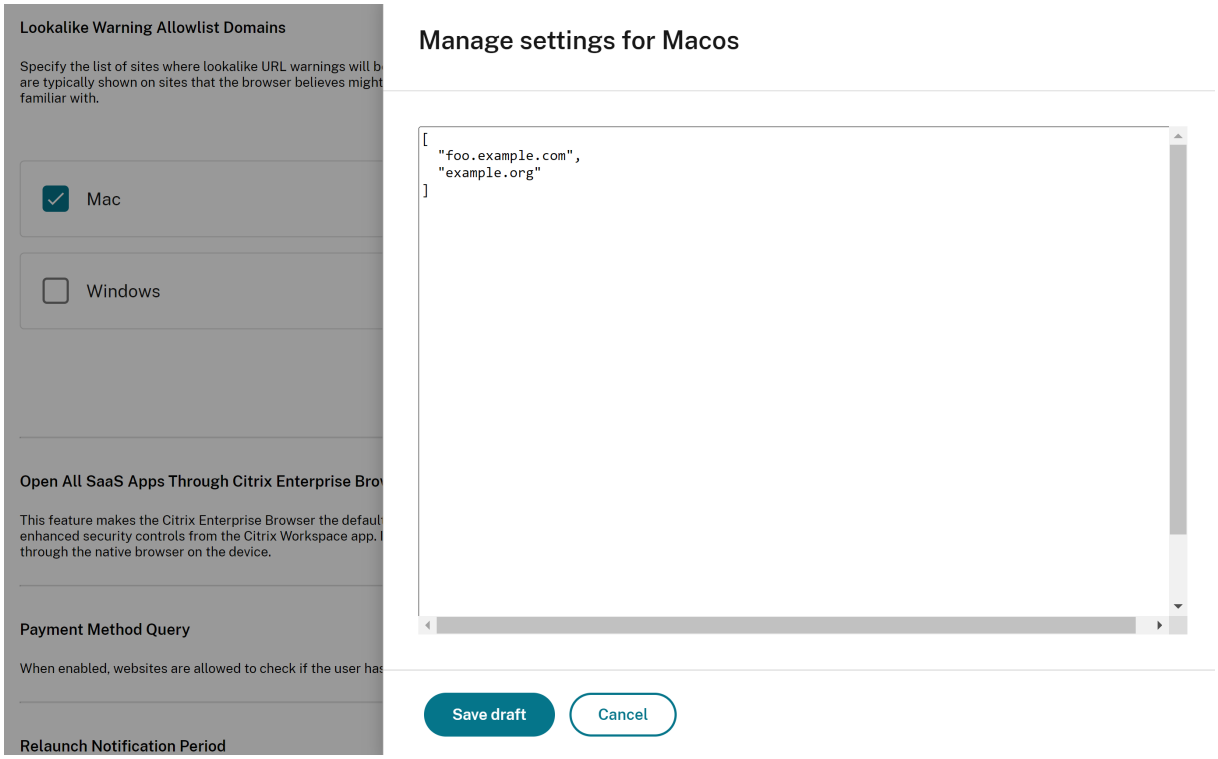
      "name": "look alike warning allowlist domains",
      "value": [
```

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

```
            "foo.example.com",
            "example.org"
            ]
        }
]
```

Configuration through UI

1. Select the appropriate operating system under the **Lookalike Warning Allowlist Domains** section.
2. Click **Edit**.
3. On the **Manage setting** screen, enter the list of domains.
4. Click **Save draft**.
5. On the **Save Settings** window, click **Yes** to save the settings.



Enable payment method query

When you enable this setting, it allows websites to check if users have saved payment methods.

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

Configuration through API

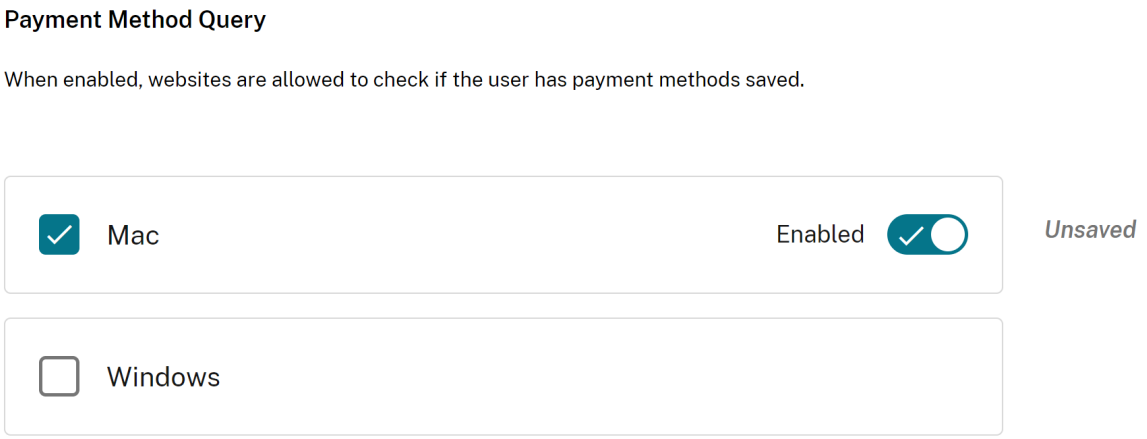
To configure, here's an example JSON file to enable payment method query. Setting the value to 'true' enables this setting whereas 'false'disables it.

```
"settings": [{

      "name": "payment method query enabled",
      "value": true
   }
 ]
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage saving browser history

You can use this setting if you want to manage the saving of the browsing history.

Configuration through API

To configure, here's an example JSON file to manage the saving of browser history. Setting the value to 'true'doesn't save the browsing history. The value 'false'saves the browsing history.

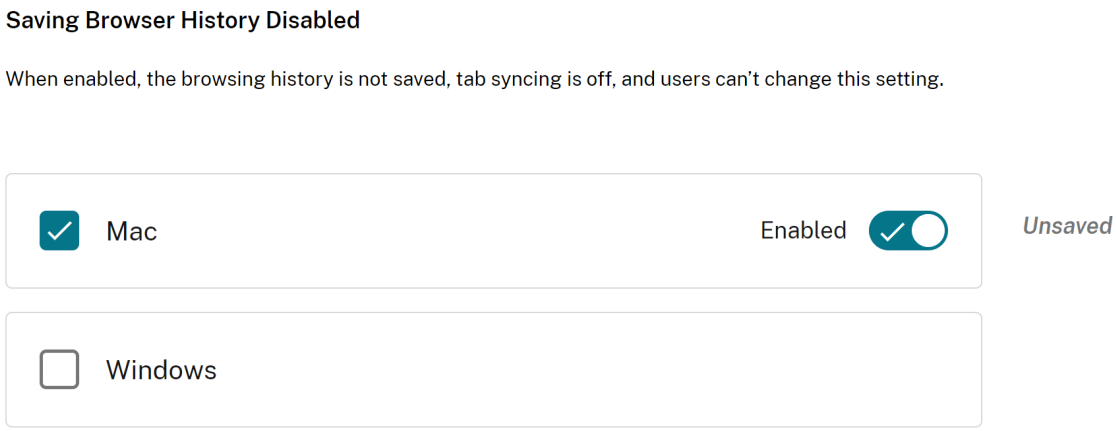
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"settings": [{

      "name": "saving browser history disabled",
      "value": true
   }
 ]
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage search suggestion

You can enable this setting if you want to turn on search suggestions in the browser's address bar.

The suggestions based on the bookmarks and browser history are unaffected by this setting.

Configuration through API

To configure, here's an example JSON file to enable the search suggestions. Set the value to 'true'to turn on the search suggestions. The value 'false'turns off the search suggestions.

```
"settings": [{

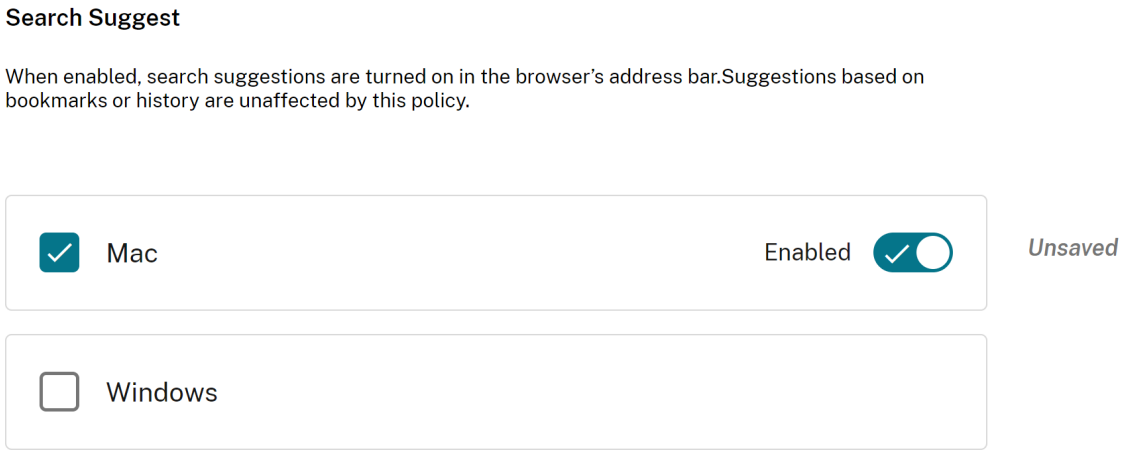
      "name": "search suggest enabled",
      "value": true
```

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

```
    }
]
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Enable export bookmark

When you enable this setting, users can see the option to export the browser's bookmark.

Configuration through API

To configure, here's an example JSON file to manage the exporting of browser bookmarks. Set the value to 'true'to enable the option to export the browser's bookmark. The value 'false'disables the option.

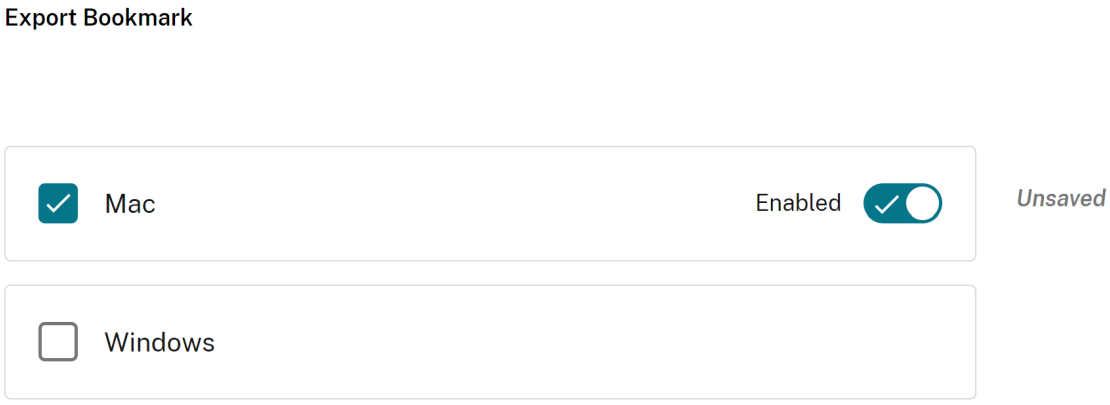
```
"settings": [{

      "name": "export bookmark allowed",
      "value": true
  }
]
```

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

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Force ephemeral profiles

When you enable this setting, it creates an ephemeral profile when users sign in to the Enterprise Browser. Ephemeral profile erases user profile data on disk when a user ends the browsing session. Users can still download files, save pages, or print them.

Configuration through API

To configure, here's an example JSON file to enable or disable the creation of ephemeral profiles. Set the value to 'true'to enable the setting that creates an ephemeral profile, which erases the profile data on disk when the user closes the browser. When you set the value to 'false', the profile data remains on the disk even after users end the browsing session.

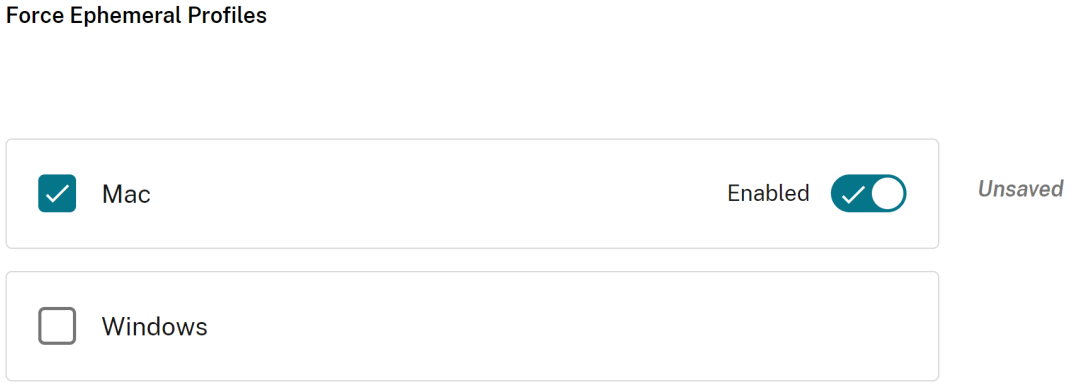
```
"settings": [{

      "name": "force ephemeral profiles",
      "value": true
   }
 ]
```

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

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



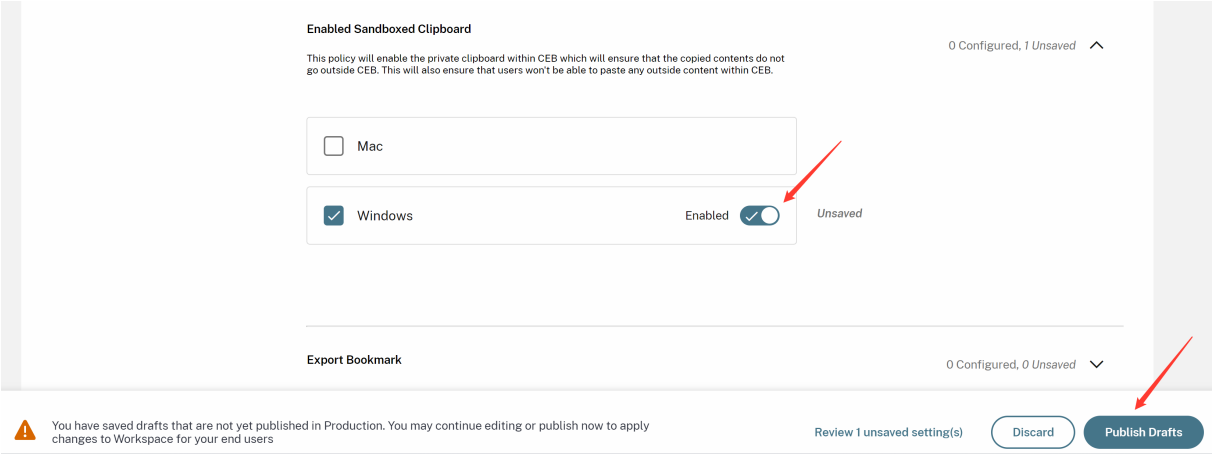
Clipboard restriction

When you manage clipboard restriction through GACS, it applies to all web pages accessed via the Citrix Enterprise Browser. Once you enable the setting, end users are unable to copy and paste contents from any web page displayed within the Citrix Enterprise Browser to any other native apps present within their system, and vice versa.

To manage the clipboard restriction, perform the following steps:

1. Navigate to **Workspace Configuration** > **App Configuration** > **Enterprise Browser** > **Security and Privacy**.
2. Select the appropriate operating system under the **Enabled Sandboxed Clipboard** section.
3. Enable or disable the toggle button as per your requirement.
4. Click **Publish Drafts**.
5. Click **Save** to save the changes for your end users.

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



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.

You can manage audio capture access using the following options:

Enable audio input: Prompt users to allow audio capture access.

Disable audio input: Prompt is turned off, and audio capture is blocked.

Unset audio input: Prompt users to allow audio capture access.

The default value is **Unset audio input**.

Configuration through API

To configure, here's an example JSON file to manage the audio capture access.

```
"settings": [{

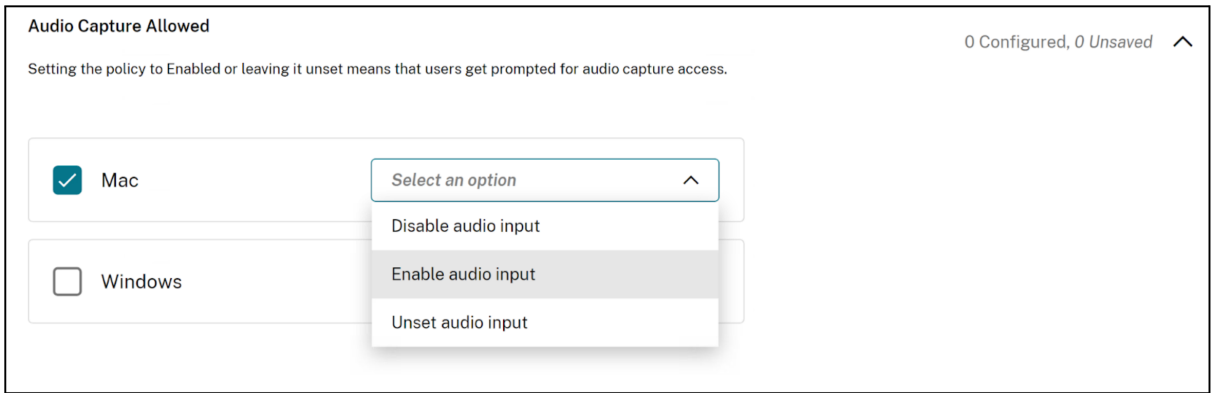
      "name": "audio capture allowed",
      "value": "Enable audio input"
   }
 ]
```

Configuration through UI

1. Select the appropriate operating system.
2. Select an option from the drop-down list.
3. Click **Publish Drafts**.

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

4. Click **Yes** to save the changes for your end users.



> **Note:**
>
> This setting applies to the built-in microphone as well as all other audio input devices.

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.

You can manage video capture access using the following options:

Enable video input: Prompt users to allow video capture access.

Disable video input: Prompt is turned off, and video capture is blocked.

Unset video input: Prompt users to allow video capture access.

The default value is **Unset video input**.

Configuration through API

To configure, here's an example JSON file to manage the video capture access.

```
"settings": [{

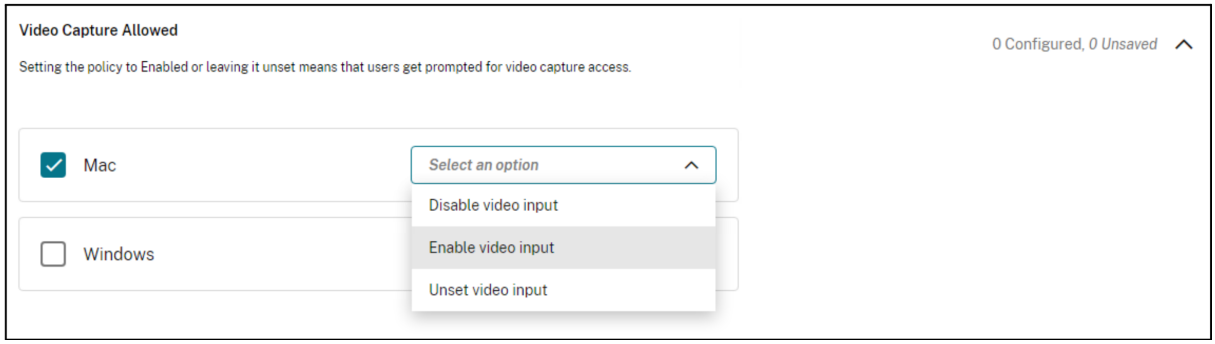
      "name": "video capture allowed",
      "value": "Enable video input"
   }
 ]
```

Configuration through UI

1. Select the appropriate operating system.

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

2. Select an option from the drop-down list.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



> **Note:**
>
> This setting applies to the built-in camera as well as all other video input devices.

Address bar

Administrators can disable the address bar of the Enterprise Browser through Global App Configuration service (GACS). The feature can be managed using one of the following ways:

Configuration through API

Here is an example JSON file for the configuration:

```
"settings": [{

      "name": "address bar",
      "value": "true"
   }
 ]
```

Set the value to **true**, which enables the address bar and makes it editable.

Set the value to **false**, which disables the address bar and keeps it read-only.

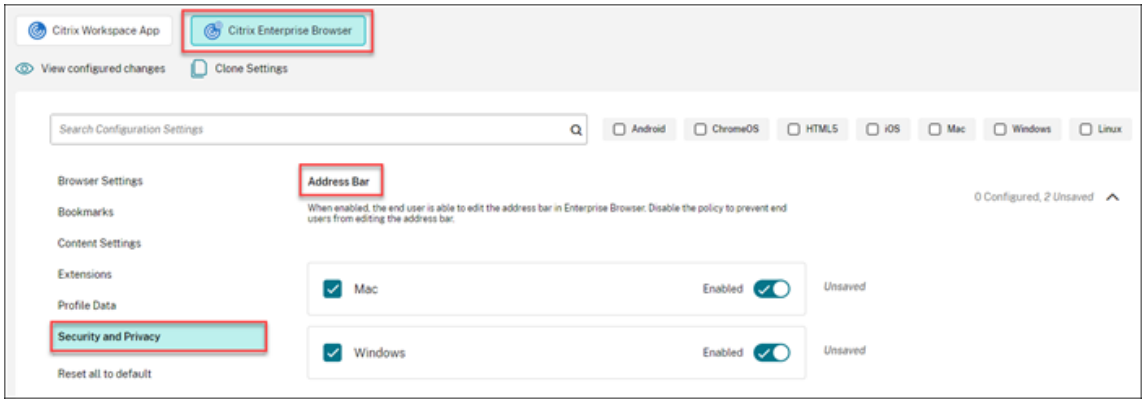
> **Note:**
>
> This policy is unset by default, which indicates that the address bar is enabled and editable.

Configuration through UI

1. Navigate to **Workspace Configuration** > **App Configuration** in Citrix Cloud.

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

2. Select the desired store from the given store list and click **Configure**.
3. Select **Citrix Enterprise Browser**.
4. Select **Security and Privacy**.
5. Under the **Address Bar** setting, select the appropriate operating system and toggle the button to enable or disable the feature.



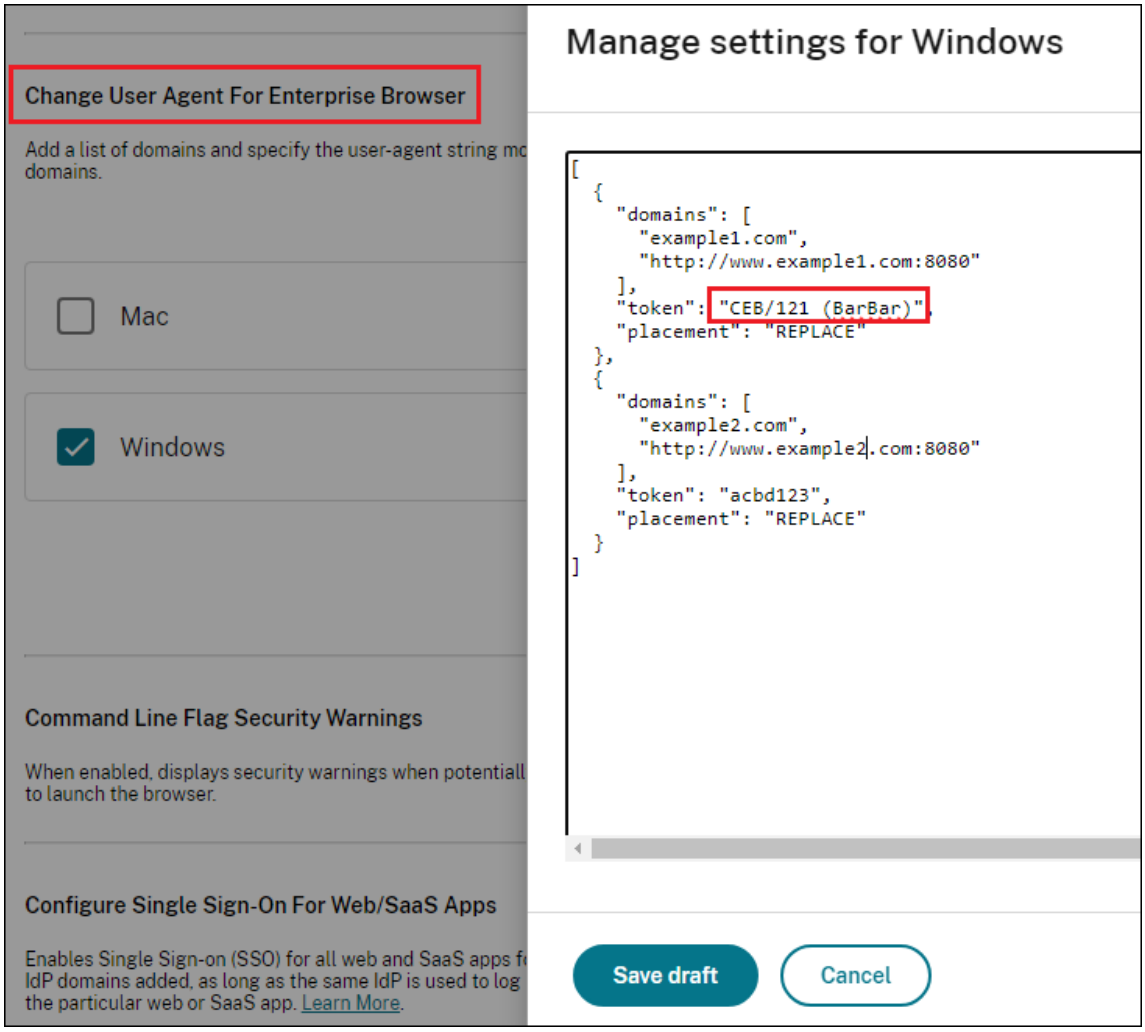
6. Click **Publish Drafts**, and then click **Save** to save the changes.

> **Note:**
>
> The address bar is enabled by default on user devices, allowing users to access and edit it.

Change user agent for Enterprise Browser

1. Navigate to **Workspace Configuration** > **App Configuration** > **Enterprise Browser** > **Security and Privacy**.
2. Select the appropriate operating system under **Change user agent For Enterprise Browser** section.
3. Click **Edit**.

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



4. On the **Manage settings** page, add the list of domains and the user-agent string using the provided JSON file example.

   > **Note:**
   >
   > - We recommend that you follow the user-agent format documented in User-Agent.
   > - The placement option **REPLACE** completely replaces the user-agent with the security token.

5. Click **Save draft**.
6. On the **Save Settings** window, click **Yes** to save the settings.

Example JSON data

The following is an example JSON file:

```
1 {
```

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

```
{

  "serviceURL": {

    "url": "https://example.cloudburrito.com:443"
   }
,
  "settings": {

    "name": "example name",
    "description": "example description",
    "useForAppConfig": true,
    "appSettings": {

      "macos": [
        {

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

              "name": "open all apps in cwb",
              "value": true
             }
,
            {

              "name": "incognito mode availability",
              "value": "Incognito mode available"
             }
,
            {

              "name": "developer tools availability",
              "value": "Allow usage of the Developer Tools"
             }
,
            {

              "name": "enable password save",
              "value": true
             }
,
            {

              "name": "Delete browsing data on exit",
              "value": [
                "browsing_history",
                "download_history"
              ]
```

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

```
55                }
56   ,
57              {
58
59                "name": "Managed bookmarks",
60                "value": [
61                  {
62
63                    "toplevel_name": "My managed bookmarks folder"
64                   }
65   ,
66                  {
67
68                    "name": "Google",
69                    "url": "google.com"
70                   }
71   ,
72                  {
73
74                    "name": "Youtube",
75                    "url": "youtube.com"
76                   }
77   ,
78                  {
79
80                    "children": [
81                      {
82
83                        "name": "Chromium",
84                        "url": "chromium.org"
85                       }
86   ,
87                      {
88
89                        "name": "Chromium Developers",
90                        "url": "dev.chromium.org"
91                       }
92
93                    ],
94                    "name": "Chrome links"
95                   }
96
97                ]
98               }
99   ,
100             {
101
102               "name": "Extension Install Allow list",
103               "value": [
104                 {
105
106                   "name": "test1",
107                   "install link": "https://chrome.google.com/webstore/
```

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

```
                        detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji
                        ?utm_term=chrome%20web%20store&utm_campaign&
                        utm_source=adwords&utm_medium=ppc&hsa_acc
                        =2427782021&hsa_cam=17624934708&hsa_grp
                        =142148219190&hsa_ad=607700050316&hsa_src=g&
                        hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                        store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                        Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZwx
                        ",
                    "id": "laankejkbhbdhmipfmgcngdelahlfoji"
                  }
,
                 {

                    "name": "test2",
                    "install link": "https://chrome.google.com/webstore/
                        detail/vimium/dbepggeogbaibhgnhhndojpepiihcmeb?
                        utm_term=chrome%20web%20store&utm_campaign&
                        utm_source=adwords&utm_medium=ppc&hsa_acc
                        =2427782021&hsa_cam=17624934708&hsa_grp
                        =142148219190&hsa_ad=607700050316&hsa_src=g&
                        hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                        store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                        Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZwx
                        ",
                    "id": "dbepggeogbaibhgnhhndojpepiihcmeb"
                  }

                ]
              }
,
              {

                "name": "Extension Install Force list",
                "value": [
                  "ohlencieiipommannpdfcmfdpjjmeolj",
                  "dipiagiiohfljcicegpgffpbnjmgjcnf"
                ]
              }
,
              {

                "name": "auto fill address enabled",
                "value": true
              }
,
              {

                "name": "auto fill credit card enabled",
                "value": true
              }
,
              {
```

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

```
143
144                 "name": "command line flag security warnings enabled",
145                 "value": true
146               }
147   ,
148               {
149
150                 "name": "payment method query enabled",
151                 "value": true
152               }
153   ,
154               {
155
156                 "name": "saving browser history disabled",
157                 "value": true
158               }
159   ,
160               {
161
162                 "name": "search suggest enabled",
163                 "value": true
164               }
165   ,
166               {
167
168                 "name": "export bookmark allowed",
169                 "value": true
170               }
171   ,
172               {
173
174                 "name": "force ephemeral profiles",
175                 "value": true
176               }
177   ,
178               {
179
180                 "name": "default cookies setting",
181                 "value": "Do not allow any site to set local data"
182               }
183   ,
184               {
185
186                 "name": "default popups setting",
187                 "value": "BlockPopups applies, but users can change this
                      setting"
188               }
189   ,
190               {
191
192                 "name": "look alike warning allowlist domains",
193                 "value": [
194                   "foo.example.com",
```

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

```
                  "example.org"
                ]
              }
  ,
              {

                "name": "extension install sources",
                "value": [
                  "https://corp.mycompany.com/*",
                  "https://corp1.mycompany1.com/*"
                ]
              }
  ,
              {

                "name": "auto launch protocols from origins",
                "value": [
                  {

                    "protocol": "sportifys",
                    "allowed_origins": [
                      "example.com",
                      "http://www.example.com:8080"
                    ]
                  }
  ,
                  {

                    "protocol": "teams",
                    "allowed_origins": [
                      "example1.com",
                      "http://www.example1.com:8080"
                    ]
                  }

                ]
              }

            ]
          }

      ],
      "windows": [
        {

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

```

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

```
                "name": "open all apps in cwb",
                "value": true
              }
  ,
             {

                "name": "incognito mode availability",
                "value": "Incognito mode available"
              }
  ,
             {

                "name": "developer tools availability",
                "value": "Allow usage of the Developer Tools"
              }
  ,
             {

                "name": "enable password save",
                "value": true
              }
  ,
             {

                "name": "Managed bookmarks",
                "value": [
                  {

                    "toplevel_name": "My managed bookmarks folder"
                  }
  ,
                  {

                    "name": "Google",
                    "url": "google.com"
                  }
  ,
                  {

                    "name": "Youtube",
                    "url": "youtube.com"
                  }
  ,
                  {

                    "children": [
                      {

                        "name": "Chromium",
                        "url": "chromium.org"
                      }
  ,
                      {
```

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

```
301
302                      "name": "Chromium Developers",
303                      "url": "dev.chromium.org"
304                     }
305
306                   ],
307                   "name": "Chrome links"
308                  }
309
310                ]
311               }
312   ,
313               {
314
315                 "name": "Extension Install Allow list",
316                 "value": [
317                   {
318
319                     "name": "test1",
320                     "install link": "https://chrome.google.com/webstore/
                          detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji
                          ?utm_term=chrome%20web%20store&utm_campaign&
                          utm_source=adwords&utm_medium=ppc&hsa_acc
                          =2427782021&hsa_cam=17624934708&hsa_grp
                          =142148219190&hsa_ad=607700050316&hsa_src=g&
                          hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                          store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                          Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZw
                          ",
321                     "id": "laankejkbhbdhmipfmgcngdelahlfoji"
322                    }
323   ,
324                    {
325
326                     "name": "test2",
327                     "install link": "https://chrome.google.com/webstore/
                          detail/vimium/dbepggeogbaibhgnhhndojpepiihcmeb?
                          utm_term=chrome%20web%20store&utm_campaign&
                          utm_source=adwords&utm_medium=ppc&hsa_acc
                          =2427782021&hsa_cam=17624934708&hsa_grp
                          =142148219190&hsa_ad=607700050316&hsa_src=g&
                          hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                          store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                          Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZw
                          ",
328                     "id": "dbepggeogbaibhgnhhndojpepiihcmeb"
329                    }
330
331                 ]
332                }
333   ,
334               {
335
```

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

```
                "name": "Extension Install Force list",
                "value": [
                  "ohlencieiipommannpdfcmfdpjjmeolj",
                  "dipiagiiohfljcicegpgffpbnjmgjcnf"
                ]
              }
  ,
              {

                "name": "Delete browsing data on exit",
                "value": [
                  "browsing_history"
                ]
              }
  ,
              {

                "name": "auto fill address enabled",
                "value": true
              }
  ,
              {

                "name": "auto fill credit card enabled",
                "value": true
              }
  ,
              {

                "name": "command line flag security warnings enabled",
                "value": true
              }
  ,
              {

                "name": "payment method query enabled",
                "value": true
              }
  ,
              {

                "name": "saving browser history disabled",
                "value": true
              }
  ,
              {

                "name": "search suggest enabled",
                "value": true
              }
  ,
              {

```

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

```
389                 "name": "export bookmark allowed",
390                 "value": true
391               }
392   ,
393               {
394
395                 "name": "force ephemeral profiles",
396                 "value": true
397               }
398   ,
399               {
400
401                 "name": "default cookies setting",
402                 "value": "Do not allow any site to set local data"
403               }
404   ,
405               {
406
407                 "name": "default popups setting",
408                 "value": "BlockPopups applies, but users can change this
                      setting"
409               }
410   ,
411               {
412
413                 "name": "look alike warning allowlist domains",
414                 "value": [
415                   "foo.example.com",
416                   "example.org"
417                 ]
418               }
419   ,
420               {
421
422                 "name": "extension install sources",
423                 "value": [
424                   "https://corp.mycompany.com/*",
425                   "https://corp1.mycompany1.com/*"
426                 ]
427               }
428   ,
429               {
430
431                 "name": "auto launch protocols from origins",
432                 "value": [
433                   {
434
435                     "protocol": "sportifys",
436                     "allowed_origins": [
437                       "example.com",
438                       "http://www.example.com:8080"
439                     ]
440                   }
```

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

```
,
                {

                  "protocol": "teams",
                  "allowed_origins": [
                    "example1.com",
                    "http://www.example1.com:8080"
                  ]
                 }

              ]
             }

          ]
         }

       ]
      }

   }

}
```

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

September 13, 2025

> **Note:**
>
> We recommend you to restart Citrix Workspace™ app when you modify the Citrix Enterprise Browser settings in GACS. However, you can also wait for the automatic refresh to complete. For more information on the sync duration of policies fetched from GACS, refer Frequency of settings update.

Single sign-on (SSO) is an authentication capability that enables you to access multiple applications using a single set of sign-in credentials. Enterprises typically use SSO authentication to simplify access to various web, on-premises, and cloud applications for a better user experience.

The SSO feature gives administrators more control over:

- User access management.
- Reduction of password-related support calls.
- Enhancement of security and compliance.

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

Previously, SSO was configured using either the PowerShell Module for Citrix Workspace Configuration or Workspace single sign-on via SPA.

From this version, the feature aims at reducing the SSO configuration to a single setting within the Global App Configuration service (GACS). This feature applies to all web and SaaS apps across platforms, without configuring the Gateway Service in the identity providers (IdPs) chain. This feature also improves the user experience, provided the same IdP is used for authentication to both the Citrix Workspace app and the web or SaaS app.

Prerequisites

- To configure this feature for Windows StoreFront, make sure to enable **Microsoft Edge WebView For StoreFront Authentication** using the steps provided in either the Using Global App Config service or Using GPO.
- Use the same identity provider (IdP) for authenticating to the Citrix Workspace app and a particular web or SaaS app.
- Enable persistent cookies within the third-party IdP configuration for a seamless SSO experience.
- The minimum Citrix Workspace app version required is Mac 2311 and Windows 2311.

Configuration through API

To configure, here's an example JSON file to enable SSO feature:

```
{

  "serviceURL": {

    "url": "https://workspacestoretest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "platform": [
        {

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

```

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

```
                "name": "Citrix Enterprise Browser SSO",
                "value": {

                  "CitrixEnterpriseBrowserSSOEnabled": true,
                  "CitrixEnterpriseBrowserSSODomains": [
                    "abc.com",
                    "def.com"
                  ]
                 }

               }

            ]
           }

       ]
      }
 ,
    "name": "Admin UI",
    "description": "Updates from Admin UI",
    "useForAppConfig": true
   }

 }
```

For more information on configuring through API, see the Global App Configuration Service developer documentation.

Configuration through UI

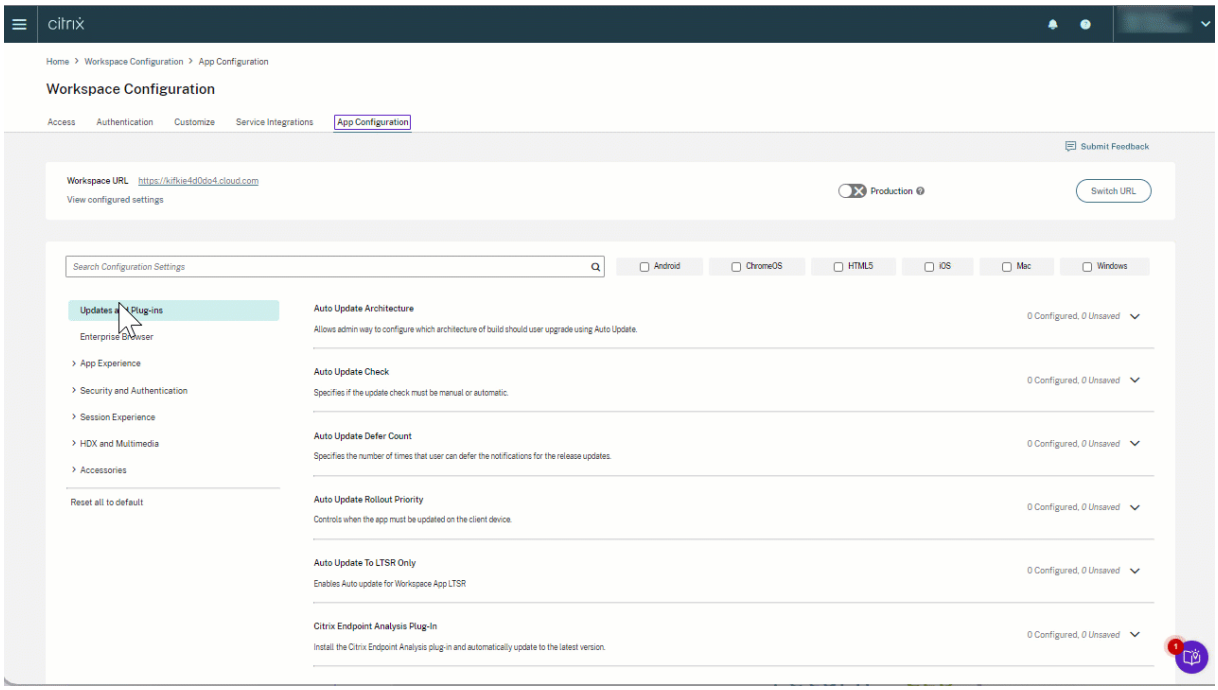
1. Go to the Citrix Cloud portal and sign in using your credentials.
2. Navigate to **Workspace Configuration** > **App Configuration** > **Enterprise Browser**.
3. Select the appropriate operating system under **Configure Single Sign-On For Web/SaaS Apps** section.
4. Click **Edit**.
5. On the **Manage setting** screen, select **Enable Single Sign-on (SSO) on Citrix Enterprise Browser**.
6. Click **Add Domain**, and enter the IdP domains you want to enable SSO for.

   > **Note:**
   >
   > IdP domain is the authentication domain associated with an Identity Provider (IdP) to validate user credentials and confirm their identity. You can configure SSO to Citrix Workspace app using your organization's Identity Provider.

7. Click **Save draft**.

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

8. On the **Save Settings** window, click **Yes** to save the settings.



Citrix Enterprise Browser™ shortcut

September 6, 2025

Starting with the Citrix Workspace app for Windows 2309 version (112.1.1.24), an administrator can configure and control the presence of the Citrix Enterprise Browser shortcut on the **Start** menu.

Similarly, on Citrix Workspace app for Mac 2307 version (113.1.1.34), on the **Launchpad** in Mac.

> **Note:**
>
> - By default, this setting is enabled for Workspace stores.

Configuration

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

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

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

> **Notes:**
>
> - 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 the following settings in any one of the following:
>
> - set the **CEBShortcutEnabled** attribute to **false** in the `web.config` file.
> - disable the **Enable Citrix Enterprise Browser shortcut** property in GPO and GACS.

Using Group Policy Object

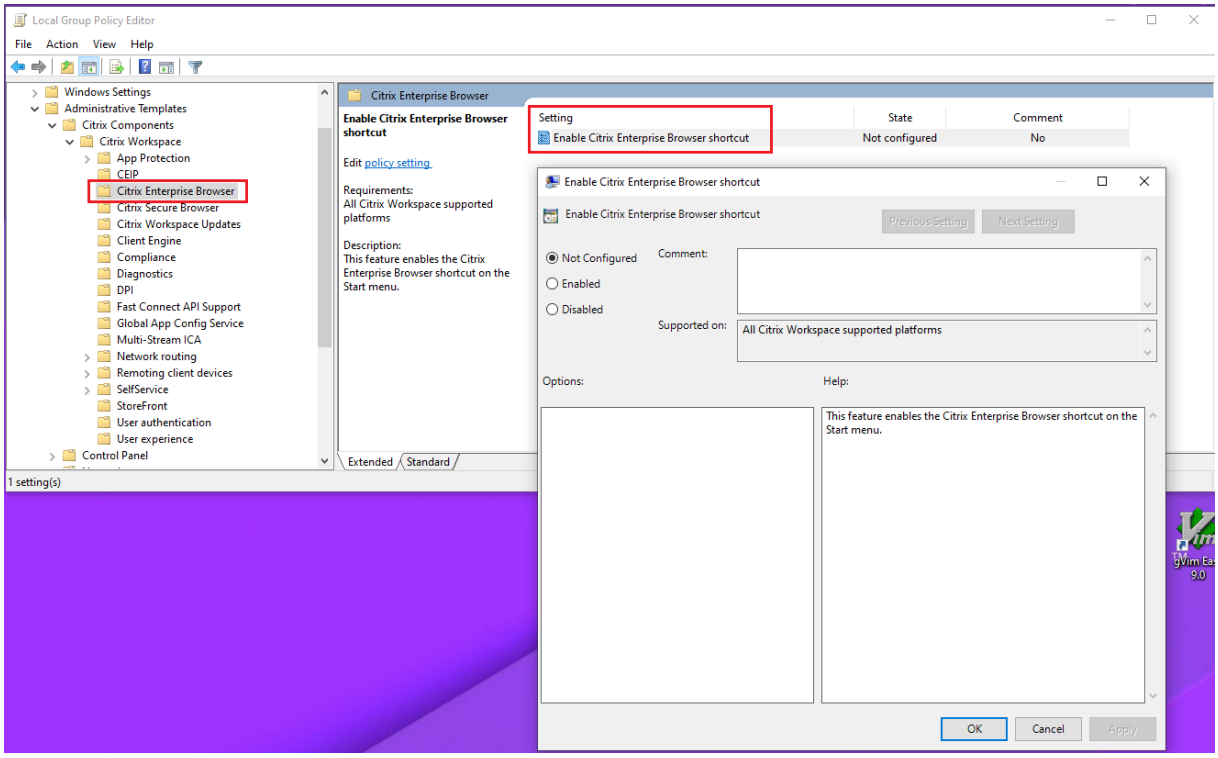
Administrators can use the **Enable Citrix Enterprise Browser shortcut** property to control the display of the Citrix Enterprise Browser shortcut on the **Start** menu.

> **Note:**
>
> Configuration through GPO is applicable on Workspace and StoreFront.

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

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace™** > **Citrix Enterprise Browser**.
3. Select the **Enable Citrix Enterprise Browser** shortcut option.

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



For more information on how to use the GPO, see Group Policy Object administrative template in Citrix Workspace app for Windows documentation.

Global App Configuration service (GACS)

Administrators can enable **Enable Citrix Enterprise Browser shortcut** as follows:

Configuration through API To configure, here's an example JSON file to enable **Enable Citrix Enterprise Browser shortcut**:

```
"settings" : [
    {

        "name": "enable citrix enterprise browser shortcut",
        "value": true
     }

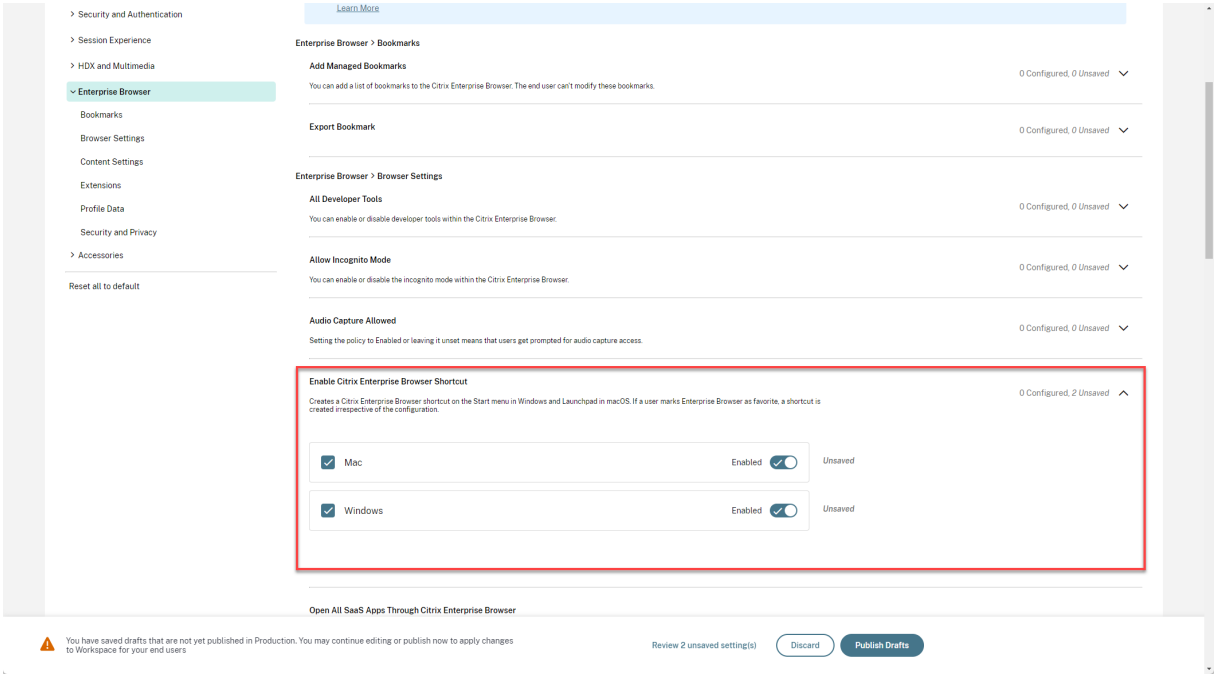
]
```

> **Note:**
>
> - The default value is **Null**.

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

Configuration through UI

1. Navigate to **Workspace Configuration** > **App Configuration**.
2. From the list of configured store URLs, select the store for which you want to map settings and then click **Configure**.
3. Navigate to **Enterprise Browser** > **Enable Citrix Enterprise Browser Shortcut**.
4. Select the appropriate operating system.
5. Enable or disable the toggle button as per your requirement.
6. Click **Publish Drafts**.
7. Click **Yes** to save the changes for your end users.



For more information on 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>
```

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

> **Note:**
>
> Configuration through `web.config` 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">`
3. Before the `</account>` tag, navigate to the properties of that user account and add the following:

```
<properties>

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

</properties>
```

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>
```

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

```
                    <clear />
                    </trustSettings>
                   <properties>
                    <clear />
            </properties>
        </metadata>
</account>
```

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.

Independent update of Citrix Enterprise Browser™

September 6, 2025

Starting with the Citrix Enterprise Browser for version 117.1.1.11, an administrator can update the Citrix Enterprise Browser independently using the stand-alone installer. You can download the installer from the Downloads page of Citrix. The following section provides detailed information about the configuration of an independent installer.

Prerequisites

For the successful update of Citrix Enterprise Browser using the independent installer, make sure that the following requirements are met. Otherwise, the installation fails with an error message.

- Make sure that the Citrix Workspace™ app is already installed on your device before installing the independent installer.
- The independent installer doesn't install Citrix Enterprise Browser when the current or higher version of Citrix Enterprise Browser is already installed.
- The independent installer doesn't install or update Citrix Enterprise Browser when the installed Citrix Workspace app version isn't compatible for update.

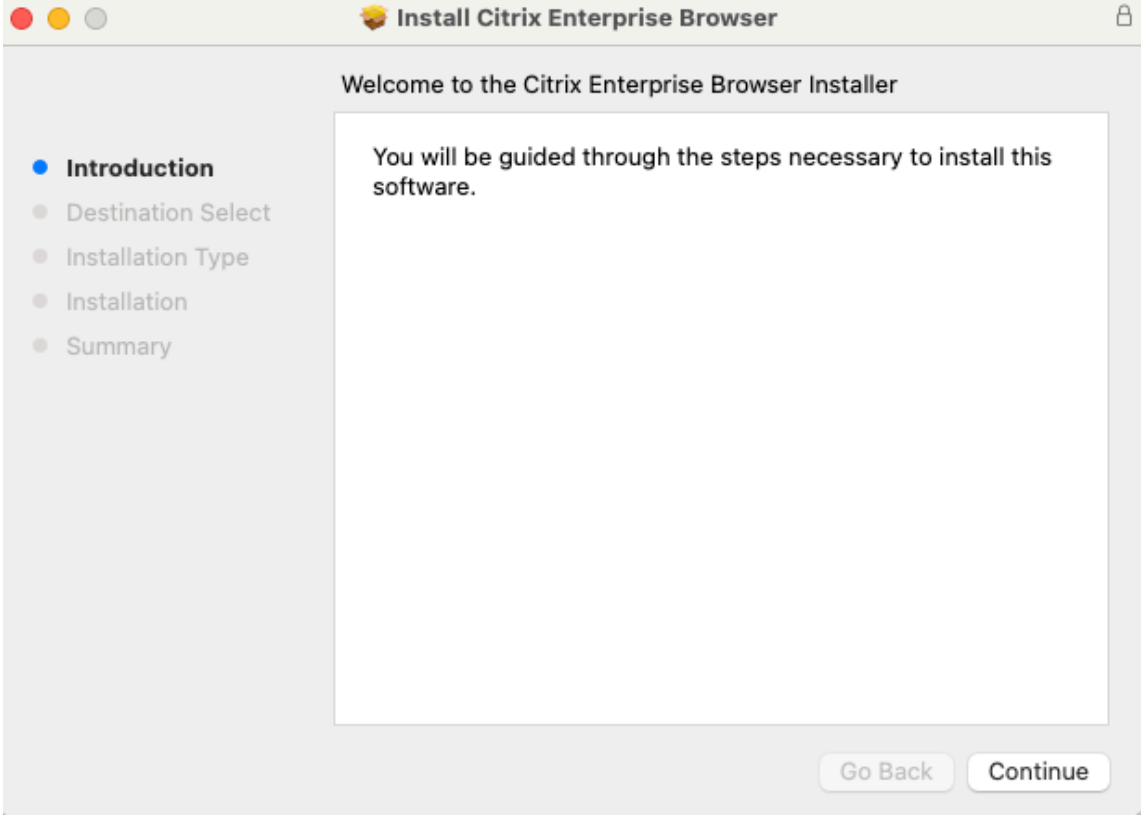
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update Citrix Enterprise Browser on Mac

Manual update

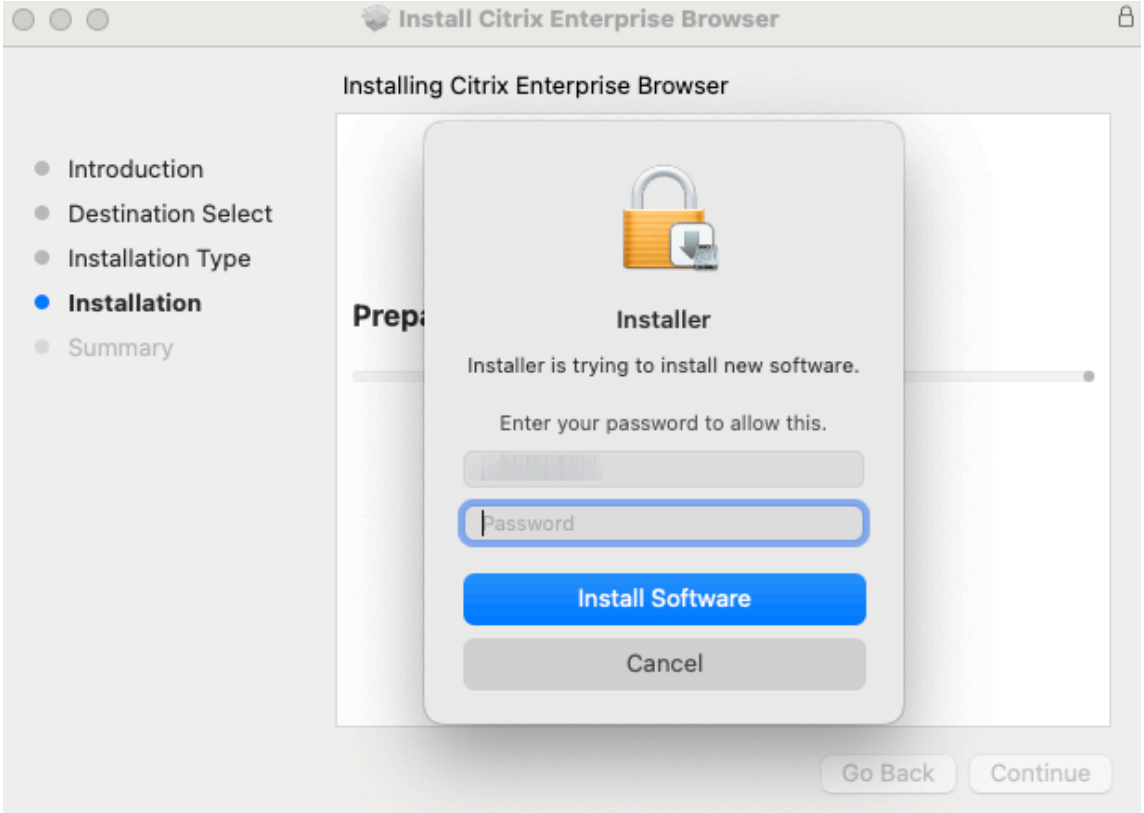
Perform the following steps to manually update Citrix Enterprise Browser using the independent installer.

1. Download the compatible version of the independent installer from the Downloads page.
2. Double-click the independent installer.
3. On the **Install Citrix Enterprise Browser** window, click **Continue**.

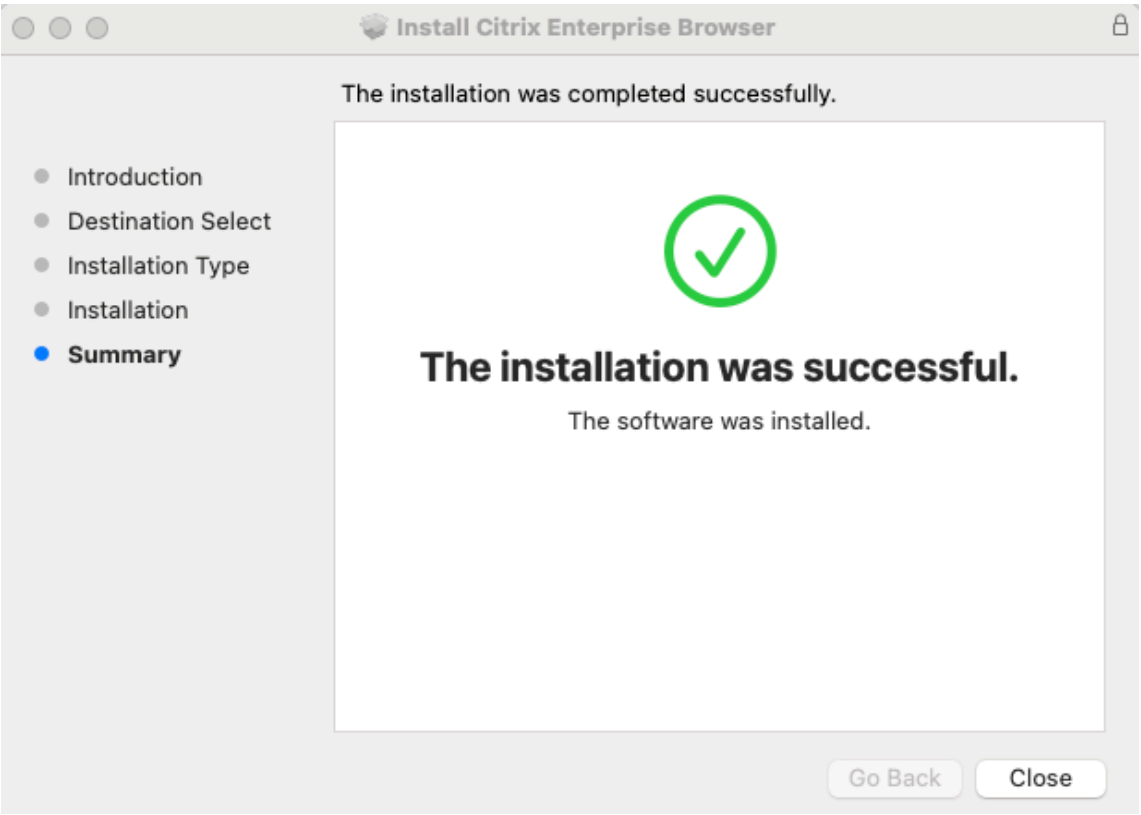


4. Enter your login credentials and then click **Install Software**.

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



"**The installation was successful**"message appears.

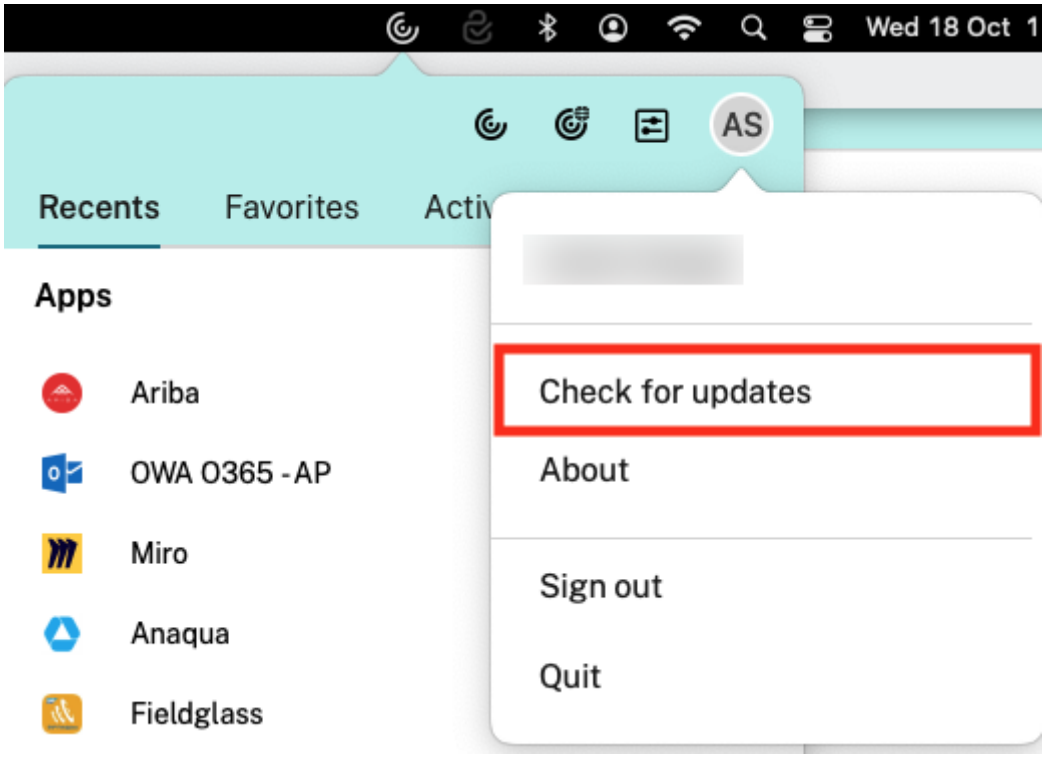


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto update

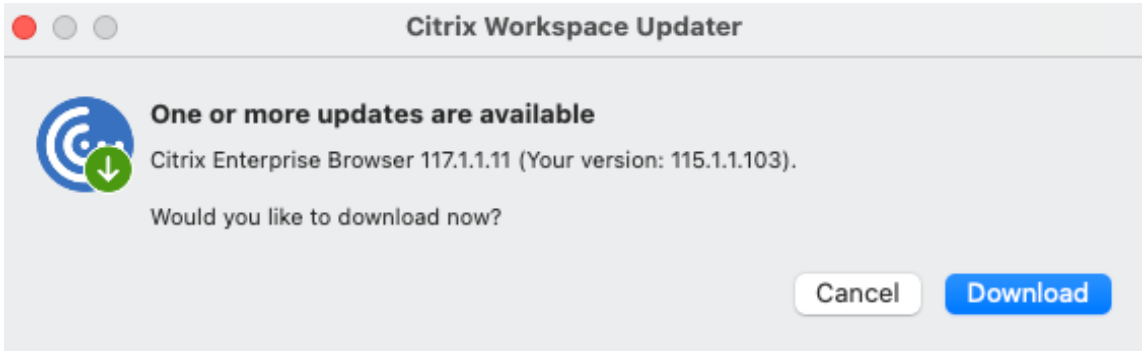
Starting with Citrix Workspace app for Mac version 2309, when the auto update feature is enabled for your Citrix Workspace app, it automatically updates the Citrix Enterprise Browser. If your Citrix Workspace app doesn't have auto update enabled, perform the following steps to update Citrix Enterprise Browser using the independent installer.

1. On your device, click the **Quick Access** icon on the menu bar.
2. Click your user profile picture, and then click **Check for updates**.



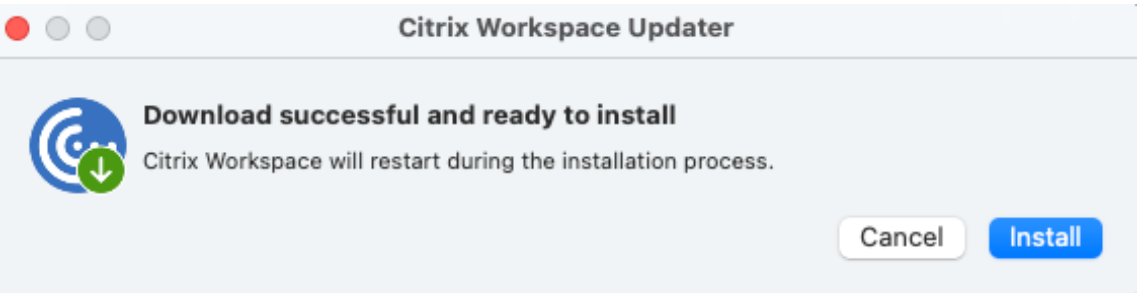
A window appears if any latest update is available.

3. On the **Citrix Workspace Updater** window, click **Download**.



4. Once the download is completed, click **Install**.

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



On successful installation, the Citrix Enterprise Browser gets updated to the latest version.



Update Citrix Enterprise Browser on Windows

Manual update

Perform the following steps to manually update Citrix Enterprise Browser using the independent installer.

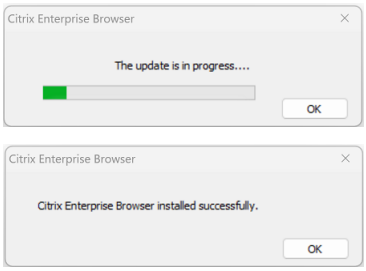
1. From the Citrix Downloads page, download the independent installer that compatible with your

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

Citrix Workspace app.

2. Right-click on the downloaded independent installer, and click **Run as administrator**.

   The update proceeds, and the installation gets completed successfully.



Command-line based update

The command-line based update provides a silent update, which allows you to perform the update in the background without being prompted with the consent dialog box.

To perform the silent update using the independent installer, launch the command prompt as an admin and type:

```
CitrixEnterpriseBrowserInstaller.exe --silent
```

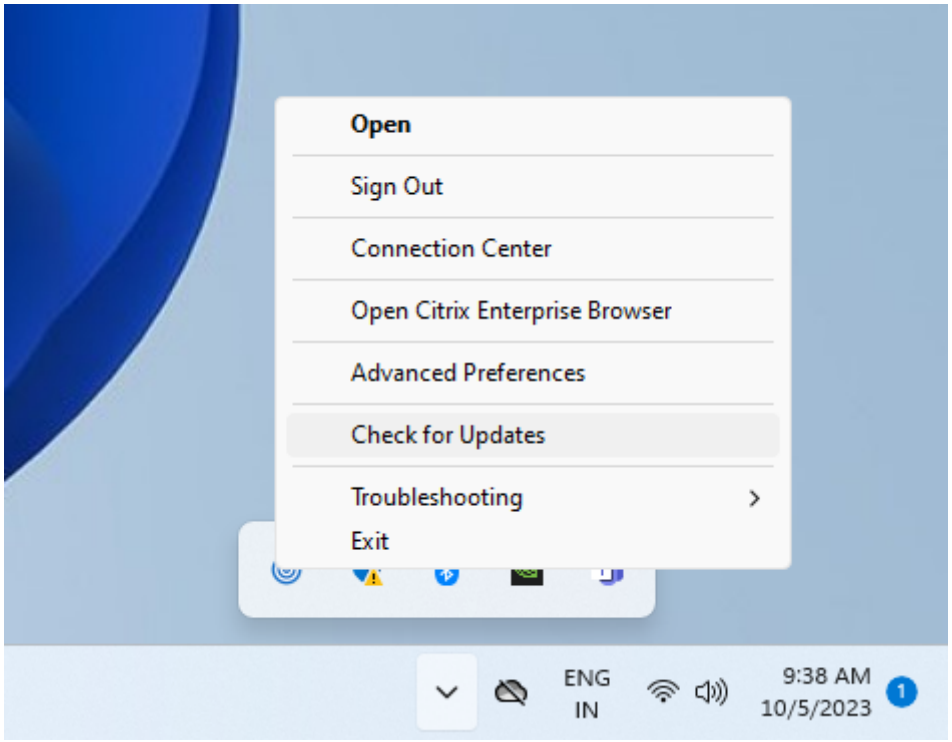
Note: If you do not meet the requirements given in the Prerequisites, the silent update doesn't update the Citrix Enterprise Browser.

Auto update

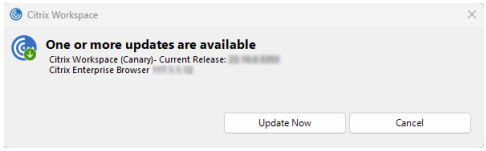
Starting with Citrix Workspace app for Windows version 2311.1, when the auto update feature is enabled for your Citrix Workspace app, it automatically updates the Citrix Enterprise Browser. If your Citrix Workspace app doesn't have auto update enabled, perform the following steps to update Citrix Enterprise Browser using the independent installer.

1. Click the **Show hidden icons** arrow on the taskbar.
2. Right-click the **Citrix Workspace** icon, and then click **Check for Updates**. A dialog box appears if any latest update is available.

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



3. Click **Update Now** on the dialog box.



Browser Data Encryption

September 6, 2025

Browser Data Encryption (formerly App Data Protection) is a feature that provides enhanced security when using the Citrix Enterprise Browser.

When you're using the Citrix Enterprise Browser with the Browser Data Encryption feature enabled in this release, the feature focuses on encrypting browser-generated data, including the following:

- Auto-fill data
- Bookmarks
- Browser cache
- Browser storage folders

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

> **Note:**
>
> Browser storage folders don't include user downloads.

- Cookies
- History
- Network cache
- Password vault
- Settings

> **Note:**
>
> You can only access the encrypted data by opening it using the Citrix Enterprise Browser.

Browser Data Encryption doesn't protect the following:

- Downloaded files
- Extensions

To configure the Browser Data Encryption feature, see Configure Browser Data Encryption.

> **Disclaimer:**
>
> Browser encryption policies provide device-level encryption for data generated through Citrix Enterprise Browser. Note that we do not guarantee that such device-level encryption through Citrix Enterprise Browser will protect any end user device. While we continue to identify and address changes to encryption technology to better optimize our product, we also do not guarantee protection of specific configurations and deployments or for users with elevated privileges.

Limitations:

- If the Browser Data Encryption feature isn't enabled in the primary store, Browser Data Encryption won't be enabled in any store. As a workaround, you can limit users to add only one store to your Citrix Workspace™ app. This ensures that Browser Data Encryption remains enabled for the connected store always.
- When Browser Data Encryption is disabled on GACS, the encrypted items (as listed in the preceding section) are deleted.

System requirements and compatibility

September 6, 2025

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

System requirements

Ensure that you meet the following requirements:

- Ensure that you have installed the Citrix Workspace™ app using administrator rights.
- Minimum version of Citrix® components:
  - Citrix Workspace app for Windows 2405.10 or later
  - Citrix Enterprise Browser app 125.1.1.19 or later

Supported operating systems

The Browser Data Encryption feature is supported on endpoints running on the following operating systems:

- Windows 11 64-bit (not supported on 32-bit)
- Windows 10 64-bit (not supported on 32-bit)

> **Note:**
>
> Browser Data Encryption is not supported inside Virtual Desktop Infrastructure (VDI).

Configure Browser Data Encryption

September 6, 2025

You can configure Browser Data Encryption for Citrix Enterprise Browser™ using one of the following methods:

- Using Global App Configuration service
- Using API

Using Global App Configuration service

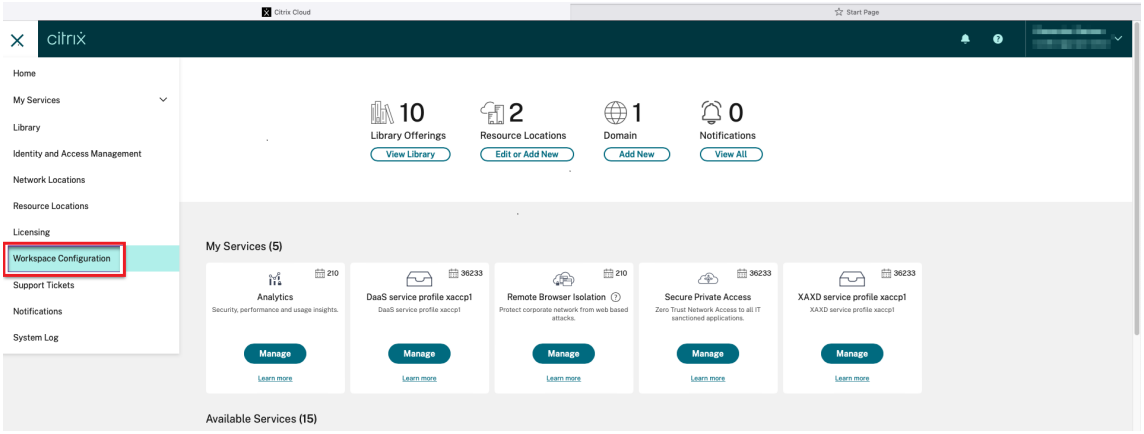
Administrators can configure the Browser Data Encryption using the Global App Configuration service (GACS) by doing the following steps:

> **Note:**
>
> - Data encryption applies to files created before and after enabling the Browser Data Encryption feature. However, the browser cache and network cache created before enabling Browser Data Encryption are deleted after you enable the Browser Data Encryption.

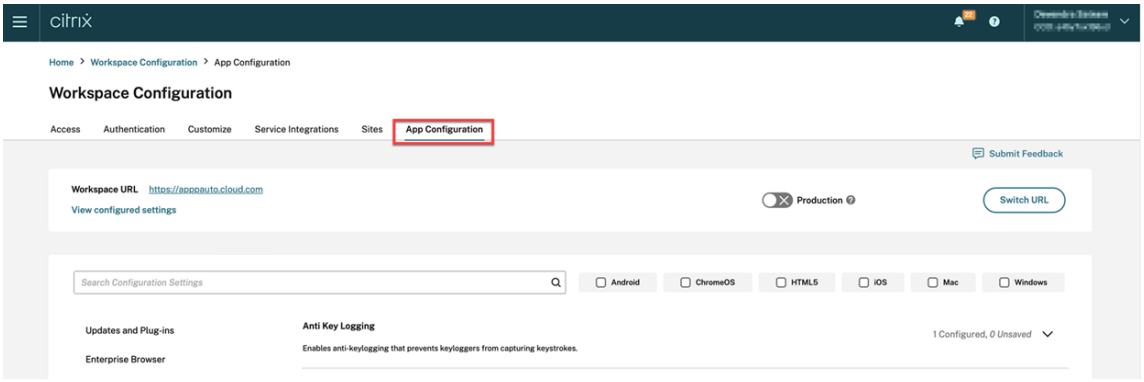
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you disable the Browser Data Encryption feature, user data is deleted.

1. Sign in to your Citrix Cloud™ account and select Workspace Configuration.

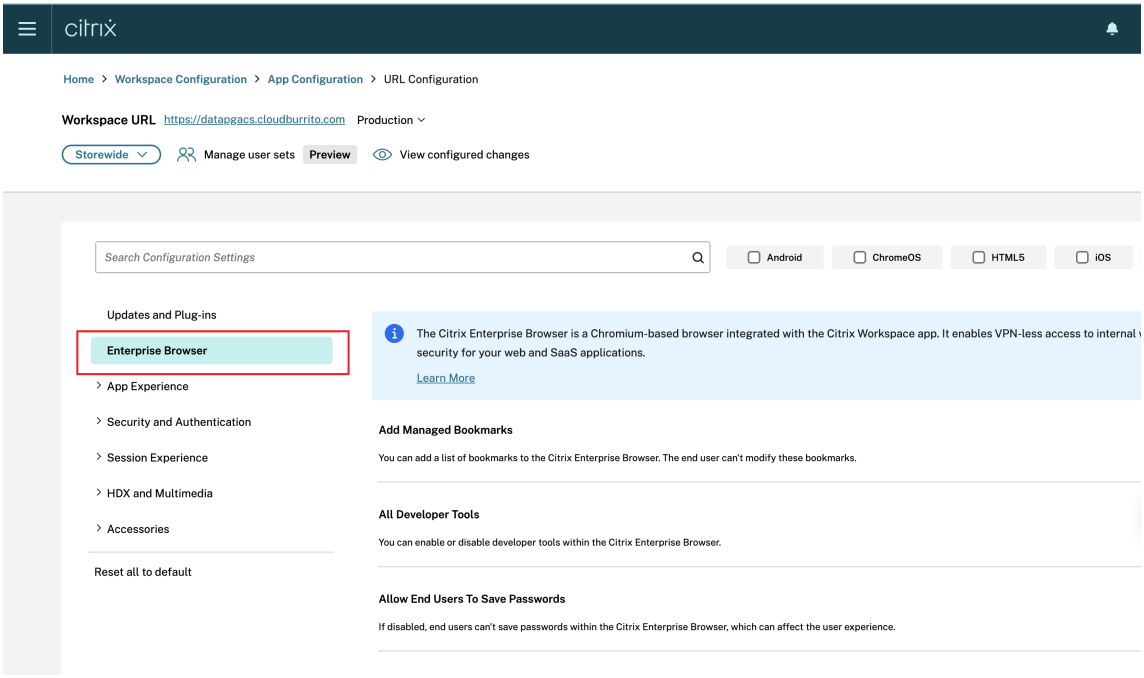


2. Click **App Configuration**.

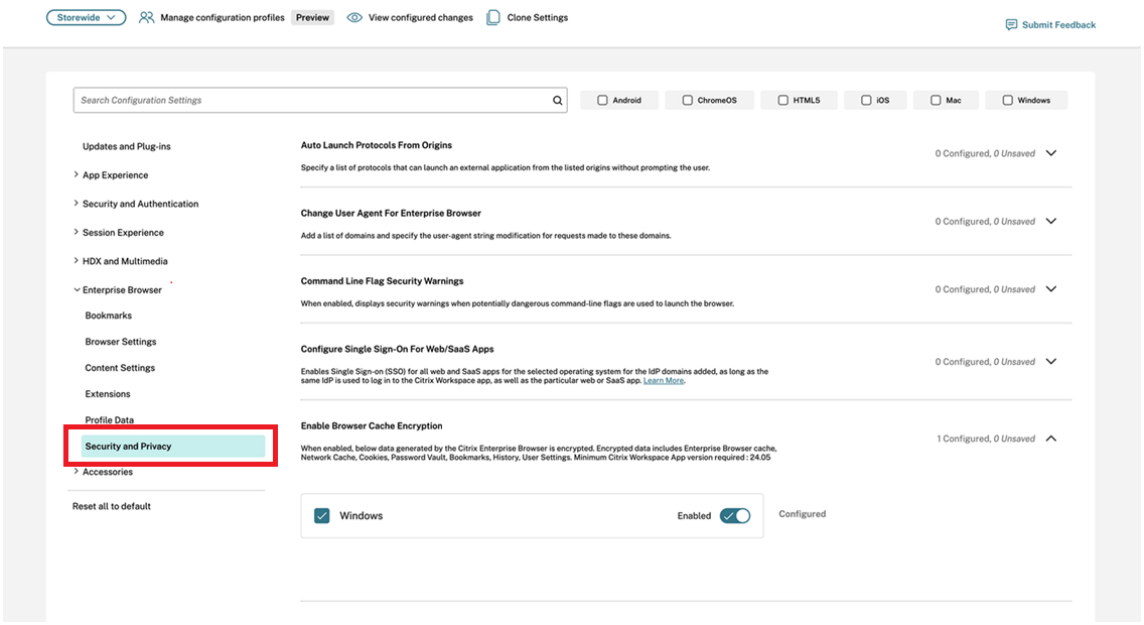


3. Select the relevant store from the list of available stores and then click **Configure**.
4. Click **Enterprise Browser**.

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

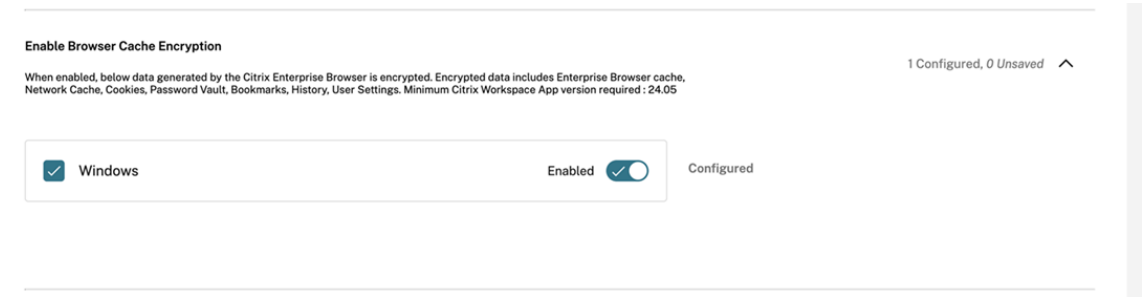


5. Click **Security and Privacy**.

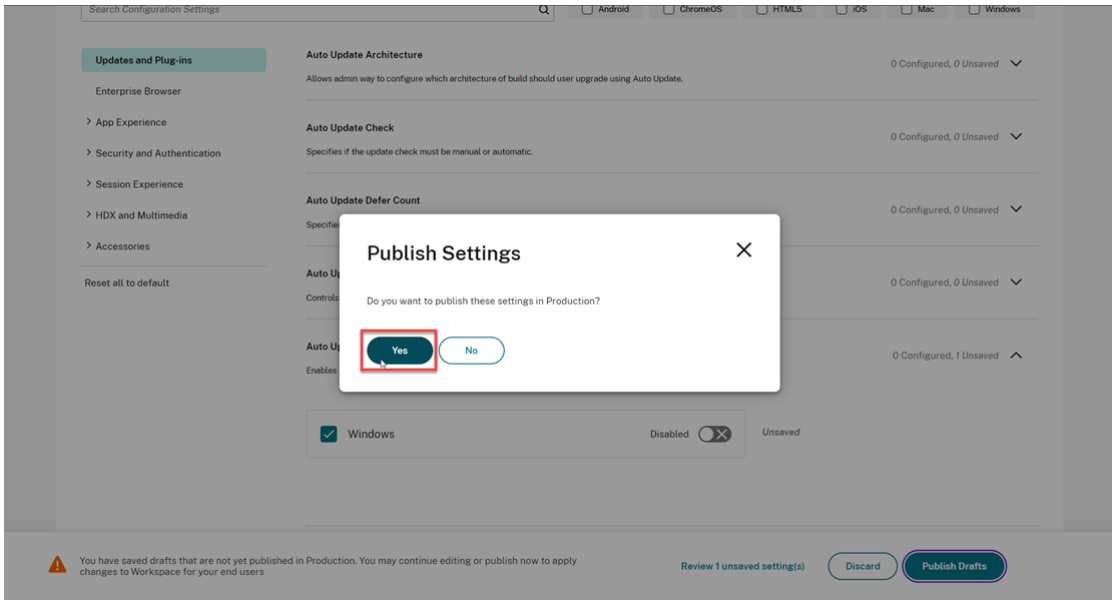


6. Click **Enable Browser Data Encryption**.
7. Select the **Windows** checkbox and then click the **Enabled** toggle button.

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



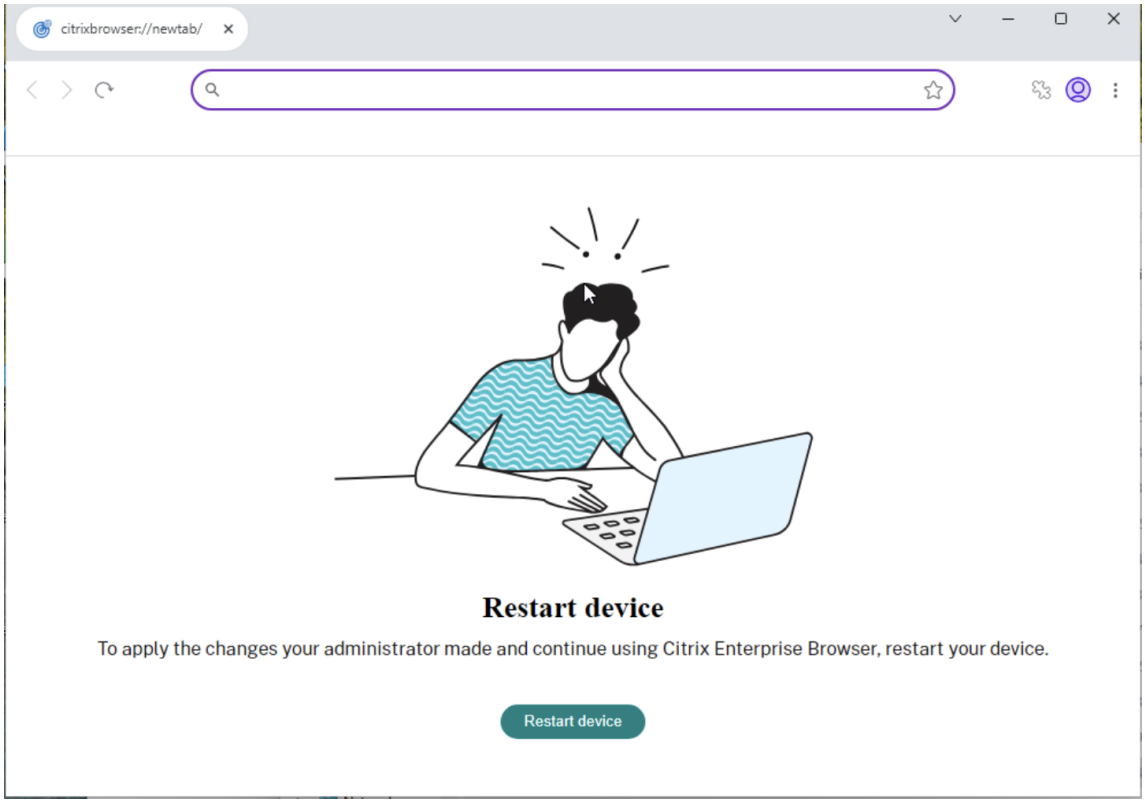
8. Click **Publish Drafts**.
9. In the **Publish Settings** dialog box, click **Yes**.



10. After enabling the Browser Data Encryption in the Global App Configuration service, refresh the Citrix Workspace™ app and then, quit and reopen Citrix Enterprise Browser for the changes to take effect.

    Click **Restart device**, to restart the device for Browser Data Encryption feature to be enabled.

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



For more information about refreshing the Citrix Workspace app, see the following:

- Refresh using a Self-Service Plugin (SSP)
- Refresh using registry keys
- Refresh manually

Using API

The administrators can use the API to configure the Browser Data Encryption feature. The following setting must be set as true to enable Browser Data Encryption:

- “name”: “enable citrix enterprise browser data encryption”
- “value”: “true”or “false”

Example: Following is a sample JSON file to enable Browser Data Encryption:

```
{

  "category": "Browser",
  "userOverride": false,
  "settings": [


{
```

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

```
        "name": "enable citrix enterprise browser data encryption",
                "value": true      }

  ]
 }
```

Troubleshooting

July 31, 2024

This article explains how to troubleshoot the Browser Data Encryption feature.

1. Check if the Browser Data Encryption service is running by running the following commands:

```
sc query CtxPkm
sc query CtxAdpPolicy
```

2. If the Browser Data Encryption service is not running, run the following command to start the service:

```
sc start CtxPkm
sc start CtxAdpPolicy
```

3. Check if the relevant drivers are running by running the following commands:

```
sc query CtxSupport
sc query CtxIsolate
sc query CtxDt2
sc query CtxDs2
```

4. If the required drivers are not running, run the following command to start them:

```
sc start CtxSupport
sc start CtxIsolate
sc start CtxDt2
sc start CtxDs2
```

5. If the Browser Data Encryption feature is still not working, collect the logs and contact `contact-data-protection@cloud.com`.

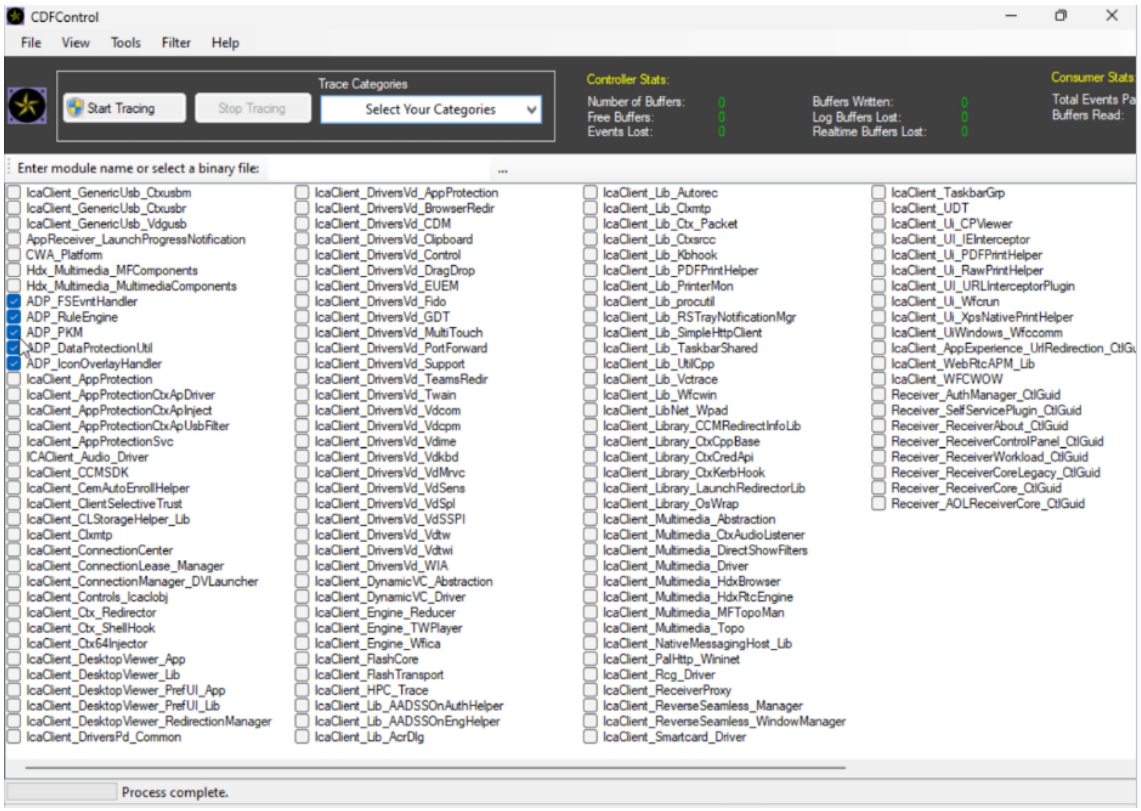
Collecting logs

To collect Browser Data Encryption logs, navigate to `C:\Program Files (x86)\Citrix\CTXReceiverLogs` and collect logs.

To collect logs for the Virtual Delivery Agent, do the following steps:

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

1. To get traces from the Browser Data Encryption service through CDF control, select all the modules as selected in the following image:



2. In certain cases, you might have to capture CDF traces from a different machine. For more information, see CTX237216.

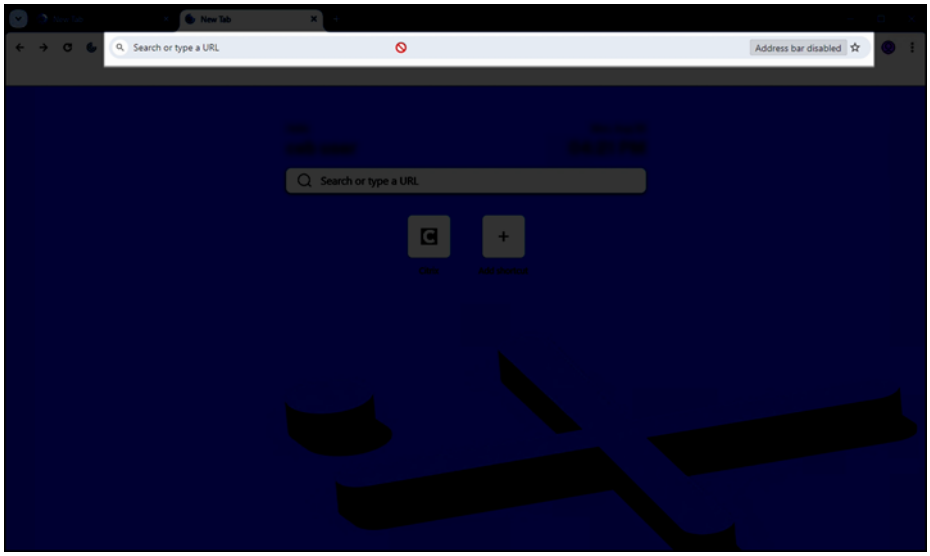
Disable the address bar of the browser

September 6, 2025

> **Note:**
>
> This feature is available on Windows and Mac platforms, starting with the release of Citrix Enterprise Browser version 127.1.1.41.

The address bar of Citrix Enterprise Browser™ can be disabled, restricting users to open only the pre-approved web and SaaS apps within the Enterprise Browser, which includes all hyperlinks within those webpages. When the address bar is disabled, it looks grayed out and uneditable, preventing users from entering URLs.

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



> **Note:**
>
> Disabling the address bar doesn't affect the functionality of web and SaaS apps opened within Citrix Enterprise Browser.

Configuration

Administrators can disable the address bar of the Enterprise Browser through Global App Configuration service (GACS). For more information, see Address bar.

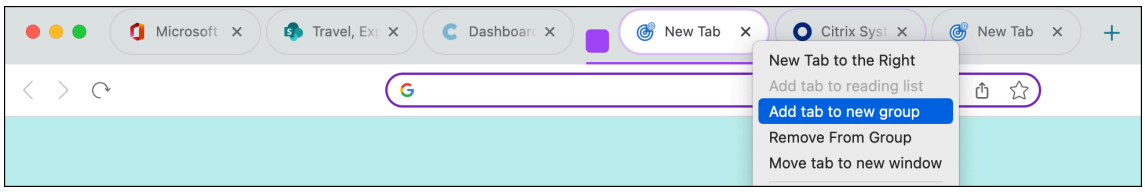
Features

September 6, 2025

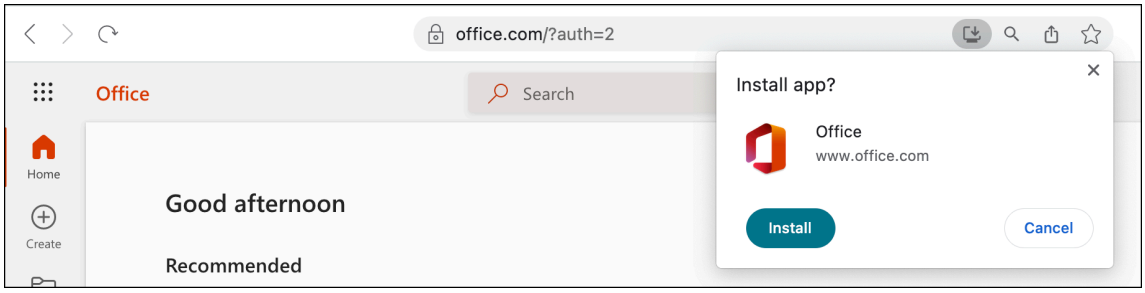
The Citrix Enterprise Browser™ (formerly Citrix Workspace™ Browser) brings you an enhanced and more native-like browser experience and supports the following features:

- **VPN-less access to internal web pages** –Access internal web apps without relying on a VPN.
- **Tabs and multiple windows** –Open multiple tabs and windows and easily switch between them. Every new web or SaaS app that you open in the Workspace app appear in a new tab in the Enterprise Browser. If many tabs are opened, the Enterprise Browser allows you to group similar tabs. You can also pin tabs in the browser window for easy access in the future. To open a tab it in a new window, simply drag the tab out of your current browser window.

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



- **Progressive Web Apps (PWA)** –PWAs are apps that are installed on your device and provide a near app-like experience on your desktop. It's a lightweight app that loads faster as it uses data cached from your previous interactions with the app. To install a PWA, simply visit a website that is available as a PWA. The **Install** icon appears next to the **Bookmark this tab** icon in the address bar as a prompt, if a PWA is available for that website.



All the installed PWAs are available in the **Applications** > **CWA Browser Apps**.

When you open a PWA, you're prompted to authenticate to the Workspace app if you aren't already signed in to the Workspace app.

> **Note:**
>
> When you open a PWA on a Mac, the Enterprise Browser window opens as well.

- **Editable omnibox** –Use the omnibox (address bar), at the top of the browser window to enter URLs or do search operations. The default search engine is Google.
- **Bookmarks** - Add frequently visited webpages to bookmarks for easy access in the future. You can import your bookmarks from other browsers, however, you can't export your bookmarks from the Citrix Enterprise Browser.
- **Dark mode** –Dark mode is applied to the Enterprise Browser only if the theme is already enabled on your system.
- **Microphone and webcam support** - Support for audio and video conferencing through various platforms. The following video conferencing solutions are supported on both Windows and macOS:
  - Microsoft Teams
  - Google Meet
  - Zoom
  - GoToMeeting

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

  - Cisco Webex

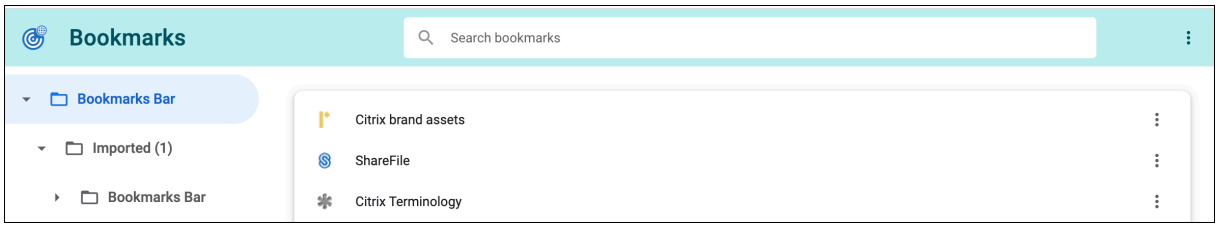
- **Proxy authentication** –Support for one-time authentication if your organization has configured a proxy server and the credentials are stored in the Windows Credentials Manager. After you sign in to the Workspace app for Windows and start a SaaS app, the app opens in the Enterprise Browser. You don't have to authentication again as the Workspace app reads your credentials from the Windows Credentials Manager. You must authenticate again if your organization has configured other proxy servers for which the Workspace app isn't able to find credentials in the Windows credentials manager.
  In all other scenarios, the browser prompts you for authentication. The credentials you provide is cached in the memory until you close the browser window.
  Proxy authentication isn't supported on macOS.
- **Analytics** –If the Citrix Analytics Service is configured, admins can gather information about user behavior and other security insights. For more information about Citrix Analytics, see Getting started section in the Citrix Analytics documentation.

  > **Note:**
  >
  > On macOS, the Citrix Analytics Service doesn't send the **End** events if a user directly closes the Citrix Workspace app.

Import bookmarks

You can import bookmarks from other browsers that you've saved as an html file into the Citrix Enterprise Browser. To import bookmarks, do the following steps:

1. Click the ellipsis icon in the browser and navigate to **Bookmarks** > **Bookmarks Manager**.
2. Select **Import bookmarks** from the available options.
3. Navigate to the location where you've saved the bookmarks and click **Open**.
   The imported bookmarks appear in your bookmarks. Double-click the **Imported** folder to view the imported bookmarks.

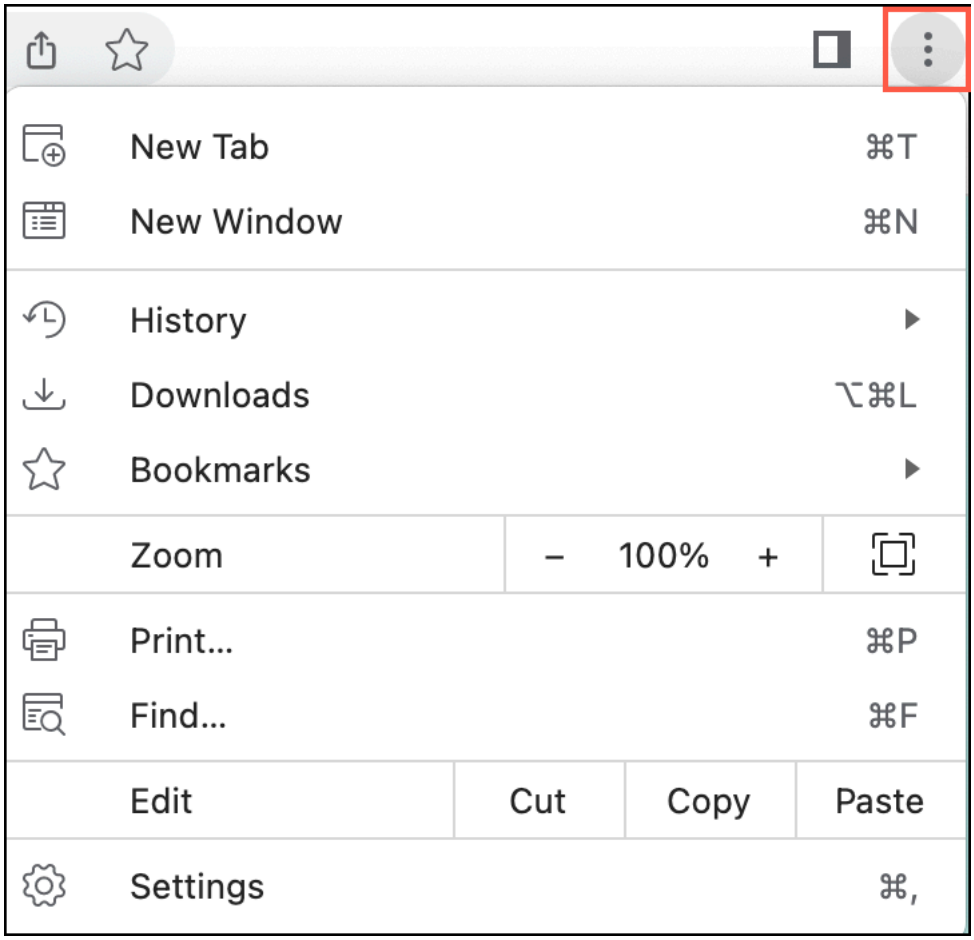


© 1997–2026 Citrix Systems, Inc. All rights reserved.

End user settings

September 6, 2025

You can customize the Citrix Enterprise Browser (formerly Citrix Workspace™ Browser) by using a range of settings that are available to you. The following options appear when you click the ellipsis icon on the top right of the webpage:



Click **Settings** to view the options along with default values or if you like to customize your browsing experience. The following settings options are available in the Enterprise Browser.

Autofill and passwords

Citrix Enterprise Browser allows you to save passwords for different websites.

When you enter a new password on a website, the Enterprise browser prompts you to save it. Click **Save** to accept.

1. To preview the password, click .

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

2. If you have saved multiple passwords for a website, click ▾. Select the password as required.
3. To enter the user name that you want to save, click the text box next to **Username**.
4. To enter the password that you want to save, click the text box next to **Password**.

Add a password manually

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Autofill and passwords** > **Password Manager**.
2. Click **Add**, and enter a website, user name, and password.
3. Click **Save**.

Add notes to your saved password

Adding notes helps you remember your account and login information. Citrix Enterprise Browser secures a note with as much protection as passwords.

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Autofill and passwords** > **Password Manager**.
2. Under **Passwords**, select the password to which you want to add the more information.
3. Click **Edit**.
4. Under **Note**, enter the note text.
5. Click **Save**.

Sign in with the previously saved password

When you save your password for a website, Citrix Enterprise Browser automatically signs you in the next time by using the previously saved password. You don't have to enter the password.

1. Go to a website that you've visited before.
2. Go to the website's sign-in form.
    - If you've saved a single user name and password for the website: Citrix Enterprise Browser fills in the sign-in form automatically.
    - If you've saved more than one user name and password: Select the **username** field and choose the sign-in information that you want to use.

Show, copy, edit, or delete your passwords

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Autofill and passwords** > **Password Manager**.

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

2. Under **Passwords**, choose the password.
    - To preview a password: Click to the right of your password.
    - To copy a password: Click to the right of your password.
    - To edit a password: Navigate to **Edit** > **Password**. Enter the new password, and then click **Save**.
    - To delete a password: Click **Delete**.

Enable or disable saving passwords

By default, Citrix Enterprise Browser prompts you to save your password. Administrators can enable or disable this option at any time.

1. At the upper-right corner of Citrix Enterprise Browser, click > **Settings** > **Autofill and passwords** > **Password Manager**.
2. On the left, select **Settings**.
3. Set the **Offer to save passwords** option on or off as required.

Sign in to websites and apps automatically

End users can enable the **Sign in automatically** option to automatically sign in to websites and apps where your login information is saved.

When you enable it, you don't need to confirm your user name and password. If you prefer to confirm your saved information when signing in, you can turn off this option.

1. At the upper-right corner of Citrix Enterprise Browser, click > **Settings** > **Autofill and passwords** > **Password Manager**.
2. On the left, select **Settings**.
3. Turn **Sign in automatically** on or off.

Add shortcut for Password Manager

Adding **Password Manager** as a shortcut on your home screen, which allows you to access the setting quickly.

1. At the upper-right corner of Citrix Enterprise Browser, click > **Settings** > **Autofill and passwords** > **Password Manager**.
2. On the left, select **Settings** > **Add shortcut**.
3. Click **Install**.

The shortcut for **Password Manager** is added to the home screen after installation.

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

Password Checkup

Check all your saved passwords to verify if they're exposed in a data breach or potentially weak and easy to guess.

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Autofill and passwords** > **Password Manager**.
2. Click **Checkup**.

Privacy and security

Check if a site's connection is secure

Citrix Enterprise Browser enhances your browsing security by notifying you if it detects an unsafe website. When a website is unsafe, the browser changes the icon next to the website address. On the address bar, check the following security icons:

- Default (Secure)
- Information (Not secure)
- Not secure (Dangerous)

You can click the icon to see more information on the website's privacy details and permissions.

> **Note:**
>
> A URL with HTTPS signifies a secure connection. Websites using HTTPS offer a higher level of security compared to those websites without it.

Enable Citrix Enterprise Browser alerts for unsecured connection

If you want the Enterprise Browser to ask you before you use an unsecured connection, do the following instructions:

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Privacy and security** > **Security**.
2. Under **Advanced**, turn on **Always use secure connections**.

When **Always use secure connections** is on, if a website doesn't support HTTPS, the Enterprise Browser displays a **Your connection is not private** warning.

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

Manage certificates

On your Windows and Mac devices, Citrix Enterprise Browser uses website certificates to authenticate and secure HTTPS connections. These certificates encrypt the communication between the website and the Enterprise Browser.

To review the certificates on your device:

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Privacy and security** > **Security**.
2. Under **Advanced**, click **Manage certificates**.

Turn "Do Not Track" on or off

Citrix Enterprise Browser includes the **Do Not Track** setting that allows you to request websites not to track your browsing activity. This setting is turned off by default.

Some websites might ignore this request and still collect your data for various purposes, such as improving security, personalizing content, and displaying relevant ads. Many websites don't change their behavior in response to "Do Not Track" requests. Citrix Enterprise Browser doesn't provide information about which websites respect these requests or how they interpret them.

1. On your computer, open Citrix Enterprise Browser.
2. Click **More** > **Settings**.
3. Click **Privacy and security** > **Third-party cookies**.
4. Turn **Send a "Do not track" request with your browsing traffic** on or off.

Incognito browsing mode

Citrix Enterprise Browser's Incognito mode helps keep users' browsing activities private from other users of the same device. When users open an Incognito window, a new browsing session starts. Any other Incognito windows opened are part of this session. Closing all Incognito windows ends the session.

In Incognito mode, the browsing history, cookies, site data, and information entered in forms aren't saved on the user device. It prevents user activity from appearing in the browser history. Websites treat users as new visitors unless they sign in to their accounts. When users exit all Incognito windows, the Enterprise Browser automatically deletes any website data and cookies linked to that specific browsing session.

Incognito mode does not make users anonymous. Administrators can still monitor users' activities if the organization manages the Enterprise Browser.

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

> **Note:**
>
> When opening an Incognito window, users can enable the **Block third-party cookies** toggle for increased privacy.

Performance

Energy Saver

Citrix Enterprise Browser lowers its image capture rate and minimizes other background tasks to extend your device's battery life. You can enable the **Energy Saver** option, which activates automatically when your device is unplugged or when the battery is low.

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Performance**.
2. Turn **Energy Saver** on or off.
3. Choose the preferred setting:
    - Turn on only when your battery is at 20% or lower.
    - Turn on when your computer is unplugged.

> **Note:**
>
> - Energy Saver does not activate while your device is plugged in.
> - Energy Saver is available on Windows and Mac devices with a battery installed.

Memory Saver

Citrix Enterprise Browser helps save your computer's memory and improve the performance of active tabs by deactivating the other inactive tabs that aren't in use. When you access an inactive tab, it reloads automatically.

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Performance**.
2. Toggle the **Memory Saver** option on or off.

Preload pages

To enhance browsing and search speed, Citrix Enterprise Browser preloads the pages you visit. The Enterprise Browser might use cookies (if permitted) and encrypt and route pages through Google servers to protect your identity from websites.

1. At the upper-right corner of Citrix Enterprise Browser, click ⋮ > **Settings** > **Performance**.
2. Toggle the **Preload pages** option on or off.

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

3. Choose the preferred setting:
    - To preload even more pages you're likely to visit, select **Extended preloading**.
    - To preload some of the pages you're likely to visit, select **Standard preloading**.

The following options are available when you right-click on a webpage.

- **Back**
- **Forward**
- **Reload**
- **Print...**
- **Share**

If you've modified any of the settings and like to restore them to their default values, go to **Settings** and click **Reset Settings**. Once you reset the settings, the following changes are applied to the Enterprise Browser:

- All the pinned tabs get unpinned.
- All cookies are removed and the site data is restored to its default.
- All site settings are restored to their default values.

> **Note:**
>
> - The functionality to add extensions has been blocked.
> - Citrix Enterprise Browser doesn't allow the user to create profiles.

Access to the following URLs is blocked:

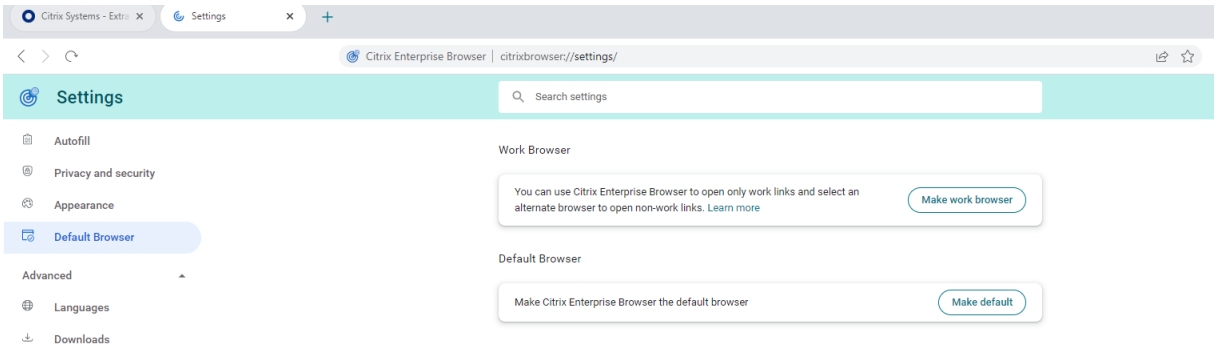
- `citrixbrowser://accessibility`
- `citrixbrowser://apps`
- `citrixbrowser://bluetooth-internals`
- `citrixbrowser://components`
- `citrixbrowser://devices`
- `citrixbrowser://download-internals`
- `citrixbrowser://flags`
- `citrixbrowser://help`
- `citrixbrowser://inspect`
- `citrixbrowser://invalidations`
- `citrixbrowser://local-state`
- `citrixbrowser://media-engagement`
- `citrixbrowser://nacl`
- `citrixbrowser://net-export`
- `citrixbrowser://net-internals`

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

- citrixbrowser://omnibox
- citrixbrowser://password-manager-internals
- citrixbrowser://settings/fonts
- citrixbrowser://settings/help
- citrixbrowser://settings/onStartup
- citrixbrowser://settings/passwords/check
- citrixbrowser://settings/payments
- citrixbrowser://settings/people
- citrixbrowser://settings/privacySandbox
- citrixbrowser://settings/search
- citrixbrowser://signin-internals
- citrixbrowser://site-engagement
- citrixbrowser://sync-internals
- citrixbrowser://term
- citrixbrowser://user-action

Set Citrix Enterprise Browser as the default browser

Once you set Citrix Enterprise Browser as your default browser, all links and apps open through the Enterprise Browser by default. This section lists the steps required to make the Enterprise Browser your default browser on various operating systems.



Windows 10

To make Citrix Enterprise Browser your default browser on Windows 10, 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 and then click **Make default**.
3. On the **Default apps** window, click the + icon under Web browser and select **Citrix Enterprise Browser** from the available options.

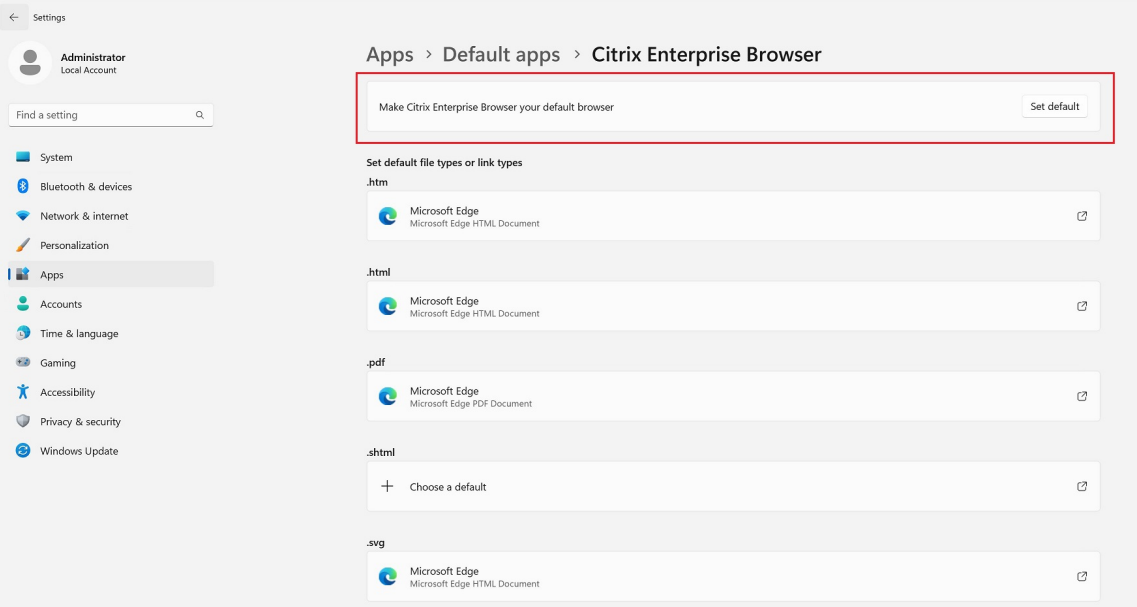
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If you already have a different browser listed under the **Web browser** section, click the existing browser name and select **Citrix Enterprise Browser** from the available options.

Windows 11

To make Citrix Enterprise Browser your default browser on Windows 11, 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 and then click **Make default**.
3. On the **Default apps** page > **Set defaults for applications** search bar, enter Citrix Enterprise Browser and click **Citrix Enterprise Browser**.
4. On the **Apps** > **Default apps** > **Citrix Enterprise Browser** page, click **Set default**.



   To verify the setting, on the **Default Browser** page > **Set a default for a file type or link type** search bar, type **HTTPS**. You must see the **Citrix Enterprise Browser** as the selected browser.

macOS

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. On the Default browser page, click **Make default**. When prompted, click **Use Citrix Enterprise Browser** to confirm your choice and apply the changes.

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

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 an administrator configures for the end user. When a user clicks any link within a native application, if it's a work link, it opens through the Enterprise Browser. If not, the end-user can open it through an alternate browser.

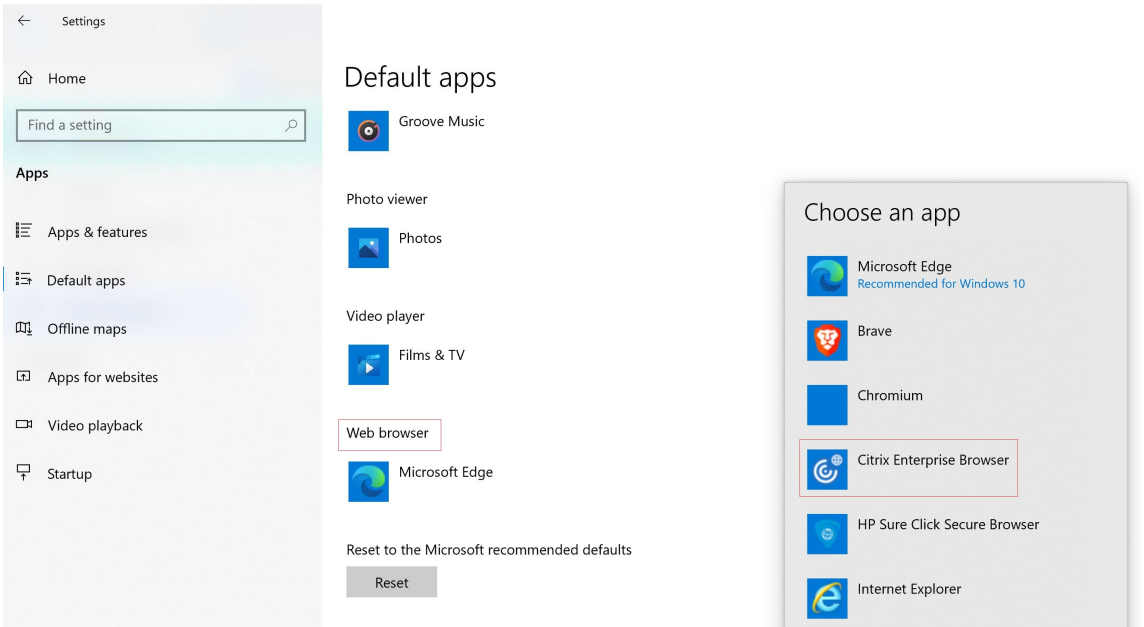
The following section lists the steps required to make Citrix Enterprise Browser your work browser on various operating systems.

Windows 10

To make Citrix Enterprise Browser your work browser on Windows 10, 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 and then click **Make work browser**.
3. On the **Default apps** window, navigate to the **Web browser** section and click the + icon. Select **Citrix Enterprise Browser** from the available options.

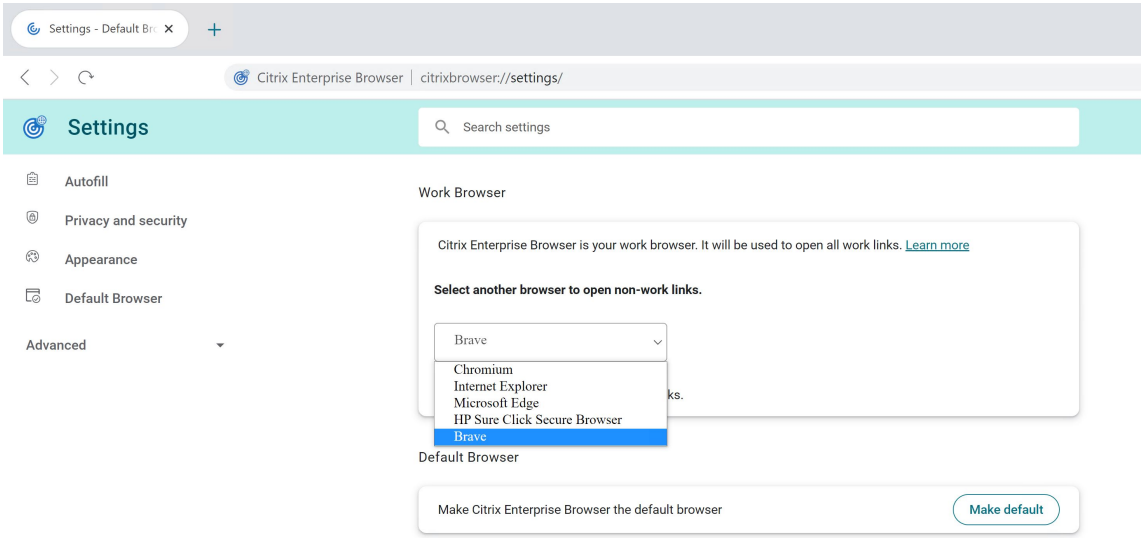
> **Note:**
>
> If you already have a different browser listed under the **Web browser** section, click the existing browser name and select **Citrix Enterprise Browser** from the available options.



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

4. (Optional) On the **Settings** page, select another browser to open non-work links using the drop-down list. The drop-down list is populated depending upon the different browsers that are available on your device.

   Any browser that is installed in the `C:\Program Files\WindowsApps` sandbox folder doesn't get counted as a browser under non-work links.

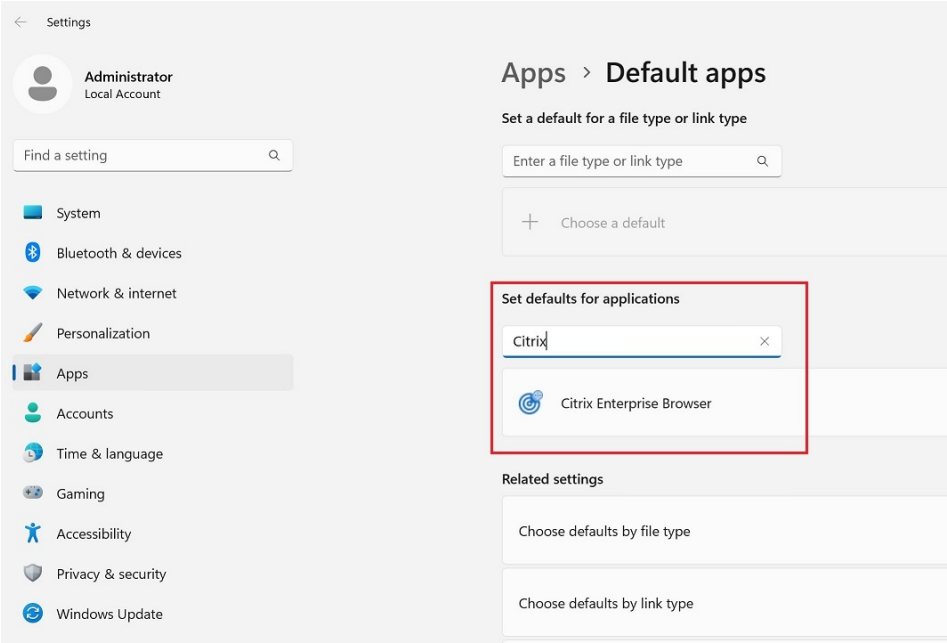


Windows 11

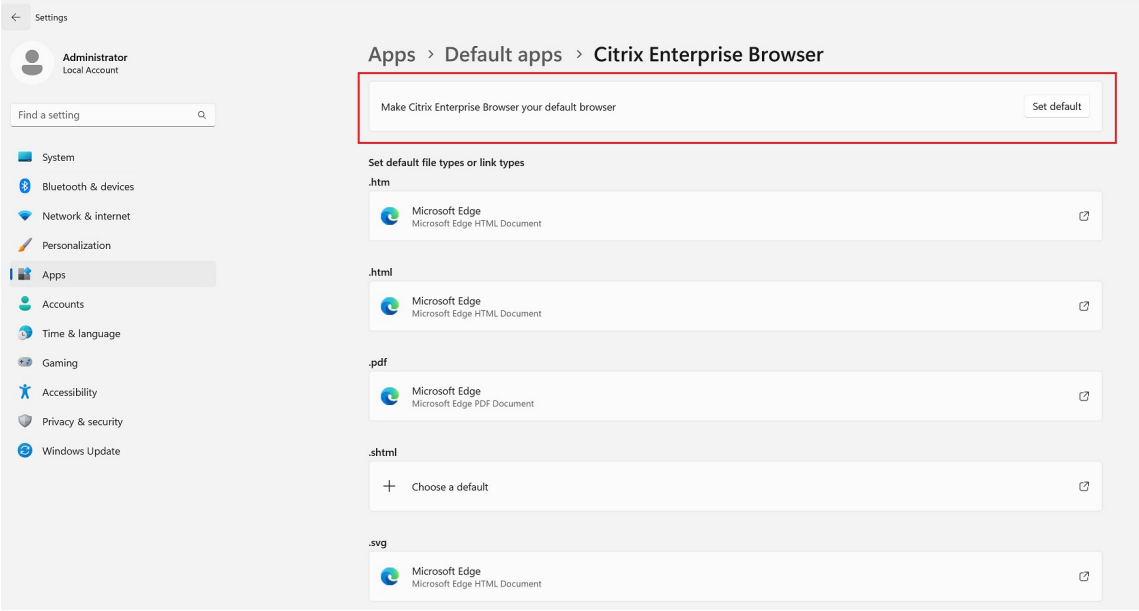
To make Citrix Enterprise Browser your work browser on Windows 11, do the following:

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 and then click **Make work browser**.
3. On the **Default apps** page > **Set defaults for applications** search bar, enter Citrix Enterprise Browser and click **Citrix Enterprise Browser**.

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



4. On the **Apps** > **Default apps** > **Citrix Enterprise Browser** page, click **Set default**.



5. (Optional) On the **Settings** page, select another browser to open non-work links using the drop-down list. The drop-down list is populated depending upon the different browsers that are available on your device. See the **Windows 10** section for the screenshot.

   Any browser that is installed in the `C:\Program Files\WindowsApps` sandbox folder doesn't get counted as a browser under non-work links.

   To verify the setting, on the **Default Browser** page > **Set a default for a file type or link type** search bar, type **HTTPS**. You must see the **Citrix Enterprise Browser** as the selected browser.

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

macOS

To make Citrix Enterprise Browser your work 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. On the Default browser page, click **Make work browser**. When prompted, click **Use "(Work) Citrix Enterprise Browser"** to confirm your choice and apply the changes.
4. (Optional) On the **Settings** page, select another browser to open non-work links using the drop-down list. Depending upon the different browsers that are available on your device, the drop-down list is populated. See the **Windows 10** section for the screenshot.

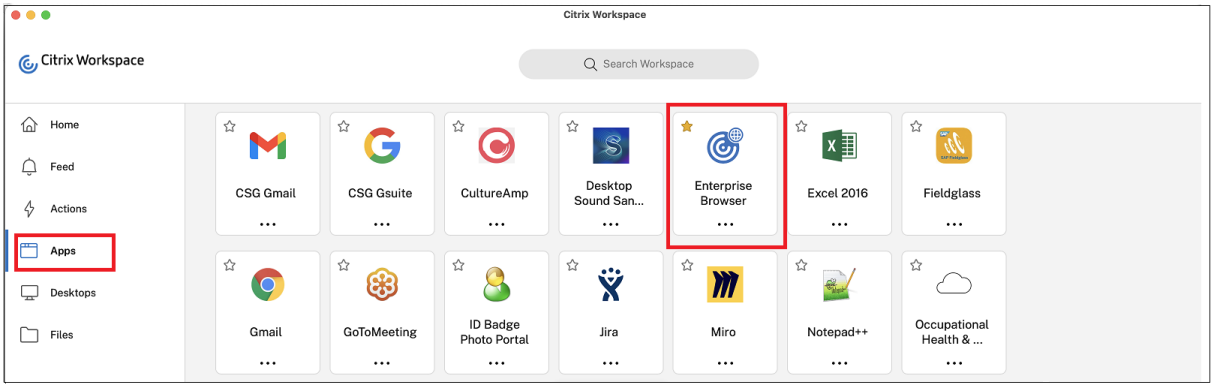
Option to start Citrix Enterprise Browser from within Citrix Workspace app

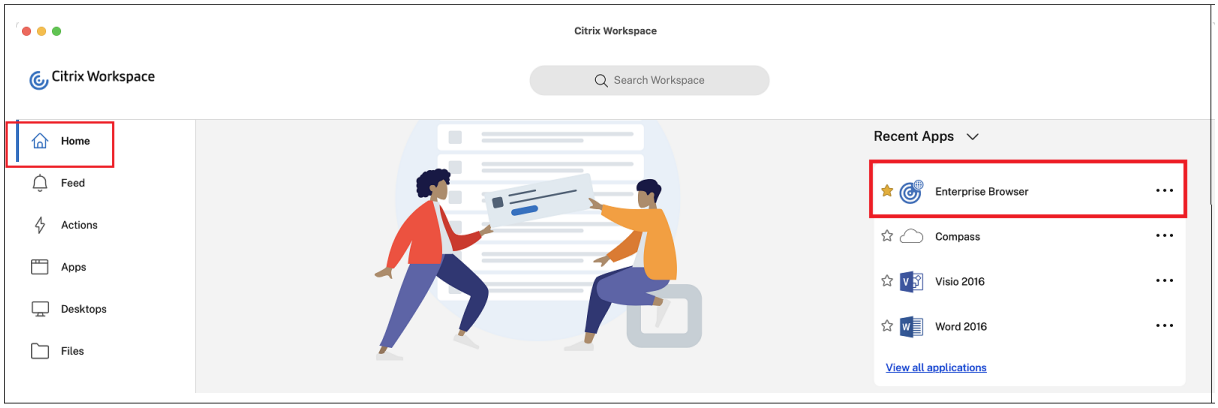
Previously, you can open the Enterprise Browser from Citrix Workspace app after opening a web or SaaS app.

Now, you can open the Enterprise Browser directly from Citrix Workspace app without requiring you to open a web or SaaS app. This feature provides easy access to Citrix Enterprise Browser and doesn't require any configurations from administrators. This feature is available by default.

> **Note:**
>
> This feature is available for Cloud customers only, and the end user must have entitlement to at least one web or SaaS app through Citrix Secure Private Access.

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





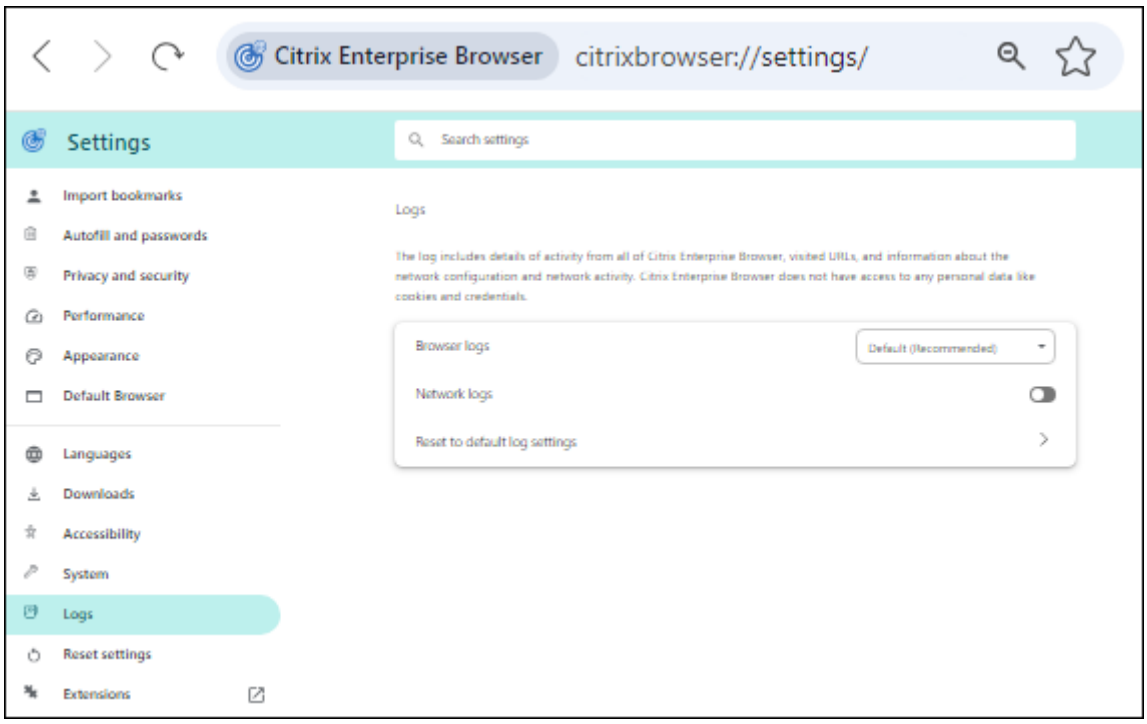
Troubleshoot

September 6, 2025

Log collection

You can collect details about browser activity and network configuration by navigating to **Settings** > **Logs**. The log collection level is set to **Default**, which is the recommended value.

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



Windows:

1. Right-click the Citrix Workspace™ app icon in the notification area and select **Advanced Preferences**.
2. Select **Log Collection**.
   The Log collection dialog appears.
3. Select one of the following log levels:
   - Low
   - Medium
   - Verbose
4. Click **Start collecting logs** and at the same time reproduce the issue to collect the related logs.
5. Click **Stop collecting logs** after the issue is reproduced.
6. Click **Save log** to save the collected logs.

The following Enterprise Browser logs appear in the **Citrix Enterprise Browser™** folder:

- `CitrixEnterpriseBrowser_debug.log` - Available based on the **Browser logs** level that you've selected in the Citrix Enterprise Browser settings.
- `CitrixEnterpriseBrowser-netlog.json` - Available if you have enabled **Network logs** in the Citrix Enterprise Browser settings.

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

> **Note:**
>
> - The default path that contains the log files is `C:\Users\<user_name>\AppData\Local\Citrix\CitrixEnterpriseBrowserV2\User Data\Logs`.

macOS:

1. Open Citrix Workspace app and go to **Preferences** > **Advanced** > **Logging**.
2. Select one of the following session log levels:
   - Disabled (Default)
   - Connection diagnostics
   - Full
3. Select one of the following store log levels:
   - Disabled (Default)
   - Normal
   - Verbose

   > **Note:**
   >
   > - The default path that contains the log files is `~/Library/Application\ Support/Citrix\ Receiver/Citrix\ Enterprise\ Browser/logs`.
4. Click **Email Log Files** to email the logs as a compressed file.

Error codes

Citrix Enterprise Browser prevents users from opening Web or SaaS apps when any unusual activity is noticed. Based on the type of activity, an alert with one of the following error codes might appear.

An end user can do the following troubleshooting steps:

1. Collect the logs for the session and save the file.
2. Close the browser and start the Web or SaaS app.
3. Contact your organization's administrator with the error code to troubleshoot further.

The administrator can open a support case and share the logs if the issue persists.

Here is the list of error codes:

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

Error code	Description
PS1001	Failed to fetch the policy document. To troubleshoot, check the address, gateway settings, your network connection and try again.
PS1002	Failed to parse the policy document.
PS1003	Failed to parse the legacy policy document.
PS1004	The certificate obtained to validate the policy document is empty.
PS1005	Failed to validate the fields in the policy document.
PS1006	Failed to validate the signature of the policy document. To troubleshoot, an administrator can verify if the end user's device time is in sync with the network time.
PS1007	Failed to validate the certificate using the root certificate authority.
PS1008	Failed to fetch the certificate to validate the policy document.
PS1009	Failed to determine the store environment.
PS1010	Failed to fetch the policy document. To troubleshoot, an administrator can close the browser and open again.
PS1011	Failed to fetch the policy document because of the expired token.
APPP-01	The website requires the App Protection component to be enabled. However, the App Protection service isn't running on the system.

© 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.