Citrix Secure Browser
## Contents

Secure Browser service 3

Get started with Secure Browser service 5

Manage and monitor secure browsers 10

Secure Browser technical security overview 19
Secure Browser service

July 27, 2022

The Citrix Secure Browser service isolates web browsing to protect the corporate network from browser-based attacks. Secure Browser service delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration. Administrators can rapidly roll out secure browsers, providing instant time-to-value. By isolating internet browsing, IT administrators can offer end users safe internet access without compromising enterprise security.

Users log on through Citrix Workspace (or Citrix Receiver) and can open web apps in the configured web browser. The website does not directly transfer any browsing data to or from the user device, so the experience is secure.

The Secure Browser service can publish secure browsers for use with:

- **Shared Passcode external web apps.** If you publish a browser with shared passcode authentication, users must enter the passcode to launch an app.

- **Authenticated external web apps.** When you publish authenticated external web apps and launch the apps using Citrix Workspace, the Secure Browser service requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector. For authenticated apps, you must add users with Citrix Cloud Library.

- **Unauthenticated external web apps.** When you publish unauthenticated external web apps and launch the apps using Citrix Workspace, the Secure Browser service requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector.

  Although typically not recommended, unauthenticated external web apps might be used for a simple proof of concept.

For more information, see Publish a secure browser.

The service also offers:

- Integration of published apps with Citrix Workspace
- Integration of published apps with on-premises StoreFront
- Simple URL allow list function for security
- Usage monitoring
- Controls for clipboard use, printing, kiosk mode, region failover, and client drive mapping
What’s new

July 2022

- **Secure Browser supports authentications for all apps with Azure Active Directory.**
  - Users can now sign in to any Secure Browser app from Citrix Workspace using Azure Active Directory credentials.
  - When Secure Browser users sign in, they use the Workspace sign-in page that you configured for your site. For more information, see Integration with Citrix Workspace.

September 2021

- **Secure Browser supports bidirectional audio.** Bidirectional audio is available in Secure Browser.
- **Secure Browser launches from launch.cloud.com are authenticated by Citrix Cloud authentication.** When users launch Secure Browser apps using the launch.cloud.com URL, Citrix Cloud authentication handles their credentials. This enhances security but does not change the user experience.

March 2021

- **Secure Browser supports authentication with Azure Active Directory.** Users can now sign in to Secure Browser apps from Citrix Workspace using Azure Active Directory credentials. For more information, see Integration with Citrix Workspace.
- **Secure Browser lets you monitor and log off users’ active sessions.** Secure Browser provides user name, session ID, client IP, authentication type, application name, session start time, and session duration information about users’ active sessions. You can view basic information about each active session and disconnect the session if needed. For more information, see Monitor active sessions.

Releases in 2020

All releases of 2020 contain enhancements that help improve overall performance and stability.

Additional resources

For developers: Preview API for Secure Browser Service
Get started with Secure Browser service

August 8, 2022

Here’s a video about getting started with Secure Browser service.

1. Sign in to Citrix Cloud. If you don’t have an account, see Sign up for Citrix Cloud. You can request a 30-day trial of the Citrix Secure Browser service.

2. In the Secure Browser tile, click Request Trial.
3. In a few moments, you’ll receive an email (the email associated with your Citrix Cloud account). Click the Sign-in link in the email.

4. After you’re in Citrix Cloud again, click Manage on the Secure Browser tile.

5. On the Welcome to Secure Browser page, click Let’s Get Started. You’re guided to publish your first secure browser.
For information about purchasing the Citrix Secure Browser service, visit https://www.citrix.com/products/citrix-secure-browser/.

**Integration with Citrix Workspace**

Secure Browser can be integrated with Citrix Workspace. To ensure that it's integrated:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **Workspace Configuration**.
3. Select the **Service Integrations** tab.
4. Confirm that the Secure Browser service entry indicates **Enabled**. If it does not, click the ellipsis menu and select **Enable**.

If you haven't already done so, configure the Workspace URL, external connectivity, and workspace authentication for your Workspace, as described in Configure authentication to workspaces.

Secure Browser supports authentication with Active Directory and Azure Active Directory. Authentication with Active Directory is configured by default. For information about configuring authentication using Azure Active Directory, see Connect Azure Active Directory to Citrix Cloud.

If you configure authentication using Azure Active Directory, the on-premises domain containing your Active Directory domain controllers must contain one (preferably two) Cloud Connectors.
**Integrate with your on-premises StoreFront**

Citrix Virtual Apps and Desktops customers with an on-premises StoreFront can easily integrate with the Secure Browser service to provide the following benefits:

- Aggregate your published secure browsers with your existing Citrix Virtual Apps and Desktops apps for a unified store experience.
- Use native Citrix Receivers for enhanced end user experience.
- Strengthen security for Secure Browser launches by using your existing multifactor authentication solution integrated with your StoreFront.

For details, see [CTX230272](#) and the StoreFront configuration documentation.

**Publish a secure browser**

1. If you’re not already in Citrix Cloud, sign in. In the Secure Browser tile, click **Manage**.

2. On the **Manage** tab, click **Publish a Secure Browser**.

3. Select the type of secure browser to publish: shared passcode, authenticated, or unauthenticated. Then click **Continue**.

   ![Publish Secure Browser](#)

   By default, users must launch apps with shared passcode authentication using launch.cloud.com. Citrix Workspace and the Citrix Cloud Library do not support apps with shared passcode.
To use Citrix Workspace, you must publish authenticated apps and explicitly assign subscribers (users) or groups in the Citrix Cloud Library. The unauthenticated apps are available to all Workspace subscribers without user assignment.

4. Configure these settings:

- **Name**: Type a name for the app you are creating.
- **Start URL**: Specify the URL that opens when users start an app.
- **Region**: Choose the location/region for the server. Available regions are West US, East US, Southeast Asia, Australia East, and West Europe.

  If you select **Auto**, your Secure Browser connects you to the closest region based on your geolocation.

- **Passcode**: If you selected a browser with shared passcode authentication, enter the passcode to provide an enhanced secure access to your app. The passcode must be at least 8 alphanumeric characters long. Ensure that you save the passcode and share it with the users. Users must enter the passcode when they launch an app using launch.cloud.com.

- **Icon**: By default, the icon of the Google Chrome executable is used when you publish a Secure Browser. You can now choose your own icon to represent a published browser.

  Click **Change icon > Select icon** to upload the icon of your choice, or choose **Use default icon** to use the existing Google Chrome icon.

5. When you are done, click **Publish**. When the publishing completes, the **Manage tab** lists the browser you published.

  - If you published the authenticated secure browser, you must use the Citrix Cloud Library to add users or groups. Click the right arrow at the end of the row to expand the details pane containing a link to the Library.
When you click the link provided, you are guided to the Library display containing your secure browser. Click the ellipsis on the tile containing the secure browser and click **Manage Subscribers**. For information about adding subscribers, see [Assigning users and groups to service offerings using Library](#).

### Manage and monitor secure browsers

**July 25, 2022**

To manage published secure browsers:

The **Manage** tab lists the published secure browsers. To access management tasks, click the ellipsis at the end of an entry’s row, and then select the task.

If you select a menu entry, and then decide not to change anything, cancel the selection by clicking the **X** outside the dialog box.
Time-outs

Time-out settings include:

- **Idle Timeout**: The number of minutes a session can remain idle before it is ended due to inactivity.
- **Idle Warning Time**: The number of minutes before ending a session that a warning message is sent to the user.

Setting an idle timeout of 20 and an idle warning time of 5 displays a message if there is no activity in the session for 15 minutes (20 minus 5). If the user does not respond, the session ends five minutes later.

When you’re done, click **OK**.
Settings on the policies page control the following:

- **Clipboard**: Enabling the Clipboard policy allows copy and paste operations to and from the remote session. (The Clipboard button is removed from the Citrix Workspace app toolbar.) By default, this setting is disabled.

- **Printing**: Enabling printing saves the remote webpage as a PDF and transfers it to the user's device. The user can then press Ctrl-P and select the Citrix PDF printer. By default, this setting is disabled.

- **Non-kiosk**: Enabling non-kiosk mode restores the interface to the remote browser. The user can then access the address bar and create multiple tabs and windows. (Disabling non-kiosk mode requires signing in again.)
mode removes the remote browser’s navigation controls and address bar.) By default, this setting is enabled (non-kiosk mode is on).

- **Region failover:** The Region failover policy automatically transfers your published browser to a different region if your current region is reporting an issue. To opt out, disable the Region failover policy. If you published the browser using the **Auto** region selection, your secure browser remains enrolled in the policy. By default, this setting is enabled.

- **Client drive mapping:** Enabling the Client drive mapping policy allows the user to upload and download files to and from the remote session. This feature is available only for sessions launched with the Citrix Workspace app. By default, this setting is disabled.
  - Users must save downloaded files only on the `ctxmnt` disk in the `Anonxxx` directory. To do that, users must navigate to the desired location for storing the file. For example, `Anonxxx > ctxmnt > C > Users > User Name > Documents`.
  - The dialog box might prompt the user to accept the **Permit all access** or **Read and Write** permissions to access the `ctxmnt` folder.

- **URL parameters:** Enabling URL parameters allows you to change a new session’s starting URL when users launch an app. For this policy to take effect, configure a local proxy server to identify suspicious websites and redirect them to Secure Browser. By default, this setting is disabled. For more information, see **Proof of Concept Guide: URL Redirection to Secure Browser with Citrix ADC in Azure**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Secure Browser

- **Hostname tracking:** Use host name tracking to enable Secure Browser to log host names during a user’s session. This policy is disabled by default. This information is shared with Citrix Analytics. For more information, see Citrix Analytics.

When you’re done, click **OK**.

### Allow lists

Use the **Whitelists** task to restrict users to visiting only allowed URLs within their published Secure Browser session. This feature is available for external authenticated web apps.

Enter allow list entries in the form `hostname:port number`. Specify each entry on a new line. Asterisks are supported as wildcards. Browser requests must match at least one entry in the allow list.

For example, to set `https://example.com` as an allowed URL:

- `example.com:*` allows connection to this URL from any port.
- `example.com:80` allows connection to this URL only from port 80.
- `*:80` allows access to this URL from any port and from any links to other URLs and ports. The `*:80` format allows access to all external web apps from the published app. This format is the default setting for the web apps **External Whitelist** field.

When you’re done, click **OK**.

Advanced web filtering capabilities are available through integration with the Access Control service. Learn more at **Use case: Selective access to apps**.
You can configure URL filtering to control access methods based on pre-defined categories associated with risk models. URL filtering options include:

- **None** - Allows all categories.
- **Lenient** - Maximizes access while still controlling risk from illegal and malicious websites. Includes the following categories:
  - Adult: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - Computing and Internet: remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - Gambling: Sweepstakes, prizes, lotteries, and gambling in general.
  - Illegal and harmful: Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
  - Malware and spam: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
• **Moderate** - Minimizes risk while allowing more categories with low probability of exposure from unsecure or malicious sites. Includes the following categories:

  - **Adult**: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Business and industry**: Auctions.
  - **Computing and Internet**: Advertisements, banners, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Downloads**: Mobile app stores, storage services, downloads, and program downloads.
  - **Email**: Web-based mail and email subscriptions.
  - **Finance**: Cryptocurrency.
  - **Gambling**: Sweepstakes, prizes, lotteries, and gambling in general.
  - **Malware and spam**: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
  - **Messaging, chat, and telephony**: Instant messages and web-based chat.
  - **News, entertainment, and society**: Wordpress (posts and uploads), unsupported URLs, occult, no content, miscellaneous, horoscope, astrology, fortune telling, drinking, religions, personal webpages, blogs, and online games.
  - **Social networking**: Photo search and sharing sites, IT bulletin boards, and bulletin boards.

• **Strict** - Minimizes the risk of accessing unsecured or malicious websites. End users can still access websites with low risk. Includes the following categories:

  - **Adult**: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Business and industry**: Auctions.
  - **Computing and Internet**: Advertisements, banners, dynamic DNS, mobile apps, publishers, parked domains, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Downloads**: Mobile app stores, storage services, downloads, and program downloads.
  - **Email**: Web-based mail and email subscriptions.
  - **Finance**: Cryptocurrency and financial products.
  - **Gambling**: Sweepstakes, prizes, lotteries, and gambling in general.
  - **Illegal and harmful**: Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
  - **Jobs and resumes**: Employment, career advancement, and LinkedIn (updates, mail, connections, and jobs).
  - **Malware and spam**: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
Citrix Secure Browser

- **Messaging, chat, and telephony:** Instant messages and web-based chat.
- **News, entertainment, and society:** Wordpress (posts and uploads), accommodations, travel and tourism, unsupported URLs, politics, fashion and beauty, arts and cultural events, reference, recreation and hobbies, local communities, miscellaneous, drinking, popular topics, special events, news, society and culture, online magazines, online games, life events, occult, no content, horoscope, astrology, fortune telling, celebrity, streaming media, entertainment, venues, activities, personal webpages and blogs, and religions.
- **Social networking:** Social networks in general, YikYak (posts), Twitter (posts, mail, and follows), Vine (uploads, comments, and messages), Google+ (photo and video uploads, posts, video chat, and comments), Instagram (uploads and comments), YouTube (shares and comments), Facebook (groups, games, questions, video upload, photo uploads, events, chat, apps, posts, comments, and friends), Tumblr (posts, comments, photo, and video uploads), Pinterest (pins and comments), IT bulletin boards, and bulletin boards.

When you’re done, click **Ok**.

**Edit**

Use the **Edit** task to change the name, start URL, region of a published browser, or the passcode. When you’re done, click **Publish**.

**Delete**

Use the **Delete** task to remove a published secure browser. When you select this task, you’re prompted to confirm the deletion.
The Monitor tab provides information about users’ real-time sessions. You can monitor and disconnect one or several active sessions.

To stop a single session, select the session and click the ellipsis menu at the end of an entry’s row. Click Log off session and confirm your changes.

To disconnect multiple sessions, select the active sessions in the list and click the Log off button on the top of the page. After you confirm your changes, Secure Browser immediately disconnects all selected sessions.

The Usage tab shows the:

- Number of initiated sessions
- Number of hours used

To create a spreadsheet containing usage details, click Export to CSV and select a timeframe.
Secure Browser technical security overview

July 25, 2022

Secure Browser Service is a SaaS product managed and operated by Citrix. It allows access to web applications via an intermediate web browser hosted in the cloud.

Cloud service

The Citrix Secure Browser Service consists of web browsers running on Virtual Delivery Agents (VDAs) along with the management console used to manage and connect users to these VDAs. Citrix Cloud manages the operation of these components, including the security and patching of operating systems, web browsers, and Citrix components.

While using Secure Browser service, hosted web browsers track user’s browsing history and perform caching of HTTP requests. Citrix uses mandatory profiles and ensures that this data is deleted when the browsing session ends.

Secure Browser service is accessed with an HTML5-compatible web browser. The service does not provide any downloadable clients. All traffic between the browser being used and cloud service is encrypted using industry-standard TLS encryption. Secure Browser supports TLS 1.2 only.

Egress traffic for Secure Browser uses specific IP addresses to protect the internal network. For the list of accepted IP addresses, see Knowledge Center article CTX286379.

Web applications

Citrix Secure Browser Service is used to deliver web applications owned by the customer or a third party. The owner of the web application is responsible for its security, including patching the web server and application against vulnerabilities.

Security of the traffic between Secure Browser and the web application depends on the encryption settings of the web server. To protect this traffic as it flows over the Internet, administrators publish HTTPS URLs.

More information

See the following resources for more security information:

- Citrix Security site: https://www.citrix.com/security
- Citrix Cloud documentation: Secure Deployment Guide for the Citrix Cloud Platform
Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).