CITRIX

# Secure Web

# Contents



 

# What's new in Secure Web

January 8, 2019

### Secure Web 18.11.5 and 18.12.0

Secure Web versions 18.11.5 and 18.12.0 contain bug fixes and performance enhancements.

### Secure Web 18.11.0

In Secure Web for iOS, cache size list for sites is no longer reported and does not appear in the app settings. The default caching functionality remains the same.

### Secure Web 18.10.5

Secure Web versions 18.9.0 to 18.10.5 contain bug fixes and performance enhancements.

### Secure Web 10.8.65

The following feature is new in Secure Web 10.8.65:

- **Pull to refresh.** In Secure Web for iOS, users can use the pull to refresh feature to update their data on the screen.
- **Search using Find in page option.** You can search for strings instantly by using the **Find in page** option. This option highlights the keywords as you search and displays the total matches on the right side of the toolbar. On relaunching, this feature retains the last searched keywords.
- **Scroll up to hide header and footer bars.** In Secure Web for iOS, the header and the footer bars are hidden as you scroll up. This allows more information to be displayed on your mobile screen when viewing web pages.

### Secure Web 10.8.60

- Support for Polish language

### Secure Web 10.8.35

- **Pull to refresh.** In Secure Web for Android, users can use the pull to refresh feature to update their data on the screen.

 

### Secure Web 10.8.15

**Secure Web supports Android Enterprise, formerly known as Android for Work**. You can create a separate work profile by using Android enterprise apps in Secure Mail. For details, see Android Enterprise in Secure Mail.

**Secure Web for Android can render web pages in desktop mode**. From the overflow menu, select **Request desktop site**. Secure Web displays the desktop version of the web site.

The following features are new in Secure Web 10.8.10.

Secure Web for iOS can render web pages in desktop mode. From the hamburger menu, select **Request Desktop Site** and Secure Web displays the desktop version of the web site.

### Secure Web 10.8.5

**Secure Mail and Secure Web for iOS and Android have revamped fonts, colors, and other UI improvements**. This facelift gives you an enriched user experience while closely aligning with Citrix brand aesthetics across our full suite of apps.

## Known and fixed issues

December 11, 2018

### Known issues in version 18.12.0

- In Secure Web for iOS, embedded videos from the external website such as CNBC is not viewable. [CXM-59576]

### Known issues in version 18.11.5

- In Secure Web for iOS, if a video is played using UIWebView, the media player crashes on expanding the video to full-screen multiple times. [CXM-58800]

### Fixed issues in version 18.11.0

- In Secure Web for iOS, you are unable to print files using AirPrint. Secure Web for iOS does not support AirPrint. [CXM-56001]
- In Secure Web for iOS, some websites scale incorrectly resulting in zooming in of the webpage. [CXM-58283]

 

- In Secure Web for iOS, special characters appear intermittently when you view certain websites in the Turkish language. [CXM-58412]

### Known issues in version 10.8.60

- In Secure Web for iOS, internal sites are not accessible from the Workspace environment, whereas the external sites are accessible. [CXM-55921]

The following issues are fixed in Secure Web. The list includes issues with MDX that affect Secure Web.

### Fixed issues in version 10.8.65

- In Secure Web for iOS, internal sites are not accessible from the Workspace environment whereas the external sites are accessible. [CXM-55921]

### Fixed issues in version 10.8.60

- Secure Web for iOS crashes when launching from Secure Hub during a fresh installation.[CXM-55417]

### Fixed issues in version 10.8.55

- In Secure Web for iOS, the spinning icon appears although certain web pages have successfully loaded on the device. [CXM-52889]

### Fixed issues in version 10.8.50

- When the Document Exchange policy is set to restricted, Secure Web stops working after trying to download a file. [CXM-48447]
- Secure Web for iOS crashes upon submitting login credentials. This issue occurs intermittently when Secure Web attempts to post data from a secure web page to a non-secure web page. [CXM-52977]

### Fixed issues in version 10.8.45

- When a proxy auto-config file with dnsResolve defined is configured in Full Tunnel mode, browsing with Secure Web is noticeably slow. [CXM-49567]
- When you zoom in by pinching the screen, Secure Web for Android refreshes the web page. [CXM-53026]

 

### Fixed issues in version 10.8.40

In Secure Web for iOS, switching to Desktop mode causes the web page to render incorrectly. This issue occurs intermittently when you switch to the Mobile mode. [CXM-52847]

### Fixed issues in version 10.8.26

The following issue is fixed in Secure Web version 10.8.26:

- Due to an update to Chrome 67 or later: Issues occur when users access intranet sites through Secure Web for Android when using Secure Browse. For details, see this Support Knowledge Center article. [CXM-52186]

### Fixed issues in version 10.8.10

#### Secure Web for iOS

After updating Secure Web for iOS to version 10.7.25, users cannot join Skype meetings. Instead, the app store opens for the Lync app. [CXM-46336]

#### Secure Web for Android

On devices that use the WebView API, including Secure Web for Android, you are unable to attach images from a gallery, although the MDX policy Block Gallery is set to **OFF**. [CXM-41475]

## Integrating and deploying Secure Web

November 30, 2018

To integrate and deliver Secure Web, follow these general steps:

1. To enable SSO to the internal network, configure Citrix Gateway.

   For HTTP traffic, Citrix ADC can provide SSO for all proxy authentication types supported by Citrix ADC. For HTTPS traffic, the Web password caching policy enables Secure Web to authenticate and provide SSO to the proxy server through MDX. MDX supports basic, digest, and NTLM proxy authentication only. The password is cached using MDX and stored in the Endpoint Management shared vault, a secure storage area for sensitive app data. For details about Citrix Gateway configuration, see Citrix Gateway.

2. Download Secure Web.

 

3. Determine how you want to configure user connections to the internal network.
4. Add Secure Web to Endpoint Management, by using the same steps as for other MDX apps and then configure MDX policies. For details about policies specific to Secure Web, see About Secure Web Policies.

## Configuring user connections

Secure Web supports the following configurations for user connections:

- **Secure browse:** Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as secure browse. This configuration is the default specified for the **Preferred VPN mode** policy. Secure browse is recommended for connections that require single sign-on (SSO).
- **Full VPN tunnel:** Connections that tunnel to the internal network can use a full VPN tunnel, configured by the **Preferred VPN** mode policy. Full VPN tunnel is recommended for connections that use client certificates or end-to-end SSL to a resource in the internal network. Full VPN tunnel handles any protocol over TCP and can be used with Windows and Mac computers as well as iOS and Android devices.
- The **Permit VPN mode switching** policy allows automatic switching between the full VPN tunnel and secure browse modes as needed. By default, this policy is off. When this policy is on, a network request that fails, due to an authentication request that cannot be handled in the preferred VPN mode, is retried in the alternate mode. For example, the full VPN tunnel mode, but not secure browse mode can accommodate server challenges for client certificates. Similarly, HTTP authentication challenges are more likely to be serviced with SSO when using secure browse mode.
- **Full VPN tunnel with PAC:** You can use a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices. A PAC file contains rules that define how web browsers select a proxy to access a given URL. PAC file rules can specify handling for both internal and external sites. Secure Web parses PAC file rules and sends the proxy server information to Citrix Gateway.
- The full VPN tunneling performance when a PAC file is used is comparable to secure browse mode. For details about PAC configuration, see Full VPN Tunneling with PAC.
- **Reverse Split Tunnel:** In the **REVERSE** mode, the traffic for intranet applications bypasses the VPN tunnel while other traffic goes through the VPN tunnel. This policy can be used to log all non-local LAN traffic.

### Configuration steps for reverse split tunneling

**To configure Split Tunneling Reverse mode on the Citrix Gateway:**

 

- Navigate to **Policies > Session** policy.
- Select the Secure Hub policy and then navigate to **Client Experience > Split Tunnel**.
- Select **REVERSE**.

**The Reverse Split Tunnel Mode Exclusion List MDX Policy in Citrix Endpoint Management:**
You configure the Reverse Split Tunnel Mode policy with the Exclusion range. The range is based on a comma-separated list of DNS suffixes and FQDN. This list defines the URLs for which traffic must be sent out on the local area network (LAN) of the device and would not be sent to Citrix ADC.

The following table notes whether Secure Web prompts a user for credentials, based on the configuration and site type:

| Connection mode | Site type | Password Caching | SSO configured for Citrix Gateway | Secure Web prompts for credentials on first access of a website | Secure Web prompts for credentials on subsequent access of the website | Secure Web prompts for credentials on after password change |
|---|---|---|---|---|---|---|
| Secure Browse | http | No | Yes | No | No | No |
| Secure Browse | https | No | Yes | No | No | No |
| Full VPN | http | No | Yes | No | No | No |
| Full VPN | https | Yes; If the Secure Web MDX policy Enable web password caching is On. | No | Yes; Required to cache the credential in Secure Web. | No | Yes |

### Full VPN Tunneling with PAC

> **Important:**
>
> If Secure Web is configured with a PAC file and Citrix ADC is configured for proxy operation, Secure Web times out. Remove Citrix Gateway traffic policies configured for proxy before using full VPN tunneling with PAC.

When you configure Secure Web for full VPN tunneling with your PAC file or proxy server, Secure Web

 

sends all traffic to the proxy through Citrix Gateway. Citrix Gateway then routes traffic according to the proxy configuration rules. In this configuration, Citrix Gateway is unaware of the PAC file or proxy server. The traffic flow is the same as for full VPN tunneling without PAC.

The following diagram shows the traffic flow when Secure Web users navigate to a web site:

In that example, the traffic rules specify that:

- Citrix Gateway directly connects to the intranet site `example1.net`.
- Traffic to intranet site `example2.net` is proxied through internal proxy servers.
- External traffic is proxied through internal proxy servers. Proxy rules block external traffic to `Facebook.com`.

### To configure full VPN tunneling with PAC

1. Validate and test the PAC file.

   > **Note:**
   >
   > For details about creating and using PAC files, see https://findproxyforurl.com/.

   Validate your PAC file using a PAC validation tool such as Pacparser. When you read your PAC file, ensure the Pacparser results are what you expect. If the PAC file has a syntax error, mobile devices silently ignore the PAC file. (A PAC file is stored only in memory on mobile devices.)

   A PAC file is processed from the top down and processing stops when a rule matches the current query.

   Test the PAC file URL with a web browser before entering into the **PAC/Proxy** field of Endpoint Management. Make sure that the computer can access the network where the PAC file is located.

   ```
   https://webserver.local/GenericPAC.pac
   https://webserver.local/GenericPAC.pac
   ```

   Tested PAC file extensions are .txt or .pac.

   The PAC file should show its contents inside the web browser.

   > **Important:**
   >
   > Each time you update the PAC file used with Secure Web, inform users that they must close and reopen Secure Web.

2. Configure Citrix Gateway:

   - Disable Citrix Gatewaysplit tunneling. If split tunneling is on and a PAC file is configured, the PAC file rules override the Citrix ADC split tunneling rules. A proxy does not override Citrix ADC split tunneling rules.

 

- Remove Citrix Gateway traffic policies configured for proxy. This step is required for Secure Web to work correctly. The following figure shows an example of the policy rules to remove.

3. Configure Secure Web policies:
   - Set the Preferred VPN mode policy to **Full VPN tunnel**.
   - Set the Permit VPN mode switching policy to **Off**.
   - Configure the PAC file URL or proxy server policy. Secure Web supports HTTP and HTTPS as well as default and non-default ports. For HTTPS, the root certificate authority must be installed on the device if the certificate is self-signed or untrusted.

     Be sure to test the URL or proxy server address in a web browser before configuring the policy.

     Example PAC file URLs:

     ```
     http[s]://example.com/proxy.pac
     http[s]://10.10.0.100/proxy.txt
     ```

     Example proxy servers (port is required):

     ```
     myhost.example.com:port
     ```

     ```
     10.10.0.100:port
     ```

     > **Note:**
     >
     > If you configure a PAC file or proxy server, do not configure PAC in system proxy settings for WiFi.

   - Set the Enable web password caching policy to **On**. Web password caching handles SSO for HTTPS sites.

     Citrix ADC can perform SSO for internal proxies if the proxy supports the same authentication infrastructure.

#### Limitations of PAC file support

Secure Web does not support:

- Failover from one proxy server to another. PAC file evaluation can return multiple proxy servers for a hostname. Secure Web uses only the first proxy server returned.
- Protocols, such as ftp and gopher in a PAC file.
- SOCKS proxy servers in a PAC file.
- Web Proxy Autodiscovery Protocol (WPAD).

 

Secure Web ignores the PAC file function alert so that Secure Web can parse a PAC file that doesn't include those calls.

## Secure Web policies

When adding Secure Web, be aware of these MDX policies that are specific to Secure Web. For all supported mobile devices:

### Allowed or blocked websites

Secure Web normally does not filter web links. You can use this policy to configure a specific list of allowed or blocked sites. You configure URL patterns to restrict the websites the browser can open, formatted as a comma-separated list. A plus sign (+) or minus sign (-) precedes each pattern in the list. The browser compared a URL against the patterns in the order listed until a match is found. When a match is found, the prefix dictates the action taken as follows:

- A minus (-) prefix instructs the browser to block the URL. In this case, the URL is treated as if the web server address could not be resolved.
- A plus (+) prefix allows the URL to be processed normally.
- If neither + or - is provided with the pattern, + (allow) is assumed.
- If the URL does not match any pattern in the list, the URL is allowed

To block all other URLs, end the list with a minus sign followed by an asterisk (-*). For example:

- The policy value `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permits HTTP URLs within `mycorp.com` domain, but blocks them elsewhere, permits HTTPS and FTP URLS anywhere, and blocks all other URLs.
- The policy value `+http://*.training.lab/*,+https://*.training.lab/*,-*` allows users to open any sites in Training.lab domain (intranet) via HTTP or HTTPS. The policy value does not let users open public URLs, such as Facebook, Google, Hotmail, regardless of protocol.

Default value is empty (all URLs allowed).

### Block pop-ups

Popups are new tabs that websites open without your permission. This policy determines whether Secure Web allows popups. If On, Secure Web prevents websites from opening pop-ups. Default value is Off.

 

### Preloaded bookmarks

Defines a preloaded set of bookmarks for the Secure Web browser. The policy is a comma-separated list of tuples that include folder name, friendly name, and web address. Each triplet should be of the form folder,name,url where folder and name may optionally be enclosed in double quotes (“).

For example, the policy values,”Mycorp, Inc. home page”,https://www.mycorp.com, ”MyCorp Links”,Account logon,https://www.mycorp.com/Accounts ”MyCorp Links /Investor Relations”,”Contact us”,https://www.mycorp.com/IR/Contactus.aspx define three bookmarks. The first is a primary link (no folder name) titled “Mycorp, Inc. home page”. The second link is placed in a folder titled “MyCorp Links” and labeled “Account logon”. The third is placed in the “Investor Relations’ subfolder of the “MyCorp Links” folder and displayed as “Contact us”.”

Default value is empty.

### Home page URL

Defines the website that Secure Web loads when started. Default value is empty (default start page).

For supported Android and iOS devices only:

### Browser user interface

Dictates the behavior and visibility of browser user interface controls for Secure Web. Normally all browsing controls are available. These include forward, backward, address bar, and the refresh/stop controls. You can configure this policy to restrict the use and visibility of some of these controls. Default value is All controls visible.

Options:

- **All controls visible.** All controls are visible and users are not restricted from using them.
- **Read-only address bar.** All controls are visible, but users cannot edit the browser address field.
- **Hide address bar.** Hides the address bar, but not other controls.
- **Hide all controls.** Suppresses the entire toolbar to provide a frameless browsing experience.

### Enable web password caching

When Secure Web users enter credentials when accessing or requesting a web resource, this policy determines whether Secure Web silently caches the password on the device. This policy applies to passwords entered in authentication dialogs and not to passwords entered in web forms.

 

If **On**, Secure Web caches all passwords users enter when requesting a web resource. If Off, Secure Web does not cache passwords and removes existing cached passwords. Default value is **Off**.

This policy is enabled only when you also set the Preferred VPN policy to Full VPN tunnel for this app.

#### Proxy servers

You can also configure proxy servers for Secure Web when used in secure browse mode. For details, see this blog post.

#### DNS suffixes

On Android, if DNS suffixes aren't configured, the VPN could fail. For details on configuring DNS suffixes, see Supporting DNS Queries by Using DNS Suffixes for Android Devices.

### Preparing intranet sites for Secure Web

This section is for website developers who need to prepare an intranet site for use with Secure Web for Android and iOS. Intranet sites designed for desktop browsers require changes to work properly on Android and iOS devices.

Secure Web relies on Android WebView and iOS UIWebView to provide web technology support. Some of the web technologies supported by Secure Web are:

- AngularJS
- ASP .NET
- JavaScript
- JQuery
- WebGL
- WebSockets

Some of the web technologies not supported by Secure Web are:

- Flash
- Java

The following table shows the HTML rendering features and technologies supported for Secure Web. X indicates the feature is available for a platform, browser, and component combination.

| Technology | iOS Secure Web | Android 5.x/6.x/7.x Secure Web |
|---|---|---|
| JavaScript engine | JavaScriptCore | V8 |

 

| Technology | iOS Secure Web | Android 5.x/6.x/7.x Secure Web |
|---|---|---|
| Local Storage | X | X |
| AppCache | X | X |
| IndexedDB | | X |
| SPDY | X | |
| WebP | | X |
| srcet | X | X |
| WebGL | | X |
| requestAnimationFrame API | | X |
| Navigation Timing API | | X |
| Resource Timing API | | X |

Technologies work the same across devices; however, Secure Web returns different user agent strings for different devices. To determine the browser version used for Secure Web, you can view its user agent string. From Secure Web, navigate to https://whatsmyuseragent.com/.

### Troubleshooting intranet sites

To troubleshoot rendering issues when your intranet site is viewed in Secure Web, compare how the website renders on Secure Web and a compatible third-party browser.

For iOS, the compatible third-party browsers for testing are Chrome and Dolphin.

For Android, the compatible third-party browser for testing is Dolphin.

> **Note:**
>
> Chrome is a native browser on Android. Do not use it for the comparison.

In iOS, make sure the browsers have device-level VPN support. You can configure this support on the device in **Settings > VPN > Add VPN Configuration**.

You can also use VPN client apps available on the App Store, such as Citrix VPN, Cisco AnyConnect, or Pulse Secure.

- If a web page renders the same for the two browsers, the issue is with your website. Update your site and make sure it works well for the OS.
- If the issue on a web page appears only in Secure Web, contact Citrix Support to open a support ticket. Please provide your troubleshooting steps, including the tested browser and OS types. If

 

Secure Web for iOS has rendering issues, please include a web archive of the page as described in the following steps. Doing so helps Citrix resolve the issue faster.

**To create a web archive file**

Using Safari on macOS 10.9 or later, you can save a web page as a web archive file (referred to as a reading list) that includes all linked files, such as images, CSS, and JavaScript.

1. From Safari, empty the **Reading List** folder: In the **Finder**, click the **Go** menu in the **Menu** bar, choose **Go to Folder**, type the path name ~/Library/Safari/ReadingListArchives/, and then delete all of the folders in that location.
2. In the **Menu** bar, go to **Safari > Preferences > Advanced** and enable **Show Develop menu** in menu bar.
3. In the **Menu** bar, go to **Develop > User Agent** and enter the Secure Web user agent: (Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. In Safari, open the web site you will save as a reading list (web archive file).
5. In the **Menu** bar, go to **Bookmarks > Add to Reading List**. This step can take a few minutes. The archiving occurs in the background.
6. Locate the archived reading list: In the **Menu** bar, go to **View > Show Reading List Sidebar**.
7. Verify the archive file:
   - Turn off network connectivity to your Mac.
   - Open the web site from the reading list.

     The web site should completely render.
8. Compress the archive file: In the **Finder**, click the **Go** menu in the **Menu** bar, choose **Go to Folder**, and then type the path name ~/Library/Safari/ReadingListArchives/. Then, compress the folder that has a random hex string as a file name. This file is the file that you can send to Citrix support when you open a support ticket.

## Secure Web Features

Secure Web uses mobile data exchange technologies to create a dedicated VPN tunnel for users to access internal and external websites and all other websites. The sites include sites with sensitive information in an environment secured by your organization's policies.

The integration of Secure Web with Secure Mail and Citrix Files offers a seamless user experience within the secure Endpoint Management container. Here are some examples of integration features:

 

- When users tap mailto links, a new email message opens in Citrix Secure Mail with no additional authentication required.
- In iOS, users can open a link in Secure Web from a native mail app by inserting **ctxmobilebrowser://** in front of the URL. For example, to open `example.com` from a native mail app, use the URL ctxmobilebrowser://example.com.
- When users click an intranet link in an email message, Secure Web goes to that site with no additional authentication required.
- Users can upload files to Citrix Files that they download from the web in Secure Web.

Secure Web users can also perform the following actions:

- Block pop-ups.

  > **Note:**
  >
  > Much of Secure Web memory goes into rendering pop-ups, so performance is often improved by blocking pop-ups in Settings.

- Bookmark their favorite sites.
- Download files.
- Save pages offline.
- Auto-save passwords.
- Clear cache/history/cookies.
- Disable cookies and HTML5 local storage.
- Securely share devices with other users.
- Search within the address bar.
- Allow web apps they run with Secure Web to access their location.
- Export and import settings.
- Open files directly in Citrix Files without having to download the files. To enable this feature, add **ctx-sf**: to the Allowed URLs policy in Endpoint Management.
- In iOS, use 3D Touch actions to open a new tab and access offline pages, favorite sites, and downloads directly from the home screen.
- In iOS, download files of any size and open them in Citrix Files or other apps.

  > **Note:**
  >
  > Putting Secure Web in the background causes the download to stop.

- Search for a term within the current page view using **Find in Page**.

Secure Web also has dynamic text support, so it displays the font that users set on their devices.

 

## iOS Data Protection

August 23, 2018

Enterprises who must meet Australian Signals Directorate (ASD) data protection requirements can use the **Enable iOS data protection** policies for Secure Mail and Secure Web. By default the policies are **Off**.

When **Enable iOS data protection** is **On** for Secure Web, Secure Web uses Class A protection level for all files in the sandbox. For details about Secure Mail data protection, see Australian Signals Directorate Data Protection. If you enable this policy, the highest data protection class is used so there is no need to also specify the **Minimum data protection class** policy.

To change the **Enable iOS data protection** policy:

1. Use the Endpoint Management console to load the Secure Web and Secure Mail MDX files to the XenMobile Server: For a new app, navigate to **Configure > Apps > Add** and then click **MDX**. For an upgrade, see Upgrade MDX or enterprise apps.
2. Use the Endpoint Management console to load the MDX files to the XenMobile Server: For a new app, navigate to **Configure > Apps > Add** and then click **MDX**. For an upgrade, see Add apps.
3. For Secure Mail, browse to the **App** settings, locate the **Enable iOS data protection** policy and set it to **On**. Devices running older operating system versions are not affected when this policy is enabled.
4. For Secure Web, browse to the **App** settings, locate the **Enable iOS data protection** policy and set it to **On**. Devices running older operating system versions are not affected when this policy is enabled.
5. Configure the app policies as usual and save your settings to deploy the app to the Endpoint Management app store.

 

**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