citrix

Secure Web

Contents

What's new in Secure Web 3

Known and fixed issues 19

Integrating and deploying Secure Web 20

iOS Data Protection 32

Secure Web features 33

What's new in Secure Web

October 27, 2021

> **Note:**
>
> Support ended for the Android 6.x and iOS 11.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app in June 2020.

What's new in the current version

Secure Web 21.10.5

Secure Web for iOS

This release includes bug fixes.

Secure Web for Android

This release includes bug fixes.

> **Note:**
>
> Support for Android 7 ends for Secure Web as of October 2021.

What's new in earlier versions

Secure Mail 21.10.0

Secure Web for Android

- **Support for Android 12**. From this release onward, Secure Web is supported on devices running Android 12.
- Secure Web meets Google Play's current target API requirements API level 30 (Android 11).

Secure Web 21.9.1

Secure Web for Android

This release includes bug fixes.

Secure Web 21.9.0

Secure Web for iOS

This release includes bug fixes.

Secure Web for Android

This release includes bug fixes.

Secure Web 21.8.5

Secure Web for Android

Support for Android 12 Beta 4 on already enrolled devices. Secure Web now supports Android 12 Beta 4. If you are considering upgrading to Android 12 Beta 4, ensure that you update Secure Hub to version 21.7.1 first. Secure Hub 21.7.1 is the minimum version required to upgrade to Android 12 Beta 4. This release ensures a seamless upgrade from Android 11 to Android 12 Beta 4 for already enrolled users.

> **Note:**
>
> Citrix is committed to providing Day 1 support for Android 12 and will add further updates to subsequent versions of Secure Web to fully support Android 12.

Secure Web 21.8.0

> **Note:**
>
> This version of Secure Web is supported only on iOS 12.1 and later. Updates are not available for Secure Web running on devices with iOS versions 12 or earlier.

Secure Web for iOS

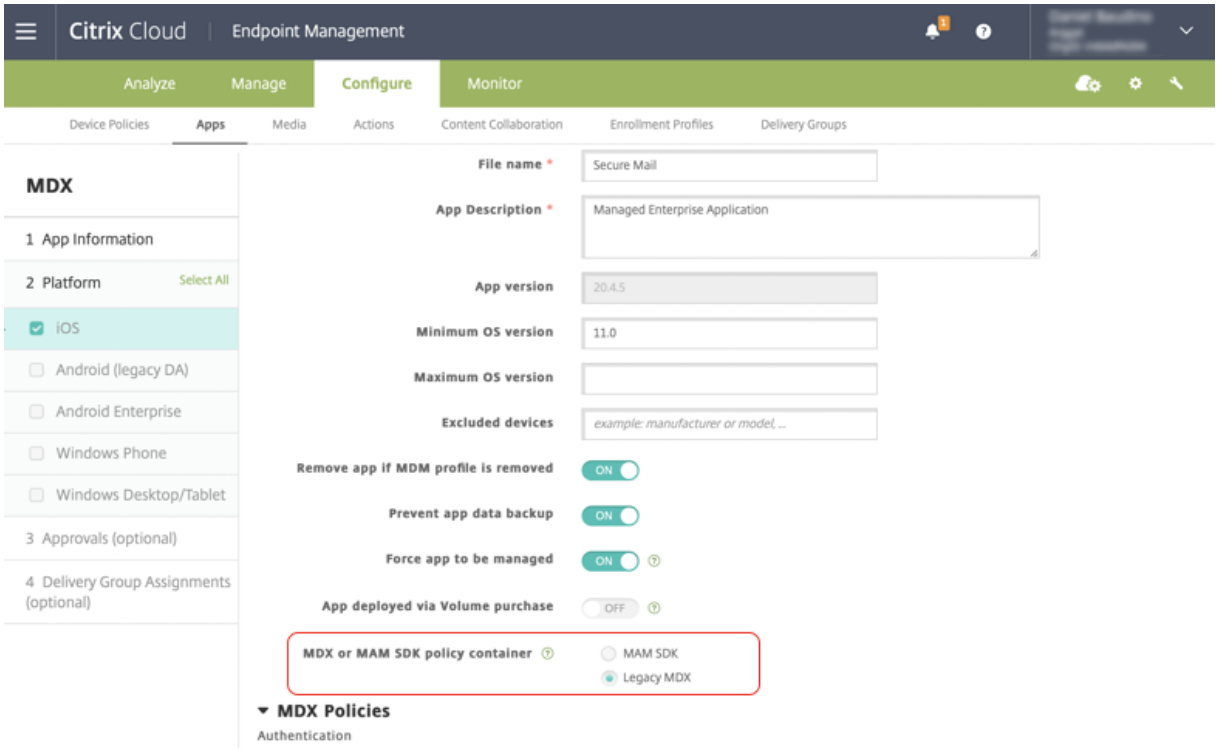
Dual mode for Secure Web

The mobile application management (MAM) SDK is available to replace areas of MDX functionality that aren't covered by the iOS platform. The MDX wrapping technology is scheduled to reach end of life (EOL) in March 2022.

Citrix Secure Web is released with both the MDX and MAM SDK frameworks to prepare for the MDX EOL, scheduled for March 2022. To continue managing your enterprise applications, you must incorporate the MAM SDK. Citrix recommends that you switch to **MAM SDK**. The dual mode functionality is intended to provide a way to transition the Secure Web app to the new MAM SDK model.

The dual mode functionality allows you to either continue managing apps using MDX (now **Legacy MDX**) or switch to the new **MAM SDK**. You get the following options for policy settings in the **MDX or MAM SDK policy container**:

- **MAM SDK**
- **Legacy MDX**



In the **MDX or MAM SDK policy container** policy, you can change your option from **Legacy MDX** to **MAM SDK**.

It is recommended that you don't switch from **MAM SDK** to **Legacy MDX** as this requires you to reinstall the app. The default value is **Legacy MDX**. Ensure that you set the same policy mode for both Secure Mail and Secure Web running on a device. You cannot have two different modes running on the same device.

When you select **MAM SDK** mode, the apps automatically switch to the MAM SDK framework and the device policies are refreshed without any further action from the administrators.

> **Note:**
>
> When you switch from the **Legacy MDX** to **MAM SDK** framework, the **Network access** policy must be modified to either **Tunneled – Web SSO** or **Unrestricted**

Prerequisites

For a successful deployment of the dual mode feature, ensure that the following requirements are met:

- Update your Citrix Endpoint Management to versions 10.12 RP2 or later, or 10.11 RP5 or later.
- Update your mobile apps to version 21.8.0 or later.
- If your organization uses third-party apps, ensure that you incorporate the MAM SDK into your third-party apps before you switch to the MAM SDK framework. All of your managed apps must

be moved to MAM SDK at one time.

Limitations

- MAM SDK only supports only platform-based encryption, and not MDX encryption.
- Duplicate policy entries are created for Secure Web if you don't update Citrix Endpoint Management to version 10.12 RP2 or later, or 10.11 RP5 or later, and the policy files are running on version 21.8.0 or later.
- When you switch to the MAM SDK mode of app management, some features are not supported or are unavailable. Also, interoperation between apps in different modes is not supported for actions such as Open-in and Copy/Paste. For example, you can't copy content from an app that is managed in the **Legacy MDX** mode into an app that is managed in the **MAM SDK** mode or vice versa. See the following table for the features that are not available in the MAM SDK mode:

Feature	Legacy MDX	MAM SDK
Shared devices	Yes	No
Intune	Yes	No
SMIME Shared Certificate vault	Yes	No
Derived credentials	Yes	No
UIWebView Tunneling	Yes	No
Full VPN	Yes	No

- The following policies are deprecated and are not available in the MAM SDK mode:
  - Allowed Secure Web domains
  - Allowed Wi-Fi networks
  - Alternate Citrix Gateway
  - Certificate label
  - Citrix reporting
  - Explicit logoff notification
  - micro VPN session required
  - micro VPN session required grace period (minutes)
  - Report file cache maximum
  - Require Wi-Fi
  - Send reports over Wi-Fi only
  - Upload token

Note:

> If you are using a client certificate for authenticating to internal servers, the client certification should be the same as the one used in the Access Gateway.

For more information about MAM SDK, see the following articles:

- MAM SDK Overview
- Citrix Developer documentation about Mobile Application Integration
- Citrix blog post
- Download SDK when you sign on to Citrix downloads

Secure Web for Android

This release includes bug fixes.

Secure Web 21.7.0

Secure Web for iOS

This release includes bug fixes.

Secure Web for Android

This release includes bug fixes.

Secure Web 21.6.0

Secure Web for iOS

This release includes bug fixes.

Secure Web for Android

This release includes bug fixes.

Secure Web for iOS 21.5.0

This release includes bug fixes.

Secure Web for Android 21.4.5

This release includes bug fixes.

Secure Web 21.3.5

Secure Web for Android

This release includes bug fixes.

Secure Web 21.3.0

Secure Web for Android

This release includes bug fixes.

Secure Web 21.2.0

Secure Web for iOS

Color revamp for Secure Web. Secure Web is compliant with Citrix brand color updates.

Secure Web for Android

- **Color revamp for Secure Web.** Secure Web is compliant with Citrix brand color updates.
- **Steady functioning on foldable devices.** Secure Web for Android includes fixes for steady functioning on foldable devices.

Secure Web 21.1.5

Secure Web for iOS

This release includes bug fixes.

Secure Web 21.1.0

This release includes bug fixes.

Secure Web 20.12.0

Secure Web for iOS

This release includes bug fixes.

Secure Web 20.11.0

This release includes bug fixes.

Secure Web 20.10.5

Secure Web for Android

Support for AndroidX libraries. As per Google's recommendation, Secure Web supports the **AndroidX** libraries, which are a replacement for the **android.support**-packaged libraries.

Secure Web 20.10.0

Secure Web for Android

Secure Web supports Google Play's current target API requirements for Android 10.

Secure Web 20.9.5

Secure Web for iOS

This release includes bug fixes.

Secure Web 20.9.0

Secure Web for Android

> **Note:**
>
> Support for Android 6.x ended on September 15, 2020.

Secure Web 20.8.5

Secure Web for Android

Secure Web for Android supports Android 11.

Secure Web 20.8.0

Secure Web for Android

Dual mode for Android release of Secure Web. A mobile application management (MAM) SDK is available to replace areas of MDX functionality that aren't covered by iOS and Android platforms. The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. To continue managing your enterprise applications, you must incorporate the MAM SDK.

From version 20.8.0, Android apps are released with the MDX and MAM SDK to prepare for the MDX EOL strategy mentioned earlier. The MDX dual mode is intended to provide a way to transition to new MAM SDKs from the legacy MDX Toolkit. Using the dual mode feature allows you to either continue

managing apps using the MDX Toolkit (now **Legacy MDX**) or switch to the new MAM SDK for app management.

Once you switch to the MAM SDK for app management, Citrix implements further changes and it does not require any action from the administrators.

For more details about the MAM SDK, see the following articles:

- MAM SDK Overview
- Citrix Developer section on Device Management
- Citrix blog post
- Download SDK when you sign on to Citrix downloads

Prerequisites

For a successful deployment of the dual mode feature, ensure the following:

- Update your Citrix Endpoint Management to versions 10.12 RP2 and later, or 10.11 RP5 and later.
- Update your mobile apps to version 20.8.0 or later.
- Update the policies file to version 20.8.0 or later.
- If your organization uses third-party apps, ensure to incorporate the MAM SDK into these apps before switching to the MAM SDK option for your Citrix mobile productivity apps. All of your managed apps must be moved to the MAM SDK at one time.

> **Note:**
>
> MAM SDK is supported for all cloud-based customers.

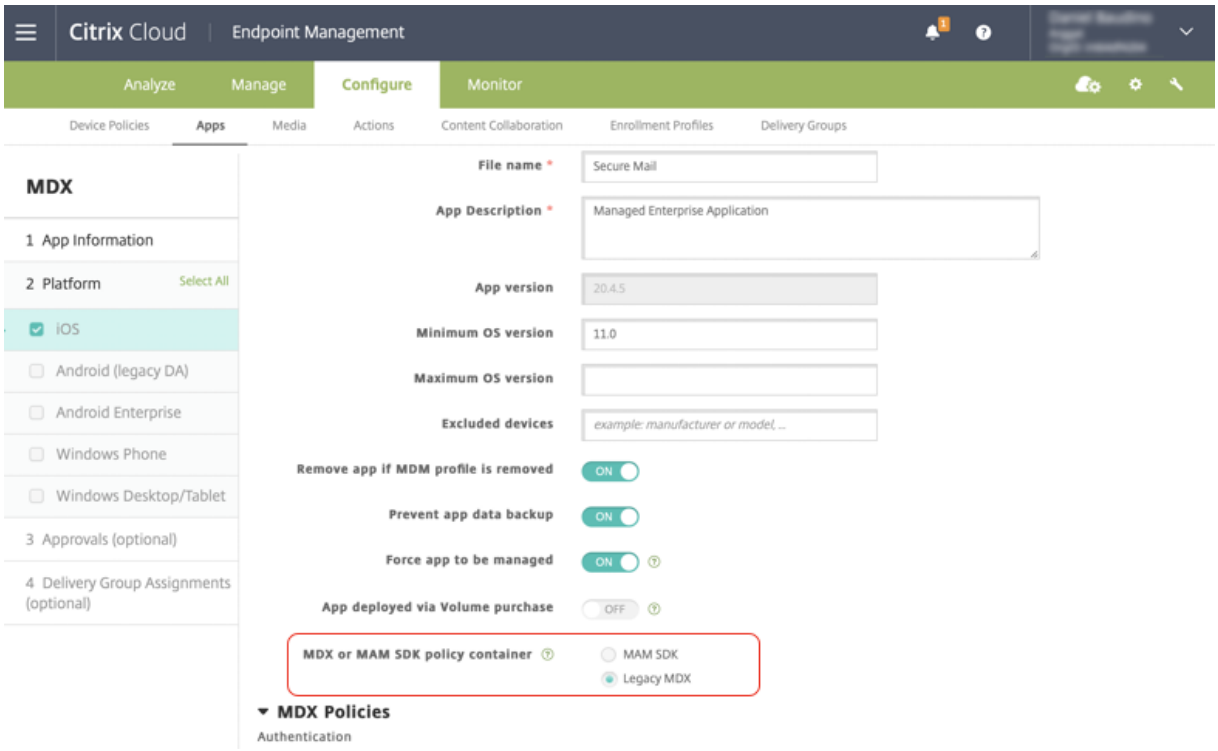
Limitations

- MAM SDK is only supported for apps published under the Android Enterprise platform on your Citrix Endpoint Management deployment. For the newly published apps, the default encryption is platform-based encryption.
- MAM SDK only supports platform-based encryption, and not MDX encryption.
- If you don't update Citrix Endpoint Management, and the policy files are running on version 20.8.0 and later for the mobile apps, then duplicate entries of the Networking policy are created for Secure Web.

When you configure Secure Web in Citrix Endpoint Management, the dual mode feature allows you to either continue managing apps using the MDX Toolkit (now **Legacy MDX**) or switch to the new **MAM SDK** for app management. Citrix recommends that you switch to **MAM SDK**, as MAM SDKs are more modular and are intended to allow you to use only a subset of the MDX functionality that your organization uses. It reduces the overall in-binary and runtime footprint of an app.

You get the following options for policy settings in the **MDX or MAM SDK policy container**:

- **MAM SDK**
- **Legacy MDX**



In the **MDX or MAM SDK policy container** policy, you can only change your option from **Legacy MDX** to MAM SDK. The option to switch from MAM SDK to **Legacy MDX** is not allowed, and you need to republish the app. The default value is MDX Legacy. Ensure that you set the same policy mode for both Secure Mail and Secure Web running on the same device. You cannot have two different modes running on the same device.

Secure Web 20.7.5

This release includes bug fixes.

Secure Web 20.7.0

Support for Multitasking. In Secure Web for iOS, use two apps simultaneously with Multitasking. To enable this feature, drag an app out of the Dock. Slide it to the right or left edge of the screen to split and enable the screen for two apps.

For latest information on mobile productivity apps, see the article Recent announcements.

Secure Web 20.6.0

This release includes bug fixes.

Secure Web 20.5.0

This release includes bug fixes.

Secure Web 20.4.5

Navigate to bookmarks in new tabs. In Secure Web for iOS, you can view, edit, and navigate to bookmarks when you open a new tab.

Secure Web 19.10.5 to 20.4.0

These releases include bug fixes.

Secure Web 19.10.0

Secure Web iOS and Android support encryption management. Encryption management allows you to use modern device platform security while also ensuring the device remains in a sufficient state to use platform security effectively. By using encryption management, you eliminate local data encryption redundancy since file system encryption is provided by the respective iOS or Android platform. To enable this feature, an admin must configure the **Encryption type** MDX policy to **Platform encryption with compliance enforcement** in the Citrix Endpoint Management console.

Encryption management allows you to use modern device platform security while also ensuring the device remains in a sufficient state to use platform security effectively. By using encryption management, you eliminate local data encryption redundancy since file system encryption is provided by the iOS or Android platform. To enable this feature, an admin must configure the **Encryption type** MDX policy to **Platform encryption with compliance enforcement** in the Citrix Endpoint Management console.

Encryption type

To use the encryption management feature, in the Citrix Endpoint Management console, set the **Encryption type** policy to **Platform encryption with compliance enforcement**. This enables encryption management and all the existing encrypted application data on users' devices seamlessly transition to a state that is encrypted by the device and not by MDX. During this transition, the app is paused for a one-time data migration. Upon successful migration, responsibility for encryption of locally stored data is transferred from MDX to the device platform. MDX continues to check compliance of the device upon each app launch. This feature works in both MDM + MAM and MAM-only environments.

When you set the **Encryption type** policy to **Platform encryption with compliance enforcement**, the new policy supersedes your existing MDX Encryption.

For details about the encryption management MDX policies for Secure Web, see the **Encryption** section in:

- MDX policies for mobile productivity apps for iOS
- MDX policies for mobile productivity apps for Android

Non-compliant device behavior

When a device falls below the minimum compliance requirements, the **Non-compliant device behavior** policy allows you to select what action is taken:

- **Allow app** – Allow the app to run normally.
- **Allow app after warning** – Warn the user that an app does not meet the minimum compliance requirements and allows the app to run. This is the default value.
- **Block app** – Block the app from running.

The following criteria determine whether a device meets the minimum compliance requirements.

Devices running iOS:

- iOS 10: An app is running operation system version that is greater than or equal to the specified version.
- Debugger access: An app does not have debugging enabled.
- Jailbroken device: An app is not running on a jailbroken device.
- Device passcode: Device passcode is ON.
- Data sharing: Data sharing is not enabled for the app.

Devices running Android:

- Android SDK 24 (Android 7 Nougat): An app is running an operation system version that is greater than or equal to the specified version.
- Debugger Access: An app does not have debugging enabled.
- Rooted devices: An app is not running on a rooted device.
- Device lock: Device passcode is ON.
- Device encrypted: An app is running on an encrypted device.

Secure Web 19.9.5

This release includes bug fixes.

Secure Web 19.9.0

Secure Web for iOS

Secure Web for iOS supports iOS 13.

Secure Web for Android

This release includes bug fixes.

Secure Web for Android 19.8.5

Secure Web for Android supports Android Q.

Secure Web 19.8.0

This release includes bug fixes.

Secure Web 19.7.5

Secure Web for iOS

This release includes performance enhancements and bug fixes.

Secure Web for Android

From this release, Secure Web for Android is only supported on devices running Android 6 or later.

Secure Web 19.3.0 to 19.6.5

These releases include performance enhancements and bug fixes.

Secure Web 19.2.0

Allow links to open in Secure Web keeping data secure. With Secure Web, a dedicated VPN tunnel allows users to access sites with sensitive information securely. This feature was already available for Secure Web for iOS. This release adds support for Android. For more details, see Secure Web features.

Secure Web versions 18.11.5 to 19.1.5

These releases include performance enhancements and bug fixes.

Secure Web 18.11.0

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

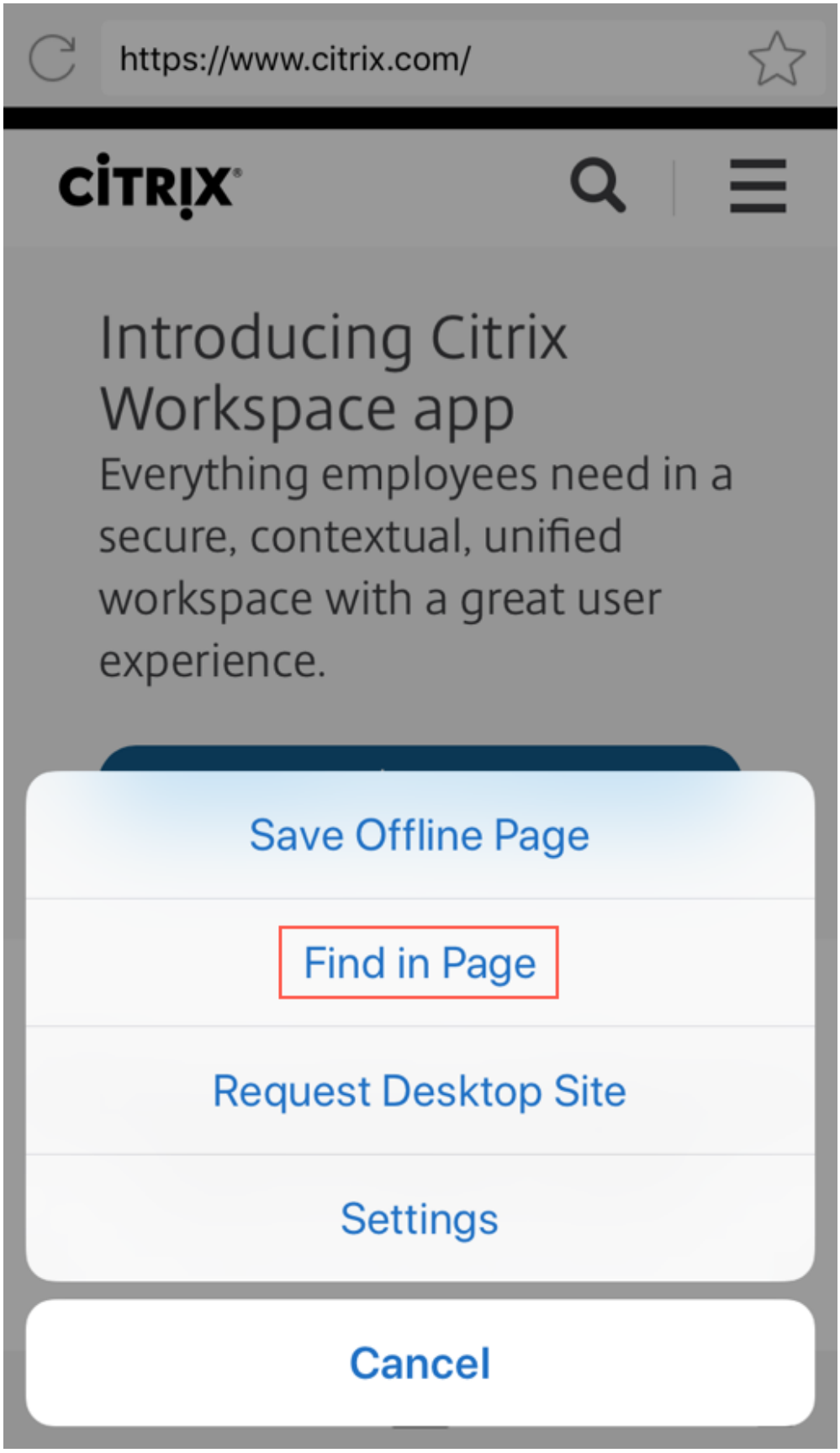
Secure Web 18.9.0 to 18.10.5

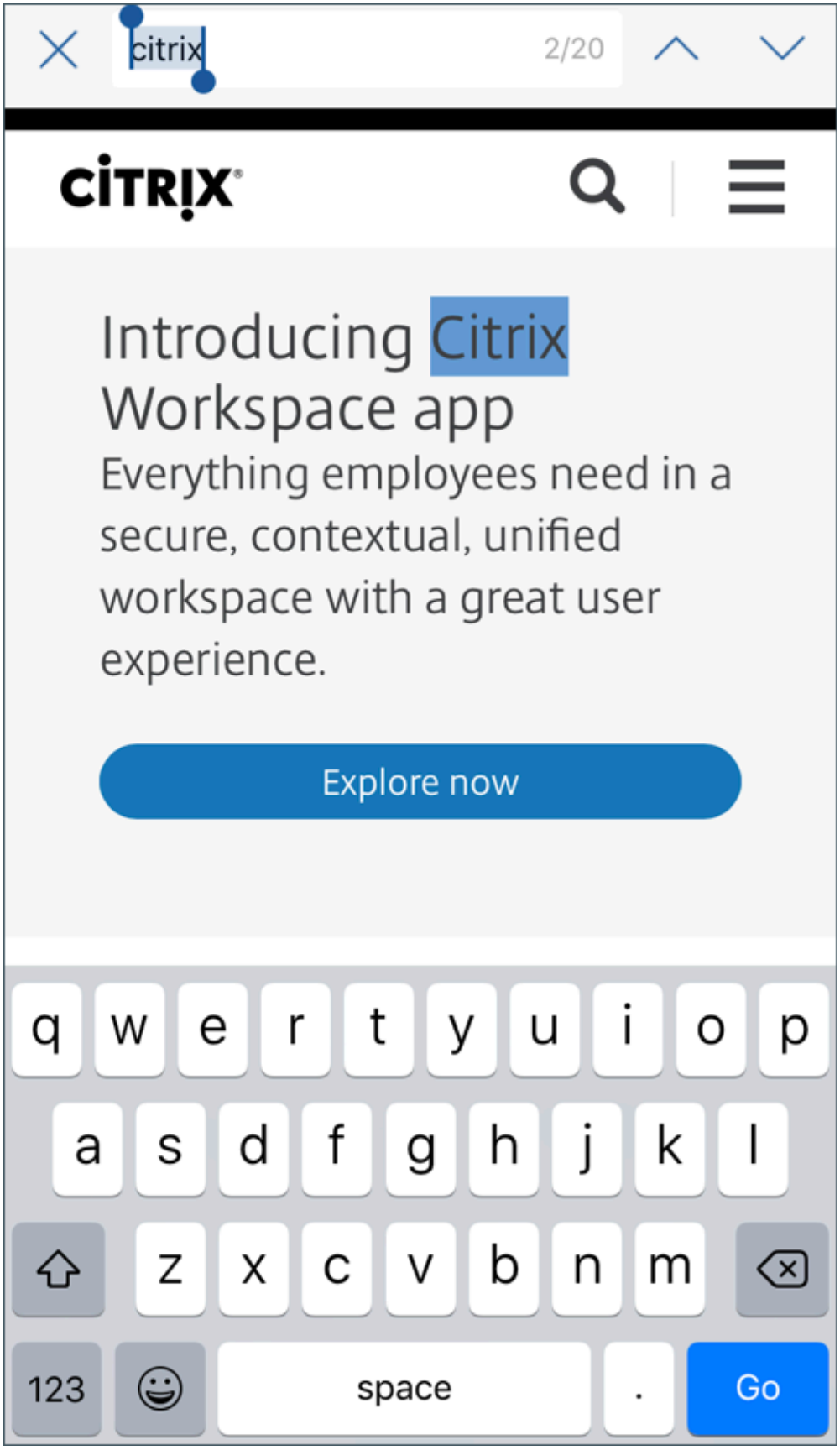
These releases include performance enhancements and bug fixes.

Secure Web 10.8.65

The following features are 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 webpages.

Secure Web 10.8.60

- Support for Polish language

Secure Web 10.8.35

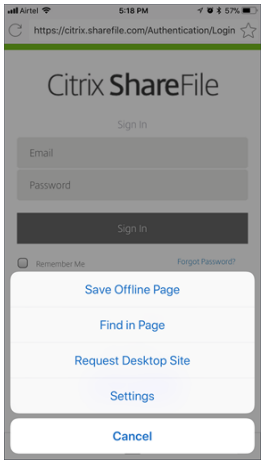
- **Pull to refresh.** In Secure Web for Android, users can use the pull to refresh feature to update their data on the screen.

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 website.

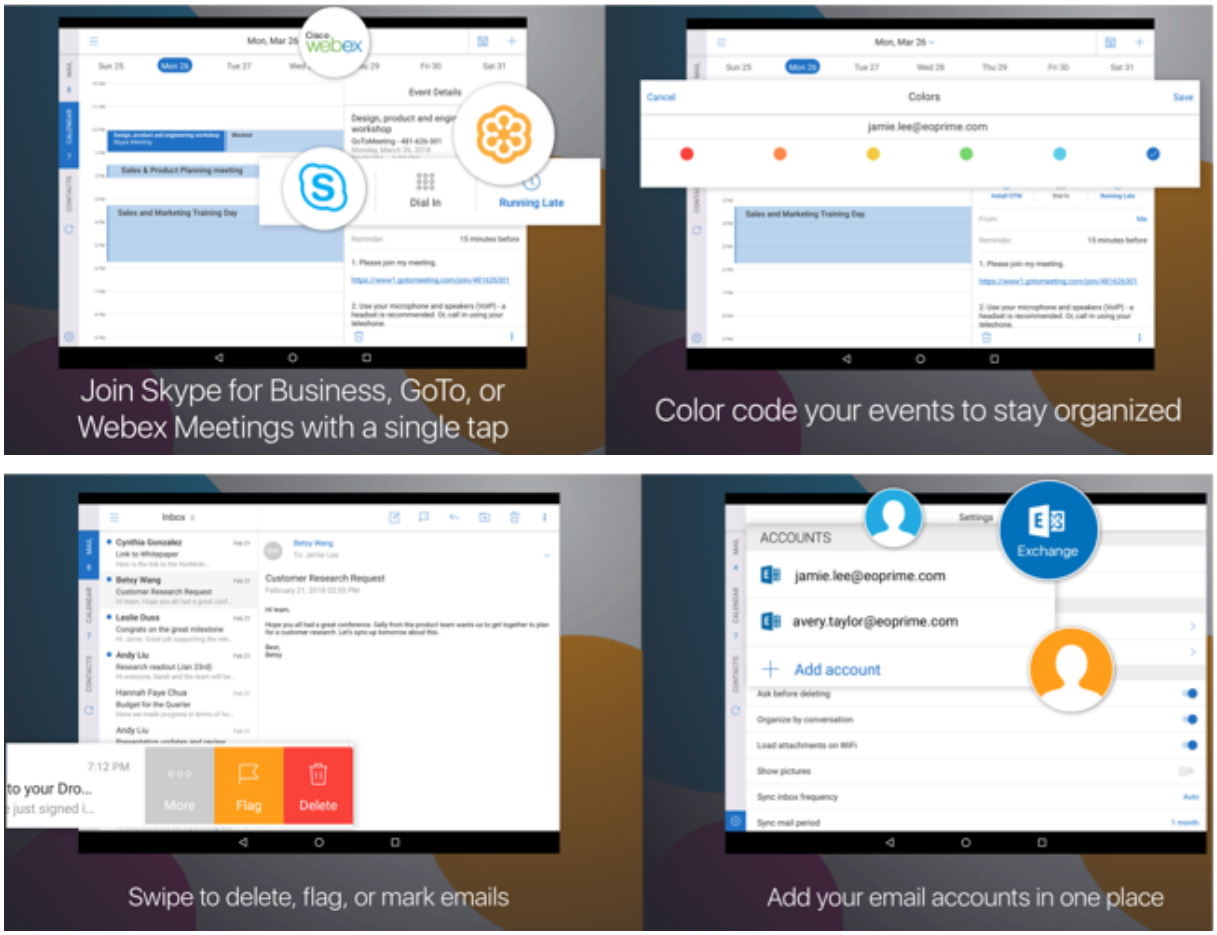
Secure Web 10.8.10

- **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 website.



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

October 27, 2021

Citrix supports upgrades from the last two versions of the mobile productivity apps.

Secure Web 21.10.5

Known issue in Secure Web 21.10.5

There are no known issues in this release.

Fixed issues in Secure Web 21.10.5

- When you click the back button on your device to go to the previous page, while viewing certain webpages in Secure Web for Android, the following error occurs: “net::ERR_CACHE_MISS” [CXM-96447]
- In Secure Web for Android, clicking hyperlinks in intranet websites opens a Google Search page instead of opening the intranet website. [CXM-100749]

Secure Web 21.10.0

There are no known or fixed issues in this release.

Secure Web 21.9.1

There are no known or fixed issues in this release.

Known and fixed issues in older versions

For known and fixed issues in older versions of Secure Web, see Known and fixed issues in older versions.

Integrating and deploying Secure Web

March 17, 2021

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 in addition to iOS and Android devices.

> **Note:**
>
> The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. To continue managing your enterprise applications, you must incorporate the MAM SDK.
> The Full VPN tunnel is not supported in Legacy MDX mode.

- 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, do the following:

1. Navigate to **Policies > Session** policy.

2. Select the Secure Hub policy and then navigate to **Client Experience > Split Tunnel**.
3. Select **REVERSE**.

The Reverse Split Tunnel Mode Exclusion list MDX policy

You configure the Reverse Split Tunnel Mode policy with the Exclusion range from within Citrix Endpoint Management. 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 LAN (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

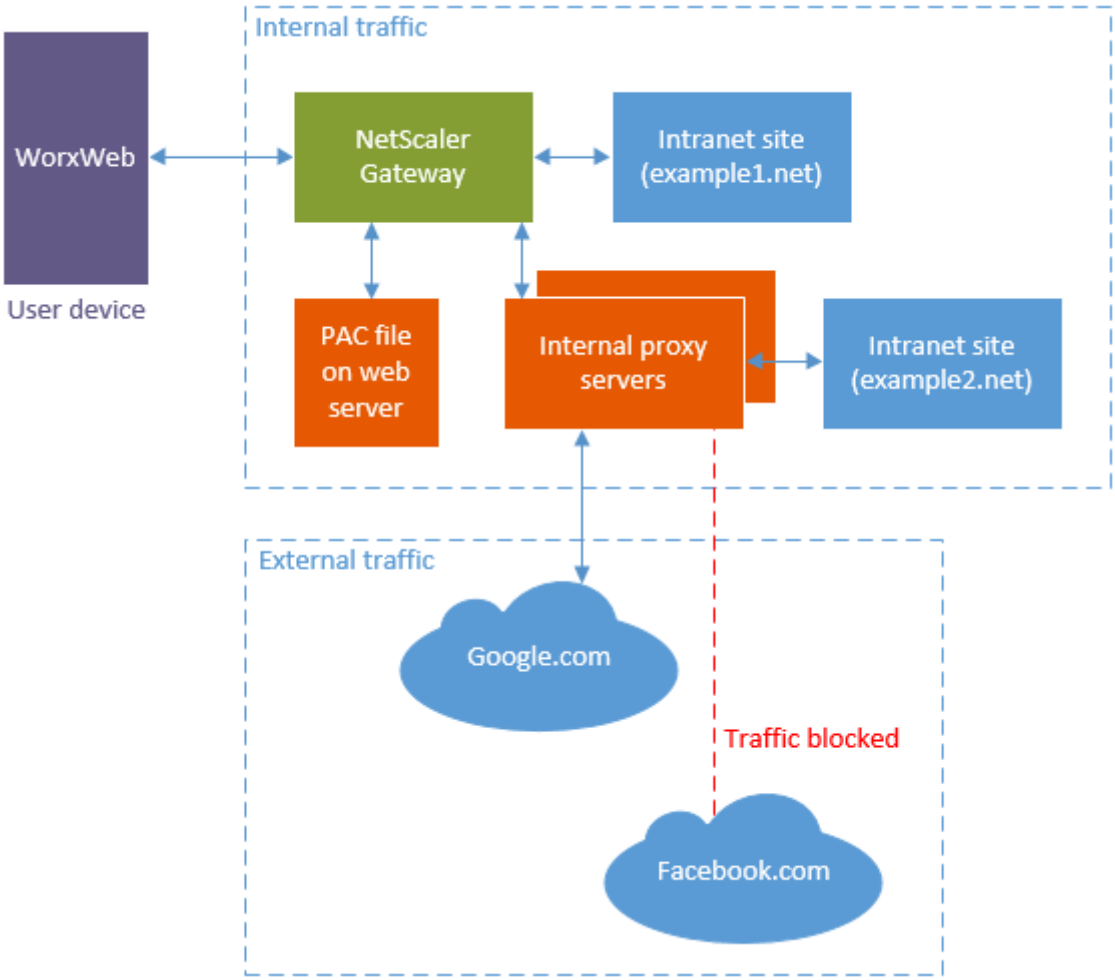
Full VPN Tunneling with PAC

> 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 website:



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, go to *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.

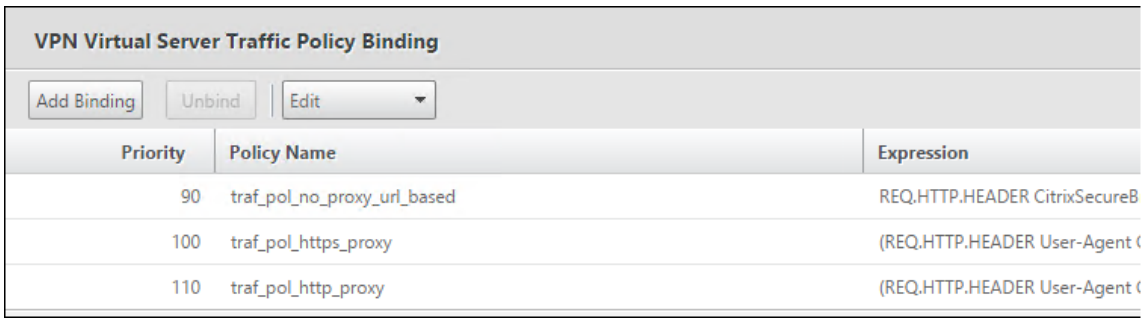
```
https://webserver.local/GenericPAC.pac
https://webserver.local/GenericPAC.pac
```

Tested PAC extensions are .txt or .pac.

The PAC file must display 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 Gateway split 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 in addition to 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 Wi-Fi.

- 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 host name. 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 cannot 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 a folder name, friendly name, and web address. Each triplet must be of the form folder, name, url where folder and name might 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 might 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 WkWebView to provide web technology support. Some of the web technologies supported by Secure Web are:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets (only in unrestricted mode)

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	Secure Web for iOS	Secure Web for Android
JavaScript engine	JavaScriptCore	V8
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 webpage 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 webpage 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.

Verify SSL connectivity

Ensure that the SSL certificate chain is properly configured. You can check for missing Root or Intermediate CAs that are not linked or installed on mobile devices by using the SSL Certificate Checker.

Many server certificates are signed by multiple hierarchical Certificate Authorities (CA), which means that the certificates form a chain. You must link these certificates. For information about installing or linking your certificates, see Install, link, and update certificates.

To create a web archive file

By using Safari on macOS 10.9 or later, you can save a webpage as a web archive file (referred to as a reading list). The web archive file 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/. Now delete all 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 website you want to 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 website from the reading list.

     The website renders completely.
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 Secure Mail with no additional authentication required.
- **Allow links to open in Secure Web keeping data secure**. With Secure Web for iOS and Android, a dedicated VPN tunnel allows users to access sites with sensitive information securely. They can click links from Secure Mail, from within Secure Web, or from a third-party app. The link opens in Secure Web, and the data is securely contained. Users can open an internal link that has the ctxmobilebrowser scheme in Secure Web. In doing so, Secure Web transforms the `ctxmobilebrowser://` prefix to `http://`. To open an HTTPS link, Secure Web transforms `ctxmobilebrowsers://` to `https://`.

This feature depends on an App Interaction MDX policy called **Inbound Document Exchange**. The policy is set to **Unrestricted** by default. This setting allows URLs to open in Secure Web. You can

change the policy setting so that only apps that you include in an allow list can communicate with Secure Web.

- 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:

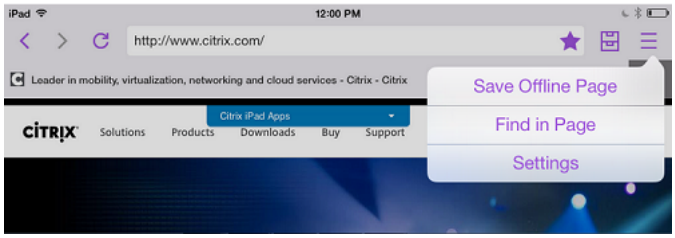
- Block pop-ups.

  > 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

February 7, 2019

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 Endpoint Management: 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 Endpoint Management: 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.

Secure Web features

June 18, 2020

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 Secure Mail with no additional authentication required.
- **Allow links to open in Secure Web keeping data secure**. With Secure Web for iOS and Android, a dedicated VPN tunnel allows users to access sites with sensitive information securely. They can click links from Secure Mail, from within Secure Web, or from a third-party app. The link opens in Secure Web, and the data is securely contained. Users can open an internal link that has the ctxmobilebrowser(s) scheme in Secure Web. In doing so, Secure Web transforms the `ctxmobilebrowser://` prefix to `http://`. To open an HTTPS link, Secure Web transforms `ctxmobilebrowsers://` to `https://`.

This feature depends on an App Interaction MDX policy called **Inbound Document Exchange**. The policy is set to **Unrestricted** by default. This setting allows URLs to open in Secure Web. You can change the policy setting so that only apps that you include in an allow list can communicate with Secure Web.

- 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.

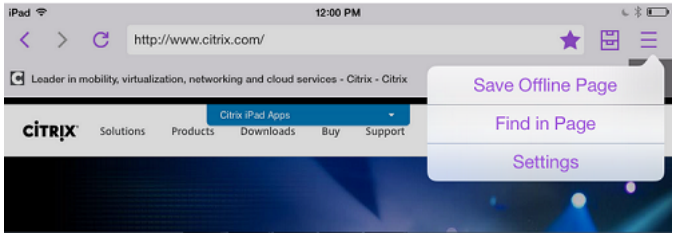
  > Note:
  >
  > Much of Secure Web memory goes into rendering pop-ups, so performance is often improved by blocking pop-ups in Settings.

- 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.

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