# Mobile productivity apps

## Contents



# Mobile productivity apps release timeline

July 4, 2024

Citrix mobile productivity apps release is a two-week cadence. Although exact dates may change, knowing this cadence can help you plan ahead. We also want to make it easier for you to manage app deployments and updates.

## About the Secure Mail and Secure Web phased release process

When new versions of Secure Mail and Secure Web are available, the releases are rolled out in a phased approach as follows:

- For iOS and Android users, Secure Mail and Secure Web updates are available in the App Store and Google Play store for an increasing percentage of users over the course of a week (seven days).
- New downloads of Secure Mail and Secure Web for iOS get the new version within this week. New downloads of Secure Mail and Secure Web for Android will run the previous version for the week, until the rollout of the new release reaches 100 percent of all users.
- For users, some features release in gradual phases.

## Prerequisites for feature flag management

If an issue occurs with Secure Hub or Secure Mail in production, we can disable an affected feature within the app code. To do so, we use feature flags and a third-party service called LaunchDarkly. You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements. For details about support in MDX since mobile productivity apps 10.6.15 for the exclusion of domains from tunneling, see the MDX Toolkit documentation. For a FAQ about feature flags and LaunchDarkly, see this Support Knowledge Center article

> **Note:**
> For advanced notice of Citrix Endpoint Management features that are being phased out, see Deprecation.

# Support for mobile productivity apps

January 17, 2024

Users who have automatic updates enabled receive the latest version from the app store. The latest version of the mobile productivity apps is as follows:

- 23.10.0 (Secure Web for Android)
- 23.9.0 (Secure Mail and Secure Web for iOS)
- 23.8.2 (Secure Mail for Android)

Citrix supports upgrades from the last two versions of the mobile productivity apps. The last two versions of the mobile productivity apps are as follows:

- 23.8.1 (Secure Mail for Android)
- 23.8.0 (Secure Web for Android)
- 23.7.0 (Secure Mail for Android, and Secure Mail for iOS)
- 23.5.0 (Secure Mail for iOS, and Secure Web for Android)
- 23.2.0 (Secure Web for iOS)
- 22.9.1 (Secure Web for iOS)

> **Important:**
>
> MDX encryption reached end of life (EOL) on September 1, 2020. For devices enrolled in legacy device administration (DA):
>
> - If you don't use MDX encryption, no action is needed.
> - If you use MDX encryption, migrate your Android devices to Android Enterprise. Devices running Android 10 must enroll or re-enroll using Android Enterprise. This includes Android devices in MAM-only mode. See Migrate device administration to Android Enterprise for details.

## Supported operating systems

Mobile productivity apps support the following operating systems:

| Product name | Operating system | Minimum deployment version | Latest version available |
|---|---|---|---|
| Secure Hub | Android | 7.x | 14.x |
| | iOS | 12.x | 17.x |
| Secure Mail | Android | 8.x | 14.x |

| Product name | Operating system | Minimum deployment version | Latest version available |
|---|---|---|---|
| Secure Web | iOS | 13.x | 17.x |
| | Android | 8.x | 14.x |
| | iOS | 13.x | 17.x |

The latest versions of Mobile productivity apps are compatible with the latest and two prior versions of Citrix Endpoint Management. For more information on the operating systems supported by Citrix Endpoint Management, see Supported device operating systems.

The latest version of Mobile productivity apps requires the latest version of Secure Hub. Ensure you keep Secure Hub up to date.

> **Note:**
>
> At any point in time, Citrix supports only the latest and the previous two versions (N, N-1, and N-2) of Android and iOS operating systems.

## Other considerations and limitations

For advanced notice of Citrix Endpoint Management features that are being phased out, see Deprecation.

### Secure Mail

- Endpoint Management currently doesn't support NetScaler 12.0.41.16 due to an issue with Secure Ticket Authority (STA) and Secure Mail. The issue is fixed in NetScaler 12.0 build 41.22.
- Support in Secure Mail for Exchange 2007 and Lotus Notes 8.5.3 reached End of Life (EOL) on September 30, 2017.
- For the best performance when sending Citrix Files attachments, the latest versions of Citrix Files are recommended. Citrix Files is not supported for Windows.
- In IBM Notes environments, you must configure the IBM Domino Traveler server, version 9.0. For details, see Integrating Exchange Server or IBM Notes Traveler Server.

> **Note:**
>
> - Citrix Files for XenMobile has reached EOL on July 1, 2023. For more information, see EOL and deprecated apps

#### Secure Web

Install the latest version of Android WebView on devices. Users can download Android WebView from the Google Play Store.

#### QuickEdit

QuickEdit remains available as a mobile productivity app. The End of Life (EOL) status is not applied on September 1, 2018 as communicated earlier.

#### Citrix Content Collaboration for Endpoint Management

Users access Citrix Content Collaboration for Endpoint Management from the public app stores after version 6.5.

#### ShareConnect

ShareConnect reached End of Life (EOL) on June 30, 2020. For details, see EOL and deprecated apps.

#### Citrix Secure Notes and Citrix Secure Tasks

Citrix Secure Notes and Citrix Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.

## Administrator tasks and considerations

June 13, 2024

This article discusses the tasks and considerations that are relevant for administrators of mobile productivity apps.

### Feature flag management

If an issue occurs with a mobile productivity app in production, we can disable an affected feature within the app code. We can disable the feature for Secure Hub, Secure Mail, and Secure Web for iOS and Android. To do so, we use feature flags and a third-party service called LaunchDarkly. You do not

need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements. For details about support since for the exclusion of domains from tunneling, see the MAM SDK documentation.

You can enable traffic and communication to LaunchDarkly in the following ways:

#### Enable traffic to the following URLs

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

#### Create an allow list by domain

Earlier, we offered a list of IP addresses to use when your internal policies require only IP addresses to be listed. Now, because Citrix has made infrastructure improvements, we are phasing out the public IP addresses starting on July 16, 2018. We recommend that you create an allow list by domain, if you can.

#### List IP addresses in an allow list

If you must list IP addresses in an allow list, for a list of all current IP address ranges, see this LaunchDarkly public IP list. You can use this list to ensure that your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Statuspage.

> Note:
>
> Public app store apps require a fresh installation the first time you deploy them. It is not possible to upgrade from the current enterprise wrapped version of the app to the public store version.
>
> With public app store distribution, you do not sign and wrap Citrix-developed apps with the MDX Toolkit. You can use the MDX Toolkit to wrap third-party or enterprise apps.

#### LaunchDarkly system requirements

- Endpoint Management 10.7 or later.
- Ensure that the apps can communicate with the following services if you have split tunneling on Citrix ADC set to **OFF**:

  - LaunchDarkly service
  - APNs listener service

## Supported app stores

Mobile productivity apps are available on the Apple App Store and Google Play.

In China, where Google Play is unavailable, Secure Hub for Android is available on the following app stores:

- https://shouji.baidu.com
- http://apk.hiapk.com
- https://apk.91.com

### Enabling public app store distribution

1. Download public-store .mdx files for both iOS and Android from the Endpoint Management downloads page.
2. Upload the .mdx files to the Endpoint Management console. The public store versions of the mobile productivity apps are still uploaded as MDX applications. Do not upload the apps as public store apps on the server. For steps, see Add apps.
3. Change policies from their defaults based on your security policies (optional).
4. Push the apps as required apps (optional). This step requires your environment to be enabled for mobile device management.
5. Install apps on the device from the App Store, Google Play, or the Endpoint Management app store.

   - On Android, the user is directed to the Play Store to install the app. On iOS, in deployments with MDM, the app installs without the user being taken to the app store.
   - When the app is installed from the App Store or Play Store, the following action occurs. The app transitions to a managed app as long the corresponding .mdx file has been uploaded to the server. When transitioning to a managed app, the app prompts for a Citrix PIN. When users enter the Citrix PIN, Secure Mail displays the account configuration screen.

6. Apps are accessible only if you're enrolled in Secure Hub and the corresponding .mdx file is on the server. If either condition is not met, users can install the app, but usage of the app is blocked.

If you currently use apps from the Citrix Ready Marketplace that are on public app stores, you're already familiar with the deployment process. Mobile productivity apps adopt the same approach that many ISVs currently use. Embed the MDX SDK within the app to make the app public-store ready.

> Note:
>
> The public store versions of the Citrix Files app for both iOS and Android are now universal. The Citrix Files app is the same for phones and tablet.

### Apple push notifications

For more information on configuring push notifications, see Configuring Secure Mail for Push Notifications.

### Public app store FAQs

- Can I deploy multiple copies of the public store app to different user groups? For example, I want to deploy different policies to different user groups.

  Upload a different .mdx file for each user group. However, in this case, a single user cannot belong to multiple groups. If users did belong to multiple groups, multiple copies of the same app are assigned to that user. Multiple copies of a public store app cannot be deployed to the same device, because the app ID can't be changed.

- Can I push public store apps as required apps?

  Yes. Pushing apps to devices requires MDM; it's not supported for MAM-only deployments.

- Do I update any traffic policies or Exchange Server rules that are based on the user agent?

  Strings for any user agent-based policies and rules by platform are as follows.

  > Important:
  >
  > Secure Notes and Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.

#### Android

| App | Server | User-agent string |
|---|---|---|
| Citrix Secure Mail | Exchange | WorxMail |
| | Lotus Notes Traveler | Apple - iPhone WorxMail |
| Citrix Secure Web | | WorxMail |
| Citrix Secure Tasks | Exchange | WorxMail |
| Citrix Secure Notes | Exchange | WorxMail |

| App | Server | User-agent string |
|---|---|---|
| | Citrix Files | Secure Notes |

### iOS

| App | Server | User-agent string |
|---|---|---|
| Citrix Secure Mail | Exchange | WorxMail |
| | Lotus Notes Traveler | Apple - iPhone WorxMail |
| Citrix Secure Web | | com.citrix.browser |
| Citrix Secure Tasks | Exchange | WorxTasks |
| Citrix Secure Notes | Exchange | WorxNotes |
| | Citrix Files | Secure Notes |

- Can I prevent app upgrades?

  No. When an update is posted on the public app store, any users who have auto updates enabled receive the update.

- Can I enforce app upgrades?

  Yes, upgrades are enforced via the Upgrade grace period policy. This policy is set when the new .mdx file corresponding to the updated version of the app is uploaded to Endpoint Management.

- How do I test the apps before the update reaches users if I can't control the update timelines?

  Similar to the process for Secure Hub, the apps are available for testing on TestFlight for iOS during the EAR period. For Android, the apps are available via the Google Play beta program during the EAR period. You can test app updates during this time.

- What happens if I don't update the new .mdx file before the automatic update reaches user devices?

  The updated app remains compatible with the older .mdx file. Any new features that depend on a new policy are not enabled.

- Will the app transition to managed if Secure Hub is installed or does the app need to be enrolled?

  Users must be enrolled in Secure Hub for the public store app to activate as a managed app (secured by MDX) and to be usable. If Secure Hub is installed, but not enrolled, the user cannot use the public store app.

- Do I need an Apple Enterprise developer account for the public store apps?

  No. Because Citrix is now maintaining the certificates and provisioning profiles for mobile productivity apps, an Apple Enterprise developer account is not required to deploy the apps to users.

- Does the end of enterprise distribution apply to any wrapped application I have deployed?

  No, it applies only to the mobile productivity apps: Secure Mail, Secure Web, and Citrix Content Collaboration for Endpoint Management, QuickEdit, and ShareConnect. Any enterprise wrapped apps you deployed that are developed in-house or by third parties can continue to use enterprise wrapping. The MDX Toolkit continues to support enterprise wrapping for app developers.

- When I install an app from Google Play, I get an Android error with error code 505.

  > Note:
  >
  > Support for Android 5.x ended on December 31, 2018.

  This is a known issue with Google Play and Android 5.x versions. If this error occurs, you can follow these steps to clear stale data on the device that prevents installation of the app:

1. Restart the device.
2. Clear the cache and data for Google Play through device settings.
3. As a last resort, remove and then add back the Google account on your device.

For more information, search this site using the following keywords "Fix Google Play Store Error 505 in Android: Unknown Error Code"

- Although the app on Google Play has been released to production and a new beta release is not available, why do I see Beta after the app title on the Google Play?

  If you are part of our Early Access Release (EAR) program, you always see Beta next to the app title. This name simply notifies users of their access level for a particular app. The Beta name indicates that users receive the most recent version of the app available. The most recent version may be the latest version is published to a production track or to a beta track.

- After installing and opening the app, users see the message App Not Authorized, even though the .mdx file is in the Endpoint Management console.

  This issue can happen if users install the app directly from the App Store or Google Play and if Secure Hub is not refreshed. Secure Hub must be refreshed when the inactivity timer is expired. Policies refresh when users open Secure Hub and reauthenticate. The app is authorized the next time users open the app.

- Do I need an access code to use the app? I see a screen prompting me to enter an access code when I install the app from the App Store or Play Store.

  If you see a screen requesting an access code, you are not enrolled in Endpoint Management through Secure Hub. Enroll with Secure Hub and ensure that the .mdx file for the app is deployed on the server. Also ensure that the app can be used. The access code is limited to Citrix internal use only. Apps require an Endpoint Management deployment to be activated.

- Can I deploy iOS public store apps via VPP or DEP?

  Endpoint Management is optimized for VPP distribution of public store apps that are not MDX-enabled. Although you can distribute the Endpoint Management public store apps with VPP, the deployment is not optimal, until we make further enhancements to Endpoint Management and the Secure Hub store to address the limitations. For a list of known issues with deploying the Endpoint Management public store apps via VPP, in addition to potential workarounds, see this article in the Citrix knowledge center.

## MDX policies for mobile productivity apps

MDX policies enable you to configure settings that Endpoint Management enforces. The policies cover authentication, device security, network requirements and access, encryption, app interaction, app restrictions, and more. Many MDX policies apply to all mobile productivity apps. Some policies are app-specific.

Policy files are provided as .mdx files for the public store versions of the mobile productivity apps. You can also configure policies in the Endpoint Management console when you add an app.

For full descriptions of the MDX policies, see the following articles in this section:

- MDX policies for mobile productivity apps at a glance
- MDX policies for mobile productivity apps for Android
- MDX policies for mobile productivity apps for iOS

The following sections describe the MDX policies related to user connections.

## Dual mode in Secure Mail for Android

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 current MDX Toolkit. Using dual mode allows you to either:

- Continue managing apps using MDX Toolkit (now named Legacy MDX in the Endpoint Management console)
- Manage apps that incorporate the new MAM SDK.

> **Note:**
>
> When you use the MAM SDK, you do not need to wrap apps.

There are no additional steps required after you switch to the MAM SDK.

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

- MAM SDK Overview
- Latest releases of MAM SDK
- Citrix Developer section on Device Management
- Citrix blog post

### 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, make sure to incorporate the MAM SDK into your third-party apps before you switch 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 supports only 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.

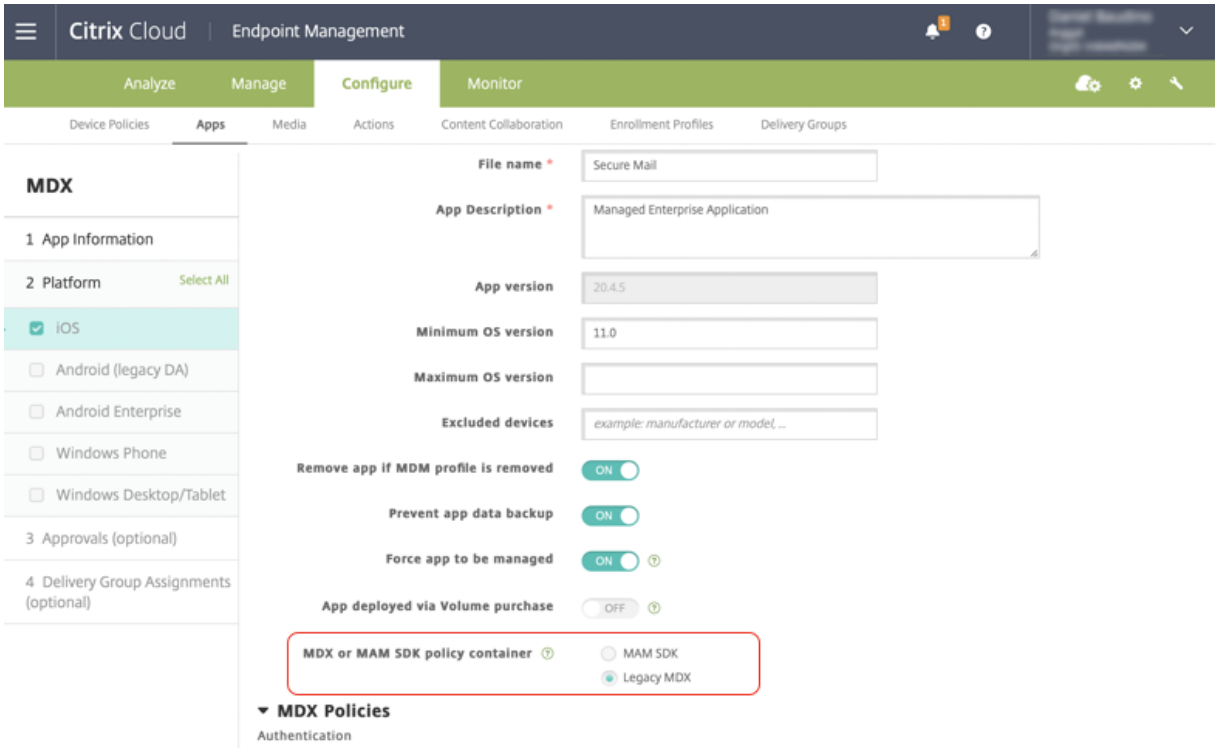
 

- If you don't update Citrix Endpoint Management, and the policy files are running on version 20.8.0 and later for the mobile apps, then duplicate entries of the Networking policy are created for Secure Mail.

When you configure Secure Mail 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 intend to allow you to use only a subset of the MDX functionality that your organization uses.

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 **Legacy MDX**. 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.

### User connections to the internal network

Connections that tunnel to the internal network can use a full VPN tunnel or a variation of a clientless VPN, referred to as Tunneled –Web SSO. The Preferred VPN mode policy controls that behavior. By default, connections use Tunneled –Web SSO, which is recommended for connections that require SSO. The full VPN tunnel setting is recommended for connections that use client certificates or end-to-end SSL to a resource in the internal network. The setting handles any protocol over TCP and can be used with Windows and Mac computers, and with iOS and Android devices.

The Permit VPN mode switching policy allows automatic switching between the full VPN tunnel and Tunneled –Web SSO 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, server challenges for client certificates can be accommodated by the full VPN tunnel mode, but not Tunneled –Web SSO mode. Similarly, HTTP authentication challenges are more likely to be serviced with SSO when using Tunneled –Web SSO mode.

### Network access restrictions

The Network access policy specifies whether restrictions are placed on network access. By default, Secure Mail access is unrestricted, which means no restrictions are placed on network access. Apps have unrestricted access to networks to which the device is connected. By default, Secure Web access is tunneled to the internal network, which means a per-application VPN tunnel back to the internal network is used for all network access and Citrix ADC split tunnel settings are used. You can also specify blocked access so that the app operates as if the device has no network connection.

Do not block the Network access policy if you want to allow features such as AirPrint, iCloud, and Facebook and Twitter APIs.

The Network access policy also interacts with the Background network services policy. For details, see Integrating Exchange Server or IBM Notes Traveler Server.

## Endpoint Management client properties

Client properties contain information that is provided directly to Secure Hub on user devices. Client properties are located in the Endpoint Management console in **Settings > Client > Client Properties**.

Client properties are used to configure settings such as the following:

### User password caching

User password caching allows the users' Active Directory password to be cached locally on the mobile device. If you enable user password caching, users are prompted to set a Citrix PIN or passcode.

### Inactivity timer

The inactivity timer defines the time in minutes that users can leave their device inactive and can access an app without being prompted for a Citrix PIN or passcode. To enable this setting for an MDX app, you must set the App passcode policy to **On**. If the App passcode policy is **Off**, users are redirected to Secure Hub to perform a full authentication. When you change this setting, the value takes effect the next time users are prompted to authenticate.

### Citrix PIN authentication

Citrix PIN simplifies the user authentication experience. The PIN is used to secure a client certificate or save Active Directory credentials locally on the device. If you configure PIN settings, the user sign-on experience is as follows:

1. When users start Secure Hub for the first time, they receive a prompt to enter a PIN, which caches the Active Directory credentials.
2. When users next start a mobile productivity app such as Secure Mail, they enter the PIN and sign on.

You use client properties to enable PIN authentication, specify the PIN type, and specify PIN strength, length, and change requirements.

## Fingerprint or touch ID authentication

Fingerprint authentication, also known as touch ID authentication, for iOS devices is an alternative to Citrix PIN. The feature is useful when wrapped apps, except for Secure Hub, are in need offline authentication, such as when the inactivity timer expires. You can enable this feature in the following authentication scenarios:

- Citrix PIN + Client certificate configuration
- Citrix PIN + Cached AD password configuration
- Citrix PIN + Client certificate configuration and Cached AD password configuration
- Citrix PIN is off

If fingerprint authentication fails or if a user cancels the fingerprint authentication prompt, the wrapped apps fall back to Citrix PIN or AD password authentication.

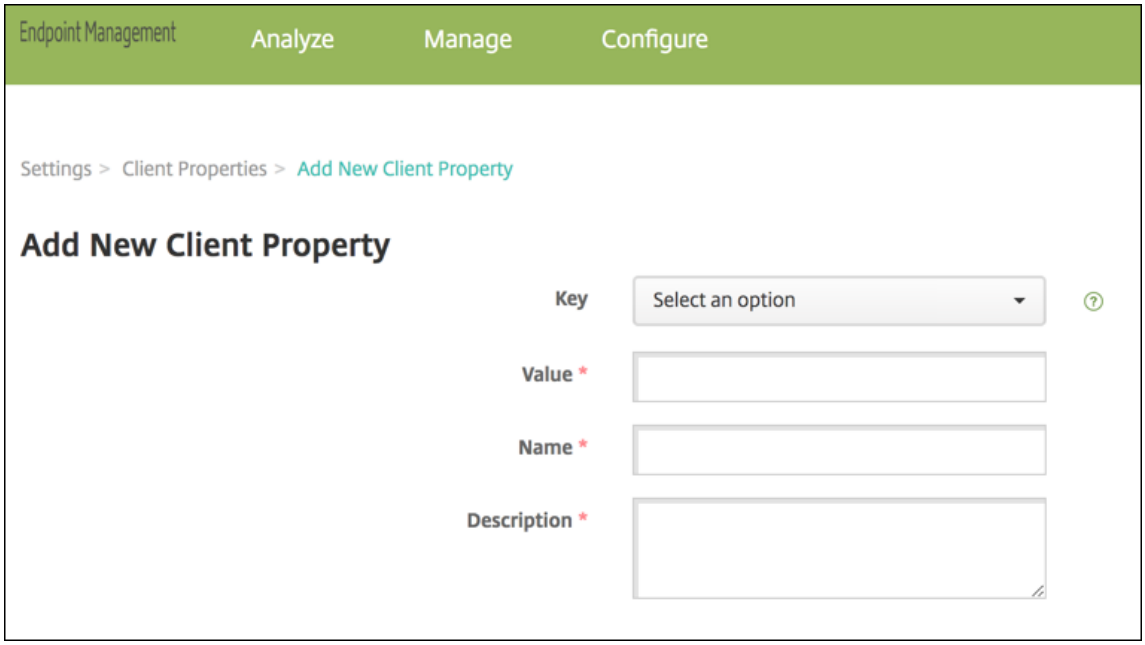
### Fingerprint authentication requirements

- iOS devices (minimum version 8.1) that support fingerprint authentication and have at least one fingerprint configured.
- User entropy must be off.

### To configure fingerprint authentication

> Important:
>
> If user entropy is on, the Enable Touch ID Authentication property is ignored. User entropy is enabled through the Encrypt secrets using the Passcode key.

1. In the Endpoint Management console, go to **Settings > Client > Client Properties**.
2. Click **Add**.




3. Add the key **ENABLE_TOUCH_ID_AUTH**, set its **Value** to **True** and then set the policy name to **Enable Fingerprint Authentication**.

After you configure fingerprint authentication, users do not need to reenroll their devices.

For more information about the Encrypt Secrets using Passcode key and client properties in general, see the Endpoint Management article about Client properties.

### Google Analytics

Citrix Secure Mail uses Google Analytics for collecting app statistics and usage information analytics data to improve product quality. Citrix does not collect or store any other personal user information.

#### Disable Google Analytics

Admins can disable Google Analytics by configuring the custom client property **DISABLE_GA**. To disable Google analytics, do the following:

1. Sign in to the Citrix Endpoint Management console and navigate to **Settings** > **Client Properties** > **Add New Client Property**.
2. Add the value **DISABLE_GA** to the **Key** field.
3. Set the value of the client property to **true**.

> **Note:**
>
> If you don't configure the value **DISABLE_GA** in the Citrix Endpoint Management console, Google Analytics data is active.

## Features by platform

May 14, 2024

The following tables summarize features for the Citrix mobile productivity apps. **X** indicates the feature is available for that platform. For features in QuickEdit, see the Citrix QuickEdit.

### Citrix Secure Hub

| Feature | iOS | Android |
|---|---|---|
| Sign on to authenticate | X | X |
| Monitor policy adherence | X | X |
| Access apps and desktops | X | X |
| HDX apps and desktops | X | X |
| Create and send issue logs | X | X |

| Feature | iOS | Android |
|---|---|---|
| Attach screenshots to logs | X | X |
| Contact help desk within app | X | X |
| Contact Citrix support within app | X | X |
| Crash collection and analysis | X | X |
| Offline authentication | X | X |
| Send logs with Citrix Secure Mail | X | X |
| Google Analytics | X | X |
| Portrait and landscape mode | X | X |
| In-app guide for trusting apps | X | X |
| When enrolled with email, automatic enrollment in Secure Mail (MAM only) | X | X |
| Touch ID offline authentication | X | X |
| Enroll with derived credentials | X | |
| Biometric authentication | | X |
| Use of Workspace apps store | X | X |

## Citrix Secure Mail

| Feature | iOS | Android |
|---|---|---|
| **Email Productivity** | | |
| Minimize drafts | X | X |
| Undo sent mails | | X |
| Encryption management | X | X |
| Widget for Calendar agenda | | X |
| Contact picture in Secure Mail | X | X |
| Support for responsive emails | X | X |
| Drafts folder auto-sync | X | X |

| Feature | iOS | Android |
|---|---|---|
| Attachments sync in **Drafts** folder | | X |
| Send, receive, reply, reply all, forward mail | X | X |
| Create, edit, delete drafts | X | X |
| Flag mail | X | X |
| Mark as unread | X | X |
| View all folders and subfolders | X | X |
| Auto-save drafts when app put in background | X | X |
| Email-to-note with Citrix Secure Notes. **Important:** Secure Notes reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps. | X | X |
| Search mail (local and server) | X | X |
| Select mail sync period (up to 1 month or All mails) | X | X |
| View unread mail | X | X |
| Secure attachment viewing/playing of images, video, and audio | X | X |
| Multiple attachments | X | X |
| Reply and forward attachments | X | X |
| Attach files from Citrix Files | X | X |
| Attach files from Citrix Files Restricted Zones and connectors | X | X |
| Attachment repository | X | X |
| Rich text editing | X | X |
| Mail notification with subject, preview on lock screen | X | X |

| Feature | iOS | Android |
|---|---|---|
| Reply to and delete mail and invitations from notification screen | X | |
| Attach or take photo | X | X |
| Select multiple messages | X | X |
| Download attachments | X | X |
| Load images inline | X | X |
| Fast sort | X | X |
| Send, receive, open, and save .zip file attachments | X | X |
| Portrait and landscape modes | X; Across mail list, mail read, compose, calendar, and contacts views | X: For mail read and compose views only |
| Pasted text maintains formatting | X | X |
| SMS from contacts | X | X |
| FaceTime from contacts | X | |
| Messages unsent due to connectivity issues or full mailbox stored in Outbox | X | X |
| Recent folders bubble up | | X |
| Pull-down mail refresh | X | X |
| Last-refresh time stamp | X | X |
| Left-swipe for message actions | X | X |
| Microsoft Exchange and IBM Notes Traveler support | X | X |
| Tap to refresh mail, calendar, and contacts | X | X |
| Honor device accessibility/font-size settings in mail views | X | X |
| S/MIME signing and encryption | X | X |
| S/MIME cert import by email | X | X |
| S/MIME, Intercede integration | X | |

| Feature | iOS | Android |
|---|---|---|
| S/MIME, Entrust integration | X | |
| Microsoft IRM protection for message body | X | X |
| Push notifications | X | X |
| Push notifications to Inbox automatically update all folders, including calendar | X | |
| Open Office 365 documents | X | X |
| 3D Touch actions | X | |
| Contextual icons on lock screen | X | X |
| Search folders | X | X |
| VIP mail folder | X | X |
| Dynamic Type support | X | X |
| Maintain expanded folders | X | X |
| Message classification markers | X | X |
| Spell check | X | |
| Attach last photo taken | X | X |
| URL preview | X | X |
| Open Citrix Files links in Citrix Files | X | X |
| Support for `.pass` files | X | |
| Select multiple emails in search mode | X | X |
| Insert images inline | X | X |
| Upgrade to Exchange ActiveSync (EAS) version 16 | X | X |
| Restrict users from using unknown or personal domains | X | |
| Support super-wide device screens | | X |
| Configure multiple Exchange accounts | X | X |

| Feature | iOS | Android |
|---|---|---|
| Swipe left or right for more actions | X | X |
| Encrypt replies to or forwards of encrypted mails | X | |
| Print emails and inline images | X | |
| Use Preview Lines in Settings to configure how many lines of an email body appear as preview in the mailbox view | X | |
| Support for responsive emails | X | X |
| In-app preview of attachments (MS Office or images.) | X | X |
| Personal contact groups | X | X |
| Migrate user names to email addresses (UPN) | X | X |
| Report phishing emails | X | X |
| Modern authentication (OAuth) | X | X |
| Print attachments | X | |
| Android Enterprise (Android for Work) | X | |
| Rich text signatures | X | |
| Rich push notifications | X | |
| Feeds | X | X |
| Photo attachment improvements | X | X |
| Group notifications | X | |
| Slack integration (Preview) | X | X |
| Manage feeds | X | |
| Internal domains | X | X |
| Manage your feeds | X | X |
| MS Teams integration | X | X |
| Self diagnostic (**Troubleshooot**) option | | X |

| Feature | iOS | Android |
|---|---|---|
| Dual mode (MAM SDK) | X | X |
| Self-diagnostic tool | | X |
| **Calendar** | | |
| Preview and import ICS files as calendar Events | | X |
| Drag and drop Calendar events | X | X |
| Day, week, month, and agenda views | X | X |
| Detailed reminders on lock screen | X | X |
| Sync for six months | X | X |
| Set events as private | X | X |
| Scroll to hour before first event | X | |
| Manual refresh options | X | X |
| Set reminders | X | X |
| Tap to map address | X | X |
| Week numbers | X | X |
| Dynamic Type support | X | X |
| Security classification markers | X | X |
| Long taps on addresses | X | |
| Set workweek start day | X | X |
| Focus view on week of selected date | X | |
| Current date always highlighted | X | X |
| Calendar attachments from attachment repository | X | X |
| Personal calendar support | X | X |
| Display conflicts with personal calendar events | | X |
| Print calendar events | X | |

| Feature | iOS | Android |
|---|---|---|
| Tap phone numbers and web addresses in a calendar subject line | X | |
| Search calendar | X | |
| **Meetings** | | |
| Reply, reply all, forward meetings | X | X |
| Organizer view of invite responses | X | X |
| Organizer view of invitees' availability with suggested availability | X | X |
| Tap to join online meetings. **Note:** For WebEx and Lync, you must configure policies in Citrix Endpoint Management to enable these apps. | X | X |
| Tap to join audio conferences | X | X |
| Schedule online meeting, audio, conference in new invite | X | X |
| Add ShareFile links to new invites | X | X |
| Forward invites with attachments | X | X |
| Tap to send "running late"email | X | X |
| Tap to reply to meeting organizer | X | X |
| Tap to reply to all meeting invites | X | X |
| Tap to reply to all meeting invitees | X | X |
| Tap to reply to all meeting invitees with attachments | X | X |
| Dial in to GoToMeeting | X | X |
| Respond to invite from lock screen or notification screen | X | X |

| Feature | iOS | Android |
|---|---|---|
| Dial in to WebEx or Lync meetings | X | X |
| Hide declined events | X | X |
| Display more than 3 simultaneous events | X | X |
| Quick view of invitee status | X | X |
| Delete, reply, reply all, add comments on canceled events | X | X |
| Show organizer name on forwarded invites | X | X |
| Shared devices | X | X |
| Join Skype for Business meetings | X | X |
| Respond to meeting notifications, such as Accept, Decline, and Tentative. | X | X |
| Respond to message notifications with Reply and Delete | X | |
| **Contacts** | | |
| Create folders in **Contacts** | | X |
| Two-way contact sync | X | X |
| Detailed contact information GAL search | X | X |
| Export and sync Secure Mail contacts to local contacts | X | X |
| Contacts: Favorite and Category | | X |
| Control which contact fields get exported | X | X |
| Non-Secure Mail contact details | X | X |
| Dynamic Type support | X | X |
| Mark contacts as VIPs | X | X |
| Share contacts with `.vcards` | X | X |

| Feature | iOS | Android |
|---|---|---|
| View contacts with long press | | X |
| Export contacts even if native mail account exists | X | X |
| View folders and subfolders | X | |
| **Settings configured on the device** | | |
| iMessage support | X | |
| Advanced options to control notifications | X | X |
| Lock-screen notification control | X | X |
| Mail and calendar notifications sounds | X | X |
| Auto refresh folders | X | X |
| Set internal and external out-of-office notifications | X | X |
| Ask before deleting | X | X |
| Threaded conversation or chronological views | X | X |
| Load attachments on Wi-Fi | X | X |
| Make load attachments on Wi-Fi default | X | X |
| Set sync mail period | X | X |
| Unlimited sync/sync all mail | | X |
| Set email signature | X | X |
| List contacts by first name or last name | X | X |
| Auto advance | X | X |
| Use home time zone | | X |
| Quick-response templates | | X |
| Push mail configuration frequency | | X |
| Export/import settings | X | X |

| Feature | iOS | Android |
|---|---|---|
| Tap the back button on the device to dismiss the floating action button options | | X |
| Microsoft Teams | X | X |

### Citrix Secure Web

| Feature | iOS | Android |
|---|---|---|
| Use two apps simultaneously with Multitasking | X | |
| Download files | X | X |
| Add favorites | X | X |
| Clear saved user names and passwords | X | X |
| Delete cache/history/cookies | X | X |
| Block pop-ups | X | X |
| Save offline pages | X | X |
| Search in address bar | X | X |
| Open downloaded items from notifications | X | X |
| Passwords auto-saved | X | X |
| Proxy support | | |
| Enterprise proxies | X | X |
| URL block lists and allow lists | X | X |
| History | X | X |
| Default home page | X | X |
| Tabs | X | X |
| Push bookmarks | X | X |
| Screen capture block | | X |
| Search in current page | X | X |

| Feature | iOS | Android |
|---|---|---|
| 3D Touch actions | X | |
| Shared devices | X | X |
| File tampering protection with shared devices | X | |
| Export/import settings | X | X |
| Portrait and landscape mode | X | X |
| Android Enterprise (Android for Work) | | X |
| Pull to refresh content on the screen | X | X |
| Secure Web as default browser | | X |

## Citrix Secure Hub

July 1, 2024

Citrix Secure Hub is the launchpad for the mobile productivity apps. Users enroll their devices in Secure Hub to gain access to the app store. From the app store, they can add Citrix-developed mobile productivity apps and third-party apps.

You can download Secure Hub and other components from the Citrix Endpoint Management downloads page.

For Secure Hub and other system requirements for the mobile productivity apps, see System requirements.

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

The following sections list the new features in current and earlier releases of Secure Hub.

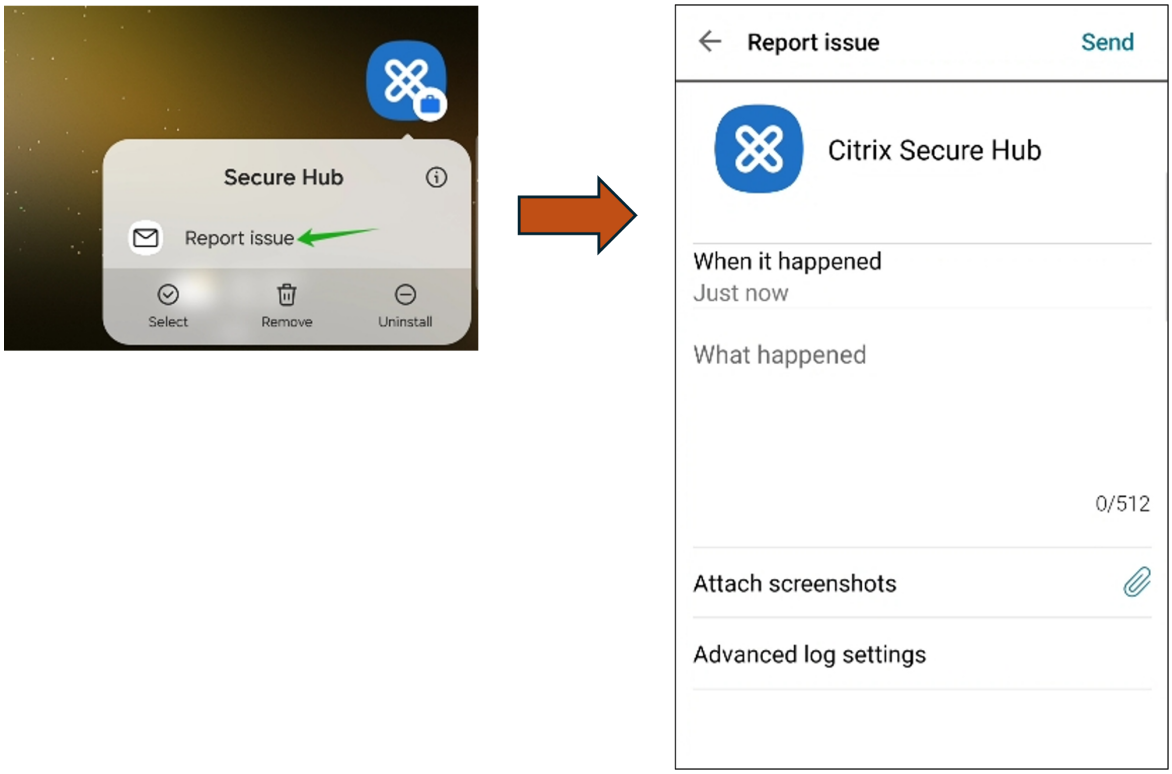
> **Note:**
>
> Support ended for the Android 6.x and iOS 11.x versions of Secure Hub in Oct 2023.

## What's new in the current version

### Secure Hub for Android 24.6.0

**Improved log collection and reporting** Secure Hub introduces an enhanced ability to report issues and send logs seamlessly without opening Secure Hub. With this release, users can access the **Report Issue** option by long-pressing the Secure Hub app icon. Upon clicking the **Report Issue** option, Secure Hub opens the **Report Issue** page directly.




## What's new in earlier versions

### Secure Hub for iOS 24.5.0

**Supports iOS 17 Return to Service** Secure Hub supports the Return to Service feature in iOS 17, which provides a more efficient and secure Mobile Device Management (MDM) experience. Previously, manual configuration was required to set it up for a new user after wiping the device. Now, the Return to Service feature automates this process, whether repurposing a company device or integrating a personal device (BYOD) with correct security policies.

With the Return to Service feature, MDM server can send an erase command that includes Wi-Fi details and a default MDM enrollment profile to the user device. The device then automatically wipes all user

data, connects to the specified Wi-Fi network, and re-enrolls itself back into the MDM server using the provided enrollment profile.

### Secure Hub for Android 24.3.0

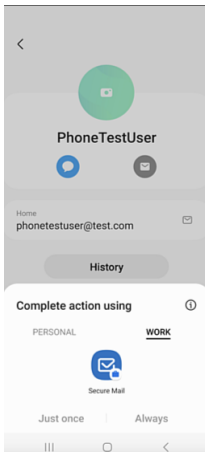
**Supports Samsung Knox Enhanced Attestation v3** Secure Hub now supports Samsung Enhanced Attestation v3, leveraging Knox attestation to strengthen security measures for Samsung devices managed through Citrix Endpoint Management. This advanced attestation protocol verifies the integrity and security status of the devices, ensuring they are not rooted and are running authorized firmware. The feature provides an essential layer of protection against security threats and ensures adherence to enterprise security policies.

### Secure Hub for Android 23.12.0

**Enhanced Security with Samsung Knox** The addition of the Knox Platform for Enterprise Key device policy in Citrix Endpoint Management significantly enhances the security features of Secure Hub on Samsung devices. This policy allows you to provide the required Samsung Knox Platform for Enterprise (KPE) license information and use the KPE licenses to enhance the security of your Samsung device. Samsung Knox ensures that enterprise data remains protected, while also maintaining ease of management and a smooth user experience.

For more information, see Knox Platform for Enterprise Key device policy.

**Access Secure Mail from user's personal profile** Users can now access and use Secure Mail in their work profile from their personal profile. When users click an email address in their personal profile address book, they get an option to use Secure Mail in their work profile. This feature offers convenience, allowing users to send an email from their personal profile. This feature is applicable on BYOD or WPCOD devices.



### Secure Hub for iOS 24.1.0

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

### Secure Hub for Android 23.12.0

**Add a hint about authentication PIN on the sign-in page** Starting with the 23.12.0 release, you can add a hint about the authentication PIN on the sign-in page. This feature is optional and applies to devices enrolled for two-factor authentication. The hint lets you know how to access the PIN.

You can configure a hint as text or a link. The hint text offers concise information about the PIN, while the link provides detailed information on how to access the PIN. For more information on how to configure a hint, see Configure hint through the Citrix Endpoint Management console.

**nFactor authentication supports single sign-on feature** Starting with Secure Hub for Android version 23.12.0, nFactor for Mobile Application Management (MAM) enrollment or login supports the single sign-on (SSO) feature. This feature allows previously entered sign-in credentials to pass through the MAM enrollment or login process, eliminating the need for users to enter them manually again. For more information on nFactor SSO property, see the Client property reference in Citrix Endpoint Management documentation.

**Support full wipe in direct boot mode** Previously, you needed to unlock the device to run a full wipe command on a rebooted device. Now, you can run a full wipe command in direct boot mode, even if the device is locked. This feature is helpful from a security viewpoint, especially when the device is in the possession of an unauthorized individual. For more information on the full wipe command, see the Security actions in Citrix Endpoint Management documentation.

**Optimized the loading speed of Secure Hub's App Store** The App Store in Secure Hub now loads faster than before, allowing users to access it more quickly.

### Secure Hub for iOS 23.11.0

**Add a hint about authentication PIN on the sign-in page** Starting with the 23.11.0 release, you can add a hint about the authentication PIN on the sign-in page. This feature is optional and applies to devices enrolled for two-factor authentication. The hint lets you know how to access the PIN.

You can configure a hint as text or a link. The hint text offers concise information about the PIN, while the link provides detailed information on how to access the PIN. For more information on how to configure a hint, see the Configure hint through the Citrix Endpoint Management console article.

**nFactor authentication supports single sign-on feature** Starting with Secure Hub for iOS version 23.11.0, nFactor for Mobile Application Management (MAM) enrollment or sign-in supports the single sign-on (SSO) feature. This feature allows previously entered sign-in credentials to pass through the MAM enrollment or sign-in process, eliminating the need for users to enter them manually again.

For more information on nFactor SSO property, see the Client property reference in Citrix Endpoint Management documentation.

### Secure Hub 23.10.0

#### Secure Hub for Android

Secure Hub for Android 23.10.0 supports Android 14. Upgrading the Secure Hub version to 23.10.0 ensures continuous support for devices that are updated to Android 14.

### Secure Hub 23.9.0

#### Secure Hub for Android

This release addresses areas that improve overall performance and stability.

### Secure Hub 23.8.1

**Secure Hub for iOS** This release addresses a few issues that help to improve overall performance and stability.

### Secure Hub 23.8.0

**Secure Hub for iOS** This release addresses a few issues that help to improve overall performance and stability.

### Secure Hub 23.7.0

#### Secure Hub for Android

**Play Integrity API** The SafetyNet Attestation API will soon be deprecated by Google as per the deprecation timeline, and migrated to the suggested Play Integrity API.

For more information, see Play Integrity API in the Citrix Endpoint Management document.

For deprecation details, see Deprecations and removals in the Citrix Endpoint Management document.

To read about the Android SafetyNet feature, see SafetyNet

### Secure Hub 23.4.0

#### Secure Hub for iOS

**Improved user experience** Starting with the 23.4.0 version, Secure Hub for iOS improves the following user experiences:

- Store experience:

  ⊠ Previously, the My Apps page appeared first. With the 23.4.0 version, the Store page appears first.

  ⊠ Previously, the Secure Hub store performed the reload action every time the user clicked the Store option.

  With the 23.4.0 version, the user experience is improved. Now, the app reloads when the user launches the app for the first time, restarts the app, or swipes down the screen.

- User interface: Previously, the Sign Off option was placed at the bottom left of the screen. With the 23.4.0 version, the Sign Off option is part of the main menu and is above the About option.
- Hyperlinks: Previously, the hyperlinks on the app's detail page appeared as plain text. With the 23.4.0 version, the hyperlinks are clickable and have an underline formatting to indicate links.

**MDX to MAM SDK transition experience** Starting with the 23.4.0 version, the transition experience from legacy MDX to MAM SDK is enhanced for iOS dual-mode apps. This feature improves the user experience when using mobile productivity apps by reducing alert messages and switching to Secure Hub.

**Use Citrix PIN to unlock apps** Previously, end user entered the device passcode to unlock apps that is based on Mobile App Management (MAM).

Starting with the 23.4.0 version, end user can enter Citrix PIN as the passcode to unlock MAM based app. Administrators can configure the complexity of the passcode using the client properties on the CEM server.

Whenever the app is inactive for more than the allowed time, end users can enter the Citrix PIN to unlock the app depending upon the configuration set by the administrators.

For Secure Hub for Android, there is a separate client property to configure how to handle with inactivity timer in MAM applications. For more information, see Separate Inactivity Timer for Android.

### Secure Hub 23.4.1

**Secure Hub for Android** This release addresses a few issues that help to improve overall performance and stability.

### Secure Hub 23.4.0

**Secure Hub for Android** This release addresses a few issues that help to improve overall performance and stability.

### Secure Hub 23.2.0

### Secure Hub for Android

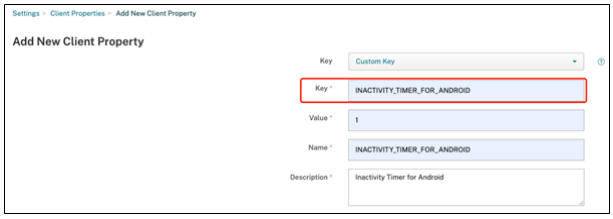
> **Note:**
>
> - No analytical data is collected for the users in European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK).

**MDX full tunnel mode VPN** The MDX Micro VPN (full tunnel mode) is deprecated.

For more information, see Deprecation in the Citrix Endpoint Management documentation.

**Separate Inactivity Timer for Android** Previously, the **Inactivity Timer** client property was common for Secure Hub for Android and iOS.

Starting with the 23.2.0 version, an IT administrator can use the new client property **Inactivity_Timer_For_Android** to separate the inactivity timer from iOS. An IT administrator can set the **Value** of the **Inactivity_Timer_For_Android** to 0 to disable Android inactivity timer independently. In this way, all apps in work profile, including Secure Hub, challenges work PIN only.




For more information on how to add and modify a client property, see Client properties in the XenMobile documentation.

**Secure Hub 22.11.0**

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 22.9.0**

**Secure Hub for Android** This release includes:

- Passcode complexity for device passcode (Android 12+)
- Support for SDK 31
- Bug fixes

**Passcode complexity for device passcode (Android 12+)** Passcode complexity is preferred than a custom password requirement. The passcode complexity level is one of the pre-defined levels. Thus, the end user is unable to set a password with a lower complexity level.

Passcode complexity for devices on Android 12+ is as follows:

- **Apply passcode complexity:** Requires a password with a complexity level defined by the platform, rather than a custom password requirement. Only for devices on Android 12+ and using Secure Hub 22.9 or later.
- **Complexity level:** Predefined levels of password complexity.
  - **None:** No password required.
  - **Low:** Passwords can be:
    - A pattern
    - A PIN with a minimum of four numbers
  - **Medium:** Passwords can be:
    - A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of four numbers
    - Alphabetic with a minimum of four characters
    - Alphanumeric with a minimum of four characters
  - **High:** Passwords can be:
    - A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of eight numbers
    - Alphabetic with a minimum of six characters
    - Alphanumeric with a minimum of six characters

> **Notes:**
>
> - For BYOD devices, passcode settings such as Minimum length, Required characters, Bio-

> metric recognition, and Advanced rules are not applicable on Android 12+. Use passcode complexity instead.
> - If passcode complexity for work profile is enabled, then passcode complexity for the device side must be enabled too.

For more information, see Android Enterprise settings in the Citrix Endpoint Management documentation.

**Secure Hub 22.7.0**

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 22.6.0**

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 22.5.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub 22.4.0**

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 22.2.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 21.11.0**

**Secure Hub for Android**

**Support for Work profile for company-owned devices** In Android Enterprise devices, you can now enroll Secure Hub in the Work profile for company-owned devices mode. This feature is available on devices running Android 11 or later. Devices previously enrolled in the Corporate Owned Personally Enabled (COPE) mode automatically migrate to the Work profile for company-owned devices mode, when the device upgrades from Android 10 to Android 11 or later.

**Secure Hub 21.10.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** **Support for Android 12**. From this release onward, Secure Hub is supported on devices running Android 12.

**Secure Hub 21.8.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub 21.7.1**

**Secure Hub for Android** **Support for Android 12 on already enrolled devices.** If you are considering upgrading to Android 12, 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. This release ensures a seamless upgrade from Android 11 to Android 12 for already enrolled users.

> **Note:**
>
> If Secure Hub is not updated to version 21.7.1 before you upgrade to Android 12, your device might require a re-enrollment or a factory reset to recover prior functionality.
>
> Citrix is committed to providing Day 1 support for Android 12 and will add further updates to subsequent versions of Secure Hub to fully support Android 12.

**Secure Hub 21.7.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 21.6.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 21.5.1**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 21.5.0**

**Secure Hub for iOS** With this release, apps wrapped with MDX Toolkit version 19.8.0 or earlier will no longer work. Ensure that you wrap your apps with the latest MDX Toolkit to resume proper functionality.

**Secure Hub 21.4.0**

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

**Secure Hub 21.3.2**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub 21.3.0**

This release includes bug fixes.

**Secure Hub 21.2.0**

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 21.1.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub 20.12.0**

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** Secure Hub for Android supports Direct Boot mode. For more information about Direct Boot mode, see the Android documentation at *Developer.android.com.*

#### Secure Hub 20.11.0

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

#### Secure Hub 20.10.5

This release includes bug fixes.

#### Secure Hub 20.9.0

**Secure Hub for iOS** Secure Hub for iOS supports iOS 14.

**Secure Hub for Android** This release includes bug fixes.

#### Secure Hub 20.7.5

#### Secure Hub for Android

- Secure Hub for Android supports Android 11.
- **Transition from Secure Hub 32-bit to 64-bit for apps**. In Secure Hub version 20.7.5, support ends for 32-bit architecture for apps, and Secure Hub has been updated to 64-bit. Citrix recommends customers to upgrade to version 20.7.5 from 20.6.5. If users skip the upgrade to Secure Hub version 20.6.5, and instead update from 20.1.5 to 20.7.5 directly, they must reauthenticate. Reauthentication involves entering credentials and resetting the Secure Hub PIN. Secure Hub version 20.6.5 is available in the Google Play Store.
- **Install updates from the App Store.** In Secure Hub for Android, if there are updates available for apps, the app is highlighted and the **Updates available** feature appears on the App Store screen.

  When you tap **Updates available**, you navigate to the store that shows the list of apps with pending updates. Tap **Details** against the app to install the updates. When the app is updated, the down arrow in **Details** is changed to a check mark.

### Secure Hub 20.6.5

**Secure Hub for Android** **Transition from 32-bit to 64-bit for apps.** The Secure Hub 20.6.5 release is the final release that supports a 32-bit architecture for Android mobile apps. In subsequent releases, Secure Hub supports the 64-bit architecture. Citrix recommends that users upgrade to Secure Hub version 20.6.5, so that users can upgrade to later versions without reauthentication. If users skip the upgrade to Secure Hub version 20.6.5, and instead update to 20.7.5 directly, they need to reauthenticate. Reauthentication involves entering credentials and resetting the Secure Hub PIN.

> **Note:**
>
> The 20.6.5 release does not block the enrollment of devices running Android 10 in device administrator mode.

**Secure Hub for iOS** **Enable a proxy configured on iOS devices.** Secure Hub for iOS requires that you enable a new client property, `ALLOW_CLIENTSIDE_PROXY`, if you want to allow users to use proxy servers that they configure in **Settings > Wi-Fi**. For more information, see `ALLOW_CLIENTSIDE_PROXY` in Client property reference.

### Secure Hub 20.3.0

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

### Secure Hub for iOS

- **Network Extension disabled.** Due to recent changes on App Store Review Guidelines, from release 20.3.0 onward, Secure Hub does not support Network Extension (NE) on devices running iOS. NE has no impact on Citrix-developed mobile productivity apps. However, the removal of NE has some impact on deployed enterprise MDX wrapped apps. End-users might experience extra flips to Secure Hub while synchronizing components such as authorization tokens, timers, and PIN retries. For more information, see https://support.citrix.com/article/CTX270296.

> **Note:**
>
> New users are not prompted to install VPN.

- **Support for enhanced enrollment profiles.** Secure Hub supports the enhanced enrollment profile features announced for Citrix Endpoint Management in Enrollment profile support.

#### Secure Hub 20.2.0

**Secure Hub for iOS** This release includes bug fixes.

#### Secure Hub 20.1.5

This release includes:

- Update to user privacy policy formatting and display. This feature update changes the Secure Hub enrollment flow.
- Bug fixes.

#### Secure Hub 19.12.5

This release includes bug fixes.

#### Secure Hub 19.11.5

This release includes bug fixes.

#### Secure Hub 19.10.5

**Secure Hub for Android** **Enroll Secure Hub in COPE mode.** In Android Enterprise devices, enroll Secure Hub in the Corporate Owned Personally Enabled (COPE) mode when Citrix Endpoint Management is configured in the COPE enrollment profile.

#### Secure Hub 19.10.0

This release includes bug fixes.

#### Secure Hub 19.9.5

**Secure Hub for iOS** This release includes bug fixes.

**Secure Hub for Android** **Support for manage keyguard features for Android Enterprise work profile and fully managed devices.** Android keyguard manages the device and work challenge lock screens. Use the Keyguard Management device policy in Citrix Endpoint Management to control keyguard management on work profile devices and Keyguard management on fully managed and dedicated devices. With keyguard management, you can specify the features available to users, such as trust agents and secure camera, before they unlock the keyguard screen. Or, you can choose to disable all keyguard features.

For more information about the feature settings and how to configure the device policy, see Keyguard Management device policy.

**Secure Hub 19.9.0**

**Secure Hub for iOS** Secure Hub for iOS supports iOS 13.

**Secure Hub for Android** This release includes bug fixes.

**Secure Hub for Android 19.8.5**

This release includes bug fixes.

**Secure Hub 19.8.0**

**Secure Hub for iOS** This release includes performance enhancements and bug fixes.

**Secure Hub for Android** **Support for Android Q.** This release includes support for Android Q. Before upgrading to the Android Q platform: See Migrate from device administration to Android Enterprise for information about how the deprecation of Google Device Administration APIs impacts devices running Android Q. Also see the blog, Citrix Endpoint Management and Android Enterprise - a Season of Change.

**Secure Hub 19.7.5**

**Secure Hub for iOS** This release includes performance enhancements and bug fixes.

**Secure Hub for Android** **Support for Samsung Knox SDK 3.x.** Secure Hub for Android supports Samsung Knox SDK 3.x. For more information about migrating to Samsung Knox 3.x, see the Samsung Knox developer documentation. This release also includes support for the new Samsung Knox namespaces. For more information about changes to old Samsung Knox namespaces, see Changes to old Samsung Knox namespaces.

> **Note:**
>
> Secure Hub for Android does not support Samsung Knox 3.x on devices running Android 5.

#### Secure Hub 19.3.5 to 19.6.6

These releases include performance enhancements and bug fixes.

#### Secure Hub 19.3.0

**Support for Samsung Knox Platform for Enterprise.** Secure Hub for Android supports Knox Platform for Enterprise (KPE) on Android Enterprise devices.

#### Secure Hub 19.2.0

This release includes performance enhancements and bug fixes.

#### Secure Hub 19.1.5

Secure Hub for Android Enterprise now supports the following policies:

- **WiFi device policy.** The Wi-Fi device policy now supports Android Enterprise. For more information about this policy, see Wi-Fi device policy.
- **Custom XML device policy.** The custom XML device policy now supports Android Enterprise. For more information about this policy, see Custom XML device policy.
- **Files device policy.** You can add script files in Citrix Endpoint Management to perform functions on Android Enterprise devices. For more information about this policy, see Files device policy.

#### Secure Hub 19.1.0

**Secure Hub has revamped fonts, colors, and other UI improvements.** This facelift gives you an enriched user experience while closely aligning with the Citrix brand aesthetics across our full suite of mobile productivity apps.

#### Secure Hub 18.12.0

This release includes performance enhancements and bug fixes.

#### Secure Hub 18.11.5

- **Restrictions device policy settings for Android Enterprise.** New settings for the Restrictions device policy allow users access to these features on Android Enterprise devices: status bar, lock screen keyguard, account management, location sharing, and keeping the device screen on for Android Enterprise devices. For information, see Restrictions device policy.

Secure Hub 18.10.5 to 18.11.0 include performance enhancements and bug fixes.

#### Secure Hub 18.10.0

- **Support for Samsung DeX mode:** Samsung DeX enables users to connect KNOX-enabled devices to an external display to use apps, review documents, and watch videos on a PC-like interface. For information about Samsung DeX device requirements and setting up Samsung DeX, see How Samsung DeX works.

  To configure Samsung DeX mode features in Citrix Endpoint Management, update the Restrictions device policy for Samsung Knox. For information, see **Samsung KNOX settings** in Restrictions device policy.

- **Support for Android SafetyNet:** You can configure Endpoint Management to use the **Android SafetyNet** feature to assess the compatibility and security of Android devices that have Secure Hub installed. The results can be used to trigger automated actions on the devices. For information, see Android SafetyNet.

- **Prevent camera use for Android Enterprise devices:** The new **Allow use of camera** setting for the Restrictions device policy lets you prevent users from using the camera on their Android Enterprise devices. For information, see Restrictions device policy.

#### Secure Hub 10.8.60 to 18.9.0

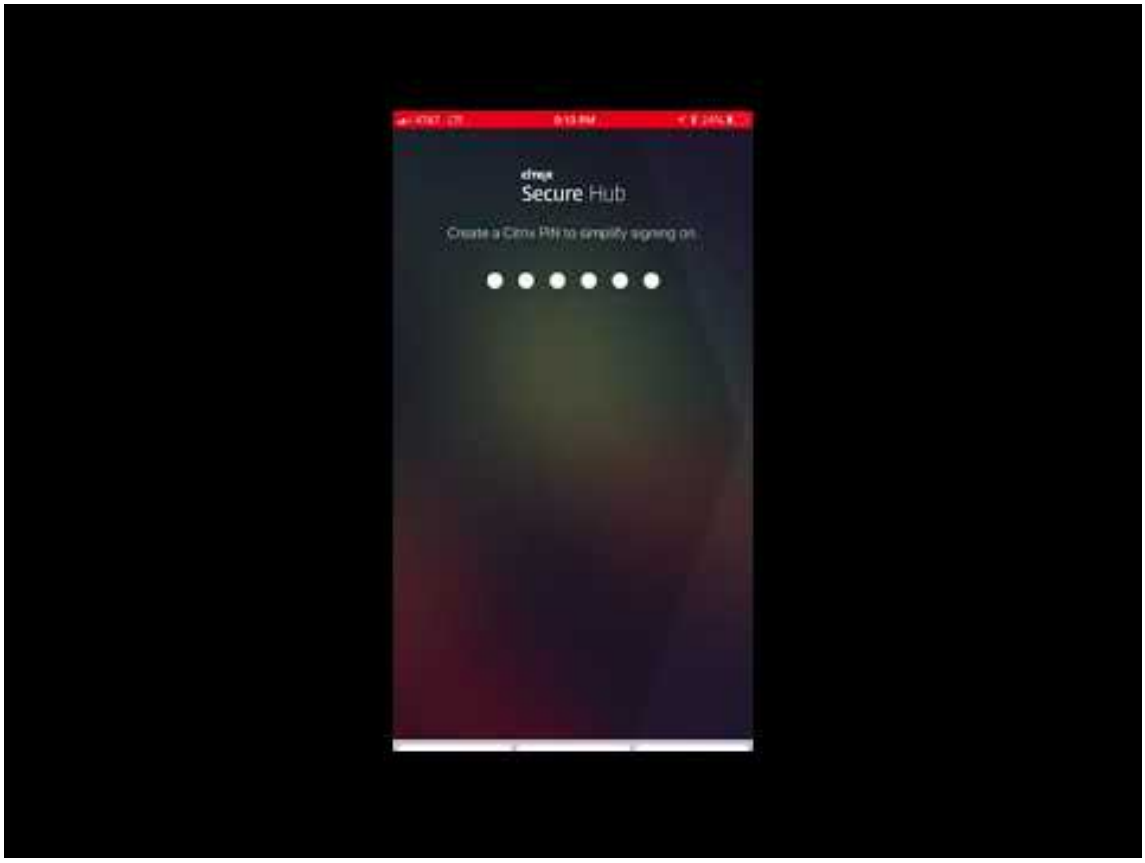
These releases include performance enhancements and bug fixes.

#### Secure Hub 10.8.60

- Support for the Polish language.
- Support for Android P.

- Support for the use of the Workspace apps store.
  When opening Secure Hub, users no longer see the Secure Hub store. An **Add Apps** button takes users to the Workspace apps store. The following video shows an iOS device performing an enrollment to Citrix Endpoint Management using the Citrix Workspace app.




> Important:
>
> This feature is only available for new customers. We don't currently support migration for existing customers.

To use this feature, configure the following:

- Enable the Password Caching and Password Authentication policies. For more information on configuring policies, see MDX policies for mobile productivity apps at a glance.
- Configure Active Directory authentication as AD or AD+Cert. We support these two modes. For more information on configuring authentication, see Domain or domain plus security token authentication.
- Enable Workspace integration for Endpoint Management. For more information on workspace integration, see Configure workspaces.

> **Important:**
>
> After this feature is enabled, Citrix Files SSO occurs through Workspace and not through Endpoint Management (formerly, XenMobile). We recommend that you disable Citrix Files integration in the Endpoint Management console before you enable Workspace integration.

**Secure Hub 10.8.55**

- The ability to pass a user name and password for the Google zero-touch and Samsung Knox Mobile Environment (KME) portal by using the configuration JSON. For details, see Samsung Knox bulk enrollment.
- When you enable certificate pinning, users cannot enroll in Endpoint Management with a self-signed certificate. If users try to enroll to Endpoint Management with a self-signed certificate, they are warned that the certificate is not trusted.

**Secure Hub 10.8.25:** Secure Hub for Android includes support for Android P devices.

> **Note:**
>
> Before upgrading to the Android P platform: Ensure that your server infrastructure is compliant with security certificates that have a matching host name in the subjectAltName (SAN) extension. To verify a host name, the server must present a certificate with a matching SAN. Certificates that don't contain a SAN matching the host name are no longer trusted. For details, see the Android Developer documentation.

**Secure Hub for iOS update on March 19, 2018:** Secure Hub version 10.8.6 for iOS is available to fix an issue with the VPP app policy. For details, see this Citrix Knowledge Center article.

**Secure Hub 10.8.5:** Support in Secure Hub for Android for COSU mode for Android Work (Android for Work). For details, see the Citrix Endpoint Management documentation.

## Administering Secure Hub

You perform most of the administration tasks related to Secure Hub during the initial configuration of Endpoint Management. To make Secure Hub available to users, for iOS and Android, upload Secure Hub to the iOS App Store and the Google Play Store.

Secure Hub also refreshes most MDX policies stored in Endpoint Management for the installed apps when a user's Citrix Gateway session renews after authentication using Citrix Gateway.

> **Important:**
>
> Changes to any of these policies require that a user delete and reinstall the app to apply the updated policy: Security Group, Enable encryption, and Secure Mail Exchange Server.

### Citrix PIN

You can configure Secure Hub to use the Citrix PIN, a security feature enabled in the Endpoint Management console in **Settings** > **Client Properties**. The setting requires enrolled mobile device users to sign on to Secure Hub and activate any MDX wrapped apps by using a personal identification number (PIN).

The Citrix PIN feature simplifies the user authentication experience when logging on to the secured wrapped apps. Users don't have to enter another credential like their Active Directory user name and password repeatedly.

Users who sign on to Secure Hub for the first time must enter their Active Directory user name and password. During sign-on, Secure Hub saves the Active Directory credentials or a client certificate on the user device and then prompts the user to enter a PIN. When users sign on again, they enter the PIN to access their Citrix apps and the Store securely, until the next idle timeout period ends for the active user session. Related client properties enable you to encrypt secrets using the PIN, specify the passcode type for the PIN, and specify PIN strength and length requirements. For details, see Client properties.

When fingerprint (touch ID) authentication is enabled, users can sign on by using a fingerprint when offline authentication is required because of app inactivity. Users still have to enter a PIN when signing on to Secure Hub for the first time, restarting the device, and after the inactivity timer expires. For information about enabling fingerprint authentication, see Fingerprint or touch ID authentication.

### Certificate pinning

Secure Hub for iOS and Android supports SSL certificate pinning. This feature ensures that the certificate signed by your enterprise is used when Citrix clients communicate with Endpoint Management, thus preventing connections from clients to Endpoint Management when installation of a root certificate on the device compromises the SSL session. When Secure Hub detects any changes to the server public key, Secure Hub denies the connection.

As of Android N, the operating system no longer allows user-added certificate authorities (CAs). Citrix recommends using a public root CA in place of a user-added CA.

Users upgrading to Android N might experience problems if they use private or self-signed CAs. Connections on Android N devices break under the following scenarios:

- Private/self-signed CAs and the Required Trusted CA for Endpoint Management option is set **ON.** For details, see Device management.
- Private/self-signed CAs and the Endpoint Management AutoDiscovery Service (ADS) are not reachable. Due to security concerns, when ADS is not reachable, Required Trusted CA turns **ON** even it was set as **OFF** initially.

Before you enroll devices or upgrade Secure Hub, consider enabling certificate pinning. The option is **Off** by default and managed by the ADS. When you enable certificate pinning, users cannot enroll in Endpoint Management with a self-signed certificate. If users try to enroll with a self-signed certificate, they are warned that the certificate is not trusted. Enrollment fails if users do not accept the certificate.

To use certificate pinning, request that Citrix upload certificates to the Citrix ADS server. Open a technical support case using the Citrix Support portal. Ensure that you don't send the private key to Citrix. Then, provide the following information:

- The domain containing the accounts with which users enroll.
- The Endpoint Management fully qualified domain name (FQDN).
- The Endpoint Management instance name. By default, the instance name is zdm and is case-sensitive.
- User ID Type, which can be either UPN or Email. By default, the type is UPN.
- The port used for iOS enrollment if you changed the port number from the default port 8443.
- The port through which Endpoint Management accepts connections if you changed the port number from the default port 443.
- The full URL of your Citrix Gateway.
- Optionally, an email address for your administrator.
- The PEM-formatted certificates you want added to the domain, which must be public certificates and not the private key.
- How to handle any existing server certificates: Whether to remove the old server certificate immediately (because it is compromised) or to continue to support the old server certificate until it expires.

Your technical support case is updated when your details and certificate have been added to the Citrix servers.

#### Certificate + one-time-password authentication

You can configure Citrix ADC so that Secure Hub authenticates using a certificate plus a security token that serves as a one-time password. This configuration provides a strong security option that doesn't leave an Active Directory footprint on devices.

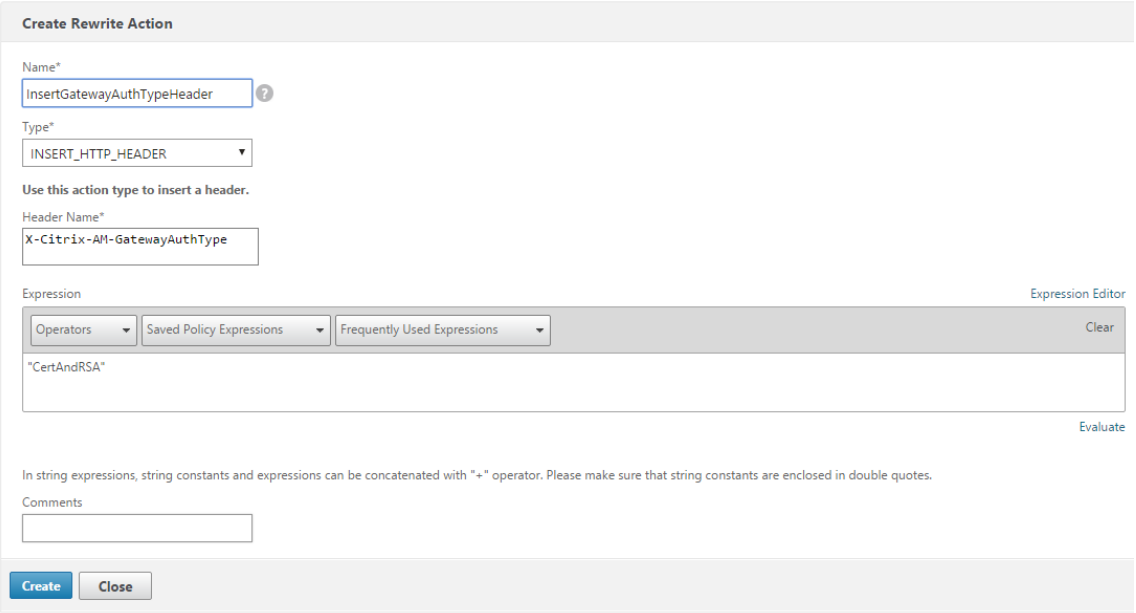
To enable Secure Hub to use the certificate + one-time-password type of authentication, do the following: Add a rewrite action and a rewrite policy in Citrix ADC that inserts a custom response header of the form **X-Citrix-AM-GatewayAuthType: CertAndRSA** to indicate the Citrix Gateway logon type.

Ordinarily, Secure Hub uses the Citrix Gateway logon type configured in the Endpoint Management console. However, this information isn't available to Secure Hub until Secure Hub completes logon for the first time. Therefore, the custom header is required.

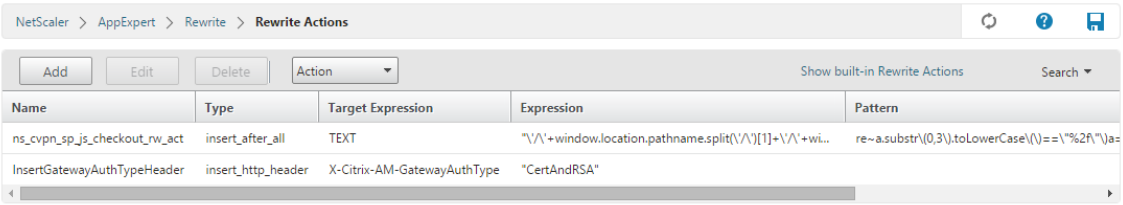
> **Note:**
>
> If different logon types are set for Endpoint Management and Citrix ADC, the Citrix ADC configuration overrides. For details, see Citrix Gateway and Endpoint Management.

1. In Citrix ADC, navigate to **Configuration > AppExpert > Rewrite > Actions**.
2. Click **Add**.

   The **Create Rewrite Action** screen appears.
3. Fill in each field as shown in the following figure and then click **Create**.

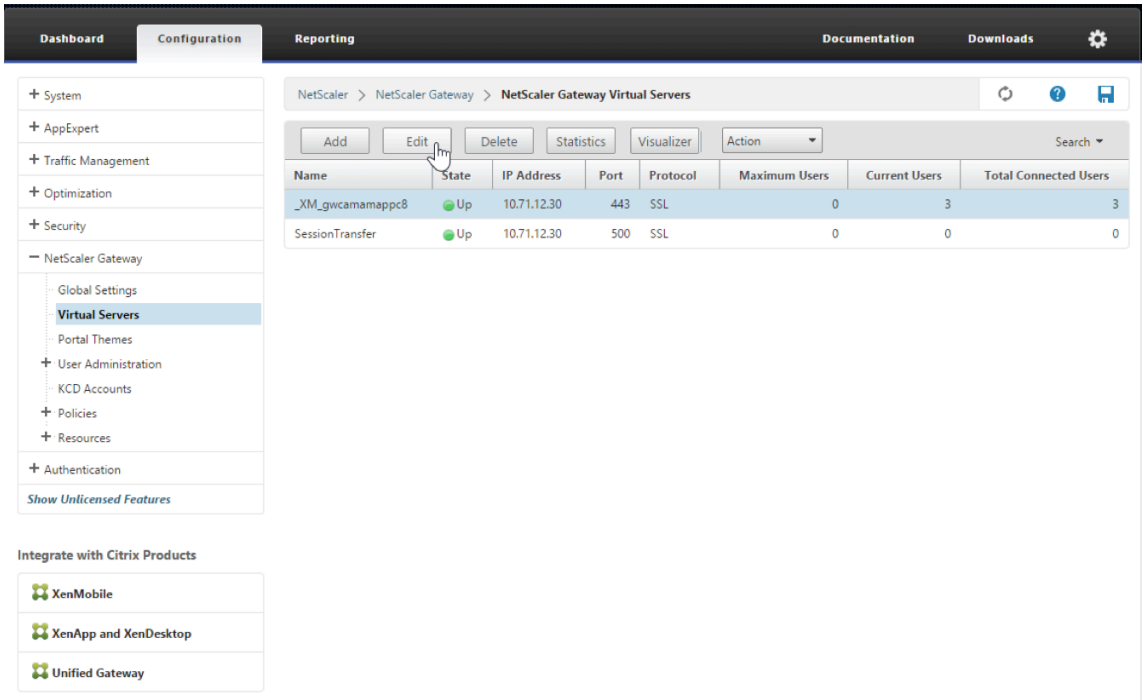



   The following result appears on the main **Rewrite Actions** screen.

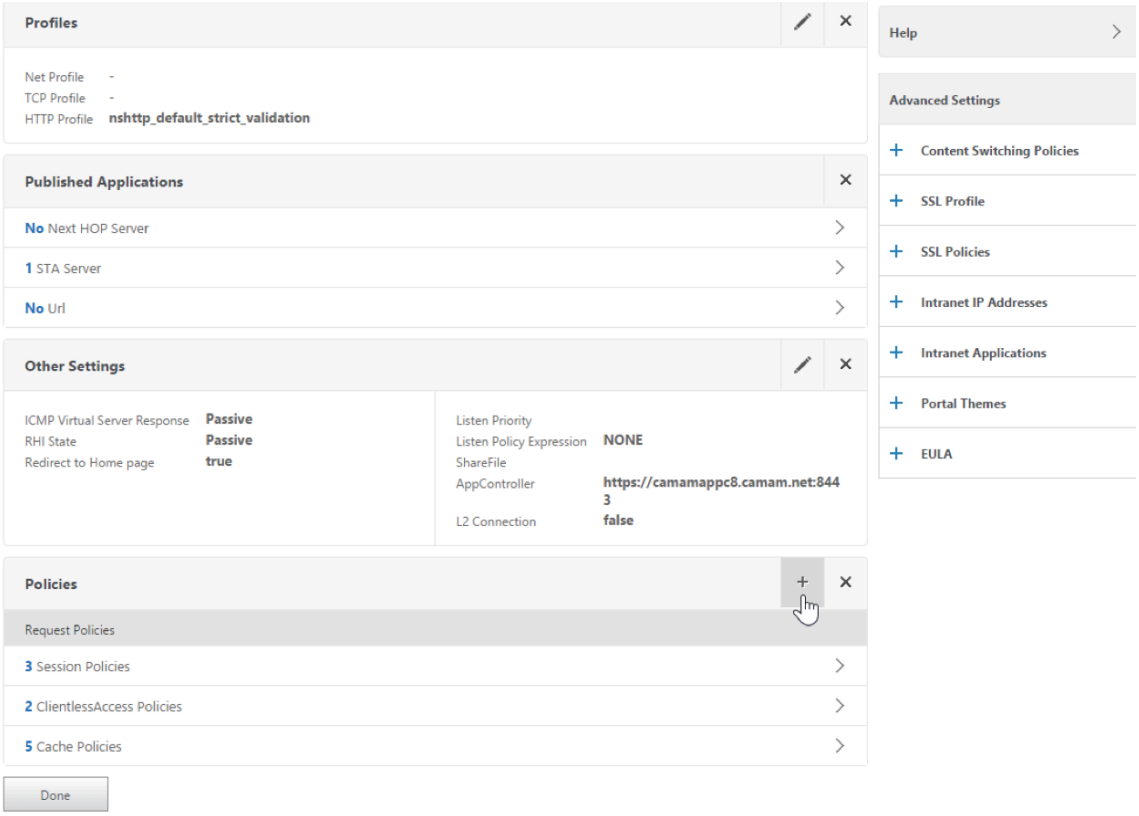



4. Bind the rewrite action to the virtual server as a rewrite policy. Go to **Configuration > NetScaler Gateway > Virtual Servers** and then select your virtual server.

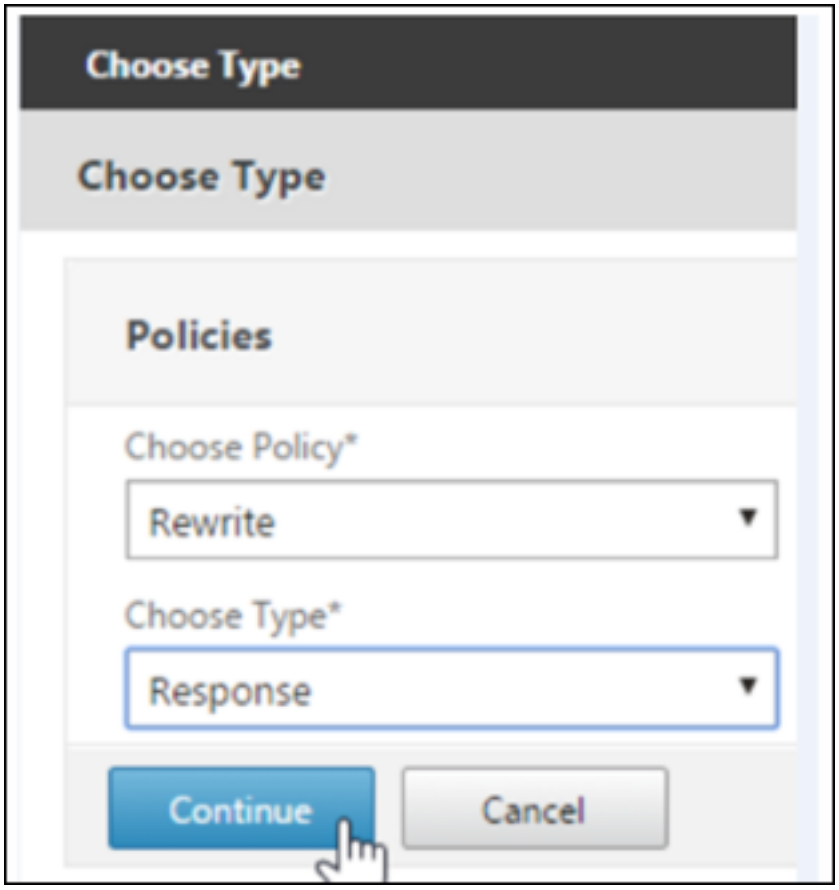



5. Click **Edit**.
6. On the **Virtual Servers configuration** screen, scroll down to **Policies**.
7. Click **+** to add a policy.



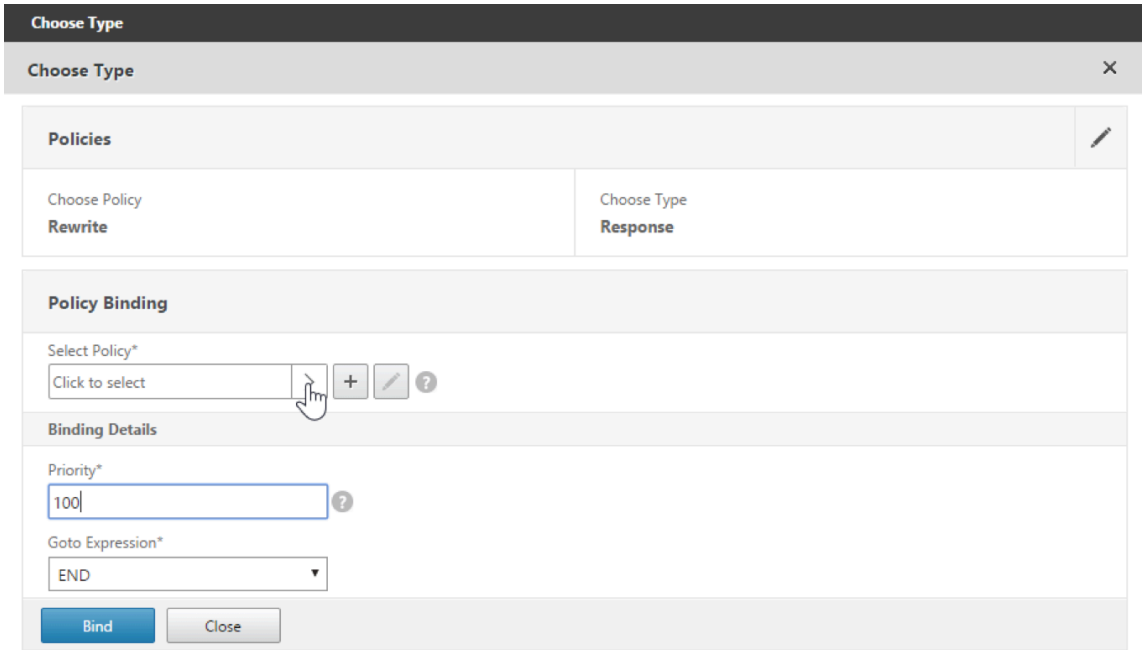
8. In the **Choose Policy** field, choose **Rewrite**.
9. In the **Choose Type** field, choose **Response**.




10. Click **Continue**.

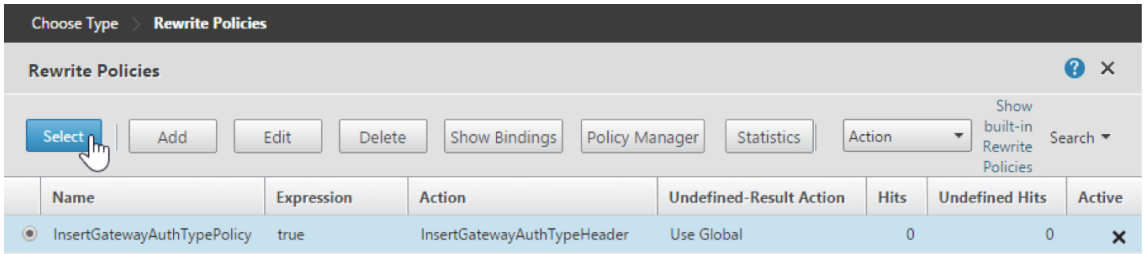
    The **Policy Binding** section expands.



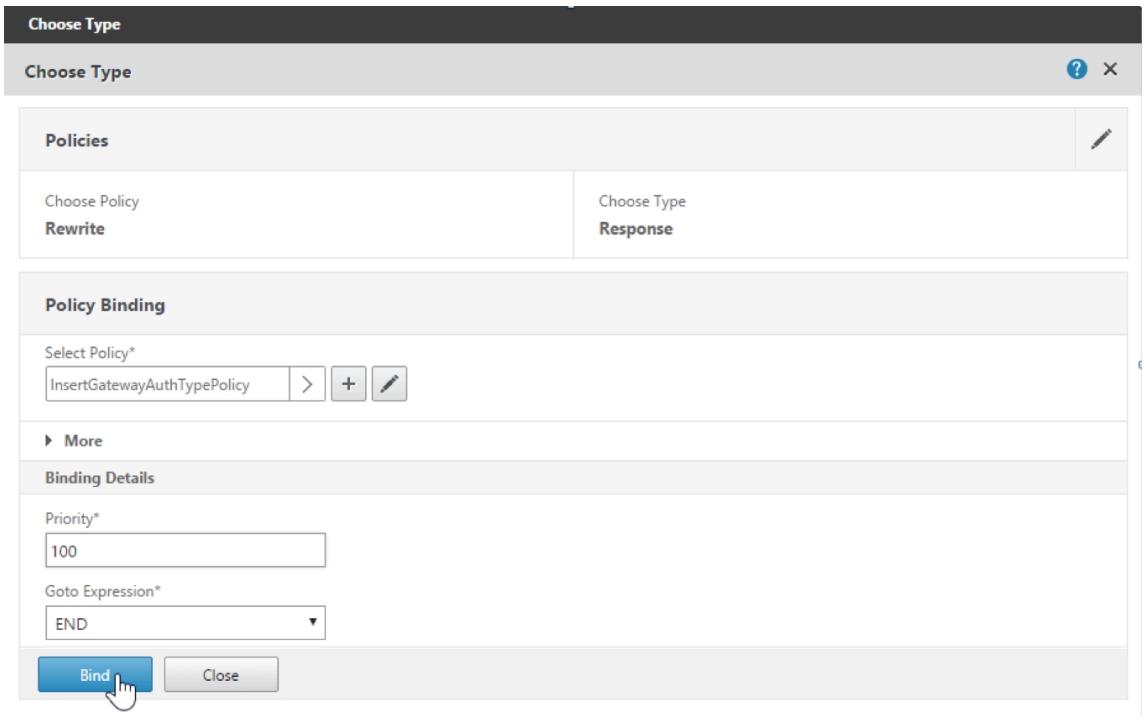

11. Click **Select Policy**.

    A screen with available policies appears.



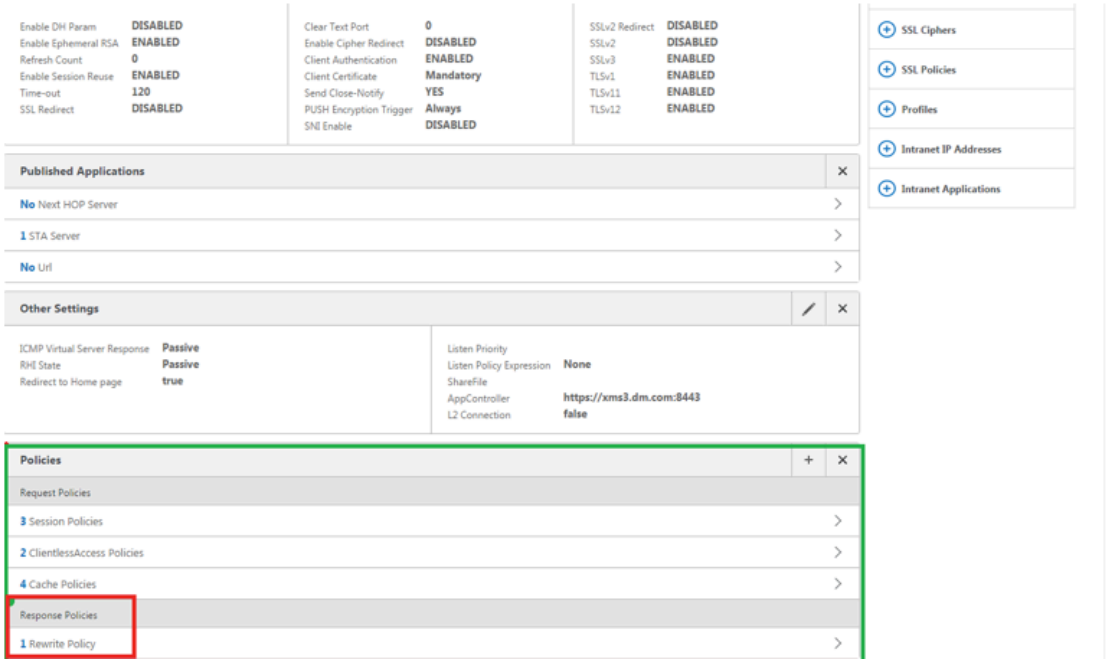

12. Click the row of the policy you created and then click **Select**. The **Policy Binding** screen appears again, with your selected policy filled in.



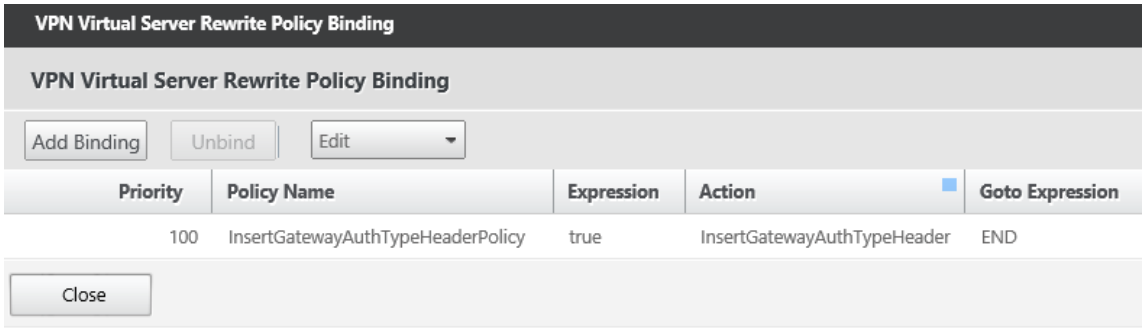

13. Click **Bind**.

    If the bind is successful, the main configuration screen appears with the completed rewrite policy shown.




14. To view the policy details, click **Rewrite Policy**.




**Port requirement for ADS connectivity for Android devices** Port configuration ensures that Android devices connecting from Secure Hub can access the Citrix ADS from within the corporate network. The ability to access ADS is important when downloading security updates made available through ADS. ADS connections might not be compatible with your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

> **Important:**
>
> Secure Hub for Android and iOS require you to allow Android devices to access ADS. For details, see Port requirements in the Citrix Endpoint Management documentation. This communication is on outbound port 443. It's highly likely that your existing environment is designed to allow this access. Customers who cannot guarantee this communication are discouraged from upgrading to Secure Hub 10.2. If you have any questions, contact Citrix support.

**Prerequisites:**

- Collect Endpoint Management and Citrix ADC certificates. The certificates must be in PEM format and must be a public certificate and not the private key.
- Contact Citrix support and place a request to enable certificate pinning. During this process, you are asked for your certificates.

The new certificate pinning improvements require that devices connect to ADS before the device enrolls. This prerequisite ensures that the latest security information is available to Secure Hub for the environment in which the device is enrolling. If devices cannot reach ADS, Secure Hub does not allow enrollment of the device. Therefore, opening up ADS access within the internal network is critical to enable devices to enroll.

To allow access to the ADS for Secure Hub for Android, open port 443 for the following IP addresses and FQDN:

| FQDN | IP address | Port | IP and port usage |
|---|---|---|---|
| `discovery.mdm.zenprise.com` | 52.5.138.94 | 443 | Secure Hub - ADS Communication |
| `discovery.mdm.zenprise.com` | 52.1.30.122 | 443 | Secure Hub - ADS Communication |
| `ads.xm.cloud.com`: note that Secure Hub version 10.6.15 and later uses `ads.xm.cloud.com`. | 34.194.83.188 | 443 | Secure Hub - ADS Communication |
| `ads.xm.cloud.com`: note that Secure Hub version 10.6.15 and later uses `ads.xm.cloud.com`. | 34.193.202.23 | 443 | Secure Hub - ADS Communication |

If certificate pinning is enabled:

- Secure Hub pins your enterprise certificate during device enrollment.
- During an upgrade, Secure Hub discards any currently pinned certificate and then pins the server certificate on the first connection for enrolled users.

  > **Note:**
  >
  > If you enable certificate pinning after an upgrade, users must enroll again.

- Certificate renewal does not require reenrollment, if the certificate public key did not change.

Certificate pinning supports leaf certificates, not intermediate or issuer certificates. Certificate pinning applies to Citrix servers, such as Endpoint Management and Citrix Gateway, and not third-party servers.

#### Disabling the Delete Account option

You can disable the **Delete Account** option in Secure Hub in environments where the Auto Discovery Services (ADS) is enabled.

Perform the following steps to disable the **Delete Account** option:

1. Configure ADS for your domain.

2. Open the **AutoDiscovery Service Information** in Citrix Endpoint Management and set the value for `displayReenrollLink` to **False**.
   By default this value is **True**.
3. If your device is enrolled in the MDM+MAM (ENT) mode, log off and log in again for the changes to take effect.
   If your device is enrolled in other modes, you must re-enroll the device.

### Using Secure Hub

Users begin by downloading Secure Hub on to their devices from the Apple or Android store.

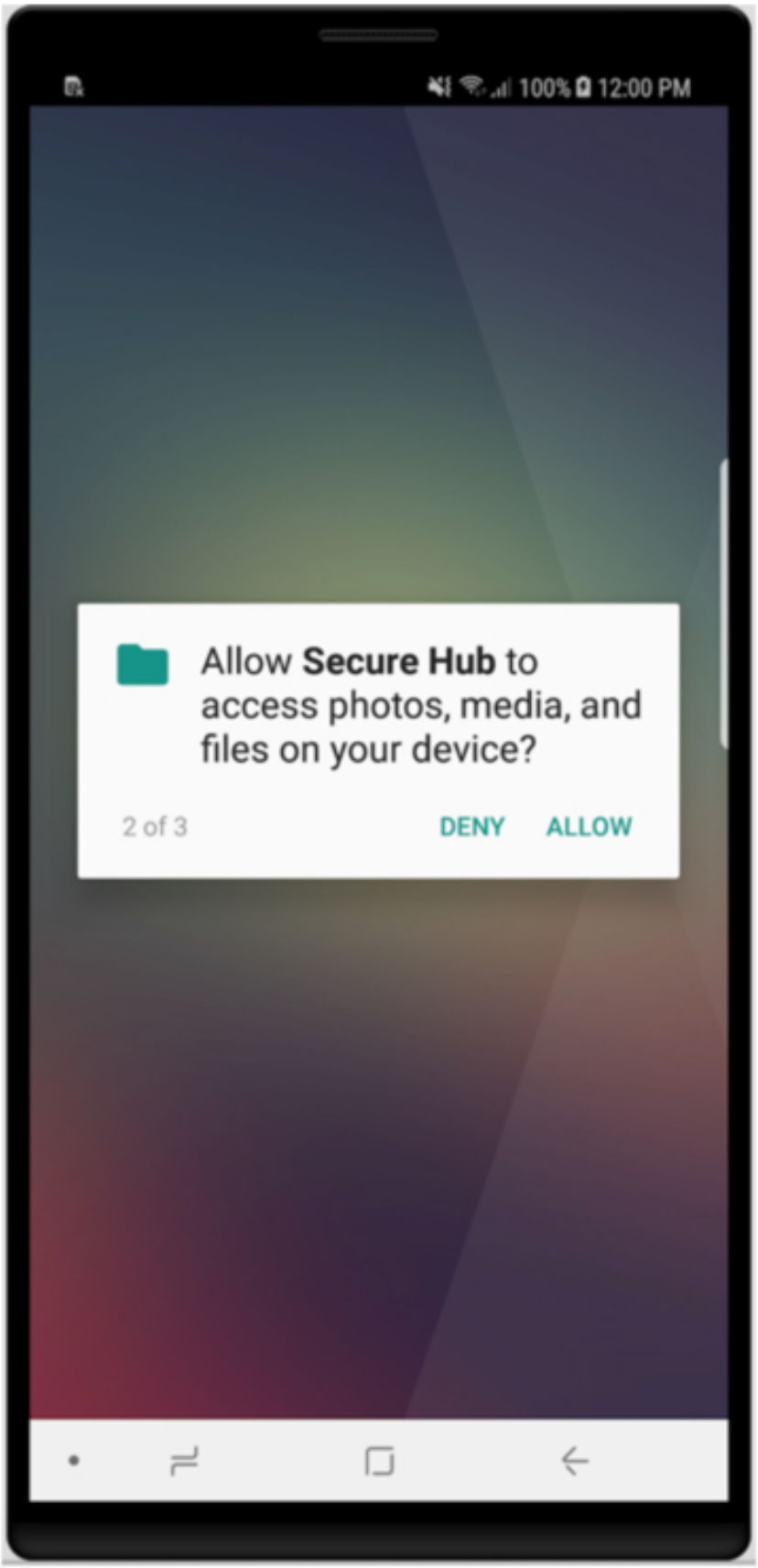
When Secure Hub opens, users enter the credentials provided by their companies to enroll their devices in Secure Hub. For more details about device enrollment, see User accounts, roles, and enrollment.

On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

This message comes from the Android operating system and not from Citrix. When you tap **Allow**, Citrix and the admins who manage Secure Hub do not view your personal data at any time. If however, you conduct a remote support session with your admin, the admin can view your personal files within the session.

Once enrolled, users see any apps and desktops that you've pushed in their **My Apps** tab. Users can add more apps from the Store. On phones, the Store link is under the **Settings** hamburger icon in the upper left-hand corner.

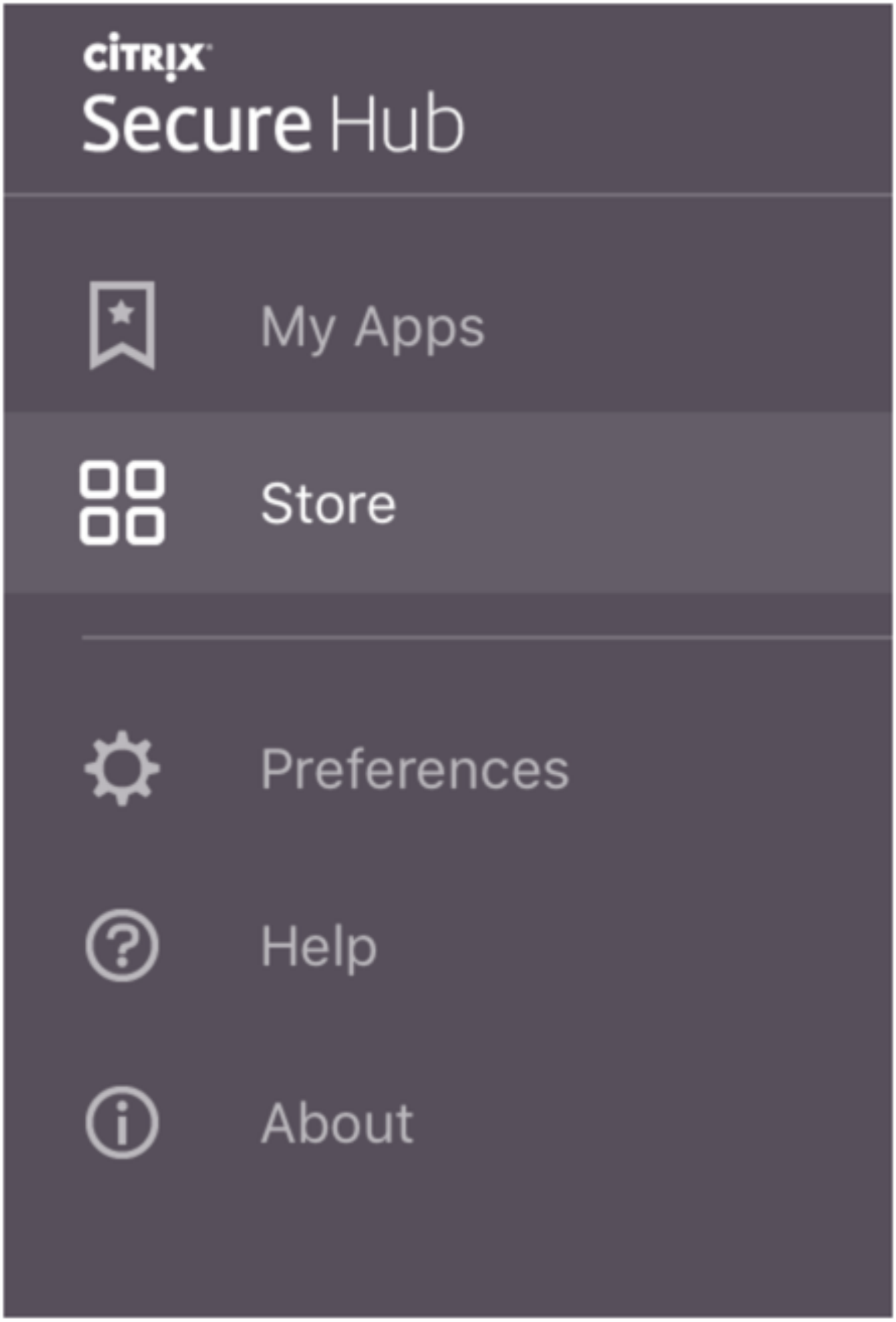
 



On tablets, the Store is a separate tab.



When users with iPhones running iOS 9 or later install mobile productivity apps from the store, they see a message. The message states that the enterprise developer, Citrix, is not trusted on that iPhone. The message notes that the app is not available for use until the developer is trusted. When this message appears, Secure Hub prompts users to view a guide that coaches them through the process of trusting Citrix enterprise apps for their iPhone.

### Automatic enrollment in Secure Mail

For MAM-only deployments, you can configure Endpoint Management so that users with Android or iOS devices who enroll in Secure Hub using email credentials are automatically enrolled in Secure Mail. Users do not have to enter more information or take more steps to enroll in Secure Mail.

On first-time use of Secure Mail, Secure Mail obtains the user's email address, domain, and user ID from Secure Hub. Secure Mail uses the email address for AutoDiscovery. The Exchange Server is identified using the domain and user ID, which enables Secure Mail to authenticate the user automatically. The user is prompted to enter a password if the policy is set to not pass through the password. The user is not, however, required to enter more information.

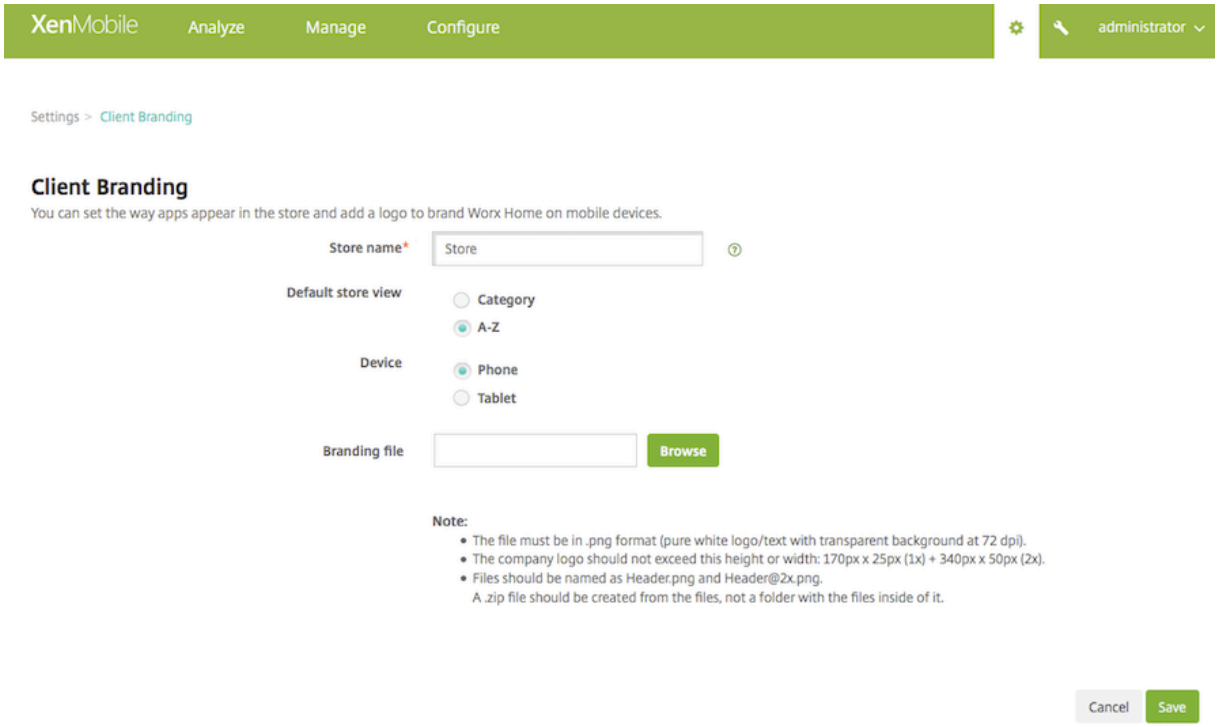
To enable this feature, create three properties:

- The server property MAM_MACRO_SUPPORT. For instructions, see Server properties.
- The client properties ENABLE_CREDENTIAL_STORE and SEND_LDAP_ATTRIBUTES. For instructions, see Client properties.

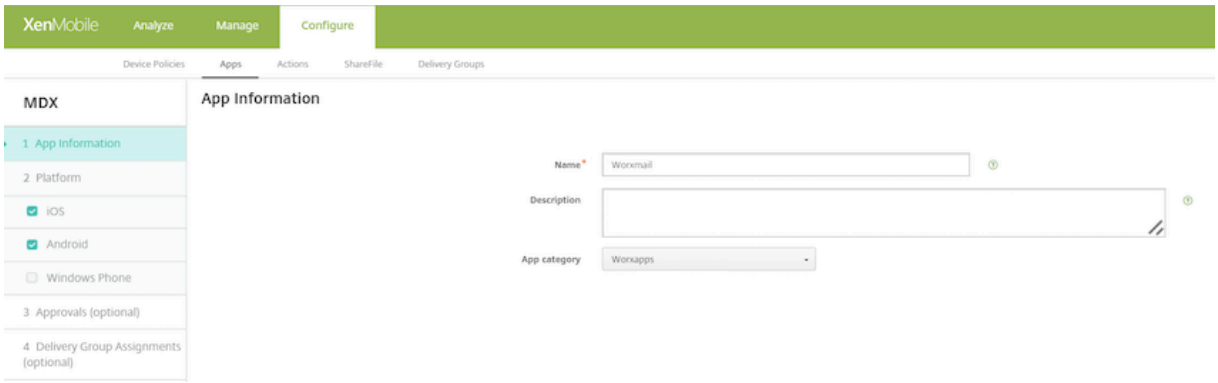
### Customized Store

If you want to customize your Store, go to **Settings > Client Branding** to change the name, add a logo, and specify how the apps appear.




You can edit app descriptions in the Endpoint Management console. Click **Configure** then click **Apps**. Select the app from the table and then click **Edit**. Select the platforms for the app with the description you're editing and then type the text in the **Description** box.

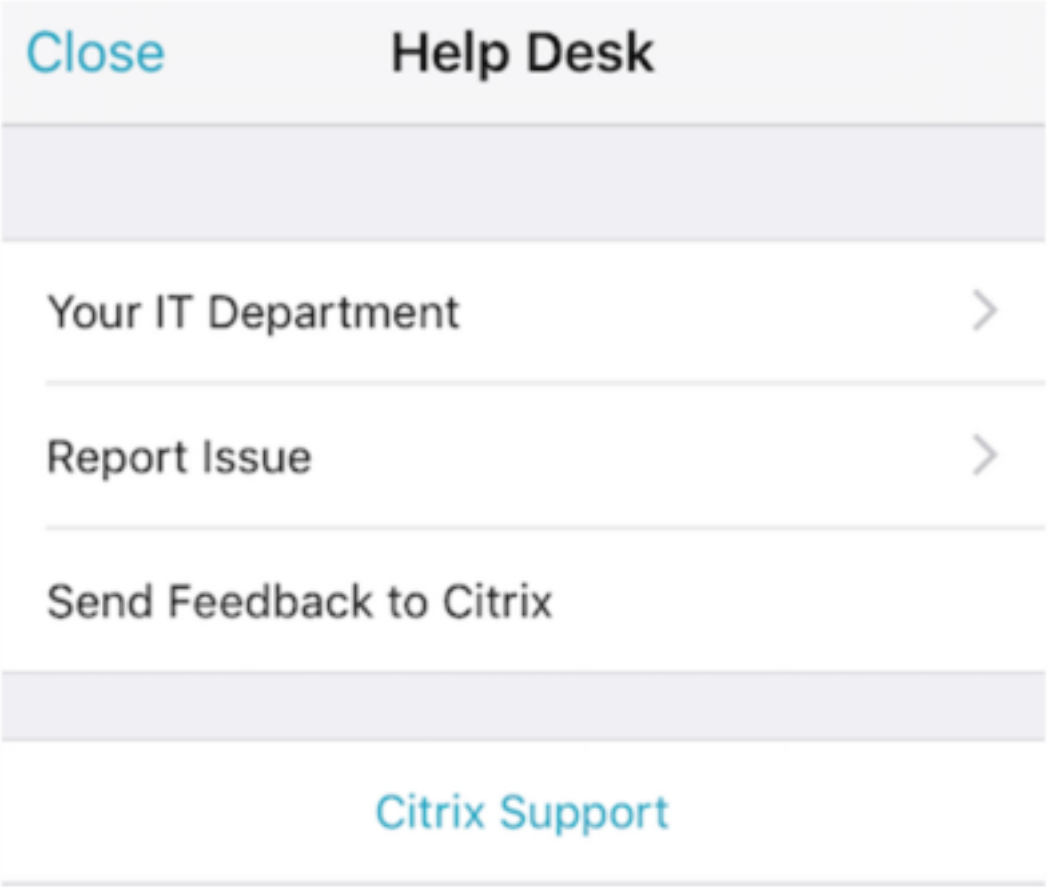



In the Store, users can browse only those apps and desktops that you've configured and secured in Endpoint Management. To add the app, users tap **Details** and then tap **Add**.

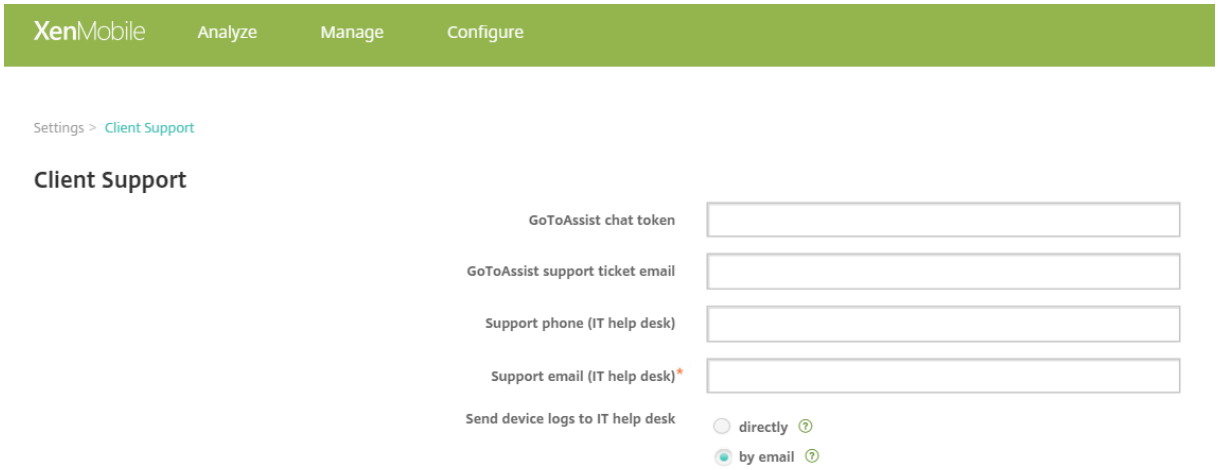
### Configured Help options

Secure Hub also offers users various ways to get help. On tablets, tapping the question mark in the upper-right corner opens help options. On phones, users tap the hamburger menu icon in the upper-left corner and then tap **Help**.




**Your IT Department** shows the telephone and email of your company help desk, which users can access directly from the app. You enter phone numbers and email addresses in the Endpoint Management console. Click the gear icon in the upper-right corner. The **Settings** page appears. Click **More** and then click **Client Support**. The screen where you enter the information appears.




**Report Issue** shows a list of apps. Users select the app that has the issue. Secure Hub automatically

generates logs and then opens a message in Secure Mail with the logs attached as a zip file. Users add subject lines and descriptions of the issue. They can also attach a screenshot.

**Send Feedback to Citrix** opens a message in Secure Mail with a Citrix support address filled in. In the body of the message, the user can enter suggestions for improving Secure Mail. If Secure Mail isn't installed on the device, the native mail program opens.

Users can also tap **Citrix Support,** which opens the Citrix Knowledge Center. From there, they can search support articles for all Citrix products.

In **Preferences**, users can find information about their accounts and devices.

### Location policies

Secure Hub also provides geo-location and geo-tracking policies if, for example, you want to ensure that a corporate-owned device does not breach a certain geographic perimeter. For details, see Location device policy.

### Crash collection and analysis

Secure Hub automatically collects and analyzes failure information so you can see what led to a particular failure. The software Crashlytics supports this function.

For more features available for iOS and Android, see the Features by platform matrix for Citrix Secure Hub.

### Generate device side logs for Secure Hub

This section explains how to generate the Secure Hub device side logs and to setup the correct debug level on them.

To obtain the Secure Mail logs do the following:

1. Go to **Secure Hub > Help > Report Issue**. Select Secure Mail from the list of apps.
   An email addressed to your organization help desk opens.
2. Change log settings only if your support team has instructed you to do so. Always confirm that the settings are properly set.
3. Return to Secure Mail and reproduce the issue. Note the time when the issue started to be reproduced, and the time when the issue happens or error message is displayed.
4. Return to **Secure Hub > Help > Report Issue**. Select Secure Mail from the list of apps.
   An email addressed to your organization help desk opens.

5. Fill in the subject line and body with a few words describing your issue. Include the timestamps gathered in step 3, and click **Send**.
   The completed message opens with zipped log files attached.
6. Click **Send** again.

   The zip files sent include the following logs:

   - CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt, and WH_logx.txt (Windows Phone)

   App info logs include information about the device and app.

## Secure Mail overview

May 30, 2024

Citrix Secure Mail lets users manage their email, calendars, and contacts on their mobile phones and tablets. To maintain continuity from Microsoft Outlook or IBM Notes accounts, Secure Mail syncs with Microsoft Exchange Server and IBM Notes Traveler Server.

As part of the Citrix suite of apps, Secure Mail benefits from single sign-on (SSO) compatibility with Citrix Secure Hub. After users sign on to Secure Hub, they can move seamlessly into Secure Mail without having to reenter their user names and passwords. You can configure Secure Mail to be pushed to users' devices automatically when the devices enroll in Secure Hub, or users can add the app from the Store.

> **Note:**
>
> Support for Exchange Server 2010 ended on October 13, 2020.

Secure Mail is compatible with:

- Exchange Server 2019 Cumulative Update 14
- Exchange Server 2019 Cumulative Update 13
- Exchange Server 2019 Cumulative Update 12
- Exchange Server 2019 Cumulative Update 11
- Exchange Server 2019 Cumulative Update 10
- Exchange Server 2019 Cumulative Update 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2016 Cumulative Update 23

- Exchange Server 2016 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 21
- Exchange Server 2016 Cumulative Update 20
- Exchange Server 2016 Cumulative Update 19
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- HCL Domino version 12.0.2 FP2
- HCL Traveler version 12.0.2.1 Build 202302010413_30
- HCL Domino 11 (formerly Lotus Notes)
- HCL Domino 10.0.1 (formerly Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (formerly Lotus Notes)
- HCL Domino 10.0.1.0 build 201811191126_20 (formerly Lotus Notes)
- HCL Domino 9.0.1.21 (formerly Lotus Notes)
- Microsoft Office 365 (Exchange Online)

To begin, download Secure Mail and other Endpoint Management components from Citrix Endpoint Management Downloads.

For Secure Mail and other mobility app system requirements, see System requirements.

For information about notifications in Secure Mail for iOS and Android when the app is running in the background or closed, see Push notifications for Secure Mail.

For iOS features supported on Secure Mail, see iOS features for Secure Mail.

For Android features supported on Secure Mail, see Android features for Secure Mail.

For iOS and Android features supported on Secure Mail, see iOS and Android features for Secure Mail.

For user help documentation, see the Citrix Secure Mail page in the Citrix User Help Center.

## Citrix Secure Web

July 11, 2023

Citrix Secure Web is an HTML5 compatible mobile web browser that provides secure access to internal and external sites. You can configure Secure Web to be pushed to user devices automatically when the devices are enrolled in Secure Hub. Alternatively, you can add the app from the Endpoint Management app store.

For Secure Web and other mobile productivity apps system requirements, see System requirements.

## Integrating and delivering Secure Web

> **Note:**
>
> The MDX Toolkit 10.7.10 is the final release that supports the wrapping of mobile productivity apps. Users access mobile productivity apps versions 10.7.5 and later from the public app stores.

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

1. To enable Single sign-on (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"later in this article.

## Configuring user connections

Secure Web supports the following configurations for user connections:

- **Tunneled –Web SSO:** Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Tunneled –Web SSO. This is the default configuration specified for the **Preferred VPN mode** policy. Tunneled –Web SSO 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. Secure Web, however, is not an app that can read client certificates stored on a mobile device. Some third-party, wrapped enterprise apps may be installed that can offer this capability. Full VPN tunnel handles any protocol over TCP and can be used with Windows and Mac computers, in addition to iOS and Android devices.

- The **Permit VPN mode switching** policy allows automatic switching between the full VPN tunnel and Tunneled –Web SSO 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, full VPN tunnel mode accomodates server challenges for client certificates, but not the Tunneled –Web SSO mode. Similarly, HTTP authentication challenges are more likely to be serviced with SSO when using Tunneled –Web SSO mode.

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 |
|---|---|---|---|---|---|---|
| Tunneled – Web SSO | HTTP | No | Yes | No | No | No |
| Tunneled – Web SSO | 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 |

## 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 decides the action to take, 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 open any sites in Training.lab domain (intranet) via HTTP or HTTPS. However, you cannot open public URLs such as Facebook, Google, and Hotmail, regardless of the 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 Tunneled –Web SSO 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

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 6.x/7.x Secure Web |
|---|---|---|
| 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 |

| Technology | iOS Secure Web | Android 6.x/7.x Secure Web |
|---|---|---|
| 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 VPN on the device by navigating to **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. Provide your troubleshooting steps, including the tested browser and OS types. If Secure Web for iOS has rendering issues, 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 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/, and then delete all 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**. The archiving occurs in the background and can take a few minutes.
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**, type the path name ~/Library/Safari/ReadingListArchives/. Now compress the folder that has a random hex string as a file name. You can send this file 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. This includes 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:

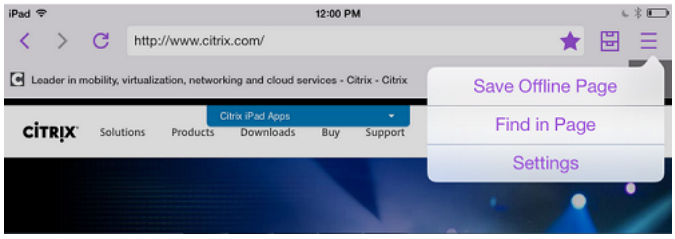
- Block pop-ups.

  > **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. The app displays the font that users set on their devices.

> **Note:**
>
> - Citrix Files for XenMobile reached EOL on July 1, 2023. For more information, see EOL and deprecated apps

## Citrix Content Collaboration for Endpoint Management

June 13, 2024

Citrix Content Collaboration for Endpoint Management clients are MDX-capable versions of Citrix Files mobile clients. These clients provide secure, integrated access to data in other MDX-wrapped apps. Citrix Content Collaboration for Endpoint Management clients also benefit from MDX features, such as micro VPN, single sign-on (SSO) with Secure Hub, and two-factor authentication.

Citrix Files is an enterprise file sync and sharing service that lets users exchange documents easily and securely. Citrix Files gives users various access options, including Citrix Files mobile clients, such as Citrix Files for Android Phone and Citrix Files for iPad.

You can integrate Citrix Files with Endpoint Management to provide the full Citrix Files feature set or to provide access only to storage zones connectors. By default, the Citrix Endpoint Management console enables configuration of Citrix Files only. To configure Endpoint Management for use with storage zones connectors instead, see Use Citrix Content Collaboration with Endpoint Management in the Citrix Endpoint Management documentation.

You use Endpoint Management, Citrix Files, storage zones controller, and Citrix ADC as follows to deploy and manage Citrix Content Collaboration for Endpoint Management clients:

- When Endpoint Management is configured with Citrix Files, Endpoint Management acts as a SAML identity provider (IdP) and deploys Citrix Content Collaboration for Endpoint Management clients. Citrix Files manages Citrix Files data. No Citrix Files data travels through Endpoint Management.
- When Endpoint Management is configured with Citrix Files or with storage zones connectors, the storage zones controller provides connectivity to data in network shares and SharePoint. Users access your stored data through the Citrix Files mobile productivity apps. Users can edit Microsoft Office documents, preview, and annotate Adobe PDF files from mobile devices.
- Citrix ADC manages requests from external users, securing their connections, load balancing requests, and handling content switching for storage zones connectors.

To download Citrix Content Collaboration for Endpoint Management clients, see Citrix downloads.

For Citrix Content Collaboration for Endpoint Management and other mobile productivity apps system requirements, see Support for mobile productivity apps.

## How Citrix Content Collaboration for Endpoint Management clients differ from Citrix Files mobile clients

The following describes the differences between Citrix Content Collaboration for Endpoint Management clients and Citrix Files mobile clients.

### User access

*Citrix Content Collaboration for Endpoint Management clients:*

Users obtain and open Citrix Content Collaboration for Endpoint Management clients from Secure Hub.

*Citrix Files mobile clients:*

Users obtain Citrix Files mobile clients from app stores.

### SSO

*Citrix Content Collaboration for Endpoint Management clients:*

For Endpoint Management integration with Citrix Files: You can configure Endpoint Management as a SAML IdP for Citrix Files. In this configuration, Secure Hub obtains a SAML token for the Citrix Content Collaboration for Endpoint Management client, using Endpoint Management as the SAML IdP. A user who starts the Citrix Content Collaboration for Endpoint Management client, but is not signed on to Secure Hub, is prompted to sign on to Secure Hub. The user does not have to know their Citrix Files domain or account information.

*Citrix Files mobile clients:*

You can configure Endpoint Management and Citrix Gateway as a SAML IdP for Citrix Files. In this configuration, a user logging on to Citrix Files using a web browser or other Citrix Files clients is redirected to the Endpoint Management environment for user authentication. After successful authentication by Endpoint Management, the user receives a SAML token that is valid for logon to their Citrix Files account.

### Micro VPN

*Citrix Content Collaboration for Endpoint Management clients:*

Remote users can connect using a VPN or micro VPN connection through Citrix Gateway to access apps and desktops in the internal network. This feature, available through Citrix ADC integration with Endpoint Management is transparent to users.

*Citrix Files mobile clients:*

Not applicable.

### Two-factor authentication

*Citrix Content Collaboration for Endpoint Management clients:*

Citrix ADC integration with Endpoint Management also supports authentication using a combination of client certificate authentication and another authentication type, such as LDAP or RADIUS.

*Citrix Files mobile clients:*

Not applicable.

### Folder permissions

*Citrix Content Collaboration for Endpoint Management clients and Citrix Files mobile clients:*

For Endpoint Management integration with Citrix Files: Determined by Citrix Files.

## Document access protection

*Citrix Content Collaboration for Endpoint Management clients:*

Users can open attachments received in Secure Mail or downloaded by any MDX-wrapped app. Only MDX-wrapped apps appear when the user performs an Open In action. Data that is from a non-wrapped app is not available to a Citrix Content Collaboration for Endpoint Management client. Secure Mail users can attach files from their Citrix Files repository without needing to download the file to the device. If a user has wrapped and unwrapped Citrix Files on a device, the wrapped Citrix Files client cannot access files in the user's personal Citrix Files account. The wrapped Citrix Files client can access only the Citrix Files subdomain configured in Endpoint Management.

*Citrix Files mobile clients:*

Users can open attachments from any app.

### Citrix Files account access

*Citrix Content Collaboration for Endpoint Management clients:*

For Endpoint Management integration with Citrix Files: To access a personal Citrix Files account or a third-party Citrix Files account, users must use a non-MDX version of Citrix Files on the device.

*Citrix Files mobile clients:*

For Endpoint Management integration with Citrix Files: Available from Citrix Files clients.

#### Device policies

*Citrix Content Collaboration for Endpoint Management clients and Citrix Files mobile clients:*

Both Endpoint Management and Citrix Files device policies apply to Citrix Content Collaboration for Endpoint Management clients. For example, from the Endpoint Management console, you can perform a device wipe. From the Citrix Files console, you can remotely wipe the Citrix Files app.

#### MDX policies

*Citrix Content Collaboration for Endpoint Management clients:*

MDX policies let you configure settings in Citrix Endpoint Management that the Endpoint Management app store enforces. Policies available only through MDX include the ability to block the camera, mic, email compose, screen capture, and clipboard cut, copy, and paste operations.

*Citrix Files mobile clients:*

Not applicable.

#### Data encryption

*Citrix Content Collaboration for Endpoint Management clients and Citrix Files mobile clients:*

Encrypts all stored data using AES-256 and protects data in transit with SSL 3.0 and a minimum of 128-bit encryption.

#### Availability

*Citrix Content Collaboration for Endpoint Management clients:*

Citrix Content Collaboration for Endpoint Management clients are included with Endpoint Management Advanced and Enterprise editions.

*Citrix Files mobile clients:*

All Endpoint Management editions include all Citrix Files features. You can integrate Endpoint Management with the full Citrix Files feature set or just storage zones connectors.

### Integrating and delivering Citrix Content Collaboration for Endpoint Management clients

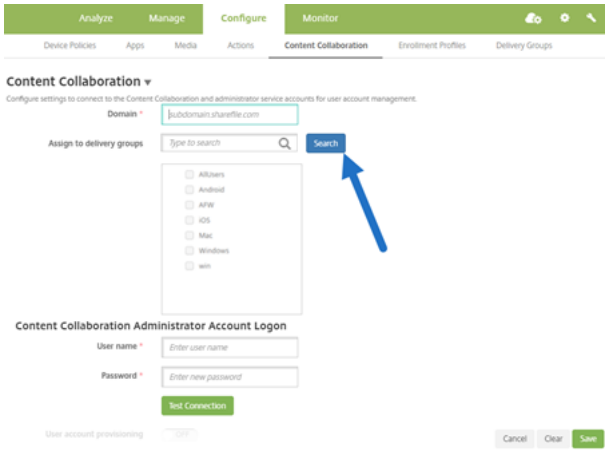
To integrate and deliver Citrix Content Collaboration for Endpoint Management clients, follow these general steps:

1. Enable Endpoint Management as a SAML IdP for Citrix Files, to provide SSO from Citrix Files clients to Citrix Files. To do so, you must configure Citrix Files account information in Endpoint Management. For more information, see "To configure Citrix Files account information in Endpoint Management for SSO"section.

   > **Important:**
   >
   > To use Endpoint Management as an SAML IdP for non-MDX Citrix Files clients, such as the Citrix Files web app and the Citrix Files Sync clients, extra configuration is required. For details, see this article on the Citrix Files support site:
   >
   > Citrix Files (ShareFile) Single Sign-On SSO. The article contains a download link to the Endpoint Management configuration guide.

2. Download the Citrix Files clients.
3. Add the Citrix Files clients to Endpoint Management. For details, see "To add Citrix Files to Endpoint Management"later in this article.
4. Validate your configuration. For details, see "To validate Citrix Files clients,"later in this article.




**About the settings:**

- Domain is the Citrix Files subdomain to be used for the clients.
- Only the users in the selected DGs have SSO access to Citrix Files from the clients.

  If a user in a DG does not have a Citrix Files account, Endpoint Management provisions the user into Citrix Files when you add the Citrix Files client to Endpoint Management.
- The Citrix Files Administrator Account Logon information is used by Endpoint Management to save the SAML settings in the Citrix Files control plane.

> **Important:**
>
> The configuration that enables SSO from Citrix Files clients to Citrix Files does not authenticate users to network shares or SharePoint document libraries. Access to those connector data sources requires authentication to the Active Directory domain in which the network shares or SharePoint servers reside.

### To configure Citrix Files account information in Endpoint Management for SSO

To enable SSO from Secure Hub to mobile productivity apps, you specify Citrix Files account and Citrix Files administrator service account information in the Endpoint Management console. With that configuration, Endpoint Management acts as a SAML IdP for Citrix Files, for mobile productivity app clients, Citrix Files clients, and non-MDX Citrix Files clients. When a user starts a mobile productivity app client, Secure Hub obtains a SAML token for the user from Endpoint Management and sends it to the Citrix Files client.

In the Endpoint Management console, click **Configure** > **Content Collaboration**, which is the former name of Citrix Files.

### To add Citrix Content Collaboration for Endpoint Management clients to Endpoint Management

When you add Citrix Content Collaboration for Endpoint Management clients to Endpoint Management, you can enable SSO access to Connector data sources from Citrix Content Collaboration for Endpoint Management clients. To do so, configure the Network access policy and the Preferred VPN mode policy as described in this section.

### Prerequisites

- Endpoint Management must be able to reach your Citrix Files subdomain. To test the connection, ping your Citrix Files subdomain from the Endpoint Management server.
- The time zone configured for your Citrix Files account and for the hypervisor running Endpoint Management must be the same. If the time zone differs, SSO requests can fail because the SAML token might not reach Citrix Files within the expected time frame. To configure the NTP server for Endpoint Management, use the Endpoint Management command-line interface.

  > **Note:**
  >
  > The Hyper-V host sets the time on a Linux VM to the local time zone and not UTC.

- Log in to the ShareFile Account as an admin and verify the SAML SSO settings in **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > **Single sign-on / SAML 2.0 Configuration**.

- Download Citrix Content Collaboration for Endpoint Management clients.

**Steps:**

1. In the Endpoint Management console, click **Configure > Apps** and then click **Add**.
2. Click **MDX**.
3. Enter a **Name** and, optionally, a **Description** and **App category** for the app.
4. Click **Next** and then upload the .mdx file for the Citrix Content Collaboration for Endpoint Management client.
5. Click **Next** to configure the app information and policies.

   The configuration that enables SSO from Citrix Content Collaboration for Endpoint Management clients to Citrix Files does not authenticate users to network shares or SharePoint document libraries.
6. To enable SSO between the Secure Hub micro VPN and storage zones controller, complete the following policy configuration:

   - Set the Network access policy to **Tunneled to the internal network**.

     In this mode, the MDX framework intercepts all network traffic from the Citrix Content Collaboration for Endpoint Management client. The network traffic is then redirected through Citrix Gateway using an app-specific micro VPN.
   - Set the Preferred VPN mode policy to **Tunneled –Web SSO**.

     In this mode of tunneling, the MDX framework terminates SSL/HTTP traffic from an MDX app, which then initiates new connections to internal connections on the user's behalf. This policy setting enables the MDX framework to detect and respond to authentication challenges issued by web servers.
7. Complete the Approvals and Delivery Group (DG) Assignments as needed.

Only the users in the selected DGs have SSO access to Citrix Files from the Citrix Content Collaboration for Endpoint Management clients. If a user in a DG does not have a Citrix Files account, Endpoint Management provisions the user into Citrix Files when you add the Citrix Content Collaboration for Endpoint Management client to Endpoint Management.

**To validate Citrix Content Collaboration for Endpoint Management clients**

1. After completing the configuration described in this article, start the Citrix Content Collaboration for Endpoint Management client. Citrix Files does not prompt you to sign on.
2. In Secure Mail, compose an email and add an attachment from Citrix Files. Your Citrix Files home page opens, without prompting you to sign on.

> **Note:**
>
> - Citrix Files for XenMobile has reached EOL on July 1, 2023. For more information, see EOL and deprecated apps

## EOL and deprecated apps

May 14, 2024

The following apps have reached End of Life(EOL) or is about to reach EOL status. When a product release reaches EOL, you can use the product within the terms of your product licensing agreement, but the available support options are limited. Historical information appears in the Knowledge Center or other online resources. The documentation is no longer updated and is provided on an as-is basis. For more information about product lifecycle milestones, see the Product Matrix.

> **Note:**
>
> For advanced notice of Citrix Endpoint Management features that are being phased out, see Deprecation.

**Citrix Files for XenMobile (MDX):** Citrix Files for XenMobile reached EOL on July 1, 2023.

We recommend customers to use Citrix Files available in Apple App store and Google Play. It is MAM SDK-ready.

**Secure Mail for Intune SDK (iOS & Android):** Secure Mail reached EOL on April 30, 2023.

**Citrix Files for Intune:** Deprecated in December 31, 2020.

We encourage you to explore the options of leveraging the platform capabilities to containerize the regular Citrix Files app (available in the app stores) via Android Enterprise (with Work Profile) and iOS User Enrollment.

**ShareConnect:** ShareConnect reached EOL on June 30, 2020.

**Secure Notes:** EOL lifecycle date was December 31, 2018.

If you require the capabilities of Secure Notes and Secure Tasks, we recommend Notate for Citrix, a third-party app that you can secure with MDX policies.

If users of Secure Notes and Secure Tasks stored data in Outlook, they can access the data in Notate. If users stored data in ShareFile, now Citrix Files, the data is not migrated.

Users can keep running Secure Notes beyond the EOL date, until their platform operating system stops supporting the user interface. We do not recommend, however, that you use an unsupported product.

**Secure Tasks:** EOL lifecycle date was December 31, 2018.

**Secure Forms:** EOL lifecycle date was March 31, 2018. Customers are encouraged to transition to Citrix ShareFile Workflows included with Citrix Files Platinum and Premium accounts. For details, see Citrix ShareFile Workflows.

**ScanDirect:** ScanDirect reached EOL on September 1, 2018.

## Allowing secure interaction with Office 365 apps

June 13, 2024

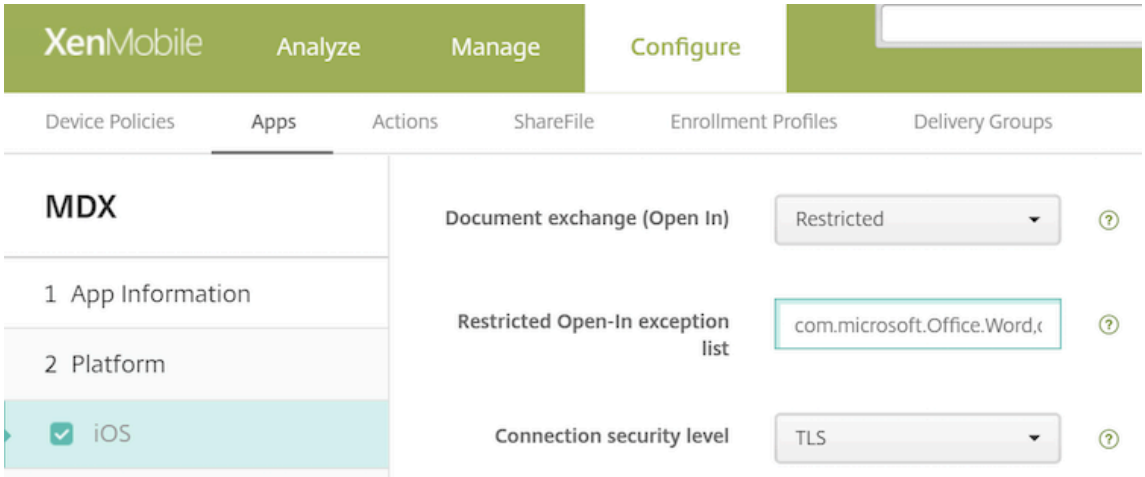
Citrix Secure Mail, Citrix Secure Web, and Citrix Files offer the option of opening the MDX container to allow users to transfer docs and data to Microsoft Office 365 apps. You manage this capability for iOS and Android platforms through the open-in policies on the Endpoint Management console.

Once opened in a Microsoft app, data is no longer secured or encrypted in the MDX container. Consider the security implications before enabling this feature. Particularly, customers concerned with data loss prevention or who are subject to HIPAA or other strict compliance requirements should weigh the trade-offs of opening the container.

### Enabling Office 365 in iOS

1. Download the latest versions of Secure Mail, Secure Web, or Citrix Files apps from the Endpoint Management downloads page.
2. Upload the files to the Endpoint Management console.
3. Locate the **Document exchange (Open In)** policy and set it to **Restricted**. In the **Restricted Open-in exception list**, Microsoft Word, Excel, PowerPoint, OneNote, and Outlook are automatically listed. For example: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook




In MDM enrollments, more controls are available for iOS devices.

You can upload iTunes apps to the Endpoint Management console and push the apps to devices. If you choose this option, set the following policies to **ON**:

- Remove app if MDM profile is removed
- Prevent app data backup
- Force the app to be managed (note that a selective wipe removes the app and any data)

To prevent documents and data flowing from Microsoft apps to unmanaged apps on the device, go to **Configure > Devices > Restrictions > iOS** on the Endpoint Management console and then set **Documents from managed apps in unmanaged apps** and **Documents from unmanaged apps in managed apps** to **OFF**.

### Enabling Office 365 in Android

1. Download the latest versions of Secure Mail, Secure Web, or Citrix Files apps from the Endpoint Management downloads page.
2. Upload the files to the Endpoint Management console.
3. Scroll down to the **Document exchange (Open In)** policy and then select **Restricted**.
4. In **Restricted Open-in exception list**, add the following package IDs:

   `{ package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }`
5. Configure other app policies as usual and the save the apps.

Users must save files from Secure Mail, Secure Web, or Citrix Files on their devices and open the files with an Office 365 app.

For both iOS and Android, users can open and edit the following types of files on their devices:

## Supported file formats

For the supported file formats, see the Microsoft Office documentation.