



Mobile productivity apps

Contents

Mobile productivity apps release timeline	3
Support for mobile productivity apps	3
Administrator tasks and considerations	5
Features by platform	16
Citrix Secure Hub	28
Secure Mail overview	55
Citrix Secure Web	56
Citrix QuickEdit for mobile productivity apps	67
ShareConnect	72
Citrix ShareFile Workflows	84
Citrix Content Collaboration for Endpoint Management	84
EOL and deprecated apps	91
Allowing secure interaction with Office 365 apps	92

Mobile productivity apps release timeline

April 30, 2020

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

October 6, 2021

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:

- 21.10.0 (Secure Mail and Secure Web for Android only)

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:

- 21.9.0 (Secure Mail and Secure Web only)
- 21.8.5 (Secure Mail and Secure Web for Android only)

Supported operating systems

The latest versions of Secure Hub, MDX Toolkit, and mobile productivity apps are compatible with the latest and two prior versions of Endpoint Management. For details, see [Supported device operating systems](#).

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

Note:

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

Supported devices for MDX encryption

Citrix supports MDX encryption on the following list of branded device families.

Android:

- Samsung Note
- Samsung Galaxy
- Google Pixel
- Motorola

iOS:

- All iOS devices with a supported OS version in the preceding list are supported for MDX encryption.

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. For details and updates, see this [Support Knowledge Center article](#).
- 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.

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. We are not applying the End of Life (EOL) status on September 1, 2018 that we had 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](#).

Secure Notes and Secure Tasks

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

Administrator tasks and considerations

June 16, 2021

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 in MDX since for the exclusion of domains from tunneling, see the [MDX Toolkit 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. For securing and deploying the native productivity apps on Windows devices, see the [Windows Information Protection device policy](#).

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

- <https://shouji.baidu.com>
- <https://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

Mobile productivity apps

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
	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](#)
- Citrix Developer section on [Device Management](#)
- [Citrix blog post](#)
- Download SDK when you sign on to [Citrix downloads](#)

Prerequisites

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

- Update your Citrix Endpoint Management to versions 10.12 RP2 and later, or 10.11 RP5 and later.
- Update your mobile apps to version 20.8.0 or later.
- Update the policies file to version 20.8.0 or later.
- If your organization uses third-party apps, 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**

The screenshot shows the Citrix Cloud Endpoint Management interface. The left sidebar contains a navigation menu with sections: MDX, 1 App Information, 2 Platform (with a 'Select All' link), 3 Approvals (optional), and 4 Delivery Group Assignments (optional). Under '2 Platform', the 'iOS' option is selected. The main content area is titled 'Configure' and shows the configuration for an app named 'Secure Mail'. Fields include: File name (Secure Mail), App Description (Managed Enterprise Application), App version (20.4.5), Minimum OS version (11.0), Maximum OS version, Excluded devices (example: manufacturer or model...), Remove app if MDM profile is removed (ON), Prevent app data backup (ON), Force app to be managed (ON), and App deployed via Volume purchase (OFF). A red box highlights the 'MDX or MAM SDK policy container' dropdown, which is currently set to 'Legacy MDX' and has 'MAM SDK' as an available option.

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 *secure browse*. The Preferred VPN mode policy controls that behavior. By default,

connections use secure browse, 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.

Secure Web for iOS and Android supports use of a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment. This situation is true if you use Citrix ADC for proxy authentication.

The Permit VPN mode switching policy allows automatic switching between the full VPN tunnel and secure browse modes as needed. By default, this policy is off. When this policy is on, a network request that fails due to an authentication request that cannot be handled in the preferred VPN mode is retried in the alternate mode. For example, server challenges for client certificates can be accommodated by the full VPN tunnel mode, but not secure browse mode. Similarly, HTTP authentication challenges are more likely to be serviced with SSO when using secure browse 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 of 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

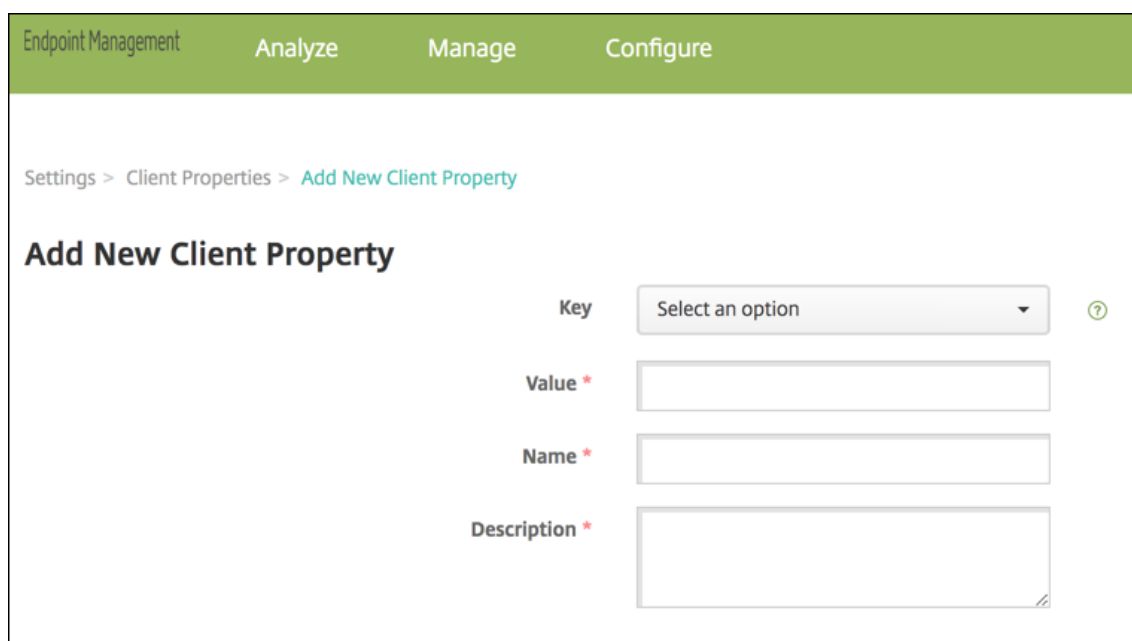
- iOS devices (minimum version 8.1) that support fingerprint authentication and have at least one fingerprint configured.
- User entropy must be off.

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](#).

Features by platform

September 15, 2021

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 article](#).

Citrix Secure Hub

Mobile productivity apps

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
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

Mobile productivity apps

Feature	iOS	Android
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
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

Mobile productivity apps

Feature	iOS	Android
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
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

Mobile productivity apps

Feature	iOS	Android
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	
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	

Mobile productivity apps

Feature	iOS	Android
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
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

Mobile productivity apps

Feature	iOS	Android
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 (Troubleshoot) option		X
Dual mode (MAM SDK)	X	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

Mobile productivity apps

Feature	iOS	Android
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	
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

Mobile productivity apps

Feature	iOS	Android
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
Dial in to WebEx or Lync meetings	X	X
Hide declined events	X	X
Display more than 3 simultaneous events	X	X

Mobile productivity apps

Feature	iOS	Android
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
View contacts with long press		X

Mobile productivity apps

Feature	iOS	Android
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

Mobile productivity apps

Feature	iOS	Android
Tap the back button on the device to dismiss the floating action button options		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
3D Touch actions	X	
Shared devices	X	X

Mobile productivity apps

Feature	iOS	Android
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

Citrix Secure Hub

October 6, 2021

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 the article [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, Secure Mail, Secure Web, and Citrix Workspace app in June 2020.

What's new in the current version

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.

What's new in earlier versions

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

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](#).

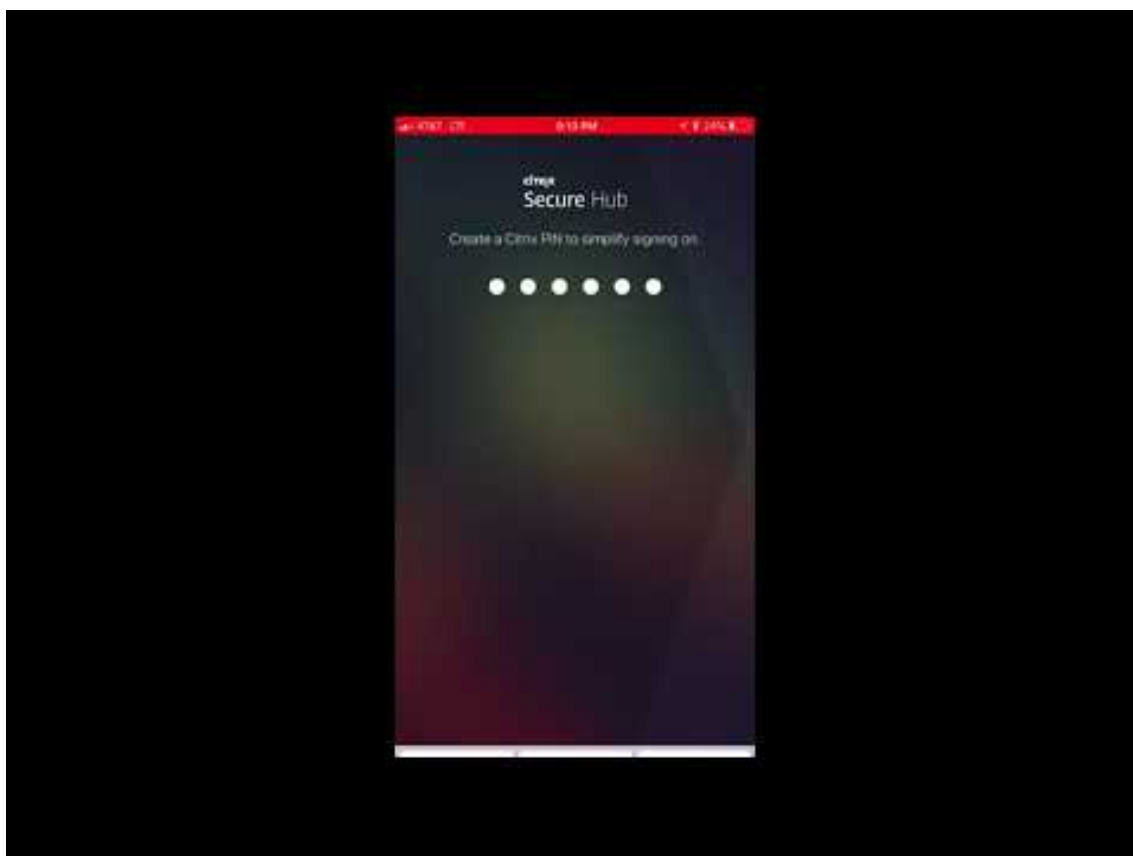
Secure Hub 10.8.60 to 18.9.0

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**.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader

Type*
INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

Expression
Expression Editor
Operators Saved Policy Expressions Frequently Used Expressions Clear
"CertAndRSA"
Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

Create Close

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

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\\'+window.location.pathname.split('\\')[1]+'\\'+wi...	re~a.substr(0,3).toLowerCase(\\)=\\'%2f\\)a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

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.

Mobile productivity apps

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

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

Profiles

- Net Profile -
- TCP Profile -
- HTTP Profile nshttp_default_strict_validation

Published Applications

- No Next HOP Server
- 1 STA Server
- No Url

Other Settings

ICMP Virtual Server Response	Passive	Listen Priority	
RHI State	Passive	Listen Policy Expression	NONE
Redirect to Home page	true	ShareFile	
		AppController	https://camamappc8.camam.net:8443
		L2 Connection	false

Policies

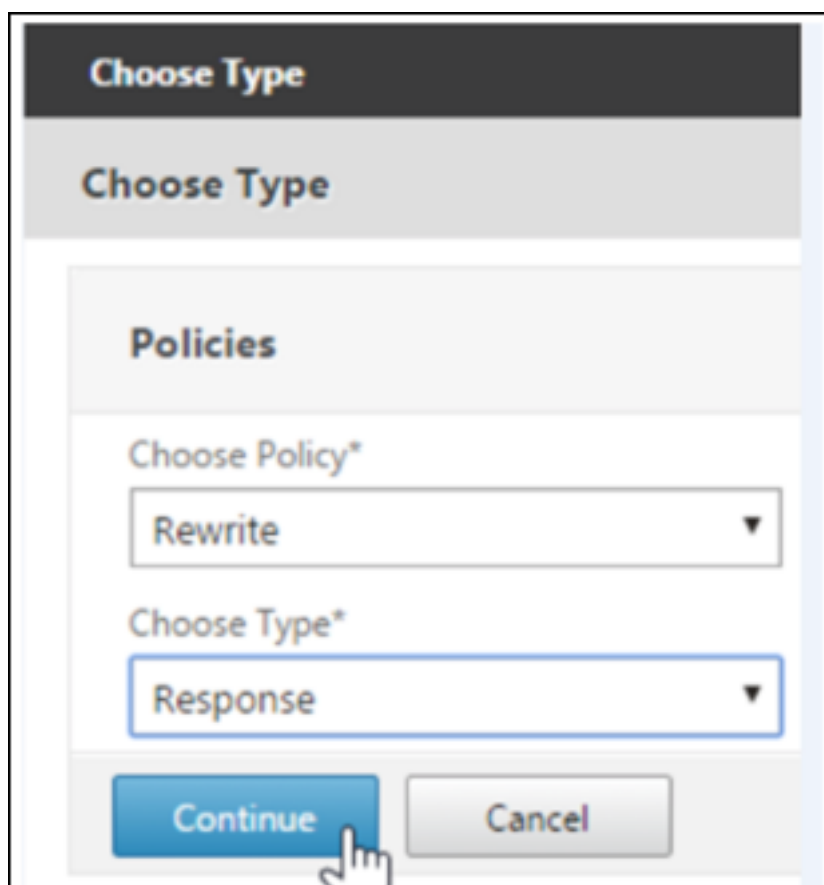
- Request Policies
- 3 Session Policies
- 2 ClientlessAccess Policies
- 5 Cache Policies

Done

Advanced Settings

- + Content Switching Policies
- + SSL Profile
- + SSL Policies
- + Intranet IP Addresses
- + Intranet Applications
- + Portal Themes
- + EULA

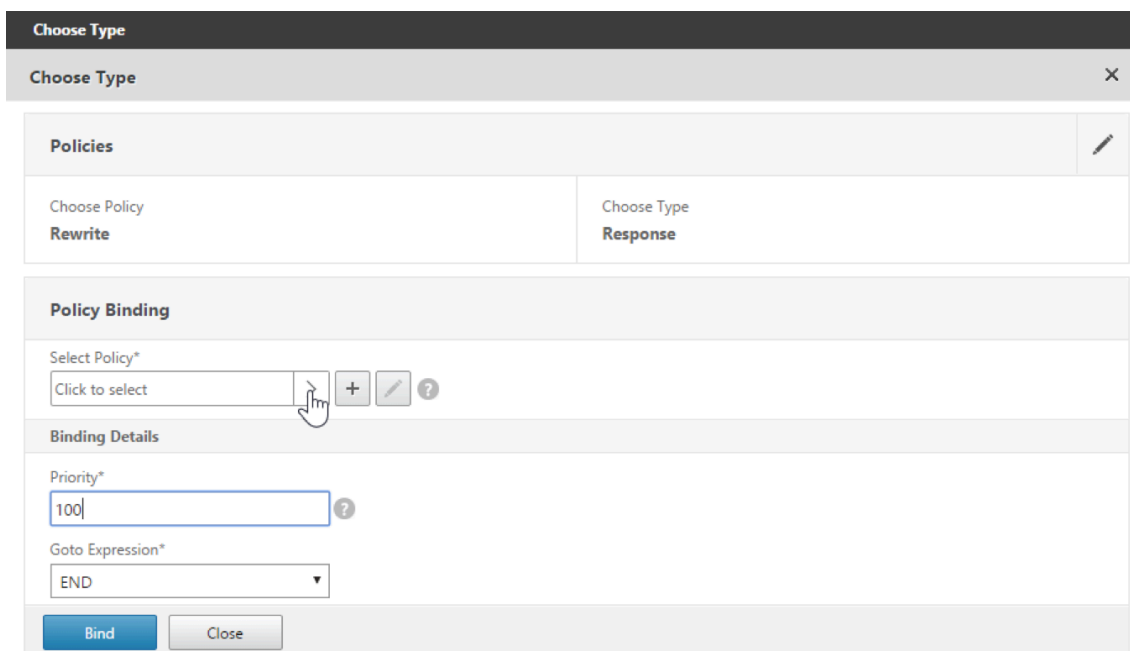
8. In the **Choose Policy** field, choose **Rewrite**.
9. In the **Choose Type** field, choose **Response**.



The screenshot shows a mobile application dialog box titled "Choose Type". The dialog has a dark header with the title "Choose Type" and a lighter grey bar below it with the same title. Underneath, there is a section titled "Policies". This section contains two dropdown menus. The first dropdown is labeled "Choose Policy*" and has "Rewrite" selected. The second dropdown is labeled "Choose Type*" and has "Response" selected. At the bottom of the dialog, there are two buttons: a blue "Continue" button and a grey "Cancel" button. A mouse cursor is pointing at the "Continue" button.

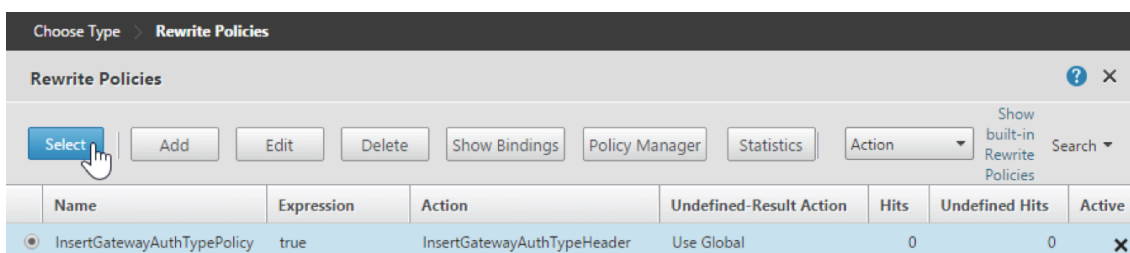
10. Click **Continue**.

The **Policy Binding** section expands.

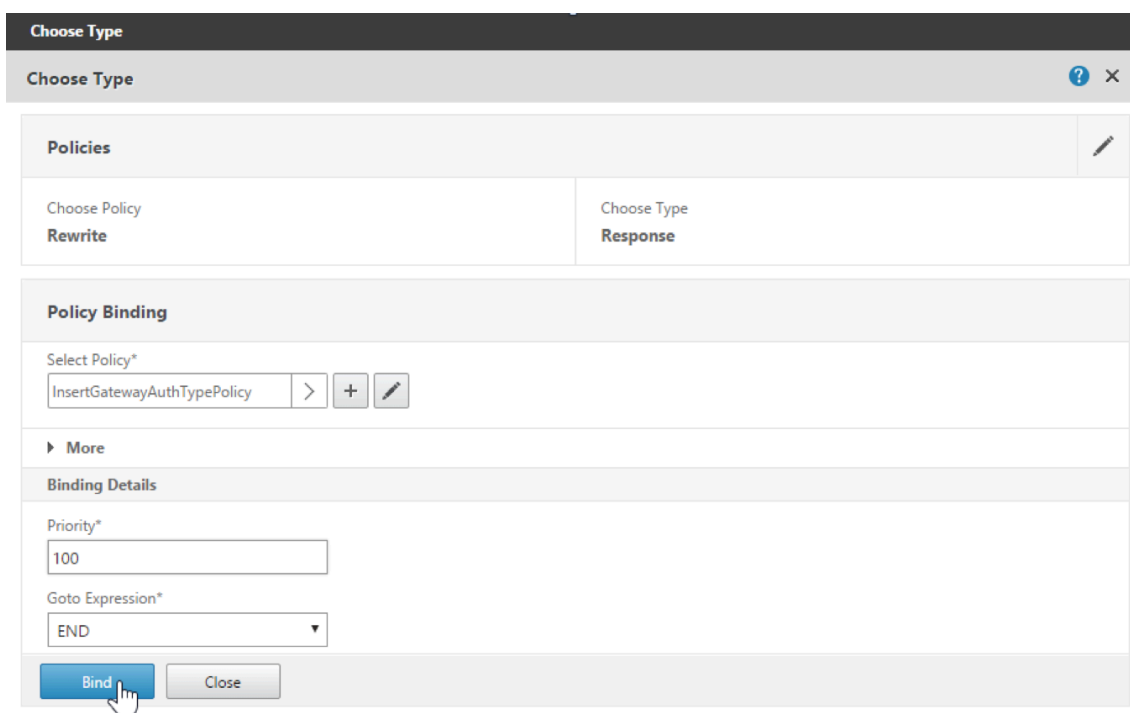


11. Click **Select Policy**.

A screen with available policies appears.

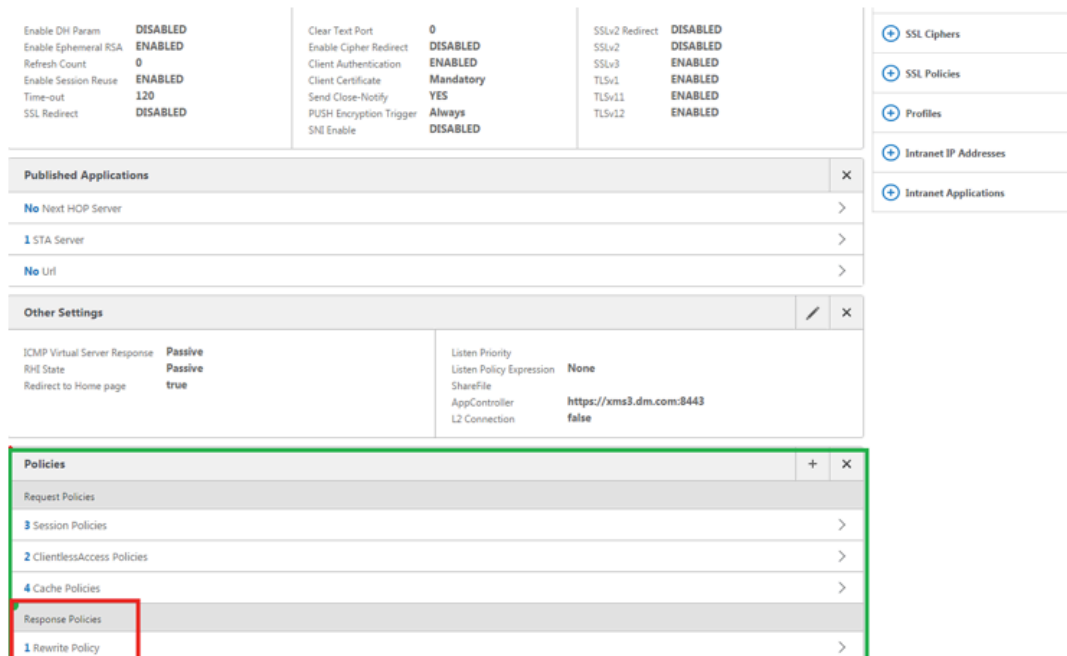


12. Click the row of the policy you created and then click **Select**. The **Policy Binding** screen appears again, with your selected policy filled in.

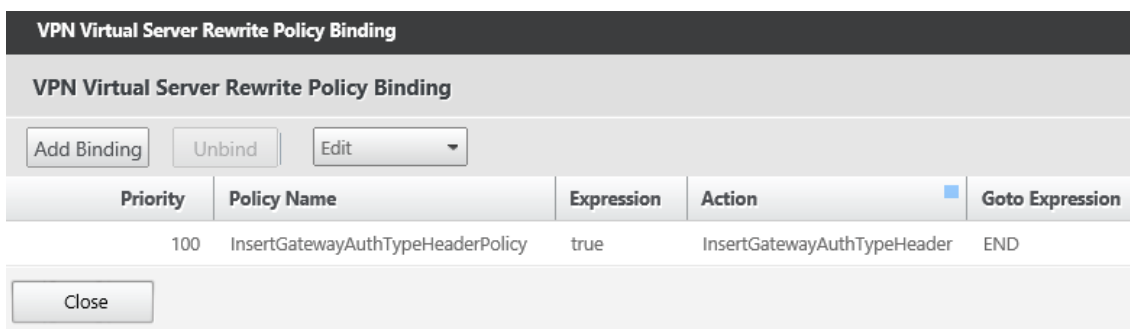


13. Click **Bind**.

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

FQDN	IP address	Port	IP and port usage
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

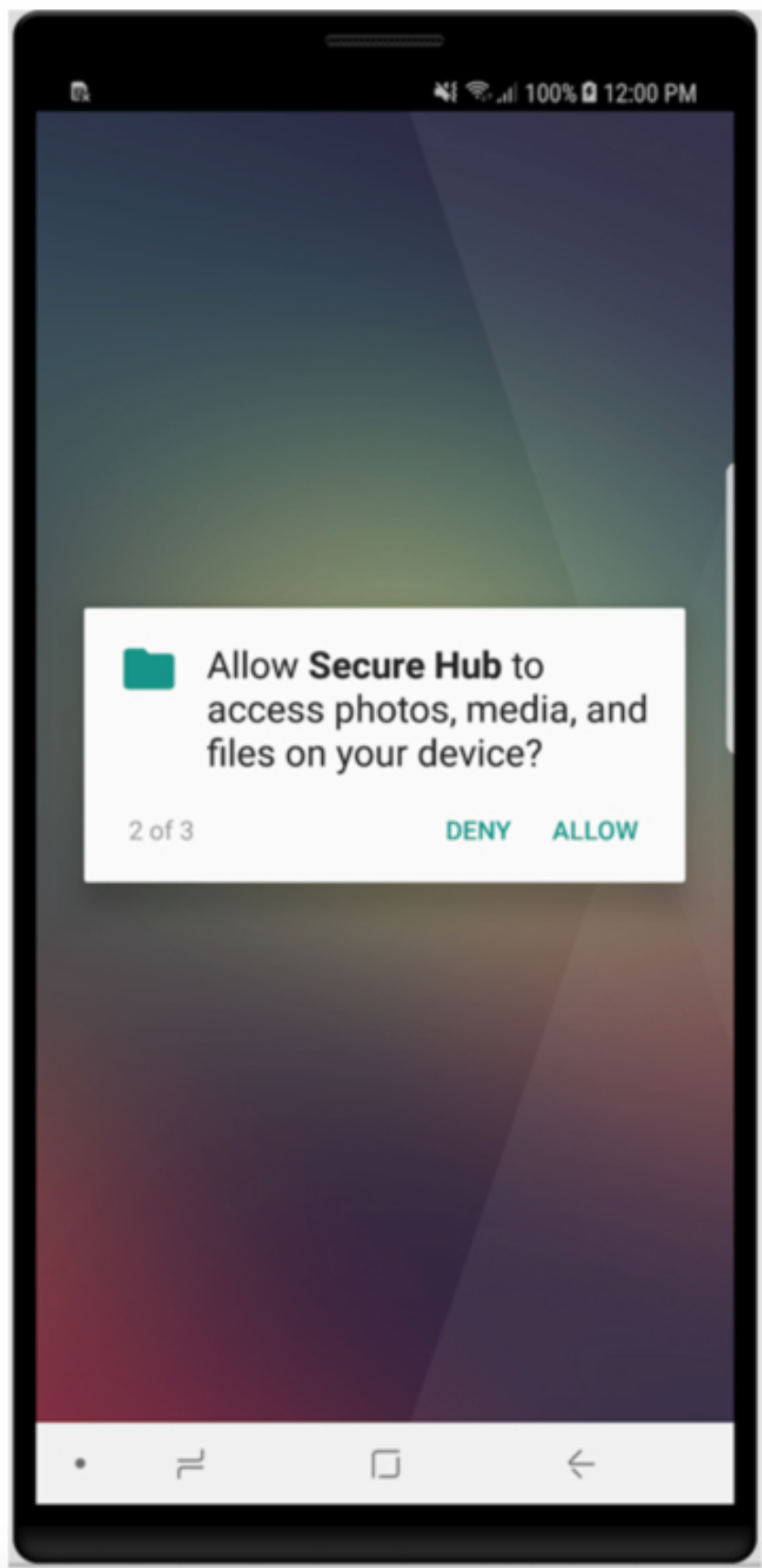
Users begin by downloading Secure Hub on to their devices from the Apple or Android store.

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](#).

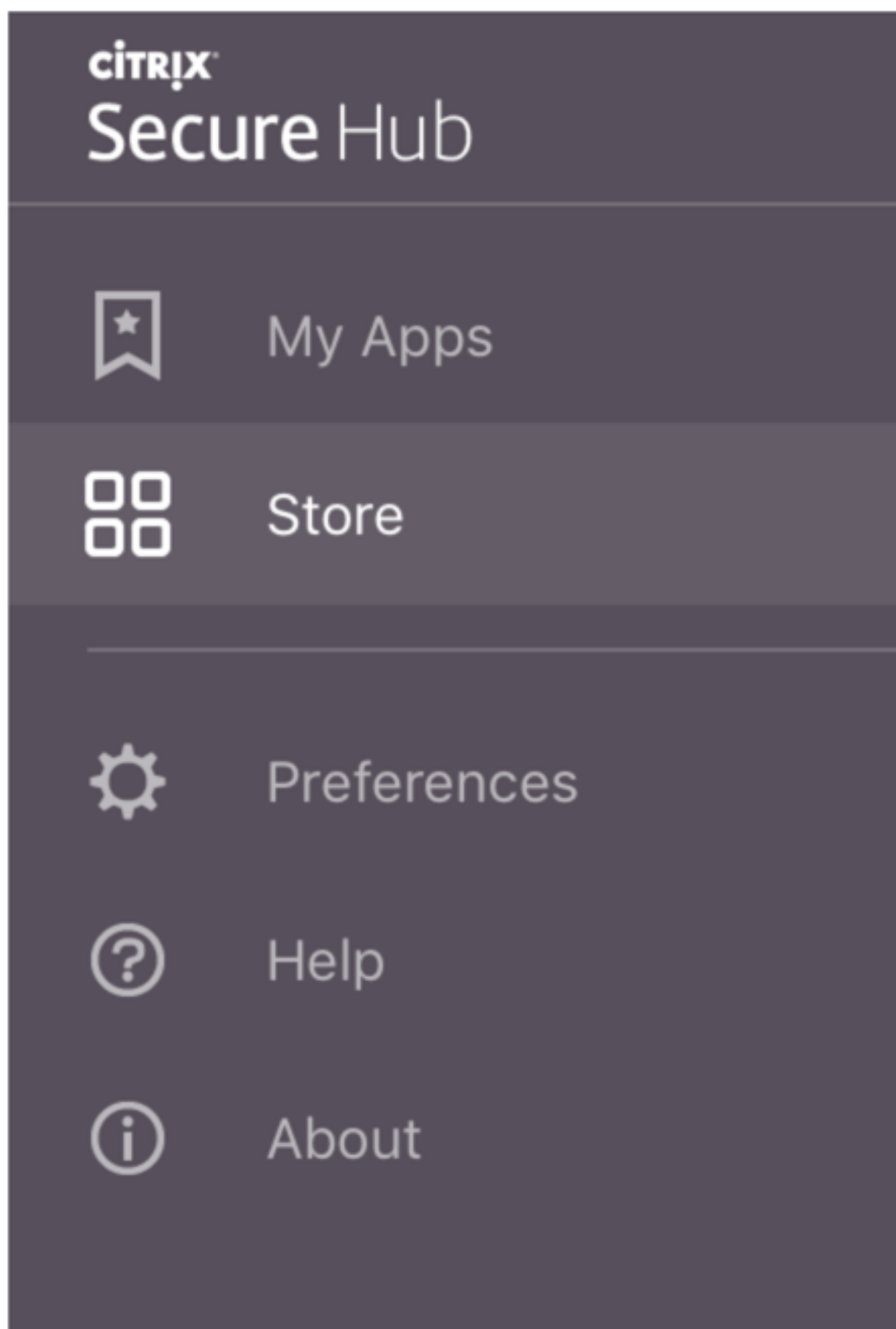
On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

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.

The screenshot shows the XenMobile interface with a green navigation bar containing 'XenMobile', 'Analyze', 'Manage', and 'Configure'. On the right, there is a user profile 'administrator' with a dropdown arrow. Below the navigation bar, the breadcrumb 'Settings > Client Branding' is visible. The main heading is 'Client Branding' with a sub-heading: 'You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.' The form includes: 'Store name*' with a text input containing 'Store' and a help icon; 'Default store view' with radio buttons for 'Category' and 'A-Z' (selected); 'Device' with radio buttons for 'Phone' (selected) and 'Tablet'; 'Branding file' with a text input and a 'Browse' button. A 'Note' section follows with three bullet points: 'The file must be in .png format (pure white logo/text with transparent background at 72 dpi).', 'The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).', and 'Files should be named as Header.png and Header@2x.png. A .zip file should be created from the files, not a folder with the files inside of it.' At the bottom right are 'Cancel' and 'Save' buttons.

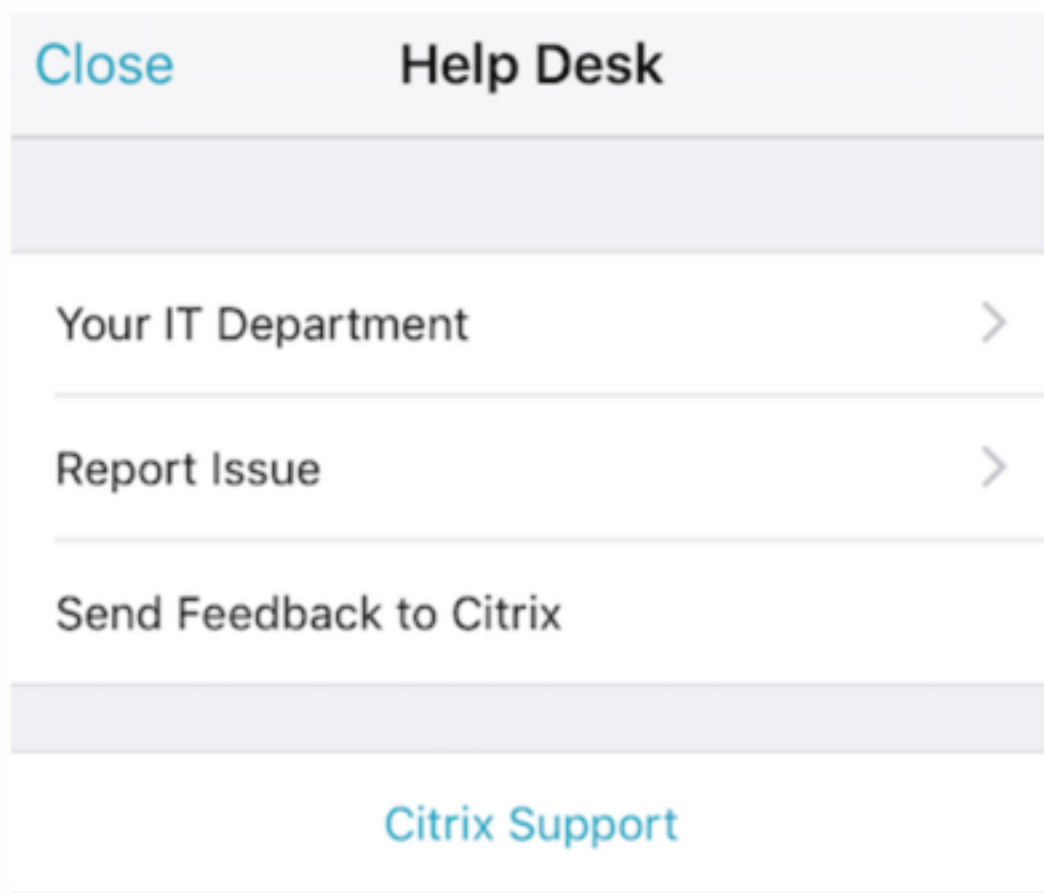
You can edit app descriptions in the Endpoint Management console. Click **Configure** then click **Apps**. Select the app from the table and then click **Edit**. Select the platforms for the app with the description you're editing and then type the text in the **Description** box.

The screenshot shows the XenMobile interface with a green navigation bar containing 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below the navigation bar, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is active, showing a table with columns for 'MDX' and 'App Information'. The table has four rows: '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The 'App Information' row is selected. To the right of the table is the 'App Information' configuration form. It includes: 'Name*' with a text input containing 'Workmail' and a help icon; 'Description' with a large text area and a help icon; and 'App category' with a dropdown menu showing 'Workapps'.

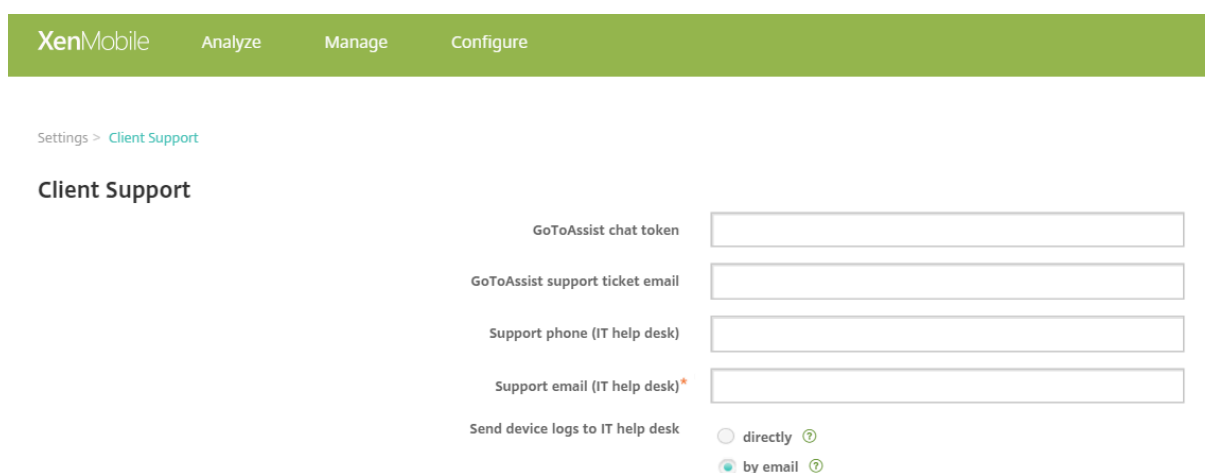
In the Store, users can browse only those apps and desktops that you've configured and secured in Endpoint Management. To add the app, users tap **Details** and then tap **Add**.

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](#).

Secure Mail overview

May 12, 2021

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 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- 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
- IBM Domino Mail Server version 10.0.1
- IBM Domino Mail Server version 9.0.1 FP10 HF197
- IBM Lotus Notes Traveler version 10.0.1.0 build 201811191126_20
- IBM Lotus Notes Traveler version 9.0.1.21
- 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

March 17, 2021

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:

- **Secure browse:** Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as secure browse. This is the default configuration specified for the **Preferred VPN mode** policy. Secure browse is recommended for connections that require single sign-on (SSO).
- **Full VPN tunnel:** Connections that tunnel to the internal network can use a full VPN tunnel, configured by the **Preferred VPN** mode policy. Full VPN tunnel is recommended for connections that use client certificates or end-to-end SSL to a resource in the internal network. 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 secure browse modes as needed. By default, this policy is off. When this policy is on, a network request that fails due to an authentication request that cannot be handled in the preferred VPN mode is retried in the alternate mode. For example, full VPN tunnel mode accommodates server challenges for client certificates, but not the secure browse mode. Similarly, HTTP

authentication challenges are more likely to be serviced with SSO when using secure browse mode.

- **Full VPN tunnel with PAC:** You can use a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices. A PAC file contains rules that define how web browsers select a proxy to access a given URL. PAC file rules can specify handling for both internal and external sites. Secure Web parses PAC file rules and sends the proxy server information to Citrix Gateway.
- The full VPN tunneling performance when a PAC file is used is comparable to secure browse mode. For details about PAC configuration, see [Full VPN Tunneling with PAC](#).

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

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

Full VPN Tunneling with PAC

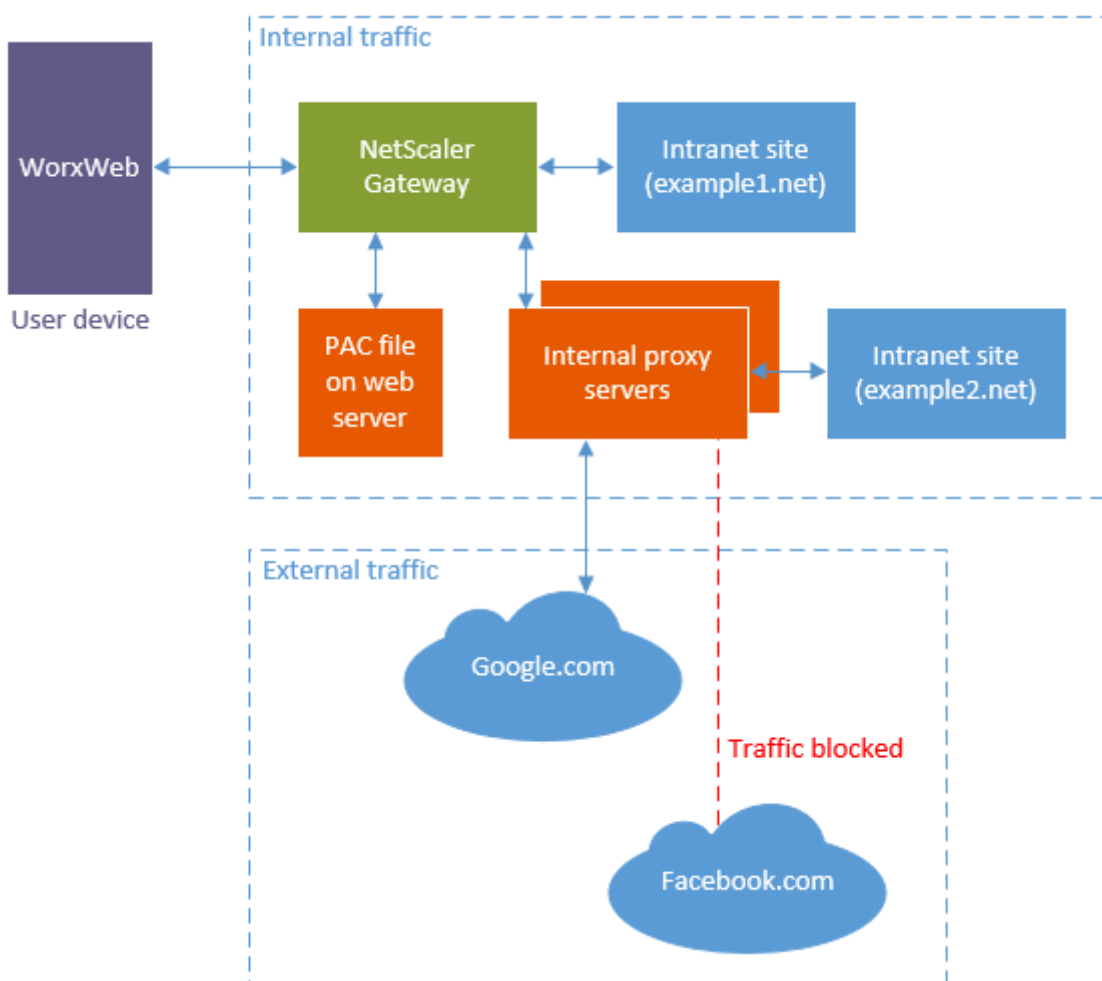
Important:

If Secure Web is configured with a PAC file and Citrix ADC is configured for proxy operation, Secure Web times out. Ensure that you remove Citrix Gateway traffic policies configured for proxy before

using full VPN tunneling with PAC.

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

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



In that example, the traffic rules specify that:

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

To configure full VPN tunneling with PAC

1. Validate and test the PAC file.

Note:

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

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

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

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

<https://webserver.local/GenericPAC.pac>

<https://webserver.local/GenericPAC.pac>

Tested PAC extensions are .txt or .pac.

The PAC file displays its contents inside the web browser.

Important:

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

2. Configure Citrix Gateway:

- Disable Citrix Gateway split tunneling. If split tunneling is on and a PAC file is configured, the PAC file rules override the Citrix ADC split tunneling rules. A proxy does not override Citrix ADC split tunneling rules.
- Remove Citrix Gateway traffic policies configured for proxy. This is required for Secure Web to work correctly. The following figure shows an example of the policy rules to remove.

VPN Virtual Server Traffic Policy Binding		
<input type="button" value="Add Binding"/>	<input type="button" value="Unbind"/>	<input type="button" value="Edit"/>
Priority	Policy Name	Expression
90	traf_pol_no_proxy_url_based	REQ.HTTP.HEADER CitrixSecureB
100	traf_pol_https_proxy	(REQ.HTTP.HEADER User-Agent
110	traf_pol_http_proxy	(REQ.HTTP.HEADER User-Agent

3. Configure Secure Web policies:

- Set the Preferred VPN mode policy to **Full VPN tunnel**.
- Set the Permit VPN mode switching policy to **Off**.

- Configure the PAC file URL or proxy server policy. Secure Web supports HTTP and HTTPS in addition to default and non-default ports. For HTTPS, the root certificate authority must be installed on the device if the certificate is self-signed or untrusted.

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

Example PAC file URLs:

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

```
http[s]://10.10.0.100/proxy.txt
```

Example proxy servers (port is required):

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

```
10.10.0.100:port
```

Note:

If you configure a PAC file or proxy server, do not configure PAC in system proxy settings for Wi-Fi.

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

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

Limitations of PAC file support

Secure Web does not support:

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

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

Secure Web policies

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

Allowed or blocked websites

Secure Web normally does not filter web links. You can use this policy to configure a specific list of allowed or blocked sites. You configure URL patterns to restrict the websites the browser can open, formatted as a comma-separated list. A plus sign (+) or minus sign (-) precedes each pattern in the list. The browser compared a URL against the patterns in the order listed until a match is found. When a match is found, the prefix 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 secure browse mode. For details, see this [blog post](#).

DNS suffixes

On Android, if DNS suffixes aren't configured, the VPN might fail. For details on configuring DNS suffixes, see [Supporting DNS Queries by Using DNS Suffixes for Android Devices](#).

Preparing intranet sites for Secure Web

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

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

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL

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
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 **ctxmobile-browser://** 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.

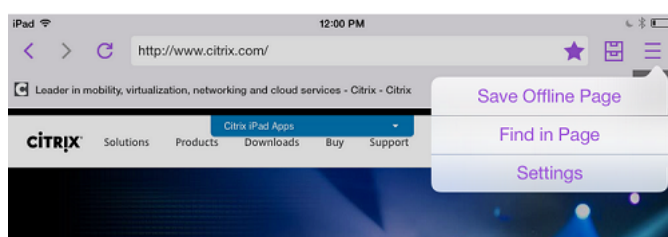
- Bookmark their favorite sites.
- Download files.
- Save pages offline.
- Auto-save passwords.
- Clear cache/history/cookies.

- 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.

Citrix QuickEdit for mobile productivity apps

May 21, 2021

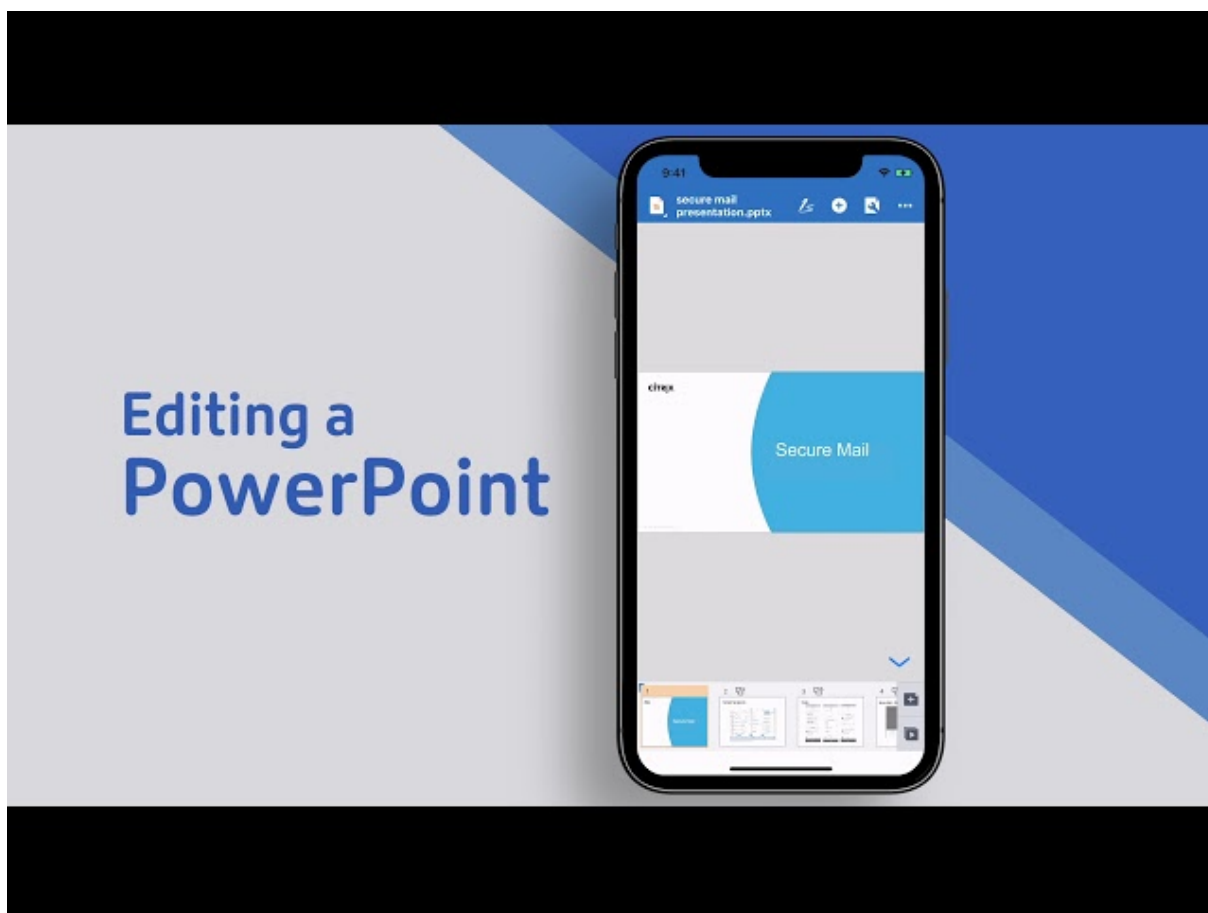
Citrix QuickEdit is the editing tool for mobile productivity apps. Its compatibility with Citrix Secure Mail and Citrix Content Collaboration for Endpoint Management allows a seamless workflow within the secure Endpoint Management environment.

Updates:

- **Update on June 19, 2020:** MDX encryption reaches end of life (EOL) on September 1, 2020. You must test and plan for migration off MDX encryption by July 2020.
- **Update on July 2, 2018:** QuickEdit remains available as a mobile productivity app. We are not applying the End of Life (EOL) status on September 1, 2018 that we had communicated earlier. Instead, we plan to make updates to the content management component of

QuickEdit.

For a video on the capabilities of Citrix QuickEdit features, see this video in the Citrix YouTube channel:



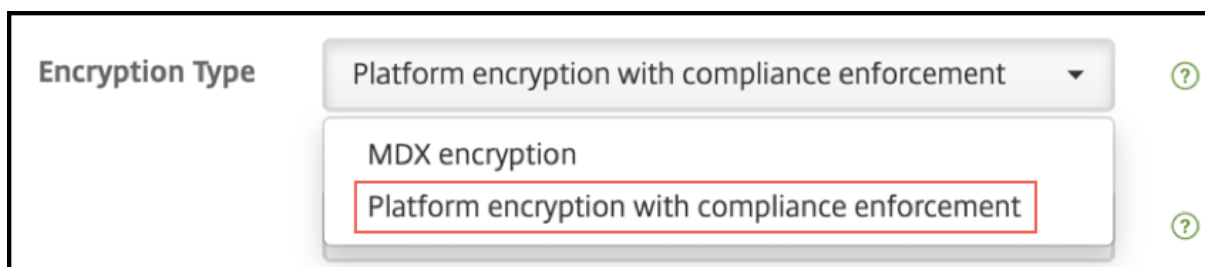
For QuickEdit and other mobile productivity app system requirements, see [System requirements](#).

You can configure QuickEdit to be pushed to user devices automatically when the devices are enrolled in Secure Hub. Alternatively, users can add the app from the app store.

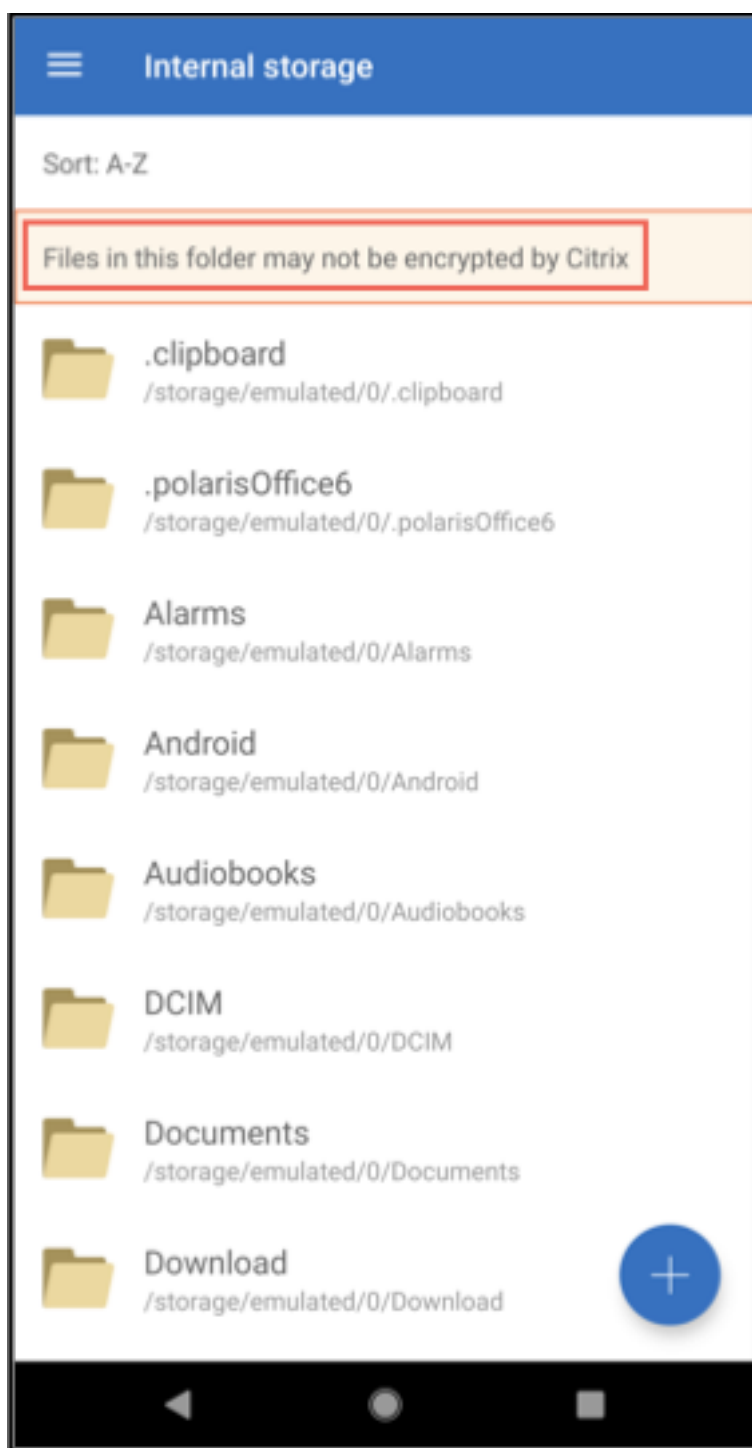
QuickEdit is also compatible with native mail programs for easy sharing or transferring of files, either as an attachment or Citrix Files link.

Encryption

With QuickEdit version 20.5.0 and later, you can choose the type of data encryption. Select **Platform encryption with compliance enforcement** encryption type for the device platform to encrypt the data.



When you select **Platform encryption with compliance enforcement** encryption type, the data remains on the SD card of your device, but will not encrypt the files present in the SD card. You receive the following warning on your device:



The only effect on the files stored on Cloud repositories is the change in the type of data encryption.

Supported file types

- Microsoft Word – .doc and .docx
- Microsoft Excel – .xls and .xlsx

- Microsoft PowerPoint – .ppt and .pptx
- .csv, .txt
- .jpeg, .png, .png, .svg, .bmp

The following file types are deprecated as of the latest release: .docm, .xlsm, .pptm, and .rft.

Integrating and delivering QuickEdit

To integrate and deliver QuickEdit with Endpoint Management, follow these general steps:

1. You can optionally enable SSO from Secure Hub. To do that, configure Citrix Files account information in Endpoint Management to enable Endpoint Management as a SAML identity provider for Citrix Files.

Configuring the Citrix Files account information in Endpoint Management is a one-time setup used for all Endpoint Management, Citrix Files, and non-MDX Citrix Files clients. For details, see [Integrating and Delivering Citrix Files Clients](#).

2. Download QuickEdit.
 - You can download QuickEdit from the [Endpoint Management downloads page](#).
 - For new users, QuickEdit is also available on the Citrix Workspace platform. For details, see [Citrix Workspace platform](#).
3. Add QuickEdit to Endpoint Management using the same steps as for other MDX apps. For details, see [Add apps](#).

Uploading files

You can upload files from your device to Cloud repositories such as ShareFile, and access them on other devices. Currently we support QuickEdit only for iOS and Android. But if the files are migrated to Cloud repositories, you can use any other tool on your device to edit the same.

Fixed and known issues in the current release

The following issues are known or fixed in the latest release.

Fixed issues

- When you try to send files to Secure Mail from QuickEdit for iOS or ScanDirect, the transfer fails. As a workaround, add the following file encryption exclusion within the policy settings for these apps: “/tmp/.com.apple.Pasteboard”. (Found in version 6.14)

Known issues

- If a page size exceeds 10,000 points (width or height), documents do not open, to prevent a potential memory error.
- Digital signatures and inline images are not supported with QuickEdit.
- On QuickEdit on iOS 12 devices, when users create a file, a “Due to insufficient memory” issue appears.
- Users can view annotations to PDF files only if the file is opened in Edit mode and the Annotations option is selected.
- When users open a PDF file that exceeds 150 MB, an “Unsupported file” error message appears.
- On QuickEdit for iPads, in the **Edit** mode, the keyboard does not appear as expected.
- Users cannot create a PowerPoint (.ppt) file that includes more than one photo.

Limitations

- QuickEdit is not supported on shared devices.
- If you are running an older version of QuickEdit that supports shared devices and you upgrade to QuickEdit for iOS versions 7.4.0 or later, all your locally managed files and folders are lost. However, Citrix Files data remains unaffected and accessible.

ShareConnect

August 12, 2020

Important:

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

With ShareConnect, users can securely connect to their computers through iPads, Android tablets, and Android phones to access their files and applications. Users can:

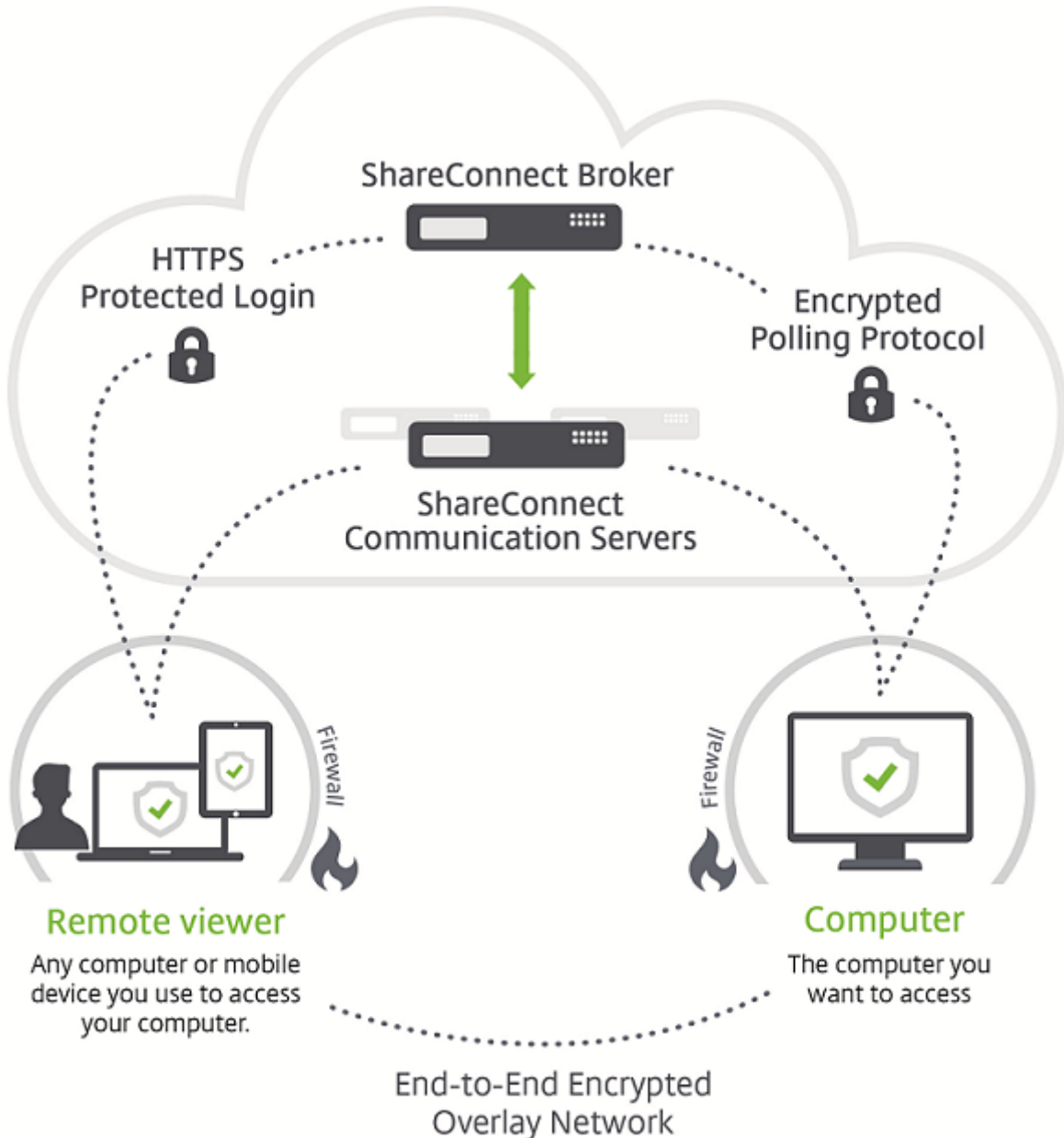
- Work on files that reside on both their computers and on connected and networked drives
- Run apps from the target machine within ShareConnect.
- Have mobile app access without the need to wrap other mobile productivity apps.
- Run ShareConnect on Citrix Virtual Desktops for mobile-optimized access.

You can download the MDX version of ShareConnect from the [Endpoint Management downloads](#) page.

For general information on how to install and use ShareConnect, see the [Citrix Knowledge Center](#).

Architecture overview

ShareConnect components include the Citrix-owned ShareConnect Broker and the ShareConnect Communication Servers, as shown in the following figure. The ShareConnect Broker is an application server and database that maps users to computers. The application then lets users know whether their host computer is online or offline. ShareConnect Communication Servers are used to exchange data between host and client computers. That data can flow through a secure micro VPN tunnel between the host and client computers based on **Endpoint Management** settings.



In addition, Citrix Files can provide user authentication through single sign-on (SSO) with a SAML Identity Provider (IdP), such as Endpoint Management or Active Directory Federation Services (ADFS). Ac-

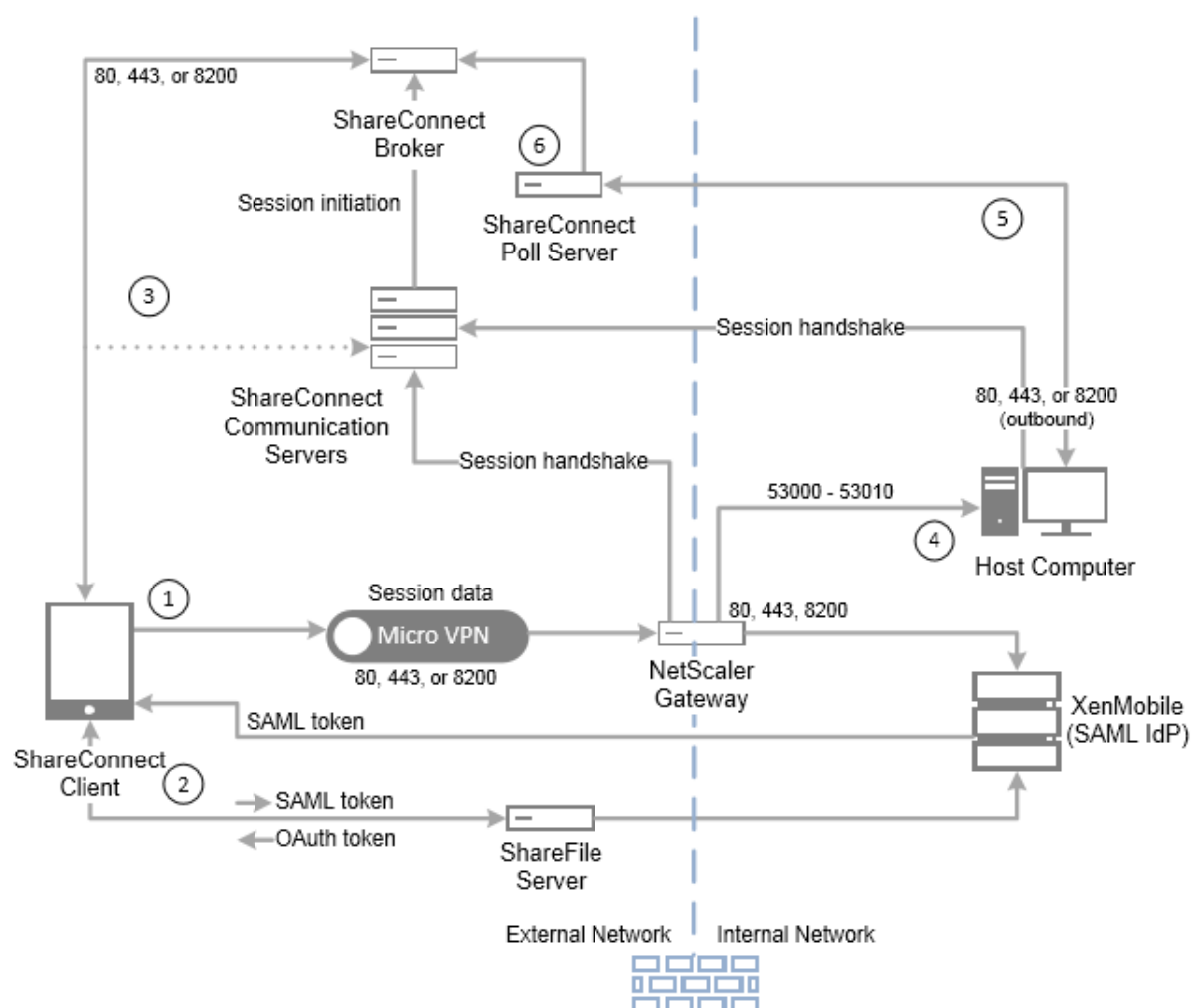
Access to resources outside of the network is provided through Citrix Gateway in a deployment with Endpoint Management.

How connections work in ShareConnect

ShareConnect establishes either direct or indirect connections:

- **Direct connections.** ShareConnect establishes a direct connection between the client computer and host computer if the computers are on the same LAN or Wi-Fi network. In this scenario, data flows directly between the client computer or mobile device being used to access a host computer. Data does not flow through the ShareConnect Communication Servers, resulting in optimal performance. For direct connections, Endpoint Management uses Citrix Gateway to provide secure access to resources outside of the local network.
- **Indirect connections.** ShareConnect establishes an indirect connection between the client computer and host computer if the computers are not directly reachable. In this scenario, data flows through the ShareConnect Communication Servers.

The following figure shows the connections used when users access a host computer from a computer or mobile device running ShareConnect using direct connections. Connection steps are described after the figure.



☒ In this scenario, Endpoint Management is configured to act as a SAML IdP for Citrix Files, to provide SSO from Secure Hub. ShareConnect requests a SAML token from Secure Hub, which in turn passes the request to Endpoint Management through Citrix Gateway. Endpoint Management then sends the SAML token to ShareConnect.

☒ ShareConnect sends the SAML token to Citrix Files for validation and to exchange the SAML token for an OAuth token.

☒ ShareConnect sends the OAuth token to the ShareConnect broker, which then sends a session token to ShareConnect.

☒ ShareConnect gets a list of host computers from the ShareConnect Broker and prompts for host computer credentials. ShareConnect then establishes a direct connection with the ShareConnect Communication Server. After the host computer validates the credentials, ShareConnect gets a list of files and apps from the host computer. After the user opens a file or app, a direct connection occurs between ShareConnect and the host computer.

☒ The ShareConnect agent on the host computer sends status messages to ShareConnect Poll Server

to indicate whether it's online or offline.

☒ The ShareConnect Poll Server sends load-balanced requests from the ShareConnect agent to the ShareConnect Broker and sends host status updates to the ShareConnect Broker.

ShareConnect security

ShareConnect uses built-in 128-bit AES encryption so that all data sent between the ShareConnect client and a host computer running the ShareConnect agent is fully encrypted from end-to-end. The encryption key is unique for each connection. Even the most sophisticated devices cannot intercept the data necessary to decode the encryption.

You typically configure ShareConnect so that data is routed directly between the ShareConnect client and a host computer. Data is not routed through the ShareConnect Communication Servers unless you configure the Network access policy for unrestricted access. For policy details, see [Add ShareConnect to Endpoint Management](#) in this article.

For direct or indirect connections, encrypted metadata, such as the IP addresses and ports needed to establish connections, is sent to ShareConnect servers.

Also, MDX wrapping of ShareConnect provides data encryption through the MDX vault. The vault encrypts MDX-wrapped apps and associated stored data on both iOS (pre-iOS 9) and Android devices. The encryption occurs by using FIPS-certified cryptographic modules provided by the OpenSSL.

Information on Security Settings and Admin controls can be found in the following security whitepapers.

[ShareConnect Security Whitepaper](#)

[ShareConnect Administrator Guide](#)

Port requirements for ShareConnect

Open the following ports to allow ShareConnect communications. The port requirements differ depending on the type of connection. The connections can be direct connections, if the computers are on the same LAN or Wi-Fi network. Or they can be indirect connections, if the client and host computers cannot directly reach each other.

For direct connections

TCP port 80 - Used for outbound connections from Citrix Gateway to app.shareconnect.com.

Source - Citrix Gateway

Destination - app.shareconnect.com

TCP port 80, 443, 8200 - At least one of these ports is required for outbound connections from Citrix Gateway to the ShareConnect Communication Server.

Source - Citrix Gateway

Destination - ShareConnect Communication Servers

TCP port 80, 443, 8200 - Used for outbound connections from ShareConnect host computers to Citrix servers.

Source - ShareConnect host computers

Destination - poll.shareconnect.com, ShareConnect Communication Servers

TCP port 443 - Used for outbound connections from Citrix Gateway to required sites.

Source - Citrix Gateway

Destination - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

TCP port 53000 - 53010 - Used for outbound connections from Citrix Gateway to ShareConnect host computers.

Source - Citrix Gateway

Destination - LAN-based ShareConnect host computers

TCP port 53000 - 53010 - Used for inbound connections from Citrix Gateway to ShareConnect host computers.

Source - Citrix Gateway

Destination - LAN-based ShareConnect host computers

For indirect connections

TCP port 80 - Used for outbound connections from the ShareConnect agent to app.shareconnect.com.

Source - ShareConnect agent

Destination - app.shareconnect.com

TCP port 80, 443, 8200 - At least one of these ports is required for outbound connections from the ShareConnect agent to the ShareConnect Communication Server.

Source - ShareConnect agent

Destination - ShareConnect Communication Servers

TCP port 80, 443, 8200 - Used for outbound connections from ShareConnect host computers to Citrix servers.

Source - ShareConnect host computers

Destination - poll.shareconnect.com, ShareConnect Communication Servers

TCP port 443 - Used for outbound connections from the ShareConnect agent to required sites.

Source -ShareConnect agent

Destination - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

Integrating and delivering ShareConnect

To integrate and deliver ShareConnect with Endpoint Management, follow these general steps:

1. You can optionally enable SSO from Secure Hub. To do that, you configure Citrix Files account information in Endpoint Management to enable Endpoint Management as a SAML IdP for Citrix Files.

Configuring the Citrix Files account information in Endpoint Management is a one-time setup. The one-time setup is used for all mobile productivity apps clients, Citrix Files clients, and non-MDX Citrix Files clients.

2. [Download](#) and wrap ShareConnect. For details, see [About the MDX Toolkit](#).
3. Add ShareConnect to Endpoint Management and configure MDX policies.
4. Install the ShareConnect agent on host computers. The ShareConnect agent is an MSI package. Therefore, you can use your existing software deployment methods to distribute and install the agent. Users must then register the host computer by signing on to the Agent using their Citrix Files credentials within one hour of installation.

Alternatively, users can install the ShareConnect agent on the computer to which they connect with ShareConnect. For details, see the “To install the ShareConnect agent on a computer” section later in this article.

Add ShareConnect to Endpoint Management

You add ShareConnect to Endpoint Management using the same steps as for other MDX apps. For details, see [Add an MDX app](#). When adding ShareConnect, configure the MDX policies for it as shown in the following table.

Policy	Value	Results
Network access	Tunneled to the internal network or Unrestricted	Tunneled to the internal network uses a per-application VPN tunnel back to the internal network for all network access. This configuration provides direct connection between ShareConnect and a host computer. Unrestricted uses Citrix-owned Communication Servers to route encrypted data between a host computer and ShareConnect. Be sure to test your setup with unrestricted access to ensure everything works, even if you plan to use Tunneled to the internal network for network access.
Preferred VPN mode	Secure browse	Sets the initial connection mode appropriately for connections that require SSO.
Enable encryption	On	Encrypts the data stored on the tablet.
Cut and copy	Unrestricted	Enables cut and copy operations for ShareConnect.
Paste	Unrestricted	Enables paste operations for ShareConnect.
Document Exchange (Open In)	Unrestricted	Permits users to open any file on the connected computer or a connected network drive from ShareConnect.

Policy	Value	Results
Save Password	Off	Requires users to enter the user name and password for their computer each time they sign on to ShareConnect.

To install the ShareConnect agent on a computer

The following steps describe how a user installs the ShareConnect agent on each physical or virtual computer they want to connect to from a supported mobile device.

Before performing these steps, the user must first install Secure Hub. Then, they follow the prompts to allow the mobile productivity apps to install on the supported mobile device.

1. Sign on to Secure Hub on the tablet.
2. Open ShareConnect.
3. Tap Email download link.

Citrix sends an email to you from no-reply@shareconnect.com.

4. From the host computer that you want to access from ShareConnect, open the email.
5. In the email, click Set up this computer.
6. Double-click **ShareConnect_Installer.exe** to begin the installation.

The ShareConnect agent installs on your host computer. During the installation, ShareConnect prompts for an email address if Citrix Files SSO is configured. Or, ShareConnect prompts for Citrix Files credentials if Citrix Files SSO is not configured.

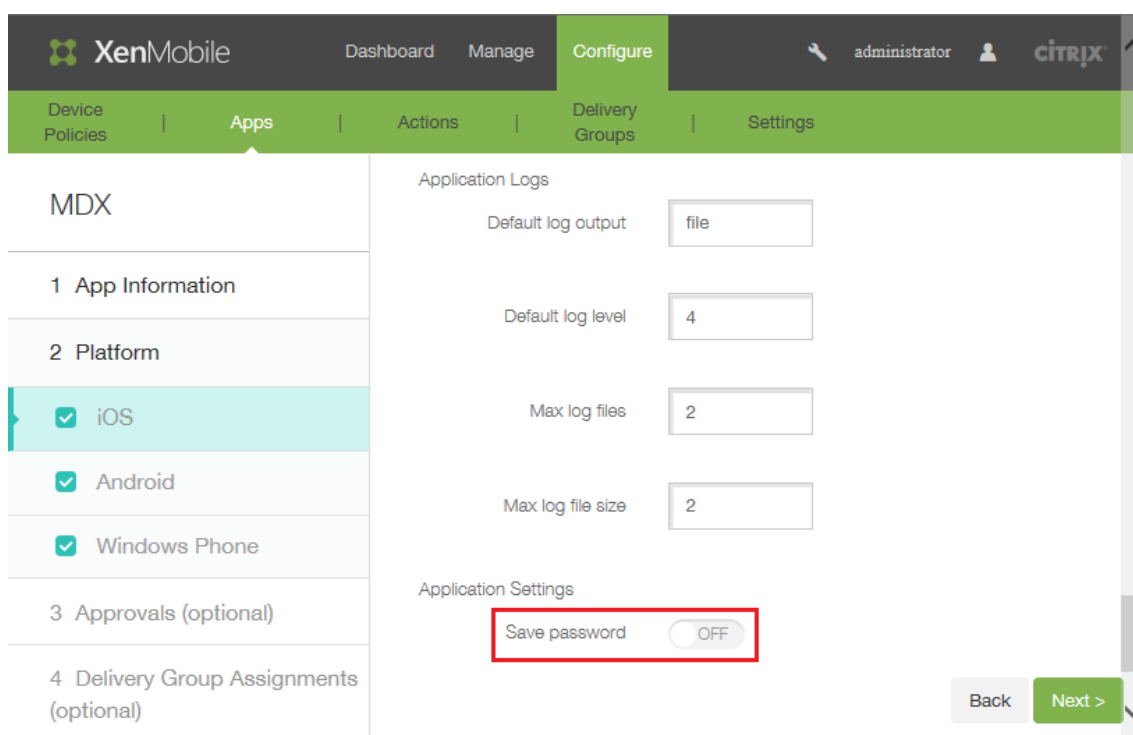
7. Follow the instructions provided in the ShareConnect and Get Started wizards.

The ShareConnect agent then registers the host computer. The host computer can connect from a ShareConnect client, if the host computer is powered on and can reach poll.shareconnect.com on at least one published port (80, 443, or 8200).

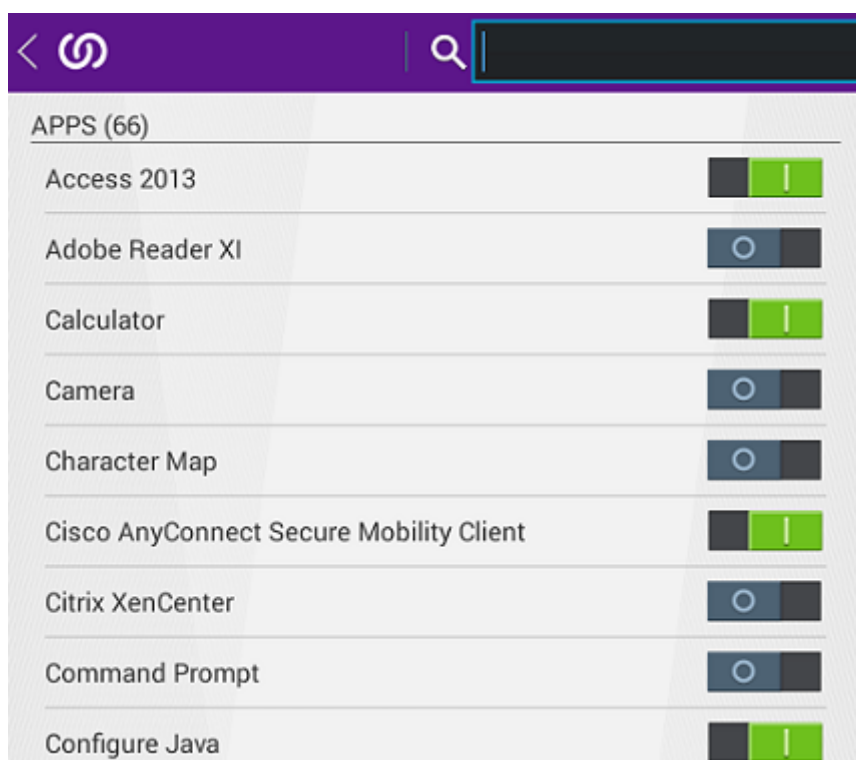
ShareConnect features

- **Add host computers.** Users can add and connect to remote host computers from supported mobile devices using ShareConnect.
- **Access files.** Users can view a list of recent files and browse and search for files on their host computer and connected drives.

- **Edit files.** From tablets, users can access desktop applications on their host computers to edit files. Users can use the applications in full screen.
- **Screen share.** Instead of viewing a single file or app, users can use the screen-sharing feature to view their host computer's desktop.
- **Citrix Files integration.** Users can move or share files between the host computer and Citrix Files.
- **Keyboard and mouse.** ShareConnect supports the simultaneous use of a Bluetooth keyboard and the Citrix XI Prototype Mouse.
- **Restricted ports.** ShareConnect uses ports 53000 to 53010 only.
- **Forced passwords for each sign-on.** For enhanced security, you can configure this option to require users to enter their computer passwords every time they sign on to ShareConnect. When the Save password policy is turned off, as shown in the following figure, users are forced to enter their sign-on credentials for every connection.



- **Add or delete apps.** Users can add or delete apps from their app tray in ShareConnect by toggling the switch beside each app to select or deselect it.



- **Cache previewed files.** ShareConnect caches already-accessed files so that the files don't download again if users preview other files and then come back to the earlier ones. This feature improves load times when users later access files.

Troubleshooting ShareConnect

ShareConnect agent installation issues

Issue	Description and resolution
<p>If a user downloads the ShareConnect agent and waits an hour or more to start the installation, the user must enter their Citrix Files account name and password to register the ShareConnect agent.</p>	<p>The ShareConnect agent installer includes a token that expires one hour after download. If a user doesn't start the installation before the token expires, the user must sign on to their Citrix Files account twice, first to register the ShareConnect agent and then to sign on to the agent after the installation completes. If users download and install the ShareConnect agent within an hour, they are prompted to sign on only once.</p>

Issue	Description and resolution
During registration of the ShareConnect agent, the agent does not connect and an error message such as “Please check your connection and try again.” appears.	Verify that the port to poll.shareconnect.com is not blocked. For details, see the System Requirements earlier in this article.

ShareConnect connection issues

Important:

To test ShareConnect, we recommend that you set the Network Access policy to **Unrestricted** to rule out issues with ports and network settings. Unrestricted access forces ShareConnect to connect through the ShareConnect Communication Servers, which typically enable you to test the connection if the ShareConnect mobile device and host computer have Internet access.

Issue	Description and resolution
ShareConnect starts, but does not connect to the host computer and does not prompt for credentials.	Verify that your setup meets the port requirements detailed earlier in this article under System Requirements.
Users are unable to sign on to ShareConnect using their Citrix Files account credentials.	SSO to ShareConnect requires that your Citrix Files account is configured with a SAML IdP. For details about using Endpoint Management as a SAML IdP, see Citrix Content Collaboration for Endpoint Management . For details about configuring other IdPs, see this Knowledge Center article . If SSO is not configured for your account, ShareConnect for iOS prompts for the user’s Citrix Files user name and password.
After users sign on to ShareConnect, ShareConnect cannot connect to the host computer.	When ShareConnect is configured for direct connections (that is, the Network access policy is set to Tunneled to the internal network), connection failures can occur if there are restrictions in network settings like firewalls blocking or proxy servers configured.

Citrix ShareFile Workflows

October 1, 2018

Note:

Secure Forms reached End of Life (EOL) on March 31, 2018. We recommend that you use Share-File WorkFlows included with Citrix Files Platinum and Premium accounts.

The ShareFile Workflows is the mobile component of the Citrix Files Custom Workflows feature. This feature allows users to create customized workflows that include multiple triggers and actions. Customized forms can be added to workflow templates and assigned to users.

When a user is assigned a form, the user can complete and submit the form via the ShareFile Workflows Mobile App. Form data storage is securely integrated with Citrix Files, where workflow files are stored for review, reference, and retrieval.

Workflow and form templates are created and managed within the Citrix Files web application.

User documentation

User documentation related to creating and managing workflow and form templates can be found in the Citrix Knowledge Center:

- [Creating a Workflow Template](#)
- [Creating a Form Template](#)
- [Submitting Forms via the Workflows mobile app](#)

Citrix Content Collaboration for Endpoint Management

March 10, 2021

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.com 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.

The screenshot shows the 'Content Collaboration' configuration page in the Citrix Endpoint Management console. The page is divided into several sections: 'Domain' (jcloudomain.sharefile.com), 'Assign to delivery groups' (with a search box and a list of operating systems), and 'Content Collaboration Administrator Account Logon' (with 'User name' and 'Password' fields). A blue arrow points to the 'Search' button in the delivery groups section. At the bottom, there are 'Cancel', 'Clear', and 'Save' buttons.

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 **Secure browse**.

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.

EOL and deprecated apps

August 12, 2020

The following apps have reached End of Life or 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](#).

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.

ShareConnect: ShareConnect reached EOL on June 30, 2020.

Allowing secure interaction with Office 365 apps

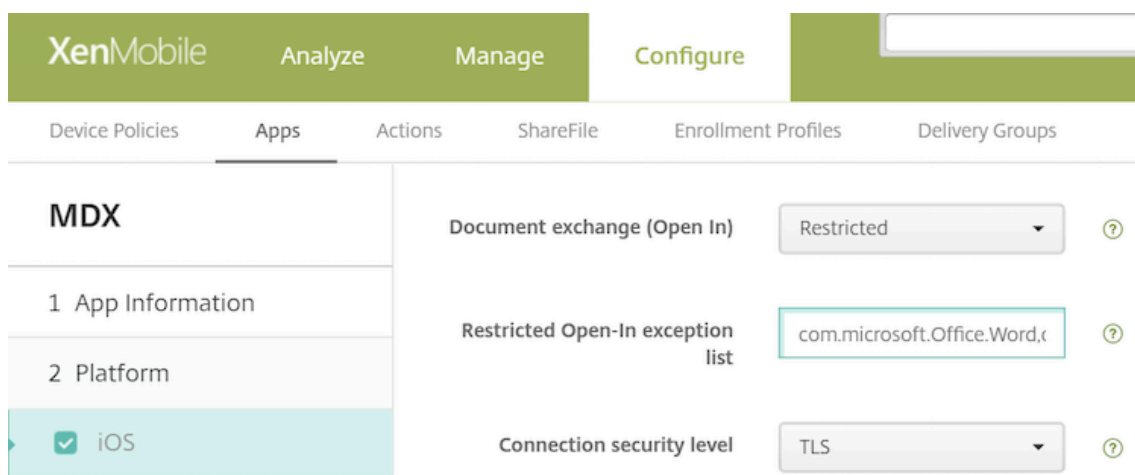
August 12, 2020

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 then 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.

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).