Mobile productivity apps

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Mobile productivity apps release timeline 2

Support for mobile productivity apps 3

Administrator tasks and considerations 5

Features by platform 17

Feature flag management 28

Secure Mail overview 29

Citrix Secure Web™ 31

Citrix Content Collaboration™ for Endpoint Management 39

EOL and deprecated apps 46

Allowing secure interaction with Office 365 apps 48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mobile productivity apps release timeline

September 7, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for mobile productivity apps

September 7, 2025

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

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

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

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

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

Supported operating systems

Mobile productivity apps support the following operating systems:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

Other considerations and limitations

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

Secure Mail

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Web

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

QuickEdit

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

Citrix Content Collaboration™ for Endpoint Management

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

ShareConnect

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

Citrix Secure Notes and Citrix Secure Tasks

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

Administrator tasks and considerations

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Enable traffic to the following URLs

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

Create an allow list by domain

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

List IP addresses in an allow list

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

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

LaunchDarkly system requirements

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- LaunchDarkly service
- APNs listener service

Supported app stores

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

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

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

Enabling public app store distribution

1. Download public-store .mdx files for both iOS and Android from the Endpoint Management downloads page.
2. Upload the .mdx files to the Endpoint Management console. The public store versions of the mobile productivity apps are still uploaded as MDX applications. Do not upload the apps as public store apps on the server. For steps, see Add apps.
3. Change policies from their defaults based on your security policies (optional).
4. Push the apps as required apps (optional). This step requires your environment to be enabled for mobile device management.
5. Install apps on the device from the App Store, Google Play, or the Endpoint Management app store.
    - On Android, the user is directed to the Play Store to install the app. On iOS, in deployments with MDM, the app installs without the user being taken to the app store.
    - When the app is installed from the App Store or Play Store, the following action occurs. The app transitions to a managed app as long the corresponding .mdx file has been uploaded to the server. When transitioning to a managed app, the app prompts for a Citrix PIN. When users enter the Citrix PIN, Secure Mail displays the account configuration screen.
6. Apps are accessible only if you're enrolled in Secure Hub and the corresponding .mdx file is on the server. If either condition is not met, users can install the app, but usage of the app is blocked.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Apple push notifications

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

Public app store FAQs

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

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

- Can I push public store apps as required apps?

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

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

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

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

Android

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App	Server	User-agent string
	Citrix Files	Secure Notes

iOS

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

- Can I prevent app upgrades?

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

- Can I enforce app upgrades?

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

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

Prerequisites

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

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

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

Limitations

- MAM SDK supports only apps published under the Android Enterprise platform on your Citrix Endpoint Management™ deployment. For the newly published apps, the default encryption is platform-based encryption.
- MAM SDK only supports platform-based encryption, and not MDX encryption.

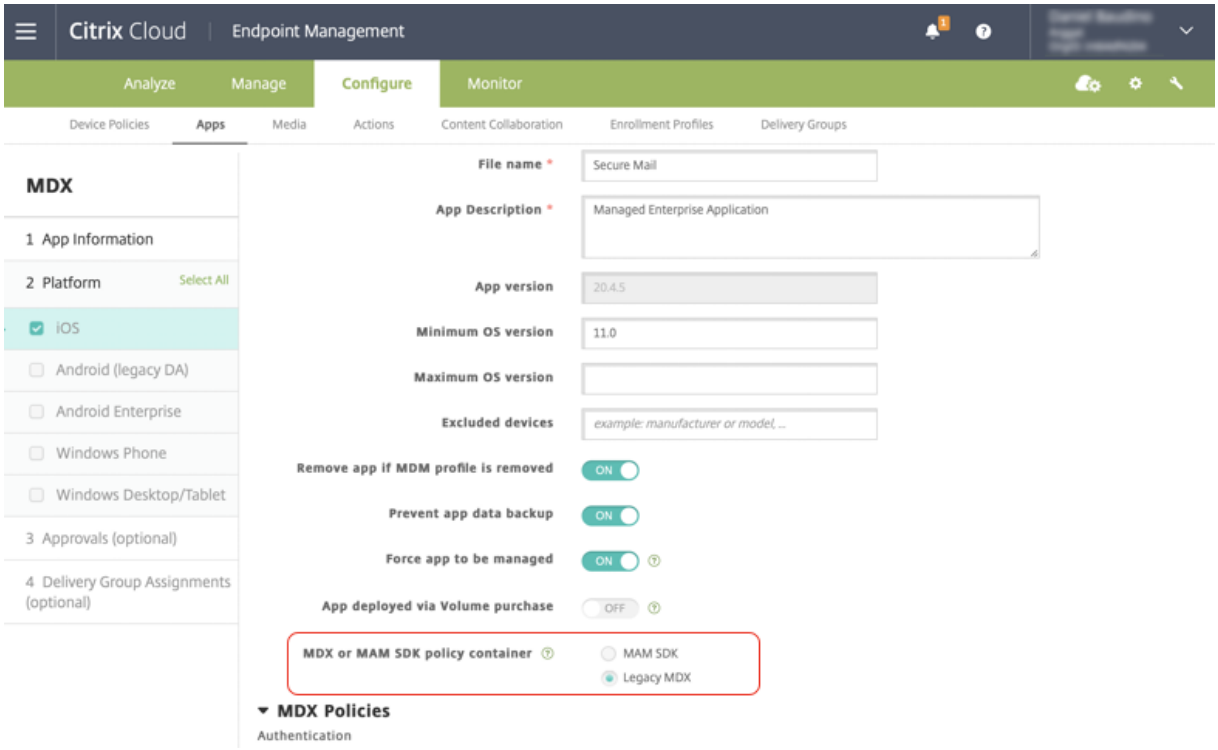
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User connections to the internal network

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

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

Network access restrictions

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

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

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

Endpoint Management client properties

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User password caching

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

Inactivity timer

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

Citrix PIN authentication

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

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

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

Fingerprint or touch ID authentication

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

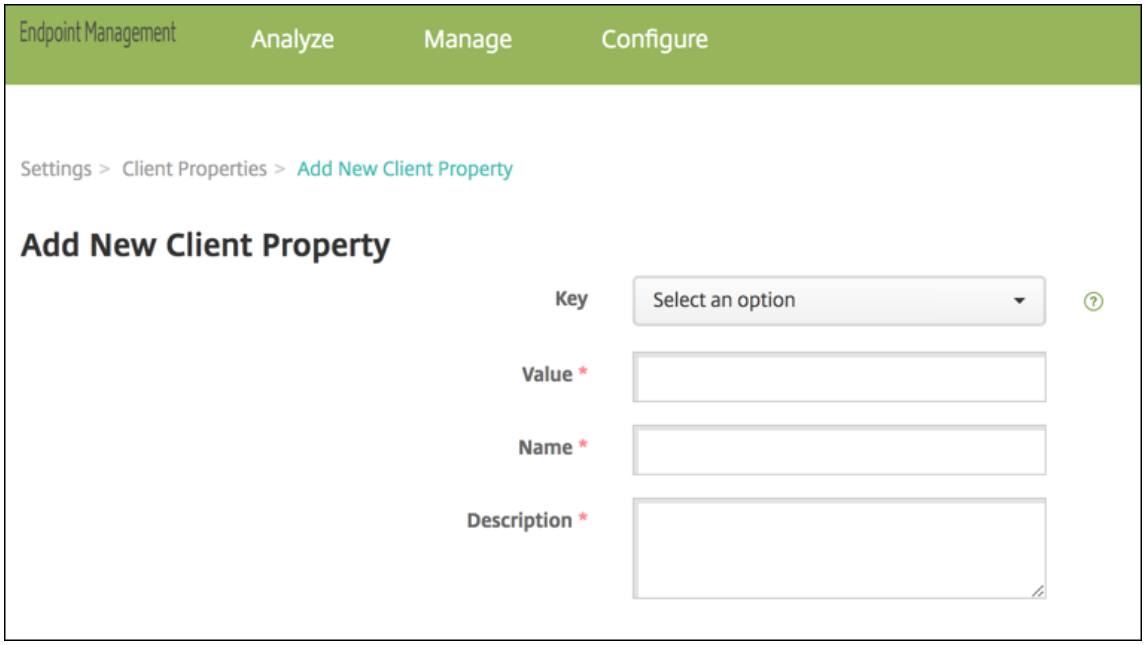
Fingerprint authentication requirements

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Analytics

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

Disable Google Analytics

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

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

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

Features by platform

September 7, 2025

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

Citrix Secure Hub™

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Citrix Secure Mail

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Citrix Secure Web™

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Feature flag management

January 17, 2025

To ensure optimal functioning of features which are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`.

Feature flags are used to enable or disable features dynamically. If an issue occurs with Mobile Productivity Apps in production, the affected feature can be disabled dynamically, even after the feature is shipped. To do so, we use feature flags managed by Citrix.

No manual configuration is needed to enable traffic for feature management, except when you have a firewall or proxy that is blocking outbound traffic. In that case, you need to enable traffic using specific URLs or IP addresses, depending on your policy requirements.

IP addresses

If you must list IP addresses in an allow list, include the following IP address to allow traffic to `features.netscalergateway.net`:

- 57.153.121.183 (for Europe West region)
- 172.202.161.151 (for US South Central region)
- 48.218.128.128 (for Japan East region)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can add these IP addresses to ensure that your firewall configurations are updated automatically in keeping with the infrastructure updates.

System requirements

If using NetScaler Gateway with split tunneling set to **OFF**, ensure that NetScaler can resolve and connect to `features.netscalergateway.net` over port 443.

The following table lists the minimum version of Mobile productivity apps that support the Feature flag management.

Mobile productivity apps	Operating system	Minimum version supported
Secure Hub	Android	24.8.0 and later
Secure Hub	iOS	24.9.0 and later
MAM SDK	Android	24.9.0 and later
MAM SDK	iOS	24.7.1 and later
Secure Mail	Android, iOS	24.9.0 and later
Secure Web	Android	24.8.0 and later
Secure Web	iOS	24.9.0 and later

Secure Mail overview

December 15, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - Support for Exchange Server 2010 ended on October 13, 2020.
> - Support for Exchange Server 2013 ended on April 11, 2023.

Secure Mail is compatible with:

- Exchange Server SE RTM
- Exchange Server 2019 Cumulative Update 15
- Exchange Server 2019 Cumulative Update 14
- Exchange Server 2019 Cumulative Update 13
- Exchange Server 2019 Cumulative Update 12
- Exchange Server 2019 Cumulative Update 11
- Exchange Server 2019 Cumulative Update 10
- Exchange Server 2019 Cumulative Update 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2016 Cumulative Update 23
- Exchange Server 2016 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 21
- Exchange Server 2016 Cumulative Update 20
- Exchange Server 2016 Cumulative Update 19
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- HCL Domino version 14.0 FP1
- HCL Domino version 12.0.2 FP2
- HCL Traveler version 12.0.2.1 Build 202302010413_30
- HCL Domino 11 (formerly Lotus Notes)
- HCL Domino 10.0.1 (formerly Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (formerly Lotus Notes)
- HCL Domino 10.0.1.0 build 201811191126_20 (formerly Lotus Notes)
- HCL Domino 9.0.1.21 (formerly Lotus Notes)
- Microsoft Office 365 (Exchange Online)

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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™

September 19, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring user connections

Secure Web supports the following configurations for user connections:

- **Tunneled –Web SSO:** Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Tunneled –Web SSO. This is the default configuration specified for the **Preferred VPN mode** policy. Tunneled –Web SSO is recommended for connections that require single sign-on (SSO).
- **Full VPN tunnel:** Connections that tunnel to the internal network can use a full VPN tunnel, configured by the **Preferred VPN** mode policy. Full VPN tunnel is recommended for connections that use client certificates or end-to-end SSL to a resource in the internal network. Secure Web, however, is not an app that can read client certificates stored on a mobile device. Some third-party, wrapped enterprise apps may be installed that can offer this capability. Full VPN tunnel handles any protocol over TCP and can be used with Windows and Mac computers, in addition to iOS and Android devices.
- The **Permit VPN mode switching** policy allows automatic switching between the full VPN tunnel and Tunneled –Web SSO modes as needed. By default, this policy is off. When this policy is on, a network request that fails due to an authentication request that cannot be handled in the preferred VPN mode is retried in the alternate mode. For example, full VPN tunnel mode accomodates server challenges for client certificates, but not the Tunneled –Web SSO mode. Similarly, HTTP authentication challenges are more likely to be serviced with SSO when using Tunneled –Web SSO mode.

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

Connection mode	Site type	Password Caching	SSO configured for Citrix Gateway	Secure Web prompts for credentials on first access of a website	Secure Web prompts for credentials on subsequent access of the website	Secure Web prompts for credentials on after password change
Tunneled – Web SSO	HTTP	No	Yes	No	No	No
Tunneled – Web SSO	HTTPS	No	Yes	No	No	No
Full VPN	HTTP	No	Yes	No	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
Full VPN	HTTPS	Yes; If the Secure Web MDX policy Enable web password caching is On.	No	Yes; Required to cache the credential in Secure Web.	No	Yes

Secure Web policies

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

Allowed or blocked websites

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

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

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

- The policy value `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permits HTTP URLs within `mycorp.com` domain, but blocks them elsewhere, permits HTTPS and FTP URLS anywhere, and blocks all other URLs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Options

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

Enable web password caching

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

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

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

Proxy servers

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

DNS suffixes

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

Preparing intranet sites for Secure Web

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WebSockets

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

- Flash
- Java

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

Technology	iOS Secure Web	Android 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Compress the archive file: In the **Finder**, click the **Go** menu in the **Menu** bar, choose **Go to Folder**, type the path name ~/Library/Safari/ReadingListArchives/. Now compress the folder that has a random hex string as a file name. You can send this file to Citrix support when you open a support ticket.

Secure Web features

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

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

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

Secure Web users can also perform the following actions:

- Block pop-ups.

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

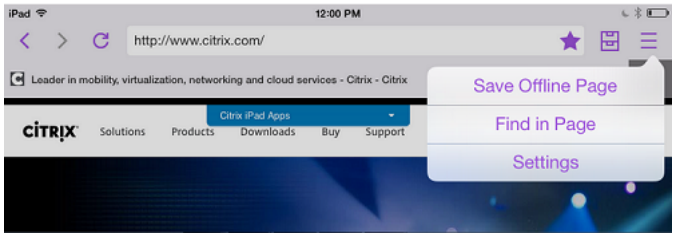
- Bookmark their favorite sites.
- Download files.
- Save pages offline.
- Auto-save passwords.
- Clear cache/history/cookies.
- Disable cookies and HTML5 local storage.
- Securely share devices with other users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Search within the address bar.
- Allow web apps they run with Secure Web to access their location.
- Export and import settings.
- Open files directly in Citrix Files without having to download the files. To enable this feature, add **ctx-sf**: to the Allowed URLs policy in Endpoint Management.
- In iOS, use 3D Touch actions to open a new tab and access offline pages, favorite sites, and downloads directly from the home screen.
- In iOS, download files of any size and open them in Citrix Files or other apps.

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

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



Secure Web also has dynamic text support. The app displays the font that users set on their devices.

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

Citrix Content Collaboration™ for Endpoint Management

September 7, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

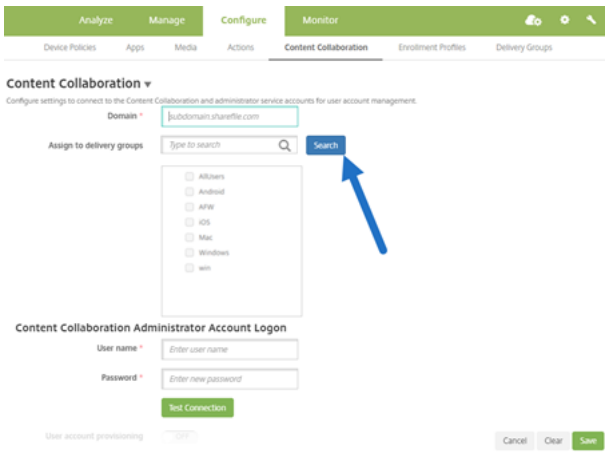
To integrate and deliver Citrix Content Collaboration for Endpoint Management clients, follow these general steps:

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

  In this mode, the MDX framework intercepts all network traffic from the Citrix Content Collaboration for Endpoint Management client. The network traffic is then redirected through Citrix Gateway using an app-specific micro VPN.

- Set the Preferred VPN mode policy to **Tunneled –Web SSO**.

  In this mode of tunneling, the MDX framework terminates SSL/HTTP traffic from an MDX app, which then initiates new connections to internal connections on the user's behalf. This policy setting enables the MDX framework to detect and respond to authentication challenges issued by web servers.

7. Complete the Approvals and Delivery Group (DG) Assignments as needed.

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

To validate Citrix Content Collaboration for Endpoint Management clients

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

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

EOL and deprecated apps

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

ShareConnect: ShareConnect reached EOL on June 30, 2020.

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

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

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

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

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

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

ScanDirect: ScanDirect reached EOL on September 1, 2018.

Full VPN tunnel: EOL date was September, 2021. For more information, see Deprecation in Citrix Endpoint Management product documentation.

Full VPN tunnel- Android: Deprecated in March, 2020. EOL date was September, 2021. We recommend customers to use MAM SDK Web SSO mode as an alternative.

Permit VPN mode switching - Android: Deprecated in March, 2020. EOL date was September, 2021.

Inbound Document Exchange - Android: Deprecated in March, 2020. EOL date was September, 2021.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allowing secure interaction with Office 365 apps

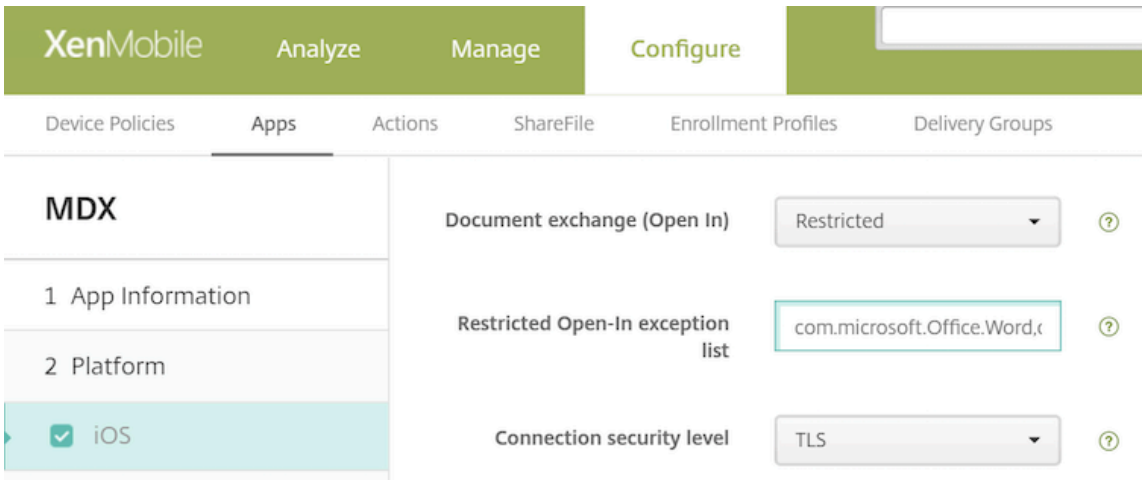
September 7, 2025

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**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Enabling Office 365 in Android

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

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.
   office.powerpoint } { package=com.microsoft.office.excel }
   ```

5. Configure other app policies as usual and the save the apps.

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

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

Supported file formats

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

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.