



Mobile productivity apps

Contents

Mobile productivity apps release timeline	21
About the Secure Mail and Secure Web phased release process	21
Prerequisites for feature flag management	21
Support for mobile productivity apps	22
Supported operating systems	22
Other considerations and limitations	23
Secure Mail	23
Secure Web	24
QuickEdit	24
Citrix Content Collaboration™ for Endpoint Management	24
ShareConnect	24
Citrix Secure Notes and Citrix Secure Tasks	24
Administrator tasks and considerations	25
Feature flag management	25
Enable traffic to the following URLs	25
Create an allow list by domain	25
List IP addresses in an allow list	25
LaunchDarkly system requirements	26
Supported app stores	26
Enabling public app store distribution	26
Apple push notifications	27
Public app store FAQs	27
Android	28
iOS	28
MDX policies for mobile productivity apps	31
Dual mode in Secure Mail for Android	31

Prerequisites	32
Limitations	33
User connections to the internal network	34
Network access restrictions	34
Endpoint Management client properties	35
User password caching	35
Inactivity timer	35
Citrix PIN authentication	35
Fingerprint or touch ID authentication	35
Fingerprint authentication requirements	36
To configure fingerprint authentication	36
Google Analytics	37
Disable Google Analytics	37
MDX policies for mobile productivity apps at a glance	38
Authentication	38
Device passcode	38
App passcode	38
Online session required grace period (minutes)	38
Maximum offline period	39
Alternate Citrix Gateway	39
Device security	39
Block jailbroken or rooted	39
Require device lock	39
Network requirements	40
Require Wi-Fi	40
Allowed Wi-Fi Networks	40
Miscellaneous access	40
App update grace period (hours)	40

Disable required upgrade	40
Erase app data on lock	40
Active poll period (minutes)	41
Encryption	41
Encryption type	41
Non-compliant device behavior	41
Enable MDX encryption	41
Encryption keys	42
Private file encryption	42
Private file encryption exclusions	42
Access limits for public files	42
Public file encryption	42
Public file encryption exclusions	43
Public file migration	43
Enable encryption	43
Database encryption exclusions	43
File encryption exclusions	44
App interaction	44
Security Group	44
Cut and copy	44
Paste	44
Document exchange (Open in)	44
URL domains excluded from filtering	45
Allowed Secure Web domains	45
Connection security level	45
Inbound document exchange (Open In)	45
Restricted Open In exception list	45
App URL schemes	45

Allowed URLs	46
Explicit logoff notifications	46
App interaction (outbound URL)	46
Domains excluded from URL filtering	46
Allowed URLs	46
Allowed Secure Web Domains	46
App restrictions	47
Block camera	47
Block gallery	47
Block Photo Library	47
Block mic record	47
Block dictation	47
Block location services	47
Block SMS compose	48
Block screen capture	48
Block device sensor	48
Block NFC	48
Block iCloud	48
Block Look Up	48
Block file backup	48
Block AirPrint	49
Block Printing	49
Block AirDrop	49
Block file attachments	49
Block email compose	49
Block Facebook and Twitter APIs	49
Obscure screen contents	50
Block third-party keyboards	50

Block app logs	50
Enable ShareFile	50
Enable Attach from Files	50
App network access	51
Network access	51
micro VPN session required	51
micro VPN session required grace period (minutes)	51
Exclusion List	51
Block localhost connections	51
Certificate label	51
App logs	52
Default log output	52
Default log level	52
Max log files	52
Max log file size	52
Redirect app logs	52
Encrypt logs	52
App geofence	53
Center point longitude	53
Center point latitude	53
Radius	53
App settings	53
Secure Mail Exchange Server	53
Secure Mail user domain	54
Background network services	54
Background services ticket expiration	54
Background network service gateway	54
Export contacts	55

Contact fields to export	55
Accept all SSL certificates	55
Control locked screen notifications	55
Use Secure Connection	55
Default email notification	55
Default sync interval	55
Mail search limit	56
Max sync interval	56
Enable week number	56
Enable downloads of attachments over Wi-Fi	56
Allow offline documents	56
Information Rights Management	57
Email classification	57
Email classification markings	57
Email classification namespace	57
Email classification version	57
Default email classification	57
Enable auto-save of draft emails	57
Enable iOS data protection	58
Push Notifications EWS HostName	58
Push notifications	58
Push notifications region	58
Enable S/MIME during first Secure Mail startup	58
Initial authentication mechanism	58
Initial authentication credentials	59
Enable week number	59
Calendar Web and Audio Options	59
S/MIME public certificate source	59

LDAP Server address	59
LDAP Base DN	59
Access LDAP anonymously	59
Allowed email domains	60
Attempt Username Migration On Authentication Failure	60
Report Phishing Mail Addresses	60
Report Phishing Mechanism	60
Skype for Business Meeting Domains	60
Export calendar	60
Enable Slack	61
Slack workspace name	61
Caller Identification	61
Analytics	61
Enable Google Analytics	61
Google Analytics level of detail	61
Reporting	62
Citrix reporting	62
Upload token	62
Send reports over Wi-Fi only	62
Reporting file cache maximum	62
OAuth support for Office 365	62
Use modern authentication for Office 365	62
Office 365 authentication mechanism	63
Trusted Exchange Online Hostnames	63
Trusted AD FS Hostnames	63
Custom user agent for modern authentication	63
Mail redirection	63
Mail redirection	63

Slack integration	64
Enable Slack	64
Slack workspace name	64
MDX policies for mobile productivity apps for Android	64
Authentication	64
App passcode	64
Maximum offline period (hours)	65
Alternate Citrix Gateway	65
Device Security	65
Block jailbroken or rooted	65
Require device encryption	65
Require device lock	66
Network Requirements	66
Require Wi-Fi	66
Allowed Wi-Fi Networks	66
Miscellaneous Access	66
App update grace period (hours)	66
Disable required upgrade	67
Erase app data on lock	67
Active poll period (minutes)	67
Encryption	67
Encryption type	67
Non-compliant device behavior	68
Encryption keys	68
Private file encryption	68
Private file encryption exclusions	68
Access limits for public files	69
Public file encryption	69

Public file encryption exclusions	70
Public file migration	70
App Interaction	71
Security Group	71
Cut and Copy	71
Paste	71
Document exchange (Open In)	71
URL domains excluded from filtering	71
Allowed Secure Web domains	72
Restricted Open-In exception list	72
Inbound document exchange (Open In)	72
Inbound document exchange whitelist	73
Connection security level	73
App Restrictions	73
Block camera	73
Block Gallery	73
Block mic record	74
Block location services	74
Block SMS compose	74
Block screen capture	74
Block device sensor	74
Block NFC	74
Block app logs	74
Block printing	74
Enable ShareFile	75
App Network Access	75
Network access	75
Micro VPN session required	75

Exclusion List	76
Block localhost connections	76
Certificate label	76
App Logs	76
Default log output	76
Default log level	76
Max log files	77
Max log file size	77
Redirect app logs	77
Encrypt logs	77
App Geofence	77
Center point longitude	77
Center point latitude	78
Radius	78
Analytics	78
Google Analytics of detail	78
App Settings	78
Secure Mail Exchange Server	78
Secure Mail user domain	78
Background network services	79
Background services ticket expiration	79
Background network service gateway	79
Export contacts	79
Contact fields to export	80
Accept all SSL certificates	80
Use secure connection	80
Information Rights Management	80
Control locked screen notifications	80

Default sync interval	80
Enable download of attachments over Wi-Fi	80
Allow offline documents	81
Enable auto-save of email drafts	81
Initial authentication Mechanism	81
Initial authentication credentials	81
Enable week number	81
Email classification	81
Email classification markings	81
Email classification namespace	82
Email classification version	82
Default email classification	82
Mail Search Limit	82
Max sync interval	82
Calendar Web and Audio Options	83
S/MIME Public Certificate Source	83
LDAP Server Address	83
LDAP Base DN	83
Access LDAP Anonymously	83
Allowed Email Domains	83
Push notifications	83
Push notifications EWS host name	84
Push notifications region	84
Attempt user name Migration On Authentication Failure	84
Report Phishing Mail Addresses	84
Report Phishing Mechanism	84
Skype for Business Meeting Domains	84
Export Calendar	85

OAuth Support for Office 365	85
Use Modern authentication for O365	85
Trusted Exchange Online Hostnames	85
Trusted AD FS Hostnames	86
Custom user agent for modern authentication	86
Slack Integration	86
Enable Slack	86
Slack workspace name	86
MDX policies for mobile productivity apps for iOS	86
Authentication	87
Device passcode	87
App passcode	87
Maximum offline period (hours)	87
Alternate Citrix Gateway	87
Device security	88
Block jailbroken or rooted	88
Network requirements	88
Require Wi-Fi	88
Allowed Wi-Fi networks	88
Miscellaneous access	88
Disable required upgrade	88
App update grace period (hours)	88
Erase app data on lock	89
Active poll period (minutes)	89
Encryption	89
Encryption type	89
Non-compliant device behavior	90
Enable MDX encryption	90

Database encryption exclusions	90
File encryption exclusions	90
App interaction	91
Cut and copy	91
Paste	91
Document exchange (Open In)	91
Restricted Open-In exception list	91
Connection security level	92
Inbound document exchange (Open In)	92
App URL schemes	92
App interaction (outbound URL)	93
Domains excluded from URL filtering	93
Allowed URLs	93
Allowed Secure Web domains	96
App Restrictions	96
Block camera	96
Block Photo Library	96
Block mic record	96
Block dictation	96
Block location services	96
Block SMS compose	96
Block email compose	97
Block iCloud	97
Block lookup	97
Block file backup	97
Block AirPrint	97
Block AirDrop	97
Block file attachments	97

Block Facebook and Twitter APIs	98
Obscure screen contents	98
Block 3rd party keyboards (iOS 11 and later only)	98
Block app logs	98
Enable ShareFile	98
Enable Attach From Files	98
App network access	98
Network access	98
Micro VPN session required	99
Micro VPN session required grace period (minutes)	99
Certificate label	99
Exclusion List	99
App logs	100
Default log output	100
Default log level	100
Max log files	100
Max log file size	100
App geofence	100
Center point longitude	100
Center point latitude	101
Radius	101
Enable Google Analytics	101
Analytics	101
Google Analytics level of detail	101
Reporting	101
Citrix reporting	101
Upload token	102
Send reports over Wi-Fi only	102

Report file cache maximum	102
App interaction	102
Explicit logoff notification	102
App settings	102
Secure Mail Exchange Server	102
Secure Mail user domain	102
Background network services	103
Background services ticket expiration	103
Background network service gateway	103
Export Contacts	103
Contact fields to export	104
Accept all SSL certificates	104
Control locked screen notifications	104
Default email notification	104
Default sync interval	104
Mail search limit	104
Max sync interval	105
Enable week number	105
Enable download of attachments over Wi-Fi	105
Allow offline documents	105
Information Rights Management	105
Email classification	105
Email classification markings	105
Email classification namespace	106
Email classification version	106
Default email classification	106
Enable auto-save of email drafts	106
Initial authentication mechanism	106

Initial authentication credentials	106
Enable auto population of user name	107
Enable iOS data protection	107
Push Notifications EWS host name	107
Push notifications	107
Push notifications region	107
S/MIME public certificate source	107
Enable S/MIME during first Secure Mail startup	108
Calendar Web and Audio Options	108
S/MIME public certificate source	108
LDAP server address	108
LDAP Base DN	108
Access LDAP Anonymously	108
Allowed Email Domains	108
Attempt user name Migration On Authentication Failure	109
Report Phishing Mail Address	109
Report Phishing Mechanism	109
Skype for Business Meeting Domains	109
Export Calendar	110
Caller Identification	110
OAuth Support for Office 365	111
Office 365 authentication mechanism	111
Trusted Exchange Online host names	111
Trusted AD FS host names	111
Mail Redirection	111
Mail Redirection	111
Slack Integration	112
Enable Slack	112

Slack workspace name	112
Features by platform	113
Citrix Secure Hub™	113
Citrix Secure Mail	114
Citrix Secure Web™	126
Feature flag management	128
IP addresses	128
System requirements	128
Citrix Secure Hub™	130
Administering Secure Hub	130
Citrix PIN	130
Certificate pinning	131
Configuring certificate + one-time-password authentication for Secure Hub	132
Port requirement for ADS connectivity for Android devices	137
Secure Hub features	139
Secure Mail overview	146
Citrix Secure Web™	148
Integrating and delivering Secure Web	148
Configuring user connections	149
Secure Web policies	150
Allowed or blocked websites	150
Block pop-ups	151
Preloaded bookmarks	151
Home page URL	152
Browser user interface	152
Options	152
Enable web password caching	152
Proxy servers	152

DNS suffixes	153
Preparing intranet sites for Secure Web	153
Troubleshooting intranet sites	154
To create a web archive file	155
Secure Web features	156
Citrix Content Collaboration™ for Endpoint Management	158
How Citrix Content Collaboration for Endpoint Management clients differ from Citrix Files mobile clients	159
User access	159
SSO	159
Micro VPN	159
Two-factor authentication	160
Folder permissions	160
Document access protection	160
Citrix Files account access	160
Device policies	161
MDX policies	161
Data encryption	161
Availability	161
Integrating and delivering Citrix Content Collaboration for Endpoint Management clients	162
To configure Citrix Files account information in Endpoint Management for SSO	163
To add Citrix Content Collaboration for Endpoint Management clients to Endpoint Management	163
Prerequisites	163
To validate Citrix Content Collaboration for Endpoint Management clients	165
EOL and deprecated apps	166
Allowing secure interaction with Office 365 apps	168
Enabling Office 365 in iOS	168

Enabling Office 365 in Android	169
Supported file formats	169
Mobile productivity apps document history	170

Mobile productivity apps release timeline

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

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
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

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

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

NOTE:

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

Other considerations and limitations

For advanced notice of Citrix Endpoint Management features that are being phased out, see [Deprecation](#).

Secure Mail

- Endpoint Management currently doesn't support NetScaler 12.0.41.16 due to an issue with Secure Ticket Authority (STA) and Secure Mail. The issue is fixed in NetScaler 12.0 build 41.22.
- Support in Secure Mail for Exchange 2007 and Lotus Notes 8.5.3 reached End of Life (EOL) on September 30, 2017.

- For the best performance when sending Citrix Files attachments, the latest versions of Citrix Files are recommended. Citrix Files is not supported for Windows.
- In IBM Notes environments, you must configure the IBM Domino Traveler server, version 9.0. For details, see [Integrating Exchange Server or IBM Notes Traveler Server](#).

NOTE:

- Citrix Files for XenMobile has reached EOL on July 1, 2023. For more information, see [EOL and deprecated apps](#)

Secure Web

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

QuickEdit

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

Citrix Content Collaboration™ for Endpoint Management

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

ShareConnect

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

Citrix Secure Notes and Citrix Secure Tasks

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

Administrator tasks and considerations

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

Feature flag management

If an issue occurs with a mobile productivity app in production, we can disable an affected feature within the app code. We can disable the feature for Secure Hub, Secure Mail, and Secure Web for iOS and Android. To do so, we use feature flags and a third-party service called LaunchDarkly. You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements. For details about support since for the exclusion of domains from tunneling, see the [MAM SDK documentation](#).

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

Enable traffic to the following URLs

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

Create an allow list by domain

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

List IP addresses in an allow list

If you must list IP addresses in an allow list, for a list of all current IP address ranges, see this [LaunchDarkly public IP list](#). You can use this list to ensure that your firewall configurations are

updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the [LaunchDarkly Statuspage](#).

Note:

Public app store apps require a fresh installation the first time you deploy them. It is not possible to upgrade from the current enterprise wrapped version of the app to the public store version.

With public app store distribution, you do not sign and wrap Citrix-developed apps with the MDX Toolkit. You can use the MDX Toolkit to wrap third-party or enterprise apps.

LaunchDarkly system requirements

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

Supported app stores

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

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

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

Enabling public app store distribution

1. Download public-store .mdx files for both iOS and Android from the [Endpoint Management downloads page](#).
2. Upload the .mdx files to the Endpoint Management console. The public store versions of the mobile productivity apps are still uploaded as MDX applications. Do not upload the apps as public store apps on the server. For steps, see [Add apps](#).

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

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

Note:

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

Apple push notifications

For more information on configuring push notifications, see [Configuring Secure Mail for Push Notifications](#).

Public app store FAQs

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

Upload a different .mdx file for each user group. However, in this case, a single user cannot belong to multiple groups. If users did belong to multiple groups, multiple copies of the same

app are assigned to that user. Multiple copies of a public store app cannot be deployed to the same device, because the app ID can't be changed.

- Can I push public store apps as required apps?

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

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

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

Important:

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

Android

APP	SERVER	USER-AGENT STRING
Citrix Secure Mail™	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web™		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	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

APP	SERVER	USER-AGENT STRING
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- Can I prevent app upgrades?

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

- Can I enforce app upgrades?

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

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

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

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

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

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

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

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

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

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

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

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

Note:

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

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

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

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

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

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

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

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

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

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

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

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

MDX policies for mobile productivity apps

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

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

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

- [MDX policies for mobile productivity apps at a glance](#)
- [MDX policies for mobile productivity apps for Android](#)
- [MDX policies for mobile productivity apps for iOS](#)

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

Dual mode in Secure Mail for Android

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

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

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

NOTE:

When you use the MAM SDK, you do not need to wrap apps.

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

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

- [MAM SDK Overview](#)
- [Latest releases of MAM SDK](#)
- Citrix Developer section on [Device Management](#)
- [Citrix blog post](#)

Prerequisites

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

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

NOTE:

MAM SDK is supported for all cloud-based customers.

Limitations

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

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

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

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

The screenshot shows the Citrix Cloud Endpoint Management console. The left sidebar has a menu with 'MDX' and '1 App Information'. The main area is titled 'MDX or MAM SDK policy container' and contains several settings:

- File name ***: Secure Mail
- App Description ***: Managed Enterprise Application
- App version**: 20.4.5
- Minimum OS version**: 11.0
- Maximum OS version**: (empty)
- 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
- App deployed via Volume purchase**: OFF
- MDX or MAM SDK policy container**: MAM SDK (selected), Legacy MDX

Below the settings, there is a section for 'MDX Policies' with a sub-section for 'Authentication'.

In the **MDX or MAM SDK policy container** policy, you can only change your option from **Legacy MDX** to **MAM SDK**. The option to switch from **MAM SDK** to **Legacy MDX** is not allowed, and you need to republish the app. The default value is **Legacy MDX**. Ensure that you set the same policy

mode for both Secure Mail and Secure Web running on the same device. You cannot have two different modes running on the same device.

User connections to the internal network

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

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

Network access restrictions

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

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

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

Endpoint Management client properties

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

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

User password caching

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

Inactivity timer

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

Citrix PIN authentication

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

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

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

Fingerprint or touch ID authentication

Fingerprint authentication, also known as touch ID authentication, for iOS devices is an alternative to Citrix PIN. The feature is useful when wrapped apps, except for Secure Hub, are in need offline

authentication, such as when the inactivity timer expires. You can enable this feature in the following authentication scenarios:

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

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

Fingerprint authentication requirements

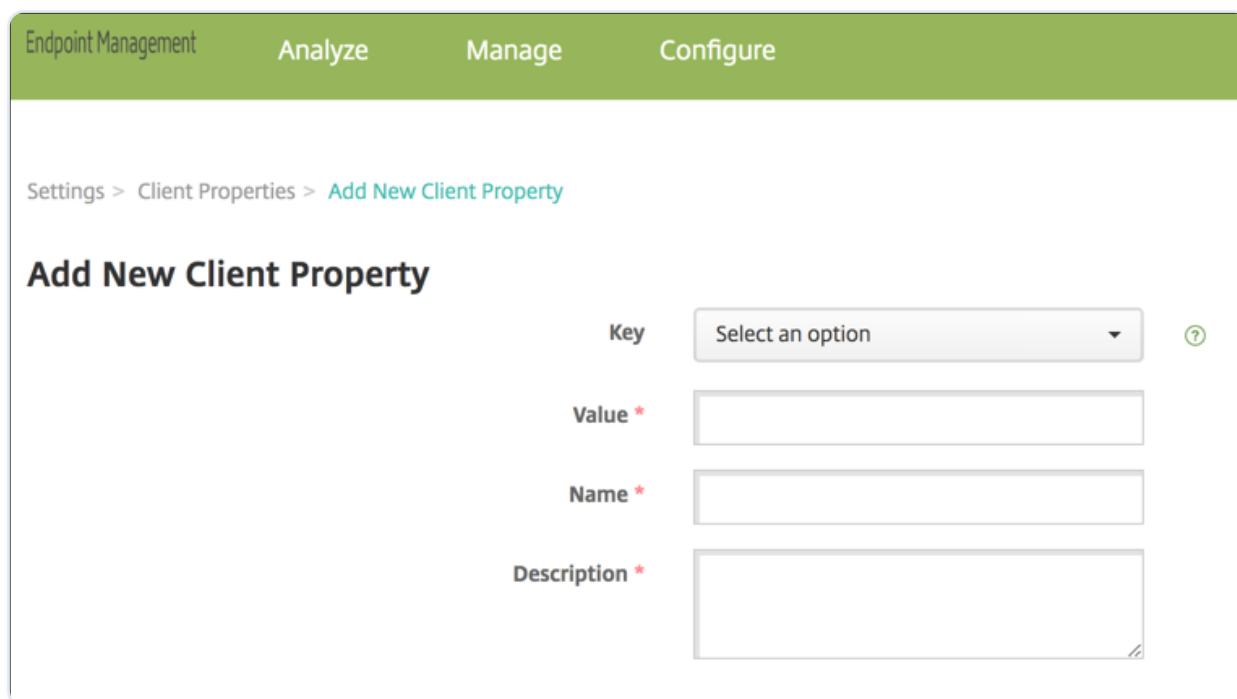
- iOS devices (minimum version 8.1) that support fingerprint authentication and have at least one fingerprint configured.
- User entropy must be off.

To configure fingerprint authentication

Important:

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

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



The screenshot shows the Citrix Endpoint Management console interface. At the top, there is a green navigation bar with the following tabs: 'Endpoint Management', 'Analyze', 'Manage', and 'Configure'. Below the navigation bar, the breadcrumb trail reads 'Settings > Client Properties > Add New Client Property'. The main heading is 'Add New Client Property'. The form contains four fields: 'Key' (a dropdown menu with 'Select an option' and a help icon), 'Value' (a text input field with a red asterisk), 'Name' (a text input field with a red asterisk), and 'Description' (a larger text input field with a red asterisk).

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

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

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

Google Analytics

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

Disable Google Analytics

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

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

NOTE:

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

MDX policies for mobile productivity apps at a glance

This article notes the MDX app policies for Citrix mobile productivity apps for iOS and Android, along with the default values. You change policy settings in the Citrix Endpoint Management console. For details, see [Add apps](#).

NOTE:

Secure Hub refreshes policies during certain actions. For details, see [Administering Secure Hub](#).

Authentication

Device passcode

- iOS: Yes
- Android: No
- Default setting: Off

NOTE:

This policy only applied to iOS 9 devices, which Citrix® no longer supports.

App passcode

- iOS: Yes
- Android: Yes
- Default setting: On

Online session required grace period (minutes)

- iOS: Yes
- Android: No

- Default setting: 0

Maximum offline period

- iOS: Yes
- Android: Yes
- Default setting: 168 hours (7 days)

Alternate Citrix Gateway

NOTE:

This policy name in the Endpoint Management console is Alternate NetScaler® Gateway.

- iOS: Yes
- Android: Yes
- Default setting: Empty

Device security

Block jailbroken or rooted

- iOS: Yes
- Android: Yes
- Default setting: On

Require device lock

- iOS: No
- Android: Yes
- Default setting: Off

NOTE:

On Android M devices, the Device PIN or passcode and Device pattern screen lock options have the same effect: With either of those options, the app is locked if the device does not have a PIN, passcode, or pattern screen lock set.

Network requirements

Require Wi-Fi

- iOS: Yes
- Android: Yes
- Default setting: Off

Allowed Wi-Fi Networks

- iOS: Yes
- Android: Yes
- Default setting: Empty

Miscellaneous access

App update grace period (hours)

- iOS: Yes
- Android: Yes
- Default setting: 168 hours (7 days)

NOTE:

Citrix recommends using a value other than zero (0). A zero value immediately prevents users, without warning, from using a running app until they download and install the update. This setting may lead to a situation in which users are forced to exit the app and potentially lose work.

Disable required upgrade

- iOS: Yes
- Android: Yes
- Default setting: On

Erase app data on lock

- iOS: Yes
- Android: Yes

- Default setting: Off

Active poll period (minutes)

- iOS: Yes
- Android: Yes
- Default setting: 60 minutes (1 hour)

NOTE:

Only set this value lower than the default for high-risk apps, or performance may be affected.

Encryption

Encryption type

- iOS: Yes
- Android: Yes
- Default setting: MDX encryption

CAUTION:

For newly added apps, when you change from **Platform encryption with compliance enforcement** to **MDX encryption**, you are forced to remove and reinstall the app. The default setting for newly added apps is **Platform encryption with compliance enforcement**.

Non-compliant device behavior

- iOS: Yes
- Android: Yes
- Default setting: Allow app after warning

Enable MDX encryption

- iOS: Yes
- Android: No

- Default setting: On

CAUTION:

If you change this policy after deploying an app, users must reinstall the app.

Encryption keys

- iOS: No
- Android: Yes
- Default setting: Offline access permitted is the only available option.

Private file encryption

- iOS: No
- Android: Yes
- Default setting: SecurityGroup

Private file encryption exclusions

- iOS: No
- Android: Yes
- Default setting: Empty

Access limits for public files

- iOS: No
- Android: Yes
- Default setting: Empty

NOTE:

Enabling the Public file encryption policy enforces this policy (changed from the Disable Option to the SecurityGroup or Application option). This policy applies only to existing, unencrypted public files and specifies when to encrypt the files.

Public file encryption

- iOS: No

- Android: Yes
- Default setting: SecurityGroup

Public file encryption exclusions

- iOS: No
- Android: Yes
- Default setting: Empty

Public file migration

- iOS: No
- Android: Yes
- Default setting: Write (RO/RW)

NOTE:

Encrypting an existing public file makes the file unavailable to other apps that do not have the same encryption key.

Enable encryption

- iOS: Yes
- Android: No
- Default setting: On

NOTE:

If you change this policy for an existing app, users must remove and reinstall the app to apply the policy change.

Database encryption exclusions

- iOS: Yes
- Android: No
- Default setting: Empty

File encryption exclusions

- iOS: Yes
- Android: No
- Default setting: Empty

App interaction

Security Group

- iOS: No
- Android: Yes
- Default setting: Empty

NOTE:

If you change this policy for an existing app, users must remove and reinstall the app to apply the policy change.

Cut and copy

- iOS: Yes
- Android: Yes
- Default setting: Restricted

Paste

- iOS: Yes
- Android: Yes
- Default setting: Unrestricted

Document exchange (Open in)

- iOS: Yes
- Android: Yes
- Default setting: Restricted

URL domains excluded from filtering

- iOS: No
- Android: Yes
- Default setting: Empty

Allowed Secure Web domains

- iOS: No
- Android: Yes
- Default setting: Empty

Connection security level

- iOS: Yes
- Android: Yes
- Default setting: TLS

Inbound document exchange (Open In)

- iOS: Yes
- Android: Yes
- Default setting: Unrestricted

Restricted Open In exception list

- iOS: Yes
- Android: Yes
- Default setting: Empty (for Android); Office 365 apps (for iOS)

NOTE:

On Android, this policy was previously named Open In exclusions. On iOS, this policy is hidden. For details, see [MDX policies for iOS apps](#).

App URL schemes

- iOS: Yes
- Android: No

- Default setting: Empty. All registered app URL schemes are blocked.

Allowed URLs

- iOS: Yes
- Android: No
- Default setting: For details about the default settings, see the App Interaction section in MDX policies for iOS apps.

Explicit logoff notifications

- iOS: Yes
- Android: No
- Default setting: Shared devices only, for Secure Mail

App interaction (outbound URL)

Domains excluded from URL filtering

- iOS: Yes
- Android: No
- Default setting: Empty

Allowed URLs

- iOS: Yes
- Android: No
- Default setting: or details about the default settings, see the App interaction (outbound URL) section in [MDX policies for iOS apps](#)

Allowed Secure Web Domains

- iOS: Yes
- Android: No
- Default setting: Empty

App restrictions

Block camera

- iOS: Yes
- Android: Yes
- Default setting: Off for iOS; On for Android

Block gallery

- iOS: No
- Android: Yes
- Default setting: Off

Block Photo Library

- iOS: Yes
- Android: No
- Default setting: On

Block mic record

- iOS: Yes
- Android: Yes
- Default setting: On

Block dictation

- iOS: Yes
- Android: No
- Default setting: On

Block location services

- iOS: Yes
- Android: Yes
- Default setting: For Android: Default value is Off for Secure Mail. Default value is On for other apps.

Block SMS compose

- iOS: Yes
- Android: Yes
- Default setting: On

Block screen capture

- iOS: No
- Android: Yes
- Default setting: On

Block device sensor

- iOS: No
- Android: Yes
- Default setting: On

Block NFC

- iOS: No
- Android: Yes
- Default setting: On

Block iCloud

- iOS: Yes
- Android: No
- Default setting: On

Block Look Up

- iOS: Yes
- Android: No
- Default setting: On

Block file backup

- iOS: Yes
- Android: No

- Default setting: On

Block AirPrint

- iOS: Yes
- Android: No
- Default setting: On

Block Printing

- iOS: No
- Android: Yes
- Default setting: On

Block AirDrop

- iOS: Yes
- Android: No
- Default setting: On

Block file attachments

- iOS: Yes
- Android: No
- Default setting: Off

Block email compose

- iOS: Yes
- Android: No
- Default setting: On

Block Facebook and Twitter APIs

- iOS: Yes
- Android: No
- Default setting: On

Obscure screen contents

- iOS: Yes
- Android: No
- Default setting: On

Block third-party keyboards

- iOS: Yes
- Android: No
- Default setting: On

NOTE

iOS 11 and later

Block app logs

- iOS: Yes
- Android: Yes
- Default setting: Off

Enable ShareFile

- iOS:
- Android: Yes
- Default setting: On

Enable Attach from Files

- iOS: Yes
- Android: No
- Default setting: On

App network access

Network access

- iOS: Yes
- Android: Yes
- Default setting: For newly uploaded apps, the default is **Blocked** for all apps, except Secure Mail. Because Intune does not have a blocked state, the default for Secure Mail is **Unrestricted**.

micro VPN session required

- iOS: Yes
- Android: Yes
- Default setting: Use Previous Setting. For newly uploaded apps, the default value is No.

micro VPN session required grace period (minutes)

- iOS: Yes
- Android: Yes
- Default setting: 0 (no grace period)

Exclusion List

- iOS: Yes
- Android: Yes
- Default setting: Empty

Block localhost connections

- iOS: No
- Android: Yes
- Default setting: Off

Certificate label

- iOS: Yes
- Android: Yes
- Default setting: Empty

App logs

Default log output

- iOS: Yes
- Android: Yes
- Default setting: file

Default log level

- iOS: Yes
- Android: Yes
- Default setting: 4 (informational messages)

Max log files

- iOS: Yes
- Android: Yes
- Default setting: 2

Max log file size

- iOS: Yes
- Android: Yes
- Default setting: 2 MB

Redirect app logs

- iOS: No
- Android: Yes
- Default setting: On

Encrypt logs

- iOS: No
- Android: Yes
- Default setting: Off

App geofence

Center point longitude

- iOS: Yes
- Android: Yes
- Default setting: 0

Center point latitude

- iOS: Yes
- Android: Yes
- Default setting: 0

Radius

- iOS: Yes
- Android: Yes
- Default setting: 0 (disabled)

NOTE:

Set the radius in meters. When set to zero, the geofence is disabled.

App settings

Secure Mail Exchange Server

- iOS: Yes
- Android: Yes
- Default setting: Empty

NOTE:

If you change this policy for an existing app, users must remove and reinstall the app to apply the policy change.

Secure Mail user domain

- iOS: Yes
- Android: Yes
- Default setting: Empty

Background network services

- iOS: Yes
- Android: Yes
- Default setting: Empty

NOTE:

If you configure this policy, set the Network access policy to Tunneled to the internal network, after which this policy takes effect. Use this policy when the Exchange Server is in your internal network and you want to use Citrix Gateway to proxy the connection to the internal Exchange Server.

Background services ticket expiration

- iOS: Yes
- Android: Yes
- Default setting: 168 hours (7 days)

Background network service gateway

- iOS: Yes
- Android: Yes
- Default setting: Empty

NOTE:

If you configure this policy, set the network access policy to Tunneled to the internal network, after which this policy takes effect. Use this policy when the Exchange Server is in your internal network or if you want to use Citrix Gateway to proxy the connection to the internal Exchange Server. This policy takes effect when you configure the Network access policy.

Export contacts

- iOS: Yes
- Android: Yes
- Default setting: Off

Contact fields to export

- iOS: Yes
- Android: Yes
- Default setting: All

Accept all SSL certificates

- iOS: Yes
- Android: Yes
- Default setting: Off

Control locked screen notifications

- iOS: Yes
- Android: Yes
- Default setting: Allow

Use Secure Connection

- iOS: No
- Android: Yes
- Default setting: On

Default email notification

- iOS: Yes
- Android: No
- Default setting: On

Default sync interval

- iOS: Yes
- Android: Yes

- Default setting: 3 days

NOTE:

The Exchange ActiveSync mailbox policy setting Maximum email age filter has priority over this policy. Secure Mail displays only the sync interval values that are less than the Maximum email age filter.

Mail search limit

- iOS: Yes
- Android: Yes
- Default setting: Unlimited

Max sync interval

- iOS: Yes
- Android: Yes
- Default setting: All

Enable week number

- iOS: Yes
- Android: Yes
- Default setting: Off

Enable downloads of attachments over Wi-Fi

- iOS: Yes
- Android: Yes
- Default setting: Off

Allow offline documents

- iOS: Yes
- Android: Yes
- Default setting: Unlimited

Information Rights Management

- iOS: Yes
- Android: Yes
- Default setting: Off

Email classification

- iOS: Yes
- Android: No
- Default setting: Off

Email classification markings

- iOS: Yes
- Android: No
- Default setting: Empty

Email classification namespace

- iOS: Yes
- Android: No
- Default setting: Empty

Email classification version

- iOS: Yes
- Android: No
- Default setting: Empty

Default email classification

- iOS: Yes
- Android: No
- Default setting: UNOFFICIAL

Enable auto-save of draft emails

- iOS: Yes
- Android: Yes

- Default setting: On

Enable iOS data protection

- iOS: Yes
- Android: No
- Default setting: Off

Push Notifications EWS HostName

- iOS: Yes
- Android: No
- Default setting: Empty

Push notifications

- iOS: Yes
- Android: No
- Default setting: Off

Push notifications region

- iOS: Yes
- Android: No
- Default setting: Americas

Enable S/MIME during first Secure Mail startup

- iOS: Yes
- Android: No
- Default setting: Off

Initial authentication mechanism

- iOS: Yes
- Android: Yes
- Default setting: Use MDX provided mail server address

Initial authentication credentials

- iOS: Yes
- Android: Yes
- Default setting: Enrollment user name

Enable week number

- iOS: Yes
- Android: Yes
- Default setting: Off

Calendar Web and Audio Options

- iOS: Yes
- Android: Yes
- Default setting: GoToMeeting and User Entered

S/MIME public certificate source

- iOS: Yes
- Android: Yes
- Default setting: Exchange

LDAP Server address

- iOS: Yes
- Android: Yes
- Default setting: Empty

LDAP Base DN

- iOS: Yes
- Android: Yes
- Default setting: Empty

Access LDAP anonymously

- iOS: Yes
- Android: Yes

- Default setting: Off

Allowed email domains

- iOS: Yes
- Android: No
- Default setting: Empty

NOTE

If empty, does not restrict domains.

Attempt Username Migration On Authentication Failure

- iOS: Yes
- Android: Yes
- Default setting: Off

Report Phishing Mail Addresses

- iOS: Yes
- Android: Yes
- Default setting: Empty

Report Phishing Mechanism

- iOS: No
- Android: Yes
- Default setting: Report via attachment (.eml)

Skype for Business Meeting Domains

- iOS: Yes
- Android: Yes
- Default setting: Empty

Export calendar

- iOS: Yes

- Android: Yes
- Default setting: Meeting time

Enable Slack

- iOS: Yes
- Android: Yes
- Default setting: Off

Slack workspace name

- iOS: Yes
- Android: Yes
- Default setting: Empty

Caller Identification

- iOS: Yes
- Android: No
- Default setting: On

NOTE:

If On, Secure Mail provides iOS with names and phone numbers of your saved contacts for caller identification.

Analytics

Enable Google Analytics

- iOS: Yes
- Android: No
- Default setting: On

Google Analytics level of detail

- iOS: Yes
- Android: Yes
- Default setting: Complete

Reporting

Citrix reporting

- iOS: Yes
- Android: No
- Default setting: Off

NOTE:

Citrix might also control this feature with a feature flag. Both the feature flag and this policy must be enabled for this feature to function.

Upload token

- iOS: Yes
- Android: No
- Default setting: Empty

Send reports over Wi-Fi only

- iOS: Yes
- Android: No
- Default setting: On

Reporting file cache maximum

- iOS: Yes
- Android: No
- Default setting: 2 MB

OAuth support for Office 365

Use modern authentication for Office 365

- iOS: No
- Android: Yes
- Default setting: Off

Office 365 authentication mechanism

- iOS: Yes
- Android: No
- Default setting: Do not use OAuth

Trusted Exchange Online Hostnames

- iOS: Yes
- Android: Yes
- Default setting: `outlook.office365.com`

Trusted AD FS Hostnames

- iOS: Yes
- Android: Yes
- Default setting: `login.microsoftonline.com`

Custom user agent for modern authentication

- iOS: No
- Android: Yes
- Default setting: Empty

NOTE:

If you do not configure this policy, the default Secure Mail user agent is used during modern authentication.

Mail redirection

Mail redirection

- iOS: Yes
- Android: No
- Default setting: Secure Mail

Slack integration

Enable Slack

- iOS: Yes
- Android: Yes
- Default setting: Off

Slack workspace name

- iOS: Yes
- Android: Yes
- Default setting: Empty

MDX policies for mobile productivity apps for Android

This article describes the MDX policies for Android apps. You change policy settings in the Citrix Endpoint Management console. For details, see [Add apps](#).

The following list does not include MDX policies specific to Secure Web. For details about the policies that appear for Secure Web, see [Secure Web policies](#).

Authentication

App passcode

If **On**, a PIN or passcode is required to unlock the app when it starts or resumes after a period of inactivity. Default value is **On**.

To configure the inactivity timer for all apps, set the INACTIVITY_TIMER value in minutes in **Client Properties** on the **Settings** tab. The default inactivity timer value is 60 minutes. To disable the inactivity timer, so that a PIN or passcode prompt appears only when the app starts, set the value to zero.

NOTE:

If you select Secure offline for the Encryption keys policy, this policy is automatically enabled.

Maximum offline period (hours)

Defines the maximum period an app can run offline without a network logon for reconfirming entitlement and refreshing policies. Default value is **168 hours** (7 days). The minimum period is 1 hour.

The user is reminded to log on at 30, 15, and 5 minutes before the period expires. After expiration, the app remains locked until the user completes a successful network logon.

Alternate Citrix Gateway

NOTE:

This policy name in the Endpoint Management console is **Alternate NetScaler® Gateway**.

Address of a specific alternate Citrix Gateway (formerly, NetScaler Gateway) that is used for authentication and for micro VPN sessions with this app. **Alternate NetScaler Gateway** is an optional policy when used with the Online session required policy forces apps to reauthenticate to the specific gateway. Such gateways would typically have different (higher assurance) authentication requirements and traffic management policies. If left empty, the server's default is always used. Default value is empty.

Device Security

Block jailbroken or rooted

If **On**, the app is locked when the device is jailbroken or rooted. If **Off**, the app can run even if the device is jailbroken or rooted. Default value is **On**.

Require device encryption

If **On**, the app is locked if the device does not have encryption configured. If **Off**, the app is allowed to run even if the device does not have encryption configured. Default value is **Off**.

NOTE:

This policy is supported only on Android 3.0 (Honeycomb). Setting the policy to **On** prevents an app from running on older versions.

Require device lock

If **Device PIN or passcode** is selected, the app is locked if the device does not have a PIN or passcode. If **Device pattern screen lock** is selected, the app is locked if the device does not have a pattern screen lock set. If **Off**, the app is allowed to run even if the device does not have a PIN, passcode, or pattern screen lock set. Default value is **Off**.

Device PIN or passcode requires a minimum version of Android 4.1 (Jelly bean). Setting the policy to **Device PIN or passcode** prevents an app from running on older versions.

On Android M devices, the **Device PIN or passcode** and **Device pattern screen lock** options have the same effect: With either of those options, the app is locked if the device does not have a PIN, passcode, or pattern screen lock set.

Network Requirements

Require Wi-Fi

If **On**, the app is locked when the device is not connected to a Wi-Fi network. If **Off**, the app can run if the device has an active connection, such as a 4G/3G, LAN, or Wi-Fi connection. Default value is **Off**.

Allowed Wi-Fi Networks

Comma-delimited list of allowed Wi-Fi networks. If the network name contains any non-alphanumeric characters (including commas), the name must be enclosed in double-quotes. App runs only if connected to one of the networks listed. If left blank, all networks are allowed. This value does not affect connections to cellular networks. Default value is blank.

Miscellaneous Access

App update grace period (hours)

Defines the grace period in which an app can be used after the system discovers that an app update is available. Default value is **168 hours** (7 days).

NOTE:

Using zero is not recommended since it immediately prevents a running app from being used until the update is downloaded and installed (without any warning to the user). This value can lead to a situation where the user running the app is forced to exit the app (potentially losing work) to comply with the required update.

Disable required upgrade

Disables the requirement that users upgrade to the newest version of the app in the App store. Default value is **ON**.

Erase app data on lock

Erases data and resets the app when the app is locked. If **Off**, app data is not erased when the app is locked. Default value is **Off**.

An app can be locked for any of the following reasons:

- Loss of app entitlement for the user
- App subscription removed
- Account removed
- Secure Hub uninstalled
- Too many app authentication failures
- Jailbroken device detected (per policy setting)
- Device placed in locked state by other administrative action

Active poll period (minutes)

When an app starts, the MDX framework polls Citrix Endpoint Management to determine current app and device status. Assuming the server running Endpoint Management can be reached, the framework returns information about the lock/erase status of the device and the enable/disable status of the app. Whether the server can be reached or not, a subsequent poll is scheduled based on the active poll period interval. After the period expires, a new poll is again attempted. Default value is **60 minutes** (1 hour).

IMPORTANT:

Only set this value lower for high-risk apps or performance might be affected.

Encryption

Encryption type

Allows you to choose whether MDX or the device platform handles the encryption of data. If you select **MDX encryption**, then MDX encrypts the data. If you select **Platform encryption with**

compliance enforcement, then the device platform encrypts the data. Default value is **MDX encryption**.

Non-compliant device behavior

Allows you to choose an action when a device does not adhere to the minimum compliance requirements of encryption. Select **Allow app** for the app to run normally. Select **Allow app after warning** for the app to run after the warning appears. Select **Block** to block the app from running. Default value is **Allow app after warning**.

Encryption keys

Enables secrets used to derive encryption keys to be persisted on the device. Offline access permitted is the only available option.

Citrix recommends that you set the Authentication policy to enable a network logon or an offline password challenge to protect access to the encrypted content.

Private file encryption

Controls the encryption of private data files in the following locations: `/data/data/<appname>` and `/mnt/sdcard/Android/data/<appname>`.

The **Disabled** option means private files are not encrypted. The **SecurityGroup** option encrypts private files using a key shared by all MDX apps in the same security group. The **Application** option encrypts private files using a key unique to this app. Default value is **SecurityGroup**.

Private file encryption exclusions

Contains a comma-separated list of file paths. Each path is a regular expression that represents one or more files that are encrypted. The file paths are relative to the internal and external sandboxes. Default value is empty.

The exclusions only apply to the following folders:

- **Internal Storage:**

```
/data/data/<your_package_name>
```

- **SD Card:**

```
/storage/emulated/\<SD Card Slot>/Android/data/<your_package_name>
```

```
/storage/emulated/legacy/Android/data/<your_package_name>
```

Examples

FILE TO EXCLUDE	VALUE IN PRIVATE FILE ENCRYPTION EXCLUSION
/data/data/com.citrix.mail/files/a.txt	^files/a.txt
All text files in /storage/emulated/0/Android/data/com.citrix.mail/files	^files/(.)+.txt\$
All files in /data/data/com.citrix.mail/files	^files/

Access limits for public files

Contains a comma-separated list. Each entry is a regular expression path followed by (NA), (RO), or (RW). Files matching the path are limited to **No Access**, **Read Only**, or **Read Write** access. The list is processed in order and the first matching path is used to set the access limit. Default value is empty.

This policy is enforced only when **Public file encryption is enabled** (changed from the **Disable** option to the **SecurityGroup** or **Application** option). This policy is applicable only to existing, unencrypted public files and specifies when these files are encrypted.

FILES TO EXCLUDE	VALUE IN PRIVATE FILE ENCRYPTION
Downloads folder on external storage read only	EXT:^Download/(RO)
All MP3 files in the Music folder on virtual storage no access	VS:^Music/(.)+.mp3\$(NA)

Public file encryption

Controls the encryption of public files. If **Disabled**, public files are not encrypted. If **SecurityGroup**, encrypts public files by using a key shared by all MDX apps in the same security group. If **Application**, encrypts public files by using a key unique to this app.

Default value is **SecurityGroup**.

Public file encryption exclusions

Contains a comma-separated list of file paths. Each path is a regular expression that represents one or more files that are not encrypted. The file paths are relative to the default external storage and to any device-specific external storage.

Public file encryption exclusions include external folder locations only.

Examples

FILE TO EXCLUDE	VALUE IN PUBLIC FILE ENCRYPTION EXCLUSION
Downloads folder on SD card	Download
All MP3 files in Music folder	\\Music/(.)+.mp3\$

Public file migration

This policy is enforced only when you enable the Public file encryption policy (changed from **Disabled** to **SecurityGroup** or **Application**). This policy is applicable only to existing, unencrypted public files and specifies when these files are encrypted. Default value is **Write (RO/RW)**.

The **Disabled** option means that the existing files are not encrypted. The **Write (RO/RW)** option encrypts the existing files only when they are opened for write-only or read-write access. The **Any** option encrypts the exist files when they are opened in any mode. Options:

- **Disabled**. Does not encrypt existing files.
- **Write (RO/RW)**. Encrypts the existing files only when they are opened for write-only or read-write access.
- **Any**. Encrypts the existing files when they are opened in any mode.

NOTES:

-New files or existing unencrypted files that are overwritten encrypt the replacement files in every case. -Encryption an existing public file makes the file unavailable to other apps that we do not have the same encryption key.

App Interaction

Security Group

Leave this field blank if you want all mobile apps managed by Citrix Endpoint Management™ to exchange information with one another. Define a security group name to manage security settings for specific sets of apps (for example, Finance or Human Resources).

CAUTION:

If you change this policy for an existing app, users must delete and reinstall the app to apply the policy change.

Cut and Copy

Blocks, permits, or restricts clipboard cut and copy operations for this app. If **Restricted**, the copied Clipboard data is placed in a private Clipboard that is only available to MDX apps. Default value is **Restricted**.

Paste

Blocks, permits, or restricts clipboard paste operations for the app. If **Restricted**, the pasted clipboard data is sourced from a private Clipboard that is only available to MDX apps. Default value is **Unrestricted**.

Document exchange (Open In)

Blocks, permits, or restricts document exchange operations for the app. If **Restricted**, documents can be exchanged only with other MDX apps and the app exceptions specified in the Restricted Open-In exception list policy. If **Unrestricted**, set the Private file encryption and Public file encryption policies to **Disabled** so that users can open documents in unwrapped apps. Default value is **Restricted**.

URL domains excluded from filtering

This policy is used to exclude certain outbound URLs from MDX filtering. Following comma-separated list of fully qualified domain names(FQDN) or DNS suffixes are excluded from any MDX filtering. If this policy contains any entries, then URLs with host fields matching at least one item in the list (via DNS suffix matching) is sent unaltered to the default browser. Default value is empty.

Allowed Secure Web domains

This policy is only in effect for the domains not excluded by a URL filtering policy. Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that are redirected to the Secure Web app when Document Exchange is Restricted.

If this policy contains any entries, only those URLs with host fields matching at least one item in the list (via DNS suffix match) are redirected to the Secure Web app when Document Exchange is Restricted.

All other URLs are sent to the default Android web browser (bypassing the Document Exchange Restricted policy). Default value is empty.

Restricted Open-In exception list

When the Document exchange (Open In) policy is **Restricted**, this list of Android intents is allowed to pass to unmanaged apps. A familiarity with Android intents is needed to add filters to the list. A filter can specify action, package, scheme, or any combination.

Examples

```
{action=android.intent.action.MAIN}

{package=com.sharefile.mobile}

{action=android.intent.action.DIAL scheme=tel}

{action=android.intent.action.VIEW scheme=msteams
package=com.microsoft.teams}
```

Caution

Be sure to consider the security implications of this policy. The exception list allows content to travel between unmanaged apps and the MDX environment.

Inbound document exchange (Open In)

Blocks, restricts, or allows inbound document exchange operations for this app. If **Restricted**, documents can be exchanged only with other MDX apps. Default value is **Unrestricted**.

If **Blocked** or **Restricted**, you can use the Inbound document exchange whitelist policy to specify apps that can send documents to this app. For information about other policy interactions, see the Block Gallery policy.

Options: **Unrestricted**, **Blocked**, or **Restricted**

Inbound document exchange whitelist

When the Inbound document exchange policy is restricted or blocked, this comma-delimited list of app IDs, including non-MDX apps, is allowed to send documents to the app. This policy is hidden and cannot be edited.

Connection security level

Determines the minimum version of TLS/SSL used for connections. If **TLS**, connections support all TLS protocols. If **SSLv3 and TLS**, connections support SSL 3.0 and TLS. Default value is **TLS**.

App Restrictions

IMPORTANT:

Be sure to consider the security implications of policies that block apps from accessing or using phone features. When those policies are **Off**, content can travel between unmanaged apps and the Secure environment.

Block camera

If **On**, prevents an app from directly using the camera hardware. Default value is **On**.

Block Gallery

If **On**, prevents an app from accessing the Gallery on the device. Default value is **Off**. This policy works along with the Inbound document exchange (Open In) policy.

- If Inbound document exchange (Open In) is set to **Restricted**, users working in the managed app cannot attach images from the Gallery, regardless of the Block Gallery setting.
- If Inbound document exchange (Open In) is set to **Unrestricted**, users working in the managed app experience the following:
 - Users can attach images if Block Gallery is set to **Off**.
 - Users are blocked from attaching images if Block Gallery is **On**.

Block mic record

If **On**, prevents an app from directly using the microphone hardware. Default value is **On**.

Block location services

If **On**, prevents an app from using the location services components (GPS or network). Default value is **Off** for Secure Mail.

Block SMS compose

If **On**, prevents an app from using the SMS compose feature used to send SMS/text messages from the app. Default value is **On**.

Block screen capture

If **On**, prevents users from taking screen captures while the app is running. Also, when the user switches apps, obscures the app screen. Default value is **On**.

When using the Android Near Field Communication (NFC) feature, some apps take a screenshot of itself before beaming the content. To enable that feature in a wrapped app, change the **Block screen capture** policy to **Off**.

Block device sensor

If **On**, prevents an app from using the device sensors (such as accelerometer, motion sensor, and gyroscope). Default value is **On**.

Block NFC

If **On**, prevents an app from using the Near Field Communications (NFC). Default value is **On**.

Block app logs

If **On**, prohibits an app from using the mobile productivity app diagnostic logging facility. If **Off**, app logs are recorded and might be collected by using the Secure Hub email support feature. Default value is **Off**.

Block printing

If **On**, prevents an app from printing data. If an app has a Share command, you must set Document Exchange (Open in) to **Restricted** or **Blocked** to block printing fully. Default value is **ON**.

Enable ShareFile

Allows users to use ShareFile to transfer files. Default value is **ON**.

App Network Access

Network access

NOTE:

Tunneled - Web SSO is the name for the **Secure Browse** in the settings. The behavior is the same.

The settings options are as follows:

- **Use Previous Settings:** Defaults to the values you had set in the earlier policies. If you change this option, you must not revert to this option. Also note that changes to the new policies do not take effect until the user upgrades the app to version 18.12.0 or later.
- **Blocked:** Networking APIs used by your app fails. Per the previous guideline, you must gracefully handle such a failure.
- **Unrestricted:** All network calls go directly and are not tunneled.
- **Tunneled - Full VPN:** All traffic from the managed app tunnels through Citrix Gateway.
- **Tunneled - Web SSO:** The HTTP/HTTPS URL is rewritten. This option allows only the tunneling of HTTP and HTTPS traffic. A significant advantage of **Tunneled - Web SSO** is single sign-on (SSO) for HTTP and HTTPS traffic and also PKINIT authentication. On Android, this option has low setup overhead and is thus the preferred option for web browsing types of operations.

If one of the **Tunneled modes** is selected, a per-app VPN tunnel in this initial mode is created back to the enterprise network. Here, Citrix Gateway split tunnel settings are used. Citrix recommends **Tunneled Full VPN** for connections that employ client certificates or end-to-end SSL to a resource in the enterprise network. Citrix recommends **Tunneled - Web SSO** for connections that require single sign-on (SSO).

Micro VPN session required

If **Yes**, the user must have a connection to the enterprise network and an active session. If **No**, an active session is not required. Default value is **Use Previous Setting**. For newly uploaded apps,

the default value is **No**. Whichever setting was selected before the upgrade to this policy remains in effect until an option other than **Use Previous Setting** is selected.

Exclusion List

Comma-delimited list of FQDNs or DNS suffixes to be accessed directly instead of through a VPN connection. This policy only applies to the **Tunneled - Web SSO** mode when Citrix Gateway is configured with Split tunnel reverse mode.

Block localhost connections

If **On**, apps are not permitted to make localhost connections. Localhost is an address (such as 127.0.0.1) for communications occurring locally on the device. The localhost bypasses the local network interface hardware and accesses network services running on the host. If **Off**, this policy overrides the Network Access policy, meaning that apps can connect outside the secure container if the device is running a proxy server locally. Default is **Off**.

Certificate label

When used with the StoreFront™ certificate integration service, this label identifies the specific certificate required for this app. If no label is provided, a certificate is not made available for use with a public key infrastructure (PKI). Default value is empty (no certificate used).

App Logs

Default log output

Determines which output mediums are used by Citrix Endpoint Management app diagnostic logging facilities by default. Possibilities are file, console, or both. Default value is file.

Default log level

Controls the default verbosity of the mobile productivity app diagnostic logging facility. Higher-level numbers include more detailed logging.

- 0 - Nothing logged
- 1 - Critical errors
- 2 - Errors
- 3 - Warnings
- 4 - Informational messages
- 5 - Detailed informational messages

- 6 through 15 - Debug levels 1 through 10

Default value is level **4** (Informational messages).

Max log files

Limits the number of log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is **2**. Maximum is **8**. The default value is **2**.

Max log file size

Limits the size in MB of the log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is **1** MB. Maximum is **5** MB. The default value is **2** MB.

Redirect app logs

If **On**, intercepts and redirects system or console logs from an app to the mobile productivity app diagnostic facility. If this setting is **Off**, app use of system or console logs is not intercepted. The default value is **On**.

Encrypt logs

If **On**, Citrix Endpoint Management encrypts diagnostic logs as it records the logs. If **Off**, diagnostic logs remain unencrypted in the app sandbox.

CAUTION:

Depending upon configured log levels, log encryption can have a noticeable impact on app performance and battery life.

Default value is **Off**.

App Geofence

Center point longitude

Longitude (X coordinate) of the center point of the point/radius geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked. The value must be expressed in signed degrees format (DDD.dddd), for example "-31.9635". West longitudes must be prefaced with a minus sign. Default value is **0**.

Center point latitude

Latitude (Y coordinate) of the center point of the point/radius geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked.

The values must be expressed in signed degrees format (DDD.dddd), for example "43.06581". Southern latitudes must be prefaced with a minus sign. Default value is **0**.

Radius

The radius of the geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked. The value must be expressed in meters. When set to zero, the geofence is disabled. Default is 0 (disabled).

Analytics

Google Analytics of detail

Citrix collects analytics data to improve product quality. Selecting Anonymous opts you out of including company identifiable information.

App Settings

Secure Mail Exchange Server

The fully qualified domain name (FQDN) for Exchange Server or, for iOS only, IBM Notes Traveler server. Default value is empty. If you provide a domain name in this field, users cannot edit it. If you leave the field empty, users provide their own server information.

CAUTION:

If you change this policy for an existing app, users must delete and reinstall the app to apply the policy change.

Secure Mail user domain

Default Active Directory domain name for Exchange users or, for iOS only, Notes users. Default value is empty.

Background network services

The FQDN and port of service addresses permitted for background network access. This value might be an Exchange Server or ActiveSync server, either in your internal network or in another network that Secure Mail connects to, such as mail.example.com:443.

If you configure this policy, set the Network access policy to **Tunneled to the internal network**. This policy takes effect when you configure the network access policy. Use this policy when the Exchange Server resides in your internal network and you want to use NetScaler Gateway to proxy the connection to the internal Exchange Server.

Default value is empty, implying that background network services are not available.

Background services ticket expiration

Time period for which a background network service ticket remains valid. After expiration, an enterprise logon will be required to renew the ticket. Default value is **168 hours** (7 days).

Background network service gateway

Alternate gateway address to use for background network services, in the form FQDN:port. This address is the Citrix Gateway FQDN and port number which Secure Mail uses to connect to the internal Exchange Server. In the Citrix Gateway configuration utility, you must configure the Secure Ticket Authority (STA) and bind the policy to the virtual server.

Default value is empty, implying that an alternate gateway does not exist.

If you configure this policy, set the Network access policy to **Tunneled to the internal network**. This policy takes effect when you configure the network access policy. Use this policy when the Exchange Server resides in your internal network and you want to use Citrix Gateway to proxy the connection to the internal Exchange Server.

Export contacts

IMPORTANT:

Do not enable this feature if users can access your Exchange Server directly (that is, outside of Citrix Gateway). Otherwise, contacts are duplicated on the device and in Exchange.

If **Off**, prevents the one-way sync of Secure Mail contacts to the device and prevents the sharing of Secure Mail contacts (as vCards). The default value is **Off**.

Contact fields to export

Controls contact fields to be exported to the address book. If **All**, all contact fields are exported. If **Name and Phone**, all name- and phone-related contact fields are exported. If **Name, Phone and Email**, all name-, phone- and email-related contact fields are exported. The default value is **All**.

Accept all SSL certificates

If **On**, Secure Mail accepts all SSL certificates (valid or not) and allows access. If **Off**, Secure Mail blocks access when a certificate error occurs and displays a warning. Default value is **Off**.

Use secure connection

If **On**, Secure Mail uses a Secured Connection. If **Off**, Secure Mail does not use a Secure Connection. Default is **On**.

Information Rights Management

If **On**, Secure Mail supports Exchange Information Rights Management (IRM) capabilities. Default value is **Off**.

Control locked screen notifications

Controls whether mail and calendar notifications appear on a locked device screen. If **Allow** is selected, all information contained in the notification appears. If **Block** is selected, notifications do not appear. If **Email sender or event title** is selected, only the name of the email sender or the title of the calendar event appears. If **Count only** is selected, only the count of mail and meeting invitations plus the time of calendar reminders appear. Default value is **Allow**.

Default sync interval

Specifies the default sync interval for Secure Mail. Secure Mail users can change the default.

The **Exchange ActiveSync mailbox** policy setting **Maximum email age filter** has priority over this policy. If you specify a Default sync interval that is larger than the maximum email age filter, the **Maximum email age** filter setting is used instead. Secure Mail displays only the sync interval values that are less than the **Active Sync Maximum email age** filter setting.

Default value is **3 days**.

Enable download of attachments over Wi-Fi

If **On**, the Secure Mail Download attachments option is enabled so that users can, by default, download attachments over internal Wi-Fi networks. If **Off**, the Secure Mail Download attachments

option is disabled so that, by default, users cannot download attachments over Wi-Fi. Default value is **Off**.

Allow offline documents

Specifies whether, and for how long, users can store offline documents on devices. Default value is **Unlimited**.

Enable auto-save of email drafts

If **On**, Secure Mail supports automatically saving messages to the **Drafts** folder. Default value is **On**.

Initial authentication Mechanism

This policy indicates whether the mail server address provided by MDX is used to populate the **Address** field on the first time use provisioning screen or the user email address is used. Default value is **Mail Server address**.

Initial authentication credentials

This policy defines the value that must be chosen as the user name to populate into the initial first time use provisioning screen. Default value is **Enrollment user name**.

Enable week number

If **On**, calendar views include the week number. Default value is **Off**.

Email classification

If **On**, Secure Mail supports email classification markings for SEC (security) and DLM (dissemination limiting markers). Classification markings appear in email headers as **X-Protective-Marking values**. Be sure to configure the related email classification policies. Default value is **Off**.

Email classification markings

Specifies the classification markings to be made available to end users. If the list is empty, Secure Mail does not include a list of protective markings. The markings list contains value pairs that are separated by semicolons. Each pair includes the value that appears in Secure Mail and the marking value that is the text appended to the email subject and header in Secure Mail. For example, in the marking pair `"UNOFFICIAL, SEC=UNOFFICIAL; "`, the list value is **"UNOFFICIAL"** and the marking value is **"SEC=UNOFFICIAL"**.

Email classification namespace

Specifies the classification namespace that is required in the email header by the classification standard used. For example, the namespace "gov.au" appears in the header as "NS=gov.au". Default value is empty.

Email classification version

Specifies the classification version that is required in the email header by the classification standard used. For example, the version "2012.3" appears in the header as "VER=2012.3". Default value is empty.

Default email classification

Specifies the protective marking that Secure Mail applies to an email if a user does not choose a marking. This value must be in the list for the Email classification markings policy. Default value is **UNOFFICIAL**.

Mail Search Limit

Restricts the amount of mail history that is accessible from mobile devices by limiting the number of days included in mail server searches. To restrict the amount of mail that is synced to a mobile device, configure the Max sync interval policy. Default value is **Unlimited**.

Max sync interval

Controls the amount of mail stored locally on a mobile device by limiting the sync period.

To restrict the time period that a device can search on the mail server, configure the Mail server search limit policy.

The values are:

- 3 days
- 1 week
- 2 weeks
- 1 month
- All

Default value is **All**.

Calendar Web and Audio Options

- **GoToMeeting and User Entered** - When this option is chosen, users are able to choose the type of conference they would like to set up. Options include GoToMeeting, which opens a GoToMeeting page, and Other Conference, which allows users to enter meeting information manually.
- **User Entered Only** - When this option is chosen, users are taken directly to the Other Conference page where they can enter meeting information manually.

S/MIME Public Certificate Source

Specifies the source of S/MIME public certificates. If **Exchange**, Secure Mail fetches certificates from Exchange Server. If **LDAP**, Secure Mail fetches certificates from the LDAP server. Default value is **Exchange**.

LDAP Server Address

LDAP server address including port number. Default value is empty.

LDAP Base DN

LDAP Base distinguished name. Default value is empty.

Access LDAP Anonymously

If this policy is **On**, Secure Mail can search LDAP without prior authentication. Default is **Off**.

Allowed Email Domains

Define a list of allowed email domains in a comma-separated format such as server.company.com,server.company.co.uk. The default value is empty, which implies that Secure Mail does not filter email domains and supports all email domains. Secure Mail matches the listed domains with the domain name in the email address.

For instance, when server.company.com is a listed domain name and the email address is user@internal.server.company.com, Secure Mail supports the email address.

Push notifications

Enables FCM based notifications about mailbox activity. If **On**, Secure Mail supports push notifications. Default value is **Off**.

Push notifications EWS host name

The server that hosts Exchange Web Services (EWS) for mail. The value must be the URL of EWS, along with the port number. Default value is empty.

Push notifications region

The region where the FCM host is located for your Secure Mail users. Options are Americas, EMEA, and PAC. Default value is Americas.

Attempt user name Migration On Authentication Failure

This policy attempts to migrate the Exchange user name to a UPN for authentication. The default value is **Off**.

Report Phishing Mail Addresses

If configured, you can report suspected phishing mails to a given email address or a list of comma-separated email addresses. The default value is empty. If you do not configure this policy, you cannot report phishing messages.

Report Phishing Mechanism

This policy indicates the mechanism used to report suspected phishing mails.

- Report via attachment (.eml) – Report phishing mails as an attachment. The attachment is sent to an email address or a list of comma-separated email addresses configured in the Report Phishing Mail Addresses policy.
- Report via forward – Report phishing mails as a forward. The mail is forwarded to an email address or a list of comma-separated email addresses configured in the Report Phishing Mail Addresses policy.

NOTE:

This policy is available only for Microsoft Exchange server.

Default is Report via attachment (.eml).

Skype for Business Meeting Domains

This policy contains a comma-separated list of domains used for Skype for Business meetings. Secure Mail already handles meetings with URL prefix as the following:

- `https://join`

- `https://meet`
- `https://lync`

With this policy, other Skype for Business domains can be added in the form `https://*domain*`. The domain can be a string of alphanumeric characters and cannot contain any special characters. Do not enter the preceding `https://` or the succeeding dot.

Example

If the policy value is `customDomain1,customDomain2`, the supported URL prefixes for Skype for Business would be: `https://customDomain1` `http://customDomain1` `https://customDomain2` `http://customDomain2`

Default value is empty.

Export Calendar

This policy allows Secure Mail calendar events to be exported to your device or personal calendar. You can view your events in your personal calendar. You can edit the events using Secure Mail. Default value is **Meeting Time**.

The following MDX policy values are available for the calendar event fields that appear in your personal calendar:

- None (Don't Export)
- Meeting Time
- Meeting Time, Location
- Meeting Time, Subject, Location
- Meeting Time, Availability, Attendees, Subject, Location, Notes

OAuth Support for Office 365

Use Modern authentication for O365

If this policy is **On**, Secure Mail uses the OAuth protocol for authentication while configuring an account on Office 365. If **Off**, Secure Mail uses Basic authentication. Default is **Off**.

Trusted Exchange Online Hostnames

Define a list of trusted Exchange Online host names that use the OAuth mechanism for authentication while configuring an account. This value is a comma-separated format such as

server.company.com, server.company.co.uk. If the list is empty, then Secure Mail uses Basic authentication for account configuration. Default value is outlook.office365.com.

Trusted AD FS Hostnames

Define a list of trusted AD FS host names for webpages where the password populates during Office 365 OAuth authentication. This value is a comma-separated format, such as

`sts.companyname.com` , `sts.company.co.uk` . If the list is empty, then Secure Mail does not auto populate passwords. Secure Mail matches the listed host names with the host name of the webpage encountered during Office 365 authentication and checks if the page uses the HTTPS protocol.

For instance, when sts.company.com is a listed host name and if the user navigates to `https://sts.company.com` , Secure Mail populates the password if the page has a password field. Default value is `login.microsoftonline.com` .

Custom user agent for modern authentication

This policy allows you to change the default user agent string for modern authentication. If configured, this user agent string is used for authentication with Microsoft AD FS. If you do not configure this policy, the default Secure Mail user agent is used during modern authentication.

Slack Integration

Enable Slack

Blocks or permits Slack integration. If **On**, the Secure Mail interface includes Slack features. If **Off**, the Secure Mail interface doesn't include Slack features.

Slack workspace name

The Slack workspace name for your company. If you provide a name, Secure Mail pre-fills the workspace name during sign-on. If you don't provide a name, users must type the workspace name (name.slack.com).

MDX policies for mobile productivity apps for iOS

This article describes the MDX policies for iOS apps. You change policy settings in the Citrix Endpoint Management console. For details, see [Add apps](#).

The following list does not include MDX policies specific to Secure Web. For details about the policies that appear for Secure Web, see [Secure Web policies](#).

Authentication

Device passcode

If **On**, a PIN or passcode is required to unlock the device when it starts or resumes after a period of inactivity. A device passcode is required to encrypt app data using Apple file encryption. Data for all apps on the device are encrypted. Default value is **Off**.

App passcode

If **On**, a PIN or passcode is required to unlock the app when it starts or resumes after a period of inactivity. Default value is **On**.

To configure the inactivity timer for all apps, set the **INACTIVITY_TIMER** value in minutes in **Client Properties** on the **Settings** tab. The default inactivity timer value is **60** minutes. To disable the inactivity timer, so that a PIN or passcode prompt appears only when the app starts, set the value to zero.

NOTE:

If you select **Secure offline** for the Encryption keys policy, this policy is automatically enabled.

Maximum offline period (hours)

Defines the maximum period an app can run without reconfirming app entitlement and refreshing policies from Citrix Endpoint Management. At expiration, log on to the server might be triggered if needed. Default value is **168** hours (7 days). The minimum period is **1** hour.

Alternate Citrix Gateway

NOTE:

This policy name in the Endpoint Management console is **Alternate NetScaler® Gateway**.

Address of a specific alternate Citrix Gateway that must be used for authentication and for micro VPN sessions with this app. This policy is optional. When used with the Online session required policy, the policy forces apps to reauthenticate to the specific gateway. Such gateways would typically have different (higher assurance) authentication requirements and traffic management policies. If left empty, the server's default gateway is always used. Default value is empty.

Device security

Block jailbroken or rooted

If **On**, the app is locked when the device is jailbroken or rooted. If **Off**, the app can run even if the device is jailbroken or rooted. Default value is **On**.

Network requirements

Require Wi-Fi

If **On**, the app is locked when the device is not connected to a Wi-Fi network. If **Off**, the app can run if the device has an active connection, such as a 4G/3G, LAN, or Wi-Fi connection. Default value is **Off**.

Allowed Wi-Fi networks

Comma-delimited list of Wi-Fi networks. If the network name contains any non-alphanumeric characters (including commas), the name must be enclosed in double-quotes. The app runs only if connected to one of the networks listed. If blank, all networks are allowed. This value does not affect connections to cellular networks. Default value is blank.

Miscellaneous access

Disable required upgrade

Disables the requirement that users upgrade to the newest version of the app in the App Store. Default value is **On**.

App update grace period (hours)

Defines the grace period that an app can continue to be used after the system has discovered that an app update is available. Default value is **168 hours (7 days)**.

NOTE:

We recommend that you do not use a value of zero. A zero value immediately prevents a running app from being used until the update is downloaded and installed (without any warning to the user). Using this value might lead to a situation where the user is forced to exit the app (potentially losing work) to comply with the required update.

Erase app data on lock

Erases data and resets the app when the app is locked. If **Off**, app data is not erased when the app is locked. Default value is **Off**.

An app can be locked for any of the following reasons:

- Loss of app entitlement for the user
- App subscription removed
- Account removed
- Secure Hub uninstalled
- Too many app authentication failures
- Jailbroken device detected (per policy setting)
- Device placed in locked state by other administrative action

Active poll period (minutes)

When an app starts, the MDX Framework polls Citrix Endpoint Management to determine current app and device status. Assuming the server running Endpoint Management can be reached, the framework returns information about the lock/erase status of the device and the enable/disable status of the app. Whether the server can be reached or not, a subsequent poll is scheduled based on the active poll period interval. After the period expires, a new poll is again attempted. Default value is **60 minutes** (1 hour).

IMPORTANT:

Only set this value lower for high-risk apps or performance might be affected.

Encryption

Encryption type

Allows you to choose whether MDX or the device platform handles the encryption of data. If you select **MDX encryption**, then MDX encrypts the data. If you select **Platform encryption with compliance enforcement**, then the device platform encrypts the data. Default value is **MDX encryption**.

Non-compliant device behavior

Allows you to choose an action when a device does not adhere to the minimum compliance requirements of encryption. Select **Allow app** for the app to run normally. Select **Allow app after warning** for the app to run after the warning appears. Select **Block** to block the app from running. Default value is **Allow app after warning**.

Enable MDX encryption

If **Off**, the data stored on the device is not encrypted. If **On**, the data stored on the device is encrypted. Default value is **On**.

CAUTION:

If you change this policy after deploying an app, users must reinstall the app.

Database encryption exclusions

Exclusion list of databases that are not automatically encrypted. To prevent database encryption for a specific database, add an entry to this comma-separated list of regular expressions. If a database path name matches any of the regular expressions, the database is excluded from encryption. The exclusion patterns support Posix 1003.2 Extended Regular Expressions syntax. The pattern matching is case-insensitive.

Examples

`\\.db$,\\.sqlite$` excludes any database path name that ends with either `.db` or `.sqlite`.

`\\Database\\unencrypteddb\\.db` matches database `unencrypteddb.db` in the Database subfolder.

`\\Database\\` matches all databases that contain `/Database/` in its path.

Default value is empty.

File encryption exclusions

Exclusion list of files that are not automatically encrypted. To prevent encryption for a specific set of files, add an entry to this comma-separated list of regular expressions. If a file path name matches any of the regular expressions, then that file is excluded from encryption. The exclusion patterns support Posix 1003.2 Extended Regular Expressions syntax. The pattern matching is case-insensitive.

Examples

`\\.log$,\\.dat$` excludes any file path name that ends with either `.log` or `.dat`.

`\\Documents\\unencrypteddoc\\.txt` matches the contents of the file `unencrypteddoc.txt` in the Documents subfolder.

`\\Documents\\UnencryptedDocs\\.*\\.txt` matches ".txt" files under the subpath /Documents/UnencryptedDocs/.

Default value is empty.

App interaction

Cut and copy

Blocks, permits, or restricts Clipboard cut and copy operations for this app. If **Restricted**, the copied Clipboard data is placed in a private Clipboard that is only available to MDX apps. Default value is **Restricted**.

Paste

Blocks, permits, or restricts Clipboard paste operations for this app. If **Restricted**, the pasted Clipboard data is sourced from a private Clipboard that is only available to MDX apps. Default value is **Unrestricted**.

Document exchange (Open In)

Blocks, permits, or restricts document exchange operations for this app. If **Restricted**, documents can be exchanged only with other MDX apps.

If **Unrestricted**, set the Enable encryption policy to **On** so that users can open documents in unwrapped apps. If the receiving app is unwrapped or has encryption disabled, Citrix Endpoint Management decrypts the document. Default value is **Restricted**.

Restricted Open-In exception list

When the Document exchange (Open In) policy is **Restricted**, an MDX app can share documents with this comma-delimited list of unmanaged app IDs. This is true even if the Document exchange(Open In) policy is **Restricted** and Enable encryption is **On**. The default exception list allows Office 365 apps:

com.microsoft.Office.Word,com.microsoft.Office.Excel,com.microsoft.Office.Powerpoint,
com.microsoft.onenote,com.microsoft.onenoteiPad,com.microsoft.Office.Outlook

Only Office 365 apps are supported for this policy.

CAUTION:

Be sure to consider the security implications of this policy. The exception list allows content to travel between unmanaged apps and the MDX environment.

Connection security level

Determines the minimum version of TLS/SSL used for connections. If **TLS**, connections support all TLS protocols. If **SSLv3 and TLS**, connections support SSL 3.0 and TLS. Default value is **TLS**.

Inbound document exchange (Open In)

Blocks, restricts, or allows inbound document exchange operations for this app. If **Restricted**, documents can be exchanged only with other MDX apps. Default value is **Unrestricted**.

If **Blocked** or **Restricted**, you can use the Inbound document exchange whitelist policy to specify apps that can send documents to this app.

Options: **Unrestricted**, **Blocked**, or **Restricted**

App URL schemes

iOS apps can dispatch URL requests to other apps that have been registered to handle specific schemes (such as "`http://`"). This facility provides a mechanism for an app to pass requests for help to another app. This policy serves to filter the schemes that are passed into this app for handling (that is, inbound URLs). Default value is empty, meaning that all registered app URL schemes are blocked.

The policy must be formatted as a comma-separated list of patterns where a plus "+" or minus "-" precedes each pattern. Inbound URLs are compared against the patterns in the order listed until a match is found. Once matched, the prefix dictates the action taken.

- A minus "-" prefix blocks the URL from being passed into this app.
- A plus "+" prefix permits the URL to be passed into the app for handling.
- If neither "+" or "-" is provided with the pattern, "+" (allow) is assumed.
- If an inbound URL does not match any pattern in the list, the URL is blocked.

The following table contains examples of App URL schemes:

SCHEME	APP THAT REQUIRES THE URL SCHEME	PURPOSE
<code>ctxmobilebrowser</code>	Secure Web-	Permit Secure Web to handle HTTP: URLs from other apps.-
<code>ctxmobilebrowsers</code>	Secure Web-	Permit Secure Web to handle HTTPS: URLs from other apps.
<code>ctxmail</code>	Secure Mail-	Permit Secure Mail to handle <code>mailto:</code> URLs from other apps.
COL-G2M	GoToMeeting-	Permit a wrapped GoToMeeting app to handle meeting requests.
<code>ctxsalesforce</code>	Citrix for Salesforce -	Permit Citrix for Salesforce to handle Salesforce requests.
<code>wbx</code>	WebEx	Permit a wrapped WebEx app to handle meeting requests.

App interaction (outbound URL)

Domains excluded from URL filtering

This policy excludes outbound URLs from any "Allowed URLs" filtering. Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes to exclude from the "Allowed URLs" filtering. If this policy is empty (the default), the defined "Allowed URLs" filtering processes are URLs. If this policy contains any entries, URLs with host fields matching at least one item in the list (via DNS suffix match) are sent unaltered to iOS. This communication bypasses the "Allowed URLs" filtering logic. Default value is empty.

Allowed URLs

iOS apps can dispatch URL requests to other applications that have been registered to handle specific schemes (such as `"http://"`). This facility provides a mechanism for an app to pass requests for help to another app. This policy serves to filter the URLs that are passed from this app to other apps for handling (that is, outbound URLs).

The policy must be formatted as a comma-separated list of patterns in which each pattern might be preceded by a plus "+" or minus "-". Outbound URLs are compared against the patterns in the order listed until a match is found. Once matched, the prefix decides the action taken. A minus "-" prefix blocks the URL from being passed out to another app. A plus "+" prefix permits the URL to be passed out to another app for handling. If neither "+" or minus "-" is provided with the pattern, "+" (allow) is assumed. A pair of values separated by "=" indicates a substitution where occurrences of the first string are replaced with the second. You can use regular-expression "\^" prefix to search the string to anchor it to the beginning of the URL. If an outbound URL does not match any pattern in the list, it is blocked.

Default`+maps.apple.com``+itunes.apple.com``\^http:=ctxmobilebrowser:``\^https:=ctxmobilebrowsers:``\^mailto:=ctxmail:``+\\^citrixreceiver:``+\\^telprompt:``+\\^tel:``+\\^lmi-g2m:``+\\^maps:ios_addr``+\\^mapitem:``+\\^sms:``+\\^facetime:``+\\^ctxnotes:``+\\^ctxnotesex:``+\\^ctxtasks:``+\\^facetime-audio:`

`+\\^itms-apps:``+\\^ctx-sf:``+\\^sharefile:``+\\^lync:``+\\^slack:``+\\^msteams:`

If the setting is blank, all URLs are blocked, except for the following:

- `http:`
- `https:`
- `+citrixreceiver: +tel:`

The following table contains examples of allowed URLs:

URL FORMAT	DESCRIPTION
<code>\\^mailto:=ctxmail:</code>	All <code>mailto:</code> URLs open in Secure Mail.
<code>\\^http:</code>	All HTTP URLs open in Secure Web.
<code>\\^https:</code>	All HTTPS URLs open in Secure Web.
<code>\\^tel:</code>	Allows user to make calls.
<code>-//www.dropbox.com</code>	Blocks Dropbox URLs dispatched from managed apps.
<code>+\\^COL-G2M:</code>	Permits managed apps to open the GoToMeeting client app.
<code>-\\^SMS:</code>	Blocks the use of a messaging chat client.
<code>-\\^wbx:</code>	Blocks managed apps from opening the WebEx client app.
<code>+\\^ctxsalesforce:</code>	Permits Citrix for Salesforce to communicate with your Salesforce server.

Allowed Secure Web domains

This policy only affects "Allowed URLs" policy entries that would redirect a URL to the Secure Web app (`\^ http:=ctxmobilebrowser:` and `\^https:=ctxmobilebrowsers:`). Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes allowed to redirect to the Secure Web app. If this policy is empty (the default), all domains can redirect to the Secure Web app. If this policy contains any entries, then only those URLs with host fields matching at least one item in the list (via DNS suffix match) redirect to the Secure Web app. All other URLs are sent unaltered to iOS, bypassing the Secure Web app. Default value is empty.

App Restrictions

Important:

Be sure to consider the security implications of policies that block apps from accessing or using phone features. When those policies are **Off**, content can travel between unmanaged apps and the Secure environment.

Block camera

If **On**, prevents an app from directly using the camera hardware. Default value is **OFF**.

Block Photo Library

If **On**, prevents an app from accessing the Photo Library on the device. Default value is **On**.

Block mic record

If **On**, prevents an app from directly using the microphone hardware. Default value is **On**.

Block dictation

If **On**, prevents an app from directly using dictation services. Default value is **On**.

Block location services

If **On**, prevents an app from using the location services components (GPS or network). Default value is **Off** for Secure Mail.

Block SMS compose

If **On**, prevents an app from using the SMS compose feature used to send SMS/text messages from the app. Default value is **On**.

Block email compose

If **On**, prevents an app from using the email compose feature used to send email messages from the app. Default value is **On**.

Block iCloud

If **On**, prevents an app from using iCloud for the storing and sharing of settings and data.

NOTE

iCloud data file is controlled by the Block file backup policy.

Default value is **On**.

Block lookup

If **On**, prevents an app from using the Lookup feature, which searches for highlighted text in the Dictionary, iTunes, the App Store, movie showtimes, nearby locations and more. Default value is **On**.

Block file backup

If **On**, prevents iCloud or iTunes from backing up data files. Default value is **On**.

Block AirPrint

If **On**, prevents an app from using AirPrint features for printing data to AirPrint-enabled printers. Default value is **On**.

Block AirDrop

If **On**, prevents an app from using AirDrop. Default value is **On**.

Block file attachments

NOTE

This policy is enforced on iOS 11 or later.

If **On**, attachment handling is disabled. Default value is **Off**.

Block Facebook and Twitter APIs

If **On**, prevents an app from using the iOS Facebook and Twitter APIs. Default value is **On**.

Obscure screen contents

If **On**, when users switch apps, the screen is obscured. This policy prevents iOS from recording screen contents and displaying thumbnails. Default value is **On**.

Block 3rd party keyboards (iOS 11 and later only)

If **On**, prevents an app from using third-party keyboard extensions on iOS 8+. Default value is **On**.

Block app logs

If **On**, prohibits an app from using the mobile productivity app diagnostic logging facility. If **Off**, app logs are recorded and might be collected by using the Secure Hub email support feature. Default value is **Off**.

Enable ShareFile

Allows users to use ShareFile to transfer files. Default value is **On**.

Enable Attach From Files

Allows users to add attachments from the iOS Files app. Default value is **On**.

App network access

Network access

NOTE:

Tunneled - Web SSO is the name for the **Secure Browse** in the settings. The behavior is the same.

The settings options are as follows:

- **Blocked**: All network access is blocked. Networking APIs used by your app fails. Per the previous guideline, you must gracefully handle such a failure.
- **Unrestricted**: All network calls go directly and are not tunneled.
- **Tunneled - Web SSO**: The HTTP/HTTPS URL is rewritten. This option allows only the tunneling of HTTP and HTTPS traffic. A significant advantage of **Tunneled - Web SSO** is single

sign-on (SSO) for HTTP and HTTPS traffic and also PKINIT authentication. On Android, this option has low setup overhead and is thus the preferred option for web browsing types of operations.

If you're using the **Tunneled - Full VPN** or the **Tunneled - Full VPN and Web SSO** policies, then you must switch to the **Tunneled - Web SSO** policy. Your emails fail to sync if you continue to use the deprecated policies.

NOTE:

If you are using **Tunneled - Full VPN** and Secure Ticket Authority (STA) is configured, then the modern authentication screen fails to load.

Micro VPN session required

If **Yes**, the user must have a connection to the enterprise network and an active session. If **No**, an active session is not required. Default value is **Use Previous Setting**. For newly uploaded apps, the default value is **No**. Whichever setting was selected before the upgrade to this new policy remains in effect until an option other than **Use Previous Setting** is selected.

Micro VPN session required grace period (minutes)

This value determines how many minutes users can use the app before the Online Session Required policy prevents them from further use (until the online session is validated). Default value is **0** (no grace period). This policy isn't applicable for integration with Microsoft Intune/EMS.

Certificate label

When used with the StoreFront™ certificate integration service, this label identifies the specific certificate required for this app. If no label is provided, a certificate is not made available for use with a public key infrastructure (PKI). Default value is empty (no certificate used).

Exclusion List

Comma-delimited list of FQDNs or DNS suffixes to be accessed directly instead of through a VPN connection. This value only applies to the **Tunneled - Web SSO** mode when Citrix Gateway is configured with Split tunnel reverse mode.

App logs

Default log output

Determines which output media are used by mobile productivity app diagnostic logging facilities by default. Possibilities are file, console, or both. Default value is **file**.

Default log level

Controls default verbosity of the mobile productivity app diagnostic logging facility. Each level includes levels of lesser values. Range of possible levels includes:

- 0 - Nothing logged
- 1 - Critical errors
- 2 - Errors
- 3 - Warnings
- 4 - Informational messages
- 5 - Detailed informational messages
- 6 through 15 - Debug levels 1 through 10

Default value is level 4 (Informational messages).

Max log files

Limits the number of log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is 2. Maximum is 8. Default value is 2.

Max log file size

Limits the size in MB of the log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is 1 MB. Maximum is 5 MB. Default value is 2 MB.

App geofence

Center point longitude

Longitude (X coordinate) of the center point of point/radius geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked.

The value must be expressed in signed degrees format (DDD.dddd), for example "-31.9635". West longitudes must be prefaced with a minus sign. Default value is **0**.

Center point latitude

Latitude (Y coordinate) of the center point of point/radius geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked.

The value must be expressed in signed degree format (DDD.dddd), for example "43.06581". Southern latitudes must be prefaced with a minus sign. Default value is **0**.

Radius

The radius of the geofence in which the app is constrained to operate. When operated outside the configured geofence, the app remains locked.

The value must be expressed in meters. When set to zero, the geofence is disabled. When the Block location serviced policy is enabled, geofencing does not work properly. Default is **0** (disabled).

Enable Google Analytics

If **On**, Citrix collects anonymous data to improve product quality. If **Off**, no data is collected. Default value is **On**.

Analytics

Google Analytics level of detail

Citrix collects analytics data to improve product quality. Selecting **Anonymous** opts users out of including company identifiable information. Default is Complete.

Reporting

Citrix reporting

If **On**, Citrix collects crash reports and diagnostics to help troubleshoot issues. If **Off**, Citrix doesn't collect data.

NOTE

Citrix might also control this feature with a feature flag. Both the feature flag and this policy must be enabled for this feature to function.

Default value is **Off**.

Upload token

You can obtain an upload token from your Citrix Insight Services (CIS) account. If you specify this optional token, CIS gives you access to crash reports and diagnostics uploaded from your devices. Citrix has access to that same information. Default value is empty.

Send reports over Wi-Fi only

If **On**, Citrix sends crash reports and diagnostics only when you're connected to a Wi-Fi network. Default value is **On**.

Report file cache maximum

Limits the size of the crash report and diagnostics bundles retained before clearing the cache. Minimum is 1 MB. Maximum is 5 MB. Default value is 2 MB.

App interaction

Explicit logoff notification

If **Disabled**, the app is not activated during a user logoff. If **Shared devices only**, the app is activated during user logoff, only if the device is configured as a shared device. Default is **Shared devices only** for Secure Mail.

App settings

Secure Mail Exchange Server

The fully qualified domain name (FQDN) for Exchange Server or, for iOS only, IBM Notes Traveler server. Default value is empty. If you provide a domain name in this field, users cannot edit it. If you leave the field empty, users provide their own server information.

CAUTION

If you change this policy for an existing app, users must delete and reinstall the app to apply the policy change.

Secure Mail user domain

Default Active Directory domain name for Exchange users or, for iOS only, Notes users. Default value is empty.

Background network services

The FQDN and port of service addresses permitted for background network access. This value might be an Exchange Server or ActiveSync server, either in your internal network or in another network that Secure Mail connects to, such as mail.example.com:443.

If you configure this policy, set the Network access policy to **Tunneled to the internal network**. This policy takes affect when you configure the network access policy. Use this policy when the Exchange Server resides in your internal network and you want to use Citrix Gateway (formerly, NetScaler Gateway) to proxy the connection to the internal Exchange Server.

Default value is empty, implying that background network services are not available.

Background services ticket expiration

Time period for which a background network service ticket will be valid. After expiration, an enterprise logon will be required to renew the ticket. Default value is **168 hours** (7 days).

Background network service gateway

Alternate gateway address to use for background network services, in the form `fqdn:port`. This value is the Citrix Gateway FQDN and port number which Secure Mail uses to connect to the internal Exchange Server. In the Citrix Gateway configuration utility, you must configure the Secure Ticket Authority (STA) and bind the policy to the virtual server. Default value is empty, implying that an alternate gateway does not exist.

If you configure this policy, set the Network access policy to **Tunneled to the internal network**. This policy takes affect when you configure the network access policy. Use this policy when the Exchange Server resides in your internal network and you want to use Citrix Gateway to proxy the connection to the internal Exchange Server.

Export Contacts

Important:

Do not enable this feature if users can access your Exchange Server directly (that is, outside of Citrix Gateway). Otherwise, duplicate contacts are created on the device and in Exchange.

If **Off**, prevents the one-way sync of Secure Mail contacts to the device and sharing Secure Mail contacts (as vCards). Default value is **Off**.

Contact fields to export

Controls contact fields to be exported to the address book. If **All**, all contact fields are exported. If **Name and Phone**, all name- and phone-related contact fields are exported. If **Name, Phone and Email**, all name-, phone- and email-related contact fields are exported.

The default value is **All**.

Accept all SSL certificates

If **On**, Secure Mail accepts all SSL certificates (valid or not) and allows access. If **Off**, Secure Mail blocks access when a certificate error occurs and displays a warning.

Default value is **Off**.

Control locked screen notifications

Controls whether mail and calendar notifications appear on a locked device screen. If **Allow**, all information contained in the notification appears. If **Block**, notifications do not appear. If **Email sender or event title**, only the name of the email sender or the title of the calendar event appears. If **Count only**, the count of mail and meeting invitations plus the time of calendar reminders appear. The default value is **Allow**.

Default email notification

If **On**, Secure Mail shows the lock screen notification for emails. Default value is **On**.

Default sync interval

Specifies the default sync interval for Secure Mail. Secure Mail users can change the default. The **Exchange ActiveSync mailbox** policy setting **Maximum email age filter** has priority over this policy. If you specify a Default sync interval that is larger than the Maximum email age filter, the **Maximum email age filter** setting is used instead.

Secure Mail displays only the sync interval values that are less than the **Active Sync Maximum email age filter** setting.

Default value is **3 days**.

Mail search limit

Restricts the amount of mail history that is accessible from mobile devices by limiting the number of days included in mail server searches. Default value is **Unlimited**.

To restrict the amount of mail that is synced to a mobile device, configure the Maximum client sync period policy.

Max sync interval

Controls the amount of mail stored locally on a mobile device by limiting the sync period. Default value is **All**. To restrict the time period that a device can search on the mail server, configure the Mail server search limit policy.

Enable week number

If **On**, calendar views include the week number. Default value is **Off**.

Enable download of attachments over Wi-Fi

If **On**, the Secure Mail Download attachments option is enabled so that users can, by default, download attachments over allowed internal Wi-Fi networks. If **Off**, the Secure Mail Download attachments option is disabled so that, by default, users cannot download attachments over Wi-Fi.

Default value is **Off**.

Allow offline documents

Specifies whether, and for how long, users can store offline documents on devices. Default value is **Unlimited**.

Information Rights Management

If **On**, Secure Mail supports Exchange Information Rights Management (IRM) capabilities. Default value is **Off**.

Email classification

If **On**, Secure Mail supports email classification markings for SEC (security) and DLM (dissemination limiting markers). Classification markings appear in email headers as "X-Protective-Marking" values. Be sure to configure the related email classification policies.

Default value is **Off**.

Email classification markings

Specifies the classification markings to be made available to users. If the list is empty, Secure Mail does not include a list of protective markings. The markings list contains value pairs that are separated by semicolons. Each pair includes the value that appears in Secure Mail and the marking value that is the text appended to the email subject and header in Secure Mail. For

example, in the marking pair "UNOFFICIAL,SEC=UNOFFICIAL;", the list value is "UNOFFICIAL" and the marking value is "SEC=UNOFFICIAL".

Email classification namespace

Specifies the classification namespace that is required in the email header by the classification standard used. For example, the namespace "gov.au" appears in the header as "NS=gov.au".

Default value is empty.

Email classification version

Specifies the classification version that is required in the email header by the classification standard used. For example, the version "2012.3" appears in the header as "VER=2012.3".

Default value is empty.

Default email classification

Specifies the protective marking that Secure Mail applies to an email if a user does not choose a marking. This value must be in the list for the Email classification markings policy.

Default value is **UNOFFICIAL**.

Enable auto-save of email drafts

If **On**, Secure Mail supports automatically saving messages to the **Drafts** folder.

Default value is **On**.

Initial authentication mechanism

This policy indicates whether the mail server address as provided by MDX or the user's email address must be used to populate the "address" field on the first time use provisioning screen.

Default value is **"Mail server address"**.

Initial authentication credentials

This policy defines the value that must be chosen as the user name to populate into the initial first time use provisioning screen.

Default value is **"Enrollment user name"**.

Enable auto population of user name

If enabled, the user name is automatically populated in the account provisioning user interface. Default value is **ON**.

Enable iOS data protection

NOTE:

This policy is intended for enterprises which must meet Australian Signals Directorate (ASD) computer security requirements.

Enables iOS data protection when working with files. If **On**, specifies the file-protection level when creating and opening files in the app sandbox. Default value is **Off**.

Push Notifications EWS host name

The server that hosts Exchange Web Services (EWS) for mail. The value must be the URL of EWS, along with the port number. Default value is empty.

Push notifications

Enables APNs-based notifications about mailbox activity. If **On**, Secure Mail supports push notifications.

Default value is **Off**.

Push notifications region

The region where the APNs host is located for Secure Mail users. Options are **Americas**, **EMEA**, and **APAC**. Default value is **Americas**.

S/MIME public certificate source

Specifies the source of S/MIME certificates. If **Email**, you must email user certificates to users, who then open the email in Secure Mail and import the attached certificates.

If **Shared vault**, a supported digital identity provider supplies certificates to the Secure App shared vault. The integration with the third-party provider requires that you publish a related app to users. See the description for the Enable S/MIME during first Secure Mail startup policy for details about the user experience.

Default value is **Email**.

Enable S/MIME during first Secure Mail startup

Determines whether Secure Mail enables S/MIME during the first Secure Mail startup, if the S/MIME certificate source policy is **Shared vault**. If **On**, Secure Mail enables S/MIME if there are certificates for the user in the shared vault. If there are no certificates in the shared vault, the user is prompted to import the certificates. In both of those scenarios, users must configure certificates from a supported digital identity provider app before creating an account in Secure Mail.

If **Off**, Secure Mail does not enable S/MIME and the user can enable it in the Secure Mail settings. Default value is **Off**.

Calendar Web and Audio Options

- **GoToMeeting and User Entered:** Users can choose the type of conference they would like to set up. Options include **GoToMeeting**, which opens a GoToMeeting page, and **Other Conference**, which allows users to enter meeting information manually.
- **User Entered Only:** Users are taken directly to the Other Conference page where they can enter meeting information manually.

S/MIME public certificate source

Specifies the source of S/MIME public certificates. If **Exchange**, Secure Mail fetches certificates from Exchange Server. If **LDAP**, Secure Mail fetches certificates from the LDAP server. Default value is **Exchange**.

LDAP server address

LDAP server address including port number. Default value is empty.

LDAP Base DN

LDAP base distinguished name. Default value is empty.

Access LDAP Anonymously

If this policy is **On**, Secure Mail can search LDAP without prior authentication. Default is **Off**.

Allowed Email Domains

Defines a list of allowed email domains in a comma-separated format such as server.company.com,server.company.co.uk. The default value is empty, which implies that Secure Mail does not filter email domains and supports all email domains. Secure Mail matches the listed domains with the domain name in the email address. For instance, when server.company.com is a

listed domain name and the email address is user@internal.server.company.com, Secure Mail supports the email address.

Attempt user name Migration On Authentication Failure

Attempts to migrate the Exchange user name to a UPN for authentication. The default value is **Off**.

Report Phishing Mail Address

If configured, you can report suspected phishing mails to a given email address or a list of comma-separated email addresses. The default value is empty. If you do not configure this policy, you will not be able to report phishing messages.

Report Phishing Mechanism

This policy indicates the mechanism used to report suspected phishing mails.

- **Report via attachment:** Report phishing mails as an attachment. The attachment is sent to an email address or a list of comma-separated email addresses configured in the Report Phishing Mail Addresses policy.
- **Report via forward:** Report phishing mails as a forward. The mail is forwarded to an email address or a list of comma-separated email addresses configured in the Report Phishing Mail Addresses policy.

NOTE:

This policy is available only for Microsoft Exchange Server.

Default is **Report via attachment**.

Skype for Business Meeting Domains

This policy contains a comma-separated list of domains used for Skype for Business meetings.

Secure Mail already handles meetings with URL prefix as the following:

- `https://join`
- `https://meet`
- `https://lync`

With this policy, other Skype for Business domains can be added in the form `https://*domain*`. The domain can be a string of alphanumeric characters and cannot contain any special characters. Do not enter the preceding `https://` or the succeeding dot.

Example:

If the policy value is **customDomain1,customDomain2**, the supported URL prefixes for Skype for Business would be:

- `https://customDomain1`
- `http://customDomain1`
- `https://customDomain2`
- `http://customDomain2`

Default value is empty.

Export Calendar

This policy allows Secure Mail calendar events to be exported to your device or personal calendar. You can view your events in your personal calendar. You can edit the events using Secure Mail. Default value is **Meeting Time**.

The following MDX policy values are available for the calendar event fields that appear in your personal calendar:

- None (Don't Export)
- Meeting Time
- Meeting Time, Location
- Meeting Time, Subject, Location
- Meeting Time, Subject, Location, Notes

Caller Identification

If **On**, Secure Mail provides the name and contact number of your saved contacts to iOS for caller identification purposes. This data is only used to identify and display details of incoming calls from your saved Secure Mail contact list. The default value is **On**.

OAuth Support for Office 365

Office 365 authentication mechanism

This policy indicates the OAuth mechanism used for authentication while configuring an account on Office 365.

- **Do not use OAuth:** OAuth is not used and Secure Mail uses Basic authentication for account configuration.
- **Use OAuth with Username and Password:** The user must provide their user name and password, and optionally an MFA code for the OAuth flow.
- **Use OAuth with Client Certificate:** The user authenticates the OAuth flow using a client certificate.

Default is "**Do not use OAuth**".

Trusted Exchange Online host names

Defines a list of trusted Exchange Online host names that use the OAuth mechanism for authentication while configuring an account. This value is a comma-separated format, such as server.company.com, server.company.co.uk. If the list is empty, Secure Mail uses Basic authentication for account configuration. Default value is **outlook.office365.com**.

Trusted AD FS host names

Define a list of trusted AD FS host names for webpages where the password populates during Office 365 OAuth authentication. This value is a comma-separated format, such as sts.companyname.com, sts.company.co.uk. If the list is empty, Secure Mail does not auto populate passwords. Secure Mail matches the listed host names with the host name of the webpage encountered during Office 365 authentication and checks if the page uses HTTPS protocol. For instance, when sts.company.com is a listed host name and if the user navigates to `https://sts.company.com`, Secure Mail populates the password if the page has a password field. Default value is **login.microsoftonline.com**.

Mail Redirection

Mail Redirection

Blocks or restricts any mail compose. Secure Mail redirects mail compose to Secure Mail. The native mail redirects mail compose to native mail if an account is set up. Default value is **Secure Mail**.

Slack Integration

Enable Slack

Blocks or permits Slack integration. If **ON**, the Secure Mail interface includes Slack features. If **OFF**, the Secure Mail interface doesn't include Slack features. Default value is **OFF**.

Slack workspace name

The Slack workspace name for your company. If you provide a name, Secure Mail pre-fills the workspace name during sign-on. If you don't provide a name, users must type the workspace name (name.slack.com). Default value is empty.

Features by platform

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
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

FEATURE	IOS	ANDROID
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
Attachments sync in Drafts folder		X
Send, receive, reply, reply all, forward mail	X	X

FEATURE	IOS	ANDROID
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

FEATURE	IOS	ANDROID
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

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

FEATURE	IOS	ANDROID
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 <code>.pass</code> 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

FEATURE	IOS	ANDROID
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	

FEATURE	IOS	ANDROID
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
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

FEATURE	IOS	ANDROID
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

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

FEATURE	IOS	ANDROID
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
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

FEATURE	IOS	ANDROID
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 <code>.vcards</code>	X	X
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

FEATURE	IOS	ANDROID
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
Tap the back button on the device to dismiss the floating action button options		X
Microsoft Teams	X	X

Citrix Secure Web™

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

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

Feature flag management

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)

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

Citrix Secure Hub™

Citrix Secure Hub is the launchpad for the Citrix Endpoint Management™ (formerly, XenMobile) experience. Users enroll their devices in Secure Hub to gain access to the Store. From the store, they can add Citrix-developed mobile productivity apps and third-party apps.

For Secure Hub and other mobile productivity apps system requirements, see [System requirements](#).

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.

In addition to providing a portal for Citrix apps, Secure Hub 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 the following 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 repeatedly enter another credential like their Active Directory user name and password.

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 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. Certificate pinning prevents 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 may 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 in AutoDiscovery Service is set **ON**. For details, see [Endpoint Management AutoDiscovery Service](#).
- Private/self-signed CAs and the AutoDiscovery Service (ADS) is 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 is managed by the Endpoint Management Auto Discovery Service (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](#). Then, provide the following information:

- The domain containing the accounts with which users will 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 Endpoint Management administrator.
- The PEM-formatted certificates you want added to the domain.

Configuring certificate + one-time-password authentication for Secure Hub

You can configure Citrix ADC so that Secure Hub authenticates by 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 this type of authentication, 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 to allow Secure Hub to do this.

Note:

If different logon types are set in Endpoint Management and Citrix ADC, the Citrix ADC configuration overrides the configuration. 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_cvprn_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.

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Buttons: Add, Edit, Delete, Statistics, Visualizer, Action

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

Integrate with Citrix Products:

- XenMobile
- XenApp and XenDesktop
- Unified Gateway

- Click **Edit**.
- On the **Virtual Servers configuration** screen, scroll down to **Policies**.
- 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

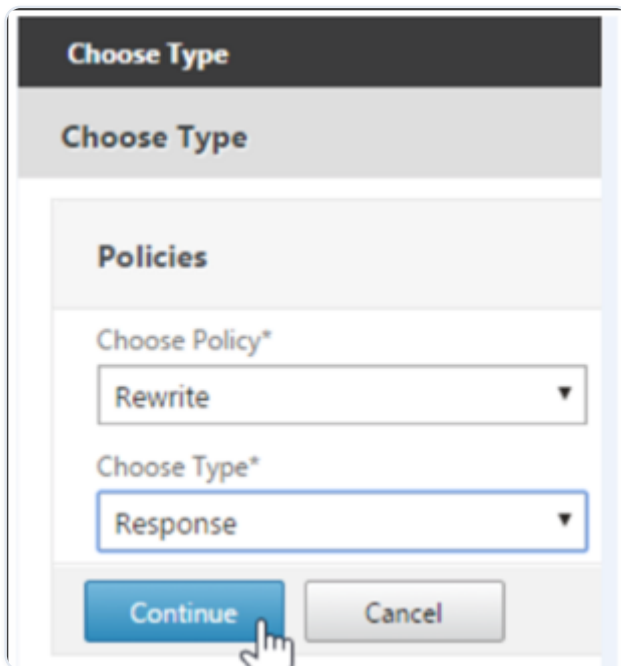
Done

Help >

Advanced Settings

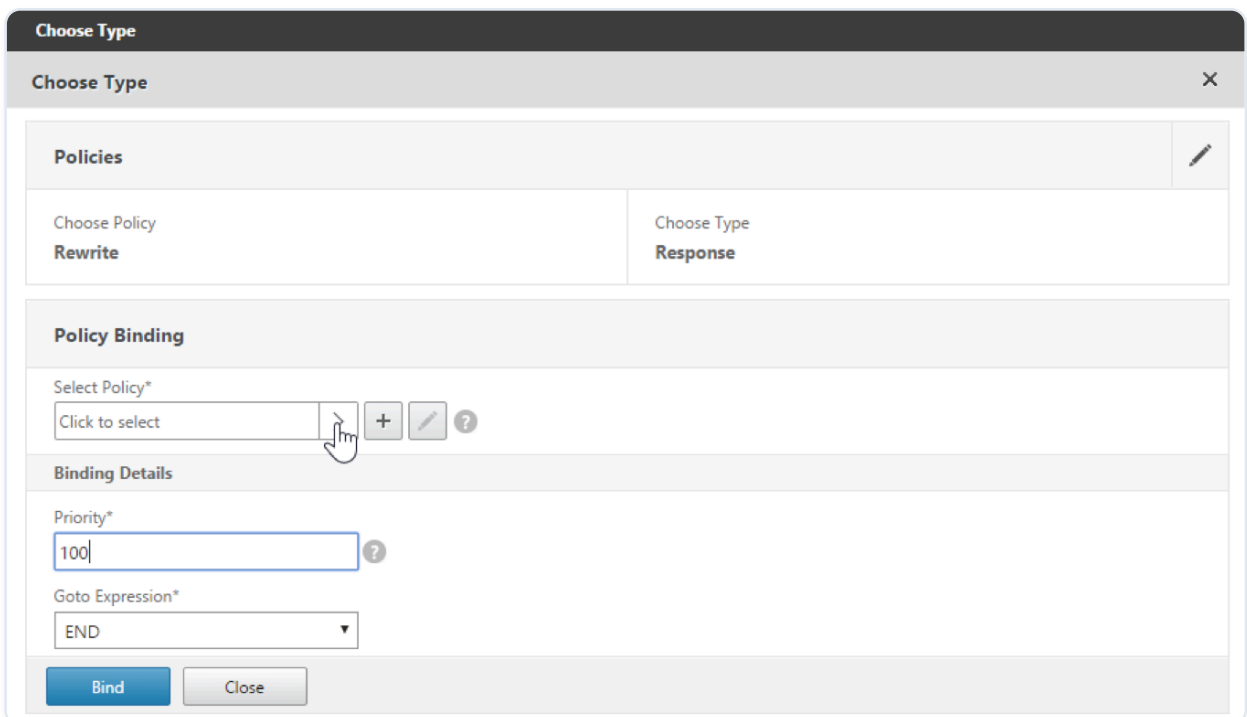
- Content Switching Policies
- SSL Profile
- SSL Policies
- Intranet IP Addresses
- Intranet Applications
- Portal Themes
- EULA

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



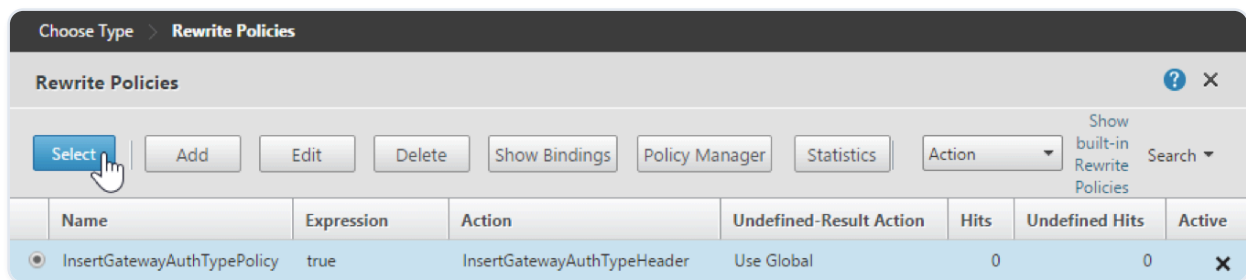
10. Click **Continue**.

The **Policy Binding** section expands.

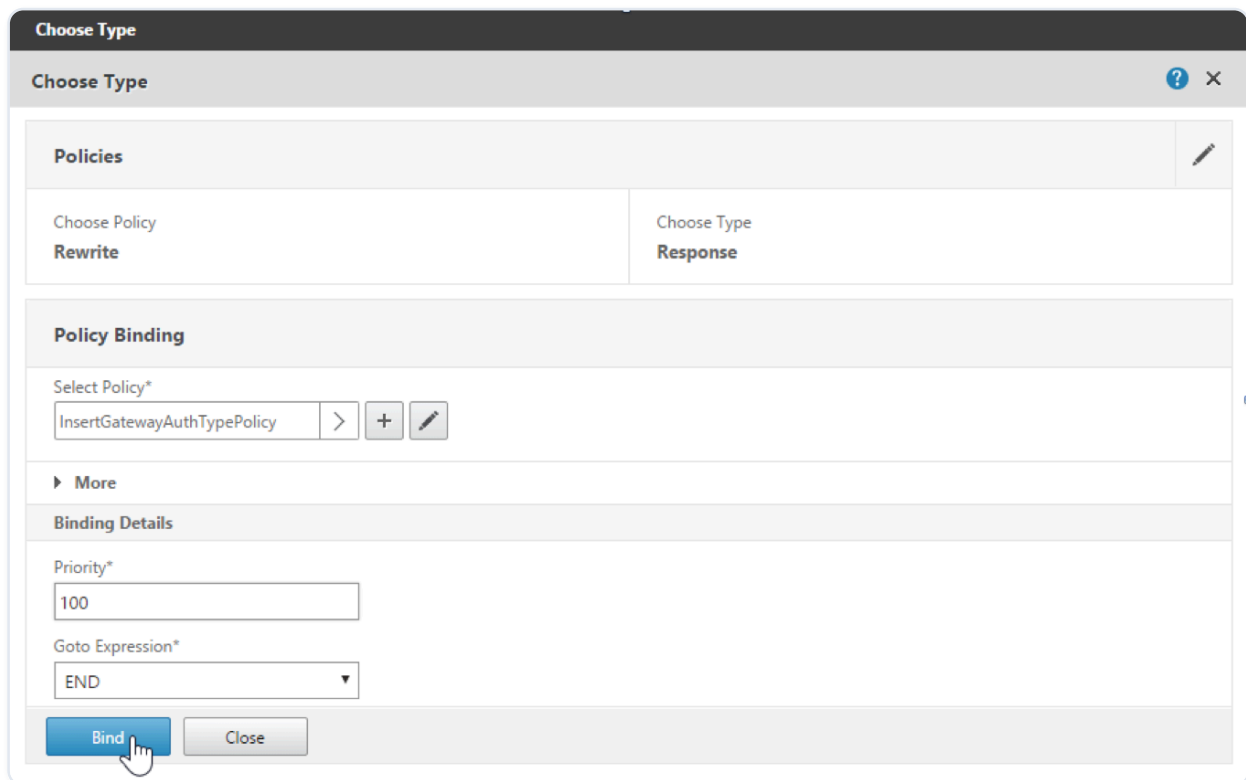


11. Click **Select Policy**.

A screen with available policies appears.



12. Click the row of the policy you just 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.

Enable DH Param
DISABLED

Enable Ephemeral RSA
ENABLED

Refresh Count
0

Enable Session Reuse
ENABLED

Time-out
120

SSL Redirect
DISABLED

Clear Text Port
0

Enable Cipher Redirect
DISABLED

Client Authentication
ENABLED

Client Certificate
Mandatory

Send Close-Notify
YES

PUSH Encryption Trigger
Always

SNI Enable
DISABLED

SSLv2 Redirect
DISABLED

SSLv2
DISABLED

SSLv3
ENABLED

TLSv1
ENABLED

TLSv1.1
ENABLED

TLSv1.2
ENABLED

SSL Ciphers

SSL Policies

Profiles

Intranet IP Addresses

Intranet Applications

Published Applications

No Next HOP Server

1 STA Server

No Uri

Other Settings

ICMP Virtual Server Response
Passive

RHI State
Passive

Redirect to Home page
true

Listen Priority
None

Listen Policy Expression
None

ShareFile
AppController

L2 Connection
https://xms3.dm.com:8443

false

Policies

Request Policies

3 Session Policies

2 ClientlessAccess Policies

4 Cache Policies

Response Policies

1 Rewrite Policy

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

VPN Virtual Server Rewrite Policy Binding

VPN Virtual Server Rewrite Policy Binding

Add Binding

Unbind

Edit

Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END

Close

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 Endpoint Management documentation. Note that 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 strongly discouraged from upgrading to Secure Hub 10.2. If you have any questions, please contact Citrix support.

To enable certificate pinning, you must do the following 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 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.ze nprise.com	52.5.138.94	443	Secure Hub - ADS Communication
discovery.mdm.ze nprise.com	52.1.30.122	443	Secure Hub - ADS Communication
ads.xm.cloud.com : note that SecureHub version 10.6.15 and later uses	34.194.83.188	443	Secure Hub - ADS Communication

FQDN	IP ADDRESS	PORT	IP AND PORT USAGE
ads.xml.cloud.com			
ads.xml.cloud.com : note that SecureHub version 10.6.15 and later uses ads.xml.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, provided that 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.

Secure Hub features

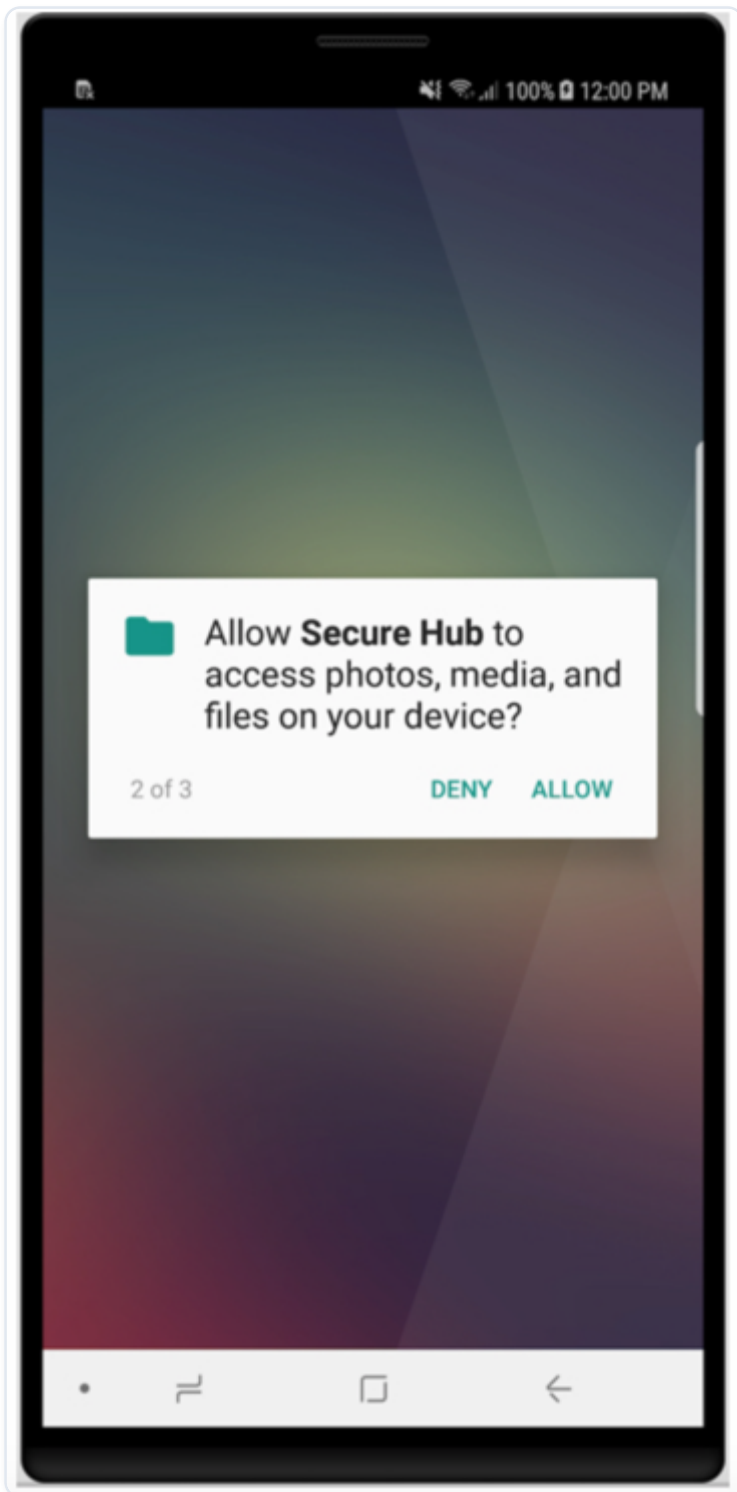
Secure Hub allows you to monitor and enforce mobile policies while providing access to the Store and live support. Users begin by downloading Secure Hub onto their devices from the Apple, Android, or Windows app store.

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 [Users, accounts, roles, and enrollment](#).

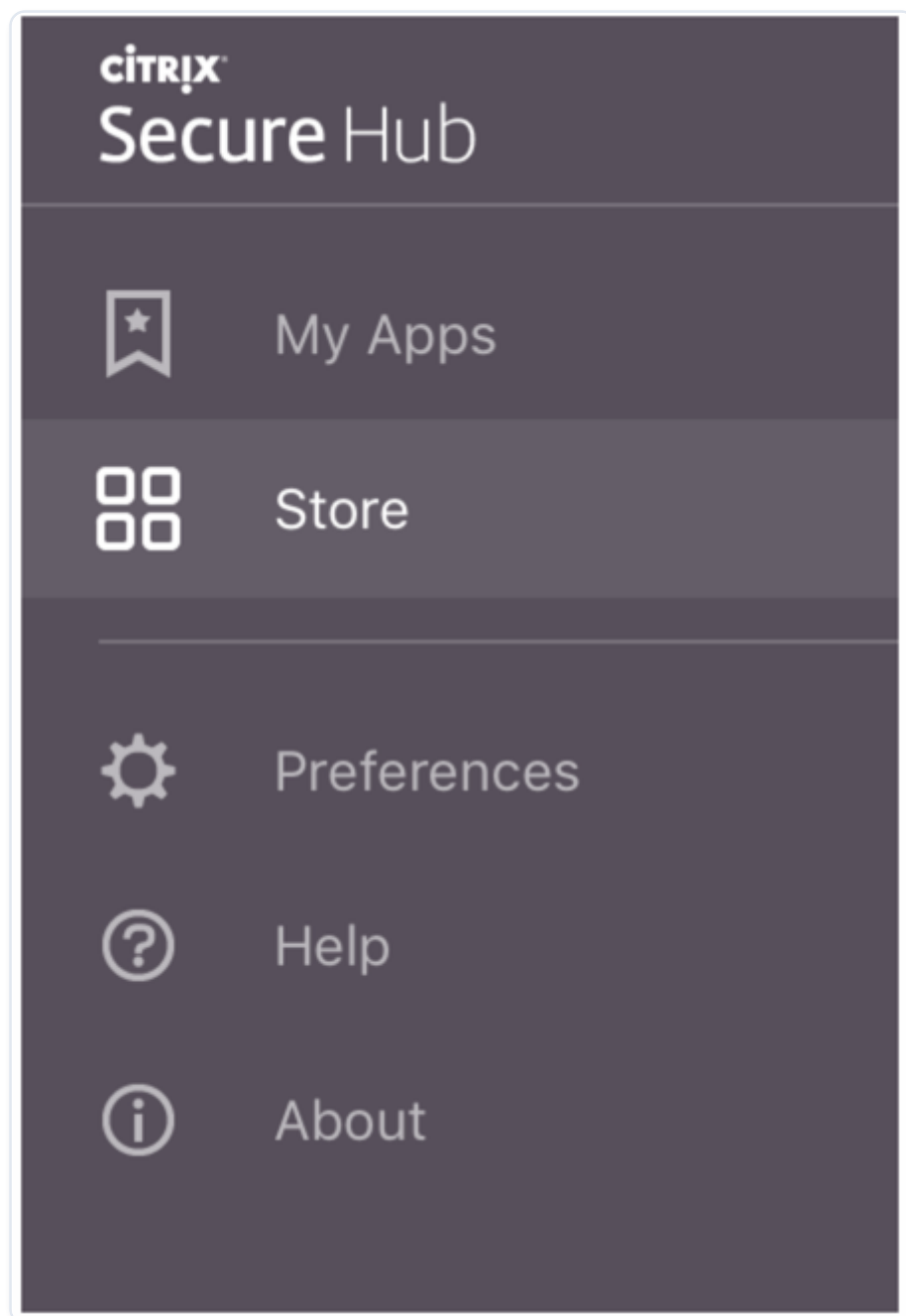
On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

Note that 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 Endpoint Management app store, they see a message stating that the enterprise developer, Citrix, is not trusted on that iPhone and the app will not be 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.

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, but the user is not required to enter any 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](#).

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

The screenshot shows the XenMobile console interface. The top navigation bar is green with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. On the right, there's a gear icon and a user profile 'administrator'. The main content area is titled 'Settings > Client Branding'. Below this, the 'Client Branding' section has a subtitle: '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'; 'Default store view' with radio buttons for 'Category' and 'A-Z' (selected); 'Device' with radio buttons for 'Phone' (selected) and 'Tablet'; and 'Branding file' with a text input and a green 'Browse' button. A 'Note' section follows with 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).', 'Files should be named as Header.png and Header@2x.png.', and '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.

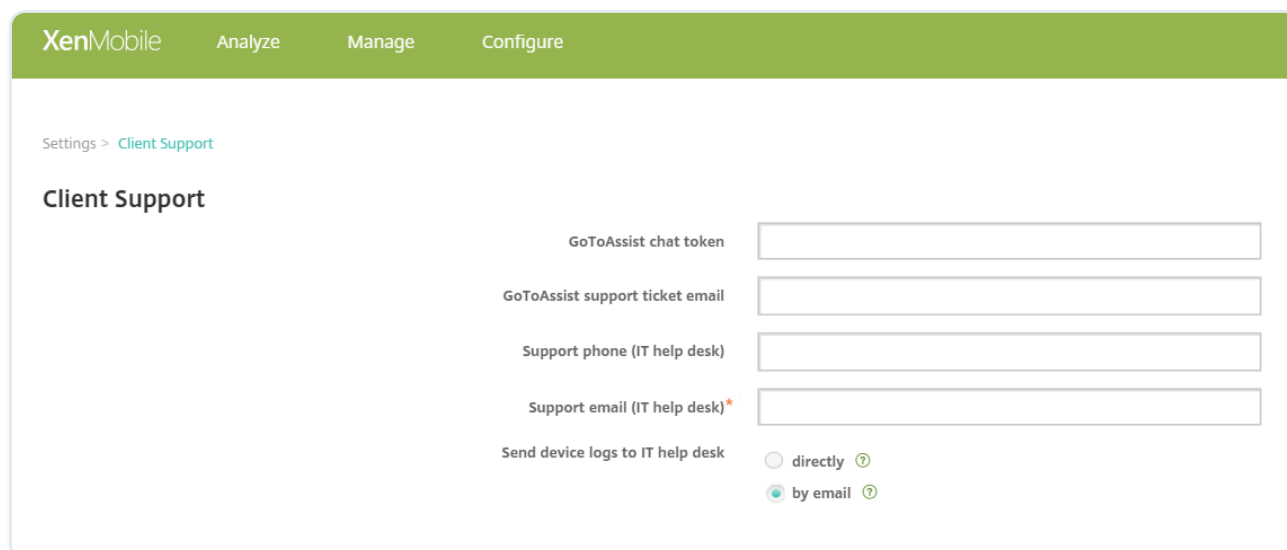
The screenshot shows the XenMobile Configure page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is selected, and the 'App Information' section is active. On the left, there is a sidebar with 'MDX' and a list of steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main area contains form fields for 'Name' (set to 'Workmail'), 'Description' (empty), and 'App category' (set to '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**.

Secure Hub also offers users a variety of 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**.

The screenshot shows the 'Help Desk' screen. At the top, there is a 'Close' button and the title 'Help Desk'. Below the title, there are three main options: 'Your IT Department', 'Report Issue', and 'Send Feedback to Citrix'. Each option has a right-pointing arrow. At the bottom, there is a 'Citrix Support' button.

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.



The screenshot shows the XenMobile interface with a green header bar containing the XenMobile logo and navigation tabs: Analyze, Manage, and Configure. Below the header, a breadcrumb trail reads 'Settings > Client Support'. The main title 'Client Support' is displayed. The settings are organized into two columns. The left column contains labels for 'GoToAssist chat token', 'GoToAssist support ticket email', 'Support phone (IT help desk)', 'Support email (IT help desk)*', and 'Send device logs to IT help desk'. The right column contains corresponding input fields: a text box for the chat token, text boxes for the support ticket email and support phone, a text box for the support email, and a radio button selection for sending device logs. The 'by email' option is selected for sending device logs. Each input field has a small question mark icon to its right.

GoToAssist chat token	
GoToAssist support ticket email	
Support phone (IT help desk)	
Support email (IT help desk)*	
Send device logs to IT help desk	☐ directly 
	☒ by email 

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.

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](#). Additionally, Secure Hub automatically collects and analyzes failure information so you can see what led to a particular failure. This function is supported by the software Crashlytics.

Secure Mail overview

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.
- 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](#).

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™

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

For Secure Web and other mobile productivity apps system requirements, see [System requirements](#).

Integrating and delivering Secure Web

NOTE:

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

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

1. To enable Single sign-on (SSO) to the internal network, configure Citrix Gateway.

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

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

Configuring user connections

Secure Web supports the following configurations for user connections:

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

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

Secure Web policies

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

Allowed or blocked websites

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

When a match is found, the prefix decides the action to take, as follows:

- A minus (-) prefix instructs the browser to block the URL. In this case, the URL is treated as if the web server address cannot be resolved.

- A plus (+) prefix allows the URL to be processed normally.
- If neither + or - is provided with the pattern, + (allow) is assumed.
- If the URL does not match any pattern in the list, the URL is allowed

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

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

Default value is empty (all URLs allowed).

Block pop-ups

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

Preloaded bookmarks

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

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

Default value is empty.

Home page URL

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

For supported Android and iOS devices only:

Browser user interface

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

Options

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

Enable web password caching

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

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

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

Proxy servers

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

DNS suffixes

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

Preparing intranet sites for Secure Web

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

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

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

TECHNOLOGY	IOS SECURE WEB	ANDROID 6.X/7.X SECURE WEB
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 **ctxmobilebrowser://** in front of the URL. For example, to open `example.com` from a native mail app, use the URL `ctxmobilebrowser://example.com`.
- When users click an intranet link in an email message, Secure Web goes to that site with no additional authentication required.
- Users can upload files to Citrix Files that they download from the web in Secure Web.

Secure Web users can also perform the following actions:

- Block pop-ups.

NOTE:

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

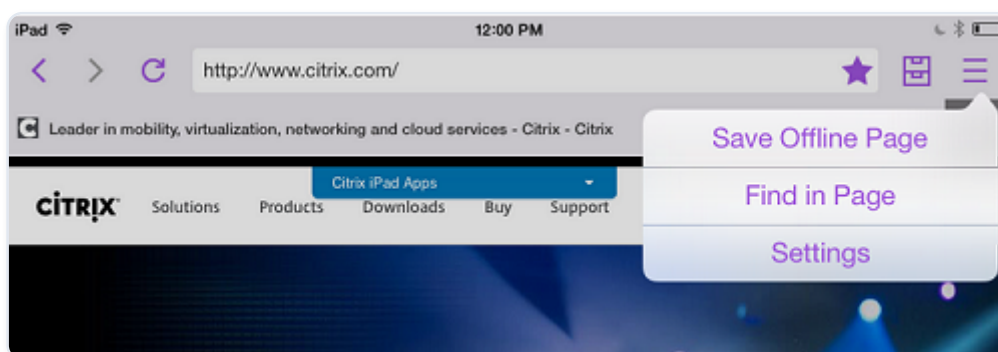
- Bookmark their favorite sites.
- Download files.
- Save pages offline.
- Auto-save passwords.
- Clear cache/history/cookies.
- Disable cookies and HTML5 local storage.
- Securely share devices with other users.
- Search within the address bar.
- Allow web apps they run with Secure Web to access their location.

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

NOTE:

Putting Secure Web in the background causes the download to stop.

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



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

NOTE:

- Citrix Files for XenMobile reached EOL on July 1, 2023. For more information, see [EOL and deprecated apps](#)

Citrix Content Collaboration™ for Endpoint Management

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.

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 login 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.

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 Citrix Endpoint Management console interface. The top navigation bar includes tabs for Analyze, Manage, Configure, and Monitor. The 'Configure' tab is selected, and within it, the 'Content Collaboration' sub-tab is active. The main content area is titled 'Content Collaboration' and contains configuration options for connecting to Citrix Files. A blue arrow points to the 'Search' button in the 'Assign to delivery groups' section.

About the settings:

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

If a user in a DG does not have a Citrix Files account, Endpoint Management provisions the user into Citrix Files when you add the Citrix Files client to Endpoint Management.

- The Citrix Files Administrator Account Logon information is used by Endpoint Management to save the SAML settings in the Citrix Files control plane.

IMPORTANT:

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

To configure Citrix Files account information in Endpoint Management for SSO

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

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

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

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

Prerequisites

- Endpoint Management must be able to reach your Citrix Files subdomain. To test the connection, ping your Citrix Files subdomain from the Endpoint Management server.
- The time zone configured for your Citrix Files account and for the hypervisor running Endpoint Management must be the same. If the time zone differs, SSO requests can fail because the

SAML token might not reach Citrix Files within the expected time frame. To configure the NTP server for Endpoint Management, use the Endpoint Management command-line interface.

NOTE:

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

- Log in to the ShareFile Account as an admin and verify the SAML SSO settings in **Settings > Admin Settings > Security > Login & Security Policy > Single sign-on / SAML 2.0 Configuration**.
- Download Citrix Content Collaboration for Endpoint Management clients.

Steps:

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

The configuration that enables SSO from Citrix Content Collaboration for Endpoint Management clients to Citrix Files does not authenticate users to network shares or SharePoint document libraries.

6. To enable SSO between the Secure Hub micro VPN and storage zones controller, complete the following policy configuration:

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

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

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

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

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

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

To validate Citrix Content Collaboration for Endpoint Management clients

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

NOTE:

- Citrix Files for XenMobile has reached EOL on July 1, 2023. For more information, see [EOL and deprecated apps](#)

EOL and deprecated apps

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

NOTE:

For advanced notice of Citrix Endpoint Management features that are being phased out, see [Deprecation](#).

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

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

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

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

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

ShareConnect: ShareConnect reached EOL on June 30, 2020.

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

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

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

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

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

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

ScanDirect: ScanDirect reached EOL on September 1, 2018.

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.

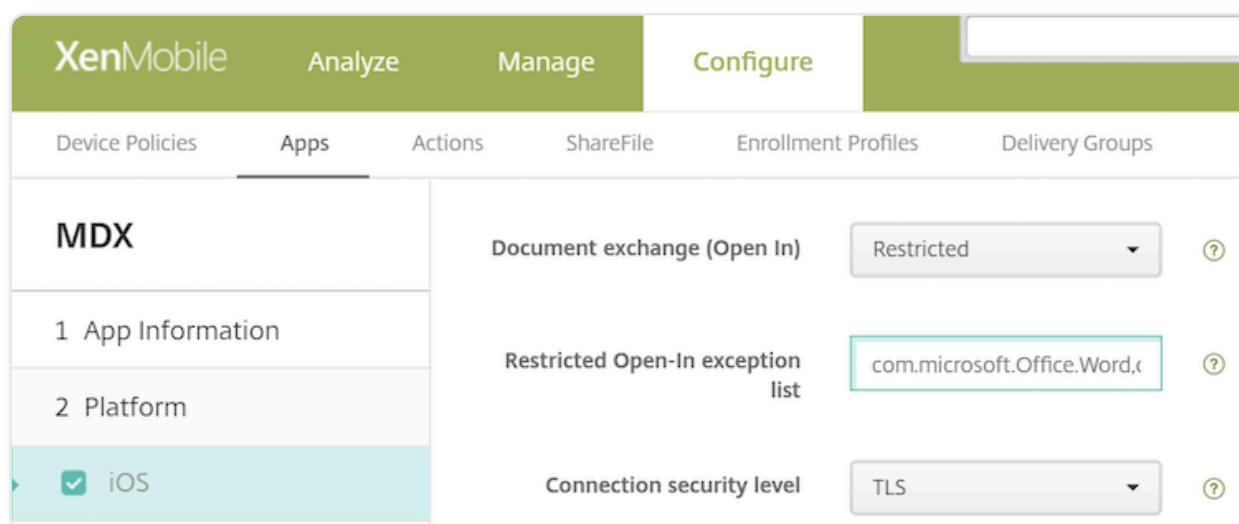
Allowing secure interaction with Office 365 apps

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.

Mobile productivity apps document history

The following table describes important changes to mobile productivity apps product documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
23 Sep 2026	Release of Secure Hub for iOS version 26.8.1	What's new in the current version
21 Sep 2026	EAR of Secure Hub for iOS 26.8.1	Next release preview
16 Sep 2026	Release of Secure Mail for iOS version 26.8.0	What's new in the current version
16 Sep 2026	Release of Secure Web for iOS version 26.8.0	What's new in the current version
15 Sep 2026	Release of Secure Hub for Android version 26.8.0	What's new in the current version
10 Sep 2026	Release of Secure Hub for iOS version 26.8.0	What's new in the current version
07 Sep 2026	EAR of Secure Hub for Android 26.8.0	Next release preview
28 Aug 2026	EAR of Secure Mail for iOS 26.8.0	Next release preview
28 Aug 2026	EAR of Secure Web for iOS 26.8.0	Next release preview
27 Aug 2026	EAR of Secure Hub for iOS 26.8.0	Next release preview
13 Jul 2026	Release of Secure Web for Android version 26.5.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
26 Jun 2026	EAR of Secure Web for Android 26.5.0	Next release preview
10 Jun 2026	Release of Secure Mail for Android version 26.5.0	What's new in the current version
04 Jun 2026	Release of Secure Mail for iOS version 26.5.0	What's new in the current version
04 Jun 2026	Release of Secure Web for iOS version 26.5.0	What's new in the current version
28 May 2026	Release of Secure Hub for Android version 26.5.0	What's new in the current version
26 May 2026	EAR of Secure Mail for Android 26.5.0	Next release preview
20 May 2026	EAR of Secure Web for iOS 26.5.0	Next release preview
20 May 2026	EAR of Secure Mail for iOS 26.5.0	Next release preview
06 May 2026	EAR of Secure Hub for Android 26.5.0	Next release preview
30 Mar 2026	Release of Secure Web for Android version 26.2.0	What's new in the current version
20 Mar 2026	EAR of Secure Web for Android 26.2.0	Next release preview
06 Mar 2026	Release of Secure Hub for Android version 26.2.0	What's new in the current version
09 Feb 2026	EAR of Secure Hub for Android 26.2.0	Next release preview
21 Jan 2026	Release of Secure Mail for iOS version 26.1.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
12 Jan 2026	Release of Secure Mail for Android version 25.12.0	What's new in the current version
07 Jan 2026	EAR of Secure Mail for iOS 26.1.0	Next release preview
06 Jan 2026	EAR of Secure Mail for Android 25.12.0	Next release preview
03 Oct 2025	Release of Secure Hub for Android version 25.10.0	What's new in the current version
23 Oct 2025	Release of Secure Mail for Android version 25.8.0	What's new in the current version
23 Oct 2025	Release of Secure Web for Android version 25.8.0	What's new in the current version
22 Oct 2025	Release of Secure Web for iOS version 25.9.0	What's new in the current version
22 Oct 2025	Release of Secure Mail for iOS version 25.9.0	What's new in the current version
15 Oct 2025	EAR of Secure Hub for Android 25.10.0	Next release preview
19 Sep 2025	EAR of Secure Mail for Android 25.8.0	Next release preview
12 Sep 2025	Release of Secure Hub for iOS version 25.8.0	What's new in the current version
12 Sep 2025	EAR of Secure Web for Android 25.8.0	Next release preview
19 Aug 2025	EAR of Secure Hub for iOS 25.8.0	Next release preview
30 Jul 2025	Release of Secure Mail for Android version 25.6.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
30 Jul 2025	Release of Secure Web for Android version 25.6.0	What's new in the current version
30 Jul 2025	Release of Secure Hub for Android version 25.7.0	What's new in the current version
23 Jul 2025	EAR of Secure Hub for Android 25.7.0	Next release preview
07 Jul 2025	EAR of Secure Web for Android 25.6.0	Next release preview
07 Jul 2025	EAR of Secure Mail for Android 25.6.0	Next release preview
07 Jul 2025	Release of Secure Hub for iOS version 25.6.0	What's new in the current version
07 Jul 2025	Release of Secure Web for iOS version 25.5.0	What's new in the current version
07 Jul 2025	Release of Secure Mail for iOS version 25.5.0	What's new in the current version
30 May 2025	EAR of Secure Web for iOS 25.5.0	Next release preview
21 May 2025	Release of Secure Hub for Android version 25.4.0	What's new in the current version
02 Apr 2025	Release of Secure Mail for Android version 25.3.0	What's new in the current version
02 Apr 2025	Release of Secure Web for Android version 25.3.0	What's new in the current version
17 Feb 2025	Release of Secure Mail for Android version 25.1.0	What's new in the current version
17 Feb 2025	Release of Secure Hub for iOS version 25.1.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
12 Feb 2025	Release of Secure Mail for iOS version 25.1.0	What's new in the current version
10 Feb 2025	Release of Secure Hub for Android version 25.1.0	What's new in the current version
10 Feb 2025	Release of Secure Web for iOS version 25.1.0	What's new in the current version
10 Feb 2025	Release of Secure Web for Android version 25.1.0	What's new in the current version
09 Dec 2024	Release of Secure Mail for iOS version 24.11.0	What's new in the current version
09 Dec 2024	Release of Secure Hub for iOS version 24.11.0	What's new in the current version
06 Dec 2024	Release of Secure Web for iOS version 24.11.0	What's new in the current version
05 Dec 2024	Release of Secure Mail for Android version 24.11.0	What's new in the current version
04 Dec 2024	EAR of Secure Mail for Android 24.11.0	Next release preview
04 Dec 2024	EAR of Secure Mail for iOS 24.11.0	Next release preview
26 Nov 2024	EAR of Secure Web for iOS 24.11.0	Next release preview
26 Nov 2024	EAR of Secure Hub for iOS 24.11.0	Next release preview
25 Nov 2024	New chapter: Feature flag management	Feature flag management
05 Nov 2024	Release of Secure Hub for Android version 24.10.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
24 Oct 2024	EAR of Secure Hub for Android 24.10.0	Next release preview
22 Oct 2024	Release of Secure Mail for Android version 24.9.1	What's new in the current version
15 Oct 2024	Release of Secure Hub for iOS version 24.9.0	What's new in the current version
09 Oct 2024	Release of Secure Web for Android version 24.9.0	What's new in the current version
09 Oct 2024	Release of Secure Mail for Android version 24.9.0	What's new in the current version
09 Oct 2024	EAR of Secure Hub for iOS 24.9.0	Next release preview
27 Sep 2024	EAR of Secure Web for Android 24.9.0	Next release preview
27 Sep 2024	EAR of Secure Mail for Android 24.9.0	Next release preview
20 Sep 2024	Release of Secure Mail for iOS version 24.9.0	What's new in the current version
16 Sep 2024	Release of Secure Web for iOS version 24.9.0	What's new in the current version
06 Sep 2024	Revised the release of Secure Hub for Android version 24.8.0	What's new in the current version
04 Sep 2024	EAR of Secure Mail for iOS 24.9.0	Next release preview
03 Sep 2024	EAR of Secure Web for iOS 24.9.0	Next release preview
02 Sep 2024	Release of Secure Hub for Android version 24.8.0	What's new in the current version

DATE	CHANGE	DESCRIPTION
28 Aug 2024	Release of Secure Web for Android version 24.8.0	What's new in the current version
23 Aug 2024	EAR of Secure Web for Android version 24.8.0	Next release preview
21 Aug 2024	EAR of Secure Hub for Android version 24.8.0	Next release preview
29 Jul 2024	Release of Secure Mail for Android version 24.7.0	Secure Mail 24.7.0: What's new in the current version
16 Jul 2024	EAR of Secure Mail for Android 24.7.0	Next release preview
01 Jul 2024	Release of Secure Hub for Android version 24.6.0	Secure Hub 24.6.0: What's new in the current version
06 May 2024	Release of Secure Hub for iOS version 24.5.0	Secure Hub 24.5.0: What's new in the current version
22 Apr 2024	Revised the release of Secure Hub for Android version 24.3.0 with a new feature.	Secure Hub 24.3.0: What's new in the current version
22 Apr 2024	Revised the release of Secure Hub for Android version 23.12.0 with new features.	Secure Hub 23.12.0: What's new in the current version
11 Apr 2024	Release of Secure Hub for Android version 24.3.0	Secure Hub 24.3.0: Bug fixes
25 Mar 2024	Release of Secure Web for iOS version 24.3.0	Secure Web 24.3.0: Bug fixes
25 Mar 2024	Release of Secure Mail for iOS version 24.3.0	Secure Mail 24.3.0: Bug fixes

DATE	CHANGE	DESCRIPTION
18 Mar 2024	Release of Secure Web for Android version 24.3.0	Secure Web 24.3.0: Bug fixes
21 Feb 2024	Release of Secure Web for iOS version 24.2.0	Secure Web 24.2.0: Bug fixes
21 Feb 2024	Release of Secure Web for iOS version 24.2.0	Secure Web 24.2.0: What's new in the current version
21 Feb 2024	Release of Secure Mail for iOS version 24.2.0	Secure Mail 24.2.0: Bug fixes
21 Feb 2024	Release of Secure Mail for iOS version 24.2.0	Secure Mail 24.2.0: What's new in the current version
19 Feb 2024	Release of Secure Web for Android version 24.1.0	Secure Web 24.1.0: Bug fixes
19 Feb 2024	Release of Secure Mail for Android version 24.1.0	Secure Mail 24.1.0: Bug fixes
19 Feb 2024	Release of Secure Mail for Android version 24.1.0	Secure Mail 24.1.0: What's new in the current version
16 Jan 2024	Release of Secure Hub for iOS version 24.1.0	Secure Hub 24.1.0: What's new in the current version
16 Jan 2024	Release of Secure Hub for iOS version 24.1.0	Secure Hub 24.1.0: Bug fixes
16 Jan 2024	Release of Secure Hub for Android version 23.12.0	Secure Hub 23.12.0: What's new in the current version and Bug fixes
04 Dec 2023	Added the obscure screen documentation	Secure Mail: Obscure screen contents
28 Nov 2023	Release of Secure Hub for iOS version 23.11.0	Secure Hub 23.11.0: What's new in the current version
28 Nov 2023	Release of Secure Hub for iOS version 23.11.0	Secure Hub 23.11.0: Bug fixes

DATE	CHANGE	DESCRIPTION
17 Nov 2023	Release of Secure Web for Android version 23.10.0	Secure Web 23.10.0: What's new in the current version
17 Nov 2023	Release of Secure Mail for Android version 23.10.0	Secure Mail 23.10.0: Bug fixes
27 Oct 2023	Release of Secure Mail for Android version 23.8.2	Secure Mail 23.8.2: What's new in the current version
19 Oct 2023	Release of Secure Hub for Android version 23.10.0	Secure Hub 23.10.0: What's new in the current version
04 Oct 2023	Release of Secure Mail for Android version 23.7.0	Secure Mail 23.7.0: What's new in the current version
04 Oct 2023	Release of Secure Mail for iOS version 23.7.0	Secure Mail 23.7.0: What's new in the current version
29 Sep 2023	Release of Secure Mail for Android version 23.8.1	Secure Mail 23.8.1: What's new in the current version
20 Sep 2023	Release of Secure Web for iOS version 23.9.0	Secure Web 23.9.0: What's new in the current version
20 Sep 2023	Release of Secure Mail for iOS version 23.9.0	Secure Mail 23.9.0: What's new in the current version
20 Sep 2023	Release of Secure Web for Android version 23.8.0	Secure Web 23.8.0: What's new in the current version
20 Sep 2023	Release of Secure Mail for Android version 23.8.0	Secure Mail 23.8.0: What's new in the current version
01 Sep 2023	Release of Secure Hub for Android version 23.9.0	Secure Hub 23.9.0: What's new in the current version
25 Aug 2023	Release of Secure Hub for iOS version 23.8.1	Secure Hub 23.8.1: What's new in the current version
08 Aug 2023	Release of Secure Hub for iOS version 23.8.0	Secure Hub 23.8.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
31 Jul 2023	Release of Secure Web for Android version 23.7.0	Secure Web 23.7.0: What's new in the current version
31 Jul 2023	Release of Secure Mail for Android version 23.7.0	Secure Mail 23.7.0: What's new in the current version
26 Jul 2023	Release of Secure Hub for Android version 23.7.0	Secure Hub 23.7.0: What's new in the current version
07 Jul 2023	Release of Secure Hub for iOS version 23.4.0	Secure Hub 23.4.0: What's new in the current version
22 Jun 2023	Added the known issue CXM-110137	Secure Mail for Android Known issues
07 Jun 2023	Release of Secure Mail for Android version 23.6.0	Secure Mail 23.6.0: What's new in the current version
31 May 2023	Release of Secure Web for iOS version 23.5.0	Secure Web 23.5.0: What's new in the current version
31 May 2023	Release of Secure Mail for iOS version 23.5.0	Secure Mail 23.5.0: What's new in the current version
26 May 2023	Release of Secure Hub for Android version 23.4.0	Secure Hub 23.4.0: What's new in the current version
23 May 2023	Release of Secure Hub for Android version 23.2.0	Secure Hub 23.2.0: What's new in the current version
12 Apr 2023	Release of Secure Web for Android version 23.3.5	Added a known issue
28 Mar 2023	Release of Secure Web for Android version 23.3.5	Secure Web 23.3.5: What's new in the current version
28 Mar 2023	Release of Secure Mail for Android version 23.3.5	Secure Mail 23.3.5: What's new in the current version
09 Jan 2023	Release of Secure Hub for Android version 22.11.0	Secure Hub 22.11.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
01 Feb 2023	Release of Secure Web for iOS and Android version 23.2.0	Secure Web 23.2.0: What's new in the current version
01 Feb 2023	Release of Secure Mail for Android version 23.2.0	Secure Mail 23.2.0: What's new in the current version
28 Oct 2022	Release of Secure Mail for Android version 22.11.0	Secure Mail 22.11.0: What's new in the current version
12 Oct 2022	Release of Secure Hub for Android version 22.9.0	Secure Hub 22.9.0: What's new in the current version
28 Sep 2022	Release of Secure Mail for Android version 22.9.0	Secure Mail 22.9.0: What's new in the current version
28 Sep 2022	Release of Secure Web for Android version 22.9.0	Secure Web 22.9.0: What's new in the current version
08 Sep 2022	Release of Secure Web for iOS version 22.9.1	Secure Web 22.9.1: What's new in the current version
07 Sep 2022	Release of Secure Web for iOS version 22.9.0	Secure Web 22.9.0: What's new in the current version
07 Sep 2022	Release of Secure Mail version 22.9.0	Secure Mail 22.9.0: What's new in the current version
01 Sep 2022	Release of Secure Web for iOS version 22.9.0	The Secure Web 22.9.0 has been rolled back on 2 Sep 2022, and we are actively working on a fix and will announce the release shortly.
01 Sep 2022	Release of Secure Mail version 22.9.0	The Secure Mail 22.9.0 has been rolled back on 2 Sep 2022, and we are actively working on a fix and will announce the release shortly.

DATE	CHANGE	DESCRIPTION
26 Jul 2022	Release of Secure Hub for Android version 22.7.0	Secure Hub 22.7.0: What's new in the current version
13 Jul 2022	Release of Secure Web for iOS version 22.6.0	Secure Web 22.6.0: What's new in the current version
14 Jun 2022	Release of Secure Mail version 22.6.0	Secure Mail 22.6.0: What's new in the current version
14 Jun 2022	Release of Secure Web for Android version 22.6.0	Secure Web 22.6.0: What's new in the current version
14 Jun 2021	Release of Secure Hub for Android version 22.6.0	Secure Hub 22.6.0: What's new in the current version
09 Feb 2022	Release of Secure Mail version 22.2.0	Secure Mail 22.2.0: What's new in the current version
09 Feb 2022	Release of Secure Web version 22.2.0	Secure Web 22.2.0: What's new in the current version
08 Dec 2021	Release of Secure Mail version 21.12.0	Secure Mail 21.12.0: What's new in the current version
08 Dec 2021	Release of Secure Web version 21.12.0	Secure Web 21.12.0: What's new in the current version
27 Oct 2021	Release of Secure Mail version 21.10.5	Secure Mail 21.10.5: What's new in the current version
27 Oct 2021	Release of Secure Web version 21.10.5	Secure Web 21.10.5: What's new in the current version
13 Oct 2021	Release of Secure Hub version 21.10.0	Secure Hub 21.10.0: What's new in the current version
13 Oct 2021	Release of Secure Mail version 21.10.0	Secure Mail 21.10.0: What's new in the current version
13 Oct 2021	Release of Secure Web version 21.10.0	Secure Web 21.10.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
20 Sep 2021	Release of Secure Mail version 21.9.1	Secure Mail 21.9.1: What's new in the current version
20 Sep 2021	Release of Secure Web version 21.9.1	Secure Web 21.9.1: What's new in the current version
08 Sep 2021	Release of Secure Mail version 21.9.0	Secure Mail 21.9.0: What's new in the current version
08 Sep 2021	Release of Secure Web version 21.9.0	Secure Web 21.9.0: What's new in the current version
24 Aug 2021	Release of Secure Mail for Android version 21.8.5	Secure Mail 21.8.5: What's new in the current version
24 Aug 2021	Release of Secure Web for Android version 21.8.5	Secure Web 21.8.5: What's new in the current version
13 Aug 2021	Release of Secure Hub for iOS version 21.8.0	Secure Hub 21.8.0: What's new in the current version
13 Aug 2021	Release of Secure Mail version 21.8.0	Secure Mail 21.8.0: What's new in the current version
13 Aug 2021	Release of Secure Web version 21.8.0	Secure Web 21.8.0: What's new in the current version
10 Aug 2021	Release of Secure Hub for Android version 21.7.1	Secure Hub 21.7.1: What's new in the current version
15 Jul 2021	Release of Secure Mail version 21.7.0	Secure Mail 21.7.0: What's new in the current version
15 Jul 2021	Release of Secure Web version 21.7.0	Secure Web 21.7.0: What's new in the current version
07 Jul 2021	Release of Secure Hub for iOS version 21.7.0	Secure Hub 21.7.0: What's new in the current version
06 Jul 2021	Release of Secure Hub for Android version 21.7.0	Secure Hub 21.7.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
24 Jun 2021	Release of Secure Mail for iOS version 21.6.0	Secure Mail 21.6.0: What's new in the current version
16 Jun 2021	Release of Secure Hub version 21.6.0	Secure Hub 21.6.0: What's new in the current version
16 Jun 2021	Release of Secure Mail for Android version 21.6.0	Secure Mail 21.6.0: What's new in the current version
16 Jun 2021	Release of Secure Web version 21.6.0	Secure Web 21.6.0: What's new in the current version
20 May 2021	Release of Secure Hub version 21.5.1	Secure Hub 21.5.1: What's new in the current version
12 May 2021	Release of Secure Hub version 21.5.0	Secure Hub 21.5.0: What's new in the current version
12 May 2021	Release of Secure Mail version 21.5.0	Secure Mail 21.5.0: What's new in the current version
12 May 2021	Release of Secure Web for iOS version 21.5.0	Secure Web 21.5.0: Bug fixes
04 May 2021	Release of Secure Mail for Android version 21.4.5	Secure Mail 21.4.5: What's new in the current version
04 May 2021	Release of Secure Web for Android version 21.4.5	Secure Web 21.4.5: Bug fixes
15 Apr 2021	Release of Secure Hub version 21.4.0	Secure Hub 21.4.0: What's new in the current version
15 Apr 2021	Release of Secure Mail for iOS version 21.4.0	Secure Mail 21.4.0: Bug fixes
31 Mar 2021	Release of Secure Hub for iOS version 21.3.2	Secure Hub 21.3.2: Bug fixes
30 Mar 2021	Release of Secure Mail for Android version 21.3.5	Secure Mail 21.3.5: What's new in the current version

DATE	CHANGE	DESCRIPTION
30 Mar 2021	Release of Secure Web for Android version 21.3.5	Secure Web 21.3.0: Bug fixes
22 Mar 2021	Release of Secure Mail for iOS version 21.3.0	Secure Mail 21.3.0: What's new in the current version
17 Mar 2021	Release of Secure Hub version 21.3.0	Secure Hub 21.3.0: Bug fixes
17 Mar 2021	Release of Secure Mail for Android version 21.3.0	Secure Mail 21.3.0: What's new in the current version
17 Mar 2021	Release of Secure Web for Android version 21.3.0	Secure Web 21.3.0: Bug fixes
24 Feb 2021	Release of Secure Mail version 21.2.0	Secure Mail 21.2.0: What's new in the current version
24 Feb 2021	Release of Secure Web version 21.2.0	Secure Web 21.2.0: What's new in the current version
18 Feb 2021	Release of Secure Hub for Android version 21.2.0	Secure Hub 21.2.0: Bug fixes
01 Feb 2021	Release of Secure Mail for iOS version 21.1.5	Secure Mail 21.1.5: Bug fixes
01 Feb 2021	Release of Secure Web for iOS version 21.1.5	Secure Web 21.1.5: Bug fixes
14 Jan 2021	Release of Secure Mail version 21.1.0	Secure Mail 21.1.0: Bug fixes
14 Jan 2021	Release of Secure Web version 21.1.0	Secure Web 21.1.0: Bug fixes
12 Jan 2021	Release of Secure Hub version 21.1.0	Secure Web 21.1.0: Bug fixes
15 Dec 2020	Release of Secure Hub version 20.12.0	Secure Hub 20.12.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
15 Dec 2020	Release of Secure Mail for iOS version 20.12.0	Secure Mail 20.12.0: Bug fixes
15 Dec 2020	Release of Secure Web for iOS version 20.12.0	Secure Web 20.12.0: Bug fixes
19 Nov 2020	Release of Secure Hub for Android version 20.11.0	Secure Hub 20.11.0: What's new in the current version
19 Nov 2020	Release of Secure Mail for Android version 20.11.0	Secure Mail 20.11.0: What's new in the current version
19 Nov 2020	Release of Secure Web for Android version 20.11.0	Secure Web 20.11.0: Bug fixes
17 Nov 2020	Release of Secure Mail for iOS version 20.11.0	Secure Mail 20.11.0: What's new in the current version
17 Nov 2020	Release of Secure Web for iOS version 20.11.0	Secure Web 20.11.0: Bug fixes
27 Oct 2020	Release of Secure Mail version 20.10.5	Secure Mail 20.10.5: What's new in the current version
27 Oct 2020	Release of Secure Web for Android version 20.10.5	Secure Web 20.10.5: What's new in the current version
27 Oct 2020	Release of Secure Hub for iOS version 20.10.5	Secure Hub 20.10.5: Bug fixes
21 Oct 2020	Release of Secure Hub for Android version 20.10.5	Secure Hub 20.10.5: Bug fixes
15 Oct 2020	Release of Secure Mail version 20.10.0	Secure Mail 20.10.0: What's new in the current version
15 Oct 2020	Release of Secure Web for Android version 20.10.0	Secure Mail 20.10.0: What's new in the current version
29 Sep 2020	Release of Secure Mail for Android version 20.9.5	Secure Mail 20.9.5: Bug fixes

DATE	CHANGE	DESCRIPTION
29 Sep 2020	Release of Secure Web for iOS version 20.9.5	Secure Web 20.9.5: Bug fixes
17 Sep 2020	Release of Secure Mail version 20.9.0	Secure Mail 20.9.0: Bug fixes
17 Sep 2020	Release of Secure Web for Android version 20.9.0	Secure Web 20.9.0: What's new in the current version
04 Sep 2020	Release of Secure Hub version 20.9.0	Secure Hub 20.9.0: What's new in the current version
27 Aug 2020	Release of Secure Mail version 20.8.5	Secure Mail 20.8.5: What's new in the current version
27 Aug 2020	Release of Secure Web version 20.8.5	Secure Web 20.8.5: What's new in the current version
20 Aug 2020	Release of Secure Hub version 20.7.5	Secure Hub 20.7.5: What's new in the current version
19 Aug 2020	Release of Secure Mail version 20.8.0	Secure Mail 20.8.0: What's new in the current version
19 Aug 2020	Release of Secure Web version 20.8.0	Secure Web 20.8.0: What's new in the current version
12 Aug 2020	Citrix ShareConnect reached end of life (EOL).	For details, see the product lifecycle milestones in the Product Matrix .
29 Jul 2020	Release of Secure Mail version 20.7.5	Secure Mail 20.7.5: What's new in the current version
29 Jul 2020	Release of Secure Web version 20.7.5	Secure Web 20.7.5: Bug fixes
14 Jul 2020	Release of Secure Mail version 20.7.0	Secure Mail 20.7.0: Bug fixes
14 Jul 2020	Release of Secure Web version 20.7.0	Secure Web 20.7.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
10 Jul 2020	Enable a proxy configured on iOS devices to use proxy servers configured in the Wi-Fi settings.	See details in What's new in Secure Hub
06 Jul 2020	Transition from 32-bit to 64-bit for apps. Upgrade Android devices to Secure Hub version 20.6.5 to avoid reauthentication when you upgrade to later versions.	See details in What's new in Secure Hub
01 Jul 2020	Release of Secure Hub version 20.6.5	Secure Hub 20.6.5: Bug fixes
01 Jun 2020	Release of Secure Mail version 20.6.5	Secure Mail 20.6.5: Bug fixes
19 Jun 2020	Platform encryption for QuickEdit	See details in Encryption for QuickEdit
16 Jun 2020	Release of Secure Mail version 20.6.0	Secure Mail 20.6.0: Bug fixes
16 Jun 2020	Release of Secure Web version 20.6.0	Secure Web 20.6.0: Bug fixes
02 Jun 2020	MDX Encryption end of life is fast approaching. All devices must move to platform encryption before September 1, 2020	See details in recent announcements
19 May 2020	Release of Secure Mail for iOS version 20.5.0	Secure Mail 20.5.0: Bug fixes
19 May 2020	Release of Secure Web for iOS version 20.5.0	Secure Web 20.5.0: Bug fixes
11 May 2020	Release of Secure Mail for iOS version 20.4.5	Secure Mail 20.4.5: What's new in the current version

DATE	CHANGE	DESCRIPTION
11 May 2020	Release of Secure Web for iOS version 20.4.5	Secure Web 20.4.5: What's new in the current version
28 Apr 2020	Release of Secure Mail for Android version 20.4.5	Secure Mail 20.4.5: What's new in the current version
28 Apr 2020	Release of Secure Web for Android version 20.4.5	Secure Web 20.4.5: Bug fixes
21 Apr 2020	Release of Secure Mail for iOS version 20.4.0	Secure Mail 20.4.0: What's new in the current version
21 Apr 2020	Release of Secure Web for iOS version 20.4.0	Secure Web 20.4.0: Bug fixes
14 Apr 2020	Release of Secure Mail for Android version 20.4.0	Secure Mail 20.4.0: What's new in the current version
14 Apr 2020	Release of Secure Web for Android version 20.4.0	Secure Web 20.4.0: Bug fixes
31 Mar 2020	Release of Secure Hub for iOS version 20.3.0	Secure Hub 20.3.0: What's new in the current version
24 Mar 2020	Release of Secure Mail version 20.3.0	Secure Mail 20.3.0: What's new in the current version
24 Mar 2020	Release of Secure Web version 20.3.0	Secure Web 20.3.0: Bug fixes
11 Feb 2020	Release of Secure Hub for iOS version 20.2.0	Secure Hub 20.2.0: Bug fixes
11 Feb 2020	Release of Secure Mail version 20.2.0	Secure Mail 20.2.0: What's new in the current version
29 Jan 2020	Release of Secure Hub version 20.1.5	Secure Hub 20.1.5: Bug fixes
29 Jan 2020	Release of Secure Mail version 20.1.5	Secure Mail 20.1.5: What's new in the current version

DATE	CHANGE	DESCRIPTION
07 Jan 2020	Release of Secure Mail version 20.1.0	Secure Mail 20.1.0: What's new in the current version
12 Dec 2019	Release of Secure Hub version 19.12.5	Secure Hub 19.12.5: Bug fixes
12 Dec 2019	Release of Secure Mail version 19.12.5	Secure Mail 19.12.5: What's new in the current version
12 Dec 2019	Release of Secure Web version 19.10.5	Secure Web 19.12.5: Bug fixes
13 Nov 2019	Release of Secure Mail version 19.11.5	Secure Mail 19.11.5: What's new in the current version
13 Nov 2019	Release of Secure Web version 19.11.5	Secure Web 19.11.5: Bug fixes
06 Nov 2019	Release of Secure Hub version 19.11.5	Secure Hub 19.11.5: Bug fixes
22 Oct 2019	Release of Secure Mail for iOS version 19.10.6	Secure Mail for iOS 19.10.6: Bug fixes
15 Oct 2019	Release of Secure Mail version 19.10.5	Secure Mail 19.10.5: What's new in the current version
15 Oct 2019	Release of Secure Web version 19.10.5	Secure Web 19.10.5: Bug fixes
14 Oct 2019	Release of Secure Hub for Android version 19.10.5	Secure Hub 19.10.5: What's new in the current version
03 Oct 2019	Release of Secure Hub for iOS version 19.10.0	Secure Hub 19.10.0: Bug fixes
03 Oct 2019	Release of Secure Mail for iOS version 19.10.0	Secure Mail 19.10.0: What's new in the current version
03 Oct 2019	Release of Secure Web for iOS version 19.10.0	Secure Web 19.10.0: What's new in the current version

DATE	CHANGE	DESCRIPTION
01 Oct 2019	Release of Secure Mail for Android version 19.10.0	Secure Mail 19.10.0: What's new in the current version
01 Oct 2019	Release of Secure Web for Android version 19.10.0	Secure Web 19.10.0: What's new in the current version
24 Sep 2019	Release of Secure Hub for Android version 19.10.0	Secure Hub 19.10.0: Bug fixes
19 Sep 2019	Release of Secure Mail for iOS version 19.9.5	Secure Mail 19.9.5: What's new in the current version
19 Sep 2019	Release of Secure Web for iOS version 19.9.5	Secure Web 19.9.5: Bug fixes
17 Sep 2019	Release of Secure Mail for Android version 19.9.5	Secure Mail 19.9.5: What's new in the current version
17 Sep 2019	Release of Secure Web for Android version 19.9.5	Secure Web 19.9.5: What's new in the current version
11 Sep 2019	Release of Secure Hub for Android version 19.9.5	Secure Hub 19.9.5: What's new in the current version
04 Sep 2019	Release of Secure Mail version 19.9.0	Secure Mail 19.9.0: What's new in the current version
04 Sep 2019	Release of Secure Web version 19.9.0	Secure Web 19.9.0: What's new in the current version
03 Sep 2019	Release of Secure Hub version 19.9.0	Secure Hub 19.9.0: What's new in the current version
23 Aug 2019	Release of Secure Hub version 19.8.5	Secure Hub 19.8.5: What's new in the current version
23 Aug 2019	Release of Secure Mail for Android version 19.8.5	Secure Mail 19.8.5: Performance enhancements and bug fixes

DATE	CHANGE	DESCRIPTION
23 Aug 2019	Release of Secure Web for Android version 19.8.5	Secure Web 19.8.5: Performance enhancements and bug fixes
09 Aug 2019	Release of Secure Mail for Android version 19.8.0	Secure Mail 19.8.0: What's new in the current version
09 Aug 2019	Release of Secure Web for Android version 19.8.0	Secure Web 19.8.0: Performance enhancements and bug fixes
31 Jul 2019	Release of Secure Hub version 19.8.0	Secure Hub 19.8.0: What's new in the current version
02 Aug 2019	Release of Secure Mail for iOS version 19.8.0	Secure Mail 19.8.0: What's new in the current version
02 Aug 2019	Release of Secure Web for iOS version 19.8.0	Secure Web 19.8.0: Performance enhancements and bug fixes
18 Jul 2019	Release of Secure Hub version 19.7.5	Secure Hub 19.7.5: What's new in the current version
18 Jul 2019	Release of Secure Mail version 19.7.5	Secure Mail 19.7.5: What's new in the current version
18 Jul 2019	Release of Secure Web version 19.7.5	Secure Web 19.7.5: Performance enhancements and bug fixes
30 Jun 2019	Release of Secure Hub version 19.6.6 for iOS	Secure Hub for iOS 19.6.6: Performance enhancements and bug fixes
27 Jun 2019	List of new features for Secure Mail 19.6.5 for Android	Secure Mail 19.6.5: What's new in the current version

DATE	CHANGE	DESCRIPTION
27 Jun 2019	Release of Secure Web version 19.6.5	Secure Web 19.6.5: Performance enhancements and bug fixes
26 Jun 2019	Release of Secure Hub version 19.6.5	Secure Hub 19.6.5: known issues
17 Jun 2019	List of new features for Secure Mail 19.5.5 for iOS	Secure Mail 19.5.5: What's new in the current version
05 Jun 2019	Release of Secure Hub, Secure Mail, and Secure Web version 19.5.5 for Android	To understand the phased release process for Secure Mail and Secure Web, see Mobile productivity apps release timeline
23 May 2019	One-minute video on a Secure Mail draft sync feature for Android	Added a video on the drafts folder sync feature for Secure Mail for Android, released in version 19.5.0: Drafts folder auto-sync
08 May 2019	Release of Secure Hub version 19.5.0	Secure Hub 19.5.0 known and fixed issues
08 May 2019	Release of Secure Mail version 19.5.0	Secure Mail 19.5.0 fixed issues
08 May 2019	Release of Secure Web 19.5.0	Secure Web 19.5.0 fixed issues
05 Apr 2019	Release of Secure Hub version 19.3.5	Secure Hub 19.3.5 known and fixed issues
05 Apr 2019	Release of Secure Mail version 19.3.5	Secure Mail 19.3.5 fixed issues
05 Apr 2019	Release of Secure Web 19.3.5	Secure Web 19.3.5 fixed issues