



# MAM SDK

# Contents

|                                                   |    |
|---------------------------------------------------|----|
| MDX Toolkit                                       | 5  |
| Recent announcements                              | 5  |
| MAM SDK Non-compliant Device Behavior             | 7  |
| Data Protection                                   | 7  |
| Criteria                                          | 7  |
| Non-compliant Device Behavior                     | 8  |
| Non-compliant device behavior                     | 8  |
| MAM SDK policies for third-party apps for Android | 10 |
| App Network Access                                | 10 |
| Network access                                    | 10 |
| Exclusion List                                    | 10 |
| App Logs                                          | 11 |
| Default log output                                | 11 |
| Default log level                                 | 11 |
| Max log files                                     | 11 |
| Max log file size                                 | 11 |
| MAM SDK policies for third-party apps for iOS     | 12 |
| App Network Access                                | 12 |
| Network access                                    | 12 |
| Authentication                                    | 12 |
| App passcode                                      | 12 |
| Maximum offline period (hours)                    | 13 |
| App logs                                          | 13 |
| Default log output                                | 13 |
| Default log level                                 | 13 |
| Max log files                                     | 14 |

|                                     |    |
|-------------------------------------|----|
| Max log file size                   | 14 |
| Obscure the URLs in logs            | 14 |
| Block app logs                      | 14 |
| App interaction                     | 14 |
| Cut and Copy                        | 14 |
| Paste                               | 14 |
| Document exchange (Open In)         | 14 |
| Restricted Open-In exception list   | 15 |
| Inbound document exchange (Open In) | 15 |
| App URL schemes                     | 15 |
| App interaction (outbound URL)      | 17 |
| Allowed URLs                        | 17 |
| Compliance                          | 17 |
| Device passcode                     | 17 |
| Block jailbroken or rooted          | 17 |
| Non-compliant device behavior       | 17 |
| Erase app data on lock              | 18 |
| Active poll period (minutes)        | 18 |
| App update grace period (hours)     | 18 |
| App Restrictions                    | 19 |
| Block camera                        | 19 |
| Block Photo Library                 | 19 |
| Block mic record                    | 19 |
| Block dictation                     | 19 |
| Block location services             | 19 |
| Block SMS compose                   | 19 |
| Block iCloud                        | 20 |
| Block look up                       | 20 |

|                                                   |    |
|---------------------------------------------------|----|
| Block file backup                                 | 20 |
| Block AirPrint                                    | 20 |
| Block AirDrop                                     | 20 |
| Block Facebook and Twitter APIs                   | 20 |
| Obscure screen contents                           | 20 |
| Block 3rd party keyboards (iOS 11 and later only) | 20 |
| App geofence                                      | 21 |
| Center point longitude                            | 21 |
| Center point latitude                             | 21 |
| Radius                                            | 21 |
| MAM SDK document history                          | 22 |

# MDX Toolkit

---

The Mobile Device Experience (MDX) Toolkit is an app container technology that enhances the mobile device experience and lets you prepare apps for secure deployment with Citrix Endpoint Management™ by adding the following information to the apps:

- The code required to support mobile app management tasks, such as provisioning, custom authentication, per-app revocation, data containment policies, data encryption, and per-app virtual private networking
- Signed security certificates
- Policy information and other Endpoint Management settings

The MDX Toolkit can securely wrap apps created within your organization or third-party mobile apps.

## Recent announcements

- Apple has announced the end of support for apps using the UIWebView API to embed web content in the public app store starting December 2020. This change directly affects the Citrix® mobile productivity apps such as Secure Web and Secure Mail configured for the use of micro VPN in full tunnel mode. As part of this announcement, support for WKWebview for all Citrix mobile productivity apps is available with the release of 20.11.X.

### NOTE:

WKWebview does not support the Tunneled – Full VPN tunneling method. Customers using **Tunneled – Web SSO (Secure Browse)** as their microVPN will not be affected. Admins must switch tunneling methods to **Tunneled – Web SSO (Secure Browse)**.

- 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 toolkit is scheduled to reach end of life (EOL) in July 2023. To continue managing your enterprise applications, you must incorporate the MAM SDK.

For more details about the MAM SDK, see the Citrix Developer section on [Device Management](#). You can find more information as well in this [Citrix blog post](#).

The SDK is available for download when you sign on to [Citrix downloads](#).

# MAM SDK Non-compliant Device Behavior

---

A MAM SDK integrated application has a minimum compliance requirement that ensures that the application is safe to use by the end user. The minimum requirement is based on a set of criteria. If the criteria is not met, an administrator can decide what action the app takes by setting the **Non-compliant device behavior** policy. For more information, see [Non-compliant Device Behavior](#).

## Data Protection

When a MAM SDK integrated application is fully compliant, all the elements required to prevent data from unauthorized access or sharing with unauthorized agents are established. These elements include OS provided data encryption and access prevention.

## Criteria

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

Devices running iOS:

- **iOS 10.2:** An app is running on an operating system version that is greater than or equal to the required minimum version. Upgrading the device OS to the minimum or greater version will prevent this criteria from failing.
- **Debugger access:** An app does not have a debugger attached nor is the installed app a debug build. Ensure that the distributed app is a release build, built with a Distribution Profile and that no debugger is attached to the app to prevent this criteria from failing.
- **Jailbroken device:** An app is not running on a jailbroken device. This criteria is only evaluated if the admin has enabled the **Block jailbroken or rooted** policy.
- **Device passcode:** Device passcode is **ON**. This criteria is evaluated only if the admin has enabled the **Device Passcode** policy. The user can also enable Face ID or Touch ID on the device to prevent this criteria from failing.
- **Data sharing:** Data sharing is not enabled for the app. The app developer must set `UISupportsDocumentBrowser`, `UIFileSharingEnabled`, and `LSSupportOpeningDocumentsInPlace` keys to **NO**, or ensure that the keys are not present when specifying Bundle Information Properties for the app.

- **URLs in Logs Obfuscated:** The **Obscure the URLs in Logs** policy is enabled by the admin.

Devices running Android:

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

## Non-compliant Device Behavior

When a device falls below the minimum compliance requirements, the **Non-compliant device behavior** policy allows the admin to select the action to take:

- **Allow app:** Allow the app to run normally. The MAM SDK ignores the failure in compliance. No warning message appears to the user. This mode is not recommended, but can be used in limited distribution scenarios such as when an application is being actively developed and tested.
- **Allow app after warning:** Warn the user that an app does not meet the minimum compliance requirements and allows the app to run. This setting is the default value. This mode is not recommended for final production level applications.
- **Block app:** Block the app from running. This mode is recommended for final production level applications distributed to a wide audience.

## Non-compliant device behavior

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

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

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

## Devices running iOS:

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

## Devices running Android:

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

# MAM SDK policies for third-party apps for Android

---

This article describes the MAM SDK policies for Android third-party apps. You can change policy settings in the Citrix Endpoint Management™ console.

## 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:** Networking APIs used by your app fails. Per the previous guideline, you should 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.

### Exclusion List

Comma-delimited list of FQDNs or DNS suffixes to be accessed directly instead of through a VPN connection. This 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 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 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**. Default value is **2**.

## Max log file size

Limits the size in megabytes (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.

# MAM SDK policies for third-party apps for iOS

---

This article describes the MAM SDK policies for third-party iOS apps. You can change policy settings directly in the policy XML files or in the Citrix Endpoint Management™ console when you add an app.

## 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:** Networking APIs used by your app fails. Per the previous guideline, you should 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.

## 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 without reconfirming app entitlement and refreshing policies from Citrix Endpoint Management. At expiration, log on to the server may be triggered if needed. Default value is **168** hours (7 days). Minimum period is **1** hour.

## 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 megabytes (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.

## Obscure the URLs in logs

If **On**, intercepts and redirects system or console logs from an app to the Mobile Productivity Apps diagnostic facility. If **Off**, app use of system or console logs is not intercepted.

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 may be collected by using the Secure Hub email support feature. Default value is **Off**.

## 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 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 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 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 app can share documents with this comma-delimited list of unmanaged app IDs, 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 MAM SDK 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 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.

### NOTE:

The Inbound Document Exchange Whitelist policy only supports devices running on iOS 12.

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 should be formatted as a comma-separated list of patterns in which each pattern may be preceded by a plus "+" or minus "-". Inbound URLs are compared against the patterns in the order listed until a match is found. Once matched, the action taken is dictated by the prefix.

- 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                                                      |
|-------------------|----------------------------------|--------------------------------------------------------------|
| ctxmobilebrowser  | Secure Web-                      | Permit Secure Web to handle HTTP: URLs from other apps.-     |
| ctxmobilebrowsers | Secure Web-                      | Permit Secure Web to handle HTTPS: URLs from other apps.     |
| ctxmail           | Secure Mail-                     | Permit Secure Mail to handle mailto: URLs from other apps.   |
| COL-G2M           | GoToMeeting-                     | Permit a wrapped GoToMeeting app to handle meeting requests. |
| ctxsalesforce     | Citrix® for Salesforce-          | Permit Citrix for Salesforce to handle Salesforce requests.  |
| wbx               | WebEx                            | Permit a wrapped WebEx app to handle meeting requests.       |

## App interaction (outbound URL)

### 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 should be formatted as a comma-separated list of patterns in which each pattern may 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 action taken is dictated by the prefix. 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 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.

## Compliance

### 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**.

### 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**.

### 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**.

## 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 MAM SDK 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 may be affected.

## 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:**

Using a value of 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 might lead to a situation where the user is forced to exit the app (potentially losing work) to comply with the required update.

## 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 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 look up

If **On**, prevents an app from using the Look Up 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 data files from being backed up by iCloud or iTunes. 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 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**.

## 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.

Should be expressed in signed degrees format (DDD.dddd), for example "-31.9635". West longitudes should 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.

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

### Radius

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

Should 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).

# MAM SDK document history

---

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

| DATE        | CHANGE                                                                                 | DESCRIPTION                                                   |
|-------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------|
| 02 Nov 2020 | Added a note that apps no longer need to be wrapped if you have switched to MAM SDKs   | <a href="#">MAM SDK overview</a>                              |
| 01 Jul 2020 | Added more information about the MAM SDK to the newly created MAM SDK overview article | For more information see the <a href="#">MAM SDK overview</a> |