

MDM Solutions

Android

Manage MX Connect from MDM

The App Config community (appconfig.org) is formed to standardize the way devices and applications can be managed in enterprise environments. It makes possible for companies to manage their (large) fleet of devices and the applications that run on them in a centralized fashion using any of the MDM/EMM solutions that are part of the community. Apps that are manageable this way define a schema that contains the configurable properties and appear in the Managed Google Play Store (also called Google Play for Work Store). This Managed Google Play Store is only accessible by users of registered Organizations. All apps can be accessed through it from the normal Google Play Store but there are ones that are only visible in this specialized Store. Android devices that want to use managed apps in compliance with app config need to be set up with Android Work Profile enabled and apps need to be installed through the Managed Google Play Store (there is no way to configure apps that are installed using another method). An Organization in the Managed Google Play Store can be bound to a third party MDM/EMM solution and apps that are distributed to the devices managed by the MDM/EMM need to be first approved by the Organization's admin to appear in the Play Store app on the device. They can be installed as a mandatory app (so that they are installed automatically) or optional (the user of the phone can choose to install it).

Cognex provides support for App Config standard with its MX-series devices and compatible apps starting with remote Firmware Update and Config Upload for MX Terminals through the MX Connect application. With the App Configuration capability (see Terminology and Definitions) the MDM administrator can specify which Firmware and Config should be applied to a device or group of devices. When these are specified MX Connect will apply the Firmware Update and/or Config Upload after it is synchronized to the Android device and when it is connected to the MX Terminal (see steps below).

Please note that we support a different method for updating the Firmware and uploading a Config for MX Terminals using *Intents*, but that is not supported by every MDM that supports App Config (ex. SOTI supports Intents but MobileIron don't), and *cannot be used together* with it. Intents can be used more like *commands*: you can start a Firmware Update or Config Upload by sending an Intent to a specific device. App Config on the other hand (as its name suggest) is a *configuration*: you can specify with it which devices should have which firmware and config and they will be applied at some point automatically (if necessary). Using App Config for Firmware Update and Config Upload is the preferred way due to its simplicity.

Terminology and Definitions

The following terms are used throughout this document:

- **MX Mobile Terminal:** The MX barcode reader device, for example, MX-1502.
- **Android device:** Android smartphone inside the MX Mobile Terminal.
- **Firmware:** The firmware of the MX Mobile Terminal.
- **MX configuration:** The configuration of the MX Mobile Terminal.
- **MDM:** Mobile Device Management referring to an MDM solution, for example, SOTI or MobileIron.
- **EMM:** Enterprise Mobility Management, same as MDM (different terminology).
- **App Config (Community):** A community comprising of different OEMs, MDM/EMM vendors and app developers
- **App Config (Standard):** A standard, created by the similarly named community in order to standardize the way devices and applications managed in enterprise environments. It defines several capabilities that participant MDMs and OEMs can implement (implementing different capabilities are optional, and implementation details can differ as long as they respect the standard).
- **App Configuration capability:** The capability of the App Config standard that defines how enterprise applications should be managed from MDM by defining properties that are defined on the MDM side and influence the app's behavior. The developer of the applications need to define the properties.
- **Android (for) Enterprise / Android for Work:** It has different names but basically the Android OS's features for Enterprise users, comprising Managed Configurations/App Restrictions.
- **Android Work Profile:** Android devices enrolled to Android for Work (either directly, or through a third party MDM/EMM solution) are set up with Work Profile that is basically a separate part of the system consisting of apps and data that are managed by the enterprise. It is separated from personal apps and data and can be accessed from a dedicated UI of the phone. Apps that are installed to Work Profile can be managed via App Config from MDM/EMM solutions.
- **Managed Google Play Store / Google Play for Work Store:** The variant of the Google Play Store (the official application store for Android) meant for Enterprise users. You need to have an Organization registered in this Store to be able to use Managed Google Play Applications. This store is a *superset* of the normal Google Play Store so every normal Google Play app appears in the Managed Play Store / Google Play for Work Store but they may be manageable (ex. contain App Config features) and additional apps that are meant to be used in Enterprise environments can be accessed from there. An Organization can also have private applications in this store that only they can access.
- **Managed Google Play Applications:** The apps that appear on the Managed Play Store / Google Play for Work Store.

- **Managed Configurations:** The Android implementation of the App Config standard's App Configuration capability, provides features to manage enterprise applications from MDM.
- **App Restrictions:** Older, no longer used name for Managed Configurations on Android.

Preparation Steps

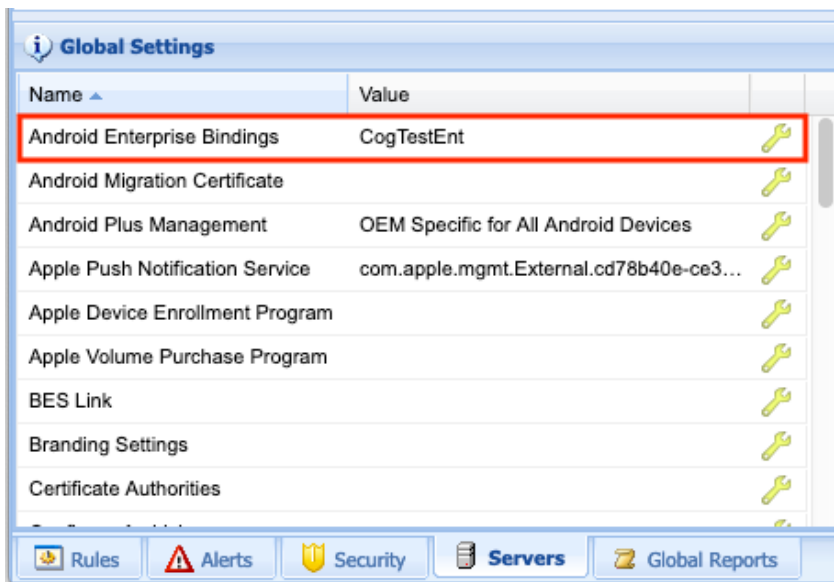
1. Register an Organization in the Managed Google Play Store (Google Play for Work Store) using Google's Managed Enterprise Enrollment page and create a binding between it and the MDM/EMM solution you use

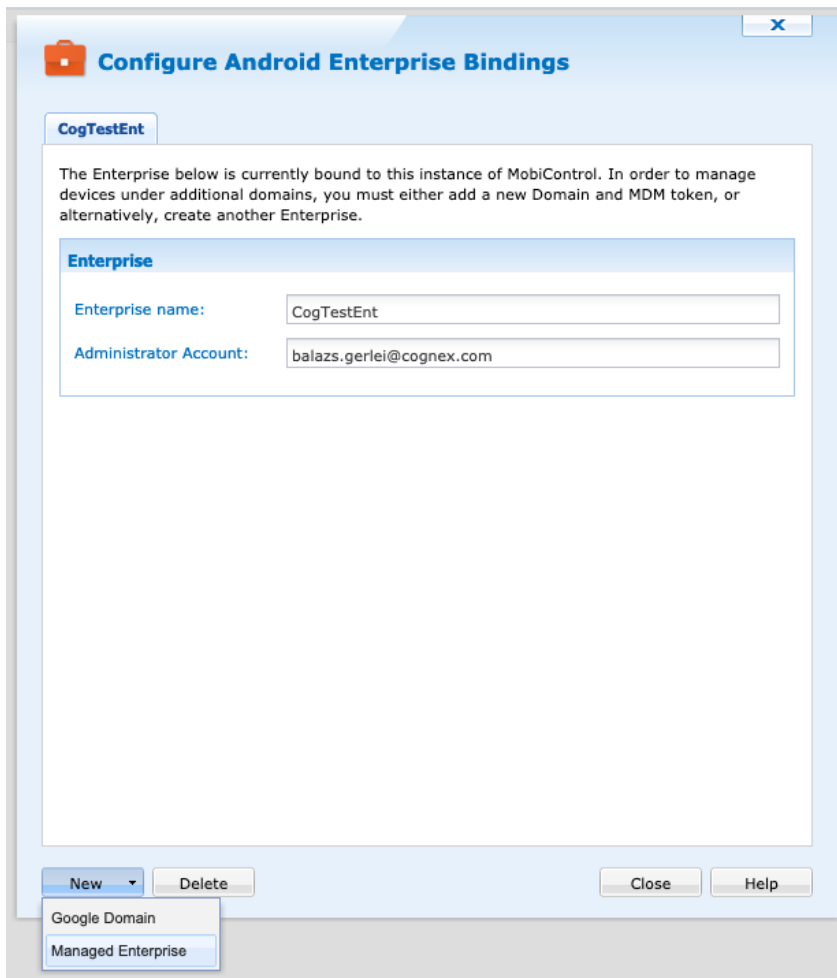
To register your organization, start from the MDM/EMM you are using and start adding the binding. You will need at least one Google Account that is *registered to Manage your business* (not a personal account).

Please note, that one Organization can only be bound to one MDM/EMM at a time.

- [SOTI](#)
- [MobileIron](#)

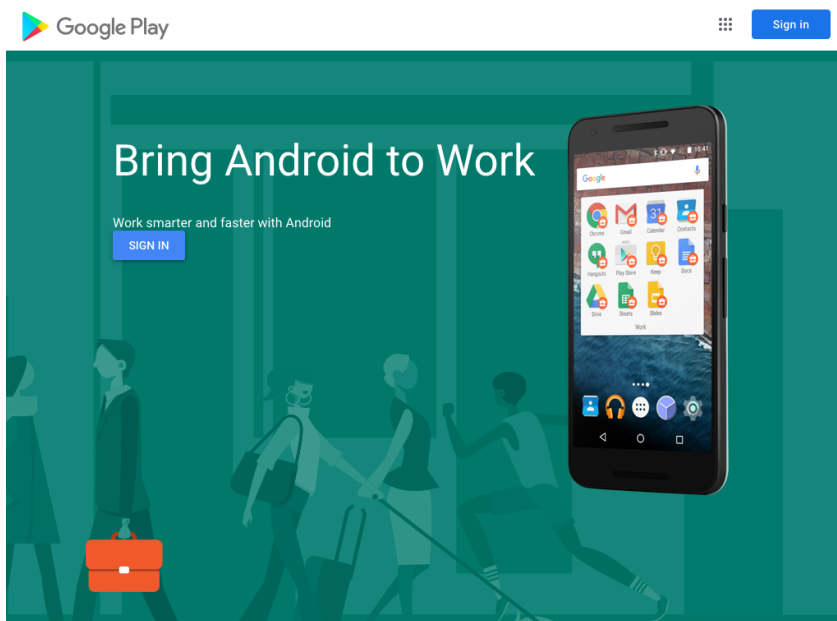
SOTI can be bound to multiple Organizations in the Managed Play Store (but one Organization still can only be bound to one MDM/EMM at a time). You can manage these Android Enterprise Bindings under Servers / Global Settings. You need to add a New Managed Enterprise.

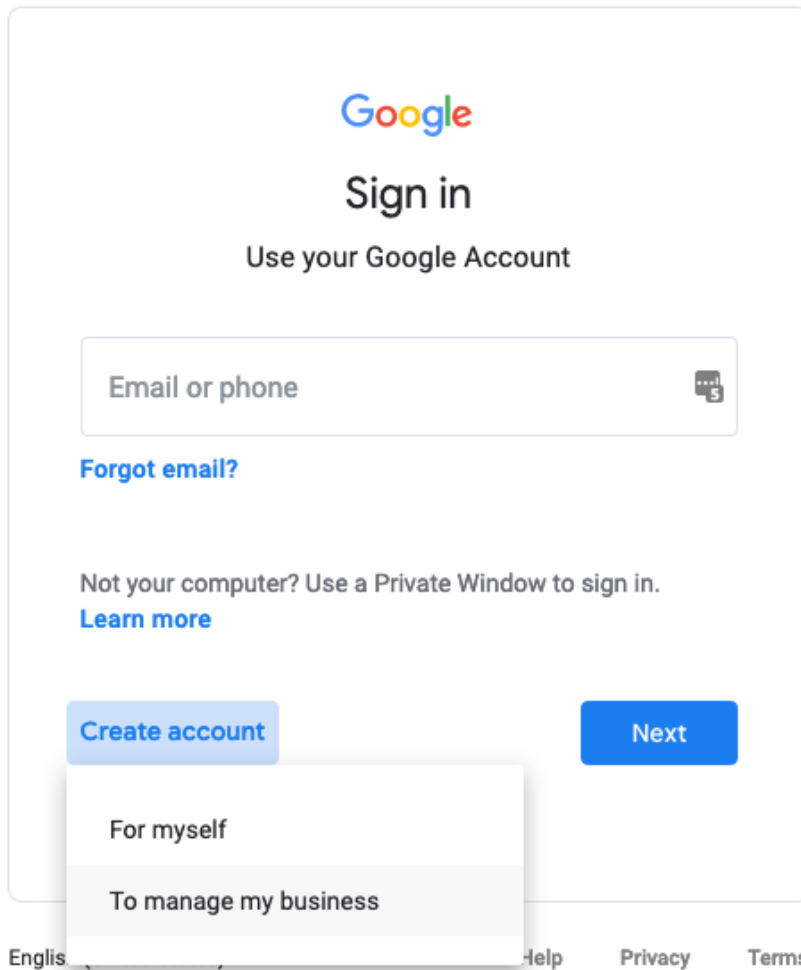




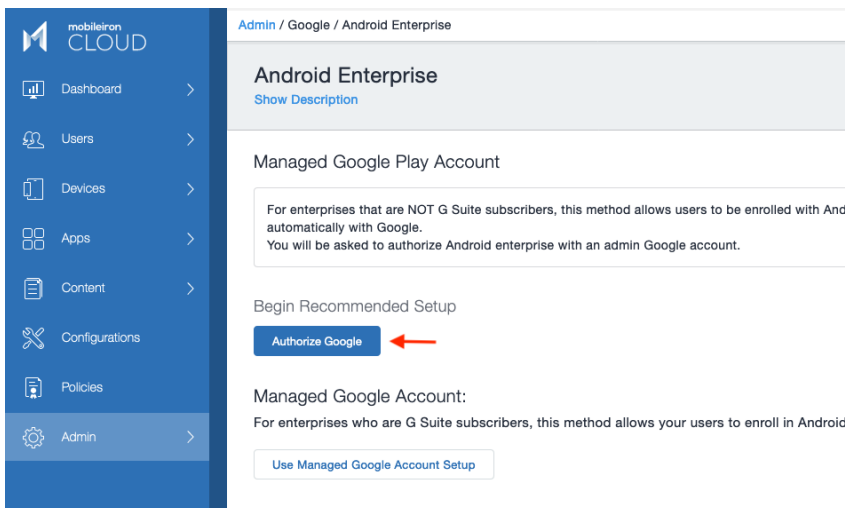
If you already registered your Organization you just need to sign in with one of the administrator accounts for that Organization, or you can register a new Google Account (remember to choose "To manage your business" as the reason for creating an account). If you register a new account and a new Organization, this new administrator account will also be the Owner of the Organization, but you can add more administrator accounts later and you can also change the owner too (the Owner account can designate another administrator as the new Owner).

You need to finish the steps on Google's page so the binding between your Organization and MobileIron is created.



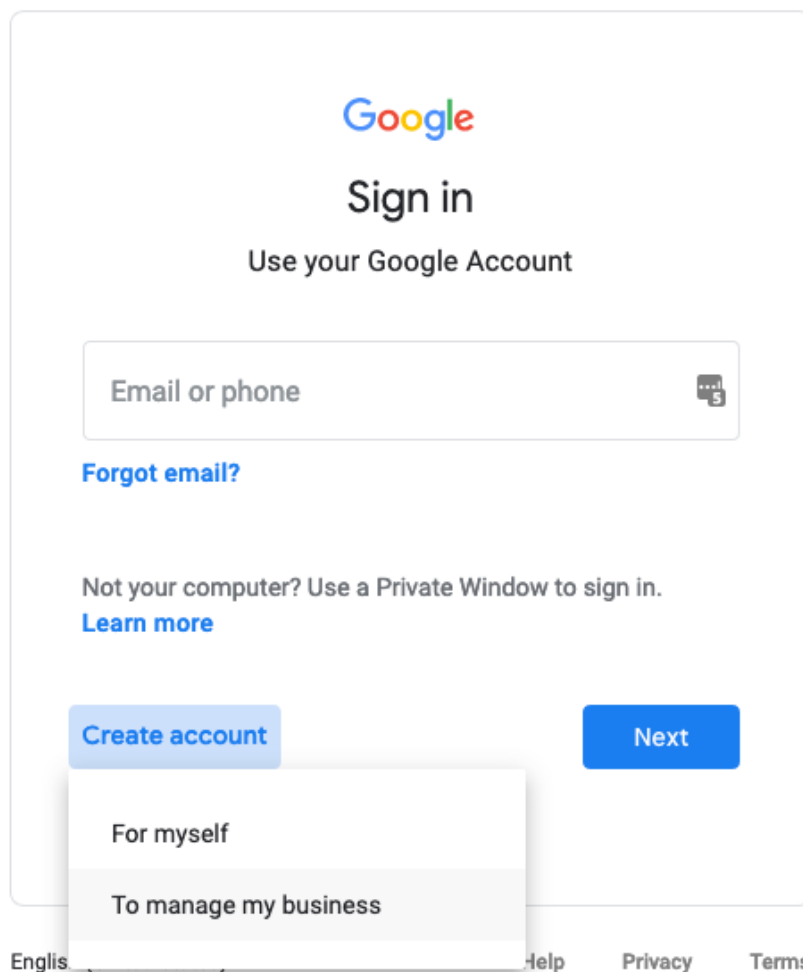
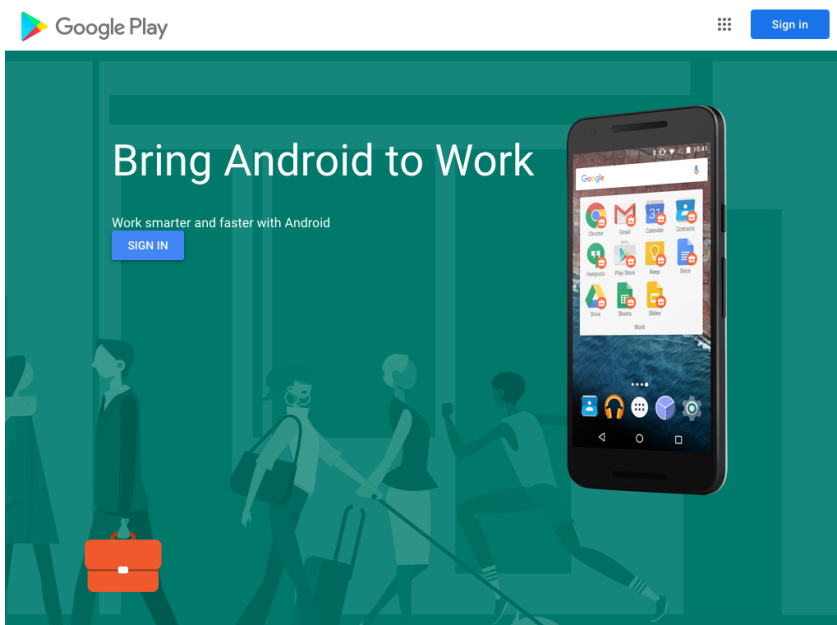


To create a binding and register your Organization in the Managed Google Play Store, you need to go to Admin / Google / Android Enterprise menu of MobileIron. You can begin the recommended setup by clicking on the Authorize Google button.



If you already registered your Organization you just need to sign in with one of the administrator accounts for that Organization, or you can register a new Google Account (remember to choose "To manage your business" as the reason for creating an account). If you register a new account and a new Organization, this new administrator account will also be the Owner of the Organization, but you can add more administrator accounts later and you can also change the owner too (the Owner account can designate another administrator as the new Owner).

You need to finish the steps on Google's page so the binding between your Organization and MobileIron is created.



2. Enroll your Android device with your MDM/EMM and set up Work Profile to use the Managed Play Store)

- SOTI
- MobileIron

With SOTI, you need to decide at the time of enrollment whether you want to use the Managed Play Store and set up a Work Profile on a particular device. So in order to use App Config, you need to Enroll your device into SOTI in a different way than other, non-managed devices. Once you enrolled a device, you can only remove or set up Work Profile again by re-enrolling it.

To Enroll a device to use the Managed Play Store and set up Work Profile, you need to create a new Add Device Rule for Android Plus devices and in the Android Enterprise step, you need to select Managed Google Play Accounts and select your Organization (that is bound to SOTI) from the dropdown. Finish creating the Add Device Rule with the options you want to use and use this Rule when Enrolling your devices so the Work Profile will be set up on them so MX Connect will available to them in the Managed Play Store.

Create Add Devices Rule

Android Enterprise Setup

For Access to the Managed Google Play Store, choose which method to use to Manage the Android Devices enrolling using this Add Device Rule. If access to the Managed Google Play Store is not required, you do not need to modify any of the options below and can continue with the Add Device Rule Creation.

☒ Managed Google Play Accounts
Available Enterprises:

☐ Managed Google Accounts
Manage the Devices using Google Accounts created in the Google Admin Portal ([Admin.Google.Com](https://admin.google.com))

☐ Skip Google Account Addition During Enrollment on Managed Android Devices

Back Next Cancel Help

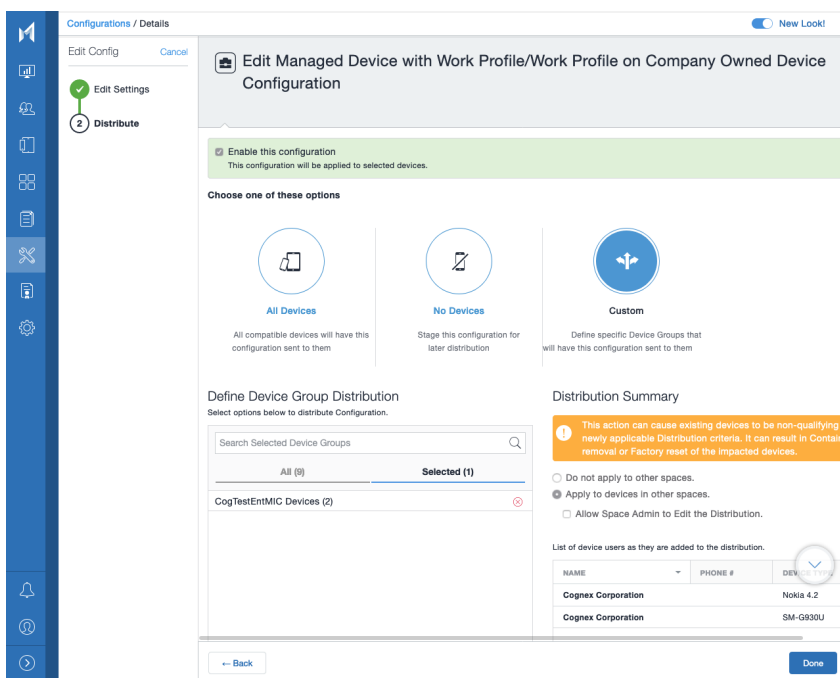
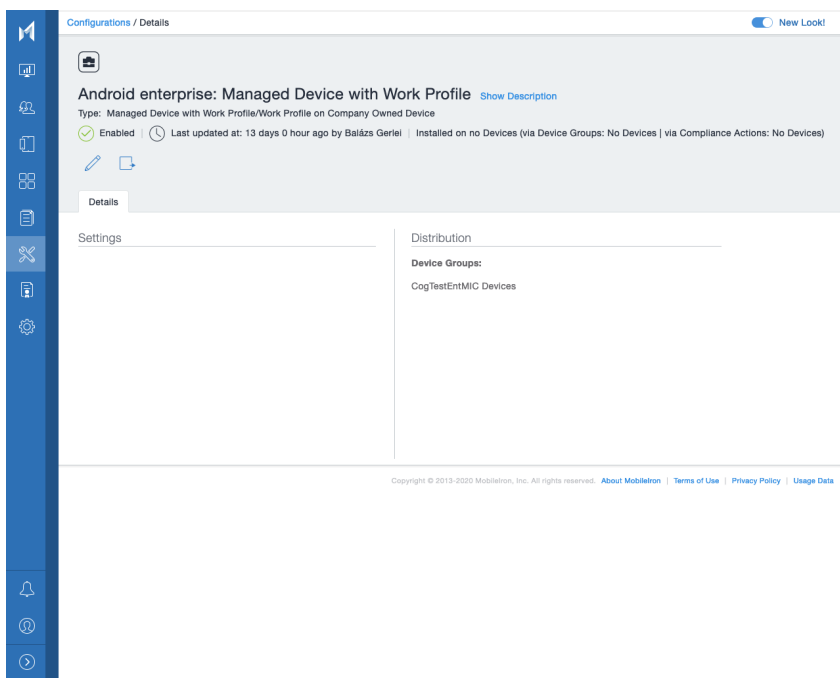
MobileIron does not require you to enroll a device in any special way if you want to use the Managed Play Store and setup Work Profile on it, but you need to add the device to a Device Group that the appropriate Configuration is distributed to. You can add or remove a device at any point (without re-enrolling it) to remove and setup Work Profile again.

After the devices are Enrolled, you need to Distribute the "Android enterprise: Managed Device with Work Profile" Configuration to them. This Configuration should be created by the system and you can distribute it to individual Devices or Device Groups (recommended). Once you Distributed this Configuration to devices, Work Profile can be set up on them, but you need to do some additional steps on the device(s) themselves so the setup completes. Once that is done, they are able to use the Managed Play Store and MX Connect can be used with Managed Configurations on them.

STATUS	NAME	UPDATED	TYPE
✓	App Catalog for Android	83 days 7 hours ago by System	Android App Catalog
✓	Default Android AppConnect Configuration	439 days 22 hours ago by System	Android AppConnect (Priority: 2001)
✓	Android enterprise: Work Profile (Android for Work)	164 days 0 hour ago by System	Android enterprise (Android for Work)
✓	Default App Runtime Permissions	439 days 22 hours ago by System	Default App Runtime Permissions (Priority: 2001)
✓	Android enterprise: Work Managed Device (Android for Work)	13 days 0 hour ago by System	Work Managed Devices (Device Owner)
✓	Android enterprise: Managed Device with Work Profile	13 days 0 hour ago by System	Managed Device with Work Profile/Work Profile on Company Owned Device
✓	Default iOS AppConnect Configuration	377 days 2 hours ago by System	iOS AppConnect (Priority: 2001)
✓	MX Connect SAM mode	378 days 20 hours ago by System	Single App Mode (Priority: 1001)
✓	MobileIron Agent CA Certificate	439 days 22 hours ago by System	Certificate
✓	Apps@Work for macOS	419 days 14 hours ago by System	Client Services
✓	Android Notification Service	439 days 22 hours ago by System	Client Services
✓	App Catalog Service	439 days 22 hours ago by System	Client Services
✓	Android AppConnect Passcode Service	439 days 22 hours ago by System	Client Services
✓	GMail	439 days 22 hours ago by System	Email
✓	Identity for Windows enrollment	439 days 22 hours ago by System	Identity Certificate (Dynamically Generated)

Showing 1 to 39 of 39

Copyright © 2019-2020 MobileIron, Inc. All rights reserved. [About MobileIron](#) | [Terms of Use](#) | [Privacy Policy](#) | [Usage Data](#)

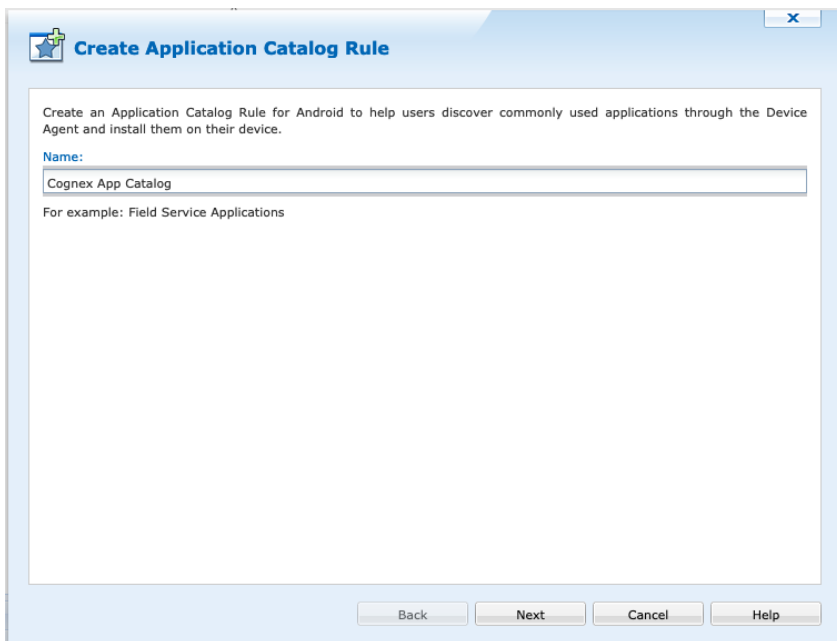
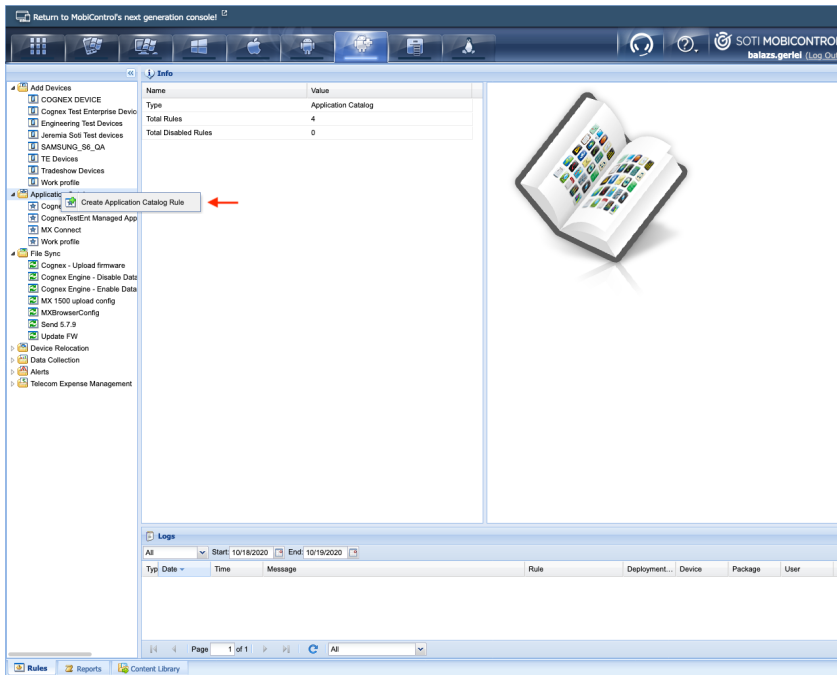


3. Approve the MX Connect app in the Managed Play Store for use in your Organization

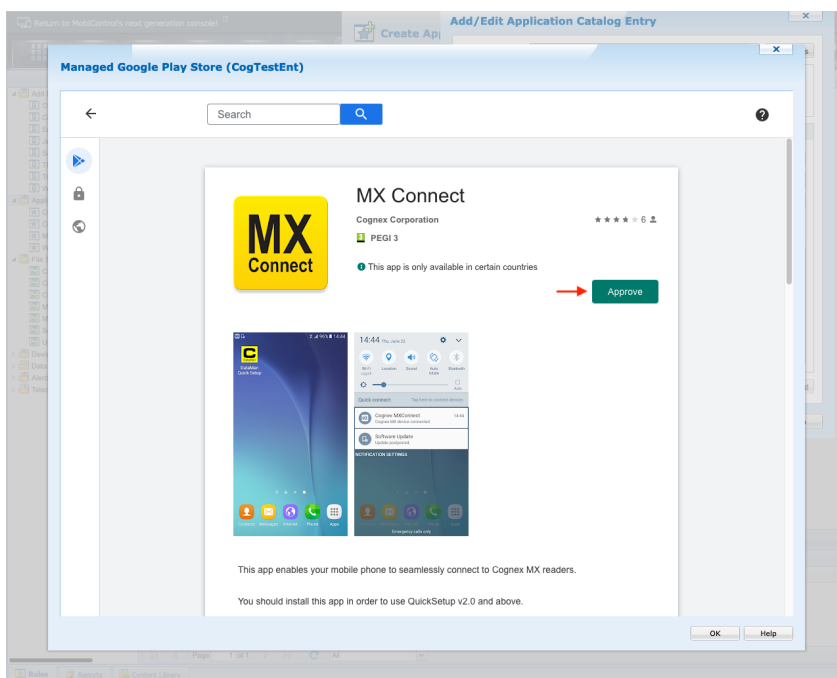
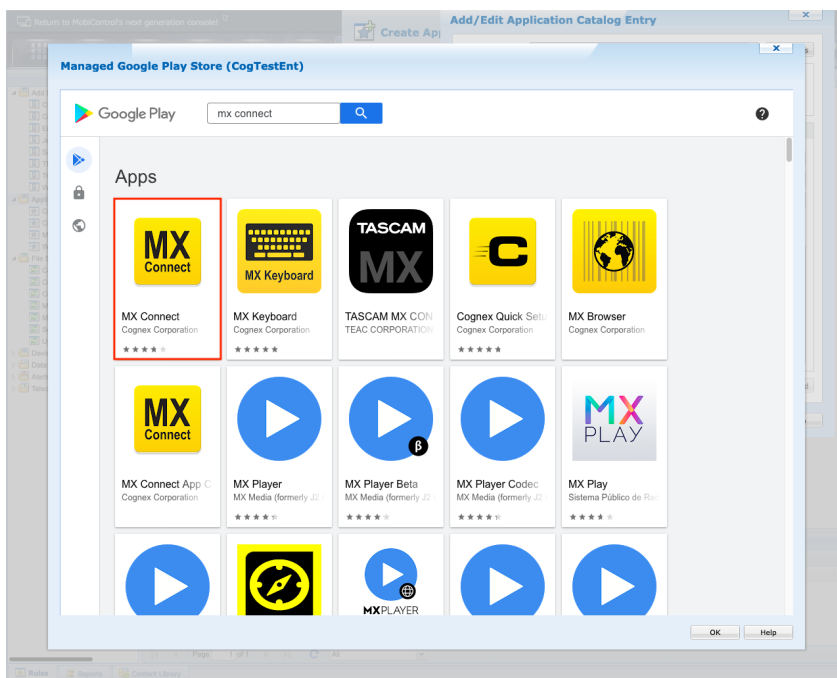
- [SOTI](#)
- [MobileIron](#)

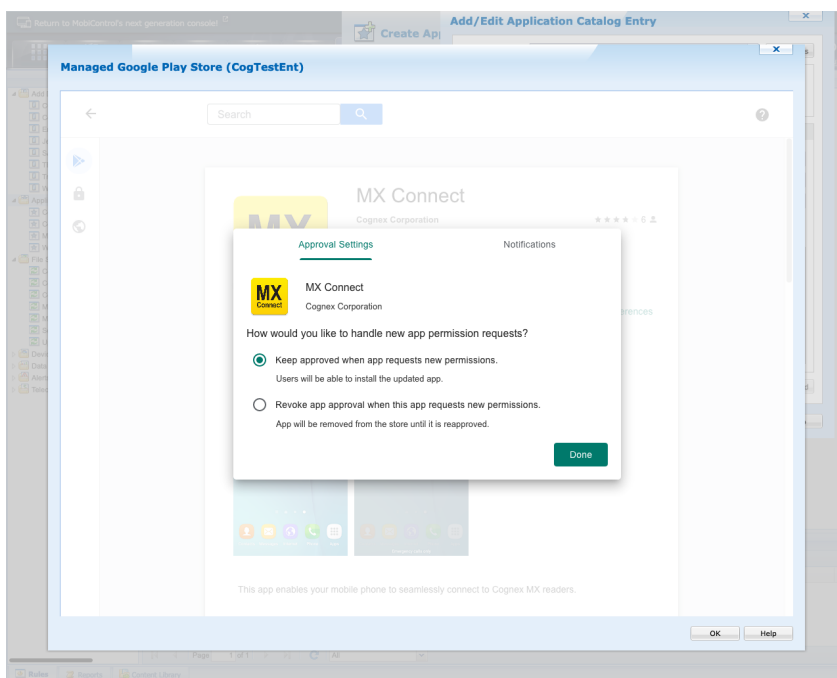
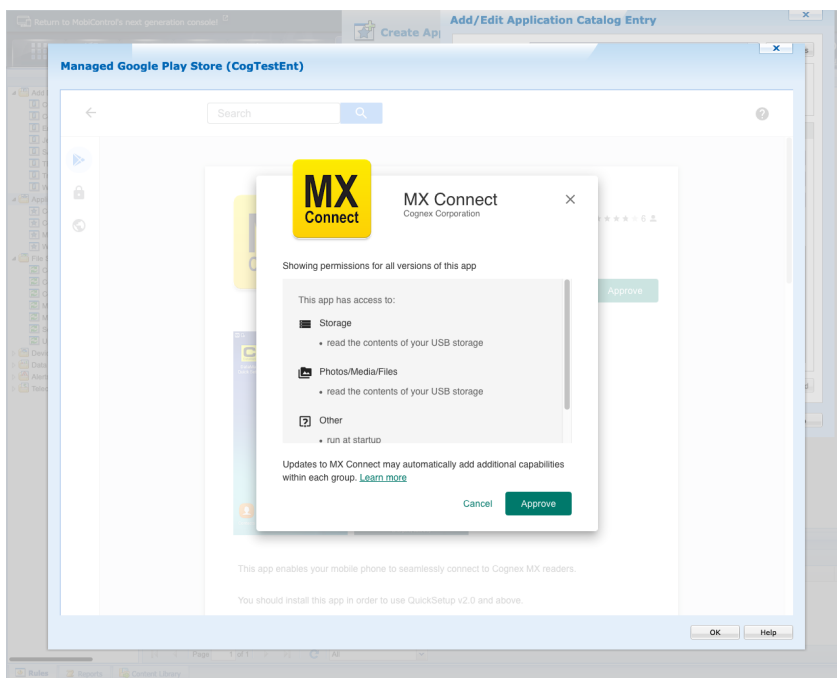
To be able to install MX Connect with SOTI and use App Configurations, it need to be approved it in the Managed Play Store itself by an administrator. MX Connect can be approved from its product page in the Managed Play Store.

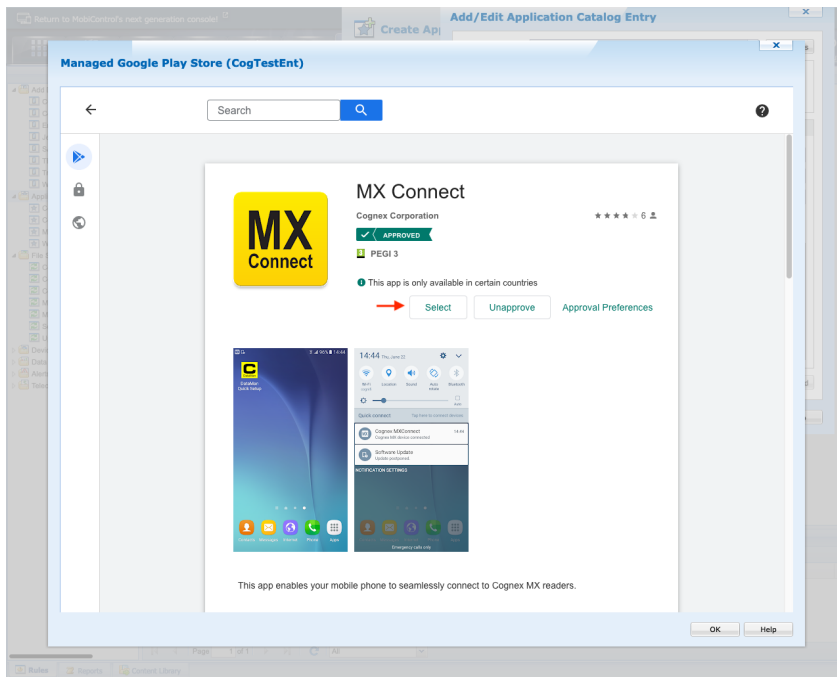
If you do not already have one (where you want to add MX Connect to) you need to Create a new Application Catalog Rule (you can do that from the menu that appears when right clicking on the Application Catalog header under Rules for Android Plus) and add MX Connect from Google Play (or alternatively you can log in directly to the Managed Google Play Store and Approve MX Connect from there).



You need to search for MX Connect and before you can successfully add it to the Application Catalog Rule, you need to Approve it.

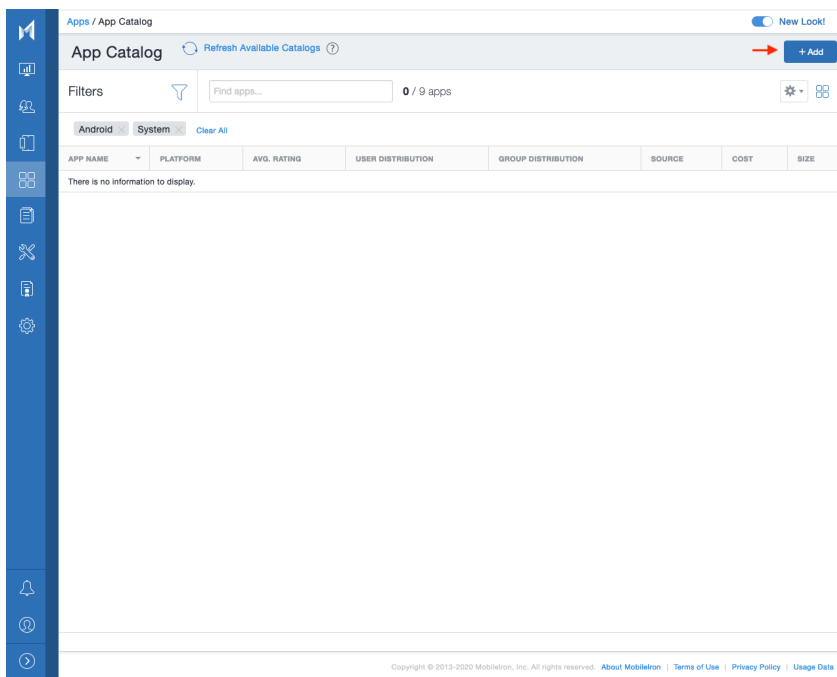




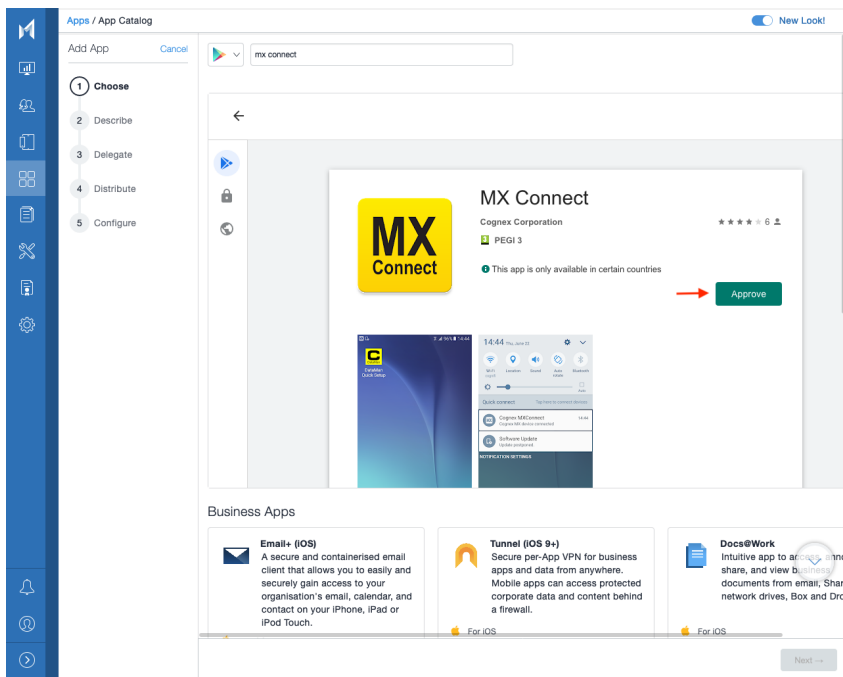
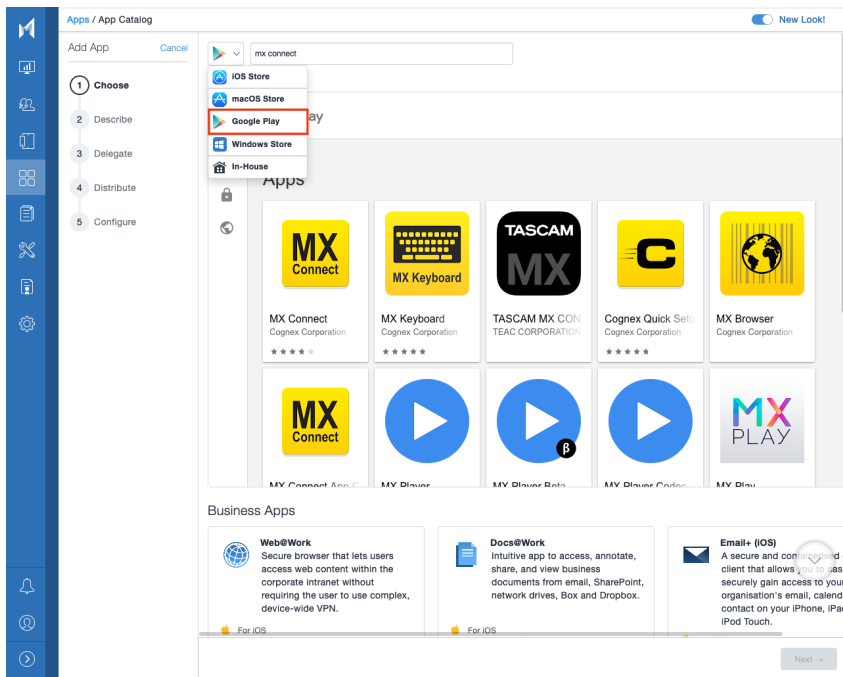


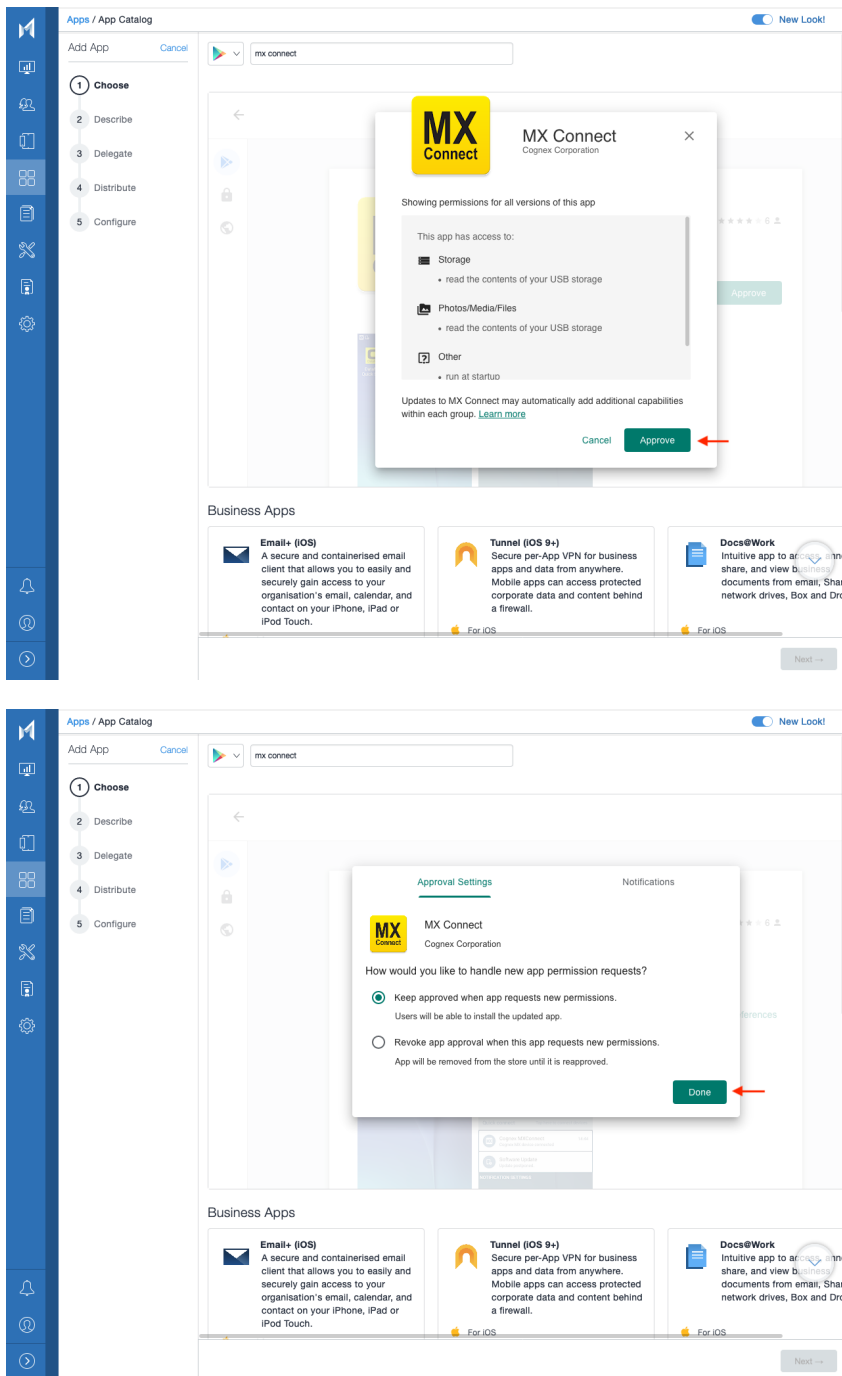
To be able to install MX Connect with MobileIron and use App Configurations, it need to be approved it in the Managed Play Store itself by an administrator. MX Connect can be approved from its product page in the Managed Play Store.

You need to start with Adding a new app to Mobile Iron App Catalog from Google Play (or alternatively you can log in directly to the Managed Google Play Store and Approve MX Connect from there).

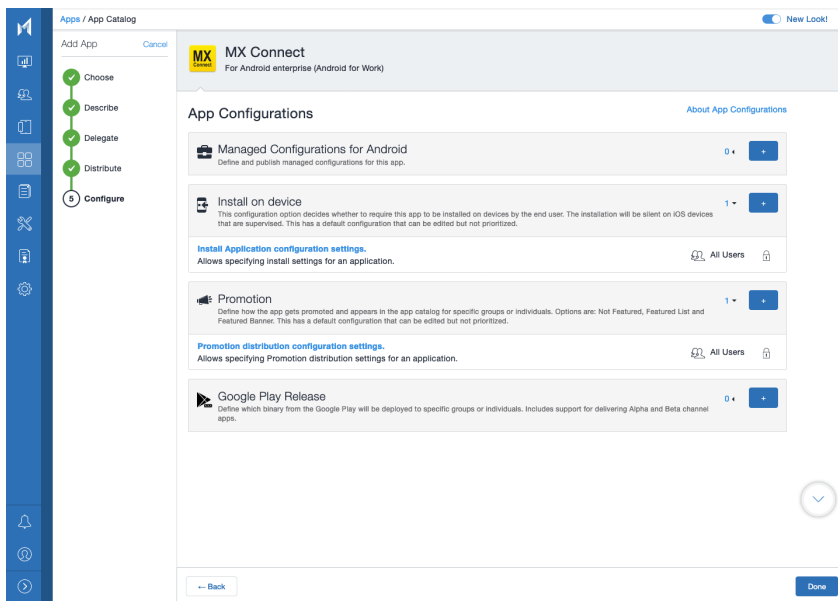
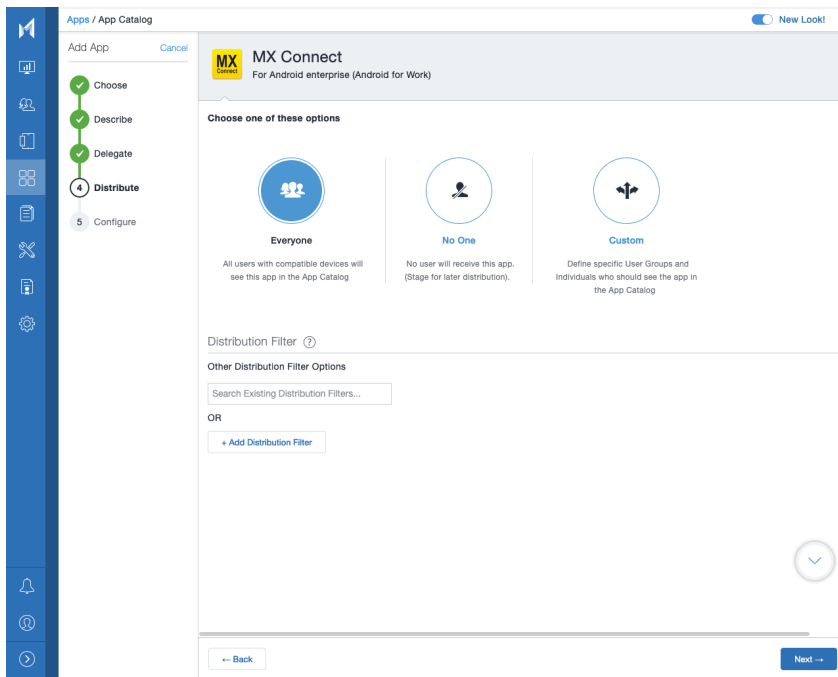


You need to search for MX Connect and before you can successfully add it to the App Catalog, you need to Approve it





You can distribute the app during the Add steps (in that case you do not need to do Step 4) and add a Managed Configuration to it too (in that case you do not need Step 5 either), but you can also do it later in separate steps.



4. Install MX Connect from the Managed Play Store

- [SOTI](#)
- [MobileIron](#)

After you approved it, you can install MX Connect from the Managed Play Store by adding it to an Application Catalog Rule. In order to have MX Connect appear in SOTI you may need to manually Sync Apps.

After you approved it, you can install MX Connect from the Managed Play Store from the App Catalog of MobileIron by setting its Distribution. In order to have MX Connect to appear in MobileIron you may need to manually Refresh Available Catalogs.

APP NAME	PLATFORM	AVG. RATING	USER DISTRIBUTION	GROUP DISTRIBUTION	SOURCE	COST	SIZE
MX Connect 1.3.1 (88)	Android	*****	0	1	Public	FREE	2.00 MB

Once the MX Connect App shows up in the Catalog, you need to Distribute it to the Users or User Groups that needs to use it.

Apps / App Catalog / Details New Look!

MX Connect  Not available | Delegation Status: App is not delegated

[Details](#) [Distribution](#) [App Configurations](#) [Reviews](#) [App Config Feedback](#)

[Edit](#)

App Information

Package ID: com.cognex.mxconnect **Category:** Tools
Size: 2.00 MB **Avg. Rating:** ★★★★★
Source: Public **Compatibility:** Compatible with Android
Cost: FREE
Date Modified: 10/4/20 7:00 AM by System
Date Created: 4/29/20 11:47 AM by 
Minimum OS Version Required: 4.4

App Delegation 

☐ Delegate this app to all spaces
☒ Do not delegate this app

What's New

Improve overall stability before raising minimum supported Android version to 5.0

Description

This app enables your mobile phone to seamlessly connect to Cognex MX readers.
 You should install this app in order to use QuickSetup v2.0 and above.
[More...](#)

Screen Shots

Copyright © 2019-2020 MobileIron, Inc. All rights reserved. [About MobileIron](#) | [Terms of Use](#) | [Privacy Policy](#) | [Usage Data](#)

Apps / App Catalog / Details New Look!

MX Connect  Not available | Delegation Status: App is not delegated

[Details](#) [Distribution](#) [App Configurations](#) [Reviews](#) [App Config Feedback](#)

[Cancel](#) [Save](#)

App Distribution

Choose one of these options


Everyone
 All users with compatible devices will see this app in the App Catalog


No One
 No user will receive this app. (Stage for later distribution).


Custom
 Define specific User Groups and Individuals who should see the app in the App Catalog

Select below to distribute this app

Users **User Groups**

Search User Groups 

All (3) **Selected (0)**

☐ MX Connect App Config Testers (1)
☐ Group A (0)
☐ Group B (0)

App Distribution Summary

This app will be sent to:

 **0 Individual Users**
 **0 User Groups**

Distribution Filter 

Other Distribution Filter Options

Search Existing Distribution Filters...

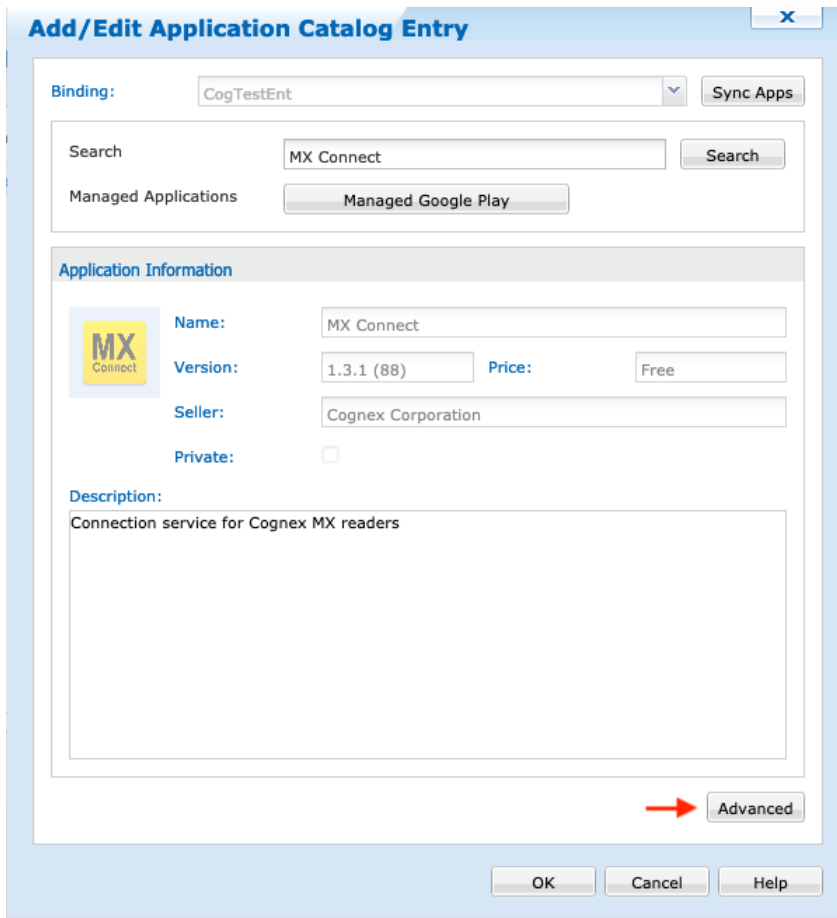
OR

[+ Add Distribution Filter](#)

5. Create a Managed Configuration / App Configuration for MX Connect

- [SOTI](#)
- [MobileIron](#)

When you add MX Connect to an Application Catalog Rule, you can also set the App Configuration values under Advanced settings for it.



Add/Edit Application Catalog Entry

Binding: CogTestEnt Sync Apps

Search: MX Connect Search

Managed Applications: Managed Google Play

Application Information

 Name: MX Connect

Version: 1.3.1 (88) Price: Free

Seller: Cognex Corporation

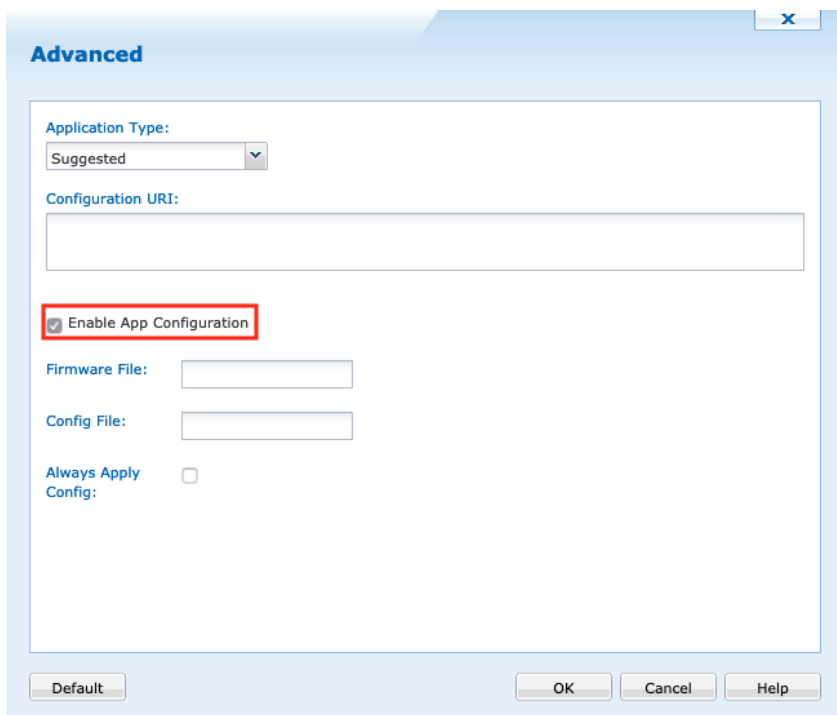
Private: ☐

Description: Connection service for Cognex MX readers

→ **Advanced**

OK Cancel Help

On the Advanced page you can select whether the app will be Mandatory installed (recommended) to every devices that are targeted by this Rule, or will be only Suggested to the users. If you use the second option, MX Connect needs to be manually installed on the Android device from the Managed Play Store.



Advanced

Application Type: Suggested

Configuration URI:

☒ **Enable App Configuration**

Firmware File:

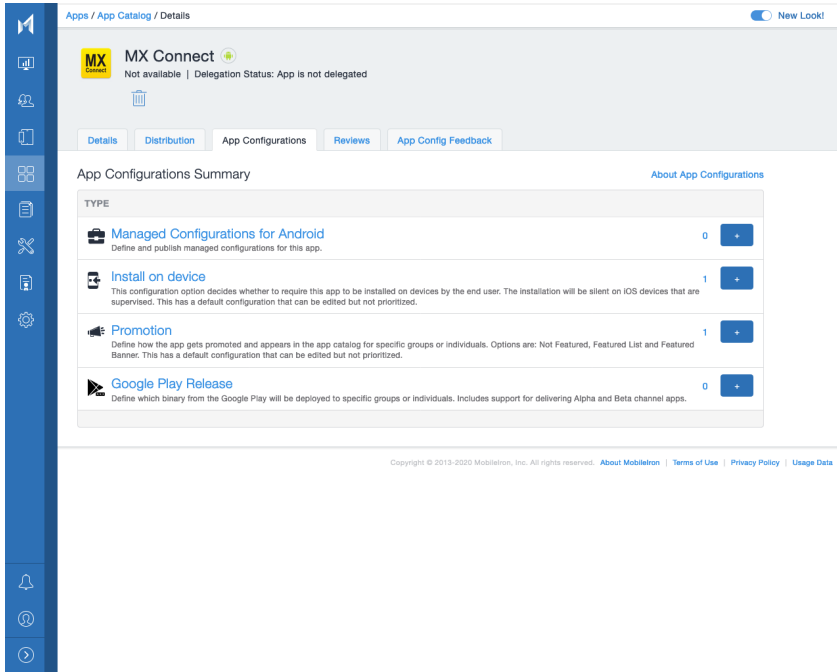
Config File:

Always Apply Config: ☐

Default OK Cancel Help

The App Configuration will be applied when MX Connect will be installed on the devices that are targeted by the Rule. You can change these App Config values later and after the Rule gets synced they will be applied on the device too.

With MobileIron you can create multiple, named App Configurations for an app, and you can distribute them in several ways: to specific users, user groups or all users that have the app installed.



Apps / App Catalog / Details New Look!

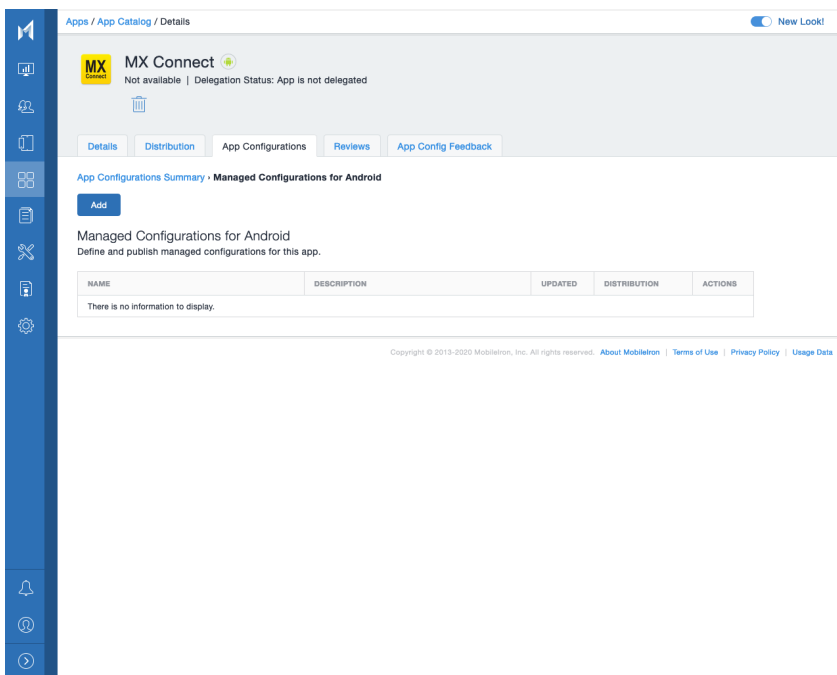
MX Connect Not available | Delegation Status: App is not delegated

[Details](#) [Distribution](#) [App Configurations](#) [Reviews](#) [App Config Feedback](#)

App Configurations Summary [About App Configurations](#)

TYPE		
Managed Configurations for Android Define and publish managed configurations for this app.	0	+
Install on device This configuration option decides whether to require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritized.	1	+
Promotion Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritized.	1	+
Google Play Release Define which binary from the Google Play will be deployed to specific groups or individuals. Includes support for delivering Alpha and Beta channel apps.	0	+

Copyright © 2013-2020 MobileIron, Inc. All rights reserved. [About MobileIron](#) | [Terms of Use](#) | [Privacy Policy](#) | [Usage Data](#)



Apps / App Catalog / Details New Look!

MX Connect Not available | Delegation Status: App is not delegated

[Details](#) [Distribution](#) [App Configurations](#) [Reviews](#) [App Config Feedback](#)

App Configurations Summary • Managed Configurations for Android

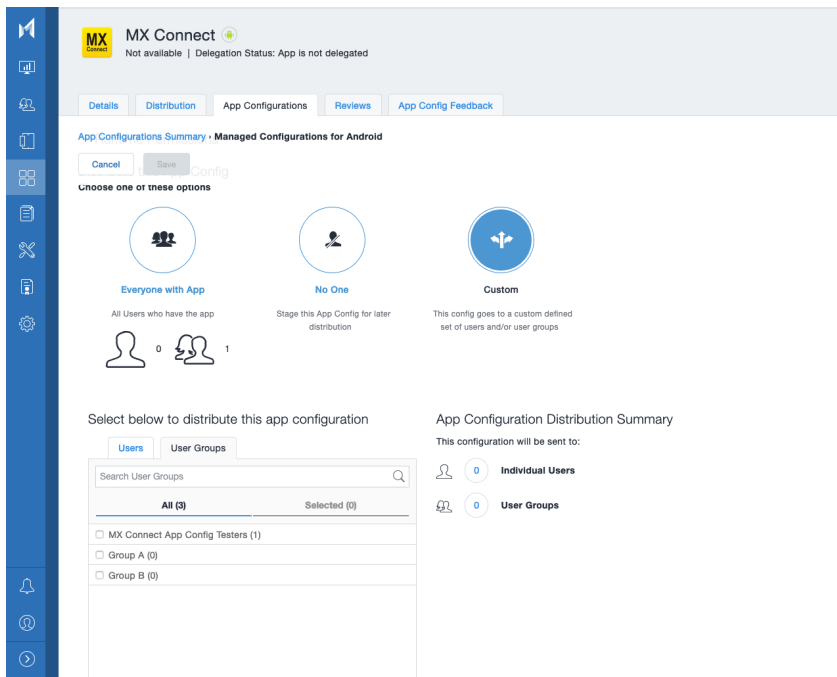
[Add](#)

Managed Configurations for Android
Define and publish managed configurations for this app.

NAME	DESCRIPTION	UPDATED	DISTRIBUTION	ACTIONS
There is no information to display.				

Copyright © 2013-2020 MobileIron, Inc. All rights reserved. [About MobileIron](#) | [Terms of Use](#) | [Privacy Policy](#) | [Usage Data](#)

This distribution don't need to be the same as the app's distribution, and the App Configuration will be applied to the users to whom both the app and the App Configuration are distributed. If there is no overlap between the distribution of the app and the App Configuration, the App Configuration won't be applied to anyone (ex. if you choose to distribute the application to Group A, and distribute an App Configuration to Group B, it won't be applied to either groups).



Update Firmware on MX Mobile Terminal from MDM

1. Change the Firmware URI in the Managed Configuration / App Configuration

- [SOTI](#)
- [MobileIron](#)

You can change the Firmware URI by editing the Advanced settings of MX Connect's entry in an App Catalog Rule in SOTI. You can set a URL for where the Firmware file is hosted on the internet (recommended), or a local path on the devices' file system. It is highly recommended to use Cognex's Firmware Update server URLs for Firmware updates. If you choose to do the update from a file you need to put the Firmware file to the device's file system, which you can do with a File Sync Rule from SOTI.

Add/Edit Application Catalog Entry

Binding:
CogTestEnt
Sync Apps

Search
MX Connect
Search

Managed Applications
Managed Google Play

Application Information


Name:
MX Connect
Version:
1.3.1 (88)
Price:
Free
Seller:
Cognex Corporation
Private:
☐

Description:
Connection service for Cognex MX readers

Advanced

OK
Cancel
Help

Advanced

Application Type:
Suggested

Configuration URI:

☒ Enable App Configuration

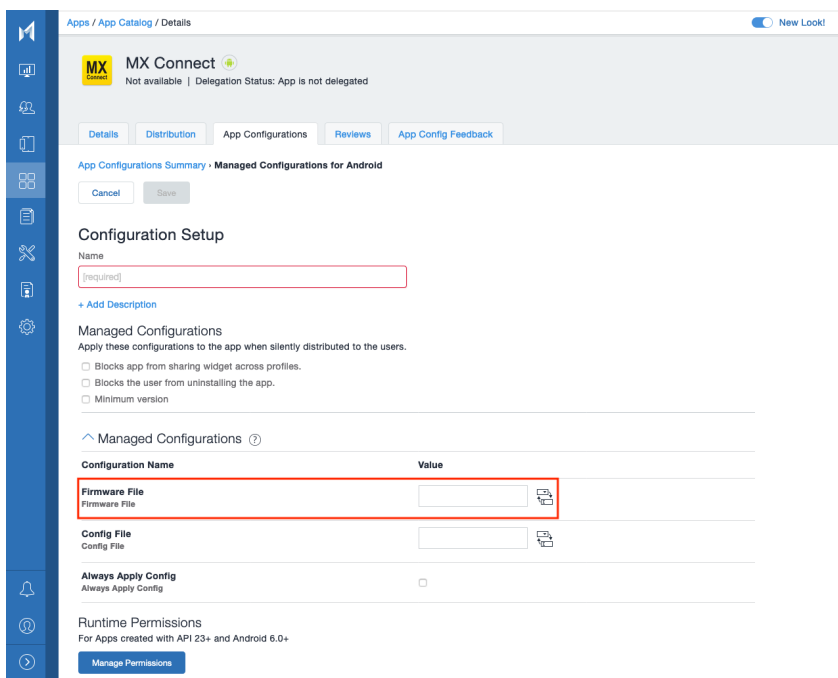
Firmware File:

Config File:

Always Apply Config:
☐

Default
OK
Cancel
Help

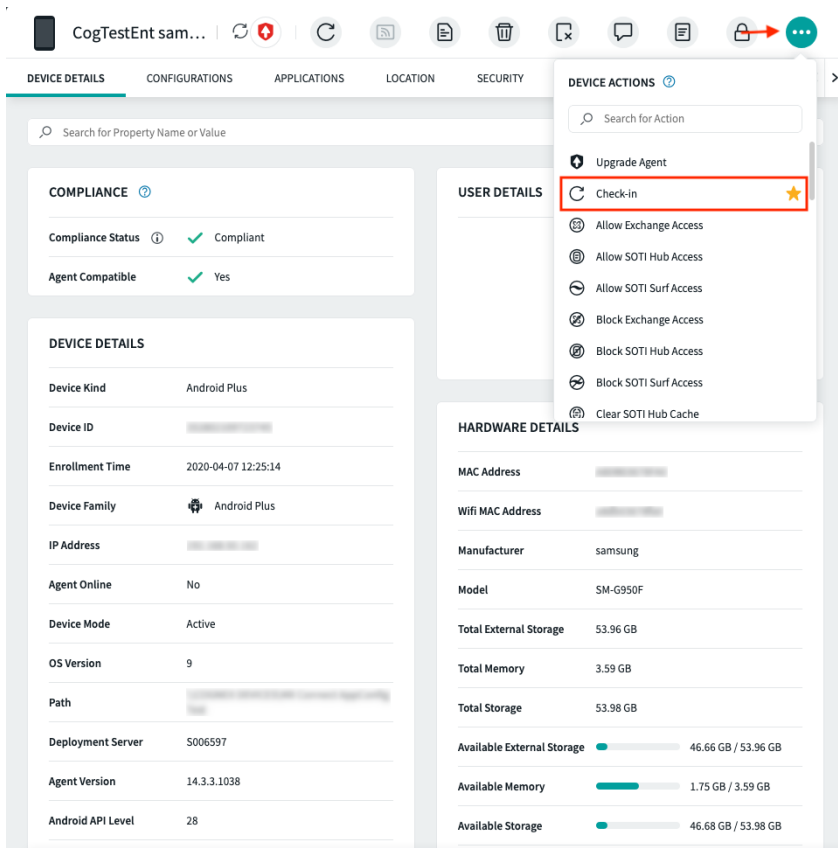
You can change the Firmware URI by editing a Managed Configuration in MobileIron. You can set a URL for where the Firmware file is hosted on the internet (recommended), or a local path on the devices' file system. It is highly recommended to use Cognex's Firmware Update server URLs for Firmware updates. If you choose to do the update from a file you need to put the Firmware file to the device's file system manually and than use it's path in the Managed Configuration.



2. Wait for the modified Managed Configuration / App Configuration to be synchronized to the Android devices, or force the synchronization

- [SOTI](#)
- [MobileIron](#)

After the App Configuration values for MX Connect are changed in an Application Catalog Rule, SOTI will send this change to all devices, that the Application Catalog Rule is targeted with. You cannot schedule when this will happen, however you can force it on a particular device by initiating a Check-in of that device from the Device Details page.



After a Managed Configuration is changed, MobileIron will send this change to all devices, that the Managed Configuration is distributed to. You cannot schedule when this will happen, however you can force it on a particular device by Forcing a Check-in of that device.

The screenshot shows the MobileIron console interface. At the top, there's a header for 'Devices / Devices / Details' with a 'New Look!' toggle. Below this, the device 'Cognex Corporation' is selected, with email 'budanoids@gmail.com' and a 'Go to Audit Trails' link. A status bar shows 'Nokia 4.2', 'Phone #: N/A', 'Space: Default Space', 'Status: Active', 'Last Check-in: 6 days 5 hours ago', and 'Client Last Check-in: 6 days 5 hours ago'. There's a 'Force Check-in' button with a red arrow. Below the status bar are tabs: Overview, Configurations, Installed Apps, Policies, Certificates, Sentry, Attributes, and Logs. The 'General' tab is active, showing a list of device attributes:

Device Location	Disabled in Privacy
Manufacturer	HMD Global
Wi-Fi MAC Address	02:00:00:00:00:00
Wi-Fi MAC Address for inventory	N/A
System Update Status	UNKNOWN
IP Address	192.168.1.10
Serial Number	12345678901234567890
Alternative Serial Number	N/A
Uptime	7 days 20 hours ago
Storage Usage	Internal: 17.34 GB available of 33.55 GB
OS/Version	Android 10
OS Build Version	00EEA_2_330_SP02
Build ID	00EEA_2_330_SP02
System Update	Unknown
Zebra Patch Version	N/A
Samsung Model	N/A

3. Wait for the updates to be completed

When the values set using App Configuration / Managed Configuration gets synced to an Android device and the Firmware URI is changed, it will be automatically installed to the MX Terminal by MX Connect. If the MX Terminal is connected when the new values are received, the installation will begin right away and if not, it will be done upon next connection. Please note that you cannot use the MX Terminal until the Firmware update is done.

Update MX Configuration on MX Mobile Terminal from MDM

1. Change the Config URI and set whether you want to Always apply config in the Managed Configuration / App Configuration

- [SOTI](#)
- [MobileIron](#)

You can change the Firmware URI by editing the Advanced settings of MX Connect's entry in an App Catalog Rule in SOTI. You can set a URL for where the Config file is hosted on the internet, or a local path on the devices' file system. You need to host your config file somewhere and set its URL if you want MX Connect to download it. If you choose to do the update from a file you need to put the Config file to the device's file system, which you can do with a File Sync Rule from SOTI.

Add/Edit Application Catalog Entry

Binding:
CogTestEnt
Sync Apps

Search
MX Connect
Search

Managed Applications
Managed Google Play

Application Information


Name:
MX Connect
Version:
1.3.1 (88)
Price:
Free
Seller:
Cognex Corporation
Private:
☐

Description:
Connection service for Cognex MX readers

Advanced

OK
Cancel
Help

Advanced

Application Type:
Suggested

Configuration URI:

☒ Enable App Configuration

Firmware File:

Config File:

Always Apply Config:
☐

Default
OK
Cancel
Help

You can also set whether the Config will be Always Applied, meaning that it will be uploaded and saved on the MX Terminal every time MX Connect connects to it. This way, even if an application (that communicates with the MX Terminal) changes the Config while it is running, the Config file that is set in MDM will be applied again as soon as that application goes into the background. You can change the Firmware URI by editing a Managed Configuration in MobileIron. You can set a URL for where the Config file is hosted on the internet, or a local path on the devices' file system. You need to host your config file somewhere and set its URL if you want MX Connect to download it. If you choose to do the update from a file you need to put the Config file to the device's file system manually and then use it's path in the Managed Configuration.

You can also set whether the Config will be Always Applied, meaning that it will be uploaded and saved on the MX Terminal every time MX Connect connects to it. This way, even if an application (that communicates with the MX Terminal) changes the Config while it is running, the Config file that is set in MDM will be applied again as soon as that application goes into the background.

Apps / App Catalog / Details New Look!

MX Connect Not available | Delegation Status: App is not delegated

Details Distribution App Configurations Reviews App Config Feedback

App Configurations Summary • Managed Configurations for Android

Cancel Save

Configuration Setup

Name

+ Add Description

Managed Configurations

Apply these configurations to the app when silently distributed to the users.

- ☐ Blocks app from sharing widget across profiles.
- ☐ Blocks the user from uninstalling the app.
- ☐ Minimum version

Managed Configurations ?

Configuration Name	Value
Firmware File Firmware File	
Config File Config File	
Always Apply Config Always Apply Config	☐

Runtime Permissions

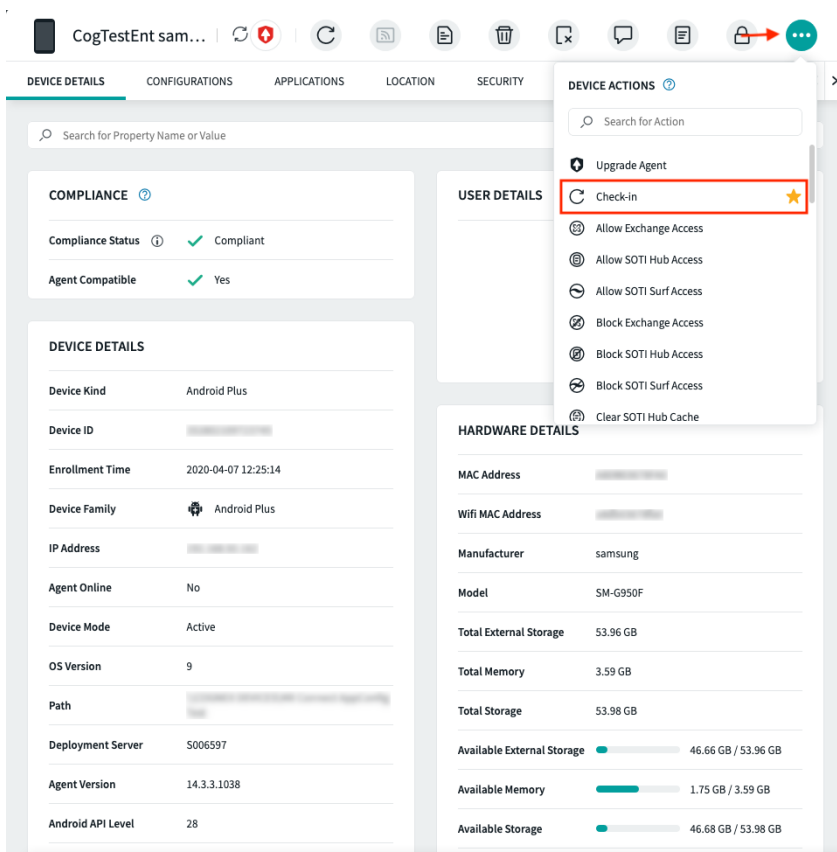
For Apps created with API 23+ and Android 6.0+

Manage Permissions

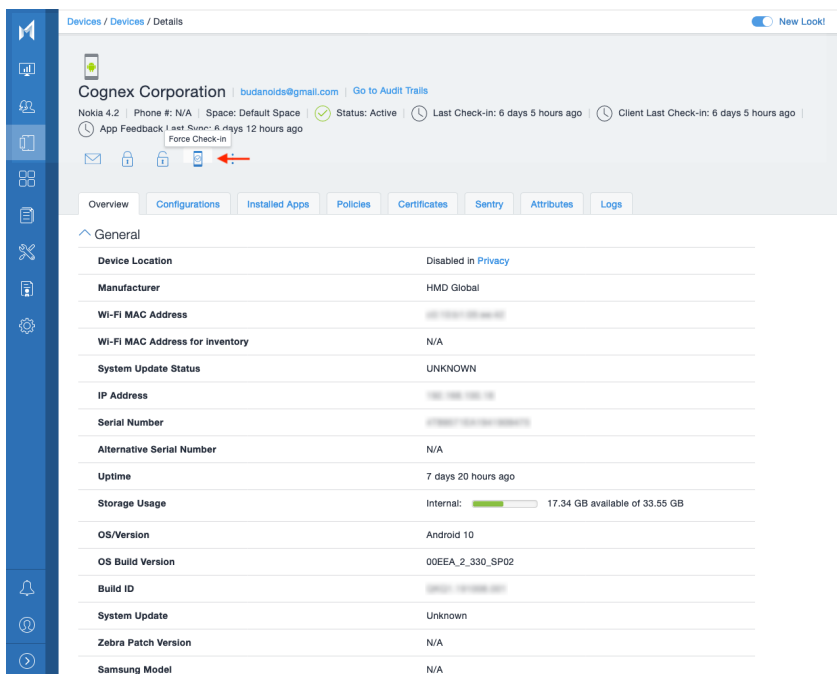
2. Wait for the modified Managed Configuration / App Configuration to be synchronized to the Android devices, or force the synchronization

- SOTI
- MobileIron

After the App Configuration values for MX Connect are changed in an Application Catalog Rule, SOTI will send this change to all devices, that the Application Catalog Rule is targeted with. You cannot schedule when this will happen, however you can force it on a particular device by initiating a Check-in of that device from the Device Details page.



After a Managed Configuration is changed, MobileIron will send this change to all devices, that the Managed Configuration is distributed to. You cannot schedule when this will happen, however you can force it on a particular device by Forcing a Check-in of that device.



3. Wait for the updates to be completed

When the values set using App Configuration / Managed Configuration gets synced to an Android device, it will be automatically installed to the MX Terminal by MX Connect if the actual file is different than the last installed one, or if Always apply config was set. If the MX Terminal is connected when the new values are received, the installation will begin right away and if not, it will be done upon next connection. Please note that you cannot use the MX Terminal until the Config upload is done, but it usually just takes a couple of seconds.

SOTI - MobiControl

Updating the firmware on an MX Mobile Terminal

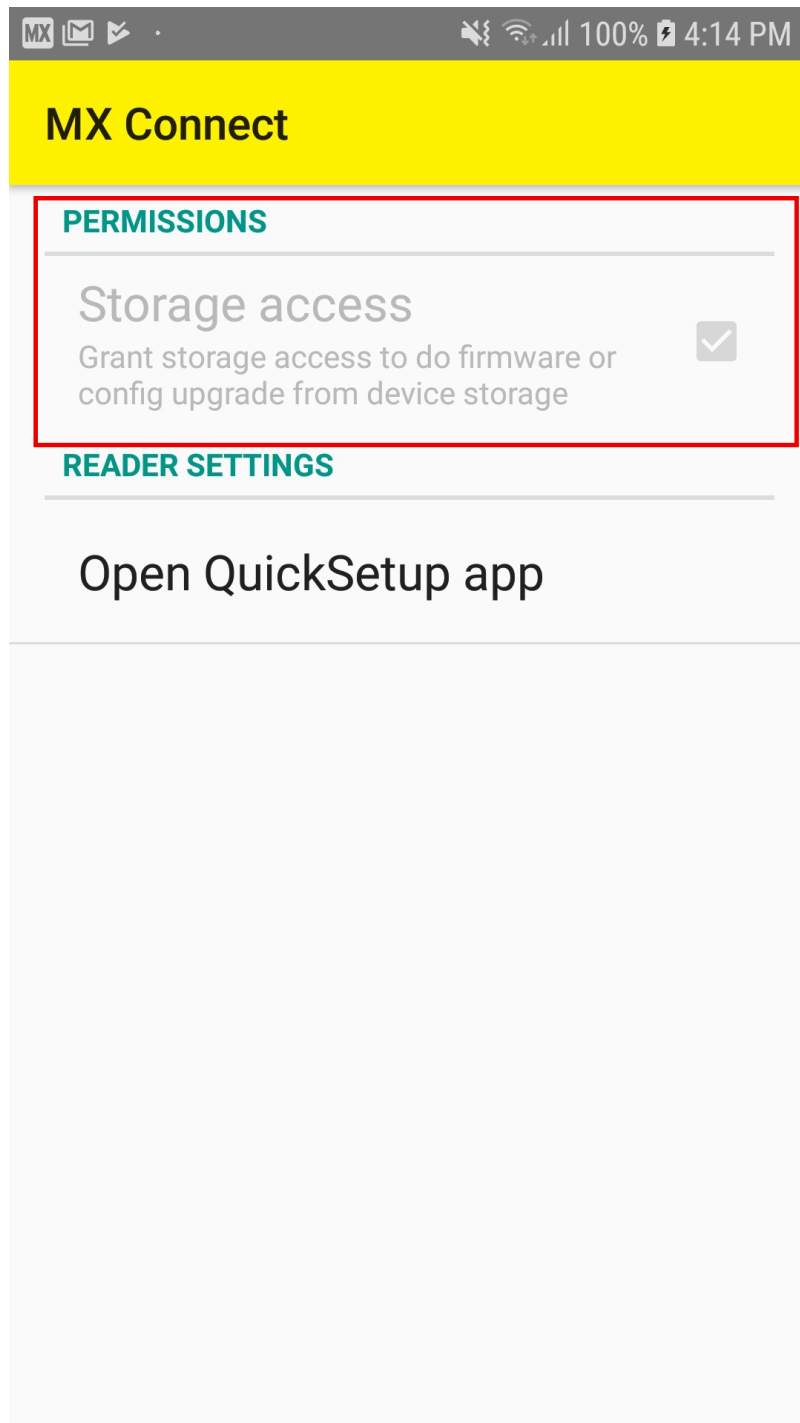
General

Cognex provides two methods for deploying new firmware upgrades to MX devices with SOTI's MobiControl:

- You can have the MX device retrieve the firmware file from a URL you provide (http or https).
- You can push the firmware file directly to the MX device.

Before performing a firmware update with MobiControl, consider the following:

- Your MX mobile terminal must have at least version v1.2.0 of MXConnect installed on the mobile phone.
- If the MX mobile terminal is not turned on when the update is sent, but the phone receives the update from MobiControl, the firmware update will take place when the MX mobile terminal is powered on. If you send out several different intents when MW mobile terminal is offline, only the last update command will be executed. (The same is true for firmware update intents.)
- There is only one way communication from MobiControl to MXConnect: this means that you cannot follow what the progress percentage and success rate of your roll-out is.
- To perform the firmware update, MXConnect will disconnect all apps from the MX mobile terminal, perform the update, then reboot the MX device (not the mobile phone). It is highly recommended to perform updates in a time period when the device is not likely to be in use.
- You cannot perform a firmware update on an MX mobile terminal that is in keyboard wedge mode (this is a limitation of Android). You must scan the configuration barcode to disable keyboard wedge mode first, apply the firmware update, then scan the configuration code to re-enable keyboard wedge mode.
- If you decide to push the firmware file directly to the MX mobile terminal, you must first grant Storage access to MXConnect. You can do this by starting MXConnect from the notification bar (swipe down on the notification bar, select MXConnect from the notification list):



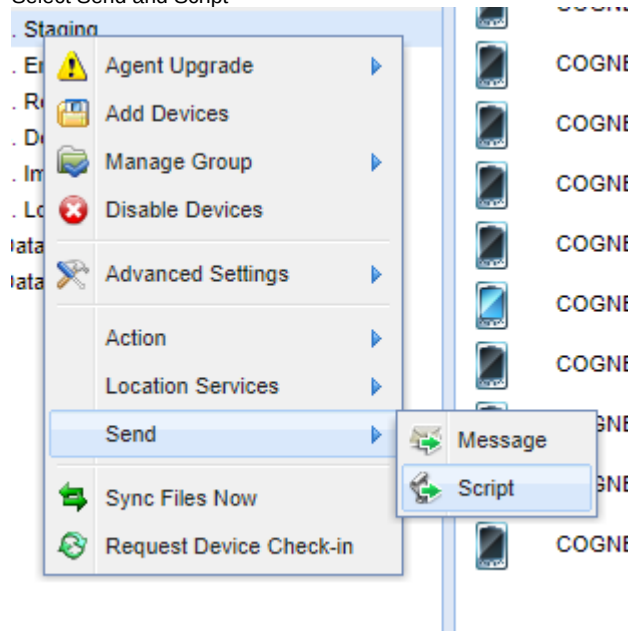
Updating firmware from a URL

When updating the MX firmware from a URL (web server), you must provide the full path to the firmware file. If your MX devices have full Internet access, you can use the Cognex server, otherwise you must host the firmware file on a server your devices can access. The following FAQ provides more information on obtaining the Cognex link or firmware file: [How to obtain firmware files for MX-1000 and MX-1502 series?](#)

Once you have the URL for the firmware file you wish to deploy, follow these steps:

1. Log into MobiControl
2. Right click on the device or device group you wish to update

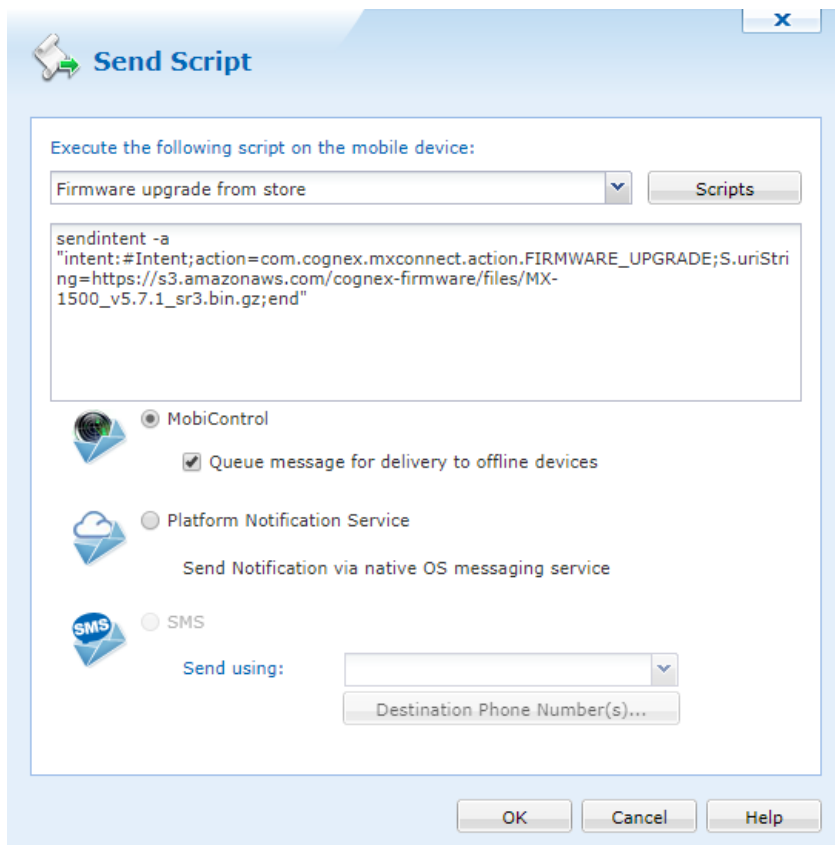
3. Select Send and Script



4. Click on Scripts (first time) or select a saved script from the drop down list.
5. Use the following script to invoke the MXConnect intent for updating firmware:

```
sendintent -a
"intent:#Intent;action=com.cognex.mxconnect.action.FIRMWARE_UPGRADE;S.uriString=https://s3.amazonaws.com/cognex-
firmware/files/MX-1500_v5.7.1_sr3.bin.gz;end"
```

Update the value of the uriString parameter with URL of the firmware file. The example above shows a URL to the Cognex firmware repository.



Updating firmware from device storage

Once you have retrieved the appropriate firmware file from the Cognex repository, follow the steps below:

1. Log into MobiControl
2. Create a new File Synch rule according to the details below. We recommend that you upload the firmware file to the mobile device's Download directory as in the example below.

Edit File Sync Rule - Cognex - Upload firmware

File Sync Rules allow you to synchronize files or folders between a server and your mobile devices.

Direction

☐ Upload file(s) from Devices to Server
☒ Download file(s) from Server to Devices

Folder

Device File / Folder Name:

Supported path macros: %sdcard%, %kioskdata%, %shareddata%, %logpath%, %tmp%
 Server File / Folder Name:

Please use either \\ or [drive]:\ for the server path and make sure Deployment Server(s) have sufficient privileges to access this folder. File path names are case sensitive for iOS and Android devices.

Options

☒ Do not use subfolders for downloading files
☐ Use Device ID as subfolders for downloading files
☐ Use Device Tree Path as subfolders for downloading files
☐ Create folders immediately after rule is saved

3. Right click on the device or device group you wish to push the file to and select Synch files now.
4. For the same device/device group, select Send and Script
5. Click on Scripts (first time) or select a saved script from the drop down list.
6. Use the following script to invoke the MXConnect intent for updating firmware:

```
sendintent -a
"intent:#Intent;action=com.cognex.mxconnect.action.FIRMWARE_UPGRADE;S.uriString=file:///storage/emulated/0/Download/MX-1500_v5.7.1_sr3.bin.gz;end"
```

Update the value of the uriString parameter with firmware filename you sent to the mobile device. The example above shows the path to the Download directory.

Updating the configuration of an MX Mobile Terminal

General

Cognex provides two methods for deploying configuration changes to MX devices with SOTI's MobiControl:

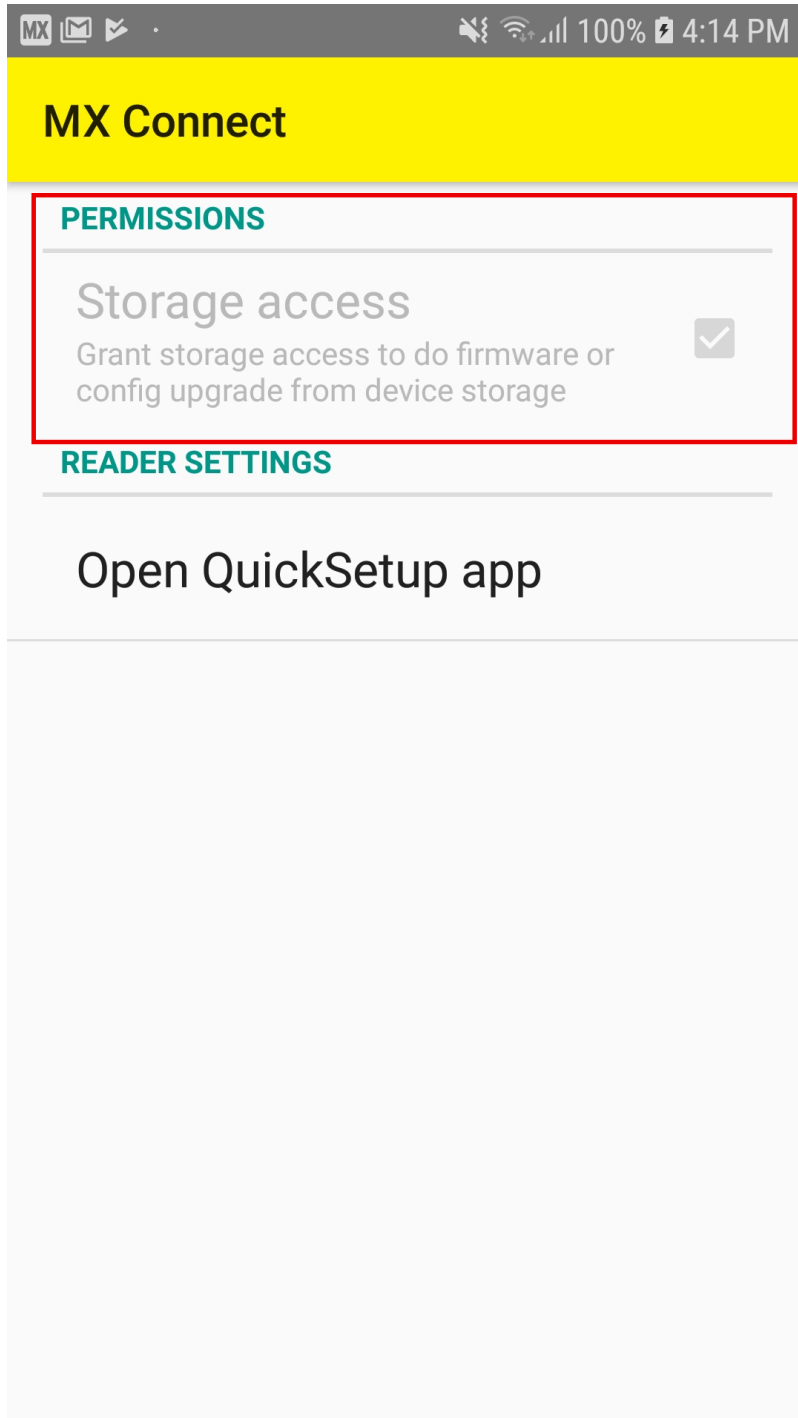
- You can have the MX device retrieve the configuration file from a URL you provide (http or https).
- You can push the configuration file directly to the MX device.

Before deploying an MX configuration with MobiControl, consider the following:

- Your MX mobile terminal must have at least version v1.2.0 of MXConnect installed on the mobile phone.
- If the MX mobile terminal is not turned on when the configuration file is sent, but the phone receives the file from MobiControl, the configuration update will take place when the MX mobile terminal is powered on. If different intents are sent out when MW mobile terminal

is offline, only the last config update command will be executed. (The same is true for firmware update intents.)

- There is only one way communication from MobiControl to MXConnect: this means that you cannot follow what the progress percentage and success rate of your roll-out is.
- To update the MX mobile terminal's configuration, MXConnect will disconnect all apps from the MX mobile terminal, perform the update, then reboot the MX device (not the mobile phone). It is highly recommended to perform updates in a time period when the device is not likely to be in use.
- You cannot update the MX mobile terminal's configuration if it is in keyboard wedge mode (this is a limitation of Android). You must scan the configuration barcode to disable keyboard wedge mode first, apply the configuration update, then scan the configuration code to re-enable keyboard wedge mode.
- If you decide to push the MX configuration file directly to the MX mobile terminal, you must first grant Storage access to MXConnect. You can do this by starting MXConnect from the notification bar (swipe down on the notification bar, select MXConnect from the notification list):

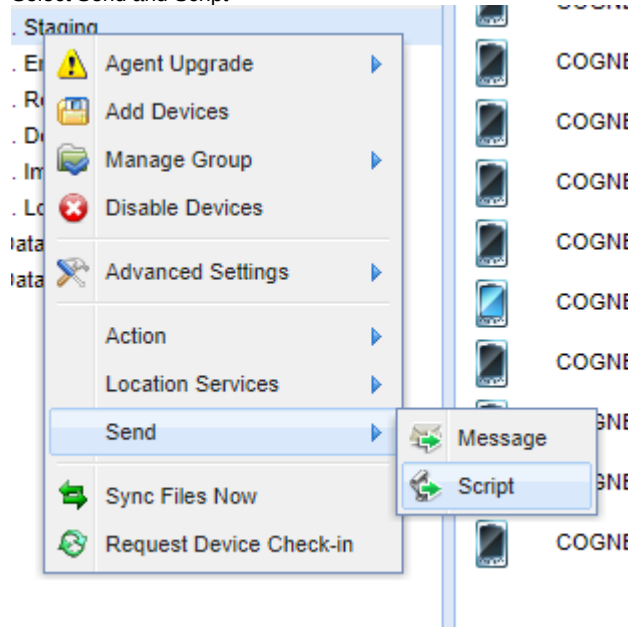


Updating the configuration from a URL

When updating the MX configuration from a URL (web server), you must provide the full path to the configuration file. You must host the configuration file on a web server your devices can access. The following FAQ provides more information on retrieving a configuration file from the setup utilities: [How to create a configuration file for MX-1000 or MX-1502 mobile terminal?](#)

Once you have the URL for the configuration file you wish to deploy, follow these steps:

1. Log into MobiControl
2. Right click on the device or device group you wish to update
3. Select Send and Script



4. Click on Scripts (first time) or select a saved script from the drop down list.
5. Use the following script to invoke the MXConnect intent for updating the MX device's configuration:

```
sendintent -a
"intent:#Intent;action=com.cognex.mxconnect.action.CONFIG_UPLOAD;S.uriString=https://yourserveraddress.com/MX-
1XXX.cfg;end"
```

Update the value of the uriString parameter with URL of the configuration file. The example above shows a URL to a fictitious server and configuration file.

Updating the configuration from device storage

Once you have retrieved the appropriate MX mobile terminal configuration file, follow the steps below:

1. Log into MobiControl
2. Create a new File Synch rule according to the details below. We recommend you upload the configuration file to the mobile device's Download directory as in the example below:

Edit File Sync Rule - Cognex - Upload firmware

File Sync Rules allow you to synchronize files or folders between a server and your mobile devices.

Direction

☐ Upload file(s) from Devices to Server
☒ Download file(s) from Server to Devices

Folder

Device File / Folder Name:

Supported path macros: %sdcard%, %kioskdata%, %shareddata%, %logpath%, %tmp%

Server File / Folder Name:

Please use either \\ or [drive]:\ for the server path and make sure Deployment Server(s) have sufficient privileges to access this folder. File path names are case sensitive for iOS and Android devices.

Options

☒ Do not use subfolders for downloading files
☐ Use Device ID as subfolders for downloading files
☐ Use Device Tree Path as subfolders for downloading files
☐ Create folders immediately after rule is saved

3. Right click on the device or device group you wish to push the file to and select Synch files now.
4. For the same device/device group, select Send and Script
5. Click on Scripts (first time) or select a saved script from the drop down list.
6. Use the following script to invoke the MXConnect intent for updating the MX device's configuration:

```
sendintent -a
"intent:#Intent;action=com.cognex.mxconnect.action.CONFIG_UPLOAD;S.uriString=file:///storage/emulated/0/Download/MX-1XXX.cfg;end"
```

Update the value of the uriString parameter with the configuration filename you sent to the mobile device. The example above shows the path to the Download directory.

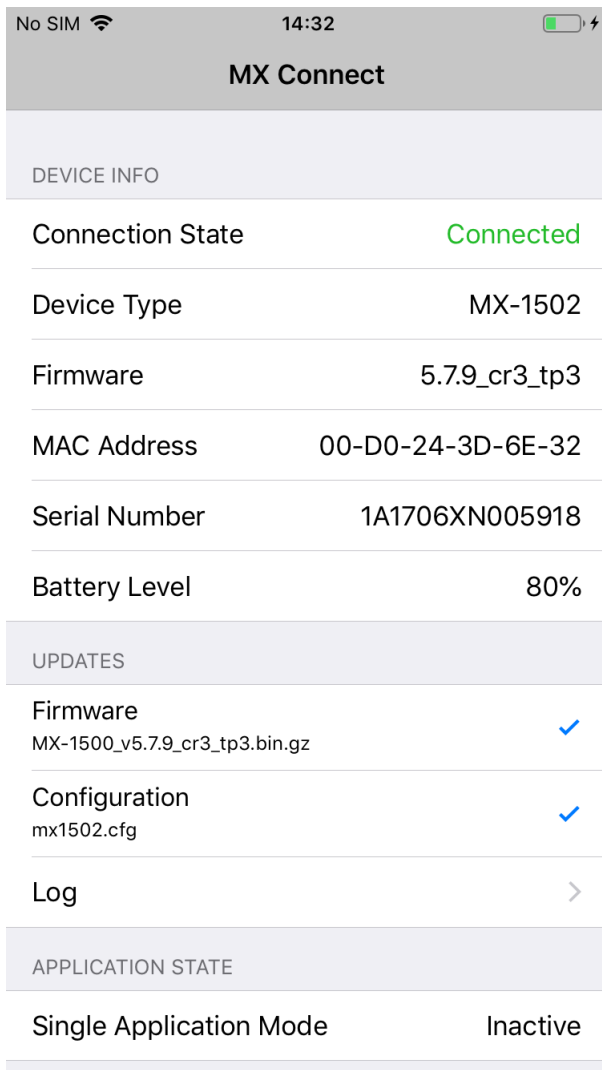
iOS

MX Connect User Guide

Functionalities

The main features of the MX Connect application are:

- Display basic information about the connected MX Mobile Terminal, for example MX-1502.
- Receive and display the configuration from the MDM server, for example JAMF.
- Perform necessary updates according to configuration received from the MDM server.
- Lock the application via Single App Mode during updates and display update status (active / inactive).
- Log and display events sorted by date.



Updating Process

In the UPDATES section of the main screen the app shows the configured firmware and MX configuration. If these configurations are installed properly, a checkmark is displayed in the rows, respectively. Although the configuration XML sent by the MDM contains URLs, MX Connect only displays the last component of these URLs. Use file names in the URLs that reflect the version of their content.

Browsing the Log

Check the log to review the history of the attached MX mobile terminal. You can check what configuration the app received, and if the updating processes were successful.

No SIM 14:33		
< Back	History	Verbose ☐
Cfg Update Started	2019-05-09 14:32	>
Cfg Update Started	2019-05-09 14:32	>
Cfg Download Failed	2019-05-09 14:32	>
Config Download OK	2019-05-09 14:32	>
Device Connected	2019-05-09 14:32	>
Device Disconnected	2019-05-08 15:43	>
Cfg Update Started	2019-05-07 17:23	>
Cfg Update Started	2019-05-07 17:23	>
Cfg Download Failed	2019-05-07 17:23	>
Config Download OK	2019-05-07 17:23	>
Device Connected	2019-05-07 17:23	>
Device Disconnected	2019-05-07 17:23	>
Cfg Update Started	2019-05-07 17:17	>
Cfg Update Started	2019-05-07 17:17	>

Tap the row in the history list and check the disclosed page for more detailed information on a particular event.

No SIM 14:33	
History	
Type	Device Disconnected
Date	2019-05-08 15:43:59
Firmware Version	5.7.9_cr3_tp3
Serial Number	1A1706XN005918

Manage MX Connect from MDM

Terminology and Definitions

The following terms are used throughout this document:

- **MX Mobile Terminal:** The MX barcode reader device, for example, MX-1502.
- **iOS device:** iPhone or iPod Touch built into an MX Mobile Terminal.
- **Firmware:** The firmware of the MX Mobile Terminal.
- **MX configuration:** The configuration of the MX Mobile Terminal.
- **App Configuration XML:** An XML formatted text containing the URLs of the update files.
- **MDM:** Mobile Device Management referring to an MDM solution, for example, Jamf.

Preparation Steps

1. Configure Apple Push Notification Service on your MDM

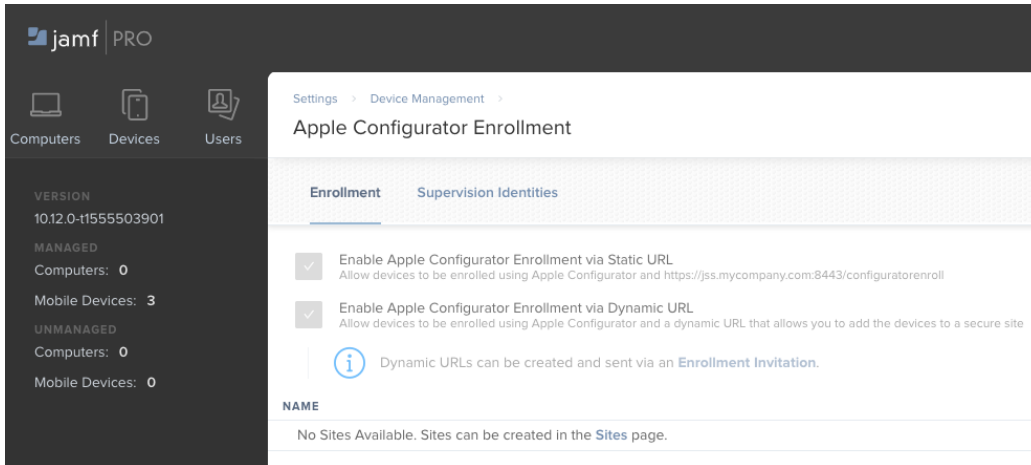
Follow the instructions to enable your MDM to communicate with mobile phones via Apple's Push Notification Service.

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
- [WorkSpace ONE](#)

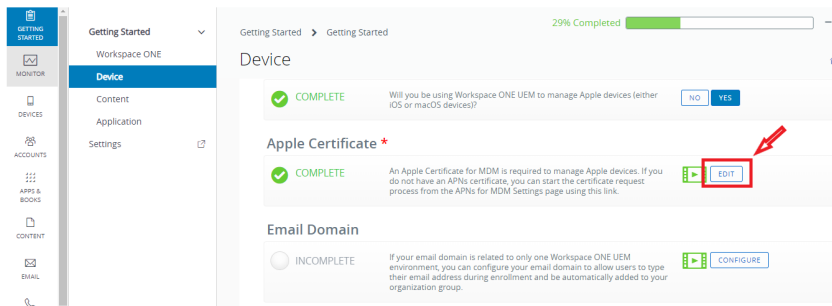
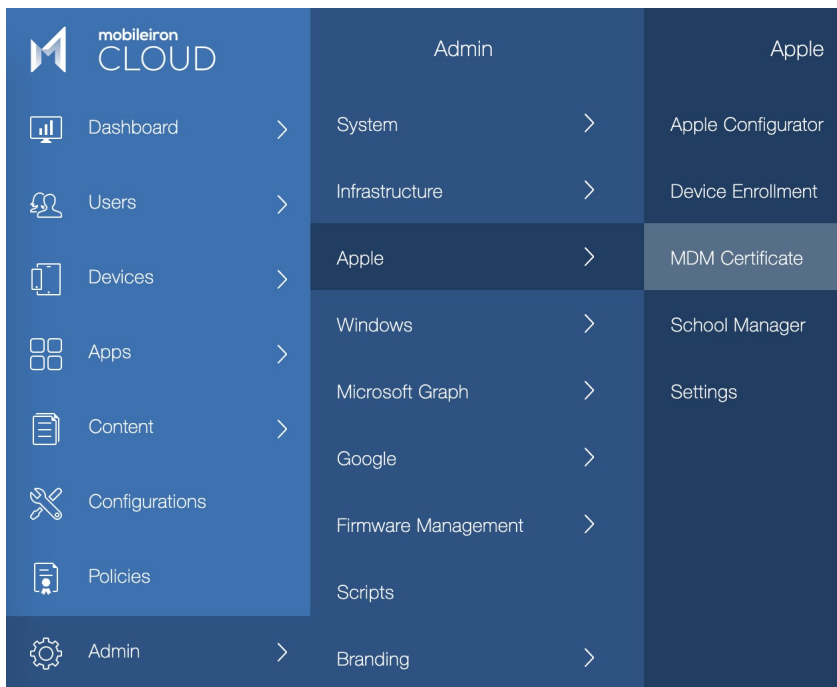
Push Certificates

Enable the required URLs during enrollment.

Apple Configurator Enrollment Settings



Using the Apple Push Notification Service



2. Make your iOS device supervised

Make your iOS device supervised by using the [Apple Configurator](#) desktop application on a Mac or by using Apple's DEP program. This is a precondition so that MDM can have more control over the mobile phone (e.g. launch and application in single app mode which is required for MX Connect updating workflow).

3. Enroll the mobile phone to the MDM.

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
-
- [Workspace ONE](#)

User-Initiated Enrollment for Mobile Devices

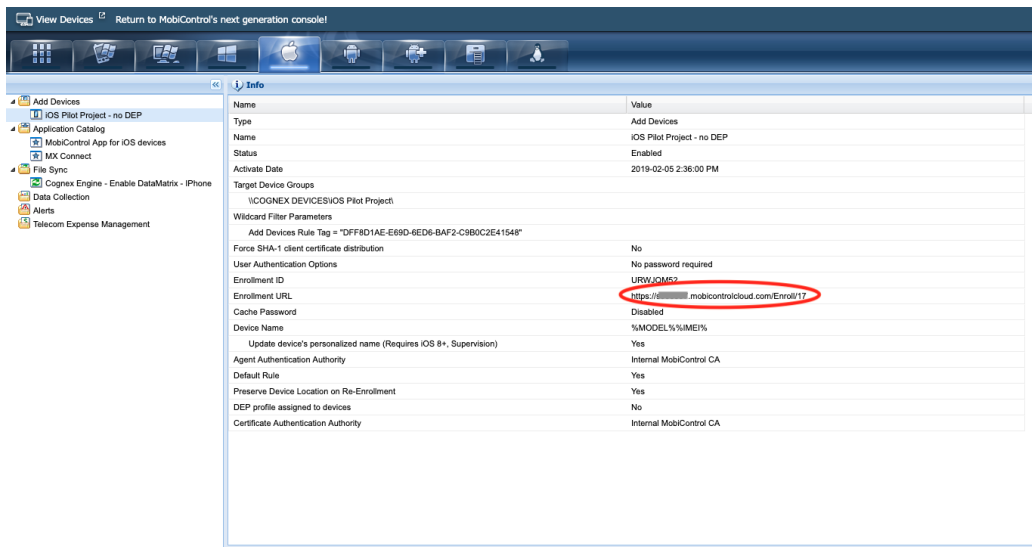
You can combine supervising and enrolling by using a supervising identity.

Supervision Identities

For more information about device enrollment, refer to [Enrollment of Mobile Devices](#).

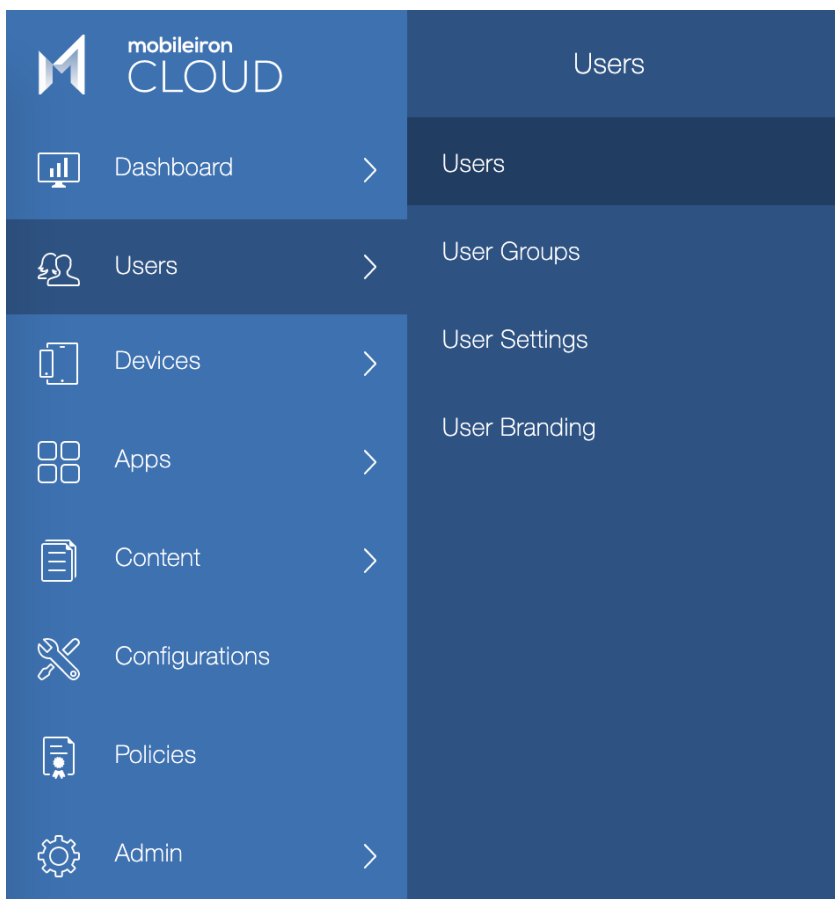
Adding iOS Devices

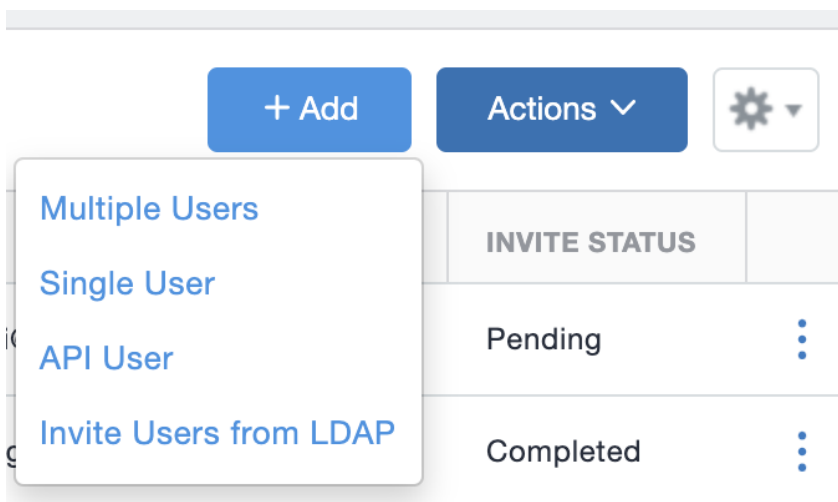
You can use the enrollment URL of your "Add Devices" rule.



There are multiple ways to enroll a device in MobileIron. You can read two examples below (for more options please check MobileIron's User's manual).

- Enrolling via invitation:





- Enrolling via Apple Business Manager:

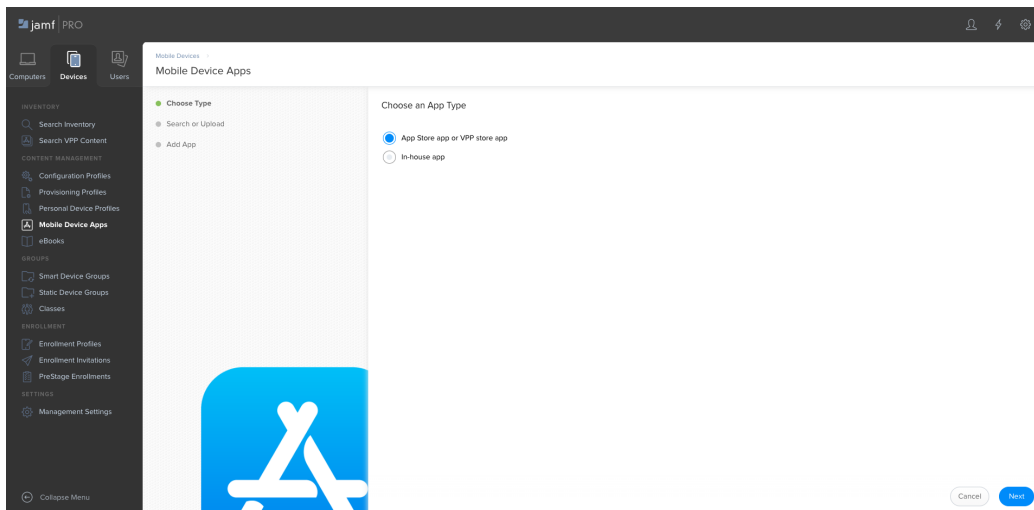


There are multiple ways to enroll a device in Workspace ONE. Check the following description: [iOS Device Enrollment Overview](#)

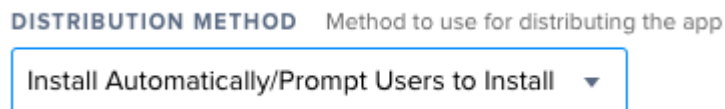
4. Install **MX Connect** app with your MDM system from the App Store.

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
- [Workspace ONE](#)

Add MX Connect to JAMF by an App Store URL.

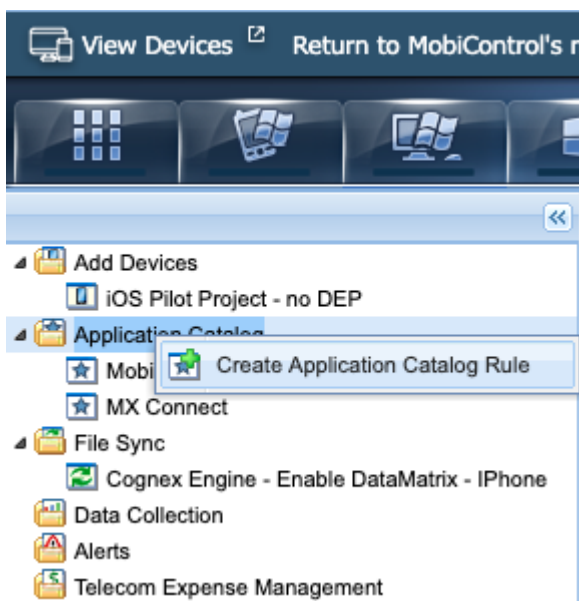


Set the distribution method to "Install Automatically" to let JAMF deploy it without user interaction.

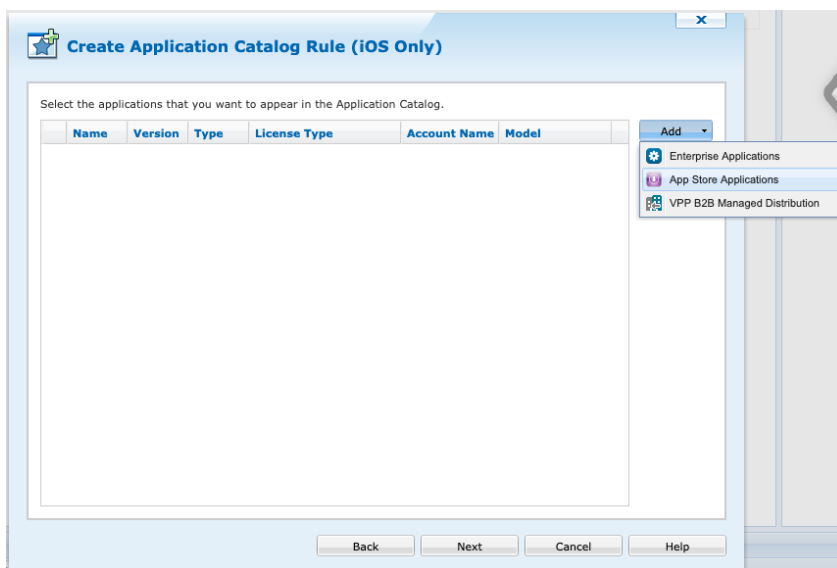


To learn more about app distribution in JAMF, read the [App Distribution](#) document.

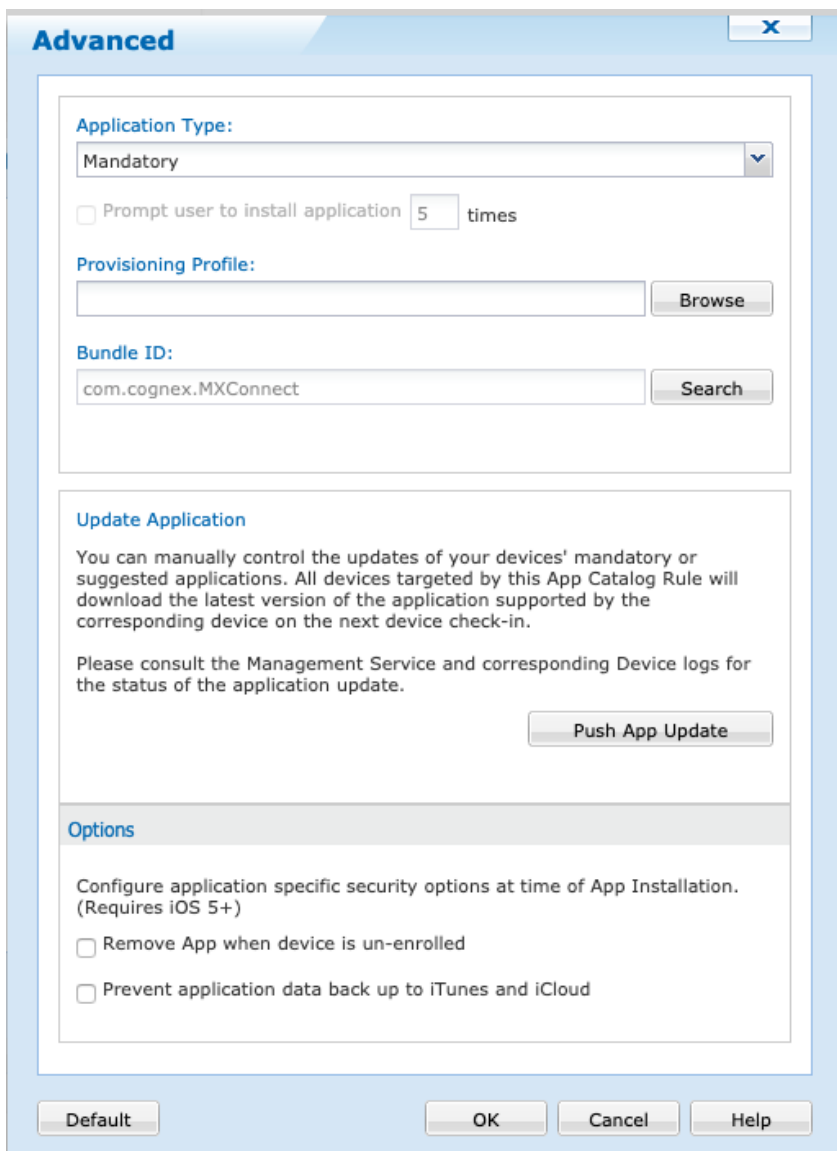
To install MX Connect app first you have to create an **Application Catalog Rule**.



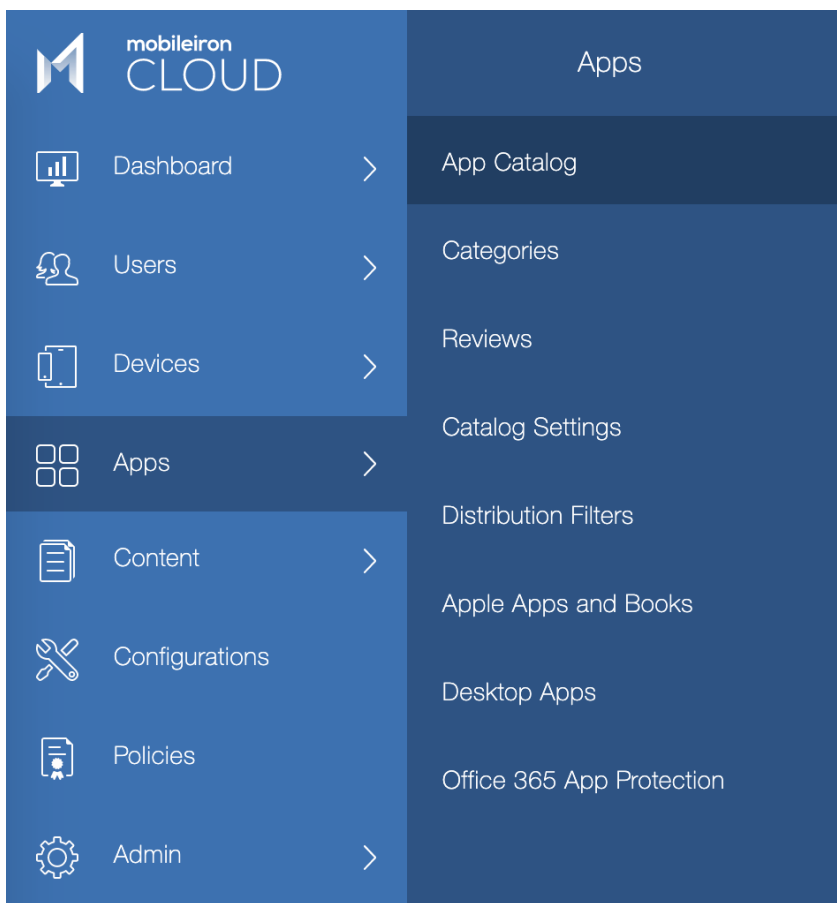
In the app catalog rule you have to add MX Connect app by any of the possible options. Most likely you will select the **App Store Applications** option.



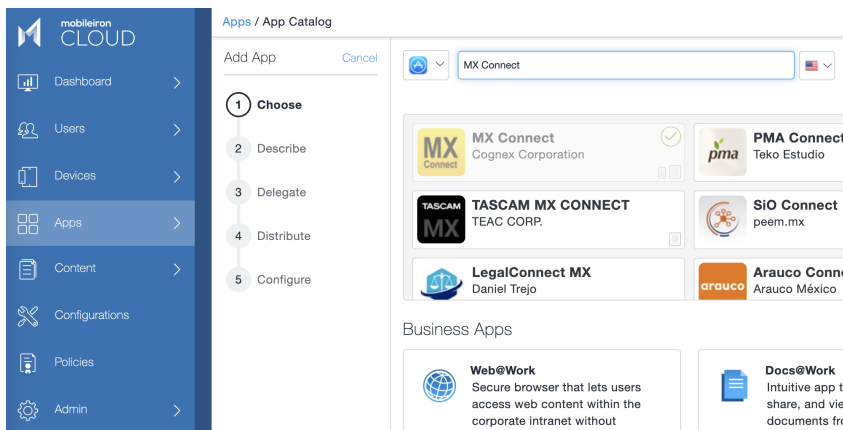
To force installing to devices set the **Application Type** field to **Mandatory**.



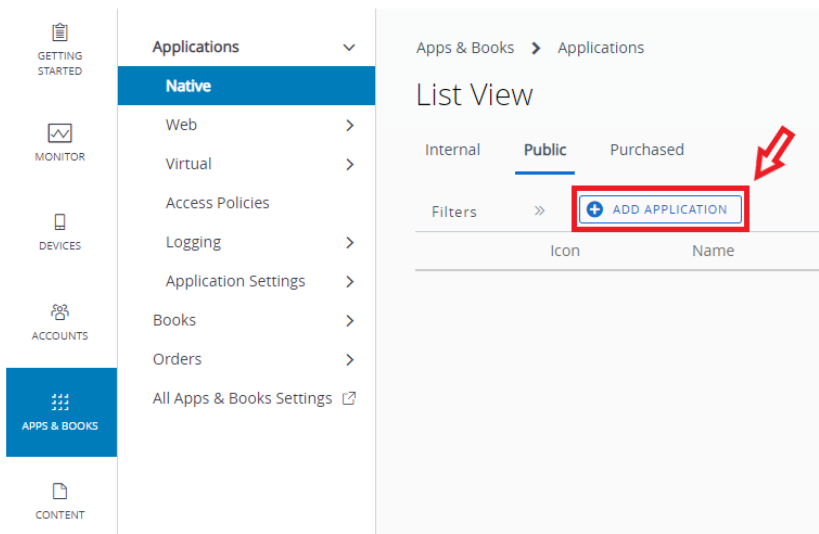
To install MX Connect application via MobileIron first you have to add it on the MDM admin site.



Click Add button.



Navigate to publicly available native apps and select "Add application":

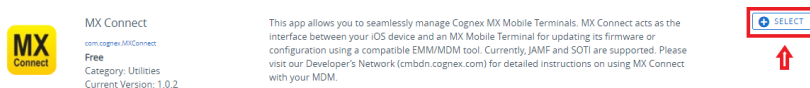


Fill out the form properly:

Add Application

Managed By	Cognex Corporation Technology
Platform *	Apple iOS
Source	SEARCH APP STORE ENTER URL
Name *	MX Connect

Select MX Connect published by Cognex Corporation:



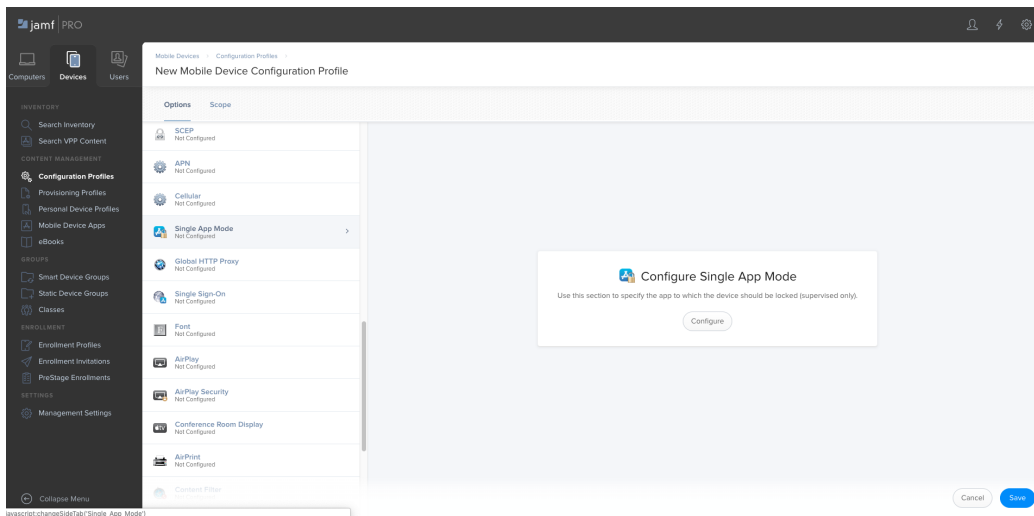
Save and assign to user group where MX mobile terminals are used. Set all other assignment properties according to your need and finally publish your changes.

5. Create a Single App Mode Configuration Profile for MX Connect.

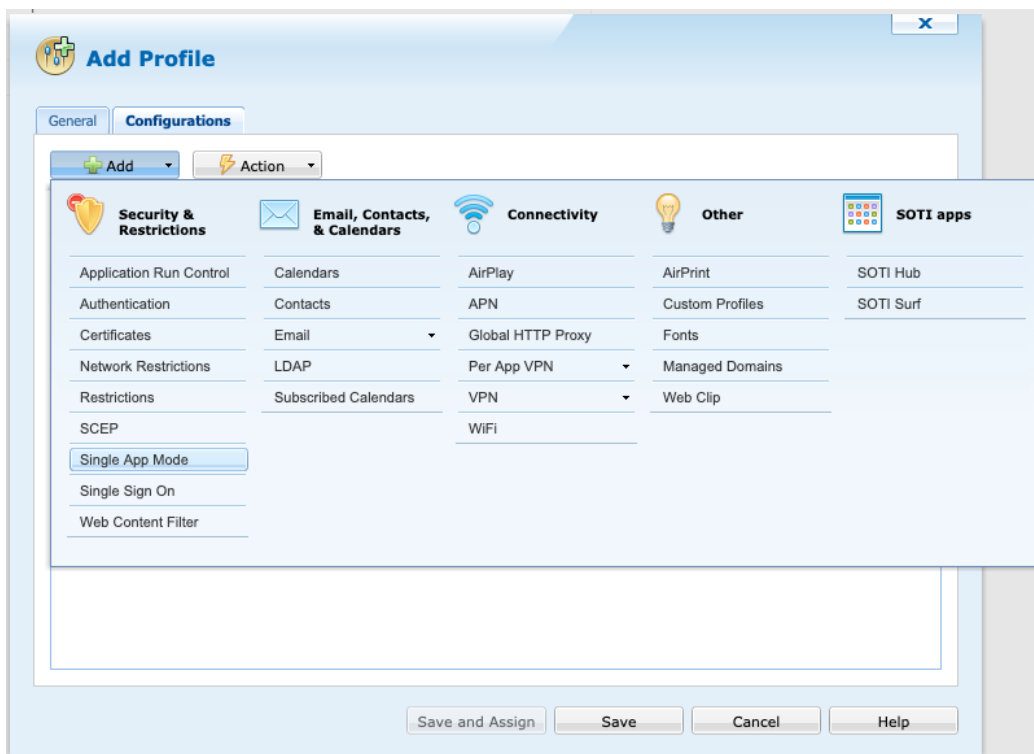
Launch the application by putting it to Single App Mode (SAM). To let your MDM put the application to SAM, create a configuration profile in your MDM that is sent out to devices in the right time. If a device receives a Single-App-Mode configuration profile for MX Connect app, the iOS device launches the app and keeps it on screen until the MDM system revokes the configuration profile.

- JAMF
- SOTI
- MobileIron
-
- Workspace ONE

You can create a Single-App-Mode configuration profile at Mobile Devices or Configuration Profiles.



You can create a Single-App-Mode configuration profile at Profiles / Add.



You can create a Single-App-Mode configuration profile at Configurations.



mobileiron
CLOUD



Dashboard



Users



Devices



Apps



Content



Configurations



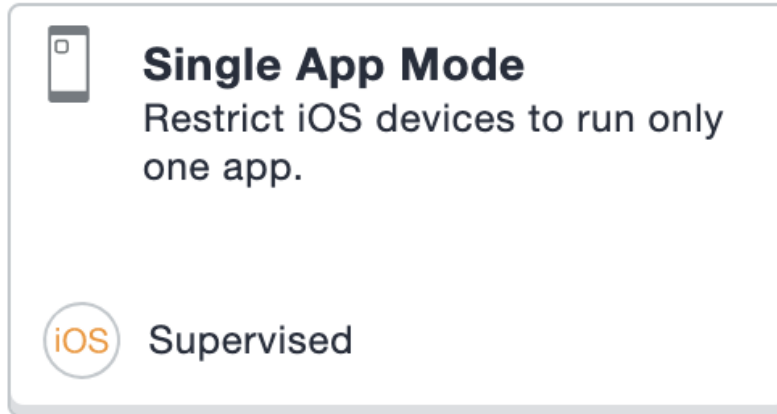
Policies



Admin



Create a new configuration and select the Single App Mode type.



To associate the MX Connect app configure the restriction by selection your hosted MX Connect app.

Configuration Setup iOS

iOS Supervised Single App Mode Options
When this configuration is installed on a supervised device, the device will launch the specified app and the functionality will be limited as specified below. Note: The device must already have the app installed prior to distributing this configuration.

Select App 0 Selected App Details

Select By Lookup **Select Manually**

MX Connect

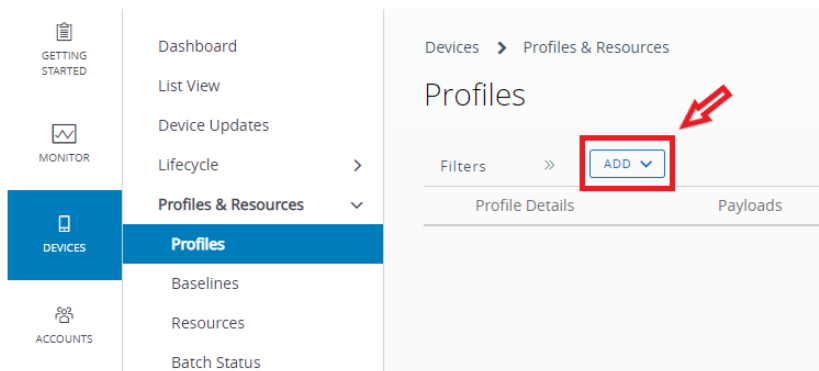
APP NAME	BUNDLE ID / PACKAGE ID	
MX Connect	com.cognex.MXConnect	Public

Please note that this is only a preparation step so please leave "Enable this configuration" option unchecked:

Edit Single App Mode Configuration
Restrict Supervised iOS devices to only run a selected app. Additionally, you can control many hardware and software features available to that specific app.

☐ Enable this configuration
This configuration will not be applied to any devices. It will be removed from all devices if it was previously applied.

Select "Add profile" for devices from the drop-down list:



iOS

Apple iOS



Device Profile

Select **Apple iOS** for Platform and **Device Profile** for Context.
Fill out **General** tab according to your needs (use *Manual for Deployment*) but leave *Smart Group* assignment empty for now. Select **Single App Mode** tab and enter the following data and then **Publish** it:

6. Create an Autonomous Single App Mode Configuration Profile for MX Connect.

Autonomous Single App Mode (ASAM) is a very similar functionality to Single-App-Mode. ASAM lets the MX Connect app to lock to the iOS device's screen and unlock when it is no longer needed.

Note that while the user of the MDM system manually issues and revokes Single-App-Mode, the Autonomous Single App Mode is activated and deactivated by MX Connect app.

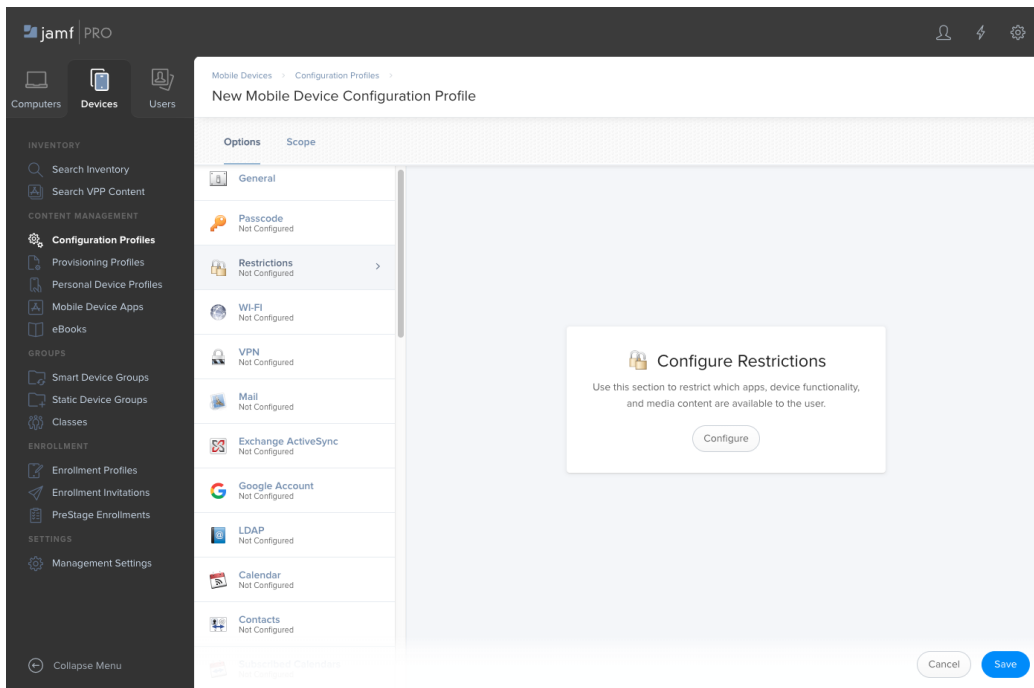
MX Connect needs this to autonomously lock to the screen during downloading and installing update files to prevent the phone's user to navigate away during installation.

To let MX Connect use ASAM, create a configuration profile with MX Connect app's bundle ID, com.cognex.MXConnect, in your MDM and issue it to all your iOS devices.

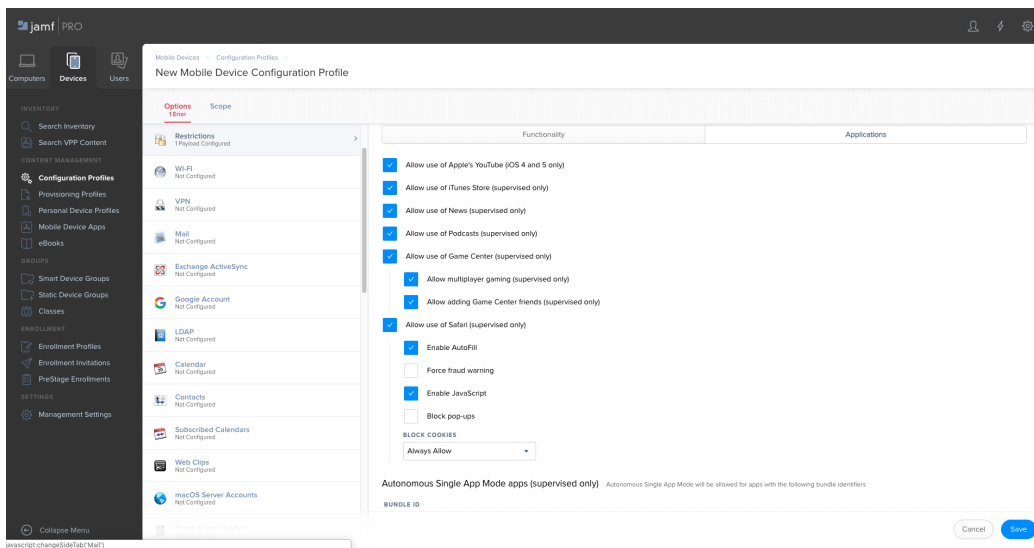
Sending out ASAM configuration profile for MX Connect does not put the app on the screen, it only gives permission to the app to do so. Issuing an ASAM configuration profile has to be done only once for an iOS device and it must not be revoked.

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
-
- [Workspace ONE](#)

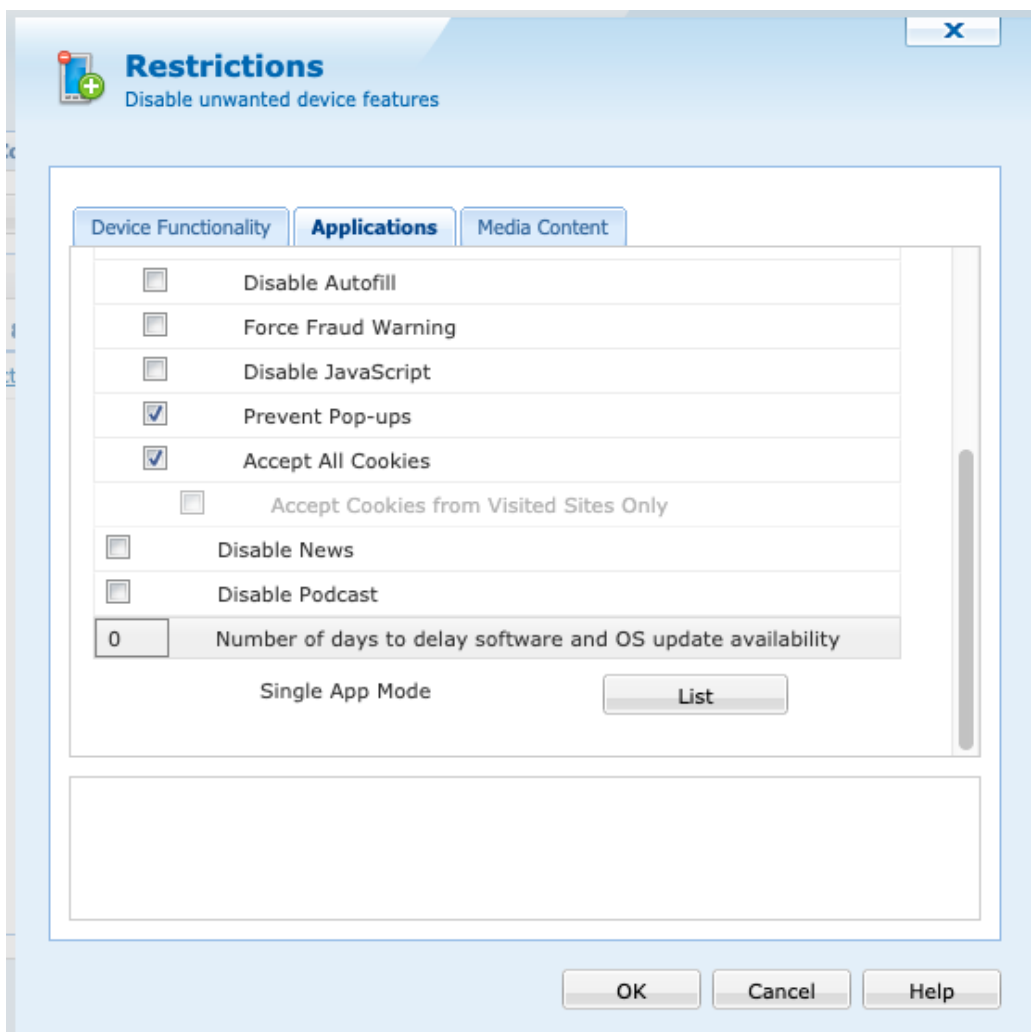
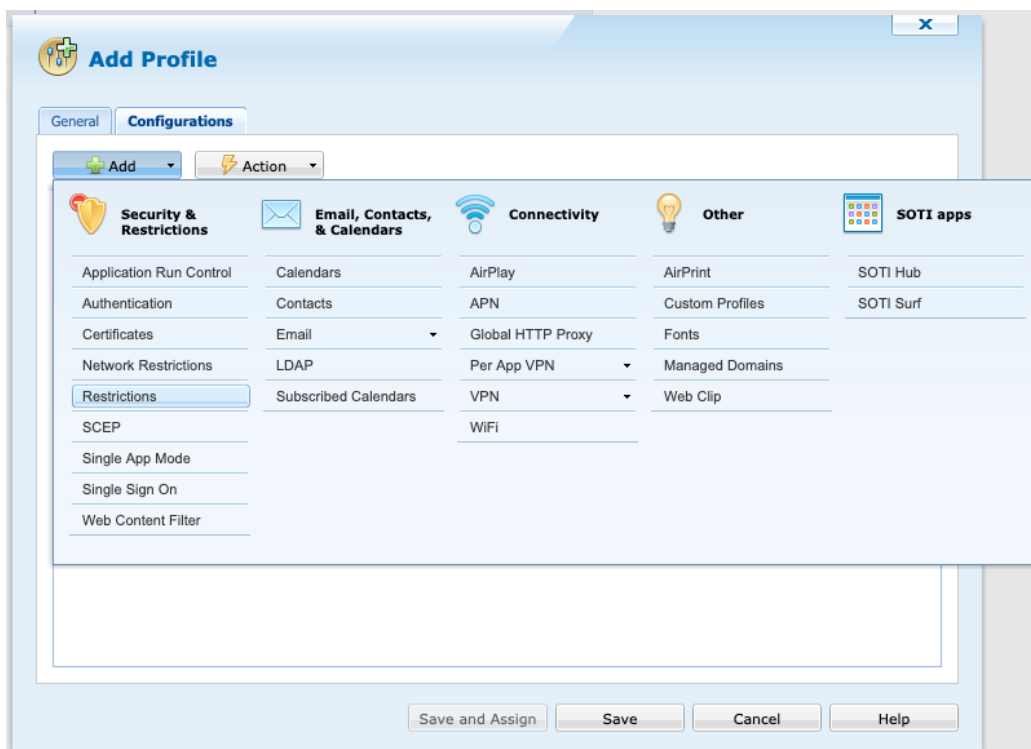
Select Restrictions to create an Autonomous Single App Mode configuration profile.



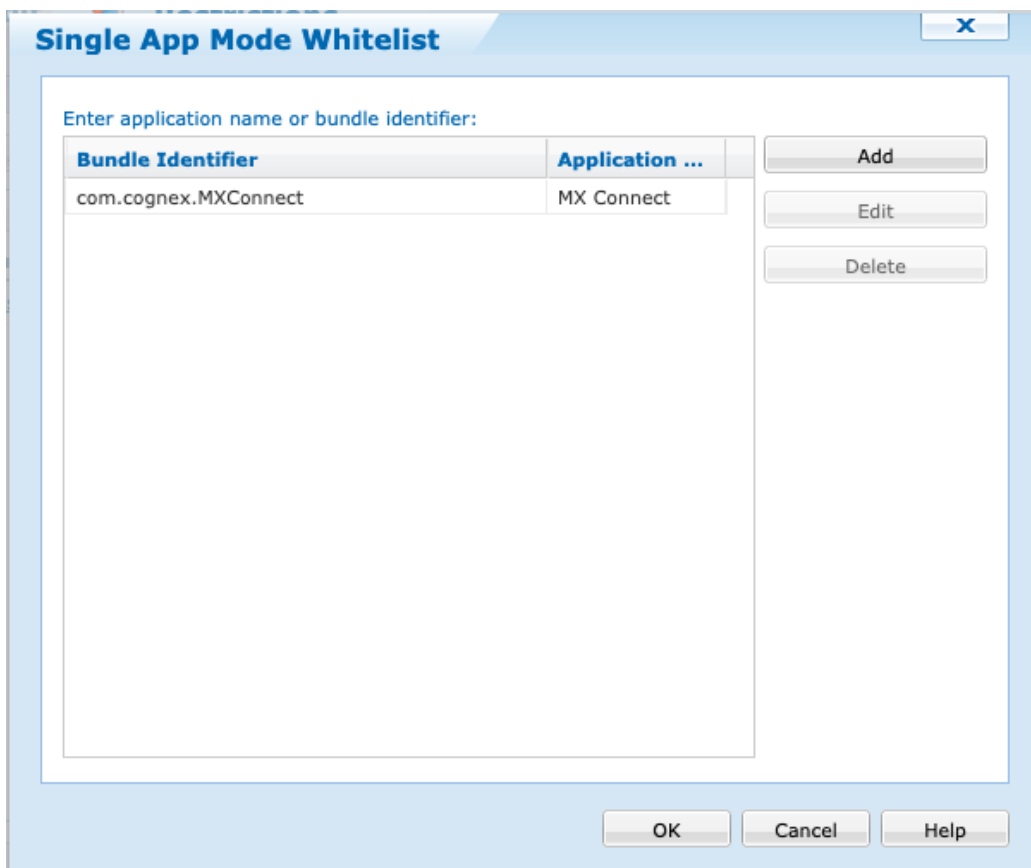
Select the Applications tab and MX Connect's bundle ID: com.cognex.MXConnect



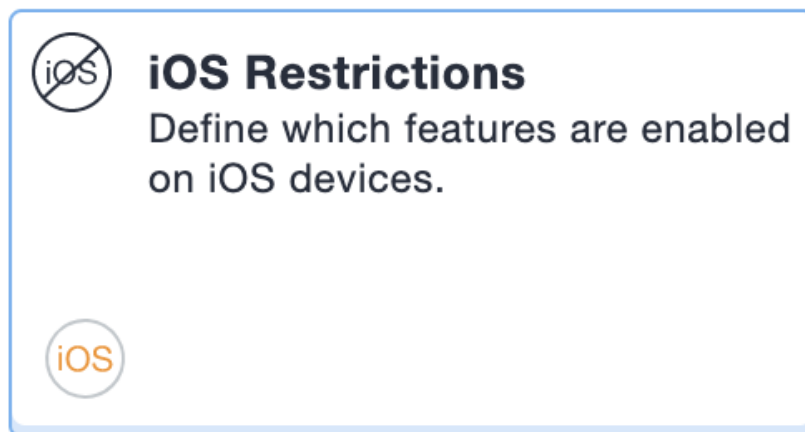
Select Restrictions to create an Autonomous Single App Mode configuration profile.



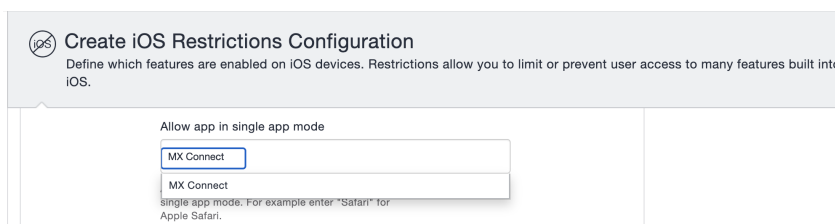
Select the Applications tab and add MX Connect's bundle ID (com.cognex.MXConnect) to the list.



To create an iOS restriction for ASAM mode for MX Connect app you have to select "iOS restriction" at type selection.



In the configuration section you have to add MX Connect to the appropriate field.



To send ASAM configuration to a particular device click on Push button on the device's Configuration tab.

Configurations

Overview
Configurations
Installed Apps
AppConnect Apps
Policies
Certificates
Sentry
Attributes
Logs

Distributed Configurations (8)
Excluded Configurations (0)

Distributed configurations on the device can be re-pushed if either an error occurred in the initial install or they are currently excluded. System configurations cannot be excluded.

Push Profiles
Exclude Profiles

	NAME	TYPE	STATUS	DISTRIBUTION METHOD	ACTIONS
☐	IOS MDM - Bulk Provisioned	Mobile Device Management	Installed	Device Group	Push Exclude
☐	Enable ASAM for MXConnect	iOS Restrictions	Installed	Device Group	Push Exclude

This option is not available on Workspace ONE for apps available in App Store.

What does it mean?

MX Connect cannot keep up single application mode during firmware upgrade roll-out if Single App Mode was turned off/deactivated too early (e.g. the update was still ongoing).

How can I avoid issues?

Inform your users not to navigate away from MX Connect if an upgrade operations has been started.

How shall I use Single App Mode?

You have to make sure that you do not disable Single App Mode until the installation of the firmware is finished on the MX mobile terminals. We would suggest to communicate a slot to your users when you plan to upgrade firmware on MX mobile terminals. 15 minutes slot should be enough to do the firmware upgrade but this may vary according to your network speed.

What happens if I disable Single App Mode when the upgrade process has not been finished?

If the user does not navigate away from MX Connect during the update process, then the operation will be finished and firmware/configuration file is rolled out to mx mobile terminal.

If the user navigates away (as MX Connect is not in single app mode user is not prevented to do this) then Firmware upgrade and configuration update may be interrupted and not processed until you start Single App Mode again.

7. Prepare a server to access firmware and configuration update files by URL.

During a firmware or configuration update MDM sends only the URLs of the update files to the MX Connect app, which downloads the update files using these URLs. Make sure that your update files are accessible by a URL, and set up a server to accomplish this requirement, if necessary. You can use Cognex' firmware storage to distribute upgrades. For more detail, refer to the [FAQ](#).

Update Firmware and Configuration on MX Mobile Terminal

1. Install MX Connect app (with your MDM system) on mobile devices.

If the MX Connect app is already installed on all iOS devices managed, skip this step (otherwise check Preparation step 4).

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
- [Workspace ONE](#)

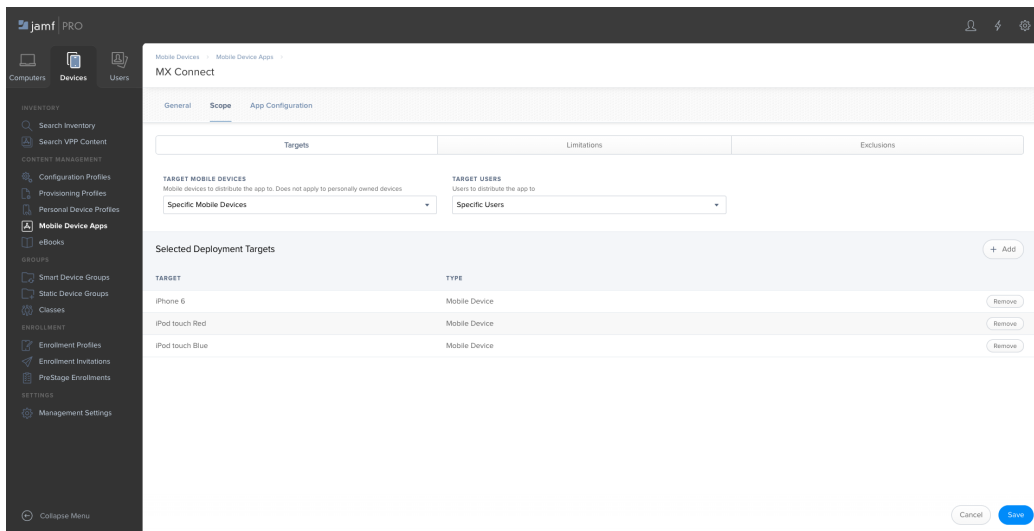
Once you have added MX Connect to your JAMF instance, apply two settings to automatically install to you device.

App install is automatic:

DISTRIBUTION METHOD Method to use for distributing the app

Install Automatically/Prompt Users to Install ▼

Add your iOS device to the app's scope:



Once you have added MX Connect to your SOTI instance, apply two settings to automatically install to you device.

Installing the app is automatic:

Advanced

X

Application Type:

Mandatory

☐ Prompt user to install application

5

 times

Provisioning Profile:

Browse

Bundle ID:

com.cognex.MXConnect

Search

Update Application

You can manually control the updates of your devices' mandatory or suggested applications. All devices targeted by this App Catalog Rule will download the latest version of the application supported by the corresponding device on the next device check-in.

Please consult the Management Service and corresponding Device logs for the status of the application update.

Push App Update

Options

Configure application specific security options at time of App Installation. (Requires iOS 5+)

☐ Remove App when device is un-enrolled
 ☐ Prevent application data back up to iTunes and iCloud

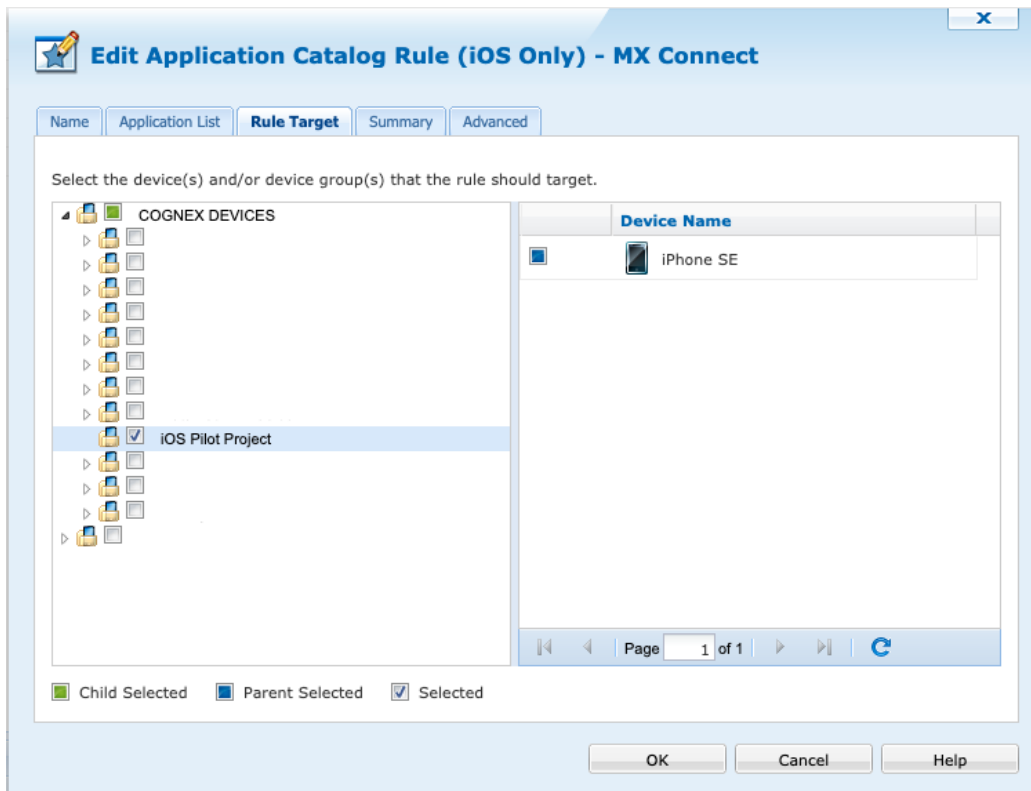
Default

OK

Cancel

Help

Add your iOS device to the app's scope:



To install MX Connect app on your device(s) you have to configure its Distribution settings in App Catalog.

[Apps](#) / [App Catalog](#) / Details

MX Connect
ios

Cognex Corporation | Delegation Status: App is not delegated

Sync new version

Details
Distribution
App Configurations
Reviews

Edit

App Distribution
Choose one of these options

Everyone

All users with compatible devices will see this app in the App Catalog

No One

No user will receive this app. (Stage for later distribution).

Custom

Define specific User Groups and Individuals who should see the app in the App Catalog

Current selection to distribute this app

Users
User Groups

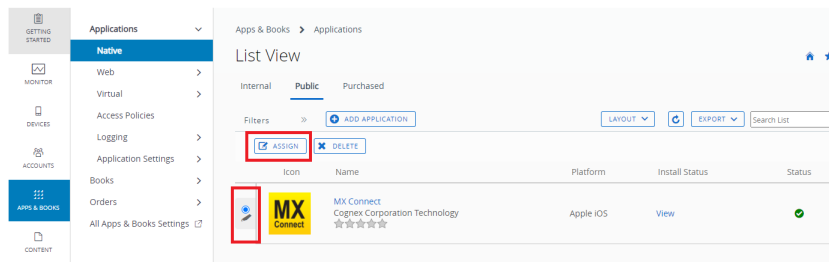
Search Selected Users

App Distribution Summary

This app will be sent to:

3 Individual Users

To install MX Connect app on your device(s) you have to configure its Assignment settings.

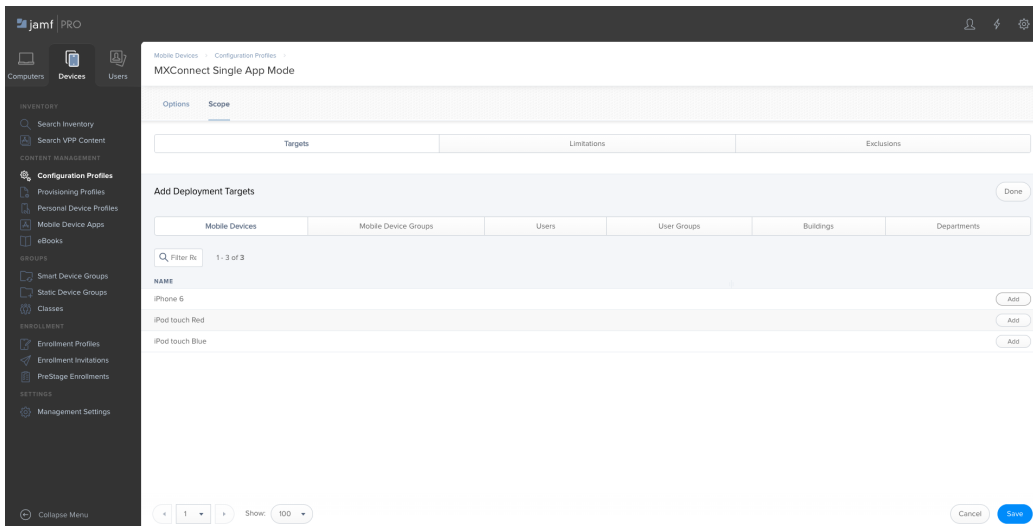


2. Launch MX Connect. To launch MX Connect, send a Single App Mode configuration profile to the iOS devices.

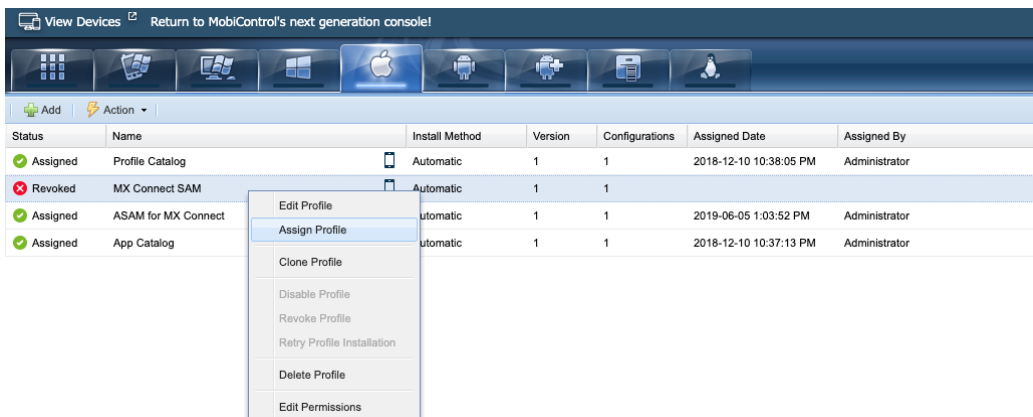
Revoke this profile manually to let the user of the iOS device switch to another application. Make sure to revoke SAM configuration profile, otherwise the company's daily workflow will be blocked because the designated application is not able to use the MX Connect.

- JAMF
- SOTI
- MobileIron
- Workspace ONE

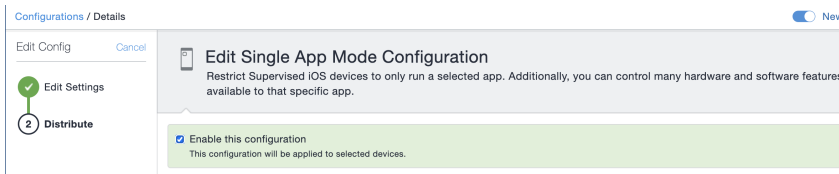
To launch MX Connect, put it to Single-App-Mode by adding your device to the SAM configuration profile's scope.



To launch MX Connect, put your device to Single-App-Mode by adding it to the SAM configuration profile's scope.

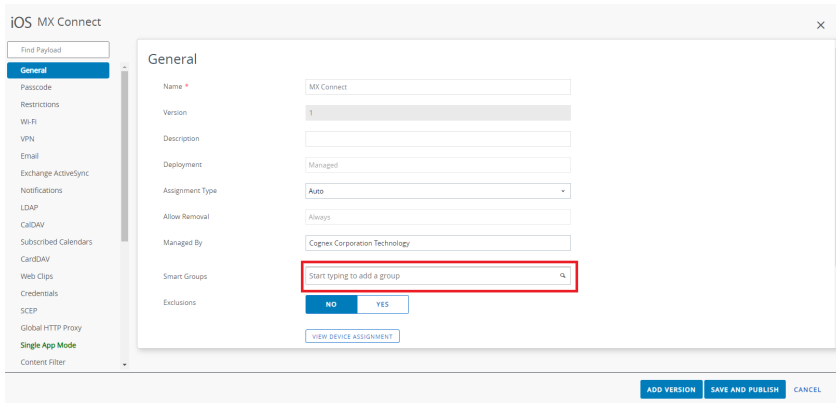


You have prepared a Single App Mode configuration. Edit this configuration and enable it by checking the appropriate option.



Please note that you have to uncheck this option after the installation process to terminate the Single App Mode.

Open the profile (that was created at Preparation step 5) and assign it to mobile phones (use smart group) where the MX terminal update is necessary.



If you revoke the Single App Mode configuration during an upgrade process, the app keeps the SAM until the installation is done. Exception is Workspace ONE as there is no Autonomous single app mode configuration for App store apps

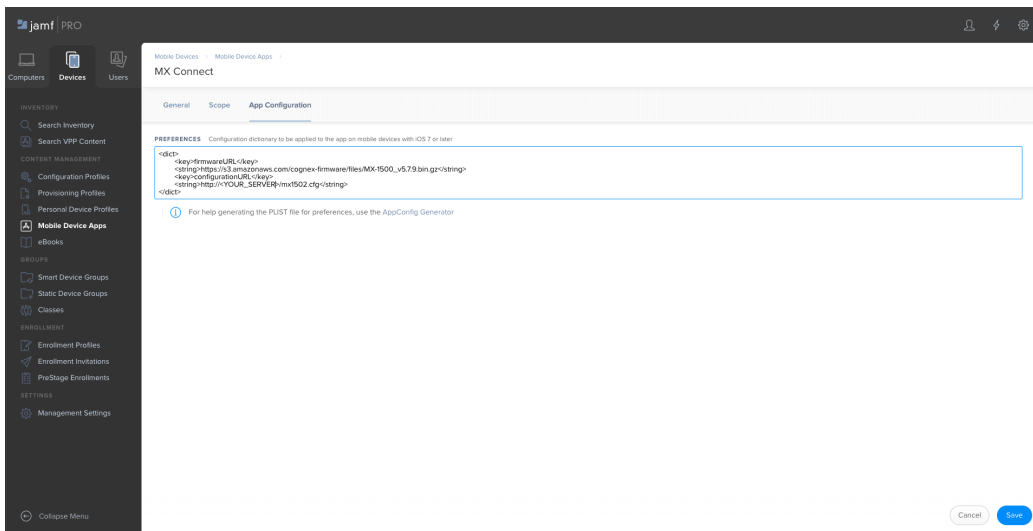
3. Send updates to the MX mobile terminal.

To send firmware or MX configuration updates, compose an XML text containing the URLs of the update files. The XML has to be provided to your MDM, which sends it to each MX Connect instance. MX Connect starts the update process upon receiving the XML configuration.

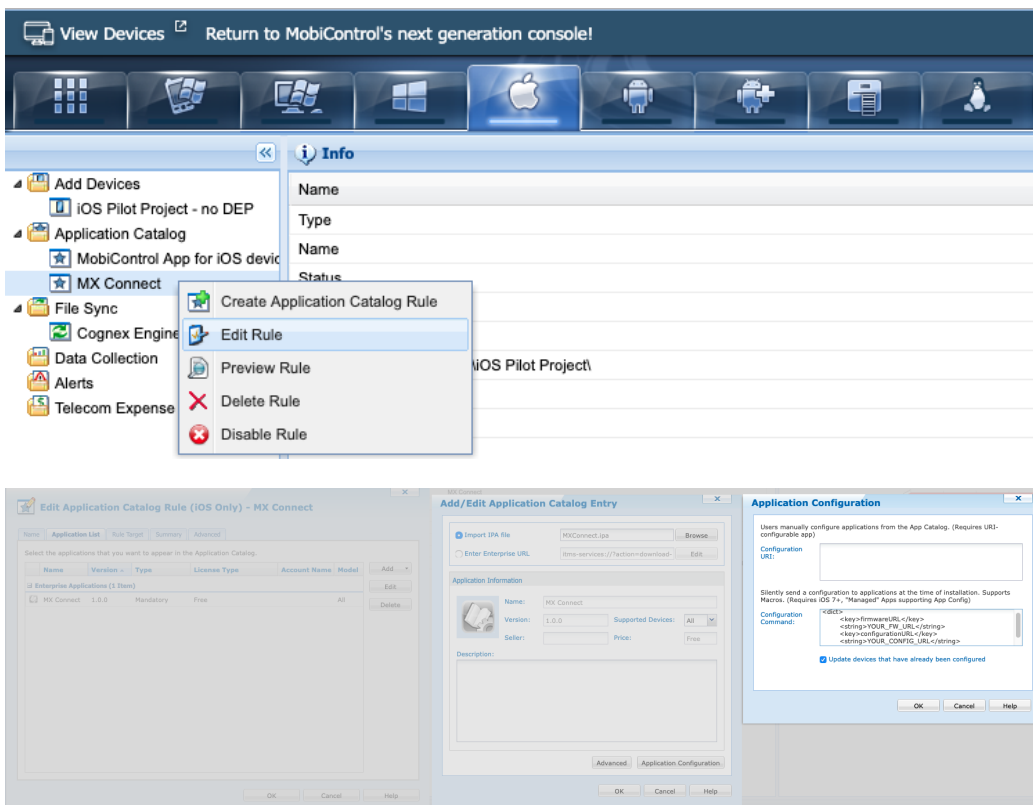
The XML composed is not a command but a configuration. The XML resides at MX Connect until the next XML configuration overwrites it. MX Connect will try to install the firmware and configuration using the defined URLs each time when the application starts. Firmware update is performed once and MX Connect checks whether the installed firmware matches with the firmware available on the MX mobile terminal. MX configuration update is performed multiple times when the application is opened, which takes only a few seconds.

- [JAMF](#)
- [SOTI](#)
- [MobileIron](#)
- [Workspace ONE](#)

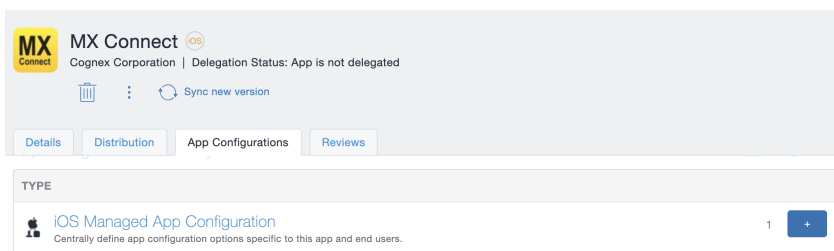
To send new updates to MX Connect, edit the App Configuration text at MX Connect's page. Use the proper form of the XML to perform a successful update.



To send new updates to MX Connect, edit the App Configuration text at MX Connect app's "Application Catalog Rule". Use the proper form of the XML to perform a successful update.



To create and send a Managed App Config go to MX Connect app's App Configuration tab and select iOS Managed App Configuration section.



Click on Add button and create a new configuration as indicated below.



MX Connect
ios

Cognex Corporation | Delegation Status: App is not delegated

Details
Distribution
App Configurations
Reviews

App Configurations Summary · **iOS Managed App Configuration**

Cancel
Save

Configuration Setup

Name

+ Add Description

Configuration Source

Source Type

None

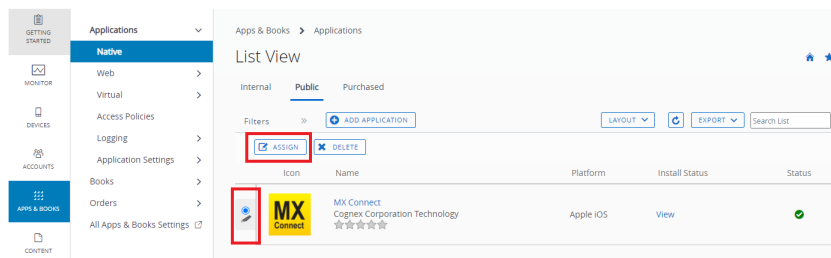
iOS Managed App Settings

Key	Value	Type
firmwareURL	my_url_to_fw_file	STRING
configurationURL	my_url_to_config_file	STRING

+ Add | Use .plist

Array type values should be separated by comma (example: 2,33,44) and date value should be in milliseconds (example: 1437496170000).

Open Application settings for MX Connect app and select Assign.



Select the actual MX Connect assignment and edit *Application configuration*. Turn on *Send configuration* setting.

MX Connect - Assignment

- Distribution
- Restrictions
- Tunnel & Other Attributes
- Application Configuration**

Application Configuration

EMM Managed Access

Only devices enrolled in EMM will be allowed to install the app and receive policies below.

Managed Access

Send Configuration

Configuration Key	Value Type	Configuration Value
firmwareURL	String	https://myserver.com/firmwares/firmware_...
configurationURL	String	https://myserver.com/configs/config_...

CANCEL
SAVE

Depending from MDM you have to enter an XML as configuration or you can add key-value pairs as a configuration or you can pick your preferred method.

- Use the following template to compose a configuration XML:

```
<dict>
  <key>firmwareURL</key>
  <string>https://myserver.com/firmwares/firmware_file_name</string>
</dict>
```

```
<key>configurationURL</key>
<string>https://myserver.com/configs/config_file_name</string>
</dict>
```

- Define the following key value pairs:

KEY	TYPE	VALUE
firmwareURL	string	https://myserver.com/firmwares/firmware_file_name
configurationURL	string	https://myserver.com/firmwares/firmware_file_name

Note that all key-string pairs are optional. MX Connect does not perform any update or check for a missing field, and does not restore any kind of default value for a missing field. If you configure both the firmwareURL and the configurationalURL with new values, MX Connect first installs the firmware rebooting the MX mobile terminal, then processes the configuration file.

- Revoke Single App Mode from MX Connect to remove devices from SAM.

Adding MDM reporting to an application

A company owning and operating many Cognex Mobile Terminals may want to remotely collect up-to-date information about battery level, battery health, installed firmware, etc. An iOS application using the cmbSDK framework can report status information of the attached Mobile Terminal to an MDM instance. Cognex mobile apps (MX Connect, Cognex Quick Setup...) can be also configured to report MX data.

Preparing your iOS application for reporting data about MX mobile terminal

Any iOS application is capable of reporting Mobile Terminal status information if it embeds and uses the cmbSDK framework.

- Update cmbSDK framework in your app to use at least 2.4.0 version.
- Configure reporting for the app in your MDM.

Configuring the reporting functionality from MDM

Reporting is done by an iOS application towards an MDM instance. The app has to be managed by the MDM instance and can only report to that MDM instance. There are a few configuration options the MDM administrator has to properly set to let the reporting feature work for a certain application. These settings are done by creating a proper Managed App Configuration including key-value pairs as the configuration of reporting. Please refer to your MDM's administration guide to learn how to edit Managed App Configuration of a managed mobile app.

Mandatory configuration fields

As described above the MDM's administrator has to compose a Managed App Configuration to define settings of the reporting. This Managed App Configuration is sent to the mobile app by the MDM to let the app process it and behave accordingly. Please note that providing a proper Managed App Configuration is mandatory to enable the reporting. Without that the cmbSDK (in the app) won't start reporting.

The mandatory configuration fields are the following.

KEY	TYPE	DESCRIPTION
-----	------	-------------

KEY	TYPE	DESCRIPTION
mxReportingEnabled	Bool	It has to be set to true to enable reporting.
mxReportingURL	String	This URL has to point to your MDM instance including port number if necessary.
mxReportingIntervalMinutes	Integer	Reporting frequency in minutes, minimum value is 1.
mdmType	String	The type of your MDM. Possible values: "AirWatch", "Jamf", "MobileIronCloudV1", "SOTI"
mdmDeviceID	String	This field is a technical field that has to be set with a constant depending on your MDM type. SOTI: %DeviceIdentifier% Jamf: \$JSSID MobileIron: \${devicePK} Workspace ONE / Airwatch: {DeviceSerialNumber}

Developer hint

It is possible to turn on/off the reporting from the source code of your application by changing *MDMReportingEnabled* property of your *CDMDataManSystem* instance. Please note that the default value is false for *MDMReportingEnabled*. Please be aware that the mandatory fields still needs to be configured in MDM.

Authentication fields

For cmbSDK connecting to your MDM instance will most likely require authentication credentials. Beside the mandatory configuration fields you also have to provide these in the Managed App Configuration as indicated in the following table.

KEY	TYPE	SOTI	JAMF	MOBILEIRON	AIRWATCH	DESCRIPTION
mdmReportingClientID	String	x				Application needs to be added as API client and generate this ID
mdmReportingClientSecret	String	x				Application needs to be added as API client and generate this secret
mdmReportingPassword	String	x	x	x	x	Password
mdmReportingUsername	String	x	x	x	x	User name
mdmTenantCode	String				x	The key value is available in the system settings when REST API access is enabled.

Please note that you have to provide a registered user's credentials that has the right to use the MDM's API for reporting. Refer to your MDM's administrator guide to learn more.

Developer hint

If you don't want to provide authentication credentials via Managed App Config for some reason these can be set by the cmbSDK's API from your app's code. It gives you full flexibility to retrieve authentication credentials in the way your company's policy requires. To do so you have to set the *defaultMDMAuthCredentials* property of *CDMDataManSystem* class.

- [Swift](#)
- [Objective-C](#)

```
var authCredentials: MDMAuthCredentials = MDMAuthCredentials()
authCredentials.username = "usr"
authCredentials.password = "pwd"
authCredentials.clientID = "myClientID"
authCredentials.clientSecret = "myClientSecret"
self.dataManSystem.defaultMDMAuthCredentials = authCredentials
self.dataManSystem.MDMReportingEnabled = true // if you want to start reporting
```

```
MDMAuthCredentials *authCredentials = [MDMAuthCredentials new];
authCredentials.username = "usr";
authCredentials.password = "pwd";
authCredentials.clientID = "myClientID";
authCredentials.clientSecret = "myClientSecret";
self.dataManSystem.defaultMDMAuthCredentials = authCredentials;
self.dataManSystem.MDMReportingEnabled = true; // if you want to start reporting
```

Please note that if you set authentication credentials both in the Managed App Config and via *defaultMDMAuthCredentials* property the fields in the Managed App Config will overwrite the fields in the *defaultMDMAuthCredentials* property per field basis. This precedence allows your MDM administrator to make some fix/change without rebuilding and deploying your application.

Reported information

The following data of the attached Mobile Terminal is collected:

ATTRIBUTE NAME	TYPE	FORMAT	DESCRIPTION
MX Device Variant	Text	MX-1XXX VARIANT	Example MX-1502 ER is shown for extended range MX-1502 mobile terminals
MX Device Name	Text		MX-1XXX-YYYYYYY names are used by default, but it may be different according to configuration
MX Serial Number	Text	14 character	
MX Pistol Grip Battery Level	Number	X	-1 means no battery is available
MX Flat Battery Level	Number		
MX Pistol Grip Battery Health	Number		

ATTRIBUTE NAME	TYPE	FORMAT	DESCRIPTION
MX Flat Battery Health	Number		
MX Firmware Version	Text	A.B.C_D	Example: 5.7.9_sr3
MX Status Date	Date	Depends from you MDM local settings	Contains the timestamp (in case of SOTI only date) for the last report.
MX Status Timestamp	Text	YYYY-MM-DD HH:MM:SS (24H)	Contains the exact timestamp for the last report. Available only on SOTI.

Custom attributes in MDM

The reported data fields appear as custom/extension attributes in MDM.

Jamf, SOTI, and Workspace ONE / Airwatch

These custom attributes are global attributes. These are assigned to all enrolled devices in case of Jamf and SOTI and are assigned only to the devices that have reported data in the case of Airwatch. By default the custom attributes are not present in an MDM instance, the properly configured mobile app creates the custom attributes automatically via the MDM's API and neither the app developer nor the MDM administrator has to take care of it.

MobileIron Cloud

Preparing custom/extension attributes to require two steps:

- First custom attributes have to be defined at Admin/System/Attributes. **MDM admin has to add manually** all relevant attributes that you want to check. Use the names from the table above but replace spaces with an underline (e.g.: MX_Pistol_Grip_Battery_Level)
- The second step is assigning these attributes to the device(s). This second step is **automatically performed the apps that includes cmbSDK**, you don't have to do it manually. So please be sure to first define the custom attributes before using cmbSDK for reporting.

Summary of all requirements

- It is possible to use your own app for reporting, but Cognex mobile apps can be also configured to send data to MDM.
- Your app has to use the cmbSDK framework (2.4.0 version or later) and has to be managed by your MDM.
- The app has to be in the foreground and has to connect to the attached Mobile Terminal via cmbSDK.
- If you are using multiple apps during your work and you want to make sure of the continuity in reporting, we suggest configuring both apps in MDM.
- The mobile phone has to have a proper network connection to reach your MDM instance.
- It is mandatory to have a proper Managed App Configuration sent to your app by your MDM to enable reporting.
- Authentication credentials have to be complete and valid for the usage of your MDM API.
- Do not modify or delete manually the created custom attributes on your MDM instance.
- In the case of MobileIron Cloud, you have to first define the custom attributes manually on the admin site.
- MX data reporting is available in Cognex apps from the following versions:
 - Cognex Quick Setup (available from version 2.4.2)
 - MX Browser (available from version 2.0.2)
 - MX Connect (available from version 1.0.2)
 - MX Keyboard (not available yet)