McAfee MVISION Mobile

SOTI MobiControl

Integration Guide

January 2021

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface 5

Audience 5

Related Documentation 5

Overview 5

Prerequisite Requirements 6

About MDM and MVISION Mobile Console Communication 6

Device Application Deployment Set Up 7

Overview 7

SOTI MobiControl User with Administrator Access 7

Google Managed Enterprise for MobiControl 8

Device Groups 9

Application Catalog Rule 10

About MVISION Mobile Deployment 11

About Deployment Options 11

Configuring Device Application Auto-Activation 13

iOS Activation 13

Android Activation 14

Android Personal Profile Auto-Activation 15

Add Devices Rule 15

Manual Activation 16

Configuration Steps 18

Synchronization Overview 18

Enrolling the Device 18

On-Demand MDM Synchronization 20

Set Up Synchronization in MVISION Mobile Console 20

Device Actions and Remediation 23

Creating a Custom Attribute 23

Available Device Actions 25

Synchronizing iOS Apps and iOS Profiles 26

Preface

This document is an administrator's guide to providing integration with SOTI MobiControl Mobile Device Management (MDM).

Audience

The intended audience for this guide is a MVISION Mobile Console administrator. This guide helps administrators to provide integration with the SOTI MobiControl MDM. The MVISION Mobile Console application provides threat protection to mobile devices. The system administrator sets policies for threats and the MDM configuration.

See "*MVISION Mobile Console Product Guide*" for more information.

Related Documentation

For more information and specific configuration information about MDM, SIEM, and iOS, Android Platforms, search for "MVISION Mobile" in the McAfee document Portal at https://docs.mcafee.com

Overview

Integration with a Mobile Device Management (MDM) is not required. However, when an MDM is integrated, the MVISION Mobile Console does the following:

- Synchronizes devices with the MDM
- Provides transparent user access to MVISION Mobile
- Provides more granular and specific protection actions

McAfee's MVISION Mobile application detects malicious activity and depending on the MDM platform, is able to take action locally. When MVISION Mobile is integrated with an MDM, protection actions can be performed by the MDM in addition to local MVISION Mobile actions, providing a very powerful protection tool. In the SOTI MobiControl integration, device synchronization is supported, along with device actions.

Prerequisite Requirements

Integration with SOTI MobiControl requires a connection between the MVISION Mobile Console and the IBM MaaS360 server. This is accomplished with the Internet using SSL.

The following table details specific requirements for the connection.

Item	Specifics
SOTI MobiControl App on an MDM Enrolled Device	Release 13.2 and above
SOTI MobiControl Console Access	Access to SOTI MobiControl website at: **https://***yourHost***.mobicontrolcloud.com/MobiControl** where *yourHost* is the URL portion provided from SOTI. Release 14.1.7 or later
An Administrator Account in SOTI MobiControl Console	You need an administrator login with the user group 'MobiControl Administrators' permission allocated.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the SOTI MobiControl console through an integration. When MVISION Mobile detects an event, it consults the current Threat Policy on the device and if there is a specific MDM action defined, this is communicated to the MVISION Mobile Console server. The MVISION Mobile Console then reaches out to the proper SOTI MobiControl server and provides the commands to perform the action described.

Device Application Deployment Set Up

Overview

This section covers device application deployment and describes the initial setup required. For the initial setup you define or configure:

- Administrator User with Access
- Device Group
- Application Catalog Rule
- Add Devices Rule
- MVISION Mobile Applications (iOS and Android)

Refer to the SOTI MobiControl documentation website for more information on how to use the console: https://www.soti.net/mc/help/v14.2/en/console/helpindex.html

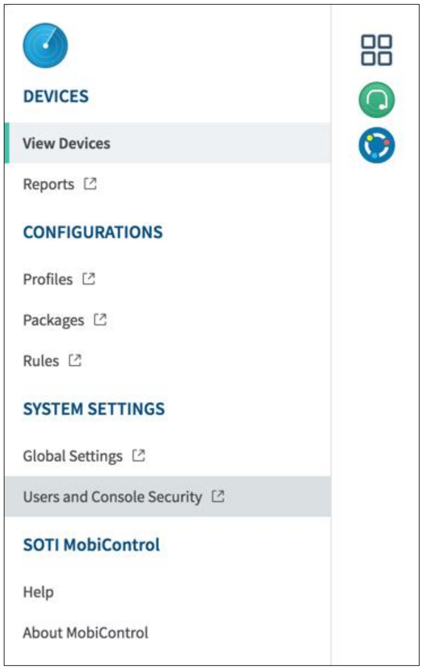
SOTI MobiControl User with Administrator Access

Log in to the SOTI MobiControl console and define a user as belonging to the 'MobiControl Administrator' user group.

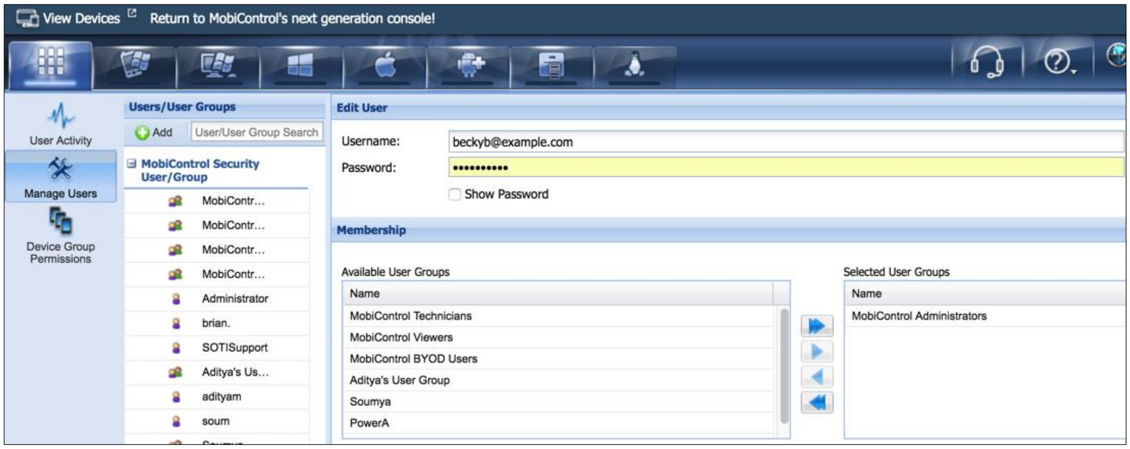
To create a SOTI MobiControl administrator with the proper access:

1. From the main menu, select **Users and Console Security**.
2. Click **Manage Users**.
3. Enter a username and password for the new administrator.
4. Select the MobiControl Administrator user group for the user.

This figure shows the menu selection for creating the user.



This figure shows the email username with the required user group. This provides the necessary permissions to create device groups and rules and integrate with MVISION Mobile Console.



Username: beckyb@example.com

Password: ••••••••••

□ Show Password

Available User Groups

Name
MobiControl Technicians
MobiControl Viewers
MobiControl BYOD Users
Aditya's User Group
Soumya
PowerA

Selected User Groups

Name
MobiControl Administrators

Google Managed Enterprise for MobiControl

For setting up Android devices, these additional setup items are needed before the Device Groups, Application Catalog Rule, or Add Devices rules are created.

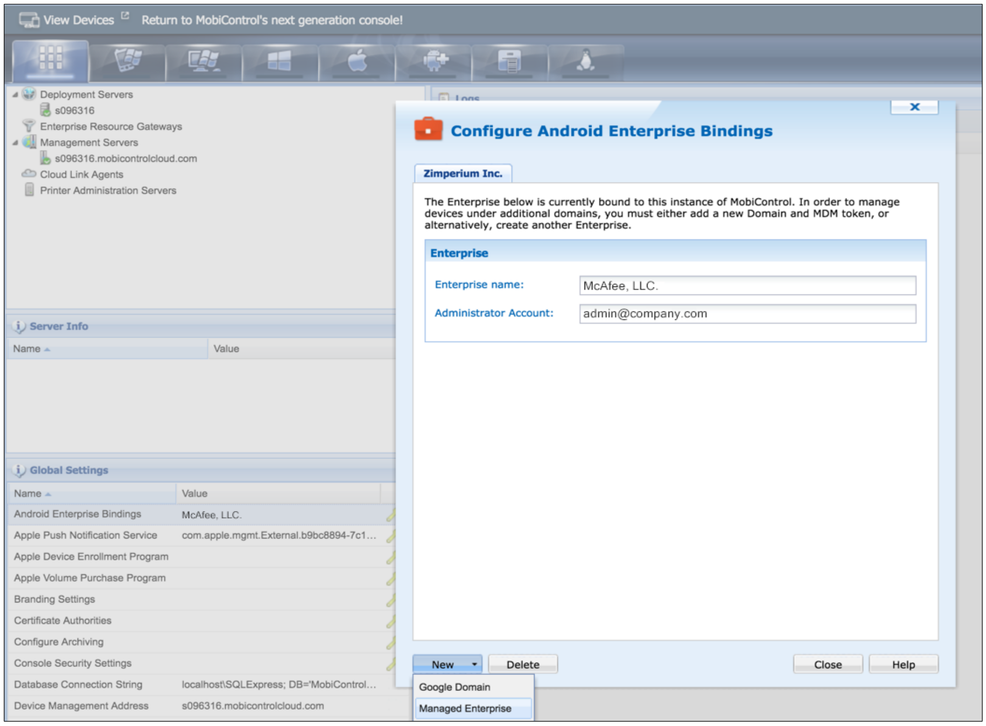
Log in to the SOTI MobiControl console and perform these steps:

1. From the main menu, select **Global Settings**.
2. Click the **Servers** tab at the bottom.
3. Click the change icon for the ‘Android Enterprise Bindings’.
4. Click **New**.
5. Click **Managed Enterprise**.
6. You are then redirected to Google's Managed Enterprise Enrollment page. Fill in any necessary information. Once you complete this setup, you are redirected back to MobiControl.
7. Click **OK** to continue.
8. Enter the Enterprise Name and the email for the administrator and click **OK** to complete the ‘Android Enterprise Bindings’ setup.

For more information, refer to SOTI MobiControl’s documentation website:

https://www.soti.net/mc/help/v14.1/en/console/devices/managing/enrolling/platforms/afw/mgpa_enterprise_create.html

This figure shows the selection of Managed Enterprise. This already has the name and email set.



Configure Android Enterprise Bindings

Zimperium Inc.

The Enterprise below is currently bound to this instance of MobiControl. In order to manage devices under additional domains, you must either add a new Domain and MDM token, or alternatively, create another Enterprise.

Enterprise

Enterprise name: McAfee, LLC.

Administrator Account: admin@company.com

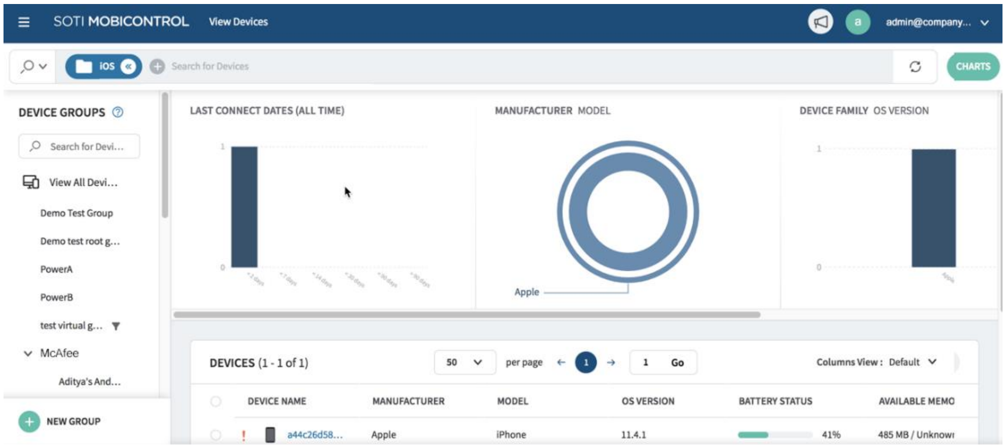
Global Settings

Name	Value
Android Enterprise Bindings	McAfee, LLC.
Apple Push Notification Service	com.apple.mgmt.External.b9bc8894-7c1…
Apple Device Enrollment Program	
Apple Volume Purchase Program	
Branding Settings	
Certificate Authorities	
Configure Archiving	
Console Security Settings	
Database Connection String	localhost\SQLExpress; DB='MobiControl…
Device Management Address	s096316.mobicontrolcloud.com

Device Groups

The device groups are used to organize and synchronize devices with MVISION Mobile Console. You can choose how your devices are organized into one or more device groups. For example, the device groups can organize devices for different device operating systems.

Rules are created within a specific OS domain, so aligning device groups in the same way is a good practice. This figure shows an example device group named 'iOS' after a sync of devices has occurred



DEVICES (1 - 1 of 1)

DEVICE NAME	MANUFACTURER	MODEL	OS VERSION	BATTERY STATUS	AVAILABLE MEMO
a44c26d58…	Apple	iPhone	11.4.1	41%	485 MB / Unknowı

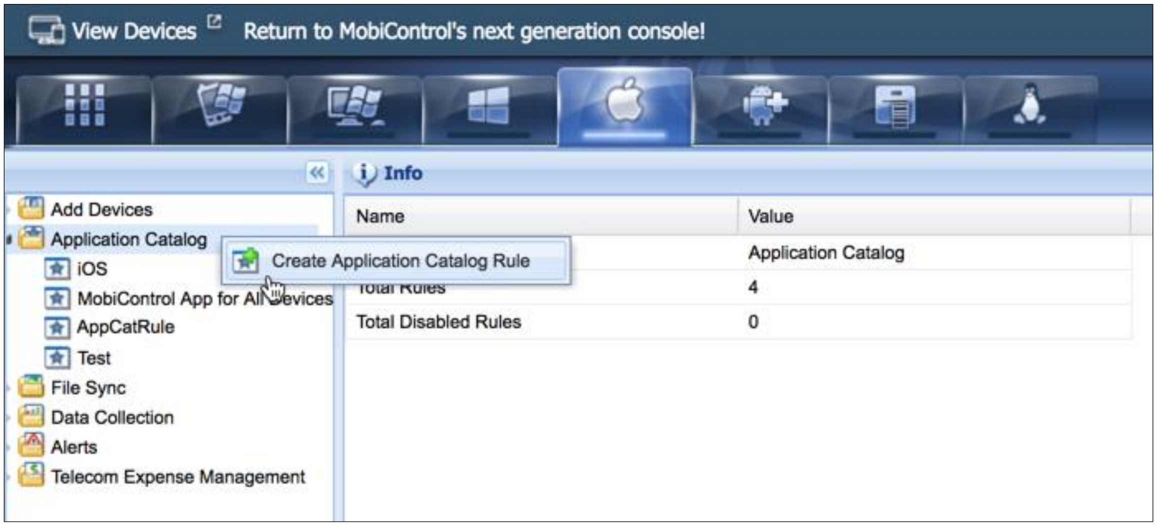
Application Catalog Rule

The application catalog rule defines a collection of the applications that are pushed to the devices. At least one application catalog rule is needed for iOS and one for Android.

To create the application catalog rule, perform these steps:

1. Select the menu icon and then select **Rules**.
2. Select the desired OS, and then right-click on **Application Catalog** to select the option to **Create Application Catalog Rule**.
3. Define at least the MVISION Mobile application for deployment on the device by:
   a. Provide a name for the rule.
   b. Select **Add** and select **Enterprise Applications** for iOS and **Managed Google Play Applications** for Android.
   c. Provide the path of the IPA or APK file for the MVISION Mobile application and the file is uploaded to the SOTI MobiControl console. See the "About MVISION Mobile Deployment" section for more information.
   d. Click **Advanced** and select the Application Type value. The mandatory value is recommended. See the "About Deployment Options" section for more information.
   e. Click **Ok** twice.

The figure shows the option to create this rule in the SOTI MobiControl console


View Devices
Return to MobiControl's next generation console!
Info
Add Devices
Application Catalog
Create Application Catalog Rule
iOS
MobiControl App for All Devices
AppCatRule
Test
File Sync
Data Collection
Alerts
Telecom Expense Management

Name	Value
	Application Catalog
Total Rules	4
Total Disabled Rules	0

Optionally include additional apps in the collection of the apps to be pushed to the device. Now the install files for the MVISION Mobile app are associated with the application catalog rule.

About MVISION Mobile Deployment

To deploy the MVISION Mobile application through SOTI MobiControl MDM, use the version of MVISION Mobile available through either the Apple App Store or Google Play Store. Both MVISION Mobile iOS and Android are in their respective public application stores, and it is good practice to deploy the latest MVISION Mobile application through SOTI MobiControl.

To obtain the MVISION Mobile application from the public application store, search the appropriate store for MVISION Mobile. Or, you can use these links:

iOS MVISION Mobile: https://apps.apple.com/us/app/mcafee-mvision-mobile/id1435156022

Android MVISION Mobile:
https://play.google.com/store/apps/details?id=com.mcafee.mvision

To deploy as an internal app, log in to SOTI MobiControl, upload the proper application file (IPA for iOS and APK for Android) to SOTI MobiControl under the appropriate application catalog rule. Then, SOTI distributes MVISION Mobile to the devices.

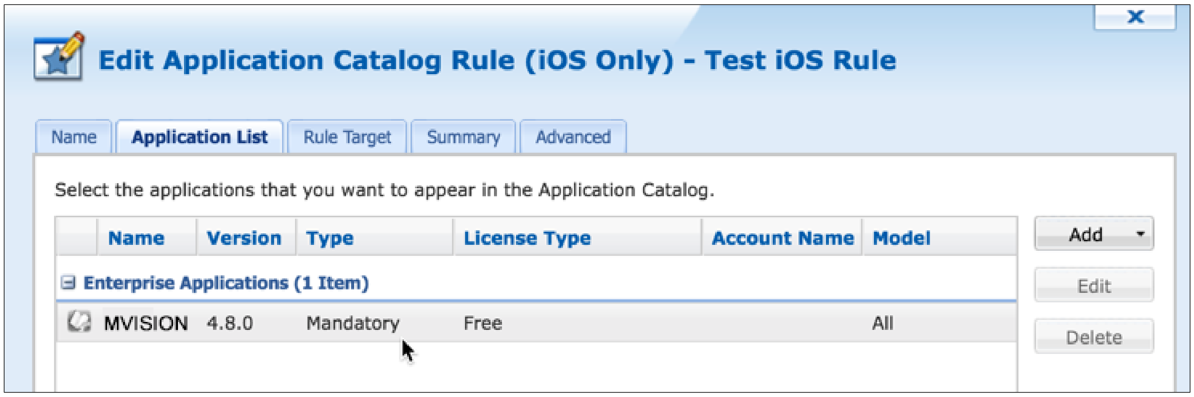
Depending on customer requirements, a custom version of the app can be needed. In that case, contact your Customer Success team, and the custom version of MVISION Mobile can be added as an internal app in SOTI.

About Deployment Options

You can deploy MVISION Mobile two different ways to the device:

- The MVISION Mobile app is pushed by SOTI MobiControl to the device and the user is prompted to accept the install request. (A Mandatory setting for the Application Type)
- The user taps on the MVISION Mobile app inside the SOTI MobiControl App Catalog and installs MVISION Mobile from there. (This is with a 'Suggested' setting for the Application Type.)

These options are determined by the type setting on the App Catalog rule. The mandatory setting pushes the MVISION Mobile app by SOTI, and the user is prompted to accept the install. This figure shows the Mandatory type setting for the application on a sample rule.

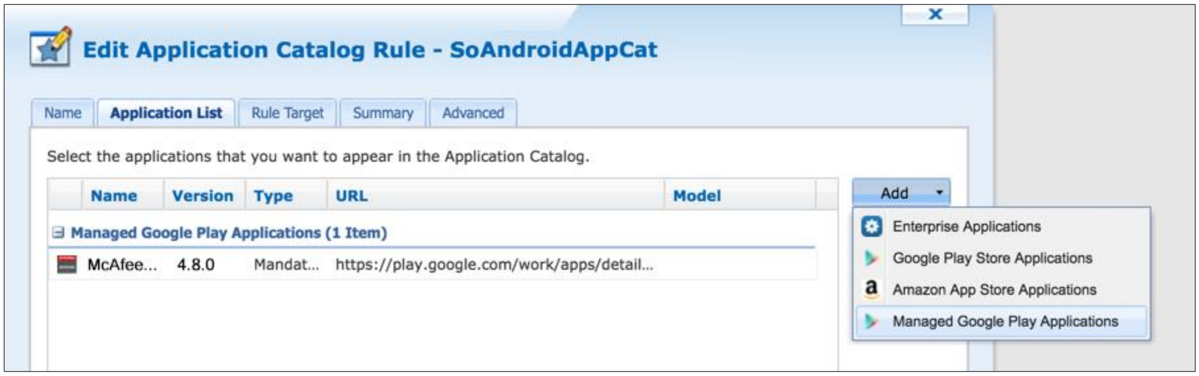


Edit Application Catalog Rule (iOS Only) - Test iOS Rule

Select the applications that you want to appear in the Application Catalog.

Name	Version	Type	License Type	Account Name	Model
Enterprise Applications (1 Item)					
MVISION	4.8.0	Mandatory	Free		All

This figure example is for adding the Android version of the application.



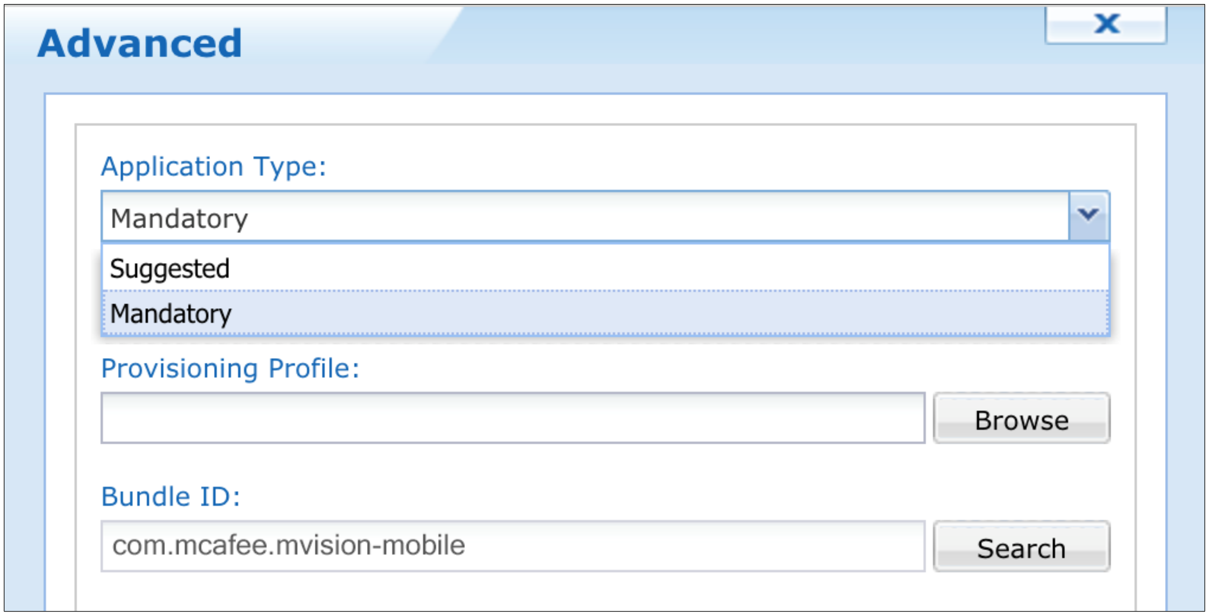
Edit Application Catalog Rule - SoAndroidAppCat

Name
Application List
Rule Target
Summary
Advanced
Add
Enterprise Applications
Google Play Store Applications
Amazon App Store Applications
Managed Google Play Applications

Select the applications that you want to appear in the Application Catalog.

Name	Version	Type	URL	Model
Managed Google Play Applications (1 Item)				
McAfee...	4.8.0	Mandat...	https://play.google.com/work/apps/detail...	

To set the type as mandatory, you select the MVISION Mobile app entry in the application list and select **Edit**. Then, click **Advanced**, and set the Application Type value to mandatory.



Advanced

Application Type: Mandatory

Provisioning Profile:

Bundle ID: com.mcafee.mvision-mobile

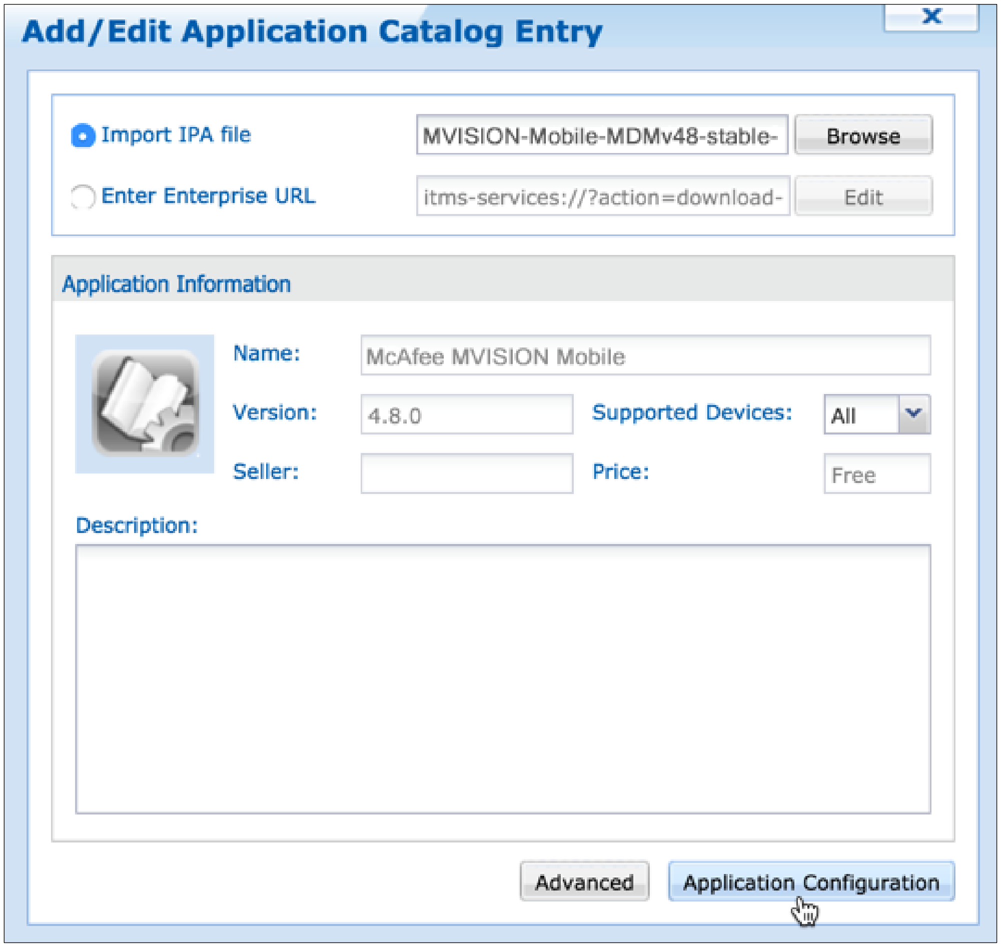
Configuring Device Application Auto-Activation

The MVISION Mobile applications for both iOS and Android Enterprise can automatically activate. The process is different on each platform as described below.

iOS Activation

McAfee's MVISION Mobile iOS application takes advantage of the application configuration when the app is pushed down to the device. This provides the best user experience, allowing the user to startup MVISION Mobile iOS without having to enter any credentials. The application configuration pre-programs MVISION Mobile iOS with the required information.

This configuration is performed within SOTI MobiControl. During the add application step, there is a configuration option. As another alternative, you can edit the application after the application is added.



Add/Edit Application Catalog Entry

● Import IPA file: MVISION-Mobile-MDMv48-stable-

○ Enter Enterprise URL: itms-services://?action=download-

Application Information

Name: McAfee MVISION Mobile

Version: 4.8.0

Supported Devices: All

Seller:

Price: Free

Description:

Use these configuration values.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	% DeviceIdentifier %
tenantid	String	Copy the value from the **Tenant ID** field on the MVISION Mobile Console **Manage** page under the **General** tab.
defaultchannel	String	Copy the value from the **Default Channel** field on the MVISION Mobile Console **Manage** page under the **General** tab.
display_eula	String	no (Optional) If this key is not used, the default displays the End User License Agreement (EULA).

NOTE: *The configuration keys are case sensitive*.

Set the PLIST XML in the Configuration Command field. This shows an example PLIST XML value.

```
<dict>
   <key>MDMDeviceID</key>
   <string>%DeviceIdentifier%</string>
   <key>defaultchannel</key>
   <string>https://acceptor.mcafee-mivision-mobile.com/srx</string>
   <key>tenantid</key>
   <string>demo</string>
</dict>
```

Android Activation

Android Enterprise users can use the managed app configuration for activations. You need to make sure you are passing the right device ID value for the configuration parameter. The configuration key variables are the same set as the PLIST variables in the "iOS Activation" section. Ensure for Android that these items are completed:

- The Android Enterprise Bindings is set up.
- The Application Catalog Rule links to the Managed Google Play Applications.
- The Add Devices Rule is linked to the Android Enterprise Binding.
- The configuration keys are set up similarly to iOS keys with the exception of the Android personal profile auto-activation keys and values.

See "Google Managed Enterprise for MobiControl" for information on setting up the Android application.

NOTE: *SOTI MobiControl requires auto-activation for Android devices.*

Android Personal Profile Auto-Activation

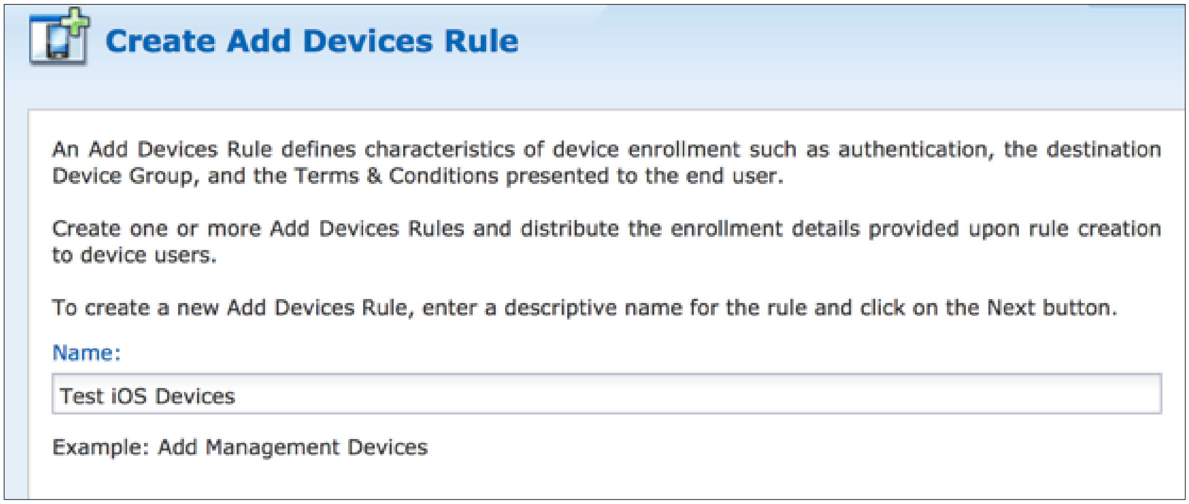
For MVISION Mobile release 4.80 and later, use these additional configuration keys and values for auto-activation for the personal profile in an Android Enterprise configuration.

Configuration Key	Value Type	Configuration Value	Notes
share_activation_data	String	true	This is required if you want to auto-activate the personal profile application. This defaults to 'false'.
activation_package	String	Bundle Id of the app to query for the activation information. The default is 'com.mcafee.mvision'.	(Optional) This is only needed if share_activation_data is true.

Add Devices Rule

Devices synchronize with MobiControl by using the 'Add Devices' rule. This rule determines the behavior of devices as they enroll with the SOTI MobiControl MDM. As you create this rule, you can select how your devices are organized into devices groups.

The example 'Test iOS Rule' in the figure is for a specific device group. It is associated with the group 'iOS' and provides the enrollment information for the user to enroll. The addition of this rule provides an enrollment profile. It supplies the enrollment information for deploying the MobiControl apps to a user's device, and then the MVISION Mobile app is pushed to the device.



Create Add Devices Rule

An Add Devices Rule defines characteristics of device enrollment such as authentication, the destination Device Group, and the Terms & Conditions presented to the end user.

Create one or more Add Devices Rules and distribute the enrollment details provided upon rule creation to device users.

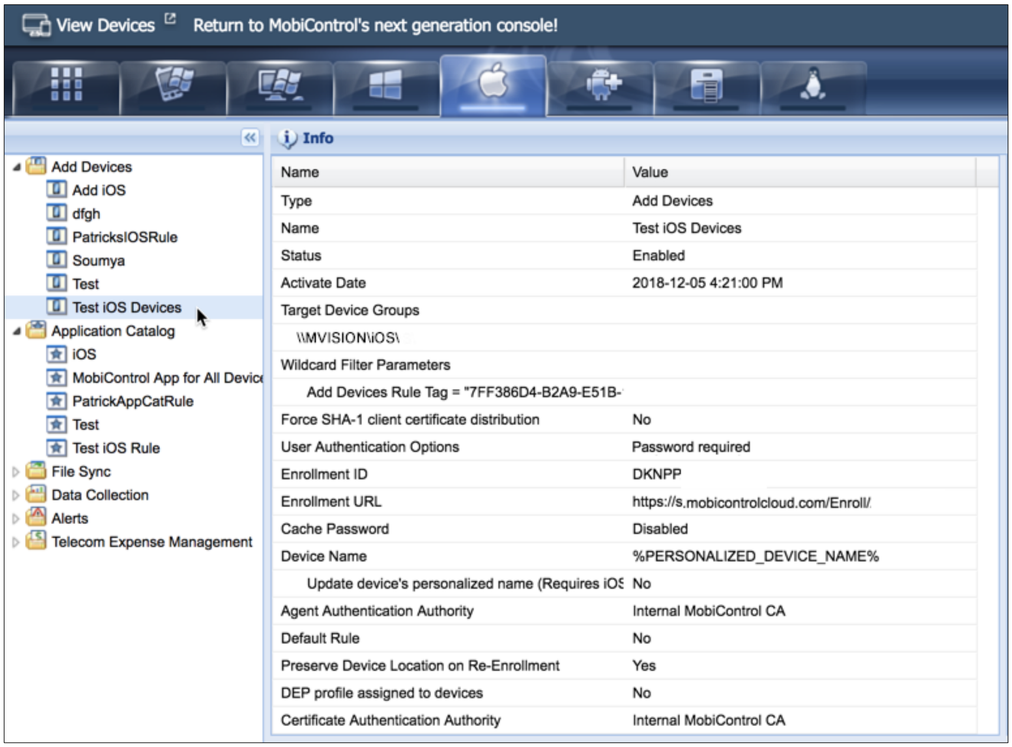
To create a new Add Devices Rule, enter a descriptive name for the rule and click on the Next button.

Name:

Test iOS Devices

Example: Add Management Devices

This figure shows the result of creating the add devices rule for iOS. It shows your 'Enrollment ID' and a URL that can be used to activate the device.



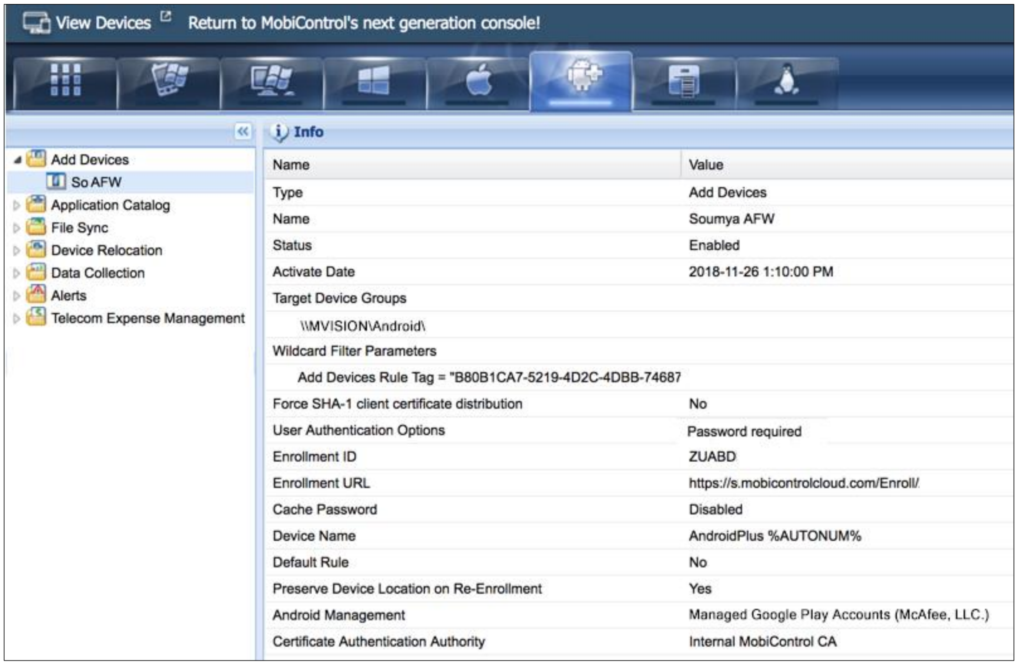
View Devices Return to MobiControl's next generation console!

- Add Devices
  - Add iOS
  - dfgh
  - PatricksIOSRule
  - Soumya
  - Test
  - Test iOS Devices
- Application Catalog
  - iOS
  - MobiControl App for All Device
  - PatrickAppCatRule
  - Test
  - Test iOS Rule
- File Sync
- Data Collection
- Alerts
- Telecom Expense Management

Info

Name	Value
Type	Add Devices
Name	Test iOS Devices
Status	Enabled
Activate Date	2018-12-05 4:21:00 PM
Target Device Groups	
\\MVISION\iOS\	
Wildcard Filter Parameters	
Add Devices Rule Tag = "7FF386D4-B2A9-E51B-	
Force SHA-1 client certificate distribution	No
User Authentication Options	Password required
Enrollment ID	DKNPP
Enrollment URL	https://s.mobicontrolcloud.com/Enroll/
Cache Password	Disabled
Device Name	%PERSONALIZED_DEVICE_NAME%
Update device's personalized name (Requires iOS	No
Agent Authentication Authority	Internal MobiControl CA
Default Rule	No
Preserve Device Location on Re-Enrollment	Yes
DEP profile assigned to devices	No
Certificate Authentication Authority	Internal MobiControl CA

This figure shows the result of creating the add devices rule for Android. You must ensure that you selected the Managed Google Play Accounts for McAfee. See "Google Managed Enterprise for MobiControl" for more information on those setup steps.



View Devices Return to MobiControl's next generation console!

- Add Devices
  - So AFW
- Application Catalog
- File Sync
- Device Relocation
- Data Collection
- Alerts
- Telecom Expense Management

Info

Name	Value
Type	Add Devices
Name	Soumya AFW
Status	Enabled
Activate Date	2018-11-26 1:10:00 PM
Target Device Groups	
\\MVISION\Android\	
Wildcard Filter Parameters	
Add Devices Rule Tag = "B80B1CA7-5219-4D2C-4DBB-74687	
Force SHA-1 client certificate distribution	No
User Authentication Options	Password required
Enrollment ID	ZUABD
Enrollment URL	https://s.mobicontrolcloud.com/Enroll/
Cache Password	Disabled
Device Name	AndroidPlus %AUTONUM%
Default Rule	No
Preserve Device Location on Re-Enrollment	Yes
Android Management	Managed Google Play Accounts (McAfee, LLC.)
Certificate Authentication Authority	Internal MobiControl CA

Manual Activation

Make sure you created:

- SOTI MobiControl device group
- Application catalog rule
- Add devices rule

Users can now activate the application in these ways from your Add Devices rule:

- Provide them with the ‘Enrollment ID’
- Provide them with an activation URL

See the “*McAfee MVISION Mobile iOS Product Guide*” and the “*McAfee MVISION Mobile Android Product Guide*” for MVISION Mobile activation information.

Configuration Steps

This section describes the SOTI MobiControl MDM and MVISION Mobile Console synchronization configuration along with the auto-activation setup options.

Synchronization Overview

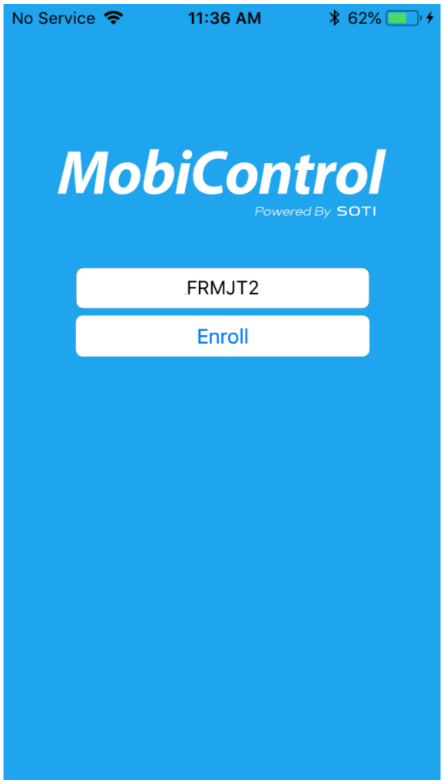
To avoid creating user credentials, devices can be synchronized through the MDM integration. This allows all user and device management functions to be handled at the MDM console.

After the initial synchronization during the MDM Integration setup, users are managed through a scheduled synchronization process that runs every four hours. If there are additional devices in the device group(s) being used for synchronization, they are added along with their associated users to MVISION Mobile Console. If users are removed, then they are removed from the MVISION Mobile Console. These changes do not remove any of the events associated with that user/device.

Enrolling the Device

After the add devices rule is defined, go to the App Store and download the 'MobiControl' app onto the device. Then the enrollment ID from the add devices rule can be entered on the MobiControl app to manually configure the applications on the device.

This figure shows where the enrollment ID is entered.

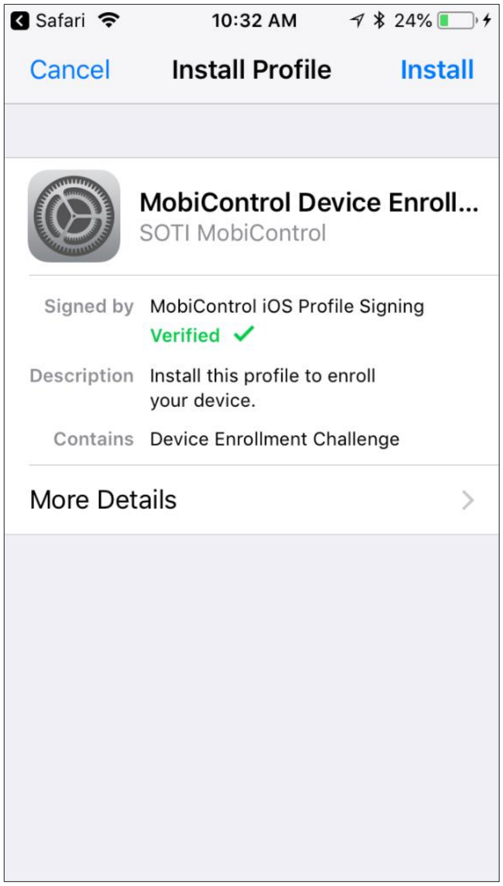


For instructions on how to install and continue on the device after given an enrollment ID, see the MobiControl Enrollment Service website:

`https://yourHost.mobicontrolcloud.com/mc/enroll/29#step2_instruction`

- where *yourHost* is the URL portion provided from SOTI.

These figures show how the device looks after one of the profiles is installed, and also the resulting applications after the enrollment is complete. If MVISION Mobile was set as a mandatory application type, then it would display also. If the application type was ‘suggested,’ then the user must open the App Catalog, and select MVISION Mobile to install it from there.



Safari 10:32 AM 24%

Cancel | **Install Profile** | Install

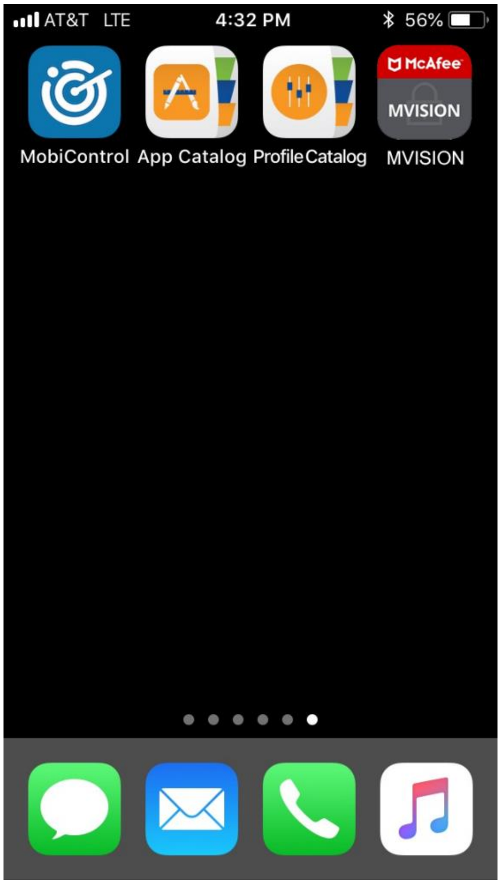
MobiControl Device Enroll...
SOTI MobiControl

Signed by: MobiControl iOS Profile Signing
Verified ✓

Description: Install this profile to enroll your device.

Contains: Device Enrollment Challenge

More Details >



On-Demand MDM Synchronization

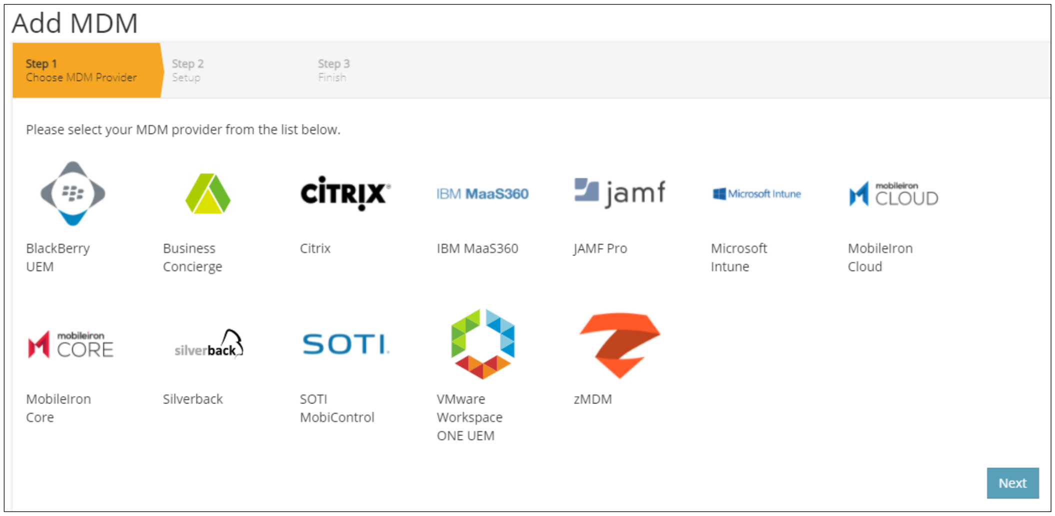
Due to the four-hour MDM synchronization window, there are times where a new MDM user has MVISION Mobile pushed down to their device and attempts to start it prior to the device actually being synchronized from the MDM. MVISION Mobile Console handles this by doing an on-demand synchronization when MVISION Mobile tries to activate, but no information yet exists for it. MVISION Mobile Console gets the identification information from MVISION Mobile used for the authentication and matches it up with the proper customer for authentication. Once that happens, MVISION Mobile Console retrieves the device and user information from the MDM configured for that customer. MVISION Mobile on that device is now authenticated and allowed to proceed.

See the "Configuring Device Application Auto-Activation" section for information on setting up iOS and Android devices.

Set Up Synchronization in MVISION Mobile Console

To set up the integration in the MVISION Mobile Console:

1. Ensure you completed adding a SOTI MobiControl administrator user in the SOTI MobiControl console. See the "SOTI MobiControl User with Administrator Access" section for these instructions.
2. Ensure that you created one or more SOTI MobiControl device groups that contain the devices to be protected. See the "Device Application Deployment Set Up" section for more information on this setup.
3. Login to MVISION Mobile Console and navigate to Manage > Integrations.
4. Click on **Add MDM** and select the SOTI MobiControl icon.



Add MDM

Please select your MDM provider from the list below.

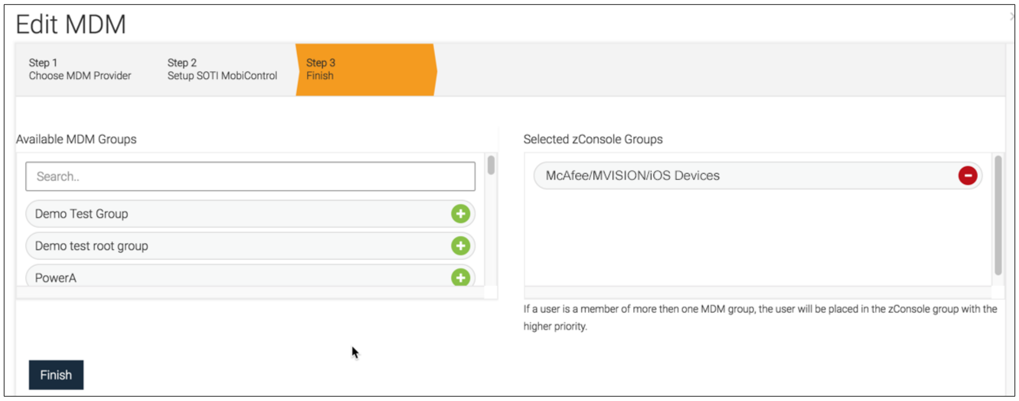
5. Enter the information for the SOTI MobiControl integration in the table.

Item	Specifics

URL	URL of the SOTI MobiControl Server which is in this format: **https://*yourHost*.mobicontrolcloud.com** where *yourHost* is the URL portion given to you by SOTI.
Username	The SOTI MobiControl Administrator username that was created and is used to log into the SOTI MobiControl console.
Password	The password of the SOTI MobiControl Administrator used to log into the SOTI console.
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This name is prepended to the group name to form the MVISION Mobile Console group name.
Background Sync	Check this box to ensure users and devices are synchronized with the chosen SOTI MobiControl Device Groups.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, such as name or email address.
API key	This is the API key value to connect to your SOTI MDM instance. This must be manually generated and obtained from SOTI. The format of this field is: *client_id***:***client_secret* where - *client_id* is the client identifier obtained from SOTI. - *client_secret* is the client secret value obtained from SOTI. - *colon* is the separator between the two fields. Contact your Customer Success team member if you have questions about this field.
Send Device Activation email via MVISION Mobile Console for iOS Devices	Check this box to send an email to the user for every iOS device synced with the MDM.
Send Device Activation email via MVISION Mobile Console for Android Devices	Check this box to send an email to the user for every Android device synced with the MDM.

6. Click **Next** and choose one or more SOTI MobiControl device groups to synchronize. The available device groups are shown on the left under the 'Available MDM Groups'

column and can be moved over to the 'Selected MVISION Mobile Groups' column by clicking on the plus sign ('+'). This can be reversed by clicking on the minus sign ('-').



If a user is a member of more then one MDM group, the user will be placed in the zConsole group with the higher priority.

7. Click **Finish** to save the configuration and start the first synchronization. Each device group selected is set up as a zConsole group for defining these settings:
    - Privacy
    - Role Access
    - Threat Policy

8. Click **Finish** to save the configuration and start the first synchronization.

If a device falls into more than one Device Group, the highest or its first device group is its MVISION Mobile Console group. To change the order of the listing, drag and drop device groups as needed.

- The device groups are retrieved, and user/device synchronization is complete.
- You can verify the completion by navigating to the Devices page in the MVISION Mobile Console and verify the device display. The device entries are greyed out until the user starts up MVISION Mobile and activates the app.

See the "*McAfee MVISION Mobile iOS Product Guide*" and "*McAfee MVISION Mobile Android Product Guide*" in the customer portal for further device activation information on iOS and Android devices, respectively. See the "*McAfee MVISION Mobile Console Product Guide*" in the customer portal for further MDM activation information.

Device Actions and Remediation

The MVISION Mobile integration with SOTI MobiControl provides a way to block access to company data such as email and other services. Profiles can be used to allow only devices below a defined mobile threat level to access certain data and services. If a threat is detected on a device and that threat has an MDM action of 'Inform EMM', then MVISION Mobile Console sends the new mobile threat level of that device to SOTI MobiControl. The mobile threat level of the device is the highest threat event classification that is pending for that device, also known as the Threat Level which is a custom attribute in the SOTI MobiControl console.

Creating a Custom Attribute

A SOTI MobiControl administrator can create and use a custom attribute to reflect the threat level for one or more devices. The custom attribute for this threat level information is named 'MVISION Threat Level.' To set SOTI MobiControl up to take actions when a device falls below a defined threat level, in the MobiControl console, perform these steps:

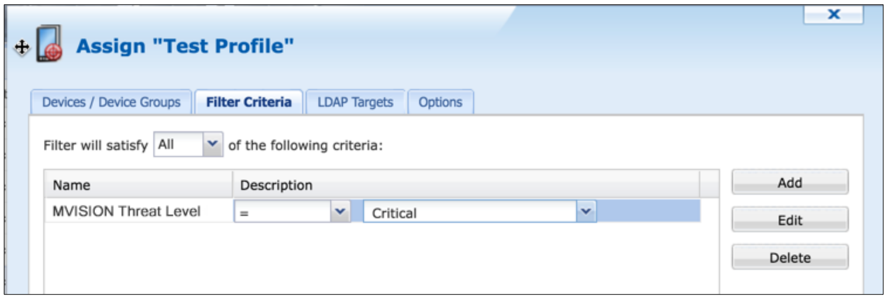
1. Create a new Profile to enforce Compliance policy.
    a. Select **Profiles** under Configurations. Create a Profile for iOS and/or Android devices which includes a compliance action.
    b. Add a configuration for what should change for the device.
2. Assign the Profile to one or more Device Groups and the Filter Criteria
    a. You can assign this after you click **Save** and **Assign**. Assign the device groups under Devices > Device Groups.
    b. Set the Filter Criteria to the Profile using the Custom Attribute. For instance, MVISION Threat Level = Elevated.
    c. Click **Assign** after the criteria is set under the Filter Criteria tab.

Note: *Custom attributes that are created are inherited by any new administrator that is created.*

For more information on creating a custom attribute refer to the SOTI documentation website:

https://www.soti.net/mc/help/v13/en/Content/Web/Devices/customAttributes.htm

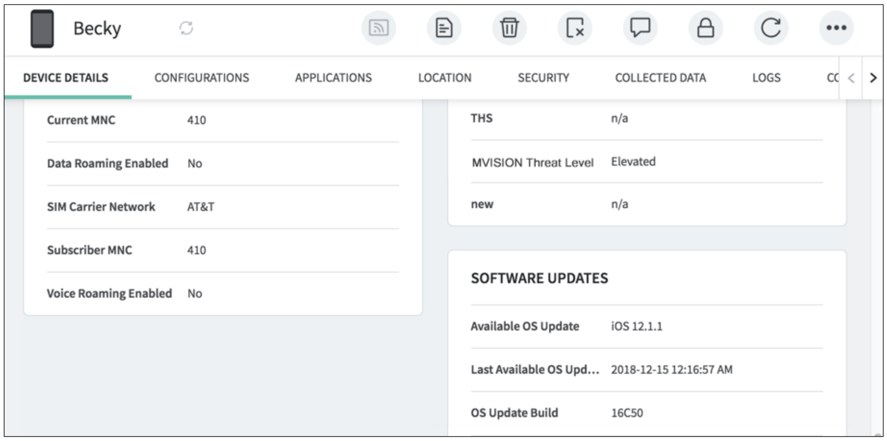
The profile is only applied to devices in the group that match the configured filter criteria. This figure shows the dialog box where you set the device group and filter criteria.



Filter will satisfy All of the following criteria:

Name	Description
MVISION Threat Level	= Critical

This figure shows the custom attribute value for a specific device.



Current MNC	410
Data Roaming Enabled	No
SIM Carrier Network	AT&T
Subscriber MNC	410
Voice Roaming Enabled	No

THS	n/a
MVISION Threat Level	Elevated
new	n/a

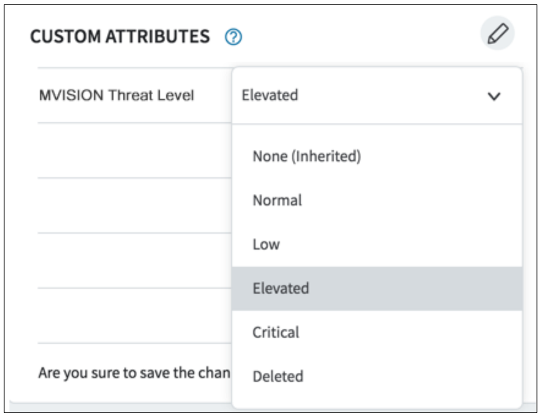
SOFTWARE UPDATES

Available OS Update	iOS 12.1.1
Last Available OS Upd…	2018-12-15 12:16:57 AM
OS Update Build	16C50

Create a profile for each OS Platform in your environment. Enter the name of the profile, and a short description. The options for the MVISION Threat Level are:

- Normal
- Low
- Elevated
- Critical
- Deleted

The threat level is typically set to 'Critical' so that when the device has a high mobile threat level, it makes the device non-compliant.



CUSTOM ATTRIBUTES

MVISION Threat Level: Elevated

Are you sure to save the chan

Then navigate to the Policy page in MVISION Mobile Console and select the MVISION Mobile Console group you want to target. For each threat classification that you want SOTI MobiControl to know about, set the MDM Action column to 'Inform EMM'. For situations where the threat can be mitigated or is no longer present, set the Mitigation Action column to 'Inform EMM' as well, and the Mobile Threat Level of the device is adjusted accordingly.

Available Device Actions

The available MDM Actions for SOTI MobiControl MDM in the MVISION Mobile Console are:

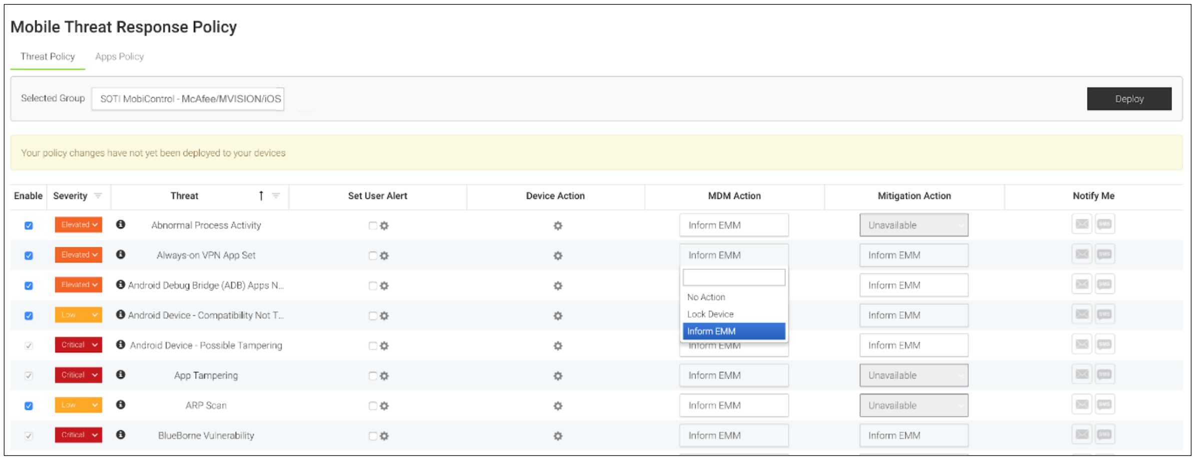
- No Action
- Lock Device
- Inform EMM

NOTE: *The default action is the 'Inform EMM' action*.

The available mitigation Actions for SOTI MobiControl MDM in the MVISION Mobile Console are:

- No Action
- Lock Device
- Inform EMM

The figure below shows the MVISION Mobile Console Policy page with the Inform EMM actions.



Mobile Threat Response Policy

Selected Group: SOTI MobiControl - McAfee/MVISION/iOS

Your policy changes have not yet been deployed to your devices

Enable	Severity	Threat	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
☑	Elevated	Abnormal Process Activity	☐		Inform EMM	Unavailable	✉ SMS
☑	Elevated	Always-on VPN App Set	☐		Inform EMM	Inform EMM	✉ SMS
☑	Elevated	Android Debug Bridge (ADB) Apps N...	☐			Inform EMM	✉ SMS
☑	Low	Android Device - Compatibility Not T...	☐			Inform EMM	✉ SMS
✓	Critical	Android Device - Possible Tampering	☐		Inform EMM	Inform EMM	✉ SMS
✓	Critical	App Tampering	☐		Inform EMM	Unavailable	✉ SMS
☑	Low	ARP Scan	☐		Inform EMM	Unavailable	✉ SMS
✓	Critical	BlueBorne Vulnerability	☐		Inform EMM	Inform EMM	✉ SMS

Synchronizing iOS Apps and iOS Profiles

For iOS, we retrieve the iOS app list through the configured MDM and evaluate if the apps are malicious or legitimate. In addition, the security and privacy risks associated with the app is provided, if the MVISION Mobile Advanced license has been purchased.

These steps allow an administrator to see the iOS apps and iOS profiles in the MVISION Mobile Console:

- The device is enrolled in the MDM and with MVISION Mobile.
- The user installs a new app on the device.
- The MDM sees the new app in the sample request update.
- MVISION Mobile sees the new app when the MDM sync is performed for that device.