McAfee MVISION Mobile

SOTI MobiControl Integration Guide

MVISION Mobile Console 4.23

June 9, 2019

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Integration with SOTI MobiControl

Overview

When a Mobile Device Management (MDM) is integrated, the MVISION Mobile Console provides the following:

- Synchronizing devices with the MDM
- Transparent user access to MVISION Mobile App
- More granular and specific protection actions

but integration with an MDM system is not required.

McAfee's MVISION Mobile App detects malicious activity and depending on the MDM platform, is able to take actions locally. When MVISION Mobile App is integrated with an MDM, protection actions can be performed by the MDM in addition to local MVISION Mobile App 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 McAfee MVISION Mobile Console and the SOTI MobiControl server.

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 App detects an event, it consults the current Threat Response Policy/Matrix resident on the device and if there is a specific MDM action defined, this is communicated to the cloud server. The cloud server 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 the following:

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

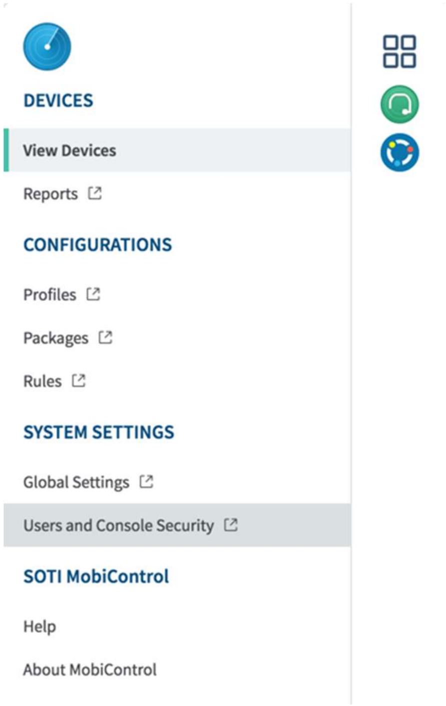
Refer to the SOTI MobiControl documentation website for more information on how to use the console: https://www.soti.net/mc/help/v14.1/en/docindex.html

SOTI MobiControl User with Administrator Access

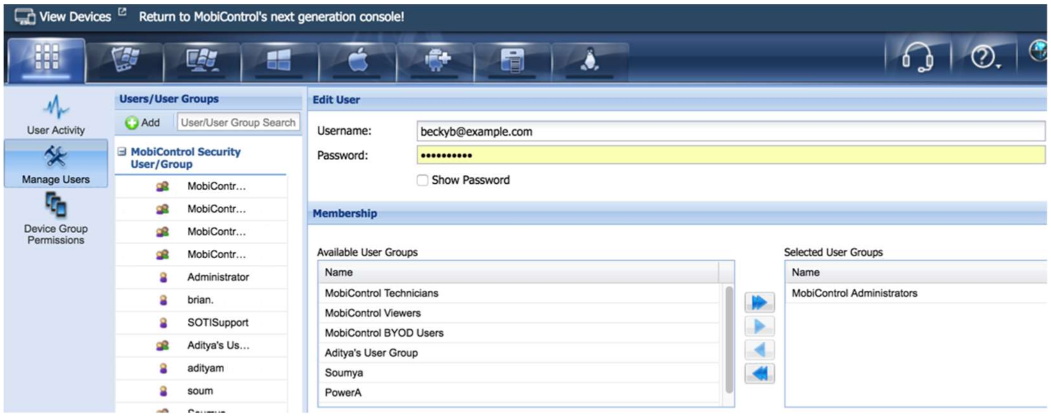
Log in to the SOTI MobiControl console and define a user as belonging to the 'MobiControl Administrator' user group. To create a SOTI MobiControl administrator with the proper access perform the following:

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: ••••••••••

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 the following:

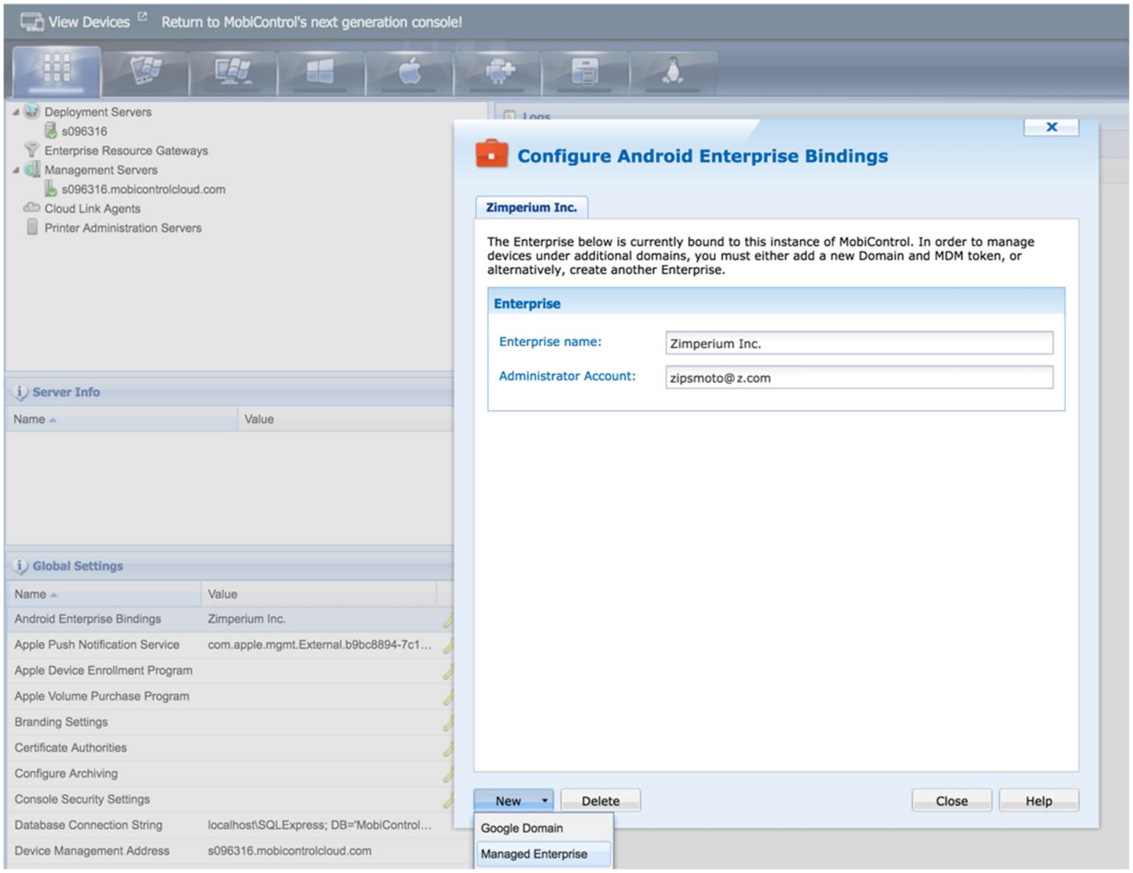
1. From the main menu, select **Global Settings**.
2. Click the **Servers** tab at the bottom.

3. Click the change icon for the ‘Android Enterprise Bindings’.
4. Click **New**.
5. Click **Managed Enterprise**.
6. You are redirected to Google's Managed Enterprise Enrollment page. 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**.
   The Android Enterprise Bindings setup is complete.

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: Zimperium Inc.

Administrator Account: zipsmoto@z.com

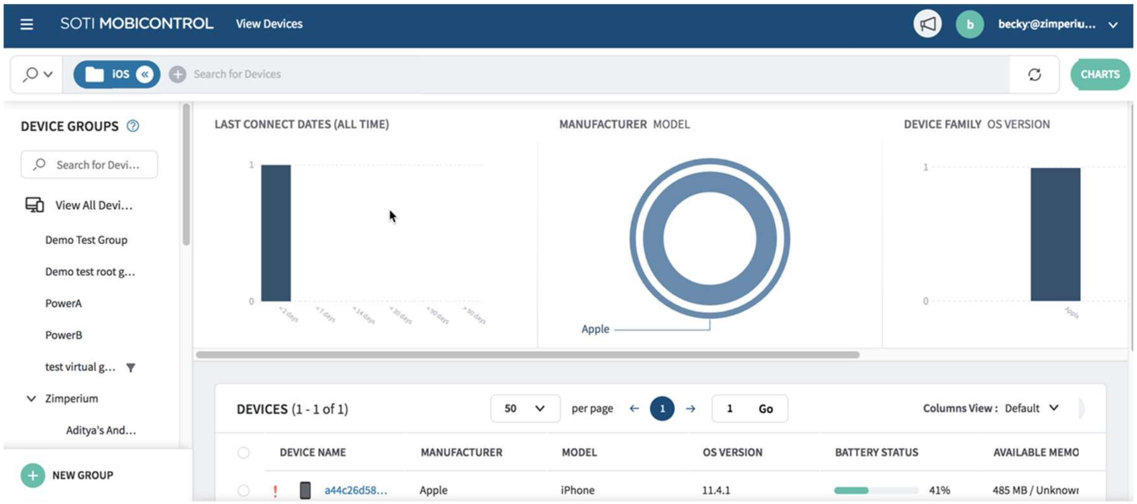
Global Settings

Name	Value
Android Enterprise Bindings	Zimperium Inc.
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.



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

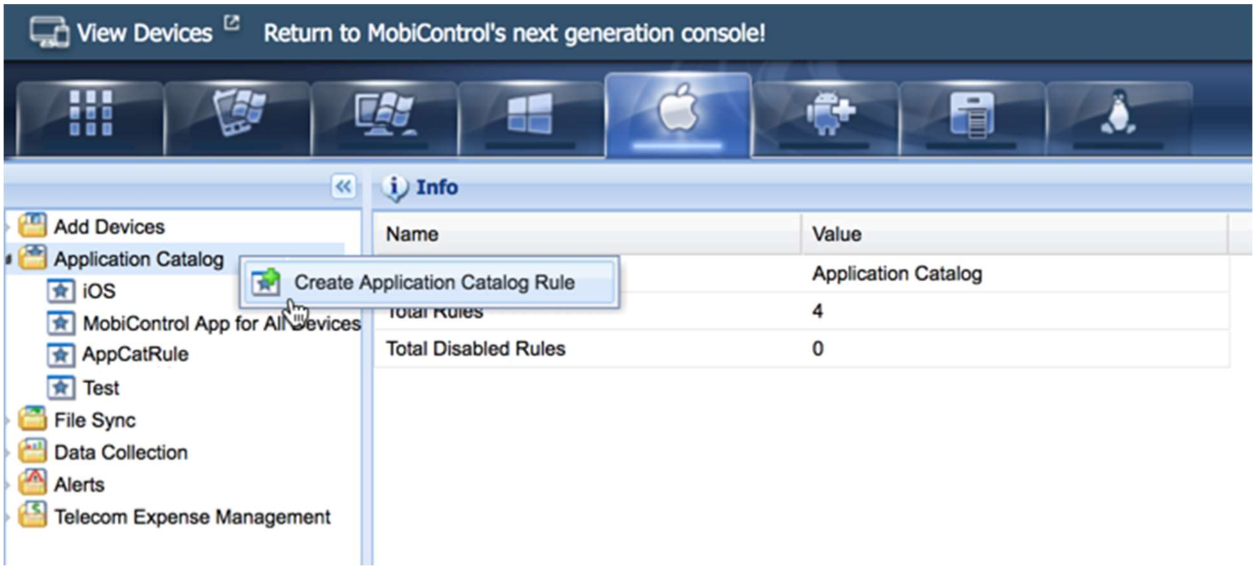
Application Catalog Rule

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 the following 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 App for deployment on the device by performing the following:
    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 App and the file is uploaded to the SOTI MobiControl console. See the “*About MVISION Mobile App 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
iOS
MobiControl App for All Devices
AppCatRule
Test
File Sync
Data Collection
Alerts
Telecom Expense Management
Create Application Catalog Rule

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 app are associated to the application catalog rule.

About MVISION Mobile App Deployment

To deploy the MVISION Mobile App through SOTI MobiControl MDM, ask your Customer Success team at McAfee for the iOS and Android version of MVISION Mobile App. Both iOS and Android MVISION Mobile App are in their respective public application stores, but it is good practice to deploy MVISION Mobile App through SOTI MobiControl as an internal app from Customer Success to ensure you have the latest available release.

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 App to the devices.

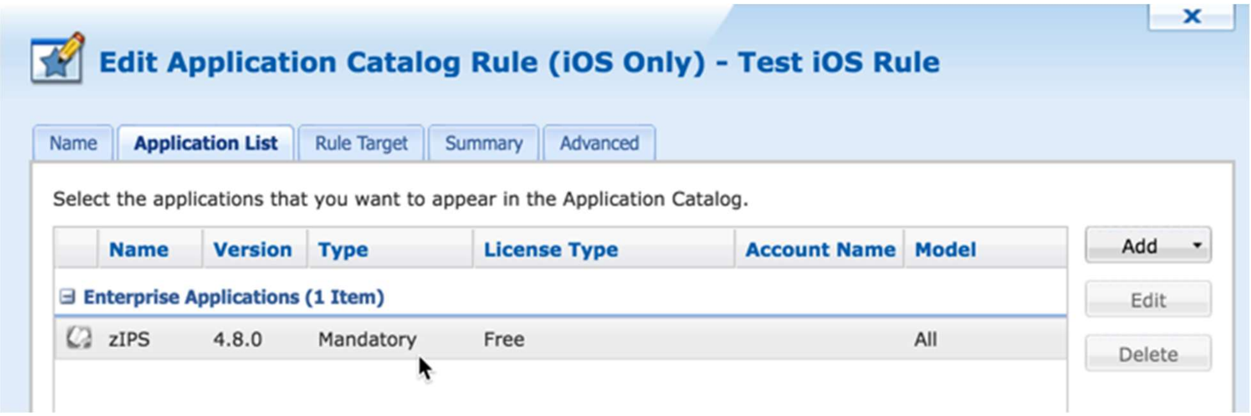
To publish the MVISION Mobile App from the public application store instead, search the appropriate store for MVISION Mobile App.

About Deployment Options

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

- The MVISION Mobile App 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 app inside the SOTI MobiControl App Catalog and installs MVISION Mobile App 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 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.

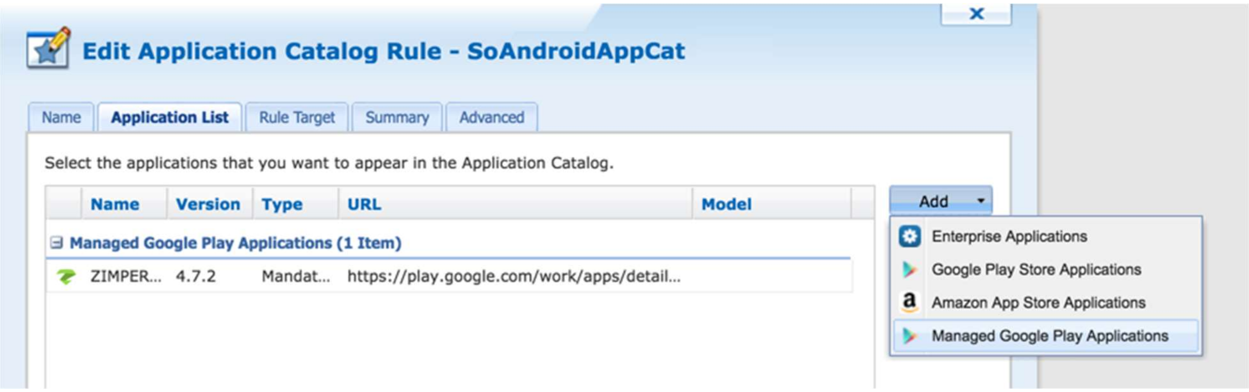


Edit Application Catalog Rule (iOS Only) - Test iOS Rule

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

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

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



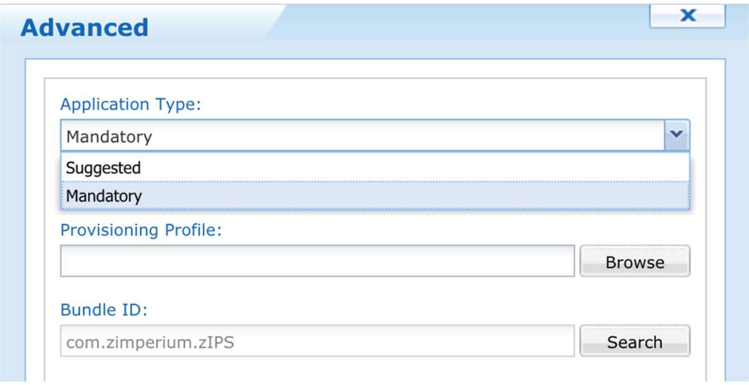
Edit Application Catalog Rule - SoAndroidAppCat

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)				
ZIMPER...	4.7.2	Mandat...	https://play.google.com/work/apps/detail...	

To set the type as mandatory, you select the MVISION Mobile App 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.zimperium.zIPS

Configuring Device Application Auto-Activation

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

iOS Activation

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 iOS MVISION Mobile App without having to enter any credentials. The application configuration pre-programs iOS MVISION Mobile App 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.

For MVISION Mobile App Release 4.8.0 or later, use these configuration values.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	%DeviceIdentifier%
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team
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.

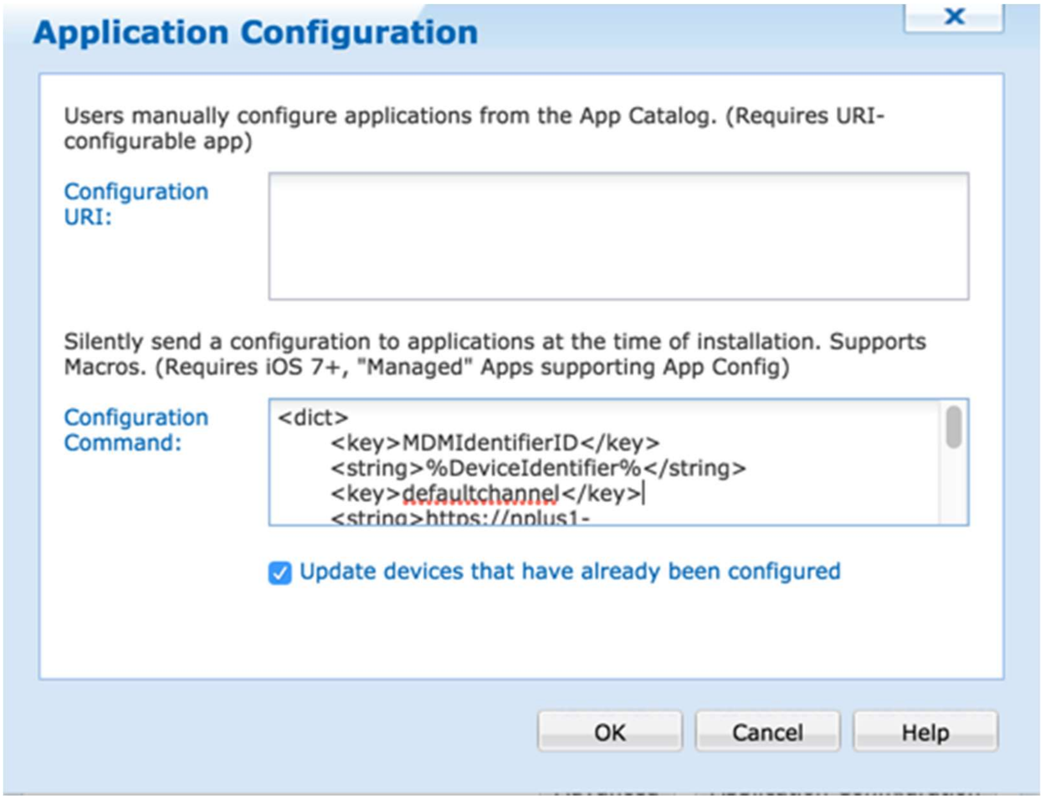
Set the PLIST XML in the Configuration Command field. This shows an example plist XML value.

```
<dict>
       <key>MDMDeviceID</key>
       <string>%DeviceIdentifier%</string>

       <key>defaultchannel</key>

       <string>https://sample-default-channel.. mcafee-mvision-
mobile.com:443/srx</string>
       <key>tenantid</key>
       <string>demo</string>
</dict>
```

This figure shows the Configuration Command field with the XML value included.



Users manually configure applications from the App Catalog. (Requires URI-configurable app)

Configuration URI:

Silently send a configuration to applications at the time of installation. Supports Macros. (Requires iOS 7+, "Managed" Apps supporting App Config)

Configuration Command:

```
<dict>
     <key>MDMIdentifierID</key>
     <string>%DeviceIdentifier%</string>
     <key>defaultchannel</key>
     <string>https://nplus1-
```

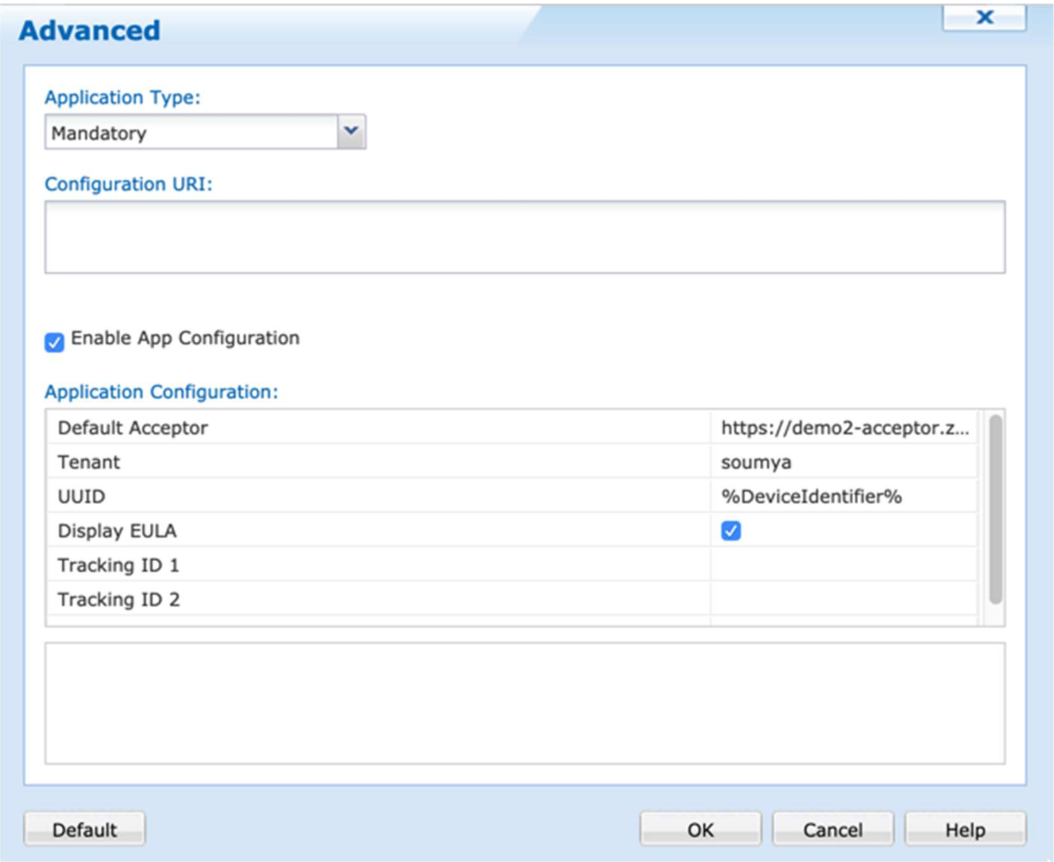
☑ Update devices that have already been configured

Android Activation

Android Enterprise (Android for Work) 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 setup.
- 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.

This figure shows setting up the configuration keys for an Android device.



Application Type: Mandatory

Configuration URI:

☑ Enable App Configuration

Application Configuration:

Default Acceptor	https://demo2-acceptor.z...
Tenant	soumya
UUID	%DeviceIdentifier%
Display EULA	☑
Tracking ID 1	
Tracking ID 2	

Note: The UUID key can be used for backward compatibility, but for MVISION Mobile App Release 4.8.x use MDMDeviceID key instead.

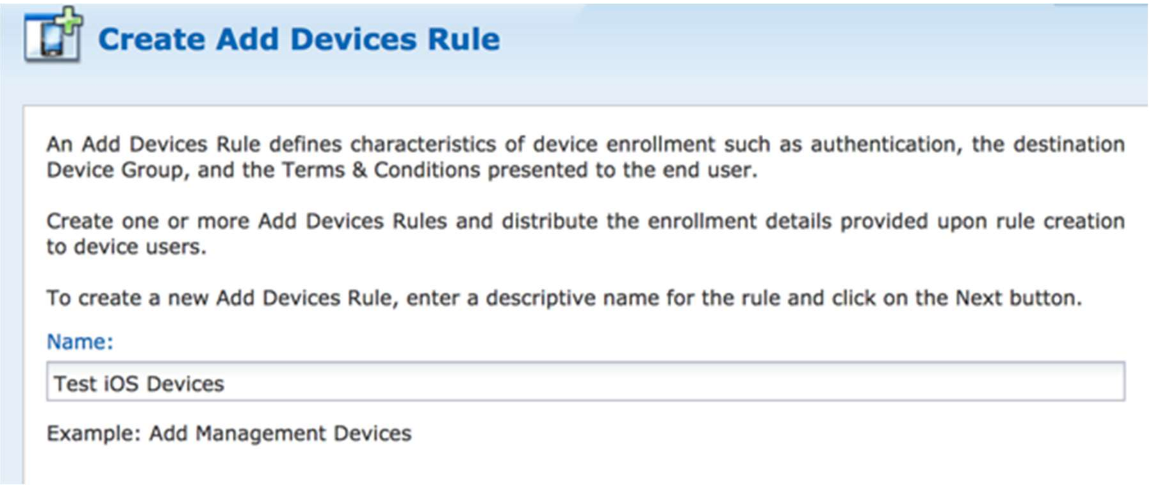
See "Google Managed Enterprise for MobiControl" for information on setting up the Android application.

Note: SOTI MobiControl requires auto-activation for Android devices.

Add Devices Rule

Devices synchronize with MobiControl using 'Add Devices' rules. 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 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.

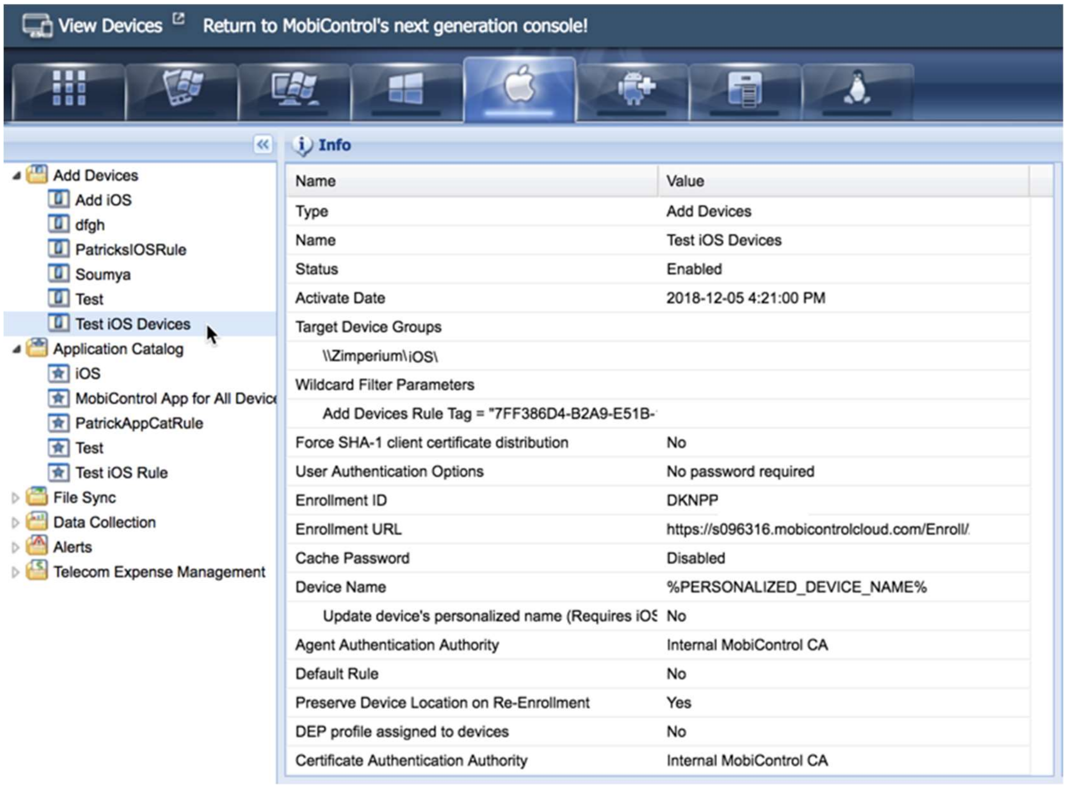
To create a new Add Devices Rule, enter a descriptive name for the rule and click on the Next button.

Name:

Test iOS Devices

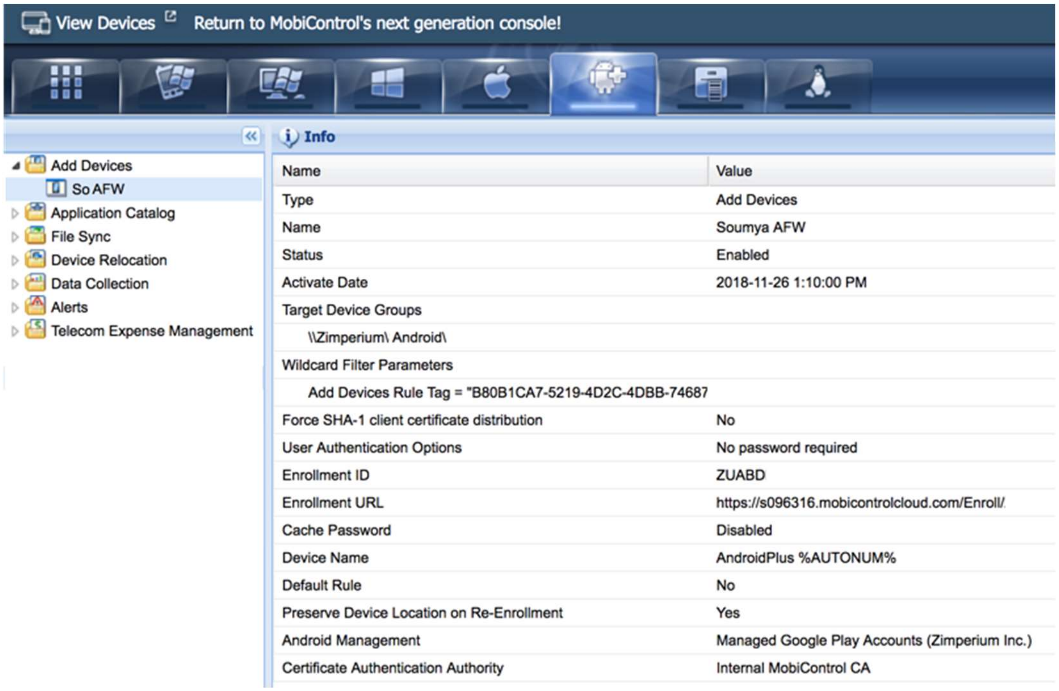
Example: Add Management Devices

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



Name	Value
Type	Add Devices
Name	Test iOS Devices
Status	Enabled
Activate Date	2018-12-05 4:21:00 PM
Target Device Groups	
\\Zimperium\iOS\	
Wildcard Filter Parameters	
Add Devices Rule Tag = "7FF386D4-B2A9-E51B-	
Force SHA-1 client certificate distribution	No
User Authentication Options	No password required
Enrollment ID	DKNPP
Enrollment URL	https://s096316.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 that setup.



Name	Value
Type	Add Devices
Name	Soumya AFW
Status	Enabled
Activate Date	2018-11-26 1:10:00 PM
Target Device Groups	
\\Zimperium\ Android\	
Wildcard Filter Parameters	
Add Devices Rule Tag = "B80B1CA7-5219-4D2C-4DBB-74687	
Force SHA-1 client certificate distribution	No
User Authentication Options	No password required
Enrollment ID	ZUABD
Enrollment URL	https://s096316.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 (Zimperium Inc.)
Certificate Authentication Authority	Internal MobiControl CA

Manual Activation

With the following created:

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

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

- Provide them with the “Enrollment ID”.
- Provide them with an activation URL.

Refer to “*iOS MVISION Mobile App Platform Guide*” and “*Android MVISION Mobile App Platform Guide*” in the customer portal for MVISION Mobile App 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

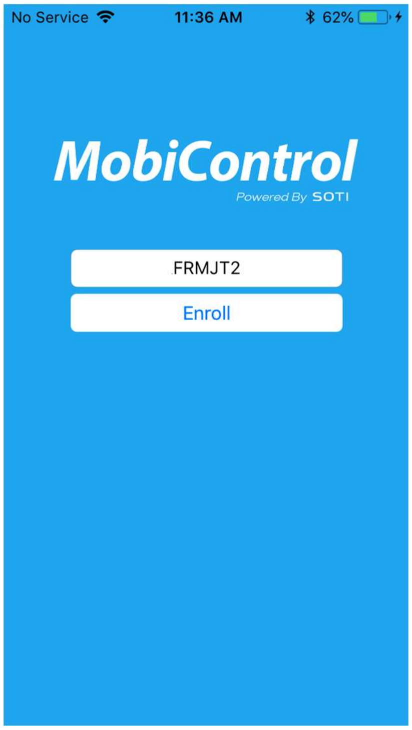
To avoid creating user credentials, devices can be synchronized through the MDM integration. This allows all user and device management functions to be handled at the MDM console.

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.

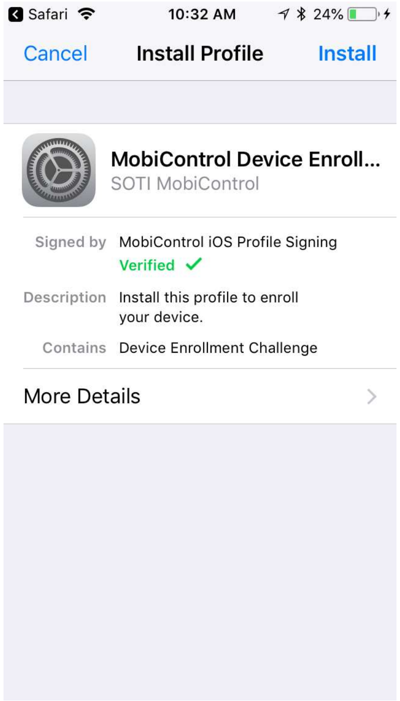


FRMJT2

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

https://s096316.mobicontrolcloud.com/mc/enroll/29#step2_instruction

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 App was set as a mandatory application type, then it would display as well. If the application type was 'suggested,' then the user must open the App Catalog, and select MVISION Mobile App to install it from there.

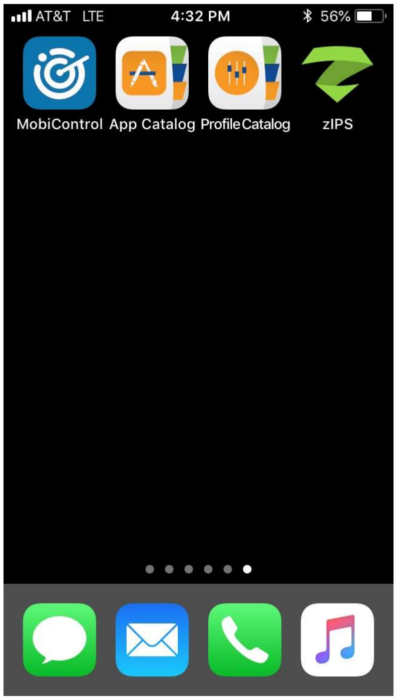


MobiControl Device Enroll...
SOTI MobiControl

Signed by: MobiControl iOS Profile Signing
Verified ✓

Description: Install this profile to enroll your device.

Contains: Device Enrollment Challenge



On-demand MDM Synchronization

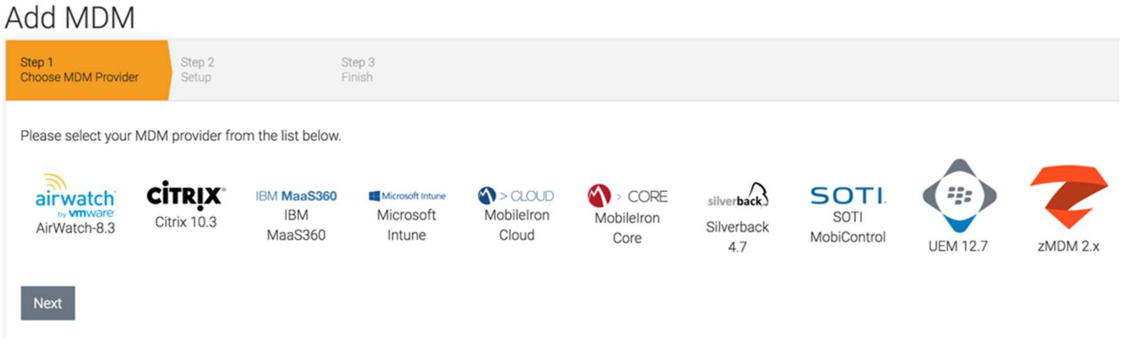
Due to the four-hour MDM synchronization window, there are times where a new MDM user has MVISION Mobile App pushed down to their device and attempts to start it prior to the device actually being synchronized from the MDM. MVISION Mobile Console handles this by doing an on-demand synchronization when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

Refer to section “Configuring Device Application Auto-Activation” for information on setting up iOS and Android devices.

Set Up Synchronization in MVISION Mobile Console

To setup device synchronization in MVISION Mobile Console, perform the following steps:

1. Ensure you completed adding a SOTI MobiControl administrator user in the SOTI MobiControl console. See “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 “Device Application Deployment Set Up” section for more information on this setup.
3. Log into MVISION Mobile Console and navigate to Manage / MDM.
4. Click on **Add MDM** and select the SOTI MobiControl icon.



Add MDM

Step 1 Choose MDM Provider

Step 2 Setup

Step 3 Finish

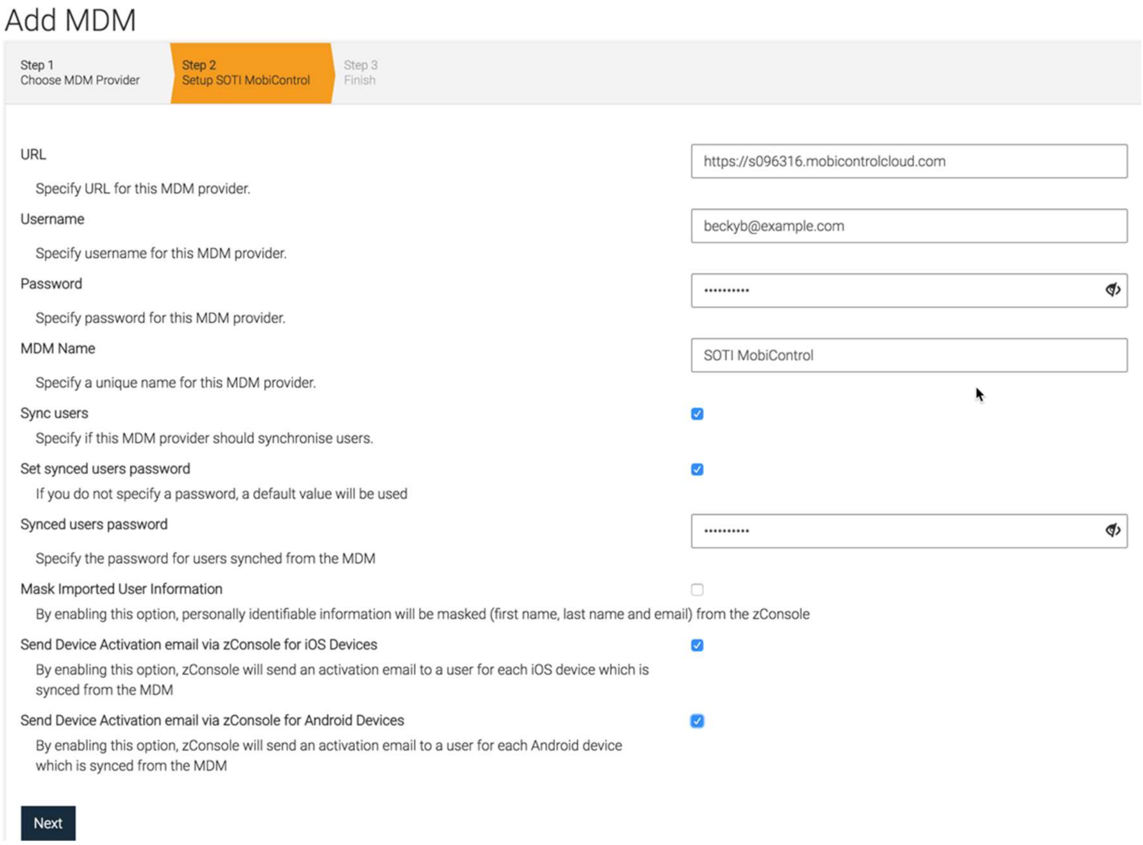
Please select your MDM provider from the list below.

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

Item	Description
URL	URL of the SOTI MobiControl Server which is the following: https://s096316.mobicontrolcloud.com
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.
Sync Users	Check this box to ensure users and devices are synchronized with the chosen SOTI MobiControl Device Groups.
Set synced users password	Check this box to override the default password during the user synchronization. If this is not checked a default password is computed as follows for all users that are synchronized: Start with the McAfee environment name (this can be supplied by your Customer Success contact), change all uppercase letters

	to lowercase and also change all spaces to dashes. Then append “1234!” to the end of the string. So, the value ‘*McAfee Test*’ becomes ‘*McAfee-test1234!*’
Synced users password	Override the value of the password to use for each user when they are synchronized with this value.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, such as name or email address.
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.

This figure shows the dialog box when fields are filled in with values.



Add MDM

Step 1 Choose MDM Provider | Step 2 Setup SOTI MobiControl | Step 3 Finish

URL — https://s096316.mobicontrolcloud.com

Specify URL for this MDM provider.

Username — beckyb@example.com

Specify username for this MDM provider.

Password — ••••••••••

Specify password for this MDM provider.

MDM Name — SOTI MobiControl

Specify a unique name for this MDM provider.

Sync users ☑

Specify if this MDM provider should synchronise users.

Set synced users password ☑

If you do not specify a password, a default value will be used

Synced users password — ••••••••••

Specify the password for users synched from the MDM

Mask Imported User Information □

By enabling this option, personally identifiable information will be masked (first name, last name and email) from the zConsole

Send Device Activation email via zConsole for iOS Devices ☑

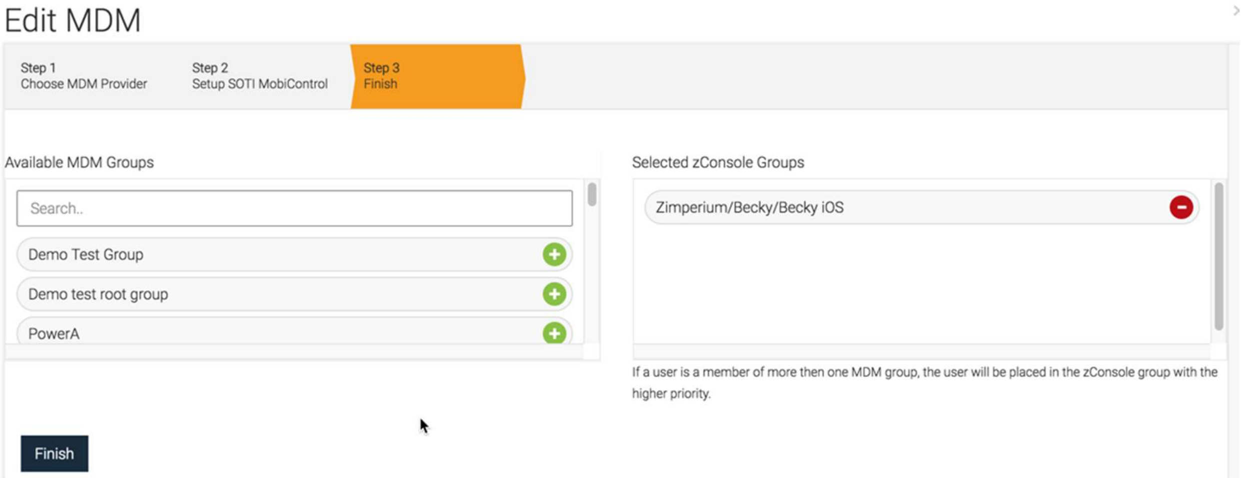
By enabling this option, zConsole will send an activation email to a user for each iOS device which is synced from the MDM

Send Device Activation email via zConsole for Android Devices ☑

By enabling this option, zConsole will send an activation email to a user for each Android device which is synced from the MDM

Next

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 Console Groups’ column by clicking on the plus sign (‘+’). This can be reversed by clicking on the minus sign (‘-’).



Edit MDM

Step 1 Choose MDM Provider | Step 2 Setup SOTI MobiControl | Step 3 Finish

Available MDM Groups

Search..

- Demo Test Group ⊕
- Demo test root group ⊕
- PowerA ⊕

Selected zConsole Groups

- Zimperium/Becky/Becky iOS ⊖

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.

Finish

7. Click **Finish** to save the configuration and start the first synchronization. Each device group selected is set up as a MVISION Mobile Console group for defining the following settings:
    - Privacy
    - Role access
    - Threat Response Policy/Matrix

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 App and activates the app.

Refer to "*iOS MVISION Mobile App Platform Guide*" and "*Android MVISION Mobile App Platform Guide*" in the customer portal for further device activation information. Refer to the "*McAfee MVISION Mobile Console Configuration Guide*" in the customer portal for further MDM activation information.

Device Actions and Remediation

The McAfee 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 "McAfee Threat Level." To set SOTI MobiControl to take actions when a device falls below a defined threat level, in the MobiControl console, perform the following steps:

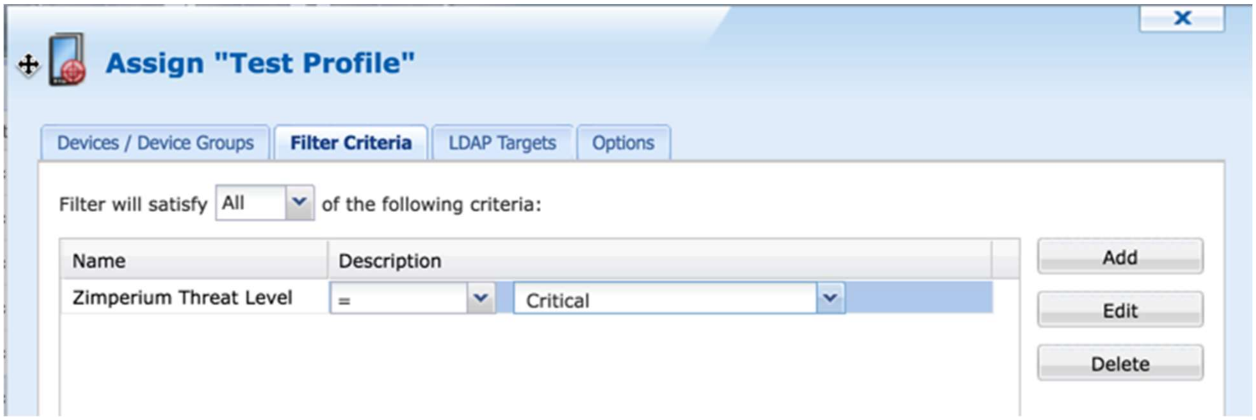
1. Create a new Profile to enforce Compliance policy.
    a. Select **Profiles** under Configurations. Create a Profile for iOS and/or Android devices which includes a compliance action.
    b. Add a configuration for what should change for the device.
2. Assign the Profile to one or more Device Groups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

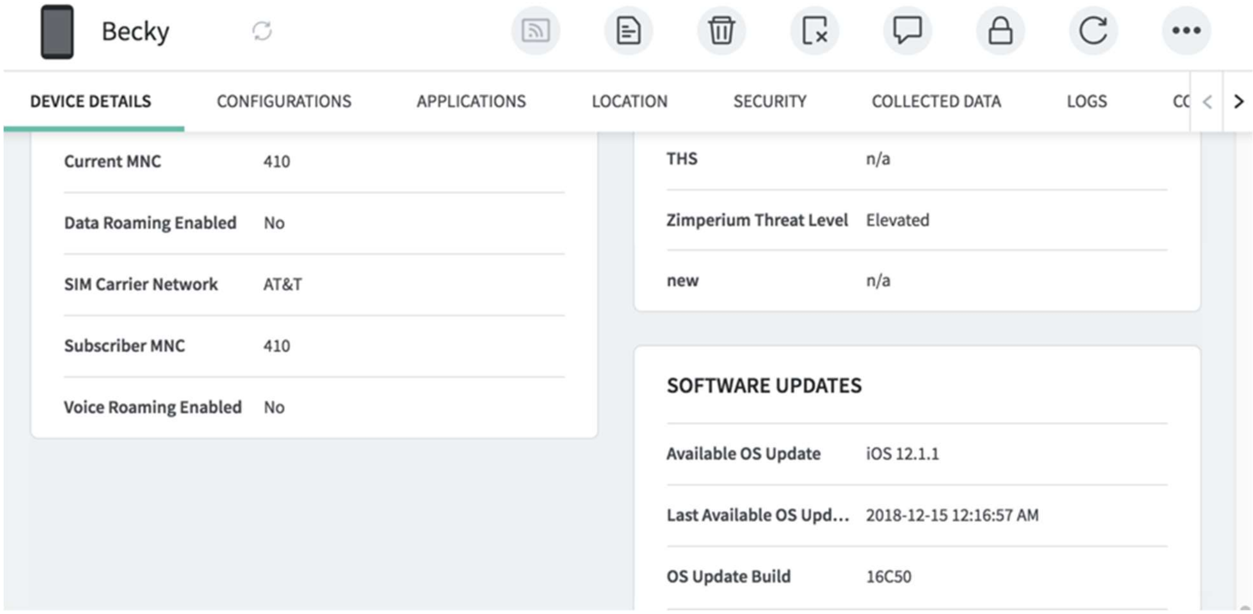
The profile is only applied to devices in the group that match the configured filter criteria. This figure shows the dialog box where you set the device group and filter criteria.


Assign "Test Profile"

Filter will satisfy All of the following criteria:

Name	Description	
Zimperium 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
Zimperium Threat Level	Elevated
new	n/a

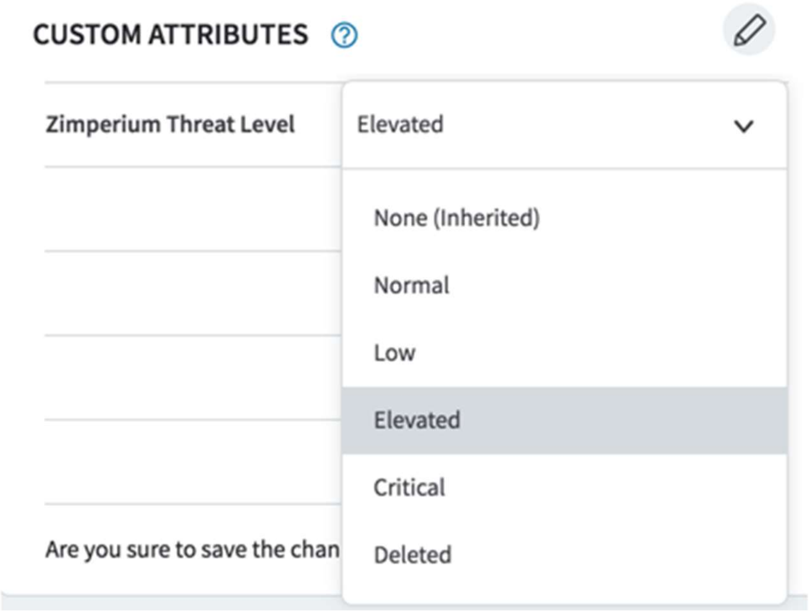
SOFTWARE UPDATES

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 McAfee Threat Level are the following:

- 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

Zimperium Threat Level: Elevated

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 the following:

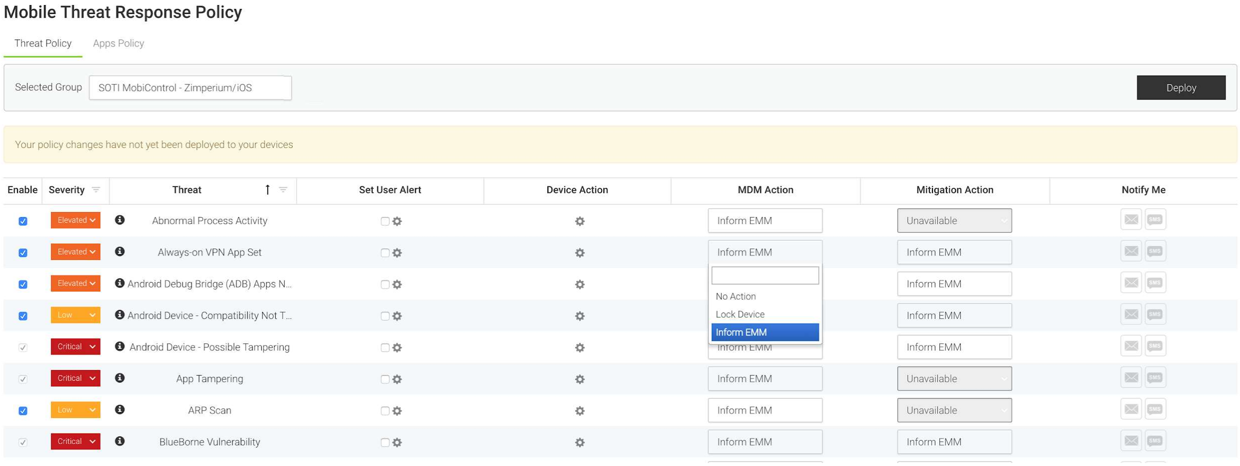
- No Action
- Lock Device
- Inform EMM

with the default being the ‘Inform EMM’ action.

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

- 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 - Zimperium/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	
☑	Elevated	Always-on VPN App Set	□		Inform EMM	Inform EMM	
☑	Elevated	Android Debug Bridge (ADB) Apps N...	□			Inform EMM	
☑	Low	Android Device - Compatibility Not T...	□			Inform EMM	
✓	Critical	Android Device - Possible Tampering	□		Inform EMM	Inform EMM	
✓	Critical	App Tampering	□		Inform EMM	Unavailable	
☑	Low	ARP Scan	□		Inform EMM	Unavailable	
✓	Critical	BlueBorne Vulnerability	□		Inform EMM	Inform EMM	

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 z3A license has been purchased.

The following 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 McAfee.
- The user installs a new app on the device.
- The MDM sees the new app in the sample request update.
- McAfee sees the new app when the MDM sync is performed for that device.