McAfee MVISION Mobile

IBM MaaS360

Integration Guide

January 2021

Contents

Preface

This document is an administrator's guide to providing integration with IBM MaaS360 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 IBM MaaS360 MDM. The MVISION Mobile Console application provides threat protection to mobile devices, and the system administrator sets policies for threats. MVISION Mobile Console also monitors and manages threats detected. 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 users and 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 IBM MaaS360 integration, device synchronization is supported. Upon detection of an event, that information is sent to IBM MaaS360 through secure API's and is instructed to carry out a defined workflow to take action on the device.

Prerequisite Requirements

Integration with IBM MaaS360 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 API connection.

Item	Specifics
IBM MaaS360 MDM Enrolled Device	Release 7.2 and above
API Administrator Account in IBM MaaS360 Management Console	Proper role defined. Refer to the "Create an Administrator User in the IBM MaaS360 Console" section.
IBM MaaS360 Web Service Access	You must have web service access to your IBM MaaS360 environment. If you need access, contact IBM MaaS360 support at the following email address: support@maas360.ibm.com
Python Access	Access to Python for optional initial setup of IBM MaaS360. This involves the ZIP file download in section "Initial Configuration" and running some provided scripts.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the IBM MaaS360 console through API access. When MVISION Mobile detects an event, it consults the current Threat Policy resident on the device and if there is a specific MDM action defined, this is communicated to the MVISION Mobile Console. The MVISION Mobile Console then reaches out to the proper IBM MaaS360 API Server and provides the commands to perform the action described.

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 or device.

Full MDM Synchronization

After the full initial synchronization during the MDM integration setup, a scheduled synchronization process runs every four hours.

On-Demand Device 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 device 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.

Set Up Device Application Deployment

Overview

This section details the steps for setting up the deployment of the device application. A script is provided to configure the IBM MaaS360 environment.

API Access

Contact IBM for API access to IBM MaaS360. MaaS360 requires these details to generate an authentication token to access their REST APIs.

- Billing Id
- App Id
- App Version
- Platform Id
- App Access Key

Make sure you have these values before attempting to set up the integration. See the "Web Services Integration Details" at this website for more information:

https://developer.ibm.com/security/maas360/maas360-getting-started/maas360-web-services-integration-details/

NOTE: *You must be logged in to see this information*.

Initial Configuration

An optional Python script can be used to perform an initial configuration in the IBM MaaS360 environment. This script configures iOS and Android MVISION Mobile app from the public store, custom attributes and several device groups.

To use this script:

1. Download the ZIP file with the scripts and Readme file at this location: https://exchange.xforce.ibmcloud.com/hub/extension/ed98f063bab8ec358fa2f49424994083
2. After logging in, this link allows you to download a ZIP file similar to the name: **ZimperiumIntegrationScriptForMaaS360**_*version*.**zip** where *version* is the version of the script and ZIP collection.

   NOTE: *If you have issues logging in or downloading the ZIP file, contact your Customer Success team.*

3. The ZIP file contains the **ReadMe_v2.0.pdf** file. This document gives the details of running the script. This content is also provided in "Appendix A - Script Information."

4. The script in the ZIP file sets up the integration on the IBM MaaS360 environment and must only be run once. As part of the initial setup it configures:
    - Two Custom Attributes
        - Zimperium Risk Posture
        - Zimperium Device
    - Risk Posture Device Groups
        - Zimperium Risk Posture Low
        - Zimperium Risk Posture Elevated
        - Zimperium Risk Posture Critical
    - A device group named ‘Zimperium Devices'. This is a test device group that can be used to synchronize any devices whose custom attribute 'Zimperium Device' is set to 'yes'. You can create your own device groups or use the predefined MaaS360 groups depending on your needs.
    - The Dashboard Alert for devices whose risk posture is set to critical.
    - App Store entry for MVISION Mobile iOS.
    - Google Play Store entry for MVISION Mobile Android.

To publish the MVISION Mobile application from the public application store, create a new public application and 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

At this point, the application is now published and installed on the assigned devices. Your users can now activate the application as described in the platform guides in the Customer Support portal.

Configuration Steps

Some configuration steps are performed on the IBM MaaS360 MDM side. Other steps are performed for MVISION Mobile Console. The following are the advantages of setting up the configuration:

- Avoid having to create user credentials and to manage the user management lifecycle.
- Devices and their associated users can be synchronized through MDM integration.

This allows all device and user management functions to be handled at the MDM console.

Create an Administrator User in the IBM MaaS360 Console

To set up device synchronization, create an IBM MaaS360 administrator with the proper access:

1. Navigate to Setup > Roles > Add Role.
2. Enter a name and description for the new role.
3. Select the Service Administrator role as the template.

Item	Specifics
Manage Custom Attributes	Ability to add, change, or delete Custom Attributes.
Selective Wipe	Ability to selectively wipe corporate data from the device.
Set Custom Attribute Value	Ability to set custom attributes.
User - Read-only	View-only access to a user's view.
View installed apps	Ability to view installed apps on a device.
View Private groups	Ability to view Private Device groups for all admins.

IBM MaaS360 API Access and Device Groups

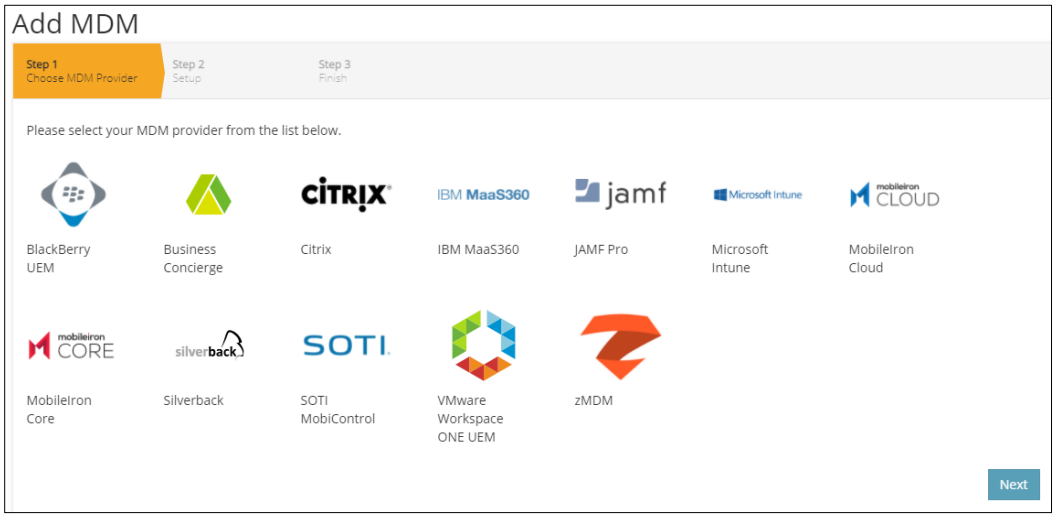
To set up API access and create device groups:

1. Call IBM Customer Support to get the REST API Key.
2. If required, create one or more Device Groups that contain the devices to be protected. If you do not want to use the predefined group, MVISION Mobile Console can use the Device Group(s) to synchronize devices and their associated users.

Set Up User and Device Synchronization in MVISION Mobile Console

To set up the integration in the MVISION Mobile Console:

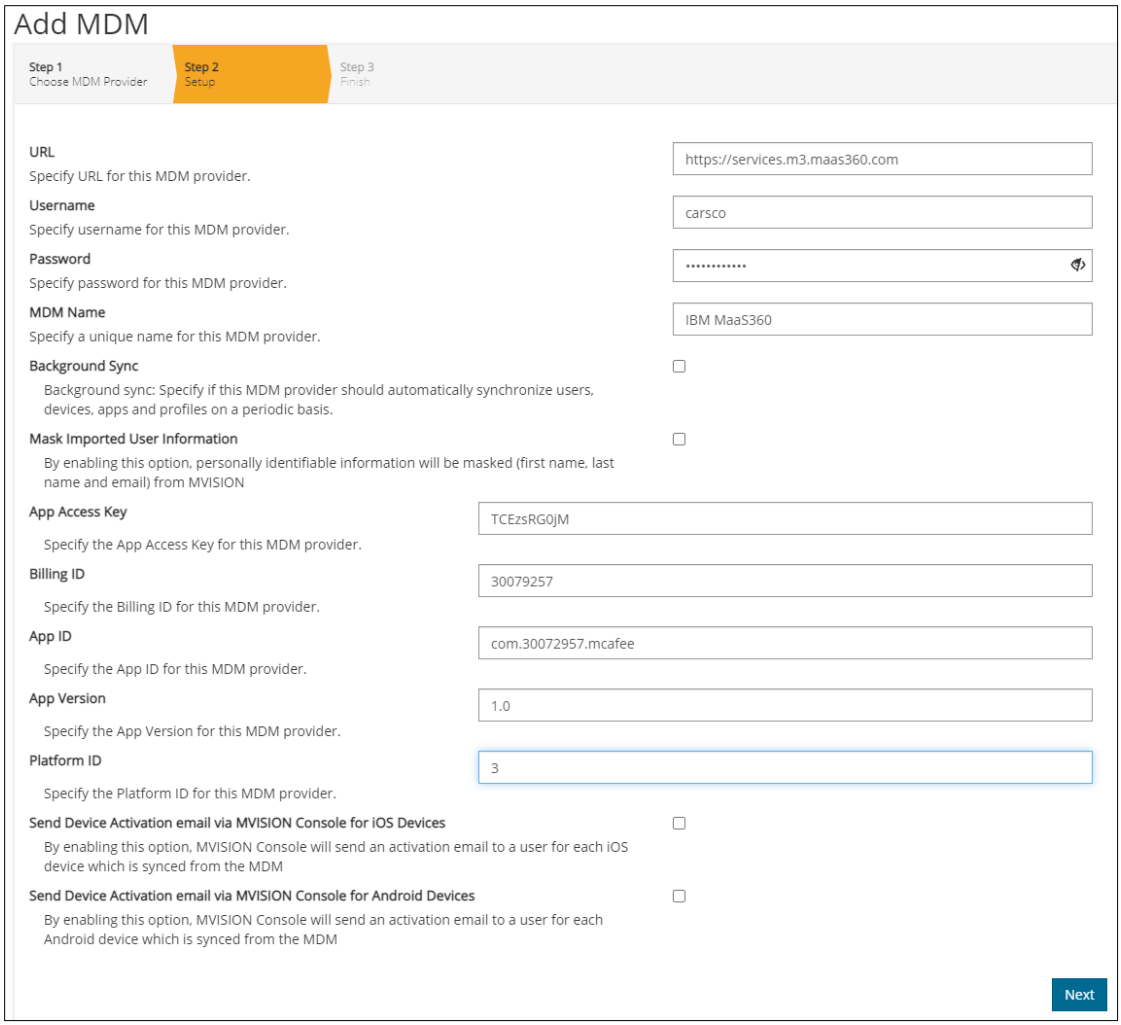
1. Login to MVISION Mobile Console and navigate to Manage/ MDM.
2. Click on **Add MDM** and select the IBM MaaS360 icon.



3. Enter the information for the IBM MaaS360 integration in the table.

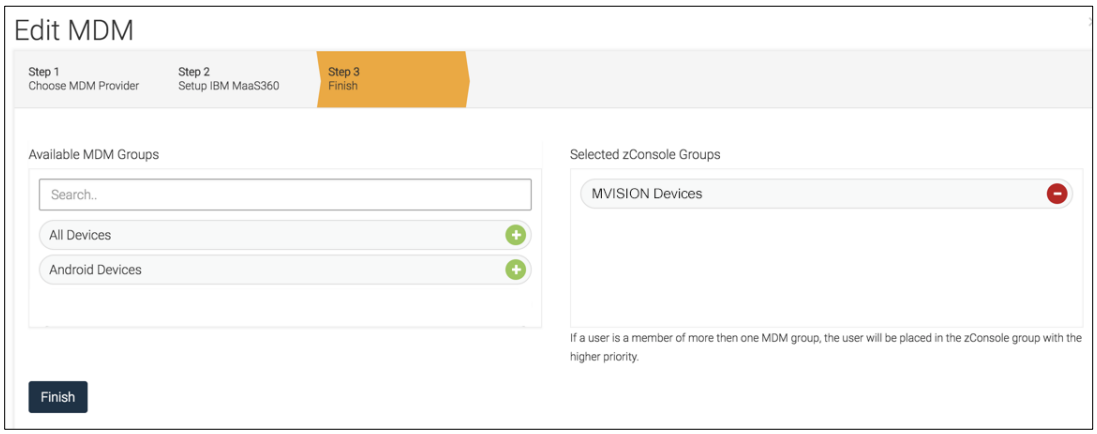
Item	Specifics
URL	URL of the IBM MaaS360 API Server.
Username	IBM MaaS360 Administrator created with the API role access.
Password	The password of the IBM MaaS360 Administrator.
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This name is prepended to the group name to form the MVISION Mobile Console group name.
Background Sync	Check this box to ensure users/devices are synchronized with the IBM MaaS360 Device Groups. You chose the groups on the next page.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, such as name or email address.
App Access Key	This is the app access key value from this MDM provider. You get the API key value from IBM after enabling the web services.
Billing ID	This is the app access key value from this MDM provider.
App ID	This is the app identifier from this MDM provider.
App Version	This is the app version from this MDM provider.

Platform ID	This is the platform id from this MDM provider.
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.



4. Click **Next**. The available Device Groups are shown under the **Available** column and can be moved over to the **Selected** column by clicking on the plus sign ('+'), or reversed by clicking on the minus sign ('-').
5. Click **Finish** to save the configuration and start the first synchronization.

Each Device Group selected is set up as MVISION Mobile Console groups for Privacy settings, Role access and Threat Policy assignments. If a device falls into more than one Device Group, the first Device Group displayed is its MVISION Mobile Console group. To change the order of the listing, drag and drop Device Groups in the UI.



You can verify the completion by navigating to the **Devices** or **Users** pages in the MVISION Mobile Console. The device entries are greyed out until the user starts up MVISION Mobile and activates the app.

Configuring Device Application Auto-Activation

The McAfee MVISION Mobile applications in 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 Managed 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 Managed Application configuration pre-programs MVISION Mobile iOS with the required information.

This configuration is performed within IBM MaaS360. During the add application step there is a configuration option.

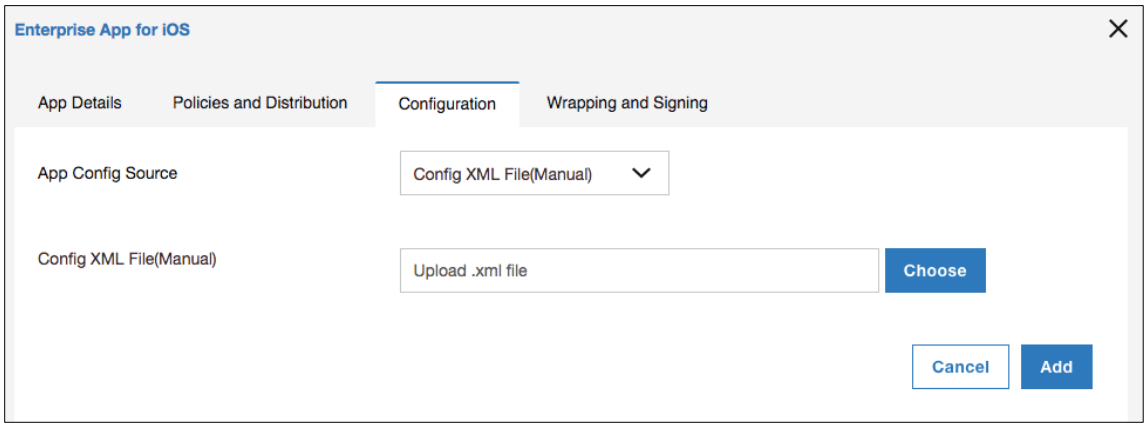
1. Configure the PLIST values and use these values and also in the PLIST XML.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	%csn%
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).
tracking_id_1	String	(Optional) Use your desired identifier.
tracking_id_2	String	(Optional) Use your desired identifier.

NOTE: *The configuration keys are case sensitive*.

2. Choose **Config XML File(Manual)** or **Key/Value** for the App Config Source.



3. If you select the XML file option, the XML file has this example content for MVISION Mobile.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList 1.0.dtd">
<plist version="1.0">
<dict>
    <key>MDMDeviceID</key>
  <string>%csn%</string>
    <key>tenantid</key>
  <string>tenant-ID</string>
    <key>defaultchannel</key>
  <string>https://acceptor.mcafee-mvision-mobile.com/srx</string>
</dict>
</plist>
```

4. If you select the Key/Value pair option, you can enter the values without having to create a file.

Android Activation

Android Enterprise users can continue to 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 variables are the same set as the PLIST variables in the "iOS Activation" section.

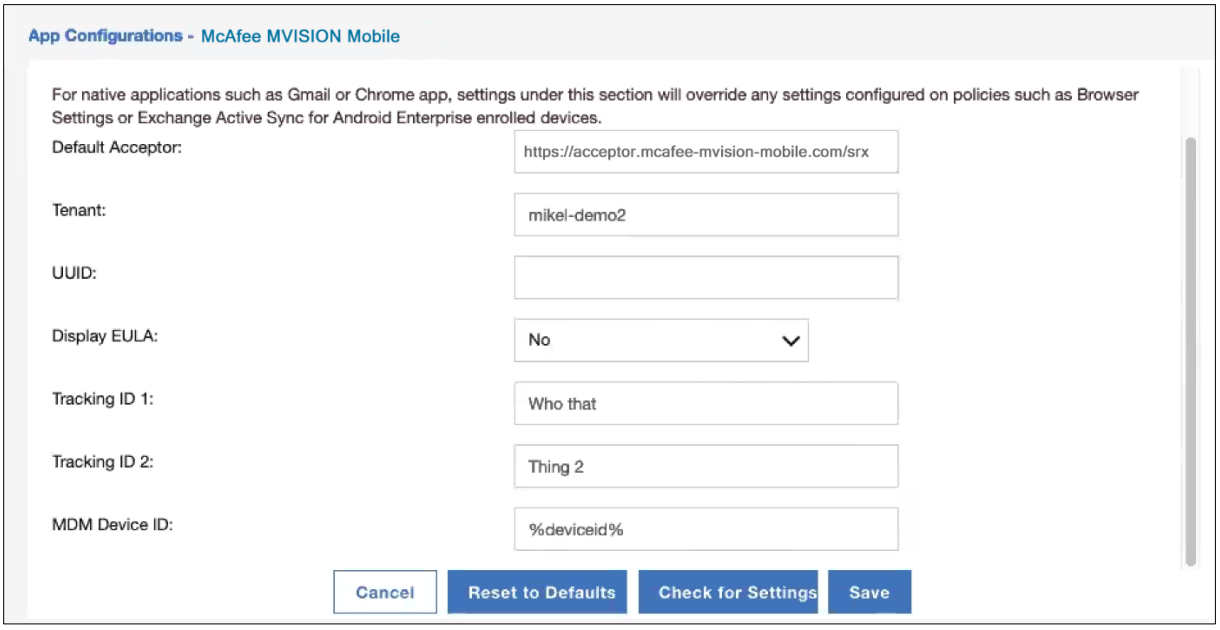
For native Android devices, activations require the use of activation URLs. These can be sent to end-users through the MVISION Mobile Console or the MDM. Clicking on MVISION Mobile without the link does not activate MVISION Mobile for Android devices. When a user runs the app with the activation URL link, it activates and downloads the proper Threat Policy.

To access activation links, navigate to MVISION Mobile Console Manage > Integrations. After the MDM is added, the activation link is provided for devices. This activation link is used along with appending the MDM device identifier. The MVISION Mobile Console page displays the expiration date and time, and if needed, the link can be regenerated.

See the "*McAfee MVISION Mobile Product Guide*" document for more information on the MDM activation links.

The administrator sends the concatenated activation link by email or text to users, along with instructions to accept the MVISION Mobile app being pushed to them.

This figure shows an example of the setting of the Key-Value pairs for Android.



Use these values in the configuration.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	%deviceis%
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).
tracking_id_1	String	(Optional) Use your desired identifier.
tracking_id_2	String	(Optional) Use your desired identifier.

NOTE: *The configuration keys are case sensitive*.

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.

Device Actions and Remediation

In MVISION Mobile Console the term 'MDM Action' is synonymous with a device action. It is an action that an administrator pushes to the device. When the integration is set up with the MDM, the administrator can select the MDM actions to perform for each threat in the MVISION Mobile Console Threat Policy definition.

Risk Postures

On the MDM, there is a custom attribute named 'McAfee Risk Posture' with the following values:

- McAfee Risk Posture Normal
- McAfee Risk Posture Low
- McAfee Risk Posture Elevated
- McAfee Risk Posture Critical

These values are used to indicate the risk level of the device. For instance, an Inform EMM action sets the 'McAfee Risk Posture' attribute to one of the values such as 'McAfee Risk Posture Critical' when a given threat occurs. This value is dependent on the settings in the MVISION Mobile Console Threat Policy definition.

Available Device Actions

IBM MaaS360 integration provides several MDM actions to push to the device. For example, choosing the 'Inform EMM' action causes the MVISION Mobile Console to notify IBM MaaS360 that a threat has occurred and sets the risk posture attribute.

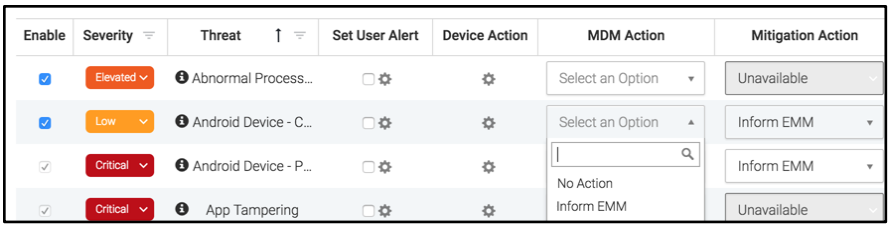
The available MDM Actions are the following:

- No Action
- Inform EMM
- Lock Device and Inform EMM
- Selective Wipe and Inform EMM

The threat policy defines which action to take for each threat. For instance, the MDM Action 'Selective Wipe' removes the enterprise apps from the device, and informs the MDM and sets the risk posture value.

When the threat is mitigated, the risk posture is set back to the 'McAfee Risk Posture Normal' value.

This figure shows a portion of an MDM Action dropdown on the Policies page for the IBM MaaS360 MDM.


Enable
Severity
Threat
Set User Alert
Device Action
MDM Action
Mitigation Action
Elevated
Abnormal Process...
Select an Option
Unavailable
Low
Android Device - C...
Select an Option
Inform EMM
Critical
Android Device - P...
Inform EMM
No Action
Inform EMM
Critical
App Tampering
Unavailable

Appendix A - Integration Script Information

The following section includes the readme file information that is in the ZIP file that you downloaded in the “Initial Configuration” section.

Objective

The included scripts set up the required attributes and entities within IBM MaaS360 for integration with McAfee MVISION Mobile Threat Defense. These scripts create the following:

- A boolean custom attribute called Zimperium Device.
- A test Zimperium device group based on the boolean custom attribute.
- A risk posture custom attribute representing normal, low, elevated, and critical risks.
- Device groups based on each risk posture of low, elevated, and critical.
- An alert for the IBM Maas360 dashboard that contains devices with a risk posture of critical.
  NOTE: *Ensure you only run the integration scripts one time*.

Also, the McAfee MVISION Mobile iOS and Android apps are loaded into the App Catalog of the IBM MaaS360 environment and are associated with the new device group.

Requirements Before Starting

The following table lists the software and access requirements that you need to begin.

Requirement	Description
Python 2.7 or higher	You must have this version of Python or higher to run these scripts. If you do not have this version, download it from this link: https://www.python.org/downloads/
IBM MaaS360 Web Service Access	You must have web service access to your IBM MaaS360 environment. If you need access, contact IBM MaaS360 support at the following email address: support@maas360.ibm.com

Script Execution Instructions

Perform these steps to run the scripts:

1. Extract the contents of the attached ZIP file into a folder. The distribution contains three Python script files and a Readme file.
2. You only need to edit the **Runner.py** file. Do not update any other files.
3. Open the **Runner.py** file in a text editor and set the values for the following parameters:
   a) WS_SERVER_BASE: This value points to the base web service URL for your MaaS360 portal, such as the following: https://services.m3.maas360.com

   b) BILLING_ID: This is the billing identifier for your organization's account in MaaS360.
   c) USERNAME: This is the username for your MaaS360 account that you use for web service access.
   d) PASSWORD: This is the password for your MaaS360 account.
   e) APP_ID: This is the App identifier provisioned in MaaS360.
   f) APP_VERSION: This is the app version of app provisioned in MaaS360.
   g) PLATFORM_ID: Set this value to 3.
   h) APP_ACCESS_KEY: This is the access key generated by MaaS360.
   NOTE: *Contact your MaaS360 support to get the values for configuring your web service access and providing these parameters for your account.*

4. After editing the file with correct values, save the file.
5. Run the script on command line by entering:
   python Runner.py

6. Confirm that the script runs successfully without any errors.