McAfee™
Together is power.

McAfee MVISION Mobile

IBM MaaS360 Integration Guide

MVISION Mobile Console 4.22

February 11, 2019

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Integration with IBM MaaS360

Overview

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

- Synchronize users and devices from the MDM
- Transparent user access to MVISION Mobile Threat Detection Application
- More granular and specific protection actions

McAfee's MVISION Mobile Threat Detection Application detects malicious activity and depending on the MDM platform, is able to take actions locally. When MVISION Mobile Threat Detection Application is integrated with an MDM, protection actions can be performed by the MDM in addition to local MVISION Mobile Threat Detection Application actions, providing a very powerful protection tool. In the phase 1 of the IBM MaaS360 integration, device and user synchronization is supported. In phase 2, upon detection of an event, that information is sent to IBM MaaS360 via secure API's and is instructed to carry out a defined workflow to take an action on the device.

Requirements

Integration with IBM MaaS360 requires a connection between the McAfee MVISION Mobile Console and the IBM MaaS360 API server. This is accomplished via the Internet using SSL on TCP port 443.

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 in section below.
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 MaaS360.

Architecture

McAfee integrates with IBM MaaS360 MDM with different configuration levels which are described in the "McAfee MVISION Mobile Console Configuration Guide" available in the customer portal. Each level is addressed further on in this document with specific configuration instructions. To achieve level 2 – 4 integrations, the MVISION Mobile Console is configured to share information with the IBM MaaS360 console through API access. When MVISION Mobile Threat Detection Application 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 IBM MaaS360 API Server and provides the commands to perform the action described.

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.

> **Important Note**: When you contact IBM for API access to IBM MaaS360, it is highly recommended that you ensure that your app id value is in the format of "**com.***accountNumber***.mcafee**" where *accountNumber* is the corporate identifier.

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 and an initial device group that can be used for synchronization. To use this script, perform the following:

- Download the script and Readme file at this location:
  https://exchange.xforce.ibmcloud.com/hub/extension/ed98f063bab8ec358fa2f49424994083

  This is used to setup the integration on the IBM MaaS360 environment and must only be run once. As part of the initial setup it configures the following:

  - The first device group, 'McAfee Devices'. This device group can be used to synchronize devices and users with MVISION Mobile Console or you can create your own device group(s) as needed.
  - iOS App Store entry for MVISION Mobile App
  - Android Google Play entry for MVISION Mobile App

  These apps are optional and if you are provided with the IPA and APK files you can proceed to add them as described below.

To deploy the MVISION Mobile App through IBM MaaS360, 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 the Android MVISION Mobile App through IBM MaaS360 as an internal app. This allows McAfee to provide updates to the MVISION Mobile App ahead of the store version.

To deploy as an internal app, login to IBM MaaS360, create a new Enterprise App and upload the proper application file (IPA for iOS and APK for Android) to IBM MaaS360. Then, distribute to the devices that are to be protected by MVISION Mobile App.

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

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.

About User Synchronization

To avoid having to create user credentials and the user management lifecycle, devices and their associated users can be synchronized through MDM integration. This allows all user management functions to be handled at the MDM console.

After the initial user 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.

Ad-Hoc 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 ad-hoc 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. For this to work correctly, MVISION Mobile App must be deployed as follows:

- **iOS**: Associate an app configuration with the MVISION Mobile App that pushes down the Tenant ID and Acceptor to be used for the ad-hoc synchronization. This is described in the section "Configuring Device Application Auto-Activation"
- **Android**: Ad-hoc MDM synchronization for Android required the MVISION Mobile App to be modified. Contact your McAfee Customer Support team to set this up for Android.

By default, each user synchronized has the same password. To determine the password, take the McAfee environment name, change upper case letters to lowercase and also change spaces to dashes. The password is the normalized environment name with "1234!" appended to the end. So, the string "*McAfee Test"* becomes "*McAfee-test1234*!".

The password used for each user can be overwritten in the MDM setup screen.

Synchronization includes the following information:

- User ID (Email address) of user.
- Device Hash ID.
- Device UUID.

Applications installed on the device.

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 setup device synchronization, perform the following:

- Create an IBM MaaS360 administrator with the proper access.
    - Navigate to: SETUP/ Roles/ Add Role
    - Enter a name and description for the new role
    - Select the Service Administrator role as the template

Name	Description
Manage Custom Attributes	Ability to add, change or delete Custom Attributes
Selective Wipe	Ability to selectively wipe corporate data from device
Set Custom Attribute Value	Ability to set custom attributes
User - Read-only	View only access to user 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

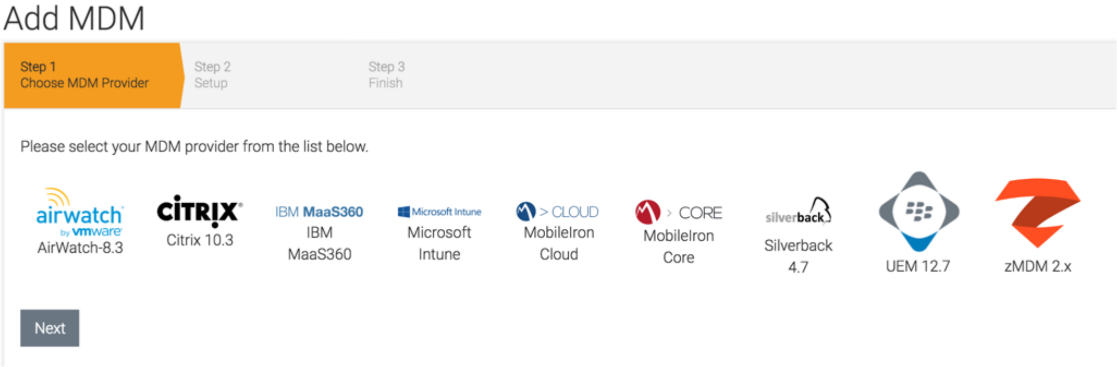
Perform the following steps:

- Call IBM to get the REST API Key (Customer Support).
- 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 uses the Device Group(s) to synchronize devices and their associated users.

Set Up User and Device Synchronization in MVISION Mobile Console

Perform the following steps:

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



Add MDM

Step 1 Choose MDM Provider

Step 2 Setup

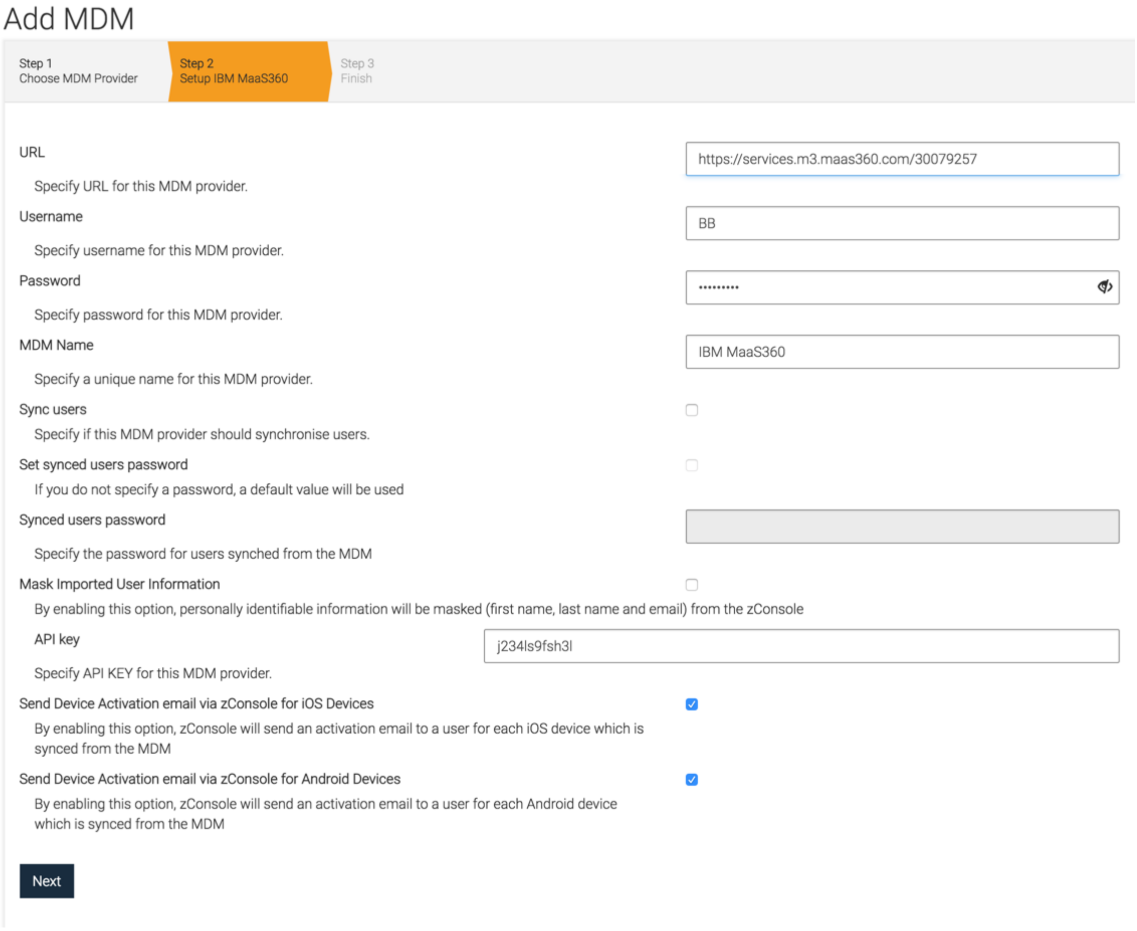
Step 3 Finish

Please select your MDM provider from the list below.

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

Item	Specifics
URL	URL of the IBM MaaS360 API Server. This string must end with the account number or corporate identifier, for instance "/30079256". **Note**: This URL may not be valid in a browser and may get a 404 error.
Username	IBM MaaS360 Administrator created with the API role access
Password	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.
Sync Users	Check this box to ensure users/devices are synchronized with the IBM MaaS360 Device Groups chosen in the next page.
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.

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	API Key used for secure authentication to the API Server.
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.



Add MDM

URL: https://services.m3.maas360.com/30079257
Specify URL for this MDM provider.

Username: BB
Specify username for this MDM provider.

Password: •••••••••
Specify password for this MDM provider.

MDM Name: IBM MaaS360
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

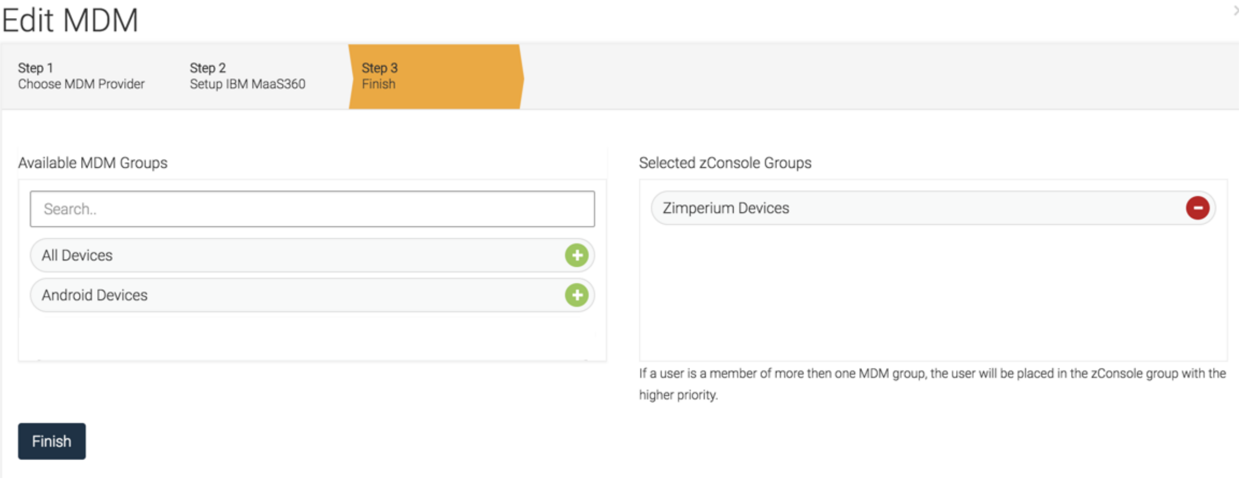
API key: j234ls9fsh3l
Specify API KEY for this MDM provider.

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

- Click **Next** and choose the Device Group(s) to synchronize with. The available Device Groups are shown on the left under the ‘Available’ column and can be moved over to the ‘Selected’ column by clicking on the plus sign (‘+’). This can be reversed by clicking on the minus sign (‘-’).
- Click **Finish** to save the configuration and start the first synchronization. Each Device Group selected is setup as MVISION Mobile Console groups for Privacy settings, Role access and Threat Response Policy/Matrix assignments. 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.



Edit MDM

Step 1
Choose MDM Provider

Step 2
Setup IBM MaaS360

Step 3
Finish

Available MDM Groups

Search..

All Devices

Android Devices

Selected zConsole Groups

Zimperium Devices

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

- The Device Groups are retrieved, and user/device synchronization is complete.
- You can verify the completion by navigating to the Devices or Users pages in the MVISION Mobile Console and verify they display. The device entries are greyed out until the user starts up MVISION Mobile App and activates the app.

Configuring Device Application Auto-Activation

The McAfee MVISION Mobile App in both iOS and Android Enterprise (Android for Work) automatically activate the user if MDM user synchronization is configured. The process is different on each platform as described below.

When a user clicks on MVISION Mobile App (iOS/Android) it auto-activates and downloads the proper TRM.

iOS Activation

McAfee's iOS MVISION Mobile App 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 iOS MVISION Mobile App without having to enter any credentials. The Managed Application configuration pre-programs iOS MVISION Mobile App with the required information.

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

For MVISION Mobile App Release 4.7.x use these values instead and also in the plist XML.

Configuration Key	Value Type	Configuration Value
uuid	String	%csn%
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team
display_eula	String	no (If this key is not used, the default displays the EULA.)

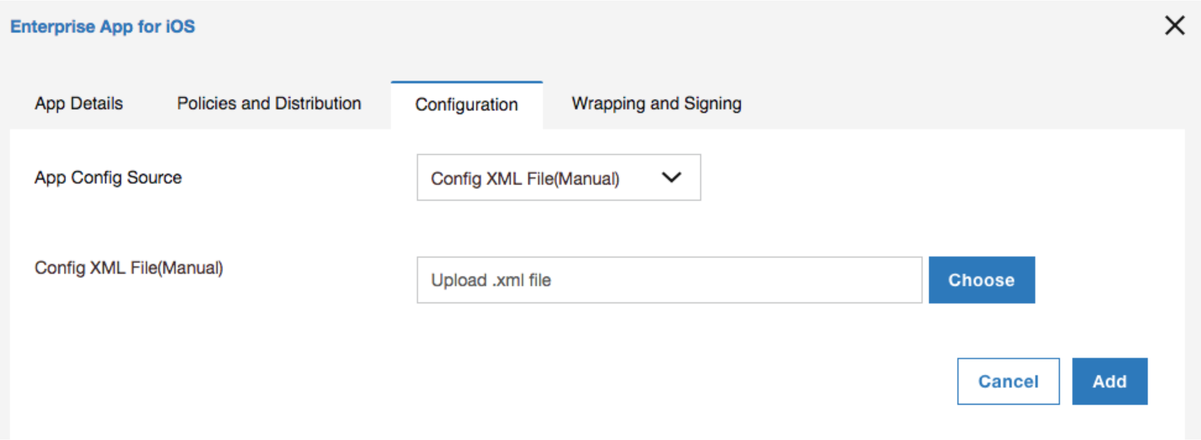
Note: The configuration keys are case sensitive.

For MVISION Mobile App Release 4.8.0 or later, use these values instead and also in the plist XML.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	%csn%
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 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.

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



App Config Source: Config XML File(Manual)

Config XML File(Manual): Upload .xml file

2) If you select the XML file option, the XML file has this example content for MVISION Mobile App Release 4.8.0:

```
<?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://sample-default-channel.McAfee.com:443/srx</string>

    </dict>

    </plist>
```

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

Android Activation

Android Enterprise (Android for Work) 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 via the MVISION Mobile Console or the MDM. Clicking on MVISION Mobile App without the link does not activate MVISION Mobile App for Android devices. When a user runs the app with the activation URL link, it activates and downloads the proper TRM.

To access activation links, use the MVISION Mobile Console Manage page and select the MDM tab. After the MDM has been 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.

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.