McAfee MVISION Mobile

AirWatch Integration Guide

Administrator's guide for providing Integration with AirWatch MDM

September 2018

Contents

Integration with AirWatch

Overview

Integration with an MDM is not required, however, when an MDM is integrated, the MVISION Mobile Console can synchronize users and devices from the MDM, provide transparent user access to MVISION Mobile Threat Detection Application and provide more granular and specific protection actions.

McAfee MVISION Mobile Threat Detection Application detects malicious activity and depending on the platform will be able to take actions locally. When MVISION Mobile Threat Detection Application is integrated with an MDM, protection actions can be performed by the MDM, providing a very powerful protection tool. Upon detection of an event, that information is sent to AirWatch via secure API's and is instructed to carry out a defined workflow to take an action on the device.

The AirWatch Administrator can setup different workflows to handle different situations/threats that the MVISION Mobile Console Administrator can choose through the policy page. AirWatch Smart Groups, Tags and Profiles are used to achieve the workflow to protect the device.

Requirements

Integration with AirWatch requires a connection between the McAfee MVISION Mobile Console and the AirWatch API server. This is accomplished via the Internet using SSL on TCP port 443. If using an AirWatch SaaS management server, there are no changes that need to occur to allow for this communication. For an On-Premise AirWatch management server, there must be an allowed path for the MVISION Mobile Console to connect to the API Server on port 443.

The following table details specific requirements for the API connection:

Item	Specifics
AirWatch MDM enrolled device	V7.2 and above (1)
API Administrator Account in AirWatch management console.	Proper Role defined in section below.
API REST Key	Provided from AirWatch Environment.
Privacy collection policy	Include Personal Applications

(1) AirWatch V8.0 through V8.1 Feature Pack 3 do not support MDM Actions.

Create an API key that only McAfee will use for communication between the MVISION Mobile Console and AirWatch. This will provide for separation of traffic from other API communications to the AirWatch API server. AirWatch monitors the API connection per API key to ensure the number of connections do not extend above a threshold which might be different for each implementation. By, using a unique API key for McAfee traffic the chances of hitting that threshold is greatly reduced. The steps to do this are listed further on in this document.

Architecture

McAfee integrates with AirWatch MDM with different configuration levels which are described in the *McAfee MVISION Mobile Console Guide* available in the support portal. Each level is addressed further

on in this document with specific configuration instructions. To achieve level 2 – 4 integrations, the MVISION Mobile Console will be configured to share information with the AirWatch console through API access. When MVISION Mobile Threat Detection Application detects an event, it consults the current Threat Response Matrix resident on the device and if there is a specific MDM action defined, this is communicated to the Cloud server. The Cloud server will then reach out to the proper AirWatch API Server and provide the commands to perform the action described.

Protection Methods

McAfee interacts with the AirWatch MDM through API's that provide the ability to modify device configurations securely over the internet. Two basic methods are used that provide granular protection capabilities.

1. WiFi Disconnect
   If a 'WiFi Disconnect' is defined as a response to a threat, the MVISION Mobile Console will send an API request to AirWatch that will create a specifically crafted WiFi profile and send that profile to the device. This profile is created in such a way that the currently connected WiFi network will be disconnected when the profile is received by the device. The WiFi profile is removed after five minutes from the time the detection occurred. This applies to iOS devices only at this time.

2. Enterprise Wipe
   Remove all company information from the device including managed apps and configurations. Then unenroll the device from AirWatch.

3. Smart Group Membership
   If a Smart Group is defined as a response to a threat, MVISION Mobile Console will instruct AirWatch to assign the device to the chosen Smart Group. The workflow assigned to that Smart Group will determine the action that AirWatch takes on the device.

   Examples of workflows are in the Appendix and at a high level consist of:

   a. Compliance policy: The Smart Group the device has been assigned to is assigned to a Compliance Policy that will allow the MDM Administrator to take any action that the compliance policy provides. This can include everything from a simple message to the device user, up through an Enterprise Wipe to remove company intellectual property to be removed from the device.
   b. Exclusion group: Assigning the device to a Smart Group used as an exclusion group in a profile will immediately remove the profile from that device.

   The mechanism to assign a device to Smart Group includes assigning a device to a Smart Group directly (AirWatch 7.2 and 7.3) or assigning a TAG to a device which in turn assigns a device to a Smart Group (AirWatch V8.0+). In either version, the result is the same.

Configuration Levels

Level 1: Basic Application Deployment

To deploy the MVISION Mobile Threat Detection Application through AirWatch, ask your Customer Success Team at McAfee for the iOS and Android version of MVISION Mobile Threat Detection Application. Both iOS and Android MVISION Mobile Threat Detection Application are in their respective public application stores, but it is good practice to deploy the Android MVISION Mobile Threat Detection Application through AirWatch as an internal app. This will allow McAfee to provide updates to the MVISION Mobile Threat Detection Application ahead of being in the store which could take some time.

To deploy as an internal app, login to AirWatch and go to the Organization Group where the application should be installed. If no appropriate Smart Group exists for the application deployment, create that as well. Create a new Internal Application and upload the proper application file (IPA for iOS and APK for Android) to AirWatch. Assign the Smart Group to the application and publish.

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

At this point the application is now published and installed on the devices in the Smart Group assigned. Your users can now activate the application as described in the platform guides in the Support Portal. They will need the User ID and Password created in the MVISION Mobile Console to access the application, unless User Synchronization is performed.

Level 2a: User Synchronization

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

After the initial User Synchronization during the MDM Integration setup, users will be managed through a scheduled synchronization process that will run every four hours. If we see additional users in the Smart Group(s) being used for synchronization, we will add them and their devices to MVISION Mobile Console. If we see users removed, then we will remove them from the MVISION Mobile Console. Doing this will 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 will have MVISION Mobile Threat Detection Application pushed down to their device and attempt 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 Threat Detection Application tries to login but no information yet exists for it. MVISION Mobile Console will get the identification information from MVISION Mobile Threat Detection Application used for the authentication and match it up with the proper customer for authentication. Once that happens, MVISION Mobile Console will retrieve that device and user information from the MDM configured for that customer. MVISION Mobile Threat

Detection Application on that device is now authenticated and allowed to proceed. For this to work correctly, MVISION Mobile Threat Detection Application must be deployed as follows:

- **iOS**: Associate an app configuration with the MVISION Mobile Threat Detection Application that pushes down the Tenant ID and Acceptor to be used for the Ad-hoc sync. This is described in the section below: Level 2b: Auto Sign-in/Advanced Application Deployment Level 2b: Auto Sign-in/Advanced Application Deployment
- **Android**: Ad-hoc MDM synchronization for Android required the MVISION Mobile Threat Detection Application to be modified. Contact your McAfee Customer Support Team to set this up for Android.

By default Each user synchronized will have 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 this: *McAfee Test* becomes *McAfee-test1234*!

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

User synchronization includes the following information:

1. User ID (Email address) of user
2. Device Hash ID
3. Device IMEI, UUID
4. Applications installed on the device. The AirWatch privacy settings for 'Personal Application' are required to be set to 'Collect'.

To setup User Synchronization;

1. Create an AirWatch administrator with the proper access.
   Navigate to: Accounts/ Administrators/ Roles/ Add Role. Provide name, Description and click on API. Select the following:

Read/Edit	Category	Name	Description
Read	REST	Devices	REST APIs for device management
Read/Edit	REST	Groups	REST APIs for group management
Read/Edit	REST	Profiles	REST APIs for device profiles
Read/Edit	REST	Users	REST APIs for enrollment user accounts
Read/Edit	REST	Tags	Access all Tag APIs (required for AirWatch V8.0+)

2. Enable REST API and retrieve the API REST Key.
   Navigate to: Groups & Settings/ All Settings/ System/ Advanced/ API/ REST API.

   Enable API Access if not already enabled.

   To create a unique REST API key:

   A. Click on the +Add button
   B. In the new entry that shows up;
      a. Enter your new service name

b. Set the account type to Admin

C. Click Save

D. Copy the new REST API key for use

3. Create one or more Smart Groups that will contain the devices that will be protected, if you do not have one that exists. MVISION Mobile Console will use the Smart Group(s) to synchronize Users and devices.
4. Enable the collection of Personal Applications.
   Navigate to: Groups & Settings/ All Settings/ Devices & Users/ General/ Privacy

   Scroll down to find the Application heading and ensure all the settings allow for collect.

5. Log in to MVISION Mobile Console and navigate to Manage/ MDM:
6. Click on Add MDM and select the correct version of AirWatch. (Note: AirWatch-8.3 supports AirWatch 9.x as well)
7. Enter information pertinent for the AirWatch integration

Item	Specifics
URL	URL of the AirWatch API Server
Username	AirWatch Administrator created with the API role access
Password	Password of the AirWatch Administrator
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This will be prepended to the group name to form the MVISION Mobile Console group name.
Sync Users	Check this box to ensure users/devices will be synchronized with the AirWatch Smartgroups chosen in the next page.
Set synced users password	Check this box to override the default password during user sync. If this is not checked a default password will be 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. So this: *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: Name, Email address
API Key	API Key used for secure authentication to the API Server.

8. Click Next and choose the Smart Group(s) to synchronize with. The available Smart Groups will show on the left under the 'Available' column and can be moved over to the 'Selected' column by clicking on the '+' sign. This can be reversed by clicking on the '-' sign. Click Finish to save the configuration and start the first synchronization. Each Smart Group selected will be setup as MVISION Mobile Console groups for Privacy settings, Role access and Threat Response Policy assignments. If a device falls into more than one Smart Group, the highest or first Smart Group

it appears in will be the MVISION Mobile Console group it will be defined to. To change the order of the listing, drag and drop Smart Groups as required.

9. The Smart Groups will be retrieved and user/device synchronization will be completed.
10. You can verify this by going to the Devices or Users pages in the MVISION Mobile Console to verify they are showing up. The device entries will be greyed out until the user starts up MVISION Mobile Threat Detection Application and logs in. Their userID will be their email address and the password defined above.

Level 2b: Auto Sign-in/Advanced Application Deployment

The McAfee MVISION Mobile Threat Detection Application applications in both iOS and Android will auto-sign-in the user if MDM user synchronization has been configured. The process is different on each platform as described below.

McAfee's iOS MVISION Mobile Threat Detection Application is written to take advantage of the Managed Application Configuration when the app is pushed down to the device. This will provide the best user experience, allowing the user to startup iOS MVISION Mobile Threat Detection Application without having to enter any credentials. The Managed Application configuration will pre-program iOS MVISION Mobile Threat Detection Application with the required information.

This configuration is done within AirWatch; During the add application step there is an option to define the deployment:

1. In this page, choose Send Application Configuration.

2. The following values should be added to this configuration:

Configuration Key	Value Type	Configuration Value
serial	String	{DeviceSerialNumber}
uuid	String	{DeviceUid}
imei	String	{DeviceIMEI}
wifimac	String	{DeviceWLANMac}

NOTE: The configuration keys have to be entered in lower case.

For iOS Ad-Hoc MDM sync to function properly, add these two new plist values:

Configuration Key	Value Type	Configuration Value
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team

3. Press Publish & Save to push this to devices in the Smart Group.

Android MVISION Mobile Threat Detection Application does not require an Application Configuration to be setup and will find the correct environment by searching for its known Device ID/Serial Number in the MVISION Mobile Console environment. If not using Ad-Hoc Sync then when the device is synced from the MDM, it will be available for enrollment.

When a user clicks on MVISION Mobile Threat Detection Application (iOS/Android) it will auto-login and download the proper TRM.

Level 3: Basic Protection

Once API integration is setup with the MDM, choosing *"Disconnect WiFi"* will cause the MVISION Mobile Console to tell AirWatch to push a WiFi profile to the device under attack that disconnects the currently connected WiFi network. This removes the device from the dirty WiFi network. The profile and Smart Group are created automatically when a device is under attack and removed as defined above. (Currently iOS only)

In addition, an MDM Action called 'Enterprise Wipe' has been added that will perform an Enterprise Wipe on the device. This will remove all company data from the device including email, apps and configurations and then unenroll the device from AirWatch.

Level 4 Granular Protection

The McAfee integration with AirWatch provides the ability to put the device in a specific Smart Group within the customer AirWatch environment. This will allow the AirWatch administrator to define specific actions, such as to remove an application, remove email access, remove/assign a profile or even unenroll a device, all of which will happen automatically. To accomplish this, the AirWatch administrator will need to coordinate with the MVISION Mobile Console administrator what specific actions are needed. MDM Integration with MVISION Mobile Console also has to be setup and functional.

Once a Smart Group is defined, you can reference that Smart Group in the pull down list under MDM Action in the Policy page. In this case when an ARP MITM occurs, the device will be placed into the 'Action1-JB' Smart Group and whatever Exclusion Profile or Compliance Policy it is applied to will take place:

Here is an example;

To remove access to company email that is configured originally by AirWatch (V8.0+):

1. In AirWatch Create an empty Smart Group that will be used to place the device that is under attack.
   a) Create an Empty Tag to be used for the assignment:
      - Groups & Settings/ All Settings/ Device & Users/ Advanced/ Tags/ Add
        Type in the TAG name and choose Type = Device.
   b) Create an empty Smart Group based on that Tag:
      - Groups & Settings/ Groups/ Assignment Groups/ Add Smart Group
        Enter new Smart Group name
        Smart Group type should be 'Select Criteria'
        Enter the new Tag name created above in the Tag section

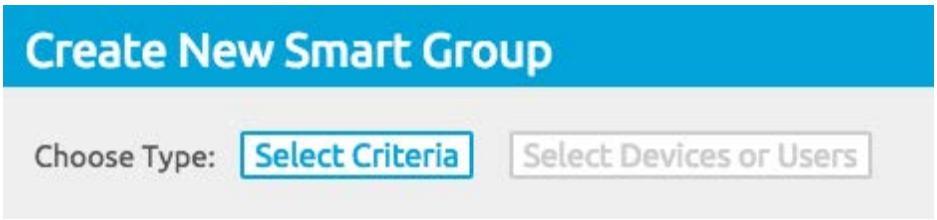
c) Create a Compliance Policy using these configuration items: (This can also be done with an exclusion group on the Exchange Profile)
   - Devices/ Compliance Policies/ List View/ Add
     Rule: Match the minimum OS (iOS or Android) requirements to be => so that this rule will always be true.
     Actions: Profile, Block/Remove Profile Type, Exchange ActiveSync
     Assignment: Assigned Smart Group should be the Smart Group created in (b) above.

2. In MVISION Mobile Console:
   - Go to Management/ MDM Settings/ Sync Now (this will make us aware of the new Smart Group).
   - Go to Policy and find the threat to assign this action to. Under MDM Action, choose this new Smart Group.
   - Deploy the TRM to all your devices.

Appendix

MDM Action Use Cases:

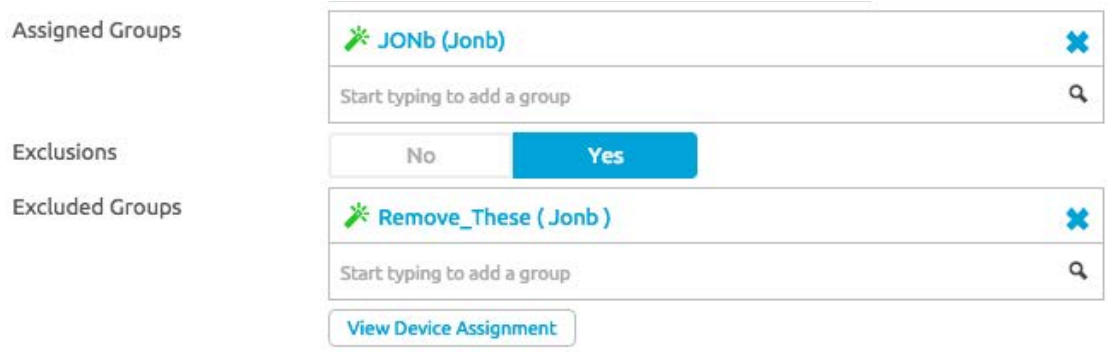
For more granular options, the MVISION Mobile Console integration with AirWatch can facilitate the following actions with Smart Groups. When defining these actions, it is important to create an empty Smart Group and choose the "Select Criteria" option. Base the Smart Group on an empty tag such as "Empty" that you can create in AirWatch.



This empty Smart Group will be assigned when a device is under a threat, the TRM will determine which Smart Group, if any, to put the device in to for the following Use Cases:

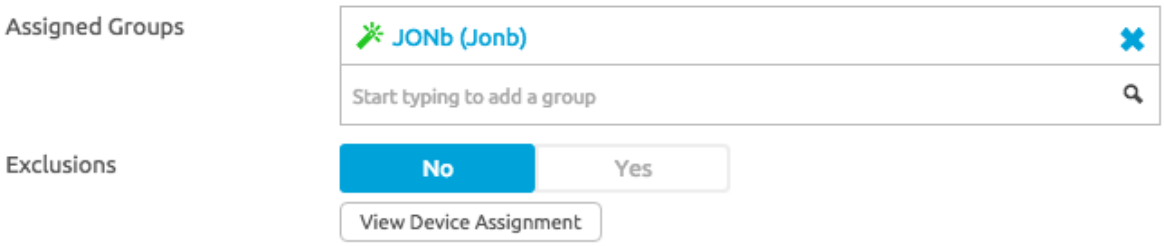
Remove a configuration profile from the device

Profiles in AirWatch can be configured with a set of Exclusion Smart Groups. A Profile will be removed from any devices placed in the Exclusion Smart Group allowing an AirWatch admin to remove Exchange profiles, VPN profiles, Wi-Fi profiles etc…



Add a configuration profile to a device

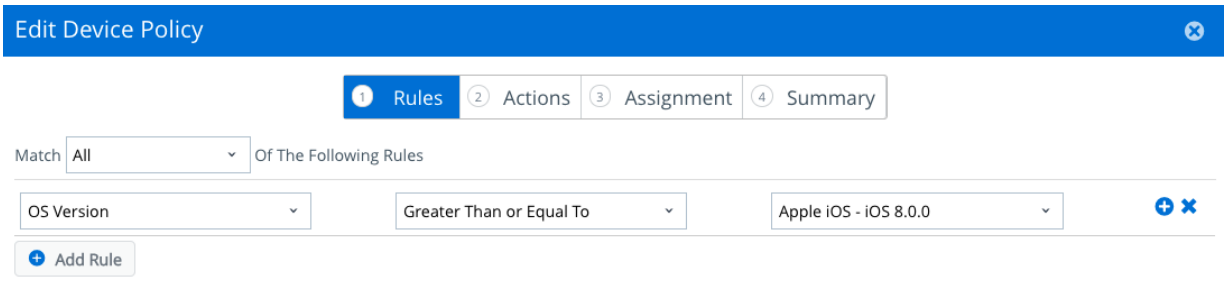
The same holds true for Profiles that you want to add to a device when they are under a threat. An example would be a profile to increase restrictions such as removing access to the camera or to add a specific VPN profile. To enable this, put the empty Smart Group in to the Assigned Groups of the Profile. This profile will then be pushed to any device that shows up in that Smart Group.



Compliance Policy

Compliance policies allow for combinations of actions, such as notify the user via Push or SMS messages and then remove access for such things as Email etc… Through the MVISION Mobile Console Policy page, the admin can assign the device to a Compliance Policy:

Create a compliance policy with a single Rule that will always be true. (The device is greater than or equal to the required minimum OS)

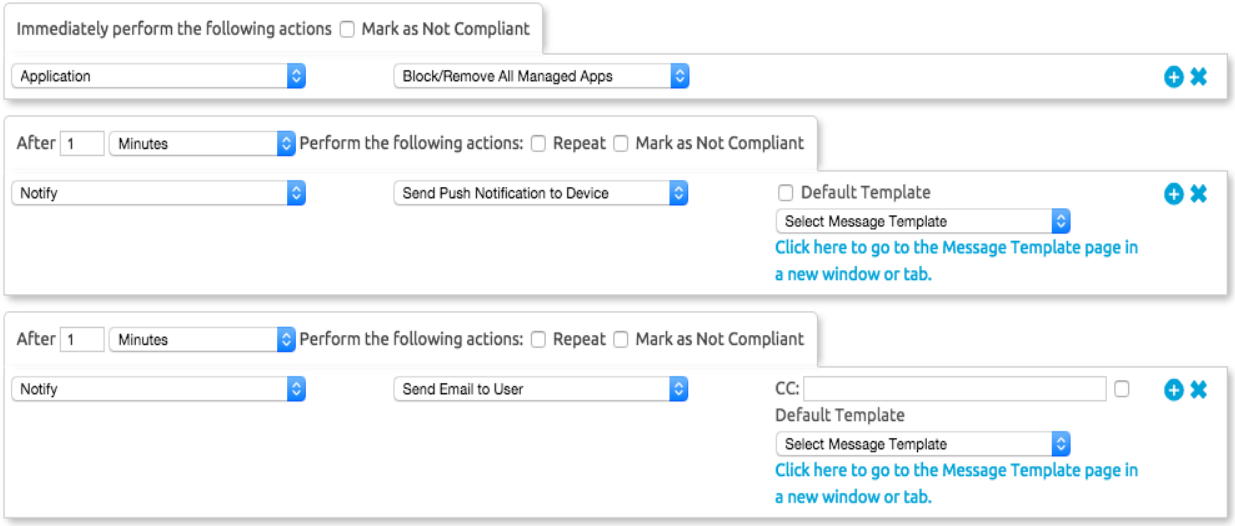


Choose any combination of the following Actions as needed to suite your Use Case. It is good practice to take an action to protect the device or remove access to company data and then to alert the user as required to let them know what is happening:

- Remove a managed application or remove all managed applications.

- Install a Compliance Profile (Used to increase restrictions on the device such as a longer PIN code etc, remove access to the camera etc)
- Remove/Add a configuration profile or profile type. (Profile type could be: Email profile, WiFi etc…)
- Send a series of alerts to the user via (SMS to device, Push notification to device, Email to user). These messages can state any thing you need, for example, tell the user why the device was found to be in risk and why certain company Intellectual Property such as Email will be remove.
- Enterprise wipe the device. (Un-enrolls device and removes only corporate data)
- Assign the blank Smart Group to the compliance policy.

A typical Action in a compliance Policy would look like this:



This Action first removes all managed apps pushed down from the MDM and then alerts the user after one minute via a PUSH message to the AirWatch Agent and then another minute as an Email to the user. This allows the Admin to create message templates that can be used in all different scenarios specific to the threat. So, there would be a compliance policy to remove access to data, perhaps another to unenroll the devices and perhaps yet another one to just to remove access to email.

The actions will be dictated by your individual company security policy and Use Cases.