



McAfee MVISION Mobile

VMware Workspace ONE UEM

Integration Guide

August 2021

## **COPYRIGHT**

Copyright © 2020 McAfee, LLC

## **TRADEMARK ATTRIBUTIONS**

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

Preface.....	5
Audience .....	5
Related Documentation .....	5
Overview.....	5
Prerequisite Requirements .....	5
About MDM and MVISION Mobile Console Communication .....	6
Console Integration Steps.....	7
Workspace ONE UEM Configuration .....	7
Enabling API Service in Workspace ONE UEM .....	7
Creating an API Administrator Role .....	8
Creating a New Administrator User in Workspace ONE .....	9
Identify or Create an Assignment Group Used for Initial Synchronization .....	10
Enabling the Collection of Personal Applications (Optional) .....	10
Setup Synchronization on Workspace ONE UEM .....	10
Adding Workspace ONE UEM MDM in the MVISION Mobile Console .....	10
User and Device Synchronization.....	15
MVISION Mobile Configuration and Deployment.....	15
Application Deployment.....	15
Recommended Method with Public Apps.....	15
Private Apps Are for Certain Use Cases .....	16
iOS Configuration and Activation .....	16
MVISION Mobile Managed Application Configuration .....	16
Zero-Touch Activation for MVISION Mobile iOS .....	18
MVISION Mobile iOS - Auto-Activation VPN Profile .....	23
Additional Configuration for DEP/ Supervised Managed Devices.....	27
Android Configuration and Activation .....	30
Native Android Setup for MVISION Mobile Cloud Infrastructure.....	30
Android Enterprise Configuration.....	31
Android Personal Profile Auto-Activation.....	31

Android Enterprise – MVISION Mobile Silent Install and Activation.....	32
Compliance Configuration and Options .....	35
Smart Groups and MVISION Mobile Console .....	35
Configuring the MDM Actions in MVISION Mobile Console .....	35
Available MDM Actions via Workspace ONE UEM.....	36
Example Device Compliance Policy .....	37
Appendix A – MDM Action Use Cases .....	39
Overview .....	39
Removing a Configuration Profile from the Device .....	39
Add a Configuration Profile to a Device .....	39
Compliance Policy .....	40
Appendix B – User’s Perspective on iOS VPN Activation .....	42

## Preface

This document is an administrator's guide to providing integration with a Workspace ONE UEM Mobile Device Management (MDM).

## Audience

The intended audience for this guide is a MVISION Mobile Console or Workspace ONE UEM administrator looking to integrate Workspace ONE UEM and the MVISION Mobile Console. 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.

## 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 an MDM is not required. However, when an MDM is integrated, the MVISION Mobile Console does the following:

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

McAfee MVISION Mobile detects malicious activity and depending on the platform is able to take actions locally. When MVISION Mobile 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 Workspace ONE UEM via secure API's and is instructed to carry out a defined workflow to take action on the device.

The VMware Workspace ONE UEM Administrator can set up different workflows to handle different situations and threats that the MVISION Mobile Console Administrator can choose through the Policy page. Workspace ONE UEM Smart Groups, Tags and Profiles are used to achieve the workflow to protect the device.

## Prerequisite Requirements

Integration with VMware Workspace ONE UEM requires a connection between the McAfee MVISION Mobile Console and the Workspace ONE UEM API server. This is accomplished via the Internet using SSL on TCP port 443. If using a Workspace ONE UEM SaaS management server, there are no changes that need to occur to allow for this communication. For an

On-Premise Workspace ONE UEM 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
<b>Workspace ONE UEM MDM Enrolled Device</b>	v7.2 and above *
<b>API Administrator Account in Workspace ONE UEM's VMware Workspace ONE UEM console</b>	Proper Role defined in section below
<b>Administrator Account in Workspace ONE UEM's VMware ONE UEM console.</b>	An Administrative account to assign the Role
<b>API REST Key</b>	Provided from Workspace ONE UEM Environment
<b>Privacy Collection Policy</b>	Include Personal Applications

**NOTE:** *Workspace ONE UEM V8.0 through V8.1 Feature Pack 3 do not support MDM Actions*

Create an API key that only McAfee MVISION Mobile uses for communication between the MVISION Mobile Console and Workspace ONE UEM. This provides for separation of traffic from other API communications to the Workspace ONE UEM API server. Workspace ONE UEM monitors the API connection per API key to ensure the connection number does not extend above a threshold. This number might be different for each implementation. By using a unique API key for McAfee MVISION Mobile traffic, the chances of hitting that threshold is reduced. These steps are listed within this document.

### About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the Workspace ONE UEM 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 server. The MVISION Mobile server then reaches out to the proper Workspace ONE UEM API Server and provide the commands to perform the action described.

## Console Integration Steps

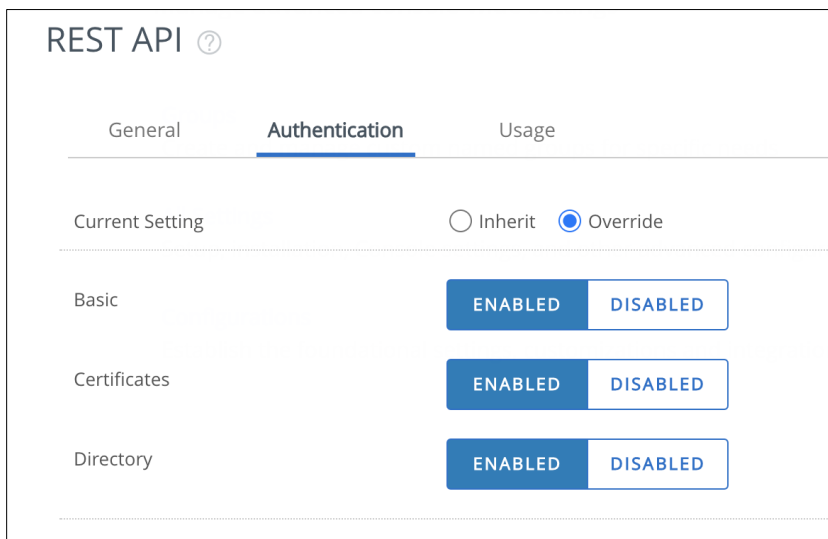
This section covers the configuration steps needed to set up the application with Workspace ONE UEM for a typical application deployment. For zero-touch activation, see the steps in the “[MVISION Mobile iOS Zero-Touch Activation](#)” section.

The steps in the sections below outline how to set up API access for the MVISION Mobile Console in Workspace ONE UEM and how to configure the integration between Workspace ONE UEM and the MVISION Mobile Console.

### Workspace ONE UEM Configuration

#### Enabling API Service in Workspace ONE UEM

1. Log in to Workspace ONE UEM
2. Navigate to this location in the console:  
**Groups & Settings -> All Settings -> System -> Advanced -> API -> REST API**
3. Click the **Authentication** tab and enable certificate-based authentication for API Calls.



The screenshot shows the 'REST API' configuration page in the Workspace ONE UEM console. The 'Authentication' tab is selected, showing three sections: 'Basic', 'Certificates', and 'Directory'. Each section has 'ENABLED' and 'DISABLED' buttons. The 'Current Setting' is set to 'Override'.

Section	Basic	Certificates	Directory
Current Setting	<input type="radio"/> Inherit	<input checked="" type="radio"/> Override	
Basic	ENABLED	DISABLED	
Certificates	ENABLED	DISABLED	
Directory	ENABLED	DISABLED	

4. Going back, under the **General** tab, create an API Key for MVISION Mobile. This is used in the MVISION Mobile Console for the integration.
  - a. Enable API Access if it is not already enabled.
    - i. To create a unique REST API key, click the **+ Add** button.
    - ii. In the new entry that shows up:
      1. Enter the new service name – *MVISIONAPI*
      2. Set the account type to Admin
  - b. Click **Save**.
  - c. Copy the new REST API Key for use in the MVISION Mobile Console.

## Creating an API Administrator Role

Select or create an Administrator account within Workspace ONE UEM console with the proper access by performing these steps:

1. In the Workspace ONE UEM console, select **Global** and then select the customer-level organization group.
2. Navigate to **Accounts**.
3. Select **Administrators**.
4. Click **Roles** and click the **Add Role** button, and this window opens.

Create Role

Name\* MVISION Mobile API Integration

Description\* REST API and Permissions

Categories All Search Resources

Read	Edit	Category	Name	Description
<input type="checkbox"/>	<input type="checkbox"/>			

Please Select A Category Or Enter Search Text To View Resources

SAVE CANCEL

5. Provide the name, for example, 'MVISION Mobile API Integration' and a description.
6. In the Categories section, click **API** and then **REST**.
  - a. Select the following based on the table information.

Read/Edit	Category	Name	Description
Read	API/REST	Devices	REST APIs for device management
Read/Edit	API/REST	Groups	REST APIs for group management
Read/Edit	API/REST	Profiles	REST APIs for device profiles
Read/Edit	API/REST	Users	REST APIs for enrollment user accounts

7. In the **Categories** section, select **Settings** and **Tags**, if this option is available on your installation.
  - a. Select the following based on the table information.



Read/Edit	Category	Name	Description
<b>Read/Edit</b>	Settings/ Tags	Tags	Access all Tag APIs. This option is not available for all Workspace ONE UEM versions.

**Note:** If you modify a device in the MVISION Mobile Console changing tags and do not see the change reflected in the Workspace ONE console, ensure that you set the read and edit permissions for tags in the VMware Workspace ONE console for this role.

## Creating a New Administrator User in Workspace ONE

Follow these steps to create a new administrator user in the Workspace ONE console:

1. Log in to Workspace ONE.
2. Create a Workspace ONE UEM Administrator User with the following additional settings:
  - a. Navigate to **Accounts**.
  - b. Click **Administrators**.
  - c. Select **List View**.
  - d. Select **Add**.
  - e. Click **Add Admin**. For instance, give the name "MVISION API Admin."
3. Give this administrator user the role and permissions that you set up previously.
  - a. Click the **Roles** tab.
  - b. Select one or more Smart Groups intended to contain the managed devices.
  - c. Then select the API Role created above, for example, *MVISION API Role*.
  - d. Apply the role to one or more Smart Groups if necessary.
4. Click the **API** tab. This is to create a certificate to use as the login to the MVISION Mobile Console.
  - a. Enable **Certificates** and create the certificate password. You need the password to the certificate twice in this process, to export the certificate, and to import the certificate into the MVISION Mobile Console.
  - b. Click **Save**.
  - c. After saving the admin account, re-open the account, enter the password created for the certificate, and export.

The screenshot shows the 'Add / Edit Admin' interface with the 'API' tab selected. Under the 'Authentication' section, 'Certificates' is chosen. The form displays the following information:

- Issued by:** CN=AW Admin User Root
- Valid From:** 1/18/2016 11:25:47 AM
- Valid To:** 1/13/2036 11:25:47 AM
- Thumbprint:** 05C2B75711A0441047D766D4644C2B421471B004

Below this information are two buttons: 'Clear Client Certificate' and 'Export Client Certificate'. The 'Export Client Certificate' button is highlighted with an orange border. At the bottom, there is a 'Certificate Password' field with a red asterisk indicating it is required.

## Identify or Create an Assignment Group Used for Initial Synchronization

Syncing between the MVISION Mobile Console and Workspace ONE UEM requires selecting a specific assignment group or multiple assignment groups. It is recommended that a group is identified for the initial sync, or is created with specific devices in it for the initial sync or setup. After the integration is complete, additional groups and devices can be added at any time. The groups are under this location in the Workspace ONE UEM console:

### Groups & Settings > Groups > Assignment Groups

## Enabling the Collection of Personal Applications (Optional)

Enabling Workspace ONE to collect the inventory of personal applications from devices makes them available to the MVISION Mobile Console for later analysis. This is the only way for MVISION Mobile to inventory apps on iOS devices as Apple restricts the collection of application inventories to MDM's only. This is not required for any other detections or functionality with MVISION Mobile and is optional based on the organization's privacy policies. This can be enabled or disabled based on device ownership settings in Workspace ONE UEM.

To enable application collection:

1. Navigate to **Groups & Settings**.
2. Select **All Setting**.
3. Click **Devices & Users**.
4. Select **General**.
5. Select **Privacy**.
6. After getting to the **Privacy** page, scroll down to find the Application heading and ensure all the settings allow for collection. These settings must be enabled for the app to sync with MVISION Mobile Console and for z3A app analysis to occur.



**Note:** For some shared MDM environments, the user may not have permission for this setting.

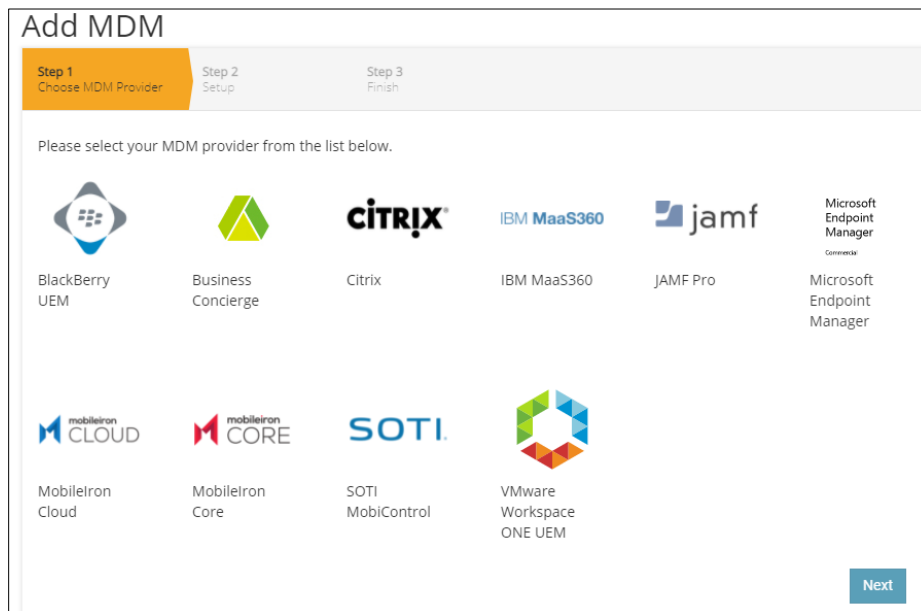
## Setup Synchronization on Workspace ONE UEM

This section describes the setup of the synchronization in the VMware Workspace ONE UEM.

## Adding Workspace ONE UEM MDM in the MVISION Mobile Console

To create the MDM Integration in the console:

1. Log into the MVISION Mobile Console and navigate to **Manage** and select **Integrations** and **MDM**.
2. Click the **Add MDM** button, and a selection of MDM options appears:



3. Select **VMware Workspace ONE UEM**.  
**NOTE:** Be sure to select the correct version of Workspace ONE UEM. Workspace ONE UEM-8.3 supports Workspace ONE 9.x as well.
4. Click **Next**, and a window opens containing fields to input the Workspace ONE API URL, admin account, and name of the UEM system, along with other configuration fields to integrate the two systems.

## Add MDM

Step 1  
Choose MDM Provider

Step 2  
Setup

Step 3  
Finish

URL

Specify URL for this MDM provider.

Choose authentication method

Choose authentication method

☐ Certificate
☒ Username/Password

Username

Specify username for this MDM provider.

Password

Specify password for this MDM provider.

MDM Name

Specify a unique name for this MDM provider.

VMware Workspace ONE UEM

Background Sync

Enable this option if you want the MDM provider to automatically synchronize users, devices, apps, and profiles on a periodic basis.

☐

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 synced from the MDM

Mask Imported User Information

Enable this option to mask personally identifiable information (first name, last name and email) on the zConsole.

☐

API key

Specify API KEY for this MDM provider.

Send Device Activation email via MVISION Console for iOS Devices

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

☐

Send Device Activation email via MVISION Console for Android Devices

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

☐

Next

- Enter the pertinent information for the Workspace ONE UEM integration.  
**NOTE:** In this guide, an MVISION API Admin account is created and an associated certificate. Use this account as the preferred authentication method.

Item	Specifics
<b>URL</b>	URL of the Workspace ONE UEM API Server
<b>Choose Authentication Method</b>	Select either Certificate or Username/Password for the desired method of authentication.
<b>Username</b>	Workspace ONE UEM Administrator created with the API role access
<b>Password</b>	Password of the Workspace ONE UEM Administrator
<b>Certificate</b>	If a Certificate authentication method is chosen then upload your certificate for authorization.
<b>Passphrase</b>	If a Certificate authentication method is chosen then provide your passphrase for the certificate.

<b>MDM Name</b>	The name used in MVISION Mobile Console to reference this MDM integration. This is prepended to the group name to form the MVISION Mobile Console group name.
<b>Background Sync</b>	Click on the checkbox to ensure devices are synchronized with the Workspace ONE UEM Smart Groups chosen on the next page.
<b>Set synced users' password</b>	<p>Click on the checkbox to override the default password during user sync. If this is not checked a default password is computed as follows for all users that are synchronized.</p> <p>Start with the MVISION environment name (this can be supplied by the Customer Success contact), change all uppercase letters to lowercase and also change all spaces to dashes. Then append '1234!' to the end.</p> <p>The <i>MDM Test</i> becomes <i>mdm-test1234!</i>.</p> <p><b>NOTE:</b> This field is only applicable to MVISION Mobile release 4.4 and earlier which has a username and password login.</p>
<b>Synced users' password</b>	<p>Override the value of the password to use for each user when they are synchronized.</p> <p><b>NOTE:</b> This field is only applicable to MVISION Mobile release 4.4 and earlier which has a username and password login.</p>
<b>Mask Imported Users Information</b>	Check this box to mask personally identifiable information about the user when displayed such as name and email address.
<b>API Key</b>	API Key used for secure authentication to the API Server.
<b>Send Device Activation email via MVISION Mobile Console for iOS Devices</b>	Check this box to send an email to the user for every iOS device synced with the MDM.
<b>Send Device Activation email via MVISION Mobile Console for Android Devices</b>	Check this box to send an email to the user for every Android device synced with the MDM.

- Click **Next** and choose the Smart Group(s) to synchronize. The available Smart Groups show 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 Smart 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

Smart Group, the highest or first Smart Group it appears in is the MVISION Mobile Console group for it. To change the order of the listing, drag and drop Smart Groups as required.

The image shows two screenshots from the McAfee MVISION Mobile Console. The top screenshot is the 'Edit MDM' window, which has a progress bar at the top with three steps: 'Step 1 Choose MDM Provider', 'Step 2 Setup AirWatch-8.3', and 'Step 3 Finish' (which is highlighted in orange). Below the progress bar, there are two sections: 'Available MDM Groups' on the left and 'Selected zConsole Groups' on the right. The 'Available MDM Groups' section lists four groups: 'Action1-JB', 'Action2-JB', 'Action3-JB', and 'Chad account', each with a green plus icon to its right. The 'Selected zConsole Groups' section lists two groups: 'JonB Devices' and 'JonB-AFW', each with a red minus icon to its right. Below these sections, there is a note: 'If a user is a member of more than one MDM group, the user will be placed in the zConsole group with the higher priority.' At the bottom left of the window is a 'Finish' button. The bottom screenshot is the 'Manage' window. It has a top navigation bar with tabs: 'General', 'Privacy', 'MDM' (which is selected), 'VPN Settings', 'Network Sinkhole Settings', 'Audit log', 'Roles', and 'Message Templates'. Below the navigation bar, there is a 'Set MDM Link Expiry' section with a dropdown set to '365 Days' and a 'Save' button. The main content area is divided into three sections. The left section is titled 'AW TechP JB MDM is Connected' and shows the AirWatch logo and a URL 'https://techp.awmdm.com/'. The middle section is titled 'Groups' and shows a list of 'Selected zConsole Groups': 'JonB KNOX Devices', 'JonB Devices', 'JonB Public Store', and 'JonB-AFW'. The right section is titled 'Activation Link for Managed Devices' and shows a URL 'https://demo-device-api.zimperium.com/activation?token=...' and a 'Link Expires : 10/02/2019'. At the bottom of the 'Manage' window, there are buttons for 'Edit', 'Sync Now', and 'Remove'.

8. Once the integration is complete, click **Sync Now** to start the user/device synchronization.
9. Once the synchronization is completed, click **Save**. This is verified over time by going to the '**Devices**' or '**Users**' pages in the MVISION Mobile Console to verify the devices are shown. The device entries are greyed out until the user starts up MVISION Mobile and activates it.

At this point, the application is published and installed on the devices in the Smart Group assigned. The users can now activate the application as described in the platform guides in the 'Support Portal'. Users need an activation URL generated in the MVISION Mobile Console or a QR code to access the application.

## User and Device Synchronization

After the initial synchronization during the MDM integration setup process, a scheduled synchronization process runs on a set interval that is configured based on the VPC in use. This synchronization adds new device records for devices that have not already enrolled in MVISION Mobile using auto login methods, and new users. For users, only the email address and the first and last name are synced.

- **New Enrollments:** If the additional users or devices join any Groups that are being used for synchronization, they are added along with their devices to MVISION Mobile Console.
- **Unenrolled Devices or Users:** If we see users or devices removed or devices marked as unenrolled, then they are removed from the MVISION Mobile Console. Doing this does not remove any of the events associated with that user or device.

The MVISION Mobile Console does provide for on-demand synchronization under the newly added MDM.

## MVISION Mobile Configuration and Deployment

### Application Deployment

There are public and private application deployments. These sections detail these options.

Both types of apps can be configured to use auto-login methods for iOS and Android for Enterprise devices. It is recommended to use autoactivation when and where possible.

### Recommended Method with Public Apps

To deploy the MVISION Mobile application through Workspace ONE UEM, access the iOS version from the App Store and the Android version from the Google Play Store.

Create a new public application and search the appropriate store for McAfee MVISION Mobile. Or use these links:

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

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

For Workspace ONE UEM, the Google Play Store MVISION Mobile link can be used with a referrer attribute for MVISION Mobile activation. Refer to *“Appendix D - Google Play Store*

*MVISION Mobile Link with Referrer Attribute" in the "McAfee MVISION Mobile Console Product Guide" for more information.*

**Note:** *The Google Play Store referrer attribute functionality is supported for Android OS version 9 or earlier. This functionality also requires the Google Play Store app Release 8.3.73 or later.*

### Private Apps Are for Certain Use Cases

To deploy as an internal app, log in to Workspace ONE UEM and navigate to the Organization Group where the application should be installed. If no appropriate Smart Group exists for the application deployment, create that also. Create a new Internal Application and upload the proper application file (IPA for iOS and APK for Android) to Workspace ONE UEM. Assign the Smart Group to the application and publish.

Please refer to the Workspace ONE UEM guide on the process to add the McAfee MVISION Mobile public app from the App Store and Google Play store. The MVISION Mobile application in both iOS and Android Enterprise can auto-activate. The process is different on each platform as described below.

To obtain the .ipk or .apk file of MVISION Mobile, contact your McAfee Customer Service team.

### iOS Configuration and 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 start up MVISION Mobile iOS without having to enter any credentials. There are several options for iOS activation. This section describes these options and see which activation option best suits your needs:

- Zero-Touch Activation
- Auto-Activation VPN

### MVISION Mobile Managed Application Configuration

The Managed Application Configuration pre-programs MVISION Mobile iOS with the required information.

The managed app configuration is done within Workspace ONE UEM. During the addition of the MVISION Mobile application, when you are assigning the Smart Group, there is an option to define the Application Configuration.

Perform these steps:

1. On this page, click **Send Application Configuration**.



Send Application Configuration ☒

Application Configuration

Configuration Key	Value Type	Configuration Value
<input type="text"/>	String	<input type="text"/>

- Use the following configuration keys and values as needed for the configuration:

**Note:** If the enrollment URL method of activation for MVISION Mobile is not being used, the PLIST configuration values can be used. For more information on the activation URL, see the “McAfee MVISION Mobile Console Product Guide.”

Configuration Key	Value Type	Configuration Value	Notes
MDMDeviceID	String	{DeviceUid}	Required
tenantid	String	Copy the value from the <b>Tenant ID</b> field on the MVISION Mobile Console <b>Manage</b> page under the <b>General</b> tab.	Required
defaultchannel	String	Copy the value from the <b>Default Channel</b> field on the MVISION Mobile Console <b>Manage</b> page under the <b>General</b> tab.	Required
tracking_id_1	String	(Optional) Use the desired identifier.	(Optional) Use the desired identifier.
tracking_id_2	String	(Optional) Use the desired identifier.	(Optional) Use the desired identifier.
display_eula	String	no	(Optional) If you do not use this key, the default display the End User License Agreement (EULA).

**Note:** The configuration keys are case sensitive if an XML configuration is used.

- Click **Publish and Save** to push this to devices in the Smart Group.

**Workaround:** If there are optional keys in the key list and the fields do not populate, such as tracking identifier fields, an error that this value is required can be received. To remove unneeded configuration values from the list of Key-Value pairs, try to remove the entries. If they cannot be removed, ensure they have no value in the field.

## Zero-Touch Activation for MVISION Mobile iOS

This feature allows an administrator to activate MTD protection on managed devices without the end-user being required to click on the installed MVISION Mobile application.

### Overview of the Setup

This describes the items that are set up for zero-touch activation and threat reporting:

- The VMware Workspace ONE UEM has an assignment group and a VPN Profile (zVPN) for the devices.
  - The device is registered with the MDM.
  - The MVISION Mobile app is pushed to the device.
  - The zVPN Profile is initially pushed to the device.
- MVISION Mobile Console has the MDM defined as an integration.
- MVISION Mobile Console has the MDM Action and Mitigation Action set for the “App Pending Activation” threat.

### A Sample Flow after the Configuration is Complete

These steps describe a sample flow once Zero-Touch Activation is configured:

1. The MVISION Mobile Console **Policy** page has the “App Pending Activation” threat with an **MDM Action** to put the device into the smart group that is associated with the VPN profile, and this installs the VPN profile. The **Mitigate Action** field is set to Remove, and once MVISION Mobile is activated the zVPN profile is removed from the device.
2. The MDM pushes the MVISION Mobile app and the zVPN Profile to the device.
3. There is a “Launch MVISION Mobile” notification on the device from the zVPN Profile, but the end-user does not activate MVISION Mobile yet.
4. A threat is generated on the device, such as a “Device Pin” threat.
5. The zVPN Profile shows a notification of the threat on the device, and MVISION Mobile is still not launched.
6. The threat is visible in the MVISION Mobile Console **Threat Log** page and:
  - The **App Name** shows “zVPN Extension.”
  - The **Detection Status** shows “Active” for the device.
  - The **App Status** shows “Pending Activation” for the device.

**Note:** This threat is logged after the dormancy period that is set for **Allowed Inactivity Time** on the **Manage** page of the MVISION Mobile Console.
7. The user launches MVISION Mobile and activates MVISION Mobile.
  - The **Detection Status** shows “Active” for the device.
  - The **App Status** shows “Active” for the device.

## Differences in Zero-Touch Activation

For information on the differences in zero-touch activation compared to a standard MVISION Mobile activation, see the “McAfee MVISION Mobile Console Product Guide” document on the support portal.

## Setting Up Zero-Touch Activation

This set of instructions describes setting up zero-touch MVISION Mobile activation and the workflow. This option provides threats being detected without the activation of MVISION Mobile on the end user’s device, where MVISION Mobile is pushed from the MDM. The user is prompted to open MVISION Mobile, but it is not a required action. A VPN profile runs on the device until the user activates the MVISION Mobile app.

**Important:** *Contact a member of the Customer Success team before performing these steps to get the defaultchannel and tenantid values for your tenant and this configuration. These values are not the same as in similar configurations. The tenantid used is not the value displayed in the MVISION Mobile Console.*

To configure zero-touch activation, perform these steps:

1. Log in to the VMware Workspace ONE console.
2. Navigate to this location and add a new smart group, for instance, named “zVPNProfile.”

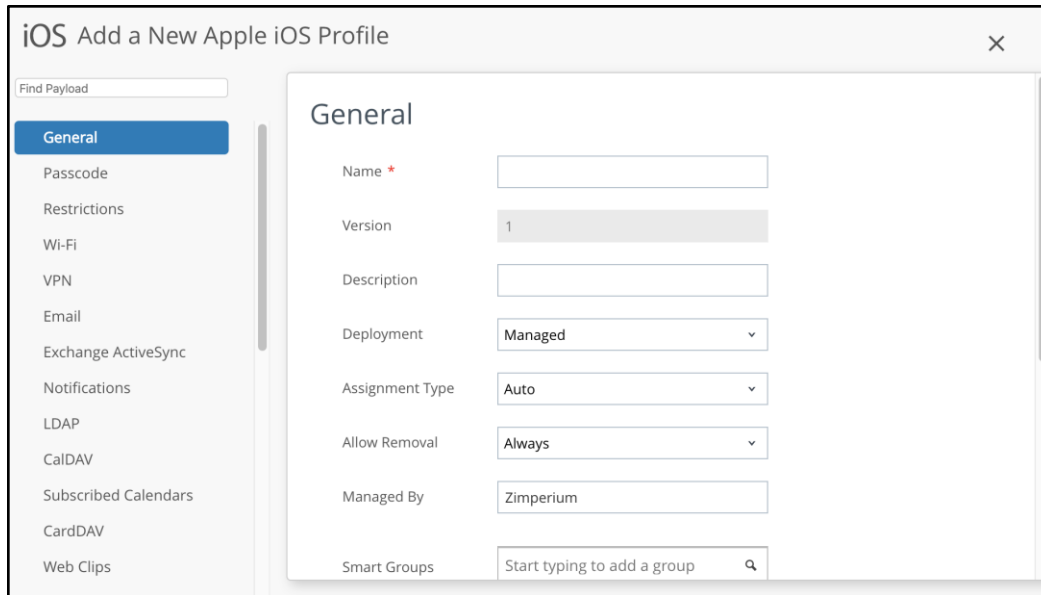
**Groups & Settings > Groups > Assignment Groups**

**Note:** *Ensure that the smart group associated with the VPN Profile and the Device Group are not the same.*

3. On the left navigation menu, navigate to this location and add a new profile.

**Resources > Profiles and Baselines > Profiles**

4. Click **Add** and the **Add Profile** window opens.
5. Select the **Apple iOS** platform, and then select **Device Profile** as in the figure.



6. On the **General** screen, enter these fields:
  - a. Name of the Profile.
  - b. Description.
  - c. The **Deployment**, **Assignment Type**, **Allow Removal**, and **Manage By** fields can be left as the default settings.
  - d. Assign the profile to the smart group created in Step 2.
  - e. The rest of the fields can be left as the default setting.

**Warning:** Do not save and publish these settings until the VPN is set up in the following steps.
7. In the navigation panel, select **VPN** and select **Configure** in the VPN window, and enter these fields:
  - a. Enter the **Connection Name**.
  - b. For the **Connection Type** field select **Custom**.
  - c. For the **Identifier** field:
    - i. Enter **com.mcafee.mvision.mobile.appstore** if you are using the App Store version of MVISION Mobile.
    - ii. Enter **com.mcafee.mvision.mobile** if you are referencing the MDM MVISION Mobile version.
  - d. For the **Server** field, enter **local**. Since MVISION Mobile uses a local VPN configuration, the server hostname/IP address value entered is not used, so any value can be entered here.
  - e. The **Account** field is not used and may be left blank.
  - f. In the **Custom Data** field, enter these values and ensure the keys are exact matches as they are case sensitive:

- i. **Key:** defaultchannel - Set the defaultchannel to the JSON endpoint value. You get this from the **Manage** page and **General** tab in the MVISION Mobile Console, and you must add “/json” string to the end. For instance:

`https://acceptor.mcafee-mvision-mobile.com/srx/json`

- ii. **Key:** tenantid - Set the tenantid according to the value that you get from the Customer Success team member for your tenant.  
**Note:** This tenantid value is not the value displayed on the **Manage** page of the MVISION Mobile Console and must be obtained from the Customer Success team.

- iii. **Key:** MDMDDeviceID: {DeviceUid}

- iv. **Key:** enable\_auth\_notification: true

The values are true or false. This controls the display of the local notification message requesting the user to launch the MVISION Mobile app.

- v. **Key:** auth\_custom\_notification\_title

Set the value to “Launch MVISION Mobile” The notification title can be changed to a custom title if desired.

- vi. **Key:** runlevel: Production

This indicates the running level for the detection and the values are “QA”, “Beta”, and “Production” and you set it to the default of Production.

- vii. **Key:** auth\_custom\_html\_base64 (Optional)

The administrator can set a custom HTML page to show up when an HTTP site is visited. It needs to be Base64-encoded before entering it in this field.

- viii. **Key:** auth\_redirect\_url: This is the redirect URL that is used to launch the app on the iOS device. The redirect URL value to use with the McAfee MVISION Mobile app is:

`mvisionmobile://login`

- g. For the **User Authentication** field, select **Certificate**.
- h. Select the **Identity Certificate** field as **None**.
- i. Enable the **Enable VPN On Demand** checkbox.

- j. Enable the **Use new on-demand keys** checkbox. Under the **On-Demand Rule** section, choose the action to **Connect**.
  - k. Under the **Criteria** section, ensure the **Interface Match** field is **Any**.
8. Under the VPN settings, consider the sample values in the figure below.

The screenshot displays the VPN configuration page with the following sections and values:

- Connection Info**
  - Connection Name: zVPN\_ZipsActivation
  - Connection Type: Custom
  - Identifier: com.zimperium.zIPS
  - Server: local
  - Account: (empty)
  - Disconnect on idle (sec): (empty)
- Custom Data**

Key	Value
defaultchannel	https://nplus1-accep
tenantid	F0046BA2-3EAB-4A4
MDMDeviceID	{DeviceUid}
enable_auth_notifi	true
auth_custom_notif	Launch zIPS
auth_custom_html	Activate Now
runlevel	Beta
- Per-App VPN Rules**
  - Per-App VPN Rules: ☐
  - Safari Domains: (empty)
- Authentication**
  - User Authentication: Certificate
  - Identity Certificate: None
  - Enable VPN On Demand: ☒
  - Use new on-demand keys: ☒
- On-Demand Rule**
  - Action: ☒ Evaluate Connection ☒ Connect ☐ Disconnect ☐ Ignore
  - Criteria: Value
  - Interface Match: Any

9. Click **Save** and **Publish**.
10. Ensure your profile is associated with the smart group you created in the initial steps.

To finish the configuration for zero-touch activation, perform these steps:

1. Log in to the MVISION Mobile Console.
2. Navigate to the **Manage** page and the **Integrations** tab, and add the VMware Workspace ONE MDM. See the [“Setting Up Synchronization on Workspace ONE UEM”](#) section for more information.

**Note:** This second step must be completed before continuing with the next steps.

3. Navigate to threat policies on the **Policy** page and the **Threat Policy** tab.
4. Select the group from the **Selected Group** field.
5. Update the **App Pending Activation** threat with **MDM Action** and **Mitigation Action** field values.

**Note:** Make sure you have the **Selected Group** drop-down list set correctly. This list is at the top of the page. MDM actions are not supported on the **Default Group** drop-down selection.

- a. Set the **MDM Action** to be the smart group you defined above “zVPNProfile” that is associated with the VPN profile.
  - b. Set the **Mitigation Action** to be **Remove**, to remove the VPN profile after the MVISION Mobile app activation.
6. **Save and Deploy** your changes.

The result is the Zero-Touch VPN is pushed to the device and begins reporting threats. The **Detection Status** for the device changes from “Pending Activation” to “Active.”

You are now set up for zero-touch activation with MVISION Mobile, the UEM, and MVISION Mobile Console.

### MSIVISION Mobile iOS - Auto-Activation VPN Profile

This setup option is different from the zero-touch activation. This option enforces activation of MVISION Mobile on the end user’s device, where MVISION Mobile was pushed from the MDM but has not been activated yet.

Using a local VPN profile pushed by UEM, Users are shown a popup notification on the device, and also a customizable web page any time they visit an HTTP URL that directs them to open the MVISION Mobile app. This is done by silently pushing a local on-device VPN to the devices which remain active only until MVISION Mobile is activated. After MVISION Mobile activation, traffic browsing resumes as normal, the VPN is automatically uninstalled from the device.

**Warning:** This feature applies to iOS 13 and above devices and should not be used with iOS versions less than iOS 13 due to a VPN related issue on the earlier iOS version. The MDM should be configured to enable this feature on devices using iOS 13 and above.

1. Navigate to **Groups & Settings, All Settings, Settings, Device & Users, Advanced**, then select **Tags** and create a new Tag, called ‘MSIVISION Auto Activation’ as the identifier.
2. Create an assignment group called ‘MSIVISION Auto Activation’ that targets devices with the ‘MSIVISION Auto Activation’ tag.

- a. Create the assignment group and under the **Criteria** and **Tags** section, add the MVISION Auto Activation Tag, and click **Save**.

**Edit Smart Group**

Name: Pending Activation  
Managed By: MikelID

Choose Type: **CRITERIA** | DEVICES OR USERS

Device Preview: **ENABLED** | DISABLED

Organization Group: All

User Group: Any

Ownership: Any

Tags: 1 Selected

☒ PendingActivation-demo - MikelDemo

Enter Tag name:  **ADD**

Platform and Operating System: 1 Selected

OEM & Model: Any

Model (Legacy): Any

Enterprise OEM Version: Any

Management Type: Any

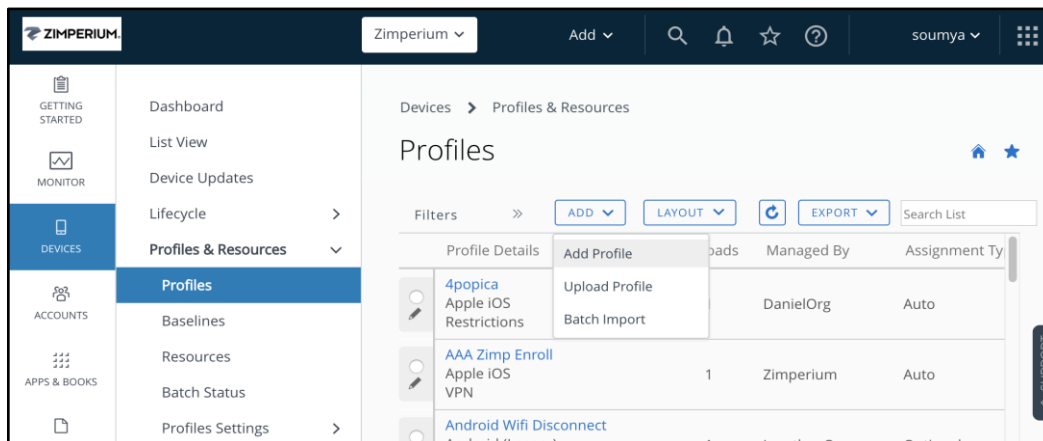
Enrollment Category: Any

Additions: None

Exclusions: None

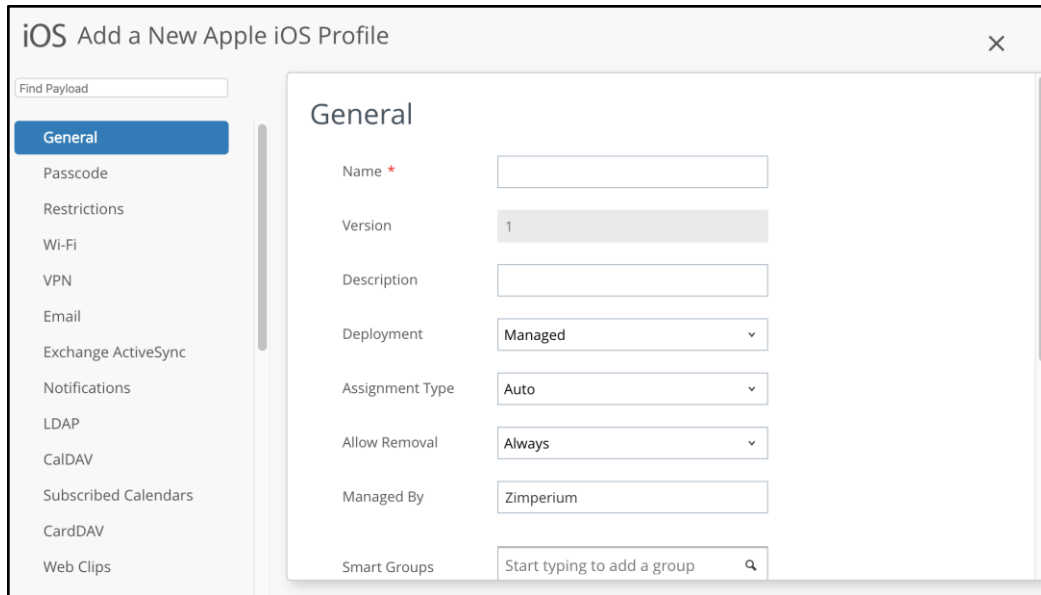
**CANCEL** **NEXT**

3. Next, navigate to **Devices** and select **Profiles & Resources**. Then select **Profiles**, and select **Add** from the drop-down menu.



4. The **Add Profile** window opens. Select the **Apple iOS** platform, and then select **Device Profile** as in the figure.





5. On the **General** screen, enter these fields:
  - a. Name of the Profile.
  - b. Description.
  - c. The **Deployment**, **Assignment Type**, **Allow Removal**, and **Manage By** fields can be left as the default settings.
  - d. Assign the profile to the 'MVISION Pending Activation' group created in Step 2. Once MVISION is activated they are automatically removed from this group.
  - e. The rest of the fields can be left as the default setting.

**Warning:** Do not save and publish these settings until the VPN is set up in the following steps.

6. In the navigation panel, select **VPN** and select **Configure** in the VPN window, and enter these fields:
  - a. Enter the Connection Name.
  - b. For Connection Type select **Custom**.
  - c. For the identifier, enter **com.mcafee.mvision.mobile.appstore** (if you are using the App Store version of MVISION Mobile).
  - d. For the **Server** field, enter **local**. Since MVISION Mobile uses a local VPN configuration, the server hostname/IP address value entered is not used, so any value can be entered here.
  - e. The **Account** field is not used and may be left blank.
  - f. In the **Custom Data** field, enter the following:
    - i. **Key:** enable\_auth\_redirect value: true

The values are true or false. This controls redirecting HTTP URLs to a customized web page requesting the user to launch the MVISION Mobile app.

- ii. **Key:** enable\_auth\_notification value: true

The values are true or false. This controls the display of the local notification message requesting the user to launch the MVISION Mobile app.

- iii. **Key:** auth\_custom\_notification\_title (Optional)

The default value is "Open app to activate." The default notification title can be changed to a custom title.

- iv. **Key:** auth\_custom\_notification\_message (Optional)

The default value is "Open the app to activate mobile threat defense on the device." The default notification message can be changed to a custom message if desired.

- v. **Key:** auth\_custom\_html\_base64 (Optional)

The administrator can set a custom HTML page to show up when an HTTP site is visited. It needs to be Base64-encoded before entering it in this field.

- vi. **Key:** auth\_redirect\_url: This is the redirect URL that is used to launch the app on the iOS device. The redirect URL value to use with the McAfee MVISION Mobile app is:

mvisionmobile://login

- g. For User Authentication select Certificate, Identity Certificate as None, and ensure **Enable VPN On Demand** is checked.

- h. Click the checkbox for Use new on-demand keys. Under On-Demand Rule, choose the action to Connect when the interface matches any value.

7. In the navigation panel, click **General**.

8. Click **Save** and **Publish**.

9. In the MVISION Mobile Console click the **Policy** menu item and click the **Threat Policy** tab.

10. Select the UEM Group you wish to enforce this compliance.

11. For the threat 'Device Pending Action' set these items:

- a. Set the **MDM Action** to 'MVISION Pending Action Group' created in step 2. This assigns the profile to devices that are pending activation. Devices are automatically marked as pending activation 24 hours after their first MDM sync to the MVISION Mobile Console.

- b. Set the **Mitigation Action** to **Remove**.

This removes the VPN profile once MVISION Mobile is activated.

### Additional Configuration for DEP/ Supervised Managed Devices

For DEP Managed devices, additional configurations are available to automate the deployment and activation of MVISION Mobile. In addition to the auto-activation VPN profile process, MVISION Mobile should be deployed automatically as a VPP application to ensure no further interaction is required to install MVISION Mobile on the device.

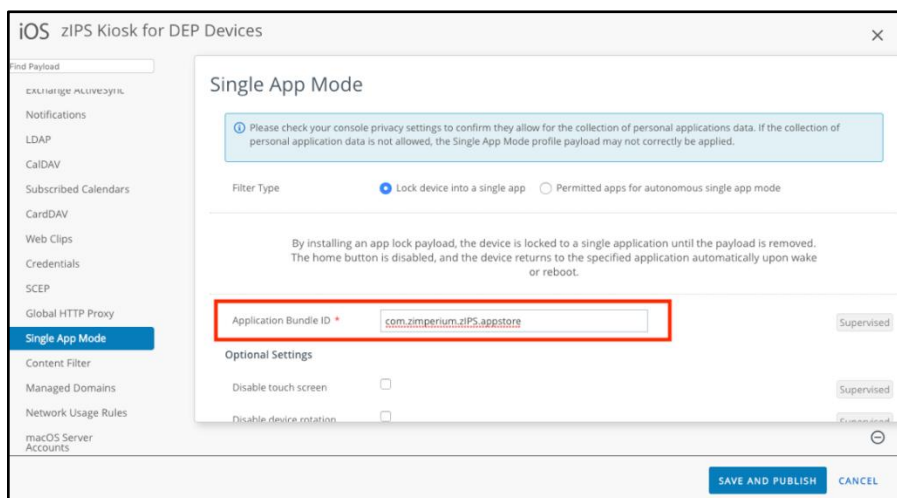
**Recommendation:** Use a combination of compliance policies and profiles to have MVISION Mobile placed in Kiosk mode, temporarily to activate MVISION Mobile, or to leverage the MVISION Mobile Auto Activation VPN Profile.

**Note:** Please see MVISION Mobile Auto-Activation VPN Profile for Tag and Smart Group setup. The following steps assume that MVISION Mobile was added and deployed as an app in Workspace ONE, has a pending MVISION Mobile activation Tag, and a Smart Group was created and assigned to the auto-activation VPN profile. Furthermore, the settings in the MVISION Mobile Console policy for Device Pending Activation and the mitigation actions are set

1. In Workspace ONE, select **Devices**.
2. Select **Profiles and Resources**.
3. Select **Profiles** and add an iOS profile.
4. In the **General** tab, enter the name of the Profile in the **Name** field, for example, **MVISION Mobile Single App Mode – Compliance**.
5. In the **Assignment Type** field, select **Compliance**, and see the figure.

The screenshot shows the configuration window for an iOS profile titled "iOS zIPS Kiosk for DEP Devices". The "General" tab is active. The "Assignment Type" dropdown is set to "Compliance" and is highlighted with a red rectangular box. Other visible fields include "Name" (zIPS Kiosk for DEP Devices), "Version" (2), "Description" (empty), "Deployment" (Managed), "Allow Removal" (Never), "Managed By" (KernOrg), and "Additional Assignment Criteria" (unchecked checkbox for "Install only on devices inside selected areas"). The "SAVE AND PUBLISH" button is at the bottom right.

6. In the navigation panel, select **Single App Mode**, and the window in the figure opens.

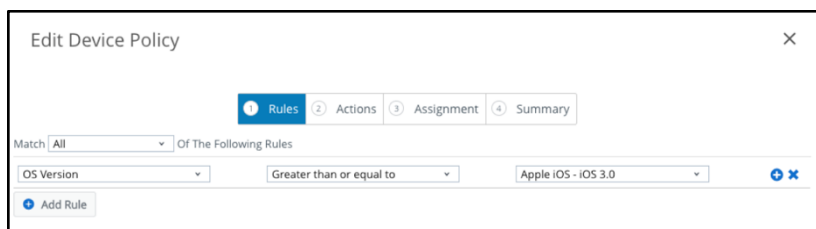


7. For the **Filter Type** field, click the **Lock device into a single app** button.
8. In the **Application Bundle ID** field, enter **com.mcafee.mvision.mobile.appstore** to add MVISION Mobile to the application bundle ID for the public app store version of MVISION Mobile.
9. Click the **Save and Publish** button.

The next step is to create the conditions, which occur when a device with the single app mode policy is assigned with built-in time delays and user notifications.

Perform these steps:

1. In the navigation panel, select **Devices**.
2. Select **Compliance Policies**.
3. Select **List View** to add a new compliance policy.
4. Click **Edit Device Policy** and the following window opens:



5. Click the **Rules** tab.

6. Select the OS Version from the drop-down menu, which must be greater than or equal to Apple iOS 3.0.
7. Click the **Actions** tab, and this window opens.

The screenshot shows the 'Edit Device Policy' window with the 'Actions' tab selected. It displays three action configurations. The third action, 'Install Compliance Profile', is highlighted with a red box. It is set to trigger 'After 7 Days' and perform the action 'Install Compliance Profile' with the profile 'zIPS Kiosk for DEP Devices'.

8. In the **Actions** window, add the desired escalation actions and timeframes, such as notifying the user via email or push message to activate MVISION Mobile on the device.
9. The last action is to install the MVISION Mobile Kiosk mode profile on the device, as marked on the screenshot above.
10. Click the **Assignments** tab, and this window in the figure opens.

The screenshot shows the 'Edit Device Policy' window with the 'Assignment' tab selected. The 'Managed By' field is set to 'KernOrg'. The 'Smart Groups' section is highlighted with a red box, showing a group named 'zIPS Pending Activation (KernOrg)'.

11. In the **Smart Groups** field, add or create the **Pending Activation** Smart Group. This is outlined in the "[MVISION Mobile iOS - Auto-Activation VPN Profile](#)" section.
12. Click the **Summary** tab.
13. In the **Summary** section, rename the policy for the OS version to an appropriate naming convention for the MVISION Mobile Pending Activation single app.

**Note:** *This configuration senses repeated notification to the user if MVISION Mobile is pending activation and at the end of the escalation period MVISION Mobile is locked into the single app mode on the device to ensure it is activated. At this point, MVISION Mobile is registered as "activated", the tag is removed from the device, the compliance policy and single app mode profile are removed from the device, and the user is allowed to exit MVISION Mobile and use the device in a normal operating mode.*

## Android Configuration and Activation

When using Android, there are three set-up options:

- Native Android Setup
- Android Enterprise using PLIST
- Android Enterprise Intent Launch

**Workaround:** *If the following is shown on an Android device, be sure to do a manual sync to get the updated values pushed to the device.*

- *A device that is already registered and the device is configured.*
- *Change the configuration.*

### Native Android Setup for MVISION Mobile Cloud Infrastructure

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 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, use the MVISION Mobile Console **Manage** page and select the **Integrations** tab and 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. MVISION Mobile Console displays the expiration date and time, and if needed, the link can be regenerated.

See the "[McAfee MVISION Mobile Console Product Guide](#)" 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.

## Android Enterprise Configuration

Android Enterprise users can continue to use the managed app config for activations. Make sure the right device ID value is passed for the configuration parameter. The variables are the same set as the variables in the [“iOS Configuration and Activation”](#) section.

For the application configuration setup, under **Apps and Books** and select **Application** and select **Native** then select **Public**, pick a SmartGroup, and click **Add Assignment**. Then scroll down and request that the application configuration is enabled.

The configuration values are described in this table.

Configuration Key	Value Type	Configuration Value	Notes
MDMDeviceID	String	{DeviceUid}	Required
UUID	String	{DeviceUid}	Optional
tenantid	String	Copy the value from the <b>Tenant ID</b> field on the MVISION Mobile Console <b>Manage</b> page under the <b>General</b> tab.	Required
defaultchannel	String	Copy the value from the <b>Default Channel</b> field on the MVISION Mobile Console <b>Manage</b> page under the <b>General</b> tab.	Required
tracking_id_1	String	(Optional) Use the desired identifier.	(Optional) Use the desired identifier.
tracking_id_2	String	(Optional) Use the desired identifier.	(Optional) Use the desired identifier.
display_eula	String	no	(Optional)  If you do not use this key, the default display the End User License Agreement (EULA).

## Android Personal Profile Auto-Activation

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 the users 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.

## Android Enterprise – MVISION Mobile Silent Install and Activation

Workspace ONE UEM has the ability to start or activate an app that is on the device through Android Enterprise and Provisioning. MVISION Mobile has the ability for the Android MVISION Mobile app to start up in either foreground or background mode.

One requirement is the Android Enterprise deployment has to use Device Owner (DO) mode. Currently, the Corporate Owned Personally Enabled (COPE) mode is not supported by Workspace ONE UEM with Provisioning. Essentially, this is a single work profile on the device with no provisions for a personal profile.

### App Setup on the Workspace ONE UEM Console

To set up the app on the Workspace ONE UEM console, perform these steps:

1. Add the public Android MVISION Mobile app to Workspace ONE UEM.
2. Add the App Config parameters described in the "[Android Enterprise Configuration](#)" section of this document.
3. When assigning the app, set it up to be auto deployed by navigating to **Apps & Books** and select **Native** then click **Public**.
4. Locate and click the **MSIVISION Mobile Android** app configured in the environment.
5. Click **Assign** and find the appropriate Smart Group.
6. Modify it and ensure that the entry for App Delivery Method is set to 'AUTO' and click **Add**.
7. Select **Save and Publish** and then select **Publish**.

### Provisioning Setup on the Workspace ONE UEM Console

To provision the auto-start feature on the Workspace ONE UEM Console, perform the following steps:

1. Navigate to **Devices** and select **Provisioning**.
2. Click **Components** and select **Files/Actions**.



3. Click **Add Files/Actions** and choose **Android**.
4. Fill in the General Information. Enter a name and description.
5. Click the **Manifest** tab.
6. Under **Install Manifest**, click **Add Action** and select **Run Intent**.

This figure displays the resulting screen.

The screenshot shows a dialog box titled "Add Manifest". It has three input fields:

- Action(s) To Perform \***: A dropdown menu with "Run Intent" selected.
- Command Line and Arguments to run \***: An empty text input field.
- TimeOut (-1 for infinite) \***: A text input field containing the value "0", with an information icon (i) to its right.

7. Enter one of the options below for the Command Line information:
  - a. Start MVISION Mobile in the Foreground. In this option the user sees it start.

`mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mcafee.mvision.mobile,class=com.mcafee.mvision.mobile.ZipsActivity`

- b. Start MVISION Mobile in the Background. In this option the user does not see it start.

`mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.mcafee.mvision.mobile,class=com.mcafee.mvision.mobile.ui.DormancyStartActivity`

8. Select '-1' for the Timeout value and click **Save**.
9. Click **Save** again and this action shows up in the list.
10. Navigate to **Devices** and select **Provisioning**.
11. Click **Product List View** and select **Add Product**.
12. Select **Android** and provide a name value. For example, enter 'MVISION Mobile' as a name value.
13. Select the same associated Smart Groups.
14. Click **Manifest** and then select **Add**.
15. Select **Install Files/Actions**.
16. In the **Files/Actions** entry box, select the action created above and click **Save**.
17. Click **Activate** and then click **Save**.
18. The Product List View displays the current status of the device with MVISION Mobile Actions.

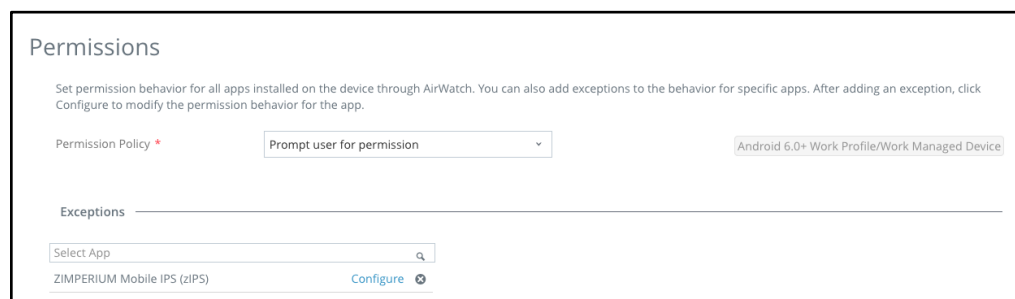
## Setting Up a Silent Install

Setting up a silent installation is optional. When the MVISION Mobile app is initially started up, there are several permission questions that Android enforces to provide access to storage, location, and other capabilities.

For a silent install, answer these questions ahead of time using profiles through the Workspace ONE UEM Console and perform the following steps:

1. Navigate to **Devices** and select **Profiles and Resources** then click **Profiles**.
2. Click **Add**, then click **Add Profile** and choose **Android**.
3. Fill in the General information and select the Smart Groups associated with the desired devices for protection.
4. On the left column, select **Permissions** and then click **Configure**.
5. For the **Permission Policy** option, choose **Prompt user for permission**.
6. Select the **MVISION Mobile** app under **Exceptions**.

This figure displays the Permission Policy selection and the selected app.



7. Click **Configure** to select the answers to use for the installed questions.
8. Choose **Grant** for all the questions that are set to pre-answer.  
**Note:** Typically, choose 'Grant' for all options. Any other choice can prompt the user in the app for a response and can be adjusted as needed.
9. Click **Save** and then click **Publish**.

## Deployment

### Device Has MVISION Mobile Already Installed

Perform the following steps when MVISION Mobile is already installed on the device:

1. Navigate to **Devices** and select **Provisioning** and then click **Product List View**.
2. The product previously created is displayed.

3. Click the radio button by the product and navigate to **More Actions**.
  4. Select **Force Reprocess** and **OK**.
- Note:** This action does not impact any devices where MVISION Mobile is already running.

### New Workspace ONE UEM Enrollment for Device

Perform these steps when MVISION Mobile is new to Workspace ONE UEM:

1. The optional profile and provisioning automatically deploys to the device.
2. The MVISION Mobile app install can be delayed due to MDM scheduling and not be installed prior to the provisioning.
3. If this occurs, perform the steps in the section [“Device Has MVISION Mobile Already Installed.”](#)

## Compliance Configuration and Options

### Smart Groups and MVISION Mobile Console

The MVISION Mobile integration with Workspace ONE UEM provides the ability to put the device in a specific Smart Group within the customer Workspace ONE UEM environment. This allows the Workspace ONE UEM administrator to define specific actions that are enacted automatically such as to remove an application, remove email access, remove or assign a profile, or even unenroll a device. To accomplish this, the Workspace ONE UEM administrator needs to coordinate with the MVISION Mobile Console administrator what specific actions are needed. MDM Integration with MVISION Mobile Console also has to be set up and functional.

Once a Smart Group is defined, the Administrator can reference that Smart Group in the pull-down list under the **MDM Action** column on the **Policy** page. In this case, when a Device Pending Activation threat occurs, the device is placed into the ‘Pending Activation’ Smart Group and the appropriate Exclusion Profile or Compliance Policy is applied.

<input type="checkbox"/>	Critical	Device Jailbroken/Rooted	<input checked="" type="checkbox"/>			Select an Option	Select an Option		
<input checked="" type="checkbox"/>	Low	Device Pending Activation	<input type="checkbox"/>			Pending Activation	Remove		
<input checked="" type="checkbox"/>	Elevated	Device Pin	<input type="checkbox"/>			Select an Option	Select an Option		

### Configuring the MDM Actions in MVISION Mobile Console

The next step is to configure the MDM actions in the MVISION Mobile Console on the **Policy** page.

1. Log into the MVISION Mobile Console, and in the navigation panel, select the **Policy** page.
2. Select the Selected Group from the drop-down list that you want to apply the compliance.
3. Scroll down to the **Device Pending Activation** event.
4. Under the **MDM Action** drop-down list, select the newly created Smart Group to associate the VPN profile in Workspace ONE UEM. In this example, Pending Activation is selected.

<input type="checkbox"/>	<b>Critical</b>		Device Jailbroken/Rooted	<input checked="" type="checkbox"/>			Select an Option	Select an Option		
<input checked="" type="checkbox"/>	<b>Low</b>		Device Pending Activation	<input type="checkbox"/>			Pending Activation	Remove		
<input checked="" type="checkbox"/>	<b>Elevated</b>		Device Pin	<input type="checkbox"/>			Select an Option	Select an Option		

5. Choose **Remove** for MDM Mitigation Action.
6. Deploy the policy.
7. Run a manual sync so new devices enrolled in MDM to get synced with the MVISION Mobile Console and show up in the “Pending Activation” state.
8. After the dormancy period has passed (as defined in MVISION Mobile Console as **Allowed Inactivity Time**), a ‘Device Pending Activation’ event gets triggered for the newly synced devices that have not yet activated MVISION Mobile.
9. See “[Appendix B – User’s Perspective on iOS VPN Activation](#)” for the user interaction with this compliance.

**Note:** This setting assigns the tag “Pending Activation” to the device if MVISION Mobile is not activated within 24 hours of the MVISION Mobile Console syncing the device record from the Workspace ONE console. Adding this tag to the device means the device is a member of the “MVISION Mobile Pending Activation” assignment group and is assigned the auto-activation VPN profile. Once MVISION Mobile is activated, the “Device Pending Activation” group is treated as automatically fixed and the remove Mitigation occurs to remove the tag from the device.

## Available MDM Actions via Workspace ONE UEM

MVISION Mobile interacts with the Workspace ONE UEM MDM through API’s that provide the ability to modify device configurations securely over the internet. Several methods are used that provide protection capabilities.

The following are the possible actions:

- **Wi-Fi Disconnect:** If 'Wi-Fi Disconnect' is defined as a response to a threat, the MVISION Mobile Console sends an API request to Workspace ONE UEM that creates a specifically crafted Wi-Fi profile and sends that profile to the device. This profile is created in such a way that the currently connected Wi-Fi network is disconnected when the profile is received by the device. The Wi-Fi profile is removed after five minutes from the time the detection occurred. This applies to iOS devices only at this time.
- **Enterprise Wipe:** As a response to a threat, this action request removes all company information from the device including managed apps and configurations. Then it un-enrolls the device from Workspace ONE UEM.
- **Assignment Group:** If an assignment is the selected Group the MVISION Mobile Console instructs Workspace ONE UEM to assign the device to the chosen assignment Group. The workflow assigned to that assignment Group determines the action that Workspace ONE UEM takes on the device. Examples of workflows are in the Appendix and at a high-level include:

- **Compliance Policy:** The Smart Group that the device has been assigned to is assigned to a Compliance Policy. This policy allows 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 action to remove company intellectual property from the device.
  - **Exclusion Group:** Assigning the device to a Smart Group used as an exclusion group in a profile immediately removes the profile from that device.
- **Remove:** This action is typically used under "Mitigation Action". If selected under Mitigation Action, it removes the tag that was assigned to the device that was selected in the **MDM Action** column, once the threat has been fixed or marked as approved.

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

## Example Device Compliance Policy

Follow these steps to create the Compliance Policy.

1. Go to **Devices** and select **Compliance Policies**.
2. Click **List View** and click **Add** and then select the platform.
3. Follow the screenshots below to complete the process.

Edit Device Policy

① Rules ② Actions ③ Assignment ④ Summary

Match **All** Of The Following Rules

Application List Does Not Contain com.mcafee.mvision.mobile.appstore

+ Add Rule

Edit Device Policy

① Rules ② Actions ③ Assignment ④ Summary

Immediately perform the following actions ☒ Mark as Not Compliant

Notify Send Email to User CC: Default Template

MVISION - Compliance Violation User

[Click here to go to the Message Template page in a new window or tab.](#)

+ Add Escalation

4. This figure shows editing the assignment attributes for the policy.

Edit Device Policy

① Rules ② Actions ③ Assignment ④ Summary

Managed By **CustomerSuccess**

Smart Groups Start typing to add a group

Exclusions NO YES

VIEW DEVICE ASSIGNMENT

5. This figure shows editing the summary attributes for the policy.

Edit Device Policy

① Rules ② Actions ③ Assignment ④ Summary

General

Name **Enterprise Compliance - MVISION Mobile Not Installed**

Description **Application List**

Device Summary

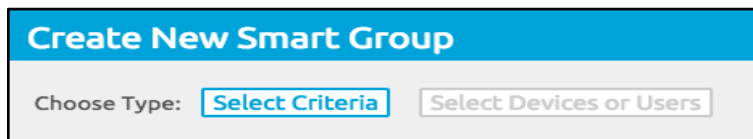
We cannot display a Device Summary at this time. Please Finish and Activate the policy. If the page does not close on it's own after clicking "Finish and Activate", please click the close button at the top right corner of the page.

**Note:** Make sure to create two Policies, one for iOS and one for Android. The message template created can be used for both Policies.

## Appendix A – MDM Action Use Cases

### Overview

For more granular options, the MVISION Mobile Console integration with Workspace ONE UEM facilitates 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' to create in Workspace ONE UEM.

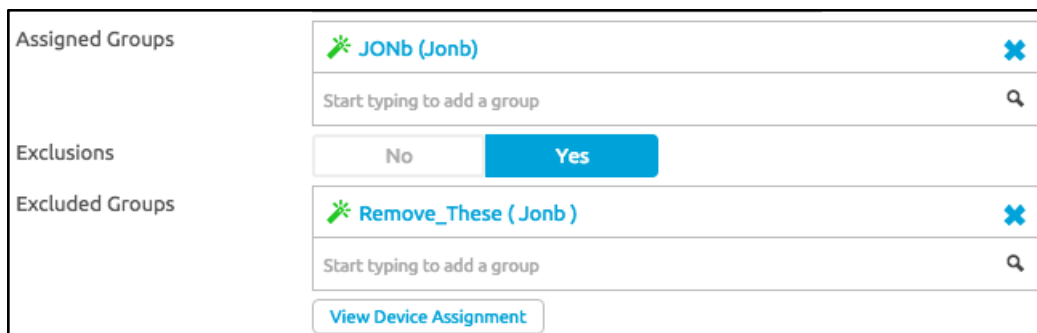


The 'Create New Smart Group' dialog box has a blue header with the title. Below the header, there is a 'Choose Type:' label followed by two buttons: 'Select Criteria' (highlighted with a blue border) and 'Select Devices or Users'.

This empty Smart Group is assigned when a device is under threat, the Threat Policy determines which Smart Group, if any, to associate the device for these use cases.

### Removing a Configuration Profile from the Device

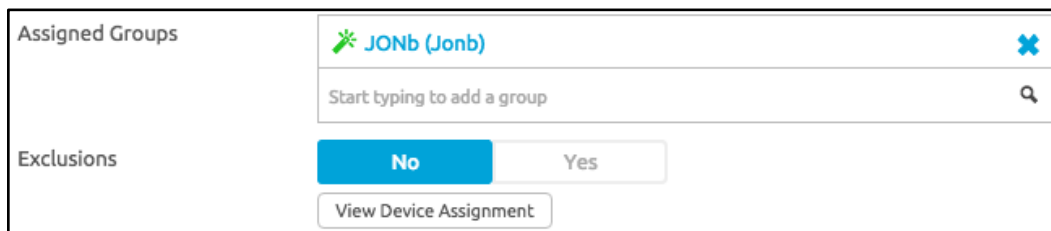
Profiles in Workspace ONE UEM are configured with a set of Exclusion Smart Groups. A Profile is removed from any devices placed in the Exclusion Smart Group allowing a Workspace ONE UEM Admin to remove Exchange profiles, VPN profiles, and Wi-Fi profiles.



This form shows settings for removing a configuration profile. It has three main sections: 'Assigned Groups' with a dropdown showing 'JONb (Jonb)' and a search bar; 'Exclusions' with 'No' and 'Yes' buttons, where 'Yes' is selected; and 'Excluded Groups' with a dropdown showing 'Remove\_These (Jonb)' and a search bar. A 'View Device Assignment' button is at the bottom.

### Add a Configuration Profile to a Device

The same holds true for Profiles that are added to a device when they are threatened. 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 into the Assigned Groups of the Profile. This profile is then pushed to any device that shows up in that Smart Group.

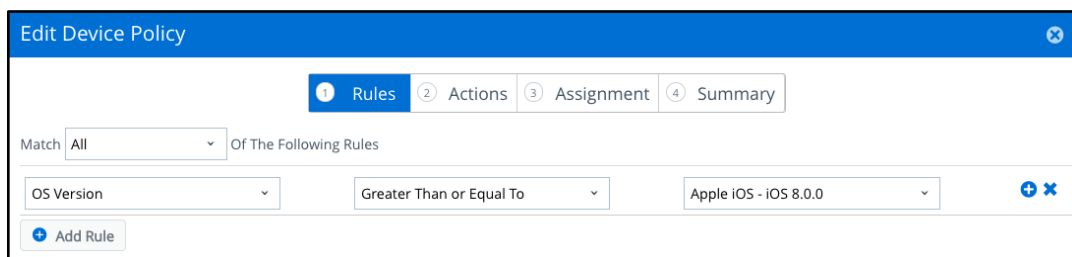


This form shows settings for adding a configuration profile. It has three main sections: 'Assigned Groups' with a dropdown showing 'JONb (Jonb)' and a search bar; 'Exclusions' with 'No' and 'Yes' buttons, where 'No' is selected; and a 'View Device Assignment' button at the bottom.

## Compliance Policy

Compliance policies allow for combinations of actions, such as notify the user via Push or SMS messages and then remove access for items such as email. Through the zConsole Policy page, the admin can assign the device to a Compliance Policy.

Create a compliance policy with a single rule that is always true such as the device must be greater than or equal to the required minimum OS.

The screenshot shows the 'Edit Device Policy' window with a blue header bar. Below the header is a tabbed interface with four tabs: 'Rules' (active), 'Actions', 'Assignment', and 'Summary'. Under the 'Rules' tab, there is a 'Match' dropdown set to 'All' and a label 'Of The Following Rules'. Below this is a rule configuration area with three fields: 'OS Version' (dropdown), 'Greater Than or Equal To' (operator dropdown), and 'Apple iOS - iOS 8.0.0' (value dropdown). To the right of these fields are '+' and 'x' icons. At the bottom left of the rule area is a '+ Add Rule' button.

Choose any combination of the following Actions as needed to suit the use case. It is good practice to take actions in order to protect the device or remove access to company data and then to alert the user to let them know what happened.

- Remove a managed application or remove all managed applications.
- Install a Compliance Profile (This is used to increase restrictions on the device such as a longer PIN code, or to remove access to the camera).
- Remove/Add a configuration profile or profile type (Profile type could be: Email profile, Wi-Fi).
- Send a series of alerts to the user via SMS to device, Push notification to device, or email to the user. These messages can state any needed message. For example, telling the user why the device was found to be at risk and why certain company intellectual property, such as email, is removed.
- Enterprise wipes 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 the following figure.

The screenshot displays a configuration interface for a compliance policy. It features two main action blocks, each with a header bar and a content area. The first block's header bar includes the text 'Immediately perform the following actions' followed by a checkbox labeled 'Mark as Not Compliant'. Below this, the first action is configured with 'Application' as the trigger and 'Block/Remove All Managed Apps' as the action. The second block's header bar includes 'After 1 Minutes' followed by a checkbox labeled 'Perform the following actions: Repeat Mark as Not Compliant'. Below this, the second action is configured with 'Notify' as the trigger and 'Send Push Notification to Device' as the action. To the right of the push notification action, there is a 'Default Template' section with a 'Select Message Template' dropdown and a link that reads 'Click here to go to the Message Template page in a new window or tab.' The third block's header bar includes 'After 1 Minutes' followed by a checkbox labeled 'Perform the following actions: Repeat Mark as Not Compliant'. Below this, the third action is configured with 'Notify' as the trigger and 'Send Email to User' as the action. To the right of the email action, there is a 'CC:' field, a 'Default Template' section with a 'Select Message Template' dropdown, and a link that reads 'Click here to go to the Message Template page in a new window or tab.'

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 Workspace ONE UEM Agent and then another minute as an email to the user. This allows the admin to create message templates that are used in all different scenarios specific to the threat. There would be a compliance policy to remove access to data, perhaps another to unenroll the devices and perhaps yet another one to remove access to email.

The actions are dictated by the individual company security policy and use cases.

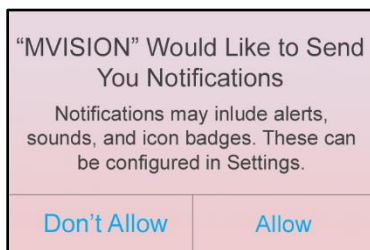
## Appendix B – User's Perspective on iOS VPN Activation

The following steps show how to activate MVISION Mobile on iOS devices:

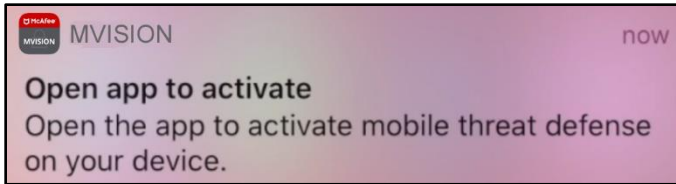
1. In the screenshot, the VPN turned on is indicated in the notification area at the top.



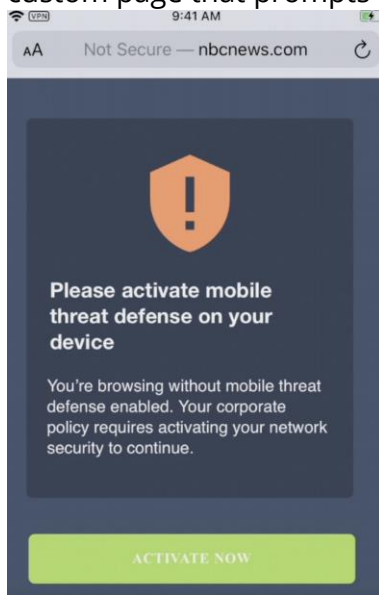
2. As a result, the end-user receives a notification popup saying MVISION Mobile would like to send notifications.



3. If the end-user clicks **Allow**, a popup notification displays asking the user to open the App. The notification title and message can be customized through the VPN profile parameters as defined in the MDM.



4. If the end-user clicks on the notification, it launches MVISION Mobile and starts the activation flow. Once MVISION Mobile is activated, the VPN profile is automatically removed from the device.
5. In case the end-user ignored the popup notification, at some point when the user visits an HTTP website through the web browser on their device. An example is in typing a URL that has not been visited previously on their device, such as apache.org or tomcat.com. MVISION Mobile VPN intercepts the communication and displays a custom page that prompts the user to activate the MVISION Mobile app.



**Note:** The look and feel of this HTML page can be customized through the VPN profile parameters as defined in the MDM.

6. Once MVISION Mobile is activated by clicking on **Activate Now** and following the prompts within MVISION Mobile, the MVISION Mobile VPN automatically uninstalls silently from the device by the MVISION Mobile Console MDM Mitigation Action to remove the device from the "Pending Activation" group.