



McAfee MVISION Mobile

MobileIron

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 MCAFEES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface.....	5
Audience	5
Related Documentation	5
Overview.....	5
System Requirements	6
About MDM and MVISION Mobile Console Communication	6
MVISION Mobile Integration with MobileIron Core	7
Application Deployment.....	7
Synchronization	8
Full MDM Synchronization.....	8
On-Demand Device Synchronization.....	8
Setup Synchronization	9
Setting up Synchronization on MVISION Mobile Console.....	11
Zero-Touch Activation for MVISION Mobile iOS for MobileIron Core.....	11
Overview of the Setup	11
A Sample Flow after the Configuration is Complete	11
Differences in Zero-Touch Activation	12
Setting Up Zero-Touch Activation for iOS.....	12
Updating Your Configuration File.....	12
Configuring within the MobileIron Core Console.....	14
Configuring within the MVISION Mobile Console.....	14
Auto Activation/Advanced Application Deployment.....	15
iOS Activation.....	15
Android Activation.....	17
Android Personal Profile Auto-Activation.....	17
Activation with MobileIron Messaging	18
Setting up the VPN Profile for MVISION Mobile	18
Configuring the VPN Profile in MobileIron Core.....	18
Configure the MDM Actions in MVISION Mobile Console.....	20
Enable CPS Event Notification	21

Enabling CPS Event Notification on the MobileIron Core	21
Device Actions	21
MVISION Mobile Integration with MobileIron Cloud	25
Synchronization	25
Full MDM Synchronization.....	25
On-Demand Device Synchronization.....	25
Setup Synchronization	25
Zero-Touch Activation for MVISION Mobile iOS for MobileIron Cloud.....	26
Overview of the Setup	26
A Sample Flow after the Configuration is Complete	26
Differences in Zero-Touch Activation	27
Setting Up Zero-Touch Activation for iOS.....	27
Updating Your Configuration File.....	27
Configuring within the MobileIron Cloud Console.....	28
Configuring within the MVISION Mobile Console.....	29
Auto Activation/Advanced Application Deployment.....	30
iOS Activation.....	30
Android Activation.....	31
Android Personal Profile Auto-Activation.....	31
Activation with MobileIron Messaging	31
Setting up the VPN Profile for MVISION Mobile	32
Configuring the VPN Profile in MobileIron Cloud	32
Configuring iOS Devices.....	32
Configure the MDM Actions in MVISION Mobile Console.....	33
VPN Auto-install and MVISION Mobile Activation on Device	33
Device Actions	36
Common Steps Setting Up Synchronization in MVISION Mobile Console.....	37
Appendix A - MobileIron Messaging and Device Activation.....	40
Appendix B - Sample Configuration File for Zero-Touch Activation.....	43

Preface

This document is an administrator's guide to providing integration with MobileIron Mobile Device Management (MDM).

Audience

The intended audience for this guide is a MVISION Mobile Console administrator. This guide helps administrators to provide integration with the MobileIron MDM. The MVISION Mobile Console application provides threat protection to mobile devices, and the system administrator sets policies for threats. MVISION Mobile Console also monitors and manages threats detected. See "MVISION Mobile Console Product Guide" for more information.

Related Documentation

For more information and specific configuration information about MDM, SIEM, and iOS, Android Platforms, search for "MVISION Mobile" in the McAfee document Portal at <https://docs.mcafee.com>

Overview

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

- Synchronizes users and devices 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 defined actions locally. However, when MVISION Mobile is integrated with an MDM, actions can be performed by the MDM, providing a very powerful protection tool.

The MobileIron Administrator can set up different workflows to handle different threats via MVISION Mobile Console that the MVISION Mobile Console Administrator can choose through the Policy page.

When a threat is detected, the MVISION Mobile Console instructs the MobileIron console to move the device to the chosen Label in the threat policy. The workflow assigned to that Label determines the action that MobileIron takes on the device. The communication from the MVISION Mobile Console to the MobileIron console is performed securely with a MobileIron API call.

System Requirements

The following table details specific requirements for MobileIron's MDM.

Item	Specifics
MobileIron MDM enrolled device	Core: minimum v9 Cloud (Current SaaS version)
MobileIron Core	Core: v9.6.0.1 iOS Mobile@Work MDM Agent: v9.7.0 Android Mobile@Work MDM Agent: v9.6.0 (Core v10.0.0.1 and Mobile@Work v10 are needed to support local MTD actions)
MobileIron Cloud	MobileIron Cloud Release 52 MobileIron Go for iOS Client: v3.2 MobileIron Go for Android Client: v2018.04.23
API Administrator Account in MobileIron management console	Set this up with the proper authorization defined in the sections below.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the MobileIron console through API REST calls. When MVISION Mobile detects an event, it consults the current Threat Policy resident on the device and if the action involves MobileIron, it is either performed locally or communicated to the MVISION Mobile Console. The MVISION Mobile Console then reaches out to the proper MobileIron API Server and provides the commands to perform the configured action.

MobileIron (MI) Core and MobileIron Cloud environments are configured differently, and this guide details each configuration in separate sections. The key difference from a MVISION Mobile Console integration point of view is that MI Core manages devices and performs actions locally while MI Cloud instances manage devices and actions via device groups.

MVISION Mobile Integration with MobileIron Core

The following sections describe the steps for app deployment, synchronization and device actions for MobileIron Core Integration with MVISION Mobile.

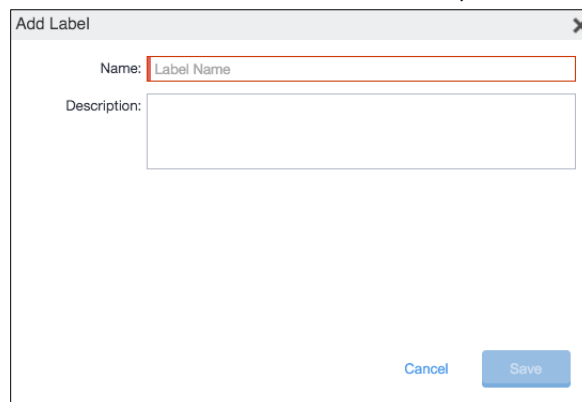
Application Deployment

If the user is not using MobileIron Threat Defense, MVISION Mobile can be deployed. To deploy the MVISION Mobile application through MobileIron, download it from the public App Store for iOS and the Google Play Store for Android and then deploy it with the steps provided.

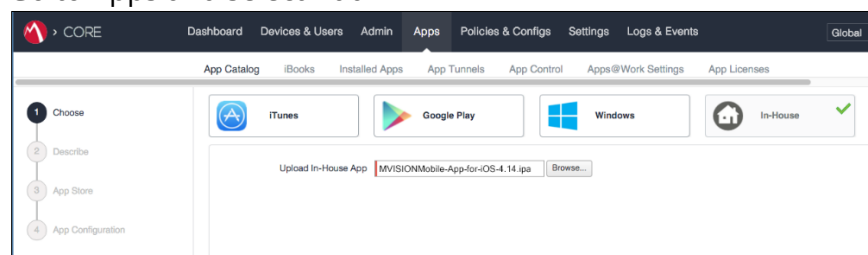
Log into MobileIron Core. If no appropriate Label exists for the application deployment, create a Label. Create a new Internal Application and upload the proper application file (IPA for iOS and APK for Android) to MobileIron. Assign the Label to the application and publish it.

Perform the following steps:

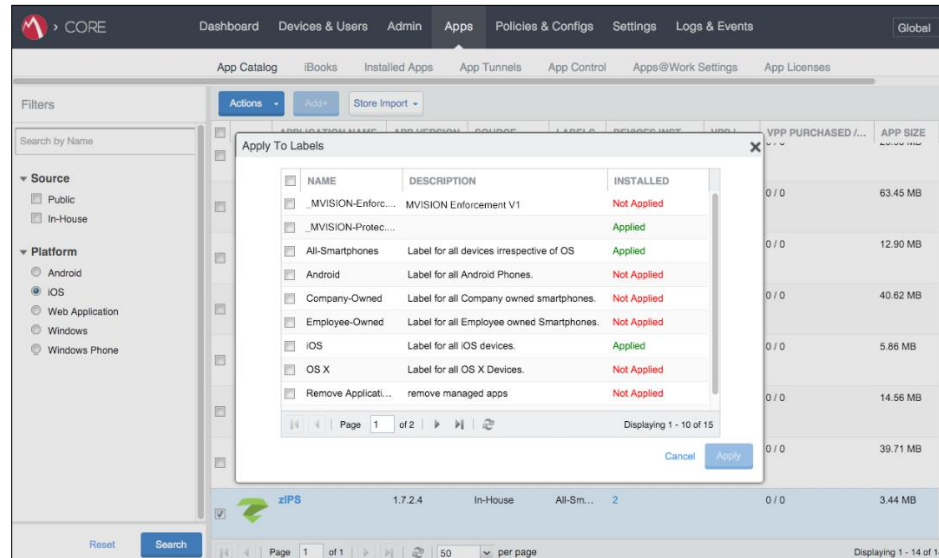
1. Create a Label to be assigned to devices that need to deploy MVISION Mobile.
 - a. Go to **Devices** and click on **Users**, then select **Labels** and select **Add Label**.



- b. Enter label name and short description.
 - c. Click **Save**.
2. Upload the MVISION Mobile application.
 - a. Go to Apps and select Add+



- b. Click **Next** and add/update information as needed in the next two screens and then click **Finish**.
 - c. The application is now ready to be deployed.
3. Assign the Label created in step 1 to this application.
 - a. Click the radio button in front of the application just imported and click **Actions** and **Apply to Label**.



- b. Choose the label created in step 1) and click **Apply**.
4. Assign this label to all devices that are required to be protected by MVISION Mobile
 - a. Navigate to **Device and Users** and select **Devices**.
 - b. Click on the radio button next to all devices to be protected.
 - c. Click **Actions** and then choose **Apply to Label**.
 - d. Choose the Label to be applied and click **Apply**.

Synchronization

Full MDM Synchronization

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

On-Demand Device Synchronization

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

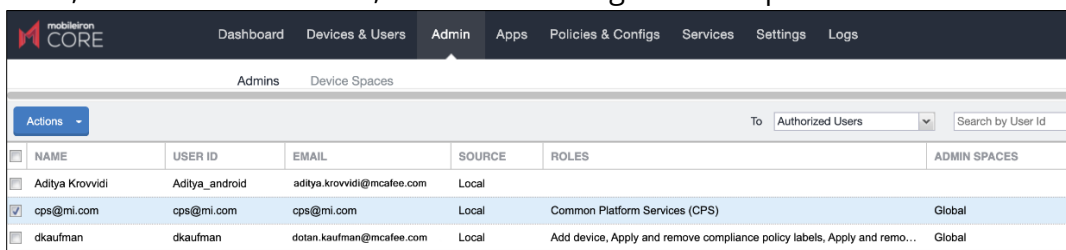
The MVISION Mobile Console application receives the identification information from MVISION Mobile used for the authentication and matches it up with the proper customer for authentication. Once that happens, MVISION Mobile Console retrieves that device and user information from the MDM configured for that customer. MVISION Mobile on that device is now authenticated and allowed to proceed. For this to work correctly, MVISION Mobile must be deployed as follows:

- **iOS:** Associate a PLIST file with the MVISION Mobile application that pushes down the fields used for the on-demand device sync. This is described in the “[Auto Activation/Advanced Application Deployment](#)” section.
- **Android:** This requires Android for Enterprise for auto-activation. Use MVISION Mobile Console activation URLs for native Android. Contact the McAfee Customer Support Team for more information on this topic.

Setup Synchronization

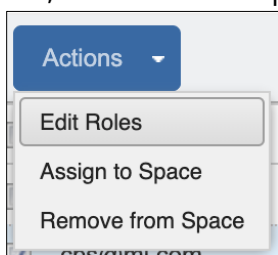
Perform the following steps:

1. Create a MobileIron administrator with the proper API access.
2. Navigate to **Devices and Users**, then select **Users**, select **Add**, and select **Add Local User**.
3. Then, select the **Admin** tab, and the following window opens:

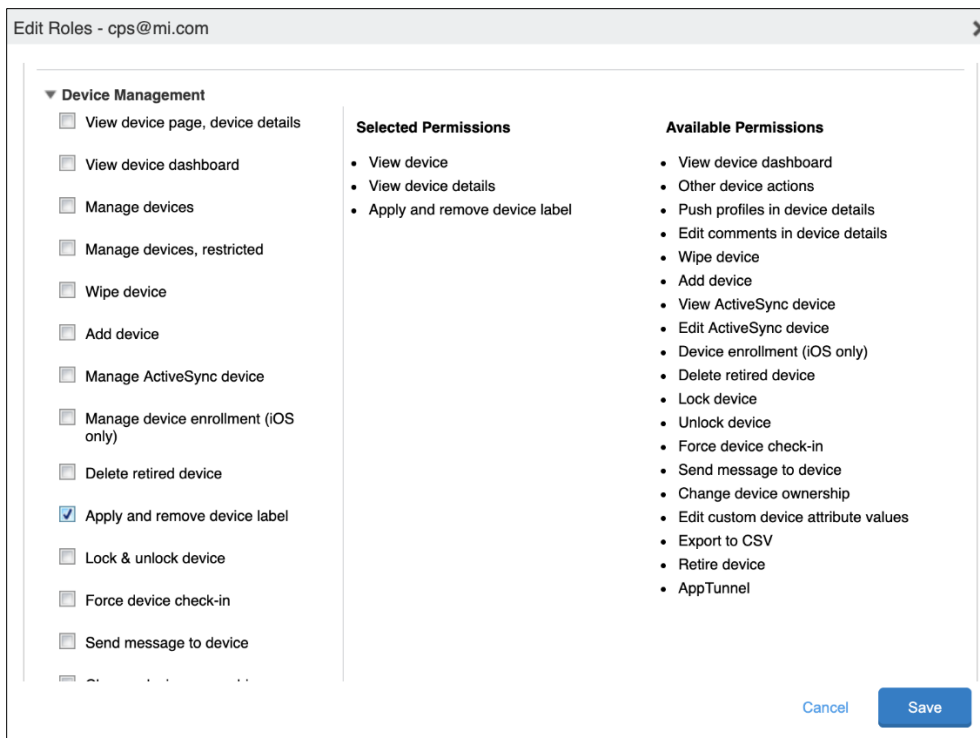


mobileiron CORE						
Dashboard Devices & Users Admin Apps Policies & Configs Services Settings Logs						
Admins Device Spaces						
Actions To Authorized Users Search by User Id						
	NAME	USER ID	EMAIL	SOURCE	ROLES	ADMIN SPACES
<input type="checkbox"/>	Aditya Krovvidi	Aditya_android	aditya.krovvidi@mcafee.com	Local		
<input checked="" type="checkbox"/>	cps@mi.com	cps@mi.com	cps@mi.com	Local	Common Platform Services (CPS)	Global
<input type="checkbox"/>	dkaufman	dkaufman	dotan.kaufman@mcafee.com	Local	Add device, Apply and remove compliance policy labels, Apply and remo...	Global

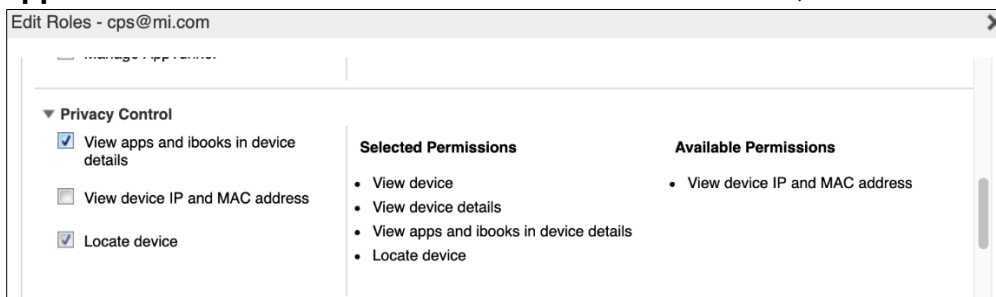
4. Click on the checkbox for the API admin user, and on the **Actions** button at the top left, click on the drop-down menu and select **Edit Roles**.



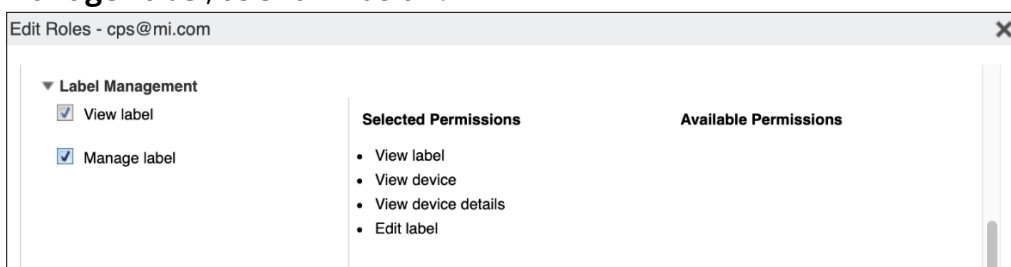
5. The **Admin Roles** pop-up window opens. If using MobileIron Core version 10.8 or later, then in the **Device Management** section, click on the checkbox for **Apply and remove device label**, as shown below. If using MobileIron Core prior to version 10.8, then the **Apply and remove device label** permission is not required.



6. Scroll down to the **Privacy Control** section, and click on the checkboxes for **View apps and ibooks in device details** and for **Locate device**, as shown below:



7. Scroll down to **Label Management**, click on the checkboxes for **View Label** and for **Manage Label**, as shown below:



8. Scroll all the way down to the **Other Roles** section. If using MobileIron Core version 10.8 or later, click on the checkbox for **Common Platform Services (CPS)**. If using

MobileIron Core prior to version 10.8 or later, an additional permission is required and click on the checkbox for **API** in the **Other Roles** section.

NOTE: *To leverage MobileIron CPS Service in MVISION Mobile Console (Apps Sync, Dynamic MTD Device Cleanup), both ports 443 and 8883 must be open on the MobileIron instance. Contact the MobileIron Support representative to ensure this is opened in order to use the feature.*

9. Click on the blue **Save** button at the bottom of the pop-up window.
10. Create one or more Labels that contain the devices that are protected if there is not one that exists. The MVISION Mobile Console uses these label(s) to synchronize devices and their associated users.

Setting up Synchronization on MVISION Mobile Console

See the [“Common Steps Setting Up Synchronization in MVISION Mobile Console”](#) section for these steps.

Verify the synchronization by going to the **Devices** or **Users** pages in the MVISION Mobile Console to see that they are showing up.

Note: *The device entries are greyed out until the user starts up MVISION Mobile and activates the applications.*

Zero-Touch Activation for MVISION Mobile iOS for MobileIron Core

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.

Note: *This feature requires MVISION Mobile Console Release 4.33 or later and MVISION Mobile Release 4.18 or later.*

Overview of the Setup

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

- The MobileIron Core console has a label 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.

A Sample Flow after the Configuration is Complete

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

1. The MDM pushes the MVISION Mobile app and the zVPN Profile to the device.
2. There is a “Launch MVISION Mobile” notification on the device from the zVPN Profile, but the end-user does not activate zIPS yet.
3. A threat is generated on the device, such as a “Device Pin” threat.

4. The zVPN Profile shows a notification of the threat on the device, and zIPS is still not launched.
5. 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.*
6. 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:

- Differences in zero-touch activation compared to a standard MVISION Mobile activation
- Overview of the interactions

See the “McAfee MVISION Mobile Console Product Guide” document on the support portal.

Setting Up Zero-Touch Activation for iOS

This instruction set describes configuring 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 sample XML configuration file, the defaultchannel, and the tenantid for your tenant and this configuration. These values are not the same values as in similar configurations. The tenantid used is not the value displayed in the MVISION Mobile Console. You also need this sample XML configuration file and you update these values in that file.*

Updating Your Configuration File

1. Contact the McAfee Customer Success team and get these items:
 - a. The default XML configuration file for zero-touch activation for MobileIron Core. See “[Appendix B - Sample Configuration File for Zero-Touch Activation](#)” for a sample of this file.
 - b. Your default channel value for zero-touch activation. This value must have “/json” at the end of the string.

- c. Your tenant id value for zero-touch activation.
2. Update the configuration file with your defaultchannel and tenantid that the Customer Success team provided.
3. Make sure the values follow these conventions and the keys are exact matches as they are case sensitive:
 - a. **Key:** defaultchannel - Set the defaultchannel to the JSON endpoint value. You get this from the **Manage** page and **General** tab in the MVISION Mobile, and you must add “/json” string to the end. For instance:

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

- b. **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.*

- c. **Key:** MDMDeviceID: \$DEVICE_UUID\$
- d. **Key:** assume_vpn_permission_granted

The values are true or false. Set this value to true to grant this permission.

- e. **Key:** enable_auth_redirect

The values are true or false. Set this value to true to authorize a redirect.

- f. **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.

- g. **Key:** auth_custom_notification_title

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

- h. **Key:** runlevel: Production (Optional)

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.

- i. **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.

- j. **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

Configuring within the MobileIron Core Console

To configure zero-touch activation, perform these steps:

1. Login to the MobileIron Core with an admin ID and password.
2. Navigate to this location and create a new label with the type as Manual.
Devices & Users > Add
3. Navigate to this location and create a new configuration profile.
Policies & Configs
4. The **Policies & Configs** window opens. Click on the drop-down menu next to **Add New** at the top left.
5. Select **Add New**, then select **iOS/macOS/tvOS**, then click on **Configuration Profile**. The **New Configuration Profile Setting** window opens.
6. In this window Enter a **Name** and a **Description** of the zero-touch profile, for instance, named "zVPNProfile."
7. Browse to the configuration profile you created in the section above and associate it to the new label you created.
8. Make sure you assign the configuration to the label that you created in Step 2.

Configuring within the MVISION Mobile Console

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 MobileIron Core MDM. See the "[Common Steps Setting up Synchronization in MVISION Mobile Console](#)" section for more information.

Note: This 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. 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 label that you defined 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.
5. **Save and Deploy** your changes.

The result is the Zero-Touch VPN is pushed to the device and begins reporting threats.

Note: The timing of this push occurs depending on the dormancy time set for the tenant on MVISION Mobile Console.

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 MobileIron Core, and MVISION Mobile Console.

Auto Activation/Advanced Application Deployment

The McAfee MVISION Mobile application in both iOS and Android Enterprise can auto activate. The process is different on each platform as described below.

iOS Activation

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

Configure the desired keys within MobileIron after adding the application.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	\$DEVICE_UUID\$
tenantid	String	Copy the value from the Tenant ID field on the MVISION Mobile Console Manage page under the General tab.
defaultchannel	String	Copy the value from the Default Channel field on the MVISION Mobile Console Manage page under the General tab.

display_eula	String	no (Optional) If this key is not used, the default displays the End User License Agreement (EULA).
tracking_id_1	String	(Optional) Use the desired identifier.
tracking_id_2	String	(Optional) Use the desired identifier.

NOTE: *The configuration keys are case sensitive.*

The PLIST file is created as a text file in the following format using the variables in the above table.

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

Add this PLIST file to MobileIron via the console by following these steps:

1. Go to **Policies and Configs** and select **Configurations** and select **Add New** and select **iOS and OS X** then select **Managed App Config**.
2. Select the file which was just created above to upload.
3. Enter the bundleID for the iOS App, com.mcafee.mvision.mobile.
NOTE: *If using the MVISION Mobile for iOS app from the Apple App Store, use the bundleID com.mcafee.mvision.mobile.appstore.*
4. Click on the radio button by the New Managed App Configuration item.
5. Go to **More Actions** and select **Add to Label**.
6. Choose the **Label** associated with MVISION Mobile iOS app.
7. Click **Apply**.

Each time the MVISION Mobile iOS app gets pushed to a device it contains the information specified in the PLIST file. When the user clicks on the MVISION Mobile app, they automatically sign into the proper MVISION Mobile Console.

Android Activation

Android Enterprise users can continue to use the managed app config for activations. Make sure the right device ID is passing the value for the configuration parameter. The variables are the same set as the PLIST variables in the “iOS Activation” section.

For native Android devices, activations require the use of activation URLs. These can be sent to end-users via the MVISION Mobile Console or the MDM. Clicking on MVISION Mobile 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. After the MDM has been added, the activation link is provided for devices. This activation link is used along with appending the MDM device identifier. The MVISION Mobile Console page displays the expiration date and time, and if needed the link can be regenerated.

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 Personal Profile Auto-Activation

For MVISION Mobile release 4.10 and later, use these additional configuration keys and values for auto-activation for the personal profile in an Android Enterprise configuration.

Configuration Key	Value Type	Configuration Value	Notes
share_activation_data	String	True	This is required if 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.

Activation with MobileIron Messaging

MobileIron supports message templates where a customized email can be sent to users. This is an optional activation method. See “Appendix A - MobileIron Messaging and Device Activation” for information on how to set up these notifications.

Setting up the VPN Profile for MVISION Mobile

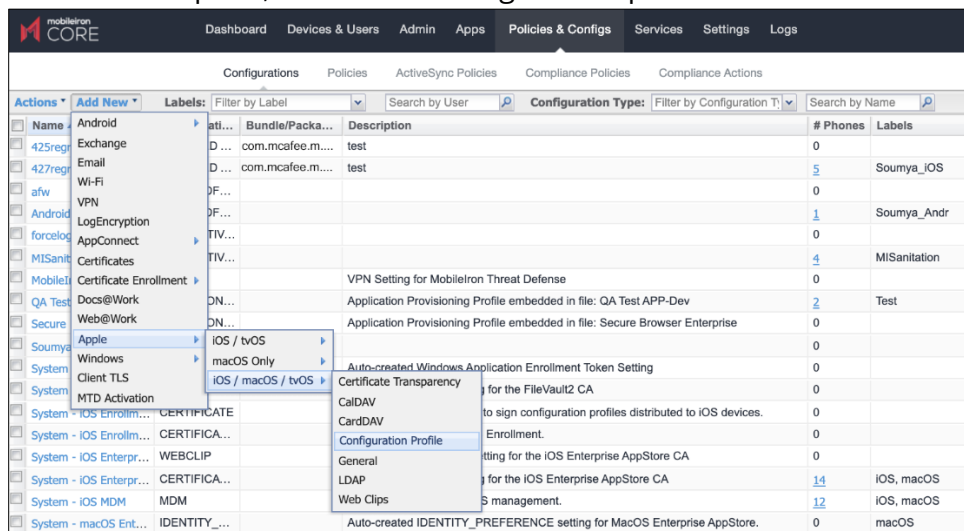
This section provides instructions for setting up the VPN Profiles.

Configuring the VPN Profile in MobileIron Core

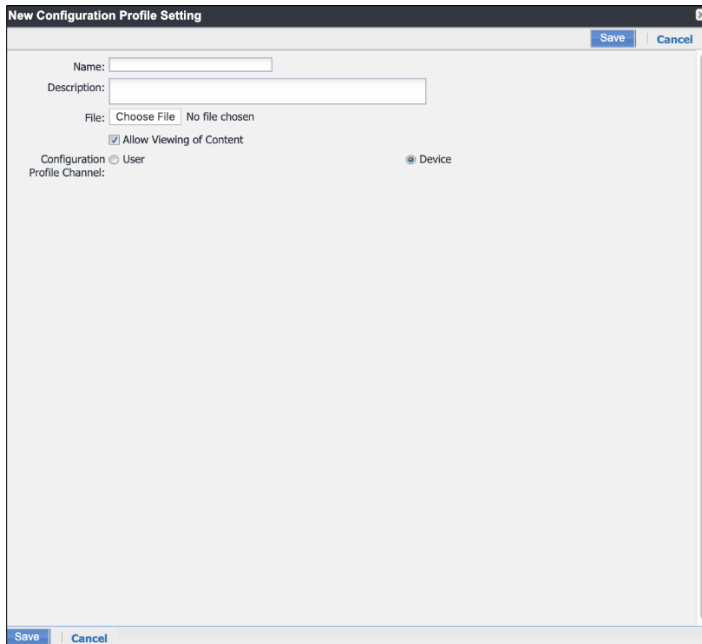
The steps to set up the VPN Profile for MVISION Mobile to be loaded onto the devices are as follows:

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. Login to the MobileIron Core with an /admin ID and password.
2. In the menu across the top, select **Policies & Configs**.
3. The **Policies & Configs** window opens. Click on the drop-down menu next to **Add New** at the top left, and the following menu opens:

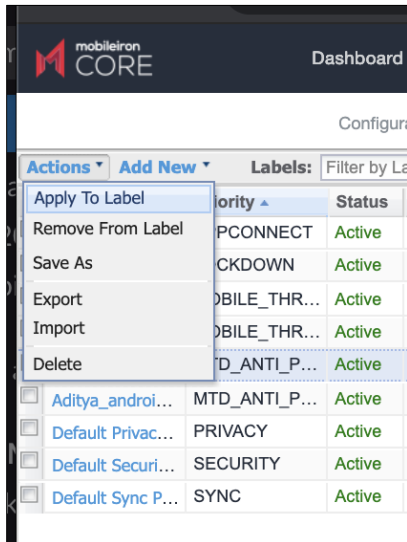


4. Select **Add New**, then select **iOS/macOS/tvOS**, then click on **Configuration Profile**.
5. The **New Configuration Profile Setting** window opens, as shown below:



6. In this window Enter a **Name** and a **Description** of the VPN Policy.
7. Obtain the mvision_vpn_app_launch file from your McAfee Customer Success contact. Upload the mvision_vpn_app_launch file as part of the new profile definition. Edit/add to key-value pairs in the **VendorConfig** section as needed:
 - a. enable_auth_redirect: true (Values of true or false. Controls redirecting HTTP URLs to a customized web page requesting the user to launch the MVISION Mobile app.)
 - b. enable_auth_notifications: true (Values of true or false. Controls display of the local notification message requesting the user to launch the MVISION Mobile app.)
 - c. auth_custom_notification_title (Optional): (Open the app to activate. The default notification title can be changed to a custom title if desired.)
 - d. auth_custom_notification_message (Optional): (Open the app to activate mobile threat defense on the device. The default notification message can be changed to a custom message, if desired.)
 - e. auth_custom_html_base64 (Optional): (The user can set a custom HTML page to display when an HTTP site is accessed, and it needs to be Base-64-encoded before entering it in this field.)
 - f. auth_redirect_url (Optional): (This is the redirect URL which is used to launch the app on the iOS device. Default value is mvisionmobile://login.) The redirect URL value can be customized. For example, the redirect URL to use with the McAfee MVISION Mobile app is:
mvisionmobile://login
8. Click on the **Save** button.

9. A pop-up menu displays to indicate that the Policy loaded successfully.
10. Click on the **Policies & Config** menu at the top of the window.
11. Click on the checkbox next to the Policy name to which this policy is to be applied
12. Click on the drop-down menu for **Actions** (at the top left).
13. Click on **Apply to Label**.



14. The devices in the selected group are assigned to this Profile and MVISION Mobile is turned on when the devices are activated.

Configure 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. Scroll down to the **Device Pending Activation** event.
3. Under the **MDM Action** drop-down list, select the MDM device group that the custom VPN configuration in MobileIron Core was associated with. Choose **Remove** for MDM Mitigation Action.

DEVICES	<input checked="" type="checkbox"/>	Low	Device Pending Activation	<input type="checkbox"/>	VPN App Launch	Remove	
PROFILES	<input checked="" type="checkbox"/>	Elevated	Device Pin	<input type="checkbox"/>	No Action	No Action	
	<input checked="" type="checkbox"/>	Normal	DNS Change	<input type="checkbox"/>	No Action	Unavailable	
USERS	<input checked="" type="checkbox"/>	Elevated	Elevation of Privileges (EOP)	<input type="checkbox"/>	Select an Option	Unavailable	

4. Deploy the policy.
5. Run a manual sync so new devices enrolled in MDM to get synced with the MVISION Mobile Console and show up in "Pending activation" state.
6. After the dormancy period has passed (as defined in the **Manage** and **General** section of the MVISION Mobile Console as "Allowed Inactivity Time"), a "Device

Pending Activation” event should get triggered for the newly synced devices that have not yet activated MVISION Mobile.

Enable CPS Event Notification

Event notification is set for both MobileIron Core and MobileIron Core when the MTD service is used. This section shows how to turn CPS event notification on for both environments.

In order to enable CPS Event Notification on the MobileIron Core, the following CLI program is used. This program invokes a message broker, enables the Event Notification Service feature, restarts the MobileIron server, and restarts Apache Tomcat in order to reload the configurations.

Before enabling messaging there are some things to consider:

- The Messaging server listens to subscribing client requests over ports 443 and 8883, and both of these ports must be open for the event notification service to function.
- If the MobileIron Core is running in a High Availability configuration, be sure to enable messaging on both the primary and secondary nodes.

To enable event notification, refer to the MobileIron Event Notification Service and Common Platform Services API Guide for the commands to enable CPS on the MobileIron Core.

Enabling CPS Event Notification on the MobileIron Core

In order to enable CPS Event Notification on the MobileIron Core, follow the steps in the MobileIron Core documentation.

Device Actions

The MVISION Mobile integration with MobileIron provides the ability to apply a specific Label to the device within the customer's MobileIron environment. This allows the MobileIron administrator to define specific actions such as:

- Quarantine a device
- Remove email access
- Assign a configuration
- Unenroll a device (This happens automatically.)

To accomplish this, the MobileIron administrator needs to coordinate with the MVISION Mobile Console administrator what specific actions are needed and do the following configuration for each one with a unique label. MDM Integration with MVISION Mobile Console also has to be set up and functional.

This Label assigned to the device is pre-assigned to a Policy that is always evaluated as TRUE which activates a Compliance Action. The configuration involves the following:

- Building an App Control Rule
 - Linking it to a Policy that is then configured to a Compliance Action.
1. Create a new App Control Rule that evaluates to be true so that whatever Policy it is used in, always runs when a device is assigned to it:
 - a. Go to **Apps** and select **App Control**.
 - b. Select **Add** and use the fields below to create a check for an application that does not exist.

Add App Control Rule

Name:

Type: ☐ Allowed ☐ Disallowed ☒ Required (Required option is only applicable to iOS and Android)

When creating policies for Android or iOS use the "Name Equals/Identifier Equals/Name Contains/Identifier Contains" values. When creating policy for Windows Phone only use the "MS Store GUID Equals" value as white/black listing based on Name/Identifier not supported on Windows Phone. EXE/Win32 Equals is only applicable to Windows 10 desktop. The Use of Publisher/PFN is only used for Windows 10 phone and desktop. When using EXE/Win32 Equals you can choose either the publisher/application for signed apps or the direct path for un-signed apps.

Rule Entries:		App Identifier/Name	Device Platform	Comment
App	Name Equals	ZaBC123NotThere	All	This will never be there

Save **Cancel**

- c. Click **Save**.
2. Define a Compliance Action which affects the device under threat:
 - a. Navigate to **Policies** and **Configs** and select **Compliance Actions**.
 - b. Click **Add+**. (To add a new Compliance Action, use the dialog box below)

- c. Click **Save**.
3. Create a Policy that keys off of the App Control Rule:
 - a. Go to **Policies and Configs** and select **Policies**.
 - b. Select **Add New**. (Choose Security from the drop-down list).
 - c. Choose a name and ensure **Active** is checked.
 - d. Enter a description of this Policy.

- e. Scroll down to **Access Control**.
- f. Click the radio button for **When a device violates the following App Control rules**.
- g. Choose the Compliance Action created earlier.
- h. Choose the App Control Rule **Always True** and move to the enabled.

- i. Click **Save**.
4. Assign a Label that is referenced in the MVISION Mobile Console threat policy.
 - a. Click the radio button in front of the new Policy.
 - b. Go to **More Actions**.
 - c. Click **Apply to Label**.
 - d. Choose the Label to apply to this Policy that can be used in the MVISION Mobile Console (if needed, create a new label).

This is a new Action that can be selected in the threat policy such as shown under the MDM actions column below. An MDM sync might have to occur for this to be visible.

MVISION Mobile Integration with MobileIron Cloud

The next steps for app deployment, synchronization, and device actions are performed on the MobileIron console for MobileIron Cloud Integration with MVISION Mobile. See the MobileIron documentation for these steps.

Synchronization

Full MDM Synchronization

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

On-Demand Device Synchronization

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

The MVISION Mobile Console application gets the identification information from MVISION Mobile used for the authentication and matches it up with the proper customer for authentication. Once that happens, MVISION Mobile Console retrieves that device and user information from the MDM configured for that customer. MVISION Mobile on that device is now authenticated and allowed to proceed. For this to work correctly, MVISION Mobile must be deployed as follows:

- **iOS:** Associate an App Configuration with the MVISION Mobile application that pushes down the fields to be used for the on-demand device sync. This is described in the section [“Auto Activation/Advanced Application Deployment.”](#)
- **Android:** This requires Android for Enterprise for auto-activation. Use MVISION Mobile Console activation URLs for native Android. Contact the McAfee Customer Support Team for more information on this topic.

Setup Synchronization

The next step is to create the MobileIron administrator with the correct API access. See the MobileIron documentation for these steps.

The next step is to create one or more device groups that contain the devices that are protected if a device group does not exist yet for this purpose. MVISION Mobile Console uses these device group(s) to synchronize devices and possibly their associated users. Set

the device groups up in the MobileIron console then follow these steps in the MVISION Mobile Console to continue the synchronization set up.

See the "[Common Steps Setting Up Synchronization in MVISION Mobile Console](#)" section for these setup steps for MVISION Mobile Console.

Zero-Touch Activation for MVISION Mobile iOS for MobileIron Cloud

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.

Note: *This feature requires MVISION Mobile Console Release 4.33 or later and MVISION Mobile Release 4.18 or later.*

Overview of the Setup

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

- The MobileIron Cloud console has a device 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.

A Sample Flow after the Configuration is Complete

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

1. The MDM pushes the MVISION Mobile app and the zVPN Profile to the device.
2. There is a "Launch MVISION Mobile" notification on the device from the zVPN Profile, but the end-user does not activate zIPS yet.
3. A threat is generated on the device, such as a "Device Pin" threat.
4. The zVPN Profile shows a notification of the threat on the device, and zIPS is still not launched.
5. 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.*
6. 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:

- Differences in zero-touch activation compared to a standard MVISION Mobile activation
- Overview of the interactions

See the “McAfee MVISION Mobile Console Product Guide” document on the support portal.

Setting Up Zero-Touch Activation for iOS

This instruction set describes configuring 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 sample XML configuration file, the defaultchannel, and the tenantid for your tenant and this configuration. These values are not the same values as in similar configurations. The tenantid used is not the value displayed in the MVISION Mobile Console. You also need this sample XML configuration file and you update these values in that file.

Updating Your Configuration File

4. Contact the McAfee Customer Success team and get these items:
 - a. The default XML configuration file for zero-touch activation for MobileIron Core. See [“Appendix B - Sample Configuration File for Zero-Touch Activation”](#) for a sample of this file.
 - b. Your default channel value for zero-touch activation. This value must have “/json” at the end of the string.
 - c. Your tenant id value for zero-touch activation.
5. Update the configuration file with your defaultchannel and tenantid that the Customer Success team provided.
6. Make sure the values follow these conventions and the keys are exact matches as they are case sensitive:
 - a. **Key:** defaultchannel - Set the defaultchannel to the JSON endpoint value. You get this from the **Manage** page and **General** tab in the MVISION Mobile, and you must add “/json” string to the end. For instance:

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

- b. **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.

- c. **Key:** MDMDeviceID: \$DEVICE_UUID\$
- d. **Key:** assume_vpn_permission_granted
The values are true or false. Set this value to true to grant this permission.
- e. **Key:** enable_auth_redirect
The values are true or false. Set this value to true to authorize a redirect.
- f. **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.
- g. **Key:** auth_custom_notification_title
Set the value to "Launch MVISION Mobile." The notification title can be changed to a custom title if desired.
- h. **Key:** runlevel: Production (Optional)
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.
- i. **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.
- j. **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

Configuring within the MobileIron Cloud Console

To configure zero-touch activation, perform these steps:

1. Login to the MobileIron Cloud with an admin ID and password.

2. Create a new Device Group.
3. Navigate to Configurations.
4. Click on **Add** -> Select **Custom Config**.
5. In this window enter a **Name** of the zero-touch profile, for instance, named "zVPNProfile."
6. Browse to the configuration profile you created in the section above and upload it to the configuration.
7. Make sure you assign the configuration to the device group that you created in step 2.

Configuring within the MVISION Mobile Console

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 MobileIron Cloud MDM. See the "[Common Steps Setting up Synchronization in MVISION Mobile Console](#)" section for more information.

Note: This 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 appropriate group in 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 label that you defined 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.

Note: The timing of this push occurs depending on the dormancy time set for the tenant on MVISION Mobile Console.

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 MobileIron Core, and MVISION Mobile Console.

Auto Activation/Advanced Application Deployment

The MVISION Mobile application for both iOS and Android Enterprise can auto-activate the user. The process is different on each platform as described below.

iOS Activation

McAfee’s iOS MVISION Mobile application takes advantage of the Managed Application Configuration when the app is pushed down to the device. This provides the best user experience, allowing the user to startup MVISION Mobile iOS without having to enter any credentials. The Managed Application configuration pre-programs MVISION Mobile iOS with this information.

See the MobileIron documentation for these steps which are performed on the MobileIron console.

The configuration keys which are needed are shown in the table below:

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	\${devicePK}
tenantid	String	Copy the value from the Tenant ID field on the MVISION Mobile Console Manage page under the General tab.
defaultchannel	String	Copy the value from the Default Channel field on the MVISION Mobile Console Manage page under the General tab.
display_eula	String	No (Optional) If this key is not used, the default displays the EULA.
tracking_id_1	String	(Optional) Use the desired identifier.
tracking_id_2	String	(Optional) Use the desired identifier.

NOTE: *The configuration keys are case sensitive.*

Each time the MVISION Mobile iOS app gets pushed to a device it contains the information specified in the PLIST file. When the user clicks on the MVISION Mobile app, they automatically sign into the proper MVISION Mobile Console environment.

Android Activation

Android Enterprise users continue to use the managed app config for activations. Verify that the right device ID value is passed for the configuration parameter. The variables are the same set as the PLIST variables in the “iOS Activation” section.

For native Android devices, activations require the use of activation URLs. These can be sent to end-users via the MVISION Mobile Console or the MDM. Clicking on MVISION Mobile 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 MDM tab. After the MDM has been added, the activation link is provided for devices. This activation link is used along with appending the MDM device identifier. The MVISION Mobile Console page displays the expiration date and time, and if needed the link can be regenerated.

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 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.

Activation with MobileIron Messaging

MobileIron supports message templates where a customized email can be sent to users. This is an optional activation method. See [“Appendix A - MobileIron Messaging and Device Activation”](#) for information on how to set up these notifications.

Setting up the VPN Profile for MVISION Mobile

VPN-based notifications for MVISION Mobile launch on iOS devices that are managed by MobileIron Cloud MDM is a new capability. Using this capability, end-users that had MVISION Mobile pushed to their devices from the MDM, but have not activated it yet, receive a popup notification, and also a customizable web page when the user visits an HTTP URL, which directs them to open the MVISION Mobile app. This is done by silently pushing a local on-device VPN to the device which remains active only until MVISION Mobile is activated. Upon activation, the VPN is automatically uninstalled from the device.

The local on-device VPN does not block or tunnel any outgoing traffic from the device except when the end-user visits an HTTP website, in which case a customizable HTML page is displayed prompting the user to activate MVISION Mobile. Once MVISION Mobile is activated, the VPN is automatically and silently removed from the device.

Configuring the VPN Profile in MobileIron Cloud

The VPN Profile is the next step and is configured in the MobileIron Console. See the MobileIron documentation for these steps.

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.*

Configuring iOS Devices

These steps are performed in the MobileIron Cloud. There are several files from Zimperium which are required in these steps, and are shown below:

1. Obtain the `mvision_vpn_app_launch` file from your McAfee Customer Success contact. Upload the `mvision_vpn_app_launch` file as part of the new profile definition. Edit/add to key-value pairs in the **VendorConfig** section as needed:
 - a. `enable_auth_redirect`: true (Values of true or false. Controls redirecting HTTP URLs to a customized web page requesting the user to launch the MVISION Mobile app.)
 - b. `enable_auth_notifications`: true (Values of true or false. Controls display of the local notification message requesting the user to launch the MVISION Mobile app.)
 - c. `auth_custom_notification_title` (Optional): (Open the app to activate. The default notification title can be changed to a custom title if desired.)
 - d. `auth_custom_notification_message` (Optional): (Open the app to activate mobile threat defense on the device. The default notification message can be changed to a custom message, if desired.)

- e. `auth_custom_html_base64` (Optional): (The user can set a custom HTML page to display when an HTTP site is accessed, and it needs to be Base-64-encoded before entering it in this field.)
 - f. `auth_redirect_url` (Optional): (This is the redirect URL which is used to launch the app on the iOS device. Default value is `mvisionmobile://login`.) The redirect URL value can be customized. For example, the redirect URL to use with the McAfee MVISION Mobile app is:
`mvisionmobile://login`
2. The next step is to associate the configuration with a device group that is assigned as a “Pending activation” device up until the point the user activates MVISION Mobile. Once MVISION Mobile is activated, the user is automatically removed from this group, based on the policy that is set up in the next section.
 3. Save the configuration.

Configure 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. Scroll down to the **Device Pending Activation** event.
3. Under the **MDM Action** drop-down list, select the MDM device group that the custom VPN configuration in MobileIron Core was associated with. Choose **Remove** for MDM Mitigation Action.

DEVICES	<input checked="" type="checkbox"/>	Low	Device Pending Activation	<input type="checkbox"/>	<input type="checkbox"/>	VPN App Launch	Remove	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
PROFILES	<input checked="" type="checkbox"/>	Elevated	Device Pin	<input type="checkbox"/>	<input type="checkbox"/>	No Action	No Action	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
USERS	<input checked="" type="checkbox"/>	Normal	DNS Change	<input type="checkbox"/>	<input type="checkbox"/>	No Action	Unavailable	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
	<input checked="" type="checkbox"/>	Elevated	Elevation of Privileges (EOP)	<input type="checkbox"/>	<input type="checkbox"/>	Select an Option	Unavailable	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

4. Deploy the policy.
5. Run a manual sync so new devices enrolled in MDM to get synced with the MVISION Mobile Console and show up in “Pending activation” state.
6. After the dormancy period has passed (as defined in the **Manage** and **General** section of the MVISION Mobile Console as “Allowed Inactivity Time”), a “Device Pending Activation” event should get triggered for the newly synced devices that have not yet activated MVISION Mobile.

VPN Auto-install and MVISION Mobile Activation on Device

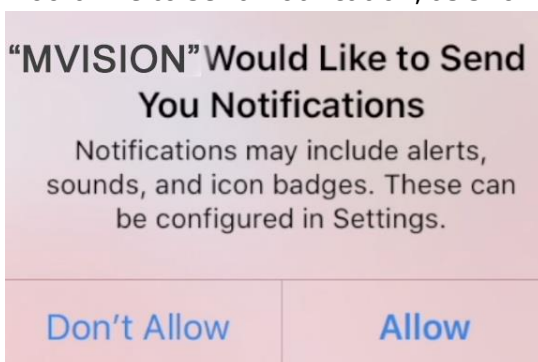
On the end user device where MVISION Mobile was pushed from the MDM and installed, but not yet activated, it still has to be activated on the device. Once the “Device Pending Activation” event gets generated on the console, the MVISION Mobile VPN is silently pushed

to the device and turned ON. This is because of the MDM action that was set in the steps above. The following steps shows how to activate MVISION Mobile on the device:

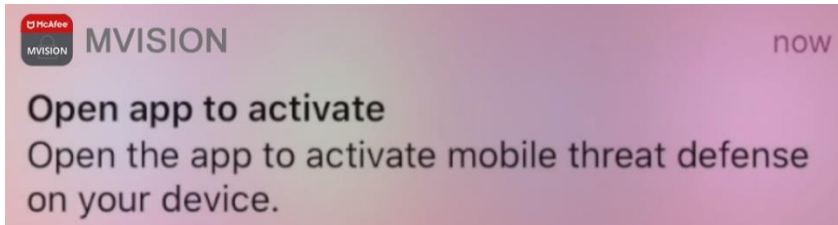
1. As shown in the screenshot below, the VPN being turned on is indicated in the notification area at the top.



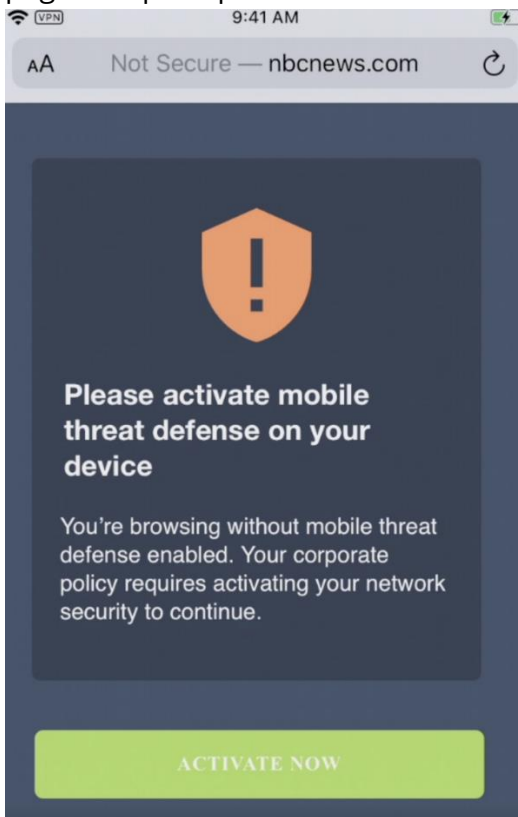
2. As a result, the end user receives a notification popup saying, MVISION Mobile would like to send notification, as shown below:



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 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 (for example, by typing a URL that has not been visited previously on their device, such as apache.org or tomcat.com.) MVISION 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 VPN is automatically uninstalled silently from the device by the MVISION Mobile Console MDM Mitigation Action to remove the device from the "Pending Activation" group.

Device Actions

The MVISION Mobile integration with MobileIron provides the ability to apply a specific Device Group to the device within the customer's MobileIron environment. This allows the MobileIron administrator to define specific actions such as:

- Quarantine a device
- Remove email access
- Assign a configuration
- Unenroll a device (which happens automatically)

To accomplish this, the MobileIron administrator needs to coordinate with the MVISION Mobile Console administrator the specific actions that are needed and do the following configuration for each one with a unique Device Group. MDM Integration with MVISION Mobile Console also has to be set up and functional.

The MobileIron Cloud integration contains one built-in MDM action to Lock the device. The following steps are not needed for that action to be used.

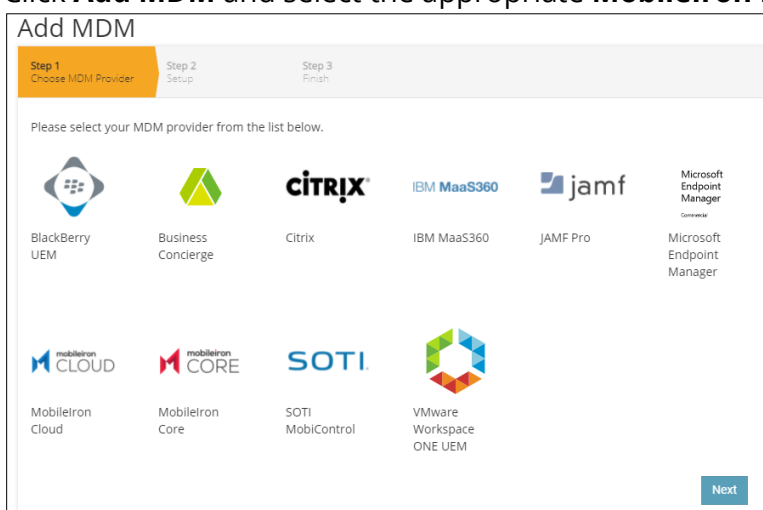
When a device is under attack and the MDM action is set to some Device Group from the integrated MobileIron server, MVISION Mobile Console assigns the device to that device group via API calls. To set this up several configurations need to be done on the MobileIron Console. Refer to the MobileIron documentation for these steps.

NOTE: *For each option selected, an appropriate entry is displayed to enter more information, such as the text to be sent to the user if 'Send Push Notification' is chosen. More than one action can be chosen by clicking on the plus sign '+' sign to add another action.*

Common Steps Setting Up Synchronization in MVISION Mobile Console

This section describes the common steps to set up synchronization in MVISION Mobile Console. These common steps describe the setup of both MobileIron Core and MobileIron Cloud MDM in MVISION Mobile Console. The MVISION Mobile Console application uses labels for MobileIron Core and device groups in MobileIron Cloud to synchronize devices and associate users to MVISION Mobile Console.

1. Log into MVISION Mobile Console
2. Navigate to **Manage > Integrations** and select **MDM**.
3. Click **Add MDM** and select the appropriate **MobileIron** icon.



4. Enter information pertinent for your MobileIron integration. The table provides a description of the fields for this step.

Add MDM

Step 1
Choose MDM Provider
Step 2
Setup
Step 3
Finish

URL
Specify URL for this MDM provider.

Username
Specify username for this MDM provider.

Password
Specify password for this MDM provider.

MDM Name
Specify a unique name for this MDM provider.

Whitelist MDM Managed Apps
By enabling this option, zConsole will automatically add MDM managed iOS and Android apps to the whitelist. Whitelisted apps are not reported as threats.

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

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

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

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

Next

Item	Specifics
URL	URL of the MobileIron API Server
Username	MobileIron Administrator created with the API role access
Password	The password of the MobileIron Administrator
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This is prepended to the group name to form the MVISION Mobile group name.
Background Sync	Check this box to ensure users/devices are synchronized with the MobileIron Labels chosen on the next page.
Whitelist MDM Managed Apps	Check this box to automatically add MDM managed iOS and Android apps to the whitelist. Whitelisted apps are not reported as threats.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, for instance, name and email address.
Send Device Activation email via MVISION Mobile Console for iOS Devices	Check this box to send an email to the user for every iOS device synced with the MDM.

Send Device Activation email via MVISION Mobile Console for Android Devices	Check this box to send an email to the user for every Android device synced with the MDM.
--	---

5. Click **Next** and in the Space field, choose **MobileIron**.
6. Choose the groups to synchronize. These groups are labels in MobileIron Core and Device Groups in MobileIron Cloud.
7. Click **Finish**.

NOTE: Spaces are used to separate managed entities for the ease of administration, such as an organizational hierarchy. Now users can sync devices for MobileIron spaces, along with the default space. When more than one label is chosen the highest label in the list has the highest priority and so on down the list. If a device is present in more than one label, the label that applies is the highest label for the device.

NOTE: When more than one group (label for MobileIron Core) is chosen the highest one in the list has the highest priority and so on down the list. If a device is present in more than one group (or label), the one that applies is the highest in the list for the device.

Appendix A - MobileIron Messaging and Device Activation

MobileIron Cloud supports messaging where to send a customized email to users. This is an optional activation method. This details the steps to configure a message template to send an email after the user's device is successfully enrolled.

Perform the following steps to set up an email after the user's device is enrolled:

1. Login to MobileIron Cloud at this website:
<https://na2.mobileiron.com>
2. Click **Policies** from the top menu.
3. Click **+ Add** to add a new policy.
4. Select **Custom Policy**.
5. Give a name to the new policy and select the policy condition that the rule of 'MDM Managed' is set to 'Yes' and the policy displays like this sample figure.

The screenshot displays the 'Custom Policy' configuration interface in MobileIron Cloud. The top navigation bar includes 'Dashboard', 'Users', 'Devices', 'Apps', 'Content', 'Configurations', 'Policies', and 'Admin'. The left sidebar shows 'Add Policy' and 'Cancel' buttons, along with a progress indicator for '1 Settings' and '2 Distribute'. The main content area is titled 'Custom Policy' with the instruction 'Create a custom policy. Set conditions and specify related actions.' Under 'Policies and Compliance Setup', the 'Name' field is filled with 'Demo Custom Policy'. Below this is a '+ Add Description' link. The 'Define Conditions' section includes a 'Learn more about Custom Policies' link and a 'Reset All' button. A condition is set: 'ANY ALL of the following rules are true:'. A single rule is defined: 'MDM Managed' is equal to 'Yes'. The summary below the rule states 'MDM Managed is equal to Yes'. Navigation buttons 'Back' and 'Next' are at the bottom.

6. Scroll down and click Send Email action.
7. Provide the required email subject and the body text. Here's an example of the email text snippet with an HTML link for the activation link.
After you have installed the MVISION Mobile app, click the link below to activate MVISION Mobile.
Activation Link:
<a href="https://acceptor.mcafee-mvision-mobile.com/activation?token=U2FsdGVkX183
. . .

bMGBnrSpI-kEIuvSE6olwZQREymFRi9h1VRMlFos&MDM_ID=\${devicePK}">Click here to activate MVISION Mobile

Note: The activation URL has the MDM identifier of \${devicePK} added to the end of the URL and is in bold above.

8. Click the checkbox in the confirmation box.
9. Click **Next**.
10. Choose the option of which devices receive the email:
 - a. All Devices
 - b. No Devices
 - c. Custom
11. Click **Done**.

This table provides the specific device identifier needed for the MDM_ID field.

MDM System	MDM Device Identifier Variable
MobileIron Core	Core: \$DEVICE_UUID\$
MobileIron Cloud	Cloud: \${devicePK}

MobileIron supports messaging where the administrator can tailor the MDM invitation email to a new user. This is changing the default email that the MDM sends. This details the steps to configure a message template to change the text for the MDM invitation email.

Perform the following steps to set up the specific text for the invitation email to a new user.

1. Login to MobileIron Cloud on this website: <https://na2.mobileiron.com>
2. Click **Admin** from the top menu.
3. Click **Email Templates**.
4. Select **End User Invitation**.
5. Select the desired language/localization and edit the template text.
6. Provide the email subject text and body.
7. Click **Preview** and **Save** when complete.

This figure shows the editing of this template.

Dashboard
Users
Devices
Apps
Content
Configurations
Policies
Admin

Admin

System
Attributes
Common Platform Services
Notifications
Notification Emails
Spaces
Support Administrators
System Use Notification
Roles Management
Infrastructure
Access
Audit Trails
App Lists
App Reputation
Certificate Authority
Connector

End User Invitation Email Templates

Edit - English Email Invitation without a PIN
From: The MobileIron Team <no-reply@mobileiron.com>
Reply To:
Subject Line
You've been invited!

Edit your email here. You can PREVIEW at any time. From the Preview screen you can SAVE or return here to make additional edits. You can also test your custom email template after it has been saved.

Cancel
Preview

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>\${productBrandName}</title>
<style>
* {

Recommended Variables

These variables are recommended because they contain important registration information typically included in End User invitation emails :

- ✓ \${userActivationUrl} ?
- ✓ \${clusterRegistrationUrl} ?
- ✓ \${endUserPortalUrl} ?

Supported Variables

The following variables are also supported :

- ✓ \${productBrandName} ?
- ✓ \${companyLogoUrl} ?

NOTE: *This template does not have any device-specific information.*

Appendix B - Sample Configuration File for Zero-Touch Activation

This is a sample XML file for the zero-touch activation. You need to get the default file and values for the keys from your Customer Success team member.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>IPv4</key>
            <dict>
                <key>OverridePrimary</key>
                <integer>0</integer>
            </dict>
            <key>PayloadDescription</key>
            <string>Configures VPN settings, including
authentication.</string>
            <key>PayloadDisplayName</key>
            <string>VPN (VPNText)</string>
            <key>PayloadIdentifier</key>
            <string>com.apple.vpn.managed.E8157946-601C-40DE-8067-
71903FAA0FA5</string>
            <key>PayloadOrganization</key>
            <string></string>
            <key>PayloadType</key>
            <string>com.apple.vpn.managed</string>
            <key>PayloadUUID</key>
            <string>E8157925-601C-40ED-8067-71903FAA0FA5</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
            <key>Proxies</key>
            <dict/>
            <key>UserDefinedName</key>
            <string>VPNText</string>
            <key>VPN</key>
            <dict>
                <key>AuthenticationMethod</key>
                <string>Certificate</string>
                <key>OnDemandEnabled</key>
                <integer>1</integer>
                <key>OnDemandRules</key>
                <array>
                    <dict>
                        <key>Action</key>
                        <string>Connect</string>
                    </dict>
                </array>
                <key>RemoteAddress</key>
                <string>localhost</string>
            </dict>
            <key>VPNSubType</key>
            <string> com.mcafee.mvision.mobile</string>
        </dict>
    </array>
</dict>
```

```

<key>VPNTType</key>
<string>VPN</string>
<key>VendorConfig</key>
<dict>
    <key>MDMDeviceID</key>
    <string>{{AADDEVICEID}}</string>
    <key>assume_vpn_permission_granted</key>
    <string>true</string>
    <key>auth_custom_html_base64</key>
    <string>Activate now</string>
    <key>auth_custom_notification_title</key>
    <string>Launch MVISION Mobile</string>
    <key>defaultchannel</key>
    <string>https://uat-acceptor.mcafee-mvision-
mobile.com/srx/json</string>
    <key>enable_auth_notification</key>
    <string>true</string>
    <key>enable_auth_redirect</key>
    <string>true</string>
    <key>tenantid</key>
    <string>710EB8FE-83BD-4BD9-98D5-3F60B3CF1859</string>
</dict>
</dict>
</array>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>VPNCustomText/V_1</string>
<key>PayloadIdentifier</key>
<string>6aca860d-05fc-4fbe-8c02-058d872b3fa6</string>
<key>PayloadOrganization</key>
<string></string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>02EE5F2D-4F3B-4E56-9EE1-2D22BDCE102A</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>

```