

McAfee MVISION Mobile

Microsoft Endpoint Manager

Integration Guide

September 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
Integration Modes	6
Prerequisite Requirements	6
About MDM, MAM, and MVISION Mobile Console Communication	7
Device Compliance Overview	7
Device Application Deployment Set Up	9
Configuration Steps	9
Integrate MVISION Mobile with Microsoft Endpoint Manager	10
Creating Groups in the Endpoint Manager Console	10
Creating Users in the Endpoint Manager Console	11
Overview on Setting Up Microsoft MDM or MAM with MVISION Mobile Console	13
Setting up Microsoft MAM Only and MVISION Mobile Console	13
Configuring MVISION Mobile for MAM Only	13
Configuring Endpoint Manager for MAM	14
Configure the MTD Connector Create and Configure the APP Protection Policy Setting Up Microsoft MDM Only and MVISION Mobile Console	14 14 17
Configuring MVISION Mobile for MDM Only	17
On-Demand Device Synchronization for MDM	17
Configuring Microsoft Endpoint Manager and Apps for MDM	17
Setting Up Microsoft MDM and MAM and Mobile Console	19
Configuring MVISION Mobile Console for MDM and MAM	19
Configuring Microsoft Endpoint Manager for MDM and MAM	20
Setting Up a Third-Party MDM + Microsoft MAM and Mobile Console	20
Configuring the Third-Party MDM	20
Configuring MVISION Mobile Console for Third-Party MDM + MAM	20
Configuring Microsoft Endpoint Manager for MAM	22

Configuring Mobile Console for MDM Only, MAM Only, or MDM and MAM	23
Configuring the Device Auto-Activation	26
Activation Steps	26
iOS Activation	27
Android Setup	28
Android Enterprise Setup with App Configuration Policy Setup with the Company Portal App Using Configuration Designer	28 29 29
Android Personal Profile Auto-Activation	30
Configuring for MVISION Mobile and iOS Zero-Touch Activation	30
Overview of the Setup	30
A Sample Flow After the Configuration is Complete	31
Differences in Zero-Touch Activation	31
Setting Up Zero-Touch Activation	31
Updating Your Configuration File Configuring within the Endpoint Manager Console Configuring within the MVISION Mobile Console Enable the Connector in the Microsoft Endpoint Manager Console	31 34 35 36
Configure the MTD Connector	36
Device Actions, Policies, and Remediation	38
Microsoft Endpoint Manager Policies	38
MVISION Mobile Console Policies	39
Appendix A – iOS User Experience for MDM	40
Appendix B – Android User Experience for MDM	41
Appendix C - Sample Configuration File for Zero-Touch Activation	42

Preface

This guide explains the process of integrating the MVISION Mobile Console and Microsoft Endpoint Manager (formerly Intune) Mobile Device Management (MDM) and Mobile Application Management (MAM) software.

Audience

The intended audience for this guide is an MVISION Mobile Console administrator. The MVISION Mobile Console application provides threat protection to mobile devices, and the system administrator sets policies for threats, and 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

When an MDM or MAM is integrated, the MVISION Mobile Console:

- Synchronizes users and devices from the MDM or Azure AD.
- 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, can take actions locally. When MVISION Mobile is integrated with an MDM, protection actions are performed by the MDM, providing a very powerful protection tool. When MVISION Mobile is integrated with MAM, the risk posture is identified as mobile threats are detected when the app is launched.

In detecting an event, the new risk posture level, defined by the severity of the event, is sent to Microsoft Endpoint Manager with secure APIs. Microsoft Endpoint Manager starts a workflow to take specific actions that match the level provided, as defined by the Microsoft Endpoint Manager Administrator.

Different workflows are created to handle different risk posture levels on devices through device compliance policies, and apps policies for security at the application level. With that threat posture from MAM, Microsoft Endpoint Manager blocks the user's access to the protected app. An example of a protected app is Outlook. With this protection it:

- Provides the user with instructions on how to resolve the issue.
- Sends the appropriate device risk posture to Microsoft Endpoint Manager.

Once the risk issue is resolved, it restores access to the app.

Integration Modes

You can set up your integration with the MVISION Mobile Console and Microsoft Endpoint Manager with these different modes:

- MDM only, which supports managed devices.
- MAM only, which supports unmanaged devices.
- MDM and MAM, which supports both managed and unmanaged devices.
- Third-party MDM and Microsoft MAM, which supports MAM for devices managed by a different MDM. This option is only for the MVISION Mobile app.

Prerequisite Requirements

Integration with Microsoft Endpoint Manager requires a connection between the McAfee MVISION Mobile Console and the Microsoft Endpoint Manager API server. This is accomplished via the Internet using SSL on TCP port 443. In a typical Microsoft Endpoint Manager deployment, there are no changes that need to occur for this communication.

The following table details specific requirements for the Microsoft Endpoint Manager integration.

Item	Specifics
Microsoft Endpoint Manager enrolled device	iOS or Android
Android Version	v6.0 or higher
iOS Version	v10.0 or higher
MVISION Mobile Ann for Android	v4.12 or higher
	The MDM with MAM and Third-Party MDM with MAM options require MVISION Mobile 4.17 or higher.
	v4.12 or higher
MVISION Mobile App for iOS	The MDM with MAM and Third-Party MDM with MAM options require MVISION Mobile 4.17 or higher.
Administrator Account for Microsoft Endpoint Manager Console	Initially, the role of "Global Administrator" is required. Once the initial setup is completed, the "Limited Administrator" with the "Intune Administrator" is sufficient.
MS Authenticator on iOS (optional)	If MS Authenticator is used, then SSO on iOS devices is required.
License Granted to User	Ensure that the "Enterprise Mobility + Security E3" or "Enterprise Mobility + Security E5" license is applied to the user created on the Microsoft Endpoint Manager console.

Azure Active Directory Global Administrative Credentials	Must have "Global Administrator" access to sign-in, read the user profile, access the directory, read directory data, and send device information to Microsoft Endpoint Manager.
MVISION Mobile Console Admin Credential	Must have Admin credentials.
Groups	You must set up your groups in Microsoft Endpoint Manager.
MDM Password	Do not use a colon(:) in the MDM password field, or use 'password' as a password value.

About MDM, MAM, and MVISION Mobile Console Communication

McAfee MVISION Mobile integrates with Microsoft Endpoint Manager MDM, and the MVISION Mobile Console is configured to share information with the Microsoft Endpoint Manager console through API access. When MVISION Mobile detects an event, it consults the current Threat Policy on the device, and if there is a specific MDM action defined, this is communicated to the MVISION Mobile Console. The MVISION Mobile Console then reaches out to the proper Microsoft Endpoint Manager API Server and performs the action defined for the device's risk posture level.

McAfee MVISION Mobile integrates with Microsoft Endpoint Manager MAM and the MVISION Mobile Console as an information source for device compliance to evaluate Conditional Access rules based on the risk that often accompanies bring-your-own-device (BYOD) issues that arise with unmanaged devices. In limiting the type of apps that users can have on their own devices (non-company-owned), this integration prevents compromised devices from spreading the malware, or actual security threat, to other devices on the network. When the MAM detects the threat, it removes the device from the network until the threat is resolved and the device is again safe to access the company network.

Device Compliance Overview

McAfee interacts with the Microsoft Endpoint Manager MDM through API's that provide the ability to modify device configurations securely over the internet. Microsoft Endpoint Manager takes specific actions based on the Device Threat Level defined for a device and the Device Health setting shown in the figure. The details of setting this up are in the "Device Actions, Policies, and Remediation" section.

Microsoft Endpoint Manager admin center				
 ≪ ↔ Home ☑ Dashboard ☑ All services 	Home > Devices > Compliance policie iOS MTD Compliance Device compliance policy P Search (Ctrl+/) «	<pre>s > iOS MTD Compliance ce Properties </pre>		
 FAVORITES Devices Apps Endpoint security Reports 	Overview Manage III Properties Monitor	Basics Edit Name iOS MTD Compliance Description		
 Lysers Groups Tenant administration Troubleshooting + support 	 Device status User status Per-setting status 	Platform iOS/iPadOS Profile type iOS compliance policy		

The possible device threat levels are Secured, Low, Medium, and High. The Admin defines the minimally acceptable device threat level in the "Device Health" policy.

These levels correspond to the McAfee MVISION Mobile severity levels:

Microsoft Endpoint Manager Device Threat Level	McAfee MVISION Mobile Threat Level
Secured	Normal
Low	Low
Medium*	Elevated
High	Critical

Note: *McAfee recommends that the user selects the minimally safe device threat level to be Medium.*

The device Risk Posture in the MVISION Mobile Console is the highest severity level of a pending event assigned to a device.

MVISION Mobile sends the device's updated risk posture in response to a threat if the Threat Policy is set to "Inform EMM" for that threat. The severity of the threat is sent to Microsoft Endpoint Manager and matched up with the device threat level on Microsoft Endpoint Manager.

Device Application Deployment Set Up

To deploy the device application, such as McAfee MVISION Mobile, through Microsoft Endpoint Manager, use the app from the App Store for the iOS version and the Google Play Store for the Android version.

Configuration Steps

Some configuration steps are performed on the Microsoft Endpoint Manager side. Other steps are performed for MVISION Mobile Console. After setting up the configuration, the following occurs:

- Devices and their associated users are synchronized through integration
- Device and user management functions are handled at the Microsoft Endpoint Manager console

Synchronization also provides SSO access so that users can utilize their Azure credentials when starting the device application. The Microsoft Authenticator app is optional for the device where MVISION Mobile or a given app is installed. If MS Authenticator is desired, set this app up in Microsoft Endpoint Manager from the App store and assign it to the same iOS devices that are protected by MVISION Mobile.

When an iOS user starts MVISION Mobile, the user is redirected to login through Microsoft Authenticator with their Azure credentials. Android users do not need to have Microsoft Authenticator on their device but still use their Azure credentials to log into MVISION Mobile. See the appendices for information on the iOS and Android user experiences.

For Microsoft Endpoint Manager, the Google Play Store MVISION Mobile link is used with a referrer attribute for MVISION Mobile activation. See the *"Appendix D - Google Play Store MVISION Mobile Link with Referrer Attribute"* in the *"MVISION Mobile Console Configuration 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.

After the initial synchronization during the MDM Integration setup, devices are managed through a scheduled synchronization process that runs every four hours. Any changes in the group(s) being used for synchronization are duplicated at the MVISION Mobile Console. If devices are removed, then they are removed from the MVISION Mobile Console. Doing this does not remove any of the events associated with that device.

Synchronization begins once the connector is available.

This link provides additional information on MAM:

https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq

Important: Do not remove an integration from the MVISION Mobile Console (or, in other words, de-provision an Endpoint Manager connection in the MVISION Mobile Console) if you have multiple Endpoint Manager connections setup in MVISION Mobile Console for the same Endpoint Manager tenant. You can edit the instance, for instance, to remove or add groups. You can remove an integration instance or a connection in MVISION Mobile Console if there is not another connection for the same Endpoint Manager tenant.

Integrate MVISION Mobile with Microsoft Endpoint Manager

This section provides the steps to integrate the MVISION Mobile apps with Microsoft Endpoint Manager. Groups and users need to be set for MDM or MAM integration.

Creating Groups in the Endpoint Manager Console

To create the Groups in the Endpoint Manager Console:

- 1. Log in to the main Microsoft Endpoint Manager console and in the navigation panel and select **Groups.**
- 2. The Groups page is shown listing all the current Groups which are defined. Click + **New group** at the top of the window.
- 3. The **New Group** window opens to allow the creation of a new group. For the **Group type**, select **Security**. This group type is **required** because only groups of this type are synchronized.

New Group	
	1
Group type *	
Security	~
Group name * ①	
Friday Group	✓
Group description ①	
Friday's Group	 Image: A set of the set of the
Membership type * 🛈	
Assigned	~
Owners	
No owners selected	
Members	
No members selected	
Create	

- 4. Enter the **Group name** and enter the **Group description**.
- 5. Select the **Membership type** of **Assigned**.

- 6. If any of the members assigned to this group are already created, click **Members**, and add the users to the group; otherwise, the members are assigned to the Group when the member is created.
- 7. Click the **Create** button, and the listing of all groups opens with the group you added.

Home > Groups All groups						
All groups All Deleted groups	+ New group ↓ Downle	oad groups 📋 🛙	evaluation. View previews -	≡≣ Columns 🐼 Pre	riew features 🛛 🛇 Got fe	edback?
X Diagnose and solve problems	₽ Search groups		+ ₇ Add filters			
Settings	Name	Object Id	Group Type	Membership Type	Email	Source
🐯 General	AC All Company	e2f0c642-423a	Microsoft 365	Assigned	allcompany@mvisionm	Cloud
Expiration	MD MVISION Demo	b8b78f7e-081	Security	Assigned		Cloud
🗱 Naming policy	m mvisionmobile	1554a918-0d3	Microsoft 365	Assigned	mvisionmobile@mvisio	Cloud
Activity						
E Access reviews						
Audit logs						
👶 Bulk operation results						
Troubleshooting + Support						
New support request						

Warning: Nested groups are not synchronized automatically. You must add nested groups manually.

Creating Users in the Endpoint Manager Console

Ensure the user is logged in as a user having the "Global Administrator" role. If the user does not have this role, create an administrator user to use for API access by performing the following steps:

- 1. Log in to Microsoft Endpoint Manager and click **Users** in the navigation panel. The list of users displays.
- 2. Click + New user, and the page opens to create the new user.
- 3. Enter the user information.
- 4. Assign the user to a Group. Click the link for Groups, and search and click the desired Group.

Grou Select gro	ps ups in which this user is to be a member	×
🔎 Sea	rch	
AC	All Company allcompany@mvisionmobile.onmicrosoft.com	
MD	MVISION Demo Selected	
m	mvisionmobile mvisionmobile@mvisionmobile.onmicrosoft.com	
Selected	d groups	
MD	MVISION Demo	Remove

- 5. When all the desired Groups are selected, click the **Select** button.
- 6. The role of the user needs to be selected. Click the link for the Roles and the list of User Roles opens.

Directory roles	
🗌 🍰 Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD i.
🗌 🍰 Global reader	Can read everything that a global administrator can, but not update anything.
🗹 🔥 Groups administrator	Can manage all aspects of groups and group settings like naming and expiratio.
🗌 🍰 Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.
🗌 🎍 Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.
🗌 🍰 Hybrid identity administrator 📕	Can enable, deploy, configure, manage, monitor, and troubleshoot cloud provis.
🗌 🍰 Insights administrator 📕	Has administrative access in the Insights app.
🔲 🍰 Insights business leader 📕	Can view and share dashboards and insights via the M365 Insights app.
🗌 🍰 Intune administrator	Can manage all aspects of the intune product.
🗌 🎍 Kaizala administrator	Can manage settings for Microsoft Kaizala.
🔲 🎍 License administrator	Ability to assign, remove and update license assignments.
🗌 🍰 Message center privacy reader	Can read Message Center posts, data privacy messages, groups, domains and s
Select	

- 7. Select the desired role(s) for the user, click the **Select** button.
- 8. Set the settings and Job Info values.

- 9. Click the **Create** button to define the user. The list of all defined users displays.
- 10. Assign the License to the User.

Overview on Setting Up Microsoft MDM or MAM with MVISION Mobile Console

Configuring the MVISION Mobile Console is required and needed to have:

- MVISION Mobile login to the MVISION Mobile backend server
- Device and user synchronization (for MDM)

This table describes the modes for Microsoft Endpoint Manager MDM and MAM.

Mode	Section Link
MDM only, which supports managed	See the <u>Setting Up Microsoft MDM Only and MVISION</u>
devices	Mobile Console section for details.
MAM only, which supports	See the <u>Setting Up Microsoft MAM Only and MVISION</u>
unmanaged devices	Mobile Console section for details.
MDM and MAM, which supports both	See the Setting Up Microsoft MDM and MAM and
managed and unmanaged devices	MVISION Mobile Console section for details.
Third-party MDM and Microsoft	See the Setting Up Third-Party MDM and Microsoft
MAM, which supports MAM for	MAM and MVISION Mobile Console section for details.
devices managed by a different MDM	

Important: Do not remove an integration from the MVISION Mobile Console (or, in other words, de-provision an Endpoint Manager connection in the MVISION Mobile Console) if you have multiple Endpoint Manager connections setup in MVISION Mobile Console for the same Endpoint Manager tenant. You can edit the instance, for instance, to remove or add groups. You can remove an integration instance or a connection in MVISION Mobile Console if there is not another connection for the same Endpoint Manager tenant.

Setting up Microsoft MAM Only and MVISION Mobile Console

Configuring Microsoft MAM involved setting up MVISION Mobile Console and Microsoft Endpoint Manager. These sections describe those configurations.

Configuring MVISION Mobile for MAM Only

After setting up groups and users, the next step is connecting the Microsoft Endpoint Manager environment to the MVISION Mobile Console.

Perform the steps in the section "<u>Configuring MVISION Mobile Console for MDM Only, MAM</u> <u>Only, or MDM and MAM</u>" to set up the MVISION Mobile Console integration for MAM. Then continue through this section and complete these steps.

Configuring Endpoint Manager for MAM

After setting up the MVISION Mobile Console, the next step is configuring the Microsoft Endpoint Manager environment for MAM. You must:

- Configure the MTD Connector
- Create the App Protection Policies

Configure the MTD Connector

Warning: If you migrate from the Zimperium connector to the MVISION Mobile connector, active devices change from "Pending Activation" status to "Active" the next time the device checks-in with the MVISION Mobile Console.

Perform these steps to set up the MTD Connector properties:

- 1. Login to Microsoft Endpoint Manager.
- 2. Click and navigate to **Tenant Administration** > **Connectors and tokens** > **Mobile Threat Defense**.
- 3. Click **McAfee MVISION Mobile** as the MTD Connector.
- Under the MDM Compliance Policy Settings section, consider turning on the sliders for Connect Android Devices, Connect iOS Devices, and Enable App Sync for iOS Devices.
- Make sure the sliders for Connect Android Devices and Connect iOS Devices are set to On in the App Protection Policy Settings area. This forces the Microsoft Office 365 apps to check for the device threat level provided by MVISION Mobile before launching.



Create and Configure the APP Protection Policy

Perform these steps to set up the app protection policy for both iOS and Android:

- 1. Login to Microsoft Endpoint Manager.
- 2. Click and navigate to **Apps > Apps Protection Policies**.
- 3. Click + Create policy
- 4. Select the type of policy, either **iOS/iPadOS or Android**.
- 5. Type a unique policy name and click **Next**.
- 6. Change the **Target to Apps on all Device Types** toggle to **No**.
- 7. Set the **Device Types** to **Unmanaged**.
- 8. Under the **Public Apps** section, click **+ Select Public Apps** and search and select one or more apps to target and click **Select**. This figure shows Microsoft Outlook selected.

Home > Apps >			Se	lect apps to targ	et ×
Create policy				11 5	
			Sea	irch by Bundle ID	~
V Basics 2 Apps 3 Data p	rotection (4) Access requirements (5)	Conditional launch 6 Assignments 7	Review + cre	Microsoft Outlook	•
Choose how you want to apply this policy	to apps on different devices. Then add at least one	e app.		Microsoft Planner	
Target to apps on all device types 🕕	Yes 🖉	No	60	Microsoft Power Apps	
Device types * ()	Unmanaged	\checkmark		Microsoft Power BI	
			2	Microsoft PowerPoint	
Public apps	Remove		-		·
No public apps selected			Selec	ted Apps:	
+ Select public apps			w	Microsoft Word	Remove
Custom apps	Remove		×	Microsoft Excel	Remove
No custom apps selected				Microsoft PowerPoint	Remove
+ Select custom apps			0	Microsoft Outlook	Remove
Previous Next					
4			2	Select	

NOTE: For a list of the currently supported MAM apps, see this website: <u>https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps</u>

- 9. After selecting the desired app(s) to target, click the **Next** button.
- 10. The **Data Protection** tab configures settings that dictate how the managed apps interface with other apps on the device. Select the settings that meet your organization's requirements and then click **Next**.
- 11. The **Access Requirements** tab configures settings that dictate how apps are launched on the device. Select the settings that meet your organization's requirements. Consider the defaults as a good baseline and then click **Next**.
- 12. The **Conditional Launch** tab configures the device conditions. In the Device Conditions section, add a setting for **Max Allowed Device Threat Level**. Select the maximum value and desired action for when the threat threshold is crossed and click **Next**. This figure shows this being set.

Important: This setting is key and links McAfee MVISION Mobile MTD to the device's threat posture. If Microsoft Endpoint Manager does not have a threat posture for the device, it communicates with the app through the SDK to alert the user to install the

McAfee MVISION Mobile app. The user is then unable to use the managed app until they install and activate MVISION Mobile.

Basics Anns	Data protection	s requirements 5 Conditional law	inch
• busies • Apps •		conditional ind	
et the sign-in security requirement a sign in to your company app. The nultiple actions can be configured f	s for your access protection polic on select the Action you want to for a single setting. Learn more a	cy. Select a Setting and enter the Value that take if users do not meet your requiremen bout conditional launch actions.	at users must me ts. In some cases,
pp conditions			
Setting	Value	Action	
Max PIN attempts	5	Reset PIN	
Offline grace period	720	Block access (minutes)	
Offline grace period	90	Wipe data (days)	
Select one	\sim		
onfigure the following conditional	launch settings for device based	conditions through your app protection p	olicy.
onfigure the following conditional imilar device based settings can be nrolled devices.	launch settings for device based configured for enrolled devices.	conditions through your app protection p Learn more about configuring device com	olicy. pliance settings f
Important! Make sure your Me on threat evaluations from the Learn more about Mobile Threa.	launch settings for device based configured for enrolled devices. oble Threat Defense Connector is s connected Mobile Threat Defense s at Defense for unenrolled devices.	conditions through your app protection p Learn more about configuring device com et up in order to properly secure your organiza ervices.	olicy. pliance settings f ation's data based
The second	launch settings for device based configured for enrolled devices. bbile Threat Defense Connector is si connected Mobile Threat Defense s at Defense for unenrolled devices. Value	conditions through your app protection p Learn more about configuring device com et up in order to properly secure your organiza ervices. Action	olicy. pliance settings f
Generations Generation	launch settings for device based configured for enrolled devices. abile Threat Defense Connector is s connected Mobile Threat Defense s at Defense for unenrolled devices. Value	conditions through your app protection p Learn more about configuring device com et up in order to properly secure your organiza rervices. Action Block access	olicy. pliance settings f ation's data based
infigure the following conditional imilar device based settings can be norlied devices. Important! Make sure your Ma on threat evaluations from the Learn more about Mobile Three Setting Jailbroken/rooted devices Max allowed device threat level	launch settings for device based a configured for enrolled devices. abbile Threat Defense Connector is si at Defense for unenrolled devices. Value Value Medium	conditions through your app protection p Learn more about configuring device com et up in order to properly secure your organize ervices. Action Block access Slock access	olicy. pliance settings f ation's data based

 The Assignments tab assigns the policy to the group or groups of users and devices. Click +Select Groups to Include and choose the desired group(s) and click Next.

Home > Apps > Create policy	Select groups to include Azure AD Groups	×
✓ Basics ✓ Apps ✓ Data protection ✓ Access requireme		
Included groups	BY BYOD-Android	
Selected groups No groups selected	DG Demo-MAM Group	
+ Select groups to include Excluded groups	DG Demo-MDM Group	
When excluding groups, you cannot mix user and device groups across include a	Selected items	
Selected groups	DG Demo-MAM Group	Remove
No groups selected		
+ Select groups to exclude		
Previous	Select	

- 14. Review the policy settings and click **Create** to add the policy.
- 15. Repeat these steps and create an app protection policy for the other platform, either **iOS/iPadOS** or **Android**, depending on what you chose for the first policy.

If you selected the MAM only mode, you now have the MAM configuration for Microsoft Endpoint Manager integration with McAfee MVISION Mobile MTD complete.

Setting Up Microsoft MDM Only and MVISION Mobile Console Configuring MVISION Mobile for MDM Only

Warning: If you configured a Microsoft Endpoint Manager integration in the MVISION Mobile Console before the 4.28.13 release, that integration uses the Zimperium connector in Microsoft Endpoint Manager. If you migrate from the Zimperium connector to the MVISION connector, active devices change from "Pending Activation" status to "Active" the next time the device checks in with MVISION Mobile Console.

For MVISION Mobile Console Release 4.28.13, configuring any new Microsoft Endpoint Manager integration sets up the integration to use the MVISION connector in Microsoft Endpoint Manager.

For MVISION Mobile Console Release 4.30.x or later, configuring any new Microsoft Endpoint Manager integration sets up the integration to use the MVISION connector in Microsoft Endpoint Manager for the first integration. Or, for additional integrations, it uses the same connector in Microsoft Endpoint Manager that you had previously.

After setting up groups and users, the next step is connecting the Microsoft Endpoint Manager environment to the MVISION Mobile Console.

Configuring the MVISION Mobile Console is required and needed to have:

- Device and User synchronization
- MVISION Mobile Console login

Perform the steps in the section "<u>Configuring MVISION Console for MDM Only, MAM Only,</u> <u>or MDM and MAM</u>" to set up the MVISION Mobile Console Integration. Then continue through the remaining sections here to configure the Microsoft Endpoint Manager and synchronization.

On-Demand Device Synchronization for MDM

Due to the four-hour synchronization window, there are times when a newly enrolled device has the MVISION Mobile app pushed down to their device and attempts to start it prior to the device actually being synchronized with the MDM. This is not an issue when integrated with Microsoft Endpoint Manager, MVISION Mobile handles on-demand device synchronization with single sign-on via Microsoft Azure and Microsoft Endpoint Manager services. To handle this, auto activation has to be enabled. This is covered in the "Configuring the Device Auto-Activation" section.

Configuring Microsoft Endpoint Manager and Apps for MDM

Perform the following steps:

- 1. Login to Microsoft Endpoint Manager.
- 2. Navigate to **Apps**.
- 3. Then click **All Apps** and **+ Add**.
- 4. Choose the **App Type** of iOS store app or Android store app and click **Select**.

Home > Apps Apps All apps		Select app type ×
Search (Cmd+/) «	$+$ Add 💍 Refresh $~ ar{ abla}$ Filte	App type
(i) Overview		Store app
All apps	Name 1	Android store app
Monitor	Acrobat Reader for Intune And	iOS store app
By platform	Adobe Acrobat Reader for Micr	Microsoft store app
Windows	Cisco Jabber for Intune	Managed Google Play app
iOS/iPadOS	Company Portal	Microsoft 365 Apps
🖵 macOS	Intune Company Portal	Windows 10
Android	Intune Managed Browser	macOS
Policy	Intune Managed Browser Andr	Microsoft Edge, version 77 and later
App protection policies	Jabber for Intune	Windows 10
App configuration policies	Managed Home Screen	macOS
iOS app provisioning profiles	Microsoft Authenticator	Microsoft Defender ATP
S mode supplemental policies	Microsoft Excel	macOS
Policies for Office apps	Microsoft Excel Android	Other
Policy sets	Microsoft Intune	Select Cancel
-		

- 5. Search the App Store for **McAfee MVISION Mobile** and then click the **Select** button.
- 6. In the **App Informatio**n tab, enter the **Information URL** and then select the **Next** button.

Home > Apps >	
Add App	
App information 2 Assign	nments ③ Review + create
Select app * 🥡	Search the App Store
Name * 🕡	McAfee MVISION Mobile
Description * (i)	NOTE: McAfee MVISION Mobile is an enterprise solution. Please consult with your company's IT organization before downloading this app. McAfee
Publisher * 🛈	McAfee, LLC.
Appstore URL	https://apps.apple.com/us/app/mcafee-mvision-mobile/id1435156022?uo=4
Minimum operating system * 🛈	ios 8.0 V
Applicable device type * (i)	2 selected V
Category 🛈	0 selected V
Show this as a featured app in the Company Portal ③	Yes No
Information URL ①	Enter a valid url
Privacy URL ①	Enter a valid url
Developer (i)	
Owner (i)	
Notes ①	
Logo 🛈	Change image

- 7. In the **Assignments** tab, select one or more groups.
- 8. Review the settings and click **Create**.
- 9. Repeat these steps for the other platform, either iOS or Android.

Setting Up Microsoft MDM and MAM and Mobile Console

This option allows you to use the Microsoft MDM and also use the Microsoft MAM functionality.

Configuring MVISION Mobile Console for MDM and MAM

After setting up groups and users, the next step is connecting the Microsoft Endpoint Manager environment to the MVISION Mobile Console.

Configuring MVISION Mobile Console is required and needed to have:

- Device and User synchronization (with MDM)
- MVISION Mobile Console login

Perform the steps in the section "<u>Configuring MVISION Mobile Console for MDM Only, MAM</u> <u>Only, or MDM and MAM</u>" to set up the MVISION Mobile Console Integration. Then continue through the remaining sections here to configure the Microsoft Endpoint Manager and synchronization.

Configuring Microsoft Endpoint Manager for MDM and MAM Step through these other sections in this document.

MDM Setup:

- Reference this section for information on device synchronization "<u>On-Demand</u> <u>Device Synchronization for MDM</u>."
- Configure the apps for MDM. See "<u>Configuring Microsoft Endpoint Manager and</u> <u>Apps for MDM</u>" for these steps.

MAM Setup:

- Configure the MTD Connector. See "<u>Configure the MTD Connector</u>" for these steps.
- Create the App Protection Policies. See "<u>Create and Configure the App Protection</u> <u>Policy</u>" for these steps.

Setting Up a Third-Party MDM + Microsoft MAM and Mobile Console

This option allows you to use an MDM other than Microsoft's MDM, and also use Microsoft's MAM functionality.

Configuring the Third-Party MDM

Configure your third-party MDM integration. Refer to the documentation on the Zimperium Support Portal for information on other MDM integrations. The link to the portal is in this section "<u>Related Documentation</u>."

Configuring MVISION Mobile Console for Third-Party MDM + MAM

After setting up groups and users, the next step is connecting the Microsoft Endpoint Manager environment to the MVISION Mobile Console.

Perform these steps to set up the MVISION Mobile Console Integration:

- 1. Login to the MVISION Mobile Console.
- 2. Navigate to the Manage page and select the Integrations > MDM tab.
- 3. Click Add MDM and select the Microsoft Endpoint Manager icon.

Add MDM					
Step 1 Choose MDM Provider	Step 2 Setup	Step 3 Finish			
Please select your M	DM provider from the	list below.			
		CITRIX	IBM MaaS360	🗾 jamf	Microsoft Endpoint Manager Correctai
BlackBerry UEM	Business Concierge	Citrix	IBM MaaS360	JAMF Pro	Microsoft Endpoint Manager
mobileiron CLOUD		SOTI			
MobileIron Cloud	MobileIron Core	SOTI MobiControl	VMware Workspace ONE UEM		
					Next

4. The next step is to add the 'MVISION Console', the 'MVISION Mobile iOS', and the 'MVISION Mobile Android' applications to the Azure Active Directory to enable the integration.

Add MDM					
Step 1 Choose MDM Provider	tep 2 Idd McAfee MVISION to AD	Step 3 Setup	Step 4 Finish		
Add the MVISION Mobile i on.	iOS, MVISION Mobile A	ndroid and MVISION	N Console applications to your Azu	ure Active Directory to enable a seamless i	ntegration with single sign-
MVISION Console	Add to Azure Activ	e Directory			
MVISION Mobile iOS	Add to Azure Activ	e Directory			
MVISION Mobile Android	Add to Azure Act	ive Directory			
					Next

a. To add the MVISION Console, click the **Add to Azure Active Directory** button for each.

The Microsoft sign-in window opens. Enter the login and password.

Note: You must authenticate successfully for all three for the integration to work successfully.

- b. The next step is to accept permission for the connection.
- c. Repeat these steps for MVISION Mobile iOS and MVISION Mobile Android.
- d. Verify that all the MVISION Mobile Console, MVISION Mobile iOS, and MVISION Mobile Android apps are accepted.
- 5. Click the **Next** button and the Add MDM **Step 3 Setup** window opens.
- 6. Select the **Third-Party MDM + Microsoft MAM** option.

dd MDM				
tep 1 hoose MDM Provider	Step 2 Add McAfee MVISION to AAD	Step 3 Setup	Step 4 Finish	
Node:				Third-Party MDM + Microsoft MAM - Support MAM for devices
his is the Azure Active Specify Tenant ID. It	Directory (AAD) ID. is the Azure Active Director	ry's Directory ID		7554c558-61aa-4e01-b90a-4534a2a3b945
MDM Name Specify a unique nar	ne for this MDM provider.			3rd Party MDM Demo

- 7. Type a unique name in the **MDM Name** field for the environment.
- 8. The integration window closes, and the MDM is added to the list of integrations.

	Demo-MAM Group
Microsoft	
Endpoint Manager	
Commercial	
https://graph.windows.net/	If a user is a member of more then one MDM group, the user
	will be placed in the zConsole group with the higher priority.

Note: The MAM ID in the MVISION Mobile Console is populated after launching MVISION Mobile from a MAM app.

Configuring Microsoft Endpoint Manager for MAM

After setting up the MVISION Mobile Console, the next step is configuring the Microsoft Endpoint Manager environment for MAM. You must:

- Configure the MTD Connector. See "<u>Configure the MTD Connector</u>" for these steps.
- Create the App Protection Policies. See "<u>Create and Configure the App Protection</u> <u>Policy</u>" for these steps.

Configuring MVISION Mobile Console for MDM Only, MAM Only, or MDM and MAM

After setting up groups and users, the next step for several modes is connecting the Microsoft Endpoint Manager environment to the MVISION Mobile Console.

Warning: If you configured a Microsoft Endpoint Manager integration in the MVISION console prior to the 4.28.13 release, then that integration is using the Zimperium connector in Microsoft Endpoint Manager. If you migrate from the Zimperium connector to the MVISION connector, active devices change from "Pending Activation" status to "Active" the next time the device checksin with MVISION Mobile Console.

Configuring any new Microsoft Endpoint Manager integration in MVISION Mobile Console Release 4.28.13 or later, sets up the integration to use the MVISION connector in Microsoft Endpoint Manager.

Perform these steps to set up the MVISION Mobile Console Integration:

- 1. Login to MVISION Mobile Console.
- 2. Navigate to the **Manage** page and select the **Integrations** > **MDM** tab.
- Click Add MDM and select the Microsoft Endpoint Manager Commercial icon.
 Add MDM



4. The next step is to add the 'MVISION Console', the 'MVISION Mobile iOS', and the 'MVISION Mobile Android' applications to the Azure Active Directory to enable the integration.

Add MDM				
Step 1 Choose MDM Provider	tep 2 Idd McAfee MVISION to IAD	Step 3 Setup	Step 4 Finan	
Add the MVISION Mobile i on.	iOS, MVISION Mobile A	ndroid and MVISION	Console applications to your Azure Active Directory to enable a seamless integration with single si	gn-
MVISION Console	Add to Azure Active	e Directory		
MVISION Mobile iOS	Add to Azure Active	e Directory		
MVISION Mobile Android	Add to Azure Act	ive Directory		
			Ne	xt

a. To add the MVISION Console, click the **Add to Azure Active Directory** button for each.

The Microsoft sign-in window opens. Enter the login and password.

Note: You must authenticate successfully for all three for the integration to work successfully.

- b. The next step is to accept permission for the connection.
- c. Repeat these steps for MVISION Mobile iOS and MVISION Mobile Android.
- 5. Verify that all the MVISION Console, MVISION Mobile iOS, and MVISION Mobile Android apps are accepted with MVISION Mobile Console only for the Government Cloud option.
- 6. Click the **Next** button and the **Add MDM Step 3 Setup** window opens.

Edit	MDM	

Step 1 Choose MDM Provider	Step 2 Add McAfee MVISION to AAD	Step 3 Setup	Step 4 Finish		
Mode:				MDM Only - Support managed devices only	
This is the Azure Active Specify Tenant ID. It is Background Sync Enable this option if apps, and profiles of	Directory (AAD) ID. the Azure Active Director you want the MDM prov n a periodic basis.	y's Directory ID ider to automatically syn	chronize users, devices,	MDM Only - Support managed devices only MDM Only - Support managed devices only MAM Only - Support unmanaged devices only MDM + MAM - Support both managed and unmanaged devices Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MDM + Microsoft MAM - Support MAM for devices managed Third-Party MAM - Support MAM - Support MAM for devices managed Third-Party MAM - Support MAM - Support MAM - Support MAM for devices managed Third-Party MAM - Support MAM - Su	jed by a different MDM
MDM Name Specify a unique name	for this MDM provider.			MVISION Demo - Microsoft Intune	
Mask Imported User Ir Enable this option to email) on the zConso	f ormation mask personally identif ple.	iable information (first na	ame, last name and		
Group Filter In the next step, only A available for selection Leaving this field blank	AD groups with names b as zConsole groups. Use c queries for all AAD grou	eginning with text includ commas to separate mu ps.	led in this field are Itiple text entries.	MVISION Demo	
				Next	

- 7. Select the option that you want:
 - a. MDM only which supports managed devices.
 - b. MAM only which supports unmanaged devices.
 - c. MDM and MAM which supports both managed and unmanaged devices.

For the third-party MDM with Microsoft MAM option, see the "<u>Setting Up a Third-</u> <u>Party MDM + Microsoft MAM and MVISION Mobile Console</u>" section.

- Select the **Background Sync** checkbox if you want synchronization to be done in a background mode.
 Note: For the MAM only option, devices do not show up in the regular device list since these devices are not managed.
- 9. Give a unique name in the **MDM Name** field for the environment.
- 10. Select if you want user information masked and not shown.
- 11. A group filter can be set, because if there is no group filter, all of the Groups appear when selecting the groups to manage. This filter is helpful when the environment is large and contains an extensive number of groups. It is recommended to use the Group Filter for ease of selecting the desired groups. Multiple group filters can be used and are separated with a comma.

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

- 12. Click Next.
- 13. Select the groups in this step. Click the green plus icon, next to the Azure group(s) to synchronize from the **Available MDM Groups** on the left. After a group is chosen, it appears in the **Selected MVISION Mobile Console Groups** on the right-hand side.

Click the **Include Nested Groups** checkbox if you want the inclusion of nested groups. With this setting, all devices in subgroups of the parent group are included in the MDM sync of the selected parent group.

Add MDM					
Step 1 Choose MDM Provider	Step 2 Add McAfee MVISION to AAD	Step 3 Setup	Step 4 Group Selection	n	Step 5 Alerts
Available Device Groups	5			Selected	d MVISION Console Groups
Search				MVIS	SION Demo
Android Enterprise			•		
СВАА			•		
			-		
 Include Nested Groups Select this option to as nested groups) in 	ups include all devices in sub n the MDM sync of the sel	groups of the parent gro ected parent group.	bup (known	If a device with the h	te is a member of more than one MDM group, the device is placed in the zConsole group higher priority.
					Next

14. Click Next.

15. Specify the MDM alerts if you want to be notified when there are MDM sync errors. If you want more than one email address, separate them by a comma. For more information on this step, see "Specifying MDM Alerts" in the "*MVISION Mobile Console Product Guide.*"

Note: This alert feature is available with MVISION Mobile Console Release 4.35 or later. MVISION Mobile Console Release 4.35.1 has the MDM alerts as the last step in this flow.

- 16. Click **Finish** to save the configuration.
- 17. Click the **Sync Now** button. Make sure you configure the threat and phishing policies for the groups selected. Refer to the *"McAfee MVISION Mobile Console Product Guide"* for more information.

Note: When creating the Administrator, after the initial setup (adding and granting the applications) and the synchronization is completed, be sure to update the user defined as the Administrator (used as the API administrator) to the "Limited administrator" directory role and select the role of "Intune administrator".

Note for MDM: Once the connector is in an available status, the synchronization is verified by going to the Devices or Users pages in the MVISION Mobile Console to see them showing up. The device entries in MVISION Mobile Console are greyed out until the user starts up MVISION Mobile and activates.

Configuring the Device Auto-Activation

The device application, typically the MVISION Mobile application, automatically performs auto-activation when integrated with Microsoft Endpoint Manager. The requirements for iOS and Android Enterprise activations are provided below.

For zero-touch activation, see the "<u>MVISION Mobile iOS Zero-Touch Activation</u>" section on those configuration steps.

Activation Steps

The Microsoft Endpoint Manager implementation has to be configured next in order to send extra information to the device app when it is pushed down to the device. To do this, perform the following steps:

- 1. Navigate to **Apps** > **App configuration policies.**
- 2. Click + Add.
- 3. Select Managed Devices.
- 4. Type a name, description, and the platform, such as Android or iOS.
- 5. Select the associated device application and click **Next**.

Home > Apps > Create app configura	ation policy	Associa Demo iOS Cont	ted a	pp Policy		;	×
		₽ Search by	name or	publisher			
1 Paries 2 Sattings 3	Assignments (A)	Name	\uparrow_{\downarrow}	Publisher	\uparrow_{\downarrow}	Туре	
• basics (2) Settings (3)	Assignments	McAfee MVI	SION M	McAfee, LLC.		iOS store app	
Name *	Demo iOS Conf	4					•
Description							
Device enrollment type	Managed devic						
Platform * (i)	iOS/iPadOS						
Targeted app * 🕕	Select app						
Previous Next		ОК					

- 6. On the **Settings** tab, select **Use Configuration Designer** and set up the configuration keys with the options described in the following sections.
- 7. Navigate to **Assignments** and select the groups that apply to this configuration.

iOS Activation

For MVISION Mobile, set up the configuration. On the **Settings** tab, select **Use Configuration Designer** and set up the configuration keys with the values using those outlined in the table.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	{{AzureADDeviceId}}
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.
tracking_id_1	String	(Optional) Use the desired identifier.
tracking_id_2	String	(Optional) Use the desired identifier.
display_eula	String	(Optional) no

	If you do not use this key, the default display
	the End User License Agreement (EULA).

NOTE: The configuration keys are case sensitive.

Android Setup

There are two options to set up the configuration for Android. This section details these two options:

- Android Enterprise with App Configuration Policy
- Android with the Company Portal App

McAfee recommends setting up the configuration with the Microsoft Endpoint Manager App Configuration Policies when possible.

Android Enterprise Setup with App Configuration Policy

To set up Android Enterprise in a Microsoft Endpoint Manager environment, you must:

- Set up the Microsoft Endpoint Manager app configuration policy for the MVISION Mobile app with the required keys below.
- If possible, remove any other variables that are not used from the list of configuration keys.

NOTE: Corporate-owned, fully managed Android Enterprise devices are not detailed in this document for enrollment.

Set up a configuration that contains the information using variables as outlined in the table.

Configuration Key	Value Type	Configuration Value
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
MDMDeviceID	String	{{AzureADDeviceId}}
display_eula	String	(Optional) no
		If you do not use this key, the default display
		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. This option is needed (instead of with the Company Portal app) for Android Enterprise devices enrolled without user-affinity, and the MDMDeviceID is required.

Setup with the Company Portal App

To set up an Android device in the Microsoft Endpoint Manager environment with the Company Portal app, you must:

- Install the Company Portal app on the device.
- Perform the setup on the MS portal console for the MVISION Mobile app to deploy.
- When MVISION Mobile is launched, if it detects the Company Portal app installed as a Device Administrator, then MVISION Mobile begins the auto-activation process. The end-user may be prompted to enter their Azure Active Directory credentials during the MVISION Mobile activation process.

Using Configuration Designer

This is the recommended mechanism for setting up the configuration with the App Configuration Policy for Android Enterprise.

The following figure shows the configuration settings set up for a policy when **Use configuration designer** is selected. This is the McAfee recommended way to set up the configuration keys.

Use the JSON editor to c	onfigu	re the disabled configuration keys.	
			×
CONFIGURATION KEY		VALUE TYPE	¢ψ
✓ Default Acceptor		string	
✓ Tenant		string	
Share Activation Data		bool	
Display EULA		bool	
Tracking ID 1		string	
Tracking ID 2		string	
✓ MDM Device ID		string	

This figure shows using the configuration designer for the MDM Device ID, Tenant, and Default Acceptor keys.

Home > Client apps - App configuration policies	> Add configuration policy >				
Add configuration policy $\ll \times$					
* Name MTD app config for Android Enterprise					
Description 0	Use the JSON editor to co	nfigure the disabled configura	ation keys.		
MTD app config for Android Enterprise	Configuration settings format 🛛	Use configuration designer			\sim
	Add				
* Device enrollment type 🚯					
Managed devices ~	CONFIGURATION KEY	VALUE TYPE	CONFIGURATION VALUE	DESCRIPTION	
* Platform 🛛	MDM Device ID	string	{{AzureADDeviceID}}		
Android ~		string	h/ 1/00-0 -00-		
Scope (Tags)	Tenant	string	b4df99c2-c26c		
0 scope(s) selected	Default Acceptor	string ~	https://acceptor.mcafee-m		
Associated app Associ					
Configuration settings Not configured					

NOTE: *Remove other variables that are not needed, if they are provided in the default configuration key list.*

Android Personal Profile Auto-Activation

You can 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 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.

Configuring for MVISION Mobile and iOS Zero-Touch Activation

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 4.33 or later and MVISION Mobile release 4.18 or later.

Overview of the Setup

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

- The Microsoft Endpoint Manager 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 devices 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 MVISION Mobile 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 MVISION Mobile 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 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 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 Endpoint Manager. See "<u>Appendix C - Sample Configuration File for Zero-Touch</u> <u>Activation</u>" 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:

Кеу	Option/Required	Key Description	Sample Value/Notes
defaultchannel	Required	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.	https://acceptor- mcafee-mvision- mobile.com/srx /json
tenantid	Required	Set the tenantid according to the value that you get from the Customer Success team member for your tenant. Note: This tenantid value may not be the value displayed on the Manage page of the MVISION Mobile Console and must be obtained from the Customer Success team.	mytenant or 1234-ABCD-5678
MDMDeviceID	Required	This is the identifier for the device for this MDM.	{{AADDEVICEID}}
assume_vpn_permission_ granted	Required	The values are true or false. Set this value to true to grant this permission.	true
enable_auth_redirect	Required	The values are true or false. Set this value to control and enable this	false

		feature. This controls redirecting HTTP URLs to a customized web page requesting the user to launch an app.	
enable_auth_notification	Required	The values are true or false. This controls the display of the local notification message requesting the user to launch the MVISION Mobile app.	true/false
auth_custom_notification _title	Required	Set the value to "Launch MVISION Mobile." The notification title can be changed to a custom title if desired.	"Launch MVISION Mobile"
runlevel	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.	Production
auth_custom_html_base6 4	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.	
VPNSubType	Required	This is the application that you want to activate. Note : This parameter can be different for some of Zimperium's customers.	com.mcafee.mvision.appstore
auth_redirect_url	Required	This is the redirect URL that is used to launch the app on the iOS device.	mvisionmobile://login

Configuring within the Endpoint Manager Console

To configure zero-touch activation, perform these steps:

- 1. Log in to the Microsoft Endpoint Manager console.
- 2. Navigate to this location and create a new profile, for instance, named "zVPNProfile." **Devices > Configuration Profiles**

Note: Ensure that the profile is assigned to the device group where your mobile device is associated.

- 3. Click **Create Profile** and the **Create a Profile** window opens.
- 4. Select the **iOS/iPadOS** platform, and then select **Profile Type** as Custom and click **Create**.
- 5. Enter a name and description and click **Next**.
- 6. In the **Configuration Settings** tab, enter a profile name.
- 7. Set the **Configuration Profile File** field to the configuration file that you updated in the above section.

Home > [Devices >
Custo iOS/iPadOS	m
🗸 Basic	cs Configuration settings (3) Assignments (4) Review + create
Configura	ation profile name * ① Demo Test ✓
Configura "ZeroVp	ation profile file * "ZeroVpn_Intune.xml"
1 2 3 4 5	<pre><?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1 <plist version="1.0"> <dict> <kev>PavloadContent</kev></dict></pre>
6	<array></array>
8	<key>IPv4</key>
9	<dict></dict>
10	<key>0verridePrimary</key>
11	<integer>0</integer>
12	
13	<key>rayloadDescription</key>
14	<pre><string>configures ven settings, including authentication.</string> </pre>
15	<pre></pre> <pre><pre><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pre>><pr< th=""></pr<></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
17	<key>PayloadIdentifier</key>
Previou	Js Next

- 8. In the **Assignments** tab, select your Azure AD Group and click **Select**.
- 9. Click **Next**.
- 10. Review your values and save the profile.

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 Microsoft Endpoint Manager MDM. See the "<u>Configuring MVISION Mobile for MDM Only</u>" section for more information.

The result of these configuration steps 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" when the VPN profile is on the device.

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

Enable the Connector in the Microsoft Endpoint Manager Console

You must set up the connector on the Azure website for MAM or MDM. If you already configured the connector for MAM in the steps above, skip this step.

This allows Microsoft Endpoint Manager to synchronize the device data with McAfee MVISION Mobile. Without setting these attributes on the connector, the Microsoft Endpoint Manager device compliance is disabled.

Configure the MTD Connector

WARNING: If you migrate from the Zimperium connector to the MVISION Mobile connector, active devices change from "Pending Activation" status to "Active" the next time the device checks-in with the MVISION Mobile Console.

Perform these steps to set up the MTD Connector properties:

- 1. Log into Microsoft Endpoint Manager.
- 2. Click and navigate to **Tenant Administration** > **Connectors and tokens** > **Mobile Threat Defense**.
- 3. Click **MVISION** as the MTD Connector.
- 4. Under the **MDM Compliance Policy Settings** section, consider turning on the sliders for **Connect Android Devices**, **Connect iOS Devices**, and **Enable App Sync for iOS Devices**.

×		Edit Connector Mobile Threat Defense
	elete	🔚 Save 🗙 Discard 间 D
	Last synchronized	Connection status
	11/12/2020, 3:00:54 PM	Unavailable
	35	MDM Compliance Policy Setting
Off On	on 5.0 and above to McAfee MVISION Mobile $ \bigcirc $	Connect Android devices of version
Off On	and above to McAfee MVISION Mobile ①	Connect iOS devices version 10.0
Off On	0	Enable App Sync for iOS Devices
Off On		Block unsupported OS versions
		Common Shared Settings ①
7	nresponsive ①	Number of days until partner is u
	rresponsive ① le admin console	Common Shared Settings ① Number of days until partner is un Open the McAfee MVISION Mobil

NOTE: Enabling the app sync option for iOS devices allows McAfee to request the iOS app data from Microsoft Endpoint Manager to use for threat analysis purposes. It is recommended to ensure this option is "On." The initial sync does not contain the iOS apps until the connector has this option enabled. Without the connect device options on, device compliance is disabled, and threats are not reported.

When the connector is in an "Available" status, verify the synchronization by going to the Devices or Users pages in the MVISION Mobile Console and see that they are showing up. The device entries in the MVISION Mobile Console are greyed out until the user starts up MVISION Mobile and activates the app.

When the connector is in an "Enabled" status, threat information and device compliance are then reported back to Microsoft Endpoint Manager, along with app sync for iOS devices (if the options are enabled as above).

Device Actions, Policies, and Remediation

The MVISION Mobile integration with Microsoft Endpoint Manager provides a way to block access to company data such as email and other services. Compliance policies are used to allow only devices below a defined device threat level to access certain data and services. If a threat is detected on a device and that threat has an MDM action of **Inform EMM**, then MVISION Mobile Console sends the new device threat level of that device to Microsoft Endpoint Manager. The device threat level is the highest threat event classification that is pending for that device, also known as the Risk Posture.

Microsoft Endpoint Manager Policies

To set Microsoft Endpoint Manager to take actions when a device falls below a defined threat level, navigate to **Devices** and **Compliance Policies** from the Microsoft Endpoint Manager console.

Home > Devices >		
Compliance policies	Policies	×
	$+$ Create Policy $\equiv\equiv$ Columns \bigtriangledown Filter \circlearrowright Refresh \downarrow Export	
🔓 Policies	One or more Threat Defense connectors are active for iOS/iPadOS but not included in an assigned compliance policy. To pro	ect
Notifications	these platforms, set up a compliance policy with the Device Threat Level rule configured under the Device Health section.	
Retire Noncompliant Devices		
Locations	Policy Name ↑↓ Platform ↑↓ Policy Type ↑↓ Assigned ↑↓ Last Modified ↑↓	,
🐯 Compliance policy settings	Android MTD Compl Android Enterprise Fully managed, dedicat Yes 12/09/20, 4:42 PM	
	iOS MTD Compliance iOS/iPadOS iOS compliance policy Yes 12/07/20, 4:18 PM	

Create policies for each OS Platform in the environment by clicking the **+ Create Policy**. Choose the platform, enter the name of the policy. On the next page for **Device Health**, select the minimally safe Device Threat Level for this platform.

Options are as follows:

- Secured
- Low
- Medium
- High

It is recommended to set it to **Medium** so that when the device has a High Device Threat level, it makes the device non-compliant. When a Critical threat is detected by the device application, it corresponds to the High Device Threat Level in Microsoft Endpoint Manager.

Conditional access policies prevent a non-compliant device from accessing those as defined resources set up by the Microsoft Endpoint Manager Administrator. When a critical threat occurs, it forces the device's compliance posture to be non-compliant. This then triggers the appropriate conditional access policy.

MVISION Mobile Console Policies

The next step is to navigate to the **Policy** page in the MVISION Mobile Console and select a **Microsoft Intune group** to target. For each threat classification that Microsoft Endpoint Manager needs to know about, set the MDM Action column to **Inform EMM**.

For situations where the threat can be mitigated or is no longer present, set the Mitigation Action column to **Inform EMM**, and the Device Threat Level of the device is adjusted accordingly.

Appendix A – iOS User Experience for MDM

After successful enrollment in Microsoft Endpoint Manager, the app is pushed down to the user's device.

MVISION Mobile App



The MVISION Mobile app is started by:

- Clicking manually on the app.
- Clicking a link sent to the user by text.
- Clicking on an email link.
- Scanning a QR code.

See the "MVISION Mobile iOS Platform Guide" for more information on the activation process.

After the activation process, MVISION Mobile displays the main dashboard showing that it is protecting the device.

4:51 1 .	?■		
NO THREATS DETECTED			
✓ Device Safety	(j)		
✓ Network Safety	(j)		
Apps Safety	(j)		
Activity Monitor			
Danger Zone			

Appendix B – Android User Experience for MDM

MVISION Mobile App



To set up Android Enterprise in a Microsoft Endpoint Manager environment, you must complete these items:

- The Company Portal app installed on the device.
- Activate as a device administrator. Within the Company Portal app, the device administrator role is one that the Company Portal needs to manage the device.
- Set up is needed on the MS portal for these applications to deploy.

The MVISION Mobile app is started by:

- Clicking manually on the app.
- Clicking a link sent to the user by text.
- Clicking on an email link.

See the *"Android MVISION Mobile Platform Guide"* for more information. When MVISION Mobile starts up in a Microsoft Endpoint Manager environment, it first tries to authenticate through Azure credentials.

Once started, the screen on the left is displayed, showing that the user is activating using the SSO Azure credentials. The user does not need to input a password. When this is completed, the user is activated and MVISION Mobile shows as protecting the device.



Appendix C - 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>
```

```
<key>VPNType</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>
```