

McAfee MVISION Mobile

Citrix XenMobile Integration Guide

Administrator's guide for providing Integration with Citrix XenMobile MDM

September 2018

COPYRIGHT

Copyright © 2018 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

Overview4Requirements4Architecture4Protection Methods5Configuration Levels5Level 1: Basic Application Deployment5Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Integration with Citrix XenMobile	. 4
Requirements4Architecture.4Protection Methods5Configuration Levels.5Level 1: Basic Application Deployment.5Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Overview	. 4
Architecture.4Protection Methods5Configuration Levels.5Level 1: Basic Application Deployment.5Level 2a: User Synchronization.6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment.8Level 3: Basic Protection.11Level 4 Granular Protection11	Requirements	. 4
Protection Methods5Configuration Levels5Level 1: Basic Application Deployment5Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Architecture	. 4
Configuration Levels5Level 1: Basic Application Deployment5Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Protection Methods	. 5
Level 1: Basic Application Deployment.5Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Configuration Levels	. 5
Level 2a: User Synchronization6User Sync Setup7Level 2b: Auto Sign-in/Advanced Application Deployment8Level 3: Basic Protection11Level 4 Granular Protection11	Level 1: Basic Application Deployment	. 5
User Sync Setup	Level 2a: User Synchronization	. 6
Level 2b: Auto Sign-in/Advanced Application Deployment	User Sync Setup	. 7
Level 3: Basic Protection	Level 2b: Auto Sign-in/Advanced Application Deployment	. 8
Level 4 Granular Protection11	Level 3: Basic Protection	11
	Level 4 Granular Protection	11

Integration with Citrix XenMobile

Overview

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

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

The Citrix XenMobile Administrator can setup access to the API server via a dedicated Administrator account that MVISION Mobile Console will use to synchronize and perform actions with. Actions supported include; Lock Device and Remove Applications.

Requirements

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

The following table details specific requirements for the API connection:

Item	Specifics
Citrix XenMobile MDM enrolled device	V10.3 and above
API Administrator Account in Citrix XenMobile management console.	<intentionallyblank></intentionallyblank>
API access TCP Port	Standard port 443 but can be setup on other ports as required.

Architecture

McAfee integrates with Citrix XenMobile MDM with different configuration levels which are described in the <u>McAfee MVISION Mobile Console Guide</u> available in the customer portal. Each level is addressed further on in this document with specific configuration instructions. To achieve level 2 – 4 integrations, the MVISION Mobile Console will be configured to share information with the Citrix XenMobile console through API access. When MVISION Mobile Threat Detection Application detects an event, it consults the current Threat Response Matrix resident on the device and if there is a specific MDM action defined, this is communicated to the Cloud server. The Cloud server will then reach out to the proper Citrix XenMobile API Server and provide the commands to perform the action described.

Protection Methods

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

- 1. Lock the Device: This prevents unauthorized access to the device during a threat and can help prevent data leakage during network based attacks.
- 2. Remove managed apps from the device: Remove all organizational applications including any company intellectual property.

Configuration Levels

Level 1: Basic Application Deployment

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

To deploy as an Enterprise app, login to Citrix XenMobile and navigate to: Configure/ Apps/. Add a new Enterprise Application and upload the proper application file (IPA for iOS, APK for Android) to Citrix XenMobile. MVISION Mobile Threat Detection Application can also be selected from the respective Public App Store (iTunes store or the Play Store). Assign the Delivery Group to the application and publish.

		Device Po	Add App				
\pp	S Show	filter	Click an app type and then follow the steps to add	d a deployable app. The app appear	s in the app table after you complete the steps.		
	Add	ි Category	MDX Apps wrapped with the MDX Toolkit to include	app policies. You can deploy	Public App Store Free or paid apps available in a public app sto	ore, such as iTunes or Google	
	Icon	App Name	Example: WorxMail	tores.	Example: GoToMeeting		
		WorxMail					
	88	WorxWeb	Web & SaaS		Enterprise		
	۵	WorxNote	Apps accessed from an internal network (Web (SaaS). You can create your own apps or choos	apps) or over a public network e from a set of app connectors	Native apps not wrapped with the MDX Toolkit and that do not contain policies found in MDX apps.		
	Ø	QuickEdit	tor single sign-on authentication to web apps. Example: GoogleApps_SAML		Example: Quick-iLaunch		
	S	ShareFile F					
	S	ShareFile 1	Web Link				
	Ø	ShareConr	A Web address (URL) to a public or private site require single sign-on.	or to a Web app that doesn't			
	©	WorxTasks					
	0	Receiver	Public App Store	Default	11/10/15 12:46 PM	3/4/16 7:51 AM	
	60	Citrix Receiver	Enterprise	Default	11/10/15 12:49 PM	2/18/16 2:30 PM	

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

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

Level 2a: User Synchronization

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

After the initial User Synchronization during the MDM Integration setup, users will be managed through a scheduled synchronization process that will run every four hours. If McAfee sees additional users in the Delivery Group(s) being used for synchronization, they will be added to the MVISION Mobile Console. If we see users removed, then we will remove them from the MVISION Mobile Console. Doing this will not remove any of the events associated with that user/device.

When user synchronization occurs, the MVISION Mobile Console requests certain information from the Citrix XenMobile MDM. The information returned for each devices includes:

- Name
- Email Address
- IMEI

- UUID
- Device ID
- Serial number

User Sync Setup

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

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

User synchronization includes the following information:

- 1. User ID (Email address) of user
- 2. Device Hash ID
- 3. Device IMEI, UUID

To setup User Synchronization;

- 1. Create a Citrix XenMobile administrator User.
 - a. Navigate to: Manage/Users/ Add Local user. Provide name, Description and choose the ADMIN role. Membership Groups do not need to be selected.
- 2. Create one or more Delivery Groups that will contain the devices that will be protected, if you do not have existing groups. MVISION Mobile Console will use the Delivery Group(s) to synchronize users and devices.
- 3. Log in to MVISION Mobile Console and go to the Management page. From there select 'MDM Settings'
- 4. Click on Add MDM and select the Citrix icon to integrate with.
- 5. Enter information pertinent for the Citrix XenMobile integration URL: URL of the Citrix XenMobile API Server

Username: Citrix XenMobile Administrator created with the API REST Role Access

Password: Password of the Citrix XenMobile Administrator created.

Sync User: Check this box to ensure users/devices will be synchronized with the Citrix XenMobile Delivery Groups chosen in the next page.

Set Synced users password: Check this box to override the default password during user sync.

Synced users password: The value of the password to use for each user when they are synchronized.

Mask Imported User Information: Check this box to mask personally identifiable information about the user: Name, Email address

- 6. Click Next and choose the Delivery Group(s) to synchronize with. The available Delivery Groups will show up by clicking in the entry box. Click Finish to save the configuration and start the first synchronization.
- 7. The Delivery Groups will be retrieved and user/device synchronization will be completed.
- 8. You can verify this by going to the Devices or Users pages in the MVISION Mobile Console to verify they are showing up. The device entries will be greyed out until the user starts up MVISION Mobile Threat Detection Application and logs in. Their userID will be their email address and the password defined above.

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

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

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

Create a plist file that contains the user/device specific information using variables as outlined below:

Configuration Key	Configuration Value
serial	\${device.serialnumber}
uuid	\${device.serialnumber}
imei	\${device.imei}
wifimac	\${device.wifiMacAddr}

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

This configuration is done within Citrix XenMobile though iOS Configuration Policies:

	Device Policies	Add a New Policy			
Dev	rice Policies Show filter	Type or select a policy from	the list	Q	Search
	Add Export	Exchange	Passcode	VPN	Location
	Policy name	Scheduling	Restrictions	WIFI	Terms & Conditions
	Passcode Policy	▼ More			
	- assessed a straig	Network access	Anns	Security	XenMobile agent
	Device Restrictions	APN	Ann Access	Android for Work App	Enterprise Hub
	Android Appl adk	Cellular	Ann Attributes	Restrictions	XenMobile Options
	Android Approce	Connection Manager	App Configuration	App Lock	XenMobile Uninstall
	Device Location Services	Personal Hotspot	App inventory	App Restrictions	End user
		Personal motaplot	App Internory	Contacts (CardDAV)	AirPlay Mirroring
	Roaming Controls	Provy	App network usage	Copy Apps to Samsung	AirPrint
	_Demo Center Android Agent Con	Reaming	App Uninstall Pertrictions	Credentials	Calendar (CalDav)
		Roaming	App uninstall restrictions	Enterprise Data Brotection	Device Name
	_Demo Center Android Connectio	Samaung roewall	Delete Elet and Felder	Protection	Font
	App Uninstall Restrictions	Custom	Delete Files and Folders	NJUSK	LDAP
		Custom VMI	Clier	managed Domains	MDM Options
	_DemoCenter Samsung SAFE API	Custom Amic	Piles	SCEP	Mail
	Restrict Apple Activation Lock	Device meanur Attestation	Provisioning Profile	Samsung MDM License Key	Organization Info
	The second s	import icos & Mác OS X Profile	Sideloading Key	storage Encryption	SSO Account

1. Navigate to Configure / Device Policies / Add

- 2. On the window above, click on '<u>More</u>' and select App Configuration.
- 3. Provide a name for this policy and click next

	Xen Mobile	Analyze	Manage	Configu	re			٠	٩	demoadmin@ci	trix.lab 🗸
	_	Device Policies	Apps	Actions	Sh	areFile	Delivery Groups				
	App Configu Policy	ıration	Policy Inf This policy lets device. After yo	ormatior you define a c u enter the di	1 configu	ration of a r ry content, y	managed app to b you can check the	e appl syntax	ied on	the iOS	×
ł	1 Policy Info		Poli	cy Name*	iOS	Plist V2					
	2 Platforms		De	scription	plist	information	for iOS zIPS, Versio	n 2			
	ios								11		
	3 Assignment										
											Next >

4. In the dropdown next to 'Identifier', select 'Add New' and add 'com.zimperium.zIPS' in the textbox. Add the PLIST info for your environment in the 'Dictionary content' entry. Note that the PLIST info isn't full XML format (no XML headers). Click on 'Check Dictionary' to verify that you have formatted it correctly. Click Next to continue. (NOTE: If you are using the MVISION Mobile Threat Detection

XenMobile	Analyze	Manage	Confi	gure	🌣 🔧 demoadmin@citrix.lab 🗸
De	vice Policies	Apps	Actions	ShareFile	Delivery Groups
App Configurati Policy	ion	Policy Info This policy lets ye the dictionary co	prmation ou define a c intent, you ca) onfiguration or an check the sy	imes of a managed app to be applied on the iOS device. After you enter yntax.
1 Policy Info				Identifier*	Add new -
2 Platforms					com.zimperium.zIPS
ios			Diction	ary content*	<dict></dict>
3 Assignment					<pre>string>s{device.serialnumber} <key>wifimac</key> <string>s{device.serialnumber}</string> <key>uuid</key> <string>s{device.serialnumber}</string> <key>uid</key> <string>s{device.imei}</string> <key>imei</key> <string>s{device.imei}</string> </pre>
					Valid XML Check Dictionary
					Back Next >

Application app from the Apple Play Store, use the bundle ID: 'com.zimperium.zIPS.appstore'.)

5. Select the Delivery Group that this policy should apply to and Save

XenMobile Analyze	e Manage	Configure		🌣 🔧 demoadmin@citrix.lab 🗸
Device Poli	cies Apps A	Actions ShareFi	ile Delivery Groups	
App Configuration Policy	App Configu This policy lets you dictionary content	uration Policy udefine a configuration , you can check the sy	on of a managed app to be app Intax.	Hied on the iOS device. After you enter the
1 Policy Info	Choose delivery groups	y Type to search s	Q Search	Delivery groups to receive app
2 Platforms		AllUse	ers	IOSDemoDG
iOS		All De Zimperiur	vices in n	Kerns DG
3 Assignment		IOSDe	emoDG	
		IOSDe	emoDGa	
		XXX		
		Kerns	DG	
		TestG	roups	
	Deployment	ent Schedule 🔊		
				Back Save

Android MVISION Mobile Threat Detection Application does not require an Application Configuration to be setup and will find the correct environment by searching for its known Device ID/Serial Number in the MVISION Mobile Console environment. User/Device synchronization makes this possible.

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

Level 3: Basic Protection

Level 3 does not apply to Citrix XenMobile at this time.

Level 4 Granular Protection

The McAfee integration with Citrix XenMobile provides the ability to either lock the device or remove all managed applications (and their data) from the device. MDM Integration with MVISION Mobile Console also has to be setup and functional.

The action to choose can be selected from the pull down list under MDM Action in the Policy page. Choose either; No Action, Lock Device or Remove Citrix Applications. When an EOP occurs, all managed apps will be removed from the device. In effect, this will remove all organizational intellectual property from the device.