McAfee MVISION Mobile

Citrix XenMobile

Integration Guide

January 2021

Contents

Preface

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

Audience

The intended audience for this guide is a 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

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 and provide more granular and specific protection actions.

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

The Citrix XenMobile Administrator can set up access to the API server via a dedicated Administrator account that MVISION Mobile Console uses to synchronize and perform actions. Actions supported include the following:

- Lock Device
- Remove Applications

Prerequisite Requirements

Integration with Citrix XenMobile requires a connection between the MVISION Mobile Console and the Citrix XenMobile API server. This is accomplished via the Internet using SSL. If you use a Citrix XenMobile SaaS management server, there are no changes that need to occur to allow 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.	Create this account.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the Citrix XenMobile console through API access. When MVISION Mobile detects an event, it consults the current Threat Policy resident on the device and if there is a specific MDM action defined, this is communicated to the server. The server then reaches out to the proper Citrix XenMobile API Server and provides the commands to perform the action described.

Protection Methods

McAfee's MVISION Mobile 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:

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

Configuration Steps

Basic Application Deployment

To access the MVISION Mobile application from the public application store, add a new Public Store App and search the appropriate store for McAfee MVISION. Or you can download the MVISION Mobile application using these links:

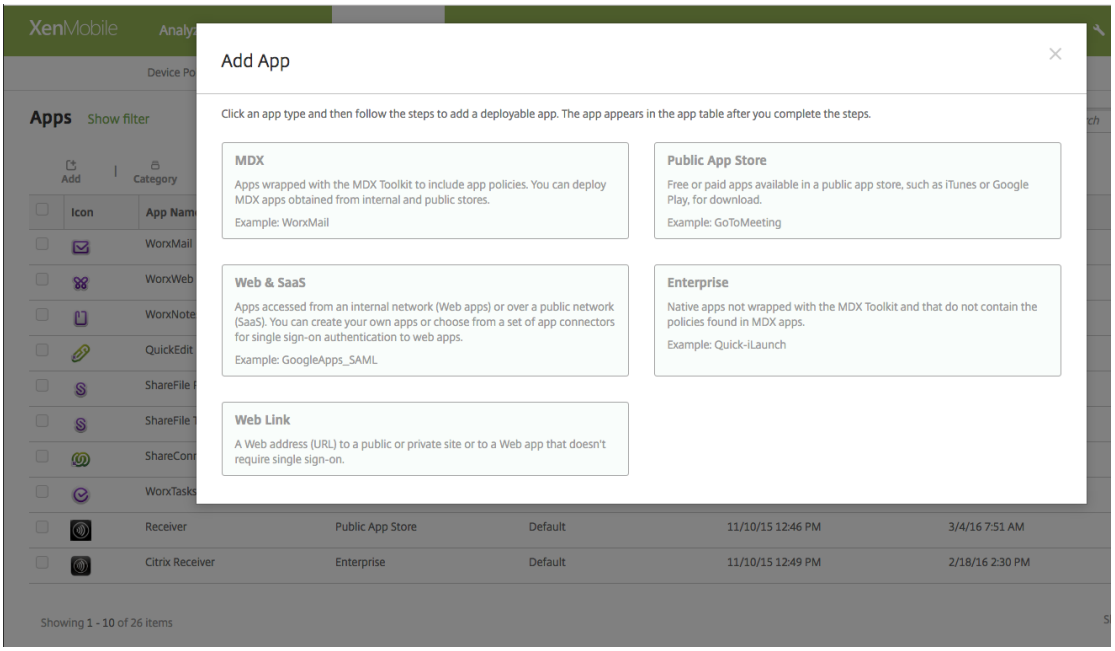
iOS MVISION Mobile: https://apps.apple.com/us/app/mcafee-mvision-mobile/id1435156022

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

To deploy as an Enterprise app, log in to Citrix XenMobile and navigate to Configure > Apps. Add a new Enterprise Application and upload either of these application files to Citrix XenMobile:

- IPA for iOS
- APK for Android

MVISION Mobile can also be selected from the iTunes store for iOS or the Google Play Store for Android. After selecting MVISION Mobile, assign the Delivery Group to the application and publish it.



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 need the activation URL created in the MVISION Mobile Console to access the application unless User Synchronization is performed, described in the next section.

MDM Synchronization

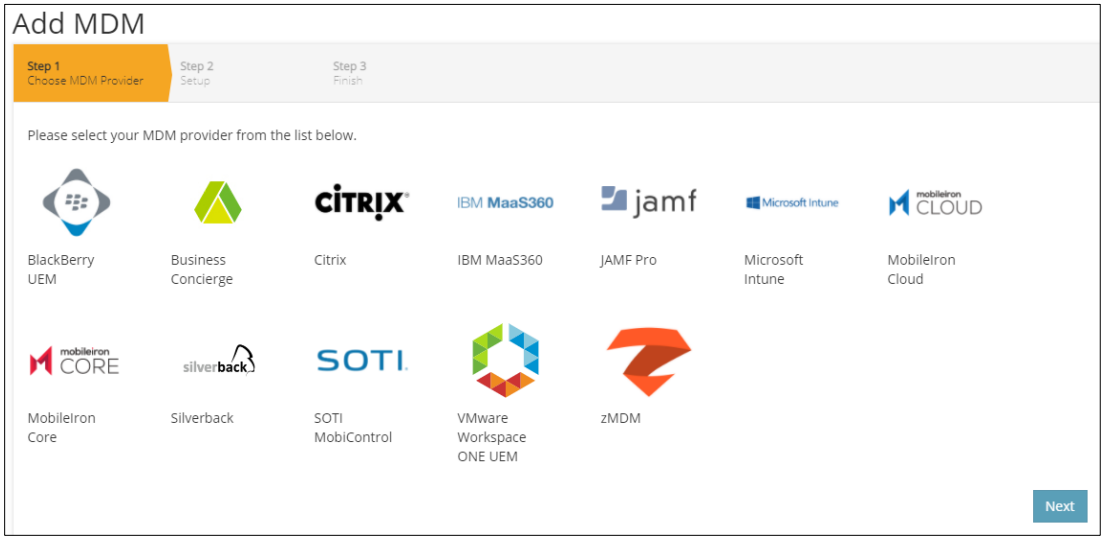
Overview

After the initial synchronization during the MDM Integration setup, devices are managed through a scheduled synchronization process that runs every four hours. If MVISION Mobile sees additional users in the Delivery Group being used for synchronization, they are added to the MVISION Mobile Console. If users are removed, then they are removed from the MVISION Mobile Console. These actions do not remove any of the events associated with that user or device.

Setting Up Synchronization

Perform these steps to set up synchronization:

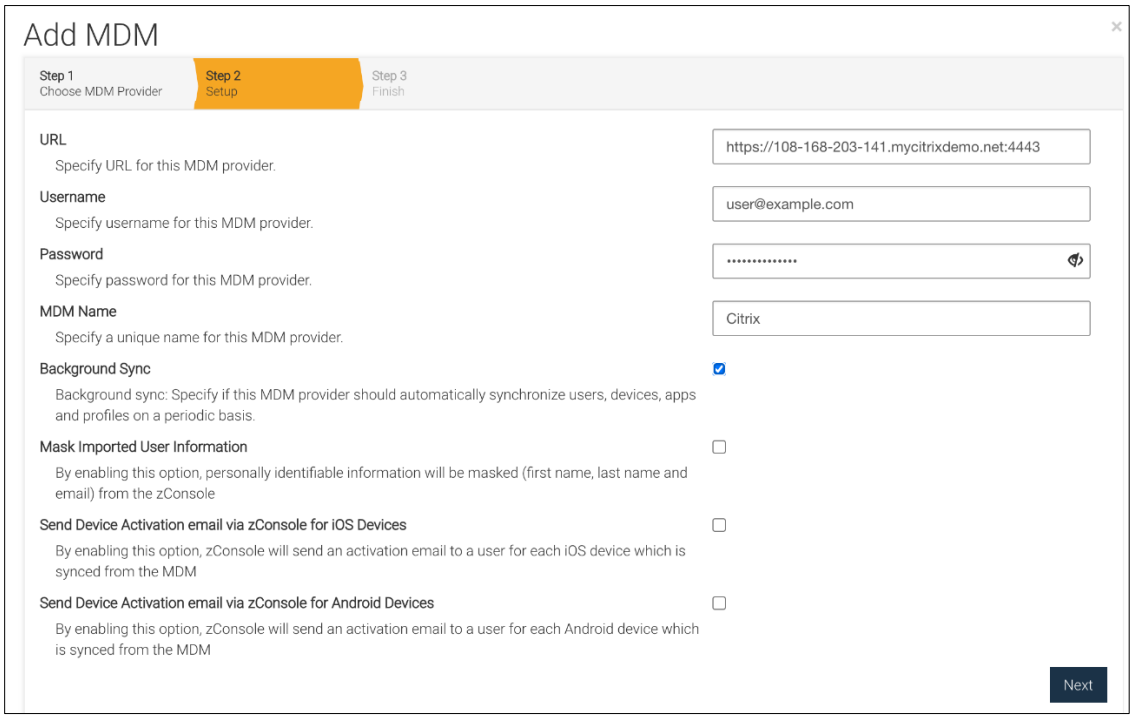
1. Log in to the Citrix XenMobile website.
2. Create a Citrix XenMobile administrator User.
    a. Navigate to Manage > Users > Add Local user.
    b. Provide a name, description, and choose the ADMIN role. Membership Groups do not need to be selected.
3. Create one or more Delivery Groups for containing the protected devices, if you do not have existing groups. zConsole uses the Delivery Group(s) to synchronize users and devices.
4. Login to zConsole and click the **Manage** menu page option. From there click the **Integrations** and **MDM** tab.
5. Click **Add MDM** and select the Citrix icon and then **Next.**



6. Enter information pertinent for the Citrix XenMobile integration.

Item	Specifics
URL	This is the URL of the Citrix XenMobile API Server.
Username	This field is the Citrix XenMobile Administrator created with the API REST Role Access.

Password	The password of the Citrix XenMobile Administrator created.
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This value is prepended to the group name to form the MVISION Mobile Console group name. This value defaults for you.
Background Sync	Check this box to ensure users and devices are synchronized with the Citrix XenMobile Delivery Groups chosen on the next page.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed such as name and email address.
Send Device Activation email via MVISION Mobile Console for iOS Devices	Check this box to send an email to the user for every iOS device synced with the MDM.
Send Device Activation email via MVISION Mobile Console for Android Devices	Check this box to send an email to the user for every Android device synced with the MDM.



7. Click **Next** and choose which Delivery Group you want to synchronize. The available Delivery Groups show up by clicking in the entry box. Click **Finish** to save the configuration and start the first synchronization.

The Delivery Groups are then retrieved, and user and device synchronization start.

You can verify this by going to the Devices or Users pages in the MVISION Mobile Console to verify they are displaying. The device entries are greyed out until the user starts up MVISION Mobile and activates the app.

Auto-Activation/Advanced Application Deployment

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

iOS Activation

Zimperium's iOS zIPS application takes advantage of the configuration variables sent to it from a PLIST file when the app is pushed down to the device. This provides the best user experience, allowing the user to startup iOS zIPS without having to enter any credentials. The application configuration initializes iOS zIPS with the required information.

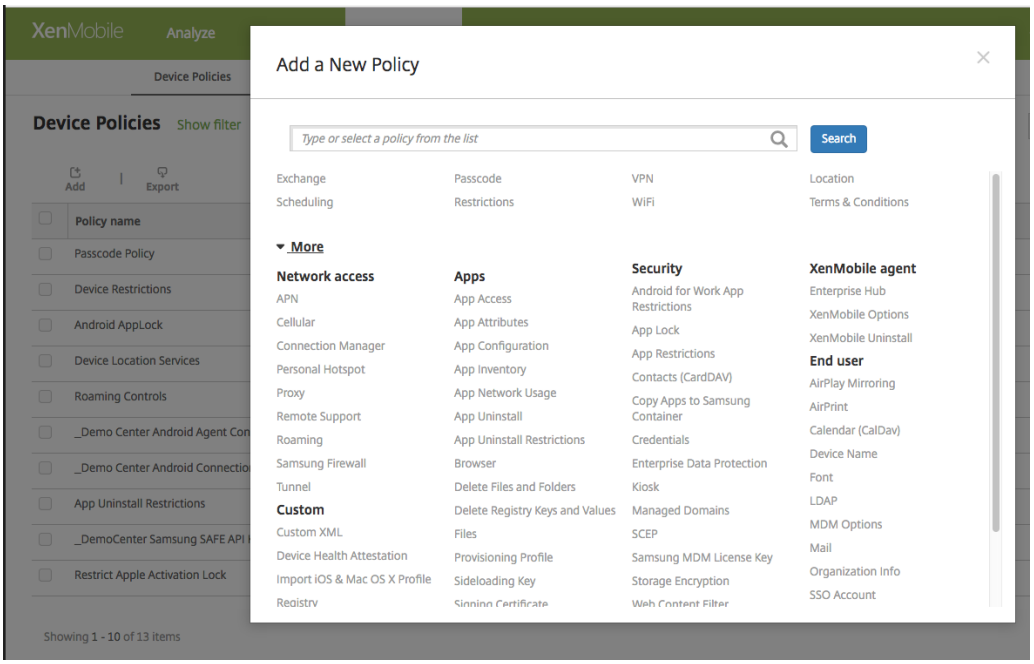
Create a file that contains these variables.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	$device.id
tenantid	String	Copy the value from the **Tenant ID** field on the MVISION Mobile Console **Manage** page under the **General** tab.
defaultchannel	String	Copy the value from the **Default Channel** field on the MVISION Mobile Console **Manage** page under the **General** tab.
display_eula	String	no (Optional) If this key is not used, the default displays the End User License Agreement (EULA).
tracking_id_1	String	(Optional) Use your desired identifier.
tracking_id_2	String	(Optional) Use your desired identifier.

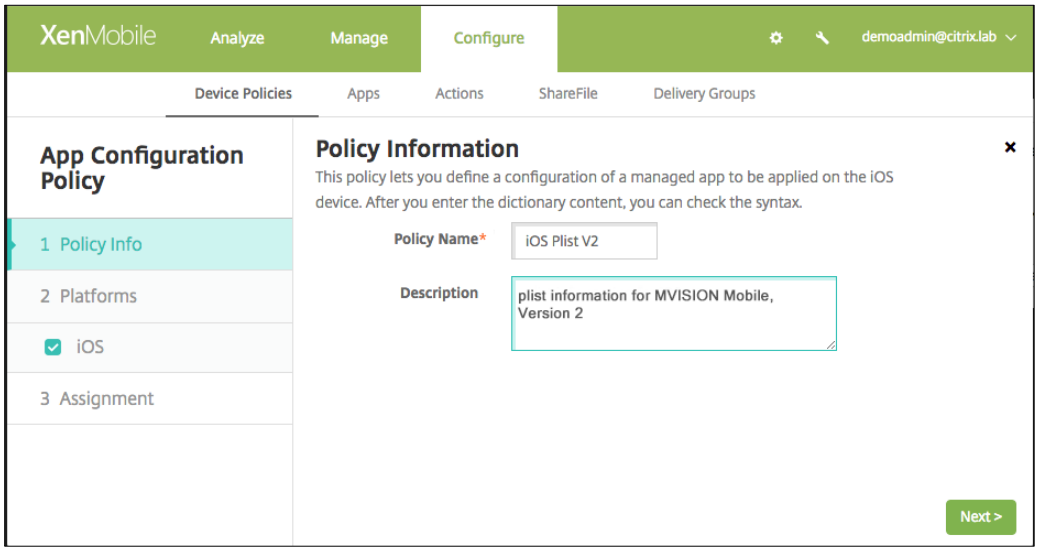
NOTE: *The configuration keys are case sensitive*.

Set up this configuration within Citrix XenMobile through iOS Configuration Policies by performing these steps:

1. Navigate to **Configure** > **Device Policies** > **Add**.
   The Add New Policy windows displays:



2. Click on **More** and select **App Configuration** under Apps.
3. Provide a name for this policy and write a description (optional). Then click **Next** as seen in the figure.



4. In the dropdown next to the 'Identifier' field, select **Add New** and add 'com.mcafee.mvision.mobile' in the textbox. If you are using the MVISION Mobile app from the Apple Play Store, use the bundle ID: 'com.mcafee.mvision.mobile.appstore'.

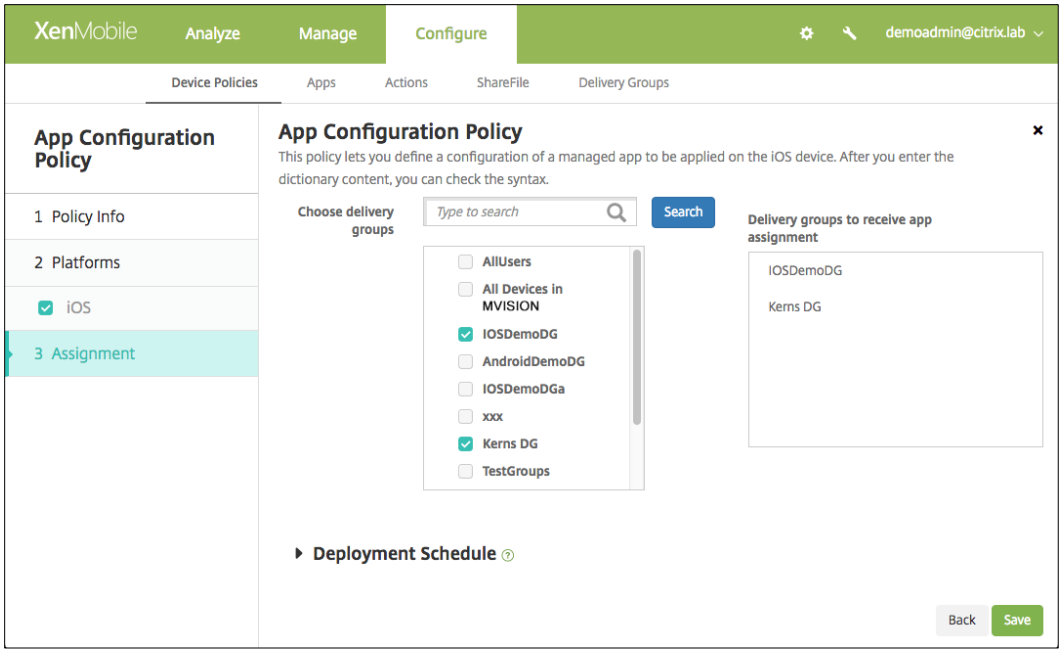
Add the PLIST info for your environment in the 'Dictionary content' field. Note that the PLIST info is not in full XML format (no XML headers). Click on **Check Dictionary** to verify that you have formatted it correctly.

This is an example of PLIST dictionary content for MVISION Mobile.

```
<dict>
   <key>MDMDeviceID</key>
   <string>$device.id</string>
   <key>defaultchannel</key>
   <string>https://acceptor.mcafee-mvision-mobile.com/srx</string>
   <key>tenantid</key>
   <string>demo</string>
</dict>
```

NOTE: *Refer to the tables in the "iOS Section" for all the PLIST configuration key options for different releases.*

5. Click **Next** to continue.
6. Select all that apply under 'Choose delivery groups' that this policy should apply to and click **Save**.



Android Activation

Android Enterprise users can use the managed app configuration for activations. You need to make sure you are passing the right device identifier value for the configuration parameter. The variables are the same set as the PLIST variables in the "iOS Activation" section. For documentation on the setup for Android Enterprise, refer to this Citrix website:

https://docs.citrix.com/en-us/xenmobile/server/provision-devices/android-for-work.html

***Note**: For the MVISION Mobile configuration key list, the UUID can still be displayed and you can remove it from the list or leave it empty.*

For native Android devices, activations require the use of activation URLs. These can be sent to end-users via the MVISION Mobile Console or the MDM. Clicking on MVISION Mobile without the link does not activate MVISION Mobile for Android devices. When a user runs the app with the activation URL link, it activates and downloads the proper Threat Policy.

To access activation links, use the MVISION Mobile Console Manage page and select the MDM tab. After the MDM has been added, the activation link is provided for devices. This activation link is used along with appending the MDM device identifier. The MVISION Mobile Console page displays the expiration date and time, and if needed, the link can be regenerated.

See the "*McAfee MVISION Mobile Console Product Guide*" for more information on the MDM activation links.

The administrator can send the concatenated activation link by email or text to users, along with instructions to accept the MVISION Mobile app being pushed to them.

Android Personal Profile Auto-Activation

For MVISION Mobile release 4.80 and later, use these additional configuration keys and values for auto-activation for the personal profile in an Android Enterprise configuration.

Configuration Key	Value Type	Configuration Value	Notes
share_activation_data	String	true	This is required if you want to auto-activate the personal profile application. This defaults to 'false'.
activation_package	String	Bundle Id of the app to query for the activation information. The default is 'com.mcafee.mvision'.	(Optional) This is only needed if share_activation_data is true.

Device Actions and Remediation

In MVISION Mobile Console the term ‘MDM Action’ is synonymous with a device action. It is an action that an administrator pushes to the device. When the integration is set up with the MDM, the administrator can select the MDM actions to perform for each threat in the MVISION Mobile Console Threat Policy definition.

Available Device Actions

The MVISION Mobile 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 set up and functional before you can invoke these actions.

You choose the device action by selecting from the drop-down list under the MDM Action column on the MVISION Mobile Console Policy page. Choose one of the following actions:

- No Action
- Lock Device
- Remove Citrix Applications

In the figure example, when an ARP MITM threat occurs, you can select the desired action. You can lock the device or remove all managed apps from the device. If you choose to remove Citrix applications, this action removes all organizational intellectual property from the device.