



McAfee MVISION Mobile

Jamf Pro

Integration Guide

January 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.....	4
Audience	4
Related Documentation	4
Overview.....	4
Prerequisite Requirements	5
About MDM and MVISION Mobile Console Communication	5
Configuration Steps.....	6
Synchronization Overview.....	6
Enrolling a Device to Jamf	6
URL and Administrator Login	6
SMTP Server Setup and an Enrollment Invitation	8
About and Enrolled Device	11
On-Demand MDM Synchronization	13
Set Up Synchronization in MVISION Mobile Console.....	13
Device Application Deployment Set Up	16
Overview	16
Jamf User with Administrator Access	16
Device Groups	17
About MVISION Mobile Deployment.....	18
Configuring Scope of Device Application	21
Assigning an Enrolled Device to a Static Device Group	22
Configuring Device Application Auto-Activation.....	22
iOS Activation.....	22
About App Configuration.....	23
Device Actions and Remediation.....	24
Available Device Actions.....	24
Synchronizing iOS Apps.....	24

Preface

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

Audience

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

Related Documentation

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

Overview

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

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

McAfee MVISION Mobile detects malicious activity and depending on the platform is able to take defined actions locally. When MVISION Mobile is integrated with an MDM, protection actions can be performed by the MDM, providing a very powerful protection tool. In the Jamf integration, device synchronization is supported, along with device actions.

Prerequisite Requirements

Integration with Jamf requires a connection between the MVISION Mobile Console and the Jamf server.

This table details specific requirements for the connection.

Item	Specifics
Jamf App on an MDM Enrolled Device	Self Service and iOS is supported.
Jamf Console Access	Access to Jamf website at: https://yourHost.jamfcloud.com where <i>yourHost</i> is the URL portion provided from Jamf. Release 10.14.0 or later
An Administrator Account in Jamf Console	You need an administrator login with the Administrator permission access.

About MDM and MVISION Mobile Console Communication

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

Configuration Steps

This section describes the Jamf MDM and MVISION Mobile Console synchronization configuration along with the device enrollment and synchronization setup options.

Synchronization Overview

Devices can be synchronized through the MDM integration. This allows device management functions to be handled at the MDM console.

After the initial synchronization during the MDM integration setup, users are managed through a scheduled synchronization process. If there are additional devices in the device group(s) being used for synchronization, they are added to MVISION Mobile Console. If devices are removed, then they are removed from the MVISION Mobile Console. These changes do not remove any of the events associated with that device.

Enrolling a Device to Jamf

There are two ways to enroll a device and they are the following:

- URL and administrator login
- SMTP Server Setup and an enrollment invitation

URL and Administrator Login

After the application deployment is set up, you can enroll a device by invoking a URL on the device and logging in as an administrator.

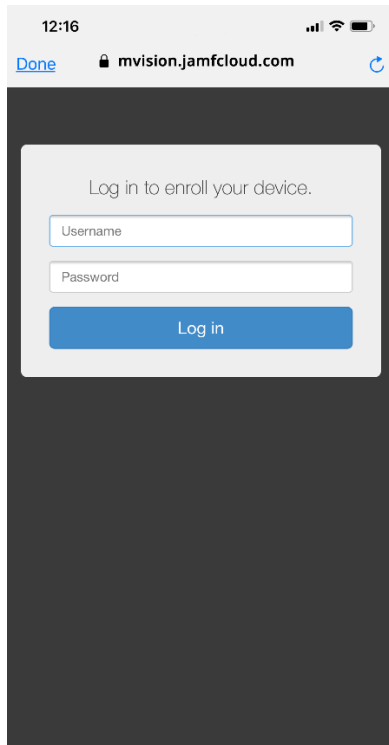
You must turn on the user-initiated enrollment for iOS devices in the Jamf console. The enrollment URL is the following website:

`https://yourHost.jamfcloud.com/enroll`

where *yourHost* is the URL portion provided from Jamf.

NOTE: Make sure the URL link has the “https” prefix or the URL may not load in a browser.

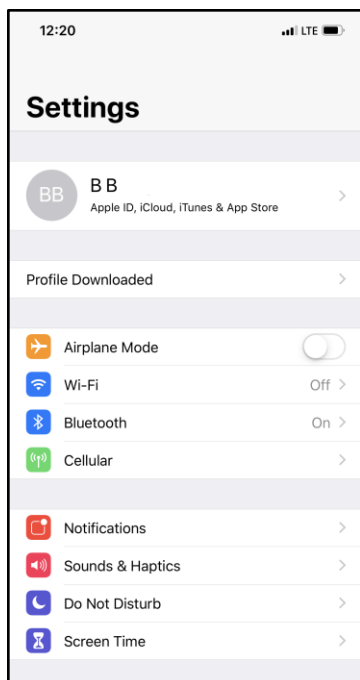
This URL brings up this screen on your iOS device.



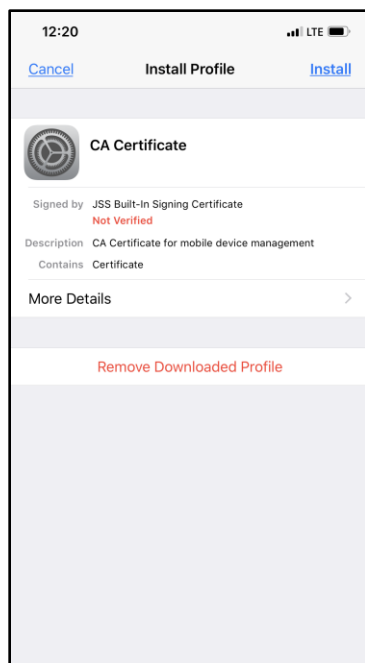
Perform the following steps:

1. Log in to the Jamf enroll page with a username and password.
NOTE: *Ensure you log in with an administrator's username and password.*
2. Skip over the "Assign to user" screen by clicking **Enroll**.
3. Click **Continue** and **Allow** for downloading the profile.
4. Click **Install** several times and **Done**, or later go to **Settings** on the device and do the additional steps below.
 - a. Click **Profile Downloaded** and install the profile.
 - b. Click **Install** and indicate to trust the profile. Then the profile is installed.

This figure shows how the profile is downloaded.



This figure shows you how the device requests you to install the profile. If you have already configured MVISION Mobile to download as an application in the Jamf console, MVISION Mobile downloads after the profile installs.



SMTP Server Setup and an Enrollment Invitation

The second option for enrolling a device does not require an administrator login. You first need to set up an SMTP Server.

Perform the following steps:

1. Log in to the Jamf console.
2. Select **Devices**.
3. Select **Management Settings**.
4. Select **System Settings**.
5. Select **SMTP Server**.
6. Provide the input field values for setting up your SMTP server.
7. Click the **Save** button.

This figure shows you an example screen of values for the SMTP server.

The screenshot displays the Jamf Pro console interface. On the left sidebar, the 'jamf PRO' logo is at the top, followed by navigation icons for 'Computers', 'Devices', and 'Users'. Below these, a summary section shows 'VERSION 10.14.0-t1563397490', 'MANAGED Computers: 1 Mobile Devices: 4', and 'UNMANAGED Computers: 0 Mobile Devices: 5'. The main content area is titled 'Settings > System Settings > SMTP Server'. It contains several configuration sections: 'Enable SMTP Server' (checked), 'SERVER AND PORT' (hostname 'smtp.mandrillapp.com' and port '587'), 'ENCRYPTION' (dropdown set to 'TLSv1.2'), 'CONNECTION TIMEOUT' (input '20' seconds), 'SENDER DISPLAY NAME' (input 'Jamf Pro Server'), and 'SENDER EMAIL ADDRESS' (input 'jamf-server@example.com'). A 'Requires Authentication' section (checked) includes fields for 'USERNAME' (input 'admin@example.com'), 'PASSWORD' (masked with dots), and 'VERIFY PASSWORD' (masked with dots).

Then, you need to set up device enrollment invitations. To complete the enrollment invitations, perform the following steps:

1. Log in to the Jamf console.
2. Select **Devices**.
3. Select **Enrollment Invitations**.
4. Click **+ New**.
5. Select **User-Initiated Enrollment** for the enrollment method.
6. Select either email or SMS messages for the invitation method.
7. Click **Next**.
8. Ensure the **Require Login** checkbox is unchecked. This figure shows this option.

9. Click **Next**.
10. Enter the email addresses and click **Next**.
11. Specify the email message details such as the subject and messages text.
12. Then click **Next** and click **Done**. This figure shows you some sample values for the message details.

After the SMTP server setup and the email being configured and sent, the recipient of the email can click on the link and enroll their device.

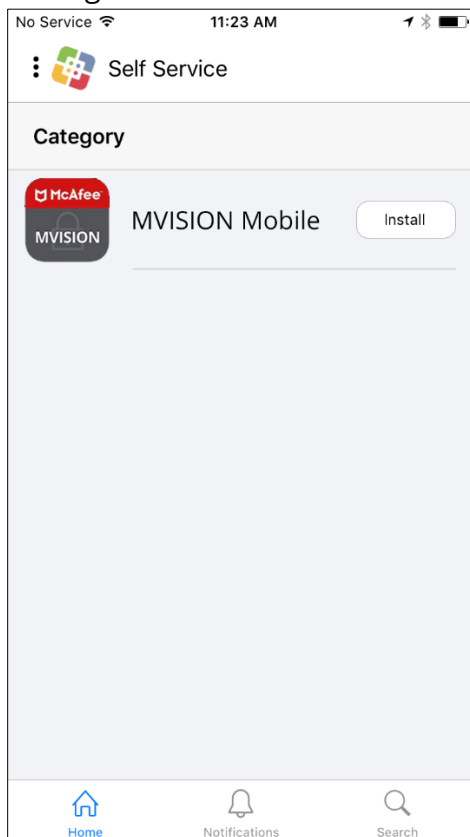
About and Enrolled Device

When a device is enrolled, and you have set up the following, the Jamf app is pushed to the device:

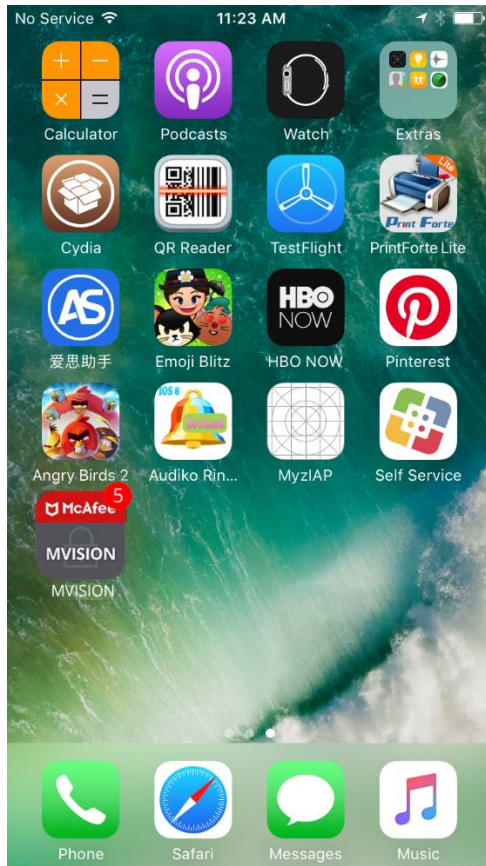
- Assign the device to a device group or a user, if desired.
- Upload or link to an app like MVISION Mobile.
- Assign the app to device groups, user groups, or devices.

You can click on the Self Service app and install the configured app.

This figure shows the MVISION Mobile app ready to install from Self Service.



This figure shows the Jamf app and MVISION Mobile is installed.



NOTE: The MVISION Mobile application displays after you have completed the items in the section [“Device Application Deployment Set Up.”](#)

On-Demand MDM Synchronization

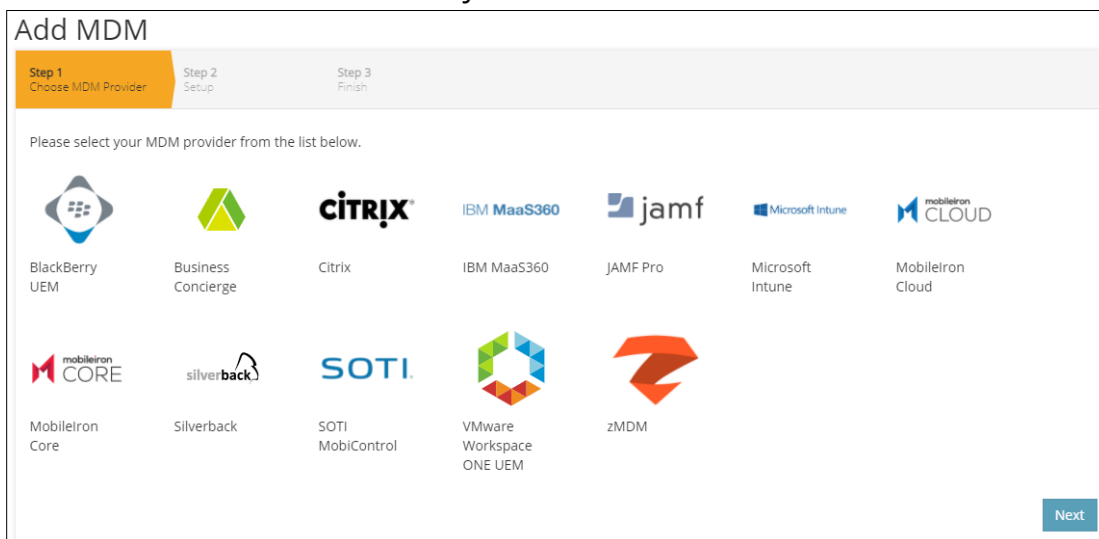
Due to the MDM synchronization window, there are times where a new MDM user has MVISION Mobile pushed down to their device and attempts to start it prior to the device actually being synchronized from the MDM. MVISION Mobile Console handles this by doing an on-demand synchronization when MVISION Mobile tries to activate, but no information yet exists for it. MVISION Mobile Console gets the identification information from MVISION Mobile used for the authentication and matches it up with the proper customer for authentication. Once that happens, MVISION Mobile Console retrieves the device and user information from the MDM configured for that customer. MVISION Mobile on that device is now authenticated and allowed to proceed.

See the [“Configuring Device Application Auto-Activation”](#) section for information on setting up iOS devices.

Set Up Synchronization in MVISION Mobile Console

To set up device synchronization in MVISION Mobile Console, perform the following steps:

1. Ensure you completed adding a Jamf administrator user in the Jamf console. See the [“Jamf User with Administrator Access”](#) section for these instructions.
2. Ensure that you created one or more Jamf device groups that contain the devices to be protected. See the [“Device Application Deployment Set Up”](#) section for more information on this setup.
3. Log into MVISION Mobile Console and navigate to Manage > Integrations.
4. Click on **Add MDM** and select the JAMF Pro icon.



5. Enter the information for the Jamf Pro integration in the table

Item	Specifics
URL	URL of the Jamf Server which is in the following format: https://yourHost.jamfcloud.com/ where <i>yourHost</i> is the URL portion given to you by Jamf.
Username	The Jamf Administrator username that was created and is used to log into the Jamf console.
Password	The password of the Jamf Administrator used to log into the Jamf console.
MDM Name	The name used in MVISION Mobile Console to reference this MDM integration. This name is prepended to the group name to form the MVISION Mobile Console group name.
Background Sync	Check this box to ensure users and devices are synchronized with the chosen Jamf Device Groups.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, such as name or 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 zConsole for Android Devices	This check box does not apply. Only iOS is supported.

This figure shows the dialog box when fields are filled in with values.

Add MDM

Step 1 Choose MDM Provider | **Step 2 Setup** | Step 3 Finish

URL
Specify URL for this MDM provider.

Username
Specify username for this MDM provider.

Password
Specify password for this MDM provider.

MDM Name
Specify a unique name for this MDM provider.

Background Sync ☒
Background sync: Specify if this MDM provider should automatically synchronize users, devices, apps and profiles on a periodic basis.

Mask Imported User Information ☐
By enabling this option, personally identifiable information will be masked (first name, last name and email) from MVISION

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

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

Next

- Click **Next** and choose one or more Jamf device groups to synchronize. The available device groups are shown on the left under the 'Available MDM Groups' column and can be moved over to the 'Selected MVISION Mobile Groups' column by clicking on the plus sign ('+'). This can be reversed by clicking on the minus sign ('-').

Add MDM

Step 1 Choose MDM Provider | Step 2 Setup JAMF Pro | **Step 3 Finish**

Available MDM Groups

- Pending Activation (+)
- Pre-sales Devices (+)
- SampleGroup (+)
- SampleUser (+)

Selected MVISION Mobile Groups

- JAMF_IOS (-)

If a user is a member of more than one MDM group, the user will be placed in the zConsole group with the higher priority.

Finish

NOTE: The groups display after you have completed the items in the section "[Device Application Deployment Set Up](#)".

7. Click **Finish** to save the configuration and start the first synchronization. Each device group selected is set up as a MVISION Mobile Console group for defining the following settings:
 - Privacy
 - Role access
 - Threat Policy

If a device falls into more than one Device Group, the highest or its first device group is its MVISION Mobile Console group. To change the order of the listing, drag and drop device groups as needed.

- The device groups are retrieved, and user/device synchronization is complete.
- You can verify the completion by navigating to the Devices page in the MVISION Mobile Console and verify the device display. The device entries are greyed out until the user starts up MVISION Mobile and activates the app.

See the *"MVISION Mobile iOS Product Guide"* on the customer portal for further device activation information on iOS devices. See the *"McAfee MVISION Mobile Console Product Guide"* in the customer portal for further MDM activation information.

Device Application Deployment Set Up

Overview

This section covers device application deployment and describes the initial setup required. For the initial setup you define or configure the following:

- Administrator User with Access
- Device Groups
- MVISION Mobile Application (iOS only)

See the Jamf documentation website for more information on how to use the console:

<https://www.jamf.com/resources/product-documentation/jamf-pro-administrators-guide/>

Jamf User with Administrator Access

Log in to the Jamf console and define a user that has administrator privileges.

To create a Jamf administrator with the proper access, perform the following:

1. From the main menu, select **Computers**.
2. Click **Management Settings**.
3. Click **System Settings**.
4. Select **Jamf Pro User Accounts and Groups**.
5. Click the **+ New** button.
6. Choose to create a standard account.

7. Enter the field values for the new administrator.
 - Ensure the Access Level is “Full Access”.
 - Ensure the Privilege Set is “Administrator”.
8. Click **Save**.

This figure shows the menu selection for creating the user.

The screenshot displays the Jamf Pro web interface. On the left is a dark sidebar with navigation icons for 'Computers', 'Devices', and 'Users'. Below these are system statistics: 'VERSION 10.14.0-11563397490', 'MANAGED Computers: 1, Mobile Devices: 3', and 'UNMANAGED Computers: 0, Mobile Devices: 6'. At the bottom of the sidebar is a 'Collapse Menu' button. The main content area shows the 'Settings > System Settings > Jamf Pro User Accounts & Groups' breadcrumb trail. The title is 'SampleUser'. There are two tabs: 'Account' (selected) and 'Privileges'. The 'Account' tab contains several form fields: 'USERNAME' (SampleUser), 'ACCESS LEVEL' (Full Access), 'PRIVILEGE SET' (Administrator), 'ACCESS STATUS' (Enabled), 'FULL NAME' (Sample User), 'EMAIL ADDRESS' (duser6532@g.com), 'PASSWORD' (masked with dots), and 'VERIFY PASSWORD' (masked with dots). There is also a checkbox for 'Force user to change password at next login'. At the bottom right of the form are buttons for 'Done', 'History', 'Clone', 'Delete', and 'Edit'.

Device Groups

There are two types of device groups available to organize and synchronize devices with MVISION Mobile Console. There are:

- Smart Device Groups
- Static Device Groups

You can choose how your devices are organized into one or more device groups. For example, device groups can organize devices for different risk postures.

When you add the Jamf MDM to the MVISION Mobile Console, the following items are created:

- Extension Attribute of the McAfee risk posture.
- Device Groups for the different risk postures.

These device groups are created with specific criteria and aligning them for specific risks, and using this is a good practice.

The figure below shows an example smart device group named 'McAfee Risk Posture Critical' that has the criteria set to the risk posture value being a 'Critical' value. The valid values are the following:

- Critical
- Elevated
- Low
- Normal

NOTE: *The spelling on these matched values is important to accurately match.*

This figure shows the criteria for a smart group named 'McAfee Risk Posture Critical'. This is created for you when you add the Jamf MDM to the MVISION Mobile Console.

The screenshot shows the configuration for a smart device group named 'McAfee Risk Posture Critical'. The interface includes a breadcrumb trail 'Mobile Devices > Smart Device Groups > McAfee Risk Posture Critical'. Below the title, there are three tabs: 'Mobile Device Group', 'Criteria' (which is selected), and 'Automated Management'. To the right of the tabs is a checkbox labeled 'Show in Jamf Pro Dashboard'. The 'Criteria' tab displays a table with four columns: 'AND/OR', 'CRITERIA', 'OPERATOR', and 'VALUE'. The table contains one row with a dropdown arrow in the 'AND/OR' column, 'McAfee Risk Posture' in the 'CRITERIA' column, 'is' in the 'OPERATOR' column, and 'Critical' in the 'VALUE' column. There is also a dropdown arrow at the end of the 'VALUE' column.

You use these device groups to manage the devices that have specific risk postures.

About MVISION Mobile Deployment

To deploy the MVISION Mobile application through Jamf MDM, use the version of MVISION Mobile available through the Apple App Store. The latest iOS MVISION Mobile is in the application stores, and it is good practice to deploy the latest MVISION Mobile application through Jamf.

To obtain the MVISION Mobile application from the public application store, search the appropriate store for MVISION Mobile. This link has the latest available version of MVISION Mobile for iOS:

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

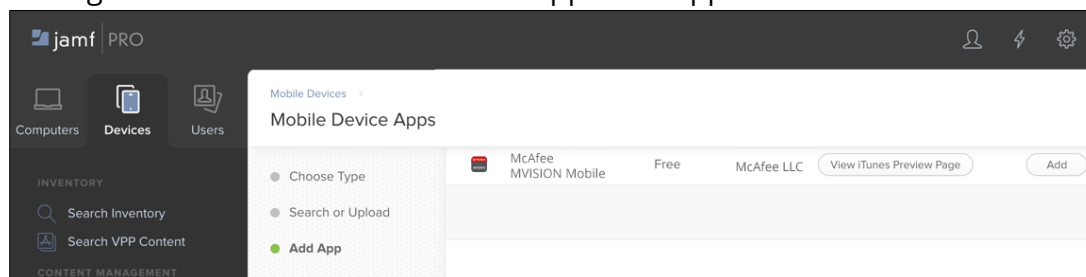
To deploy as an internal app, log in to Jamf, specify the proper application (or IPA file for iOS) to Jamf under app configuration.

Depending on customer requirements, a custom version of the app can be needed. In that case, contact your Customer Success team, and the custom version of MVISION Mobile can be added as an internal app in Jamf.

To load MVISION Mobile as an app for deployment, perform the following:

1. From the main menu, select **Devices**.
2. Select **Mobile Device Apps**.
3. Click **+ New**.
4. Choose an App Type of **App Store app**.
5. Click **Next**.
6. Type in "McAfee MVISION" in the search dialog and set the app store country as "United States".
7. Click **Next**.
8. Select McAfee MVISION Mobile by clicking the **Add** button.
9. Provide a display name and ensure you select the following on the General tab:
 - **Install Automatically/Prompt Users to Install** for the Distribution Method.
 - **Automatically Force App Updates** should be enabled.
10. For the Scope tab, you can specify specific devices, users, user groups, or you can specify all devices and users. You can specify a device user group as a specific target and this is the recommended method.
11. For the App Configuration tab, use the App Config Generator. Select the file from the repository "com.jamfsoftware.casperfocus/current" as the default. Specify the known values and add additional configuration values as needed. See the table in the "iOS Activation" section for more information.
12. Click **Save**.

This figure shows the MVISION Mobile app as an app to add.



This figure shows the attributes to select for the app on the General tab. Ensure "Automatically Force App Updates" is enabled. It is not enabled in the Jamf console by default.

Mobile Devices > Mobile Device Apps >

McAfee MVISION Mobile

General Scope VPP App Configuration

DISTRIBUTION METHOD Method to use for distributing the app

Install Automatically/Prompt Users to Install ▼

- ☒ Display app in Self Service after it is installed
- ☐ Require tethered network connection for app installation (iOS 10.3 or later)
Require the device to have a tethered network connection to download the app
- ☐ Schedule Jamf Pro to automatically check iTunes for app updates
Automatically update app description, icon, and version in Jamf Pro
- ☒ Automatically Force App Updates
Automatically force updates for this app on mobile devices (VPP-managed apps or free apps)
- ☒ Make app managed when possible
Make the app managed when managed app requirements are met

This figure shows the App Config Generator with sample values. This can be invoked from the App Configuration tab or this website:

<https://appconfig.jamfresearch.com/>

AppConfig Generator

The AppConfig Generator is a tool which assists in the generation of configuration plist for a mobile app on a device enrolled in an MDM solution.

For more information on AppConfig visit: appconfig.org or view the [AppConfig Spec Reference](#)

Follow the steps below to get started:

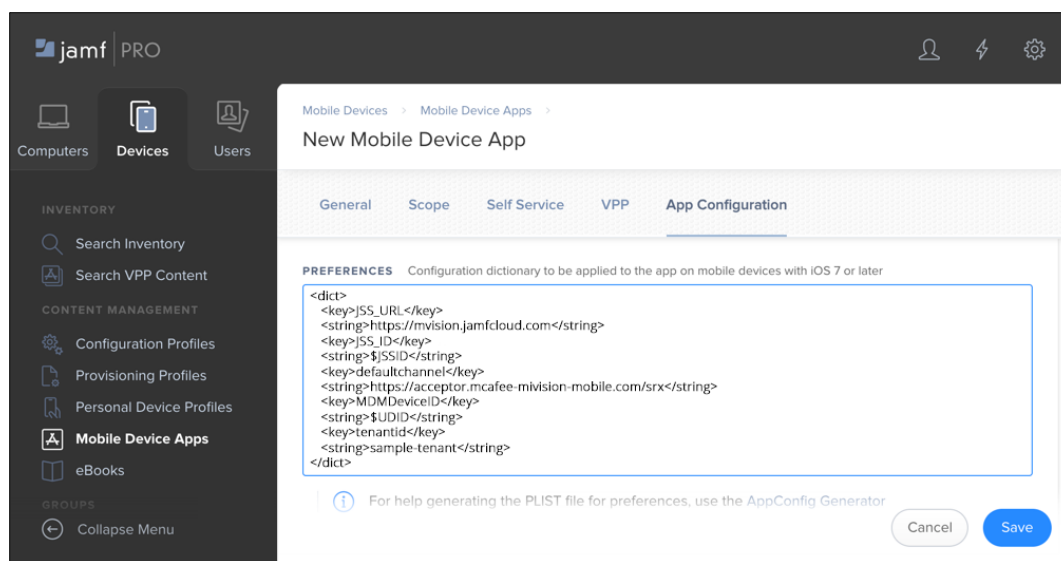
1. Fill out the presented configuration options
2. Download the plist configuration file
3. Upload the plist to your MDM provider to be installed onto the device

JSS URL

URL of your JAMF Software Server

JSS_ID

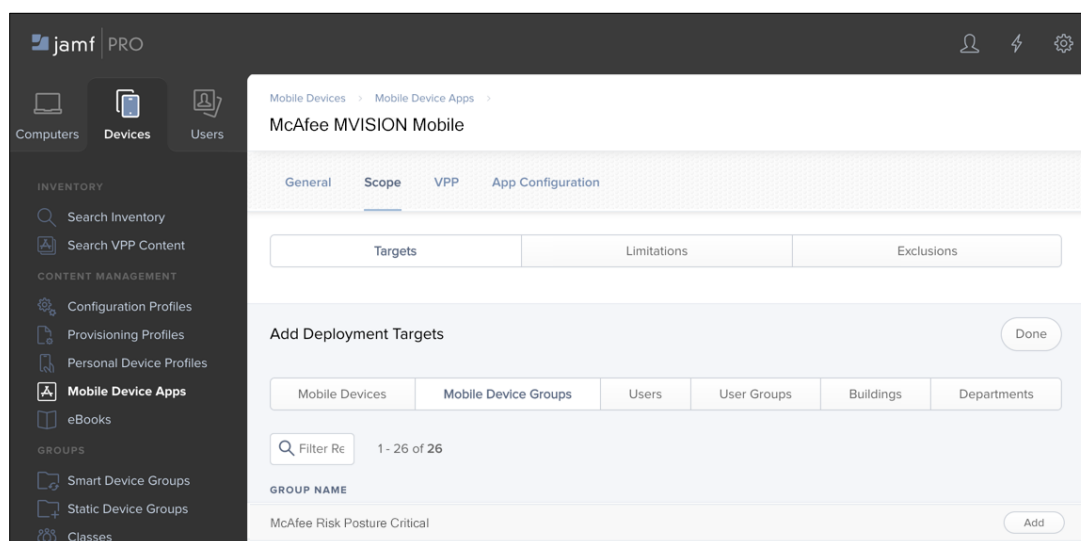
This figure shows a sample App Configuration tab populated.



Configuring Scope of Device Application

For a mobile device application like MVISION Mobile, you can define the scope of the application. You can define the scope with mobile device groups similar to the figure. Or you can define specific user groups, devices, or users.

This figure shows MVISION Mobile having a mobile device group scope of the smart group of devices with a critical risk posture.



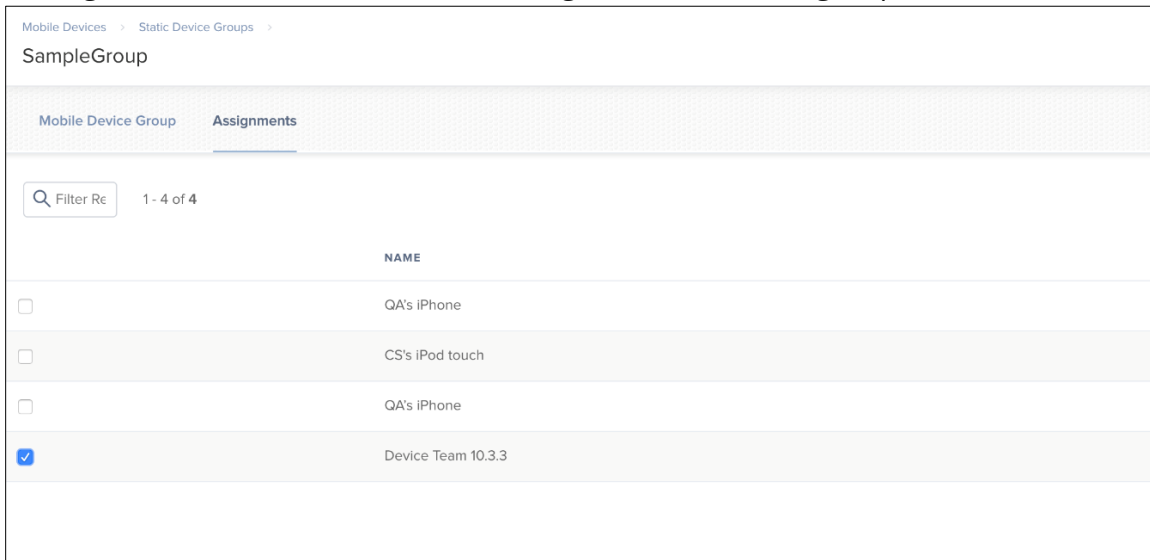
Assigning an Enrolled Device to a Static Device Group

If you decide to use Static Device Groups instead of Smart Device Groups, the following steps describe how to assign an enrolled device to a static device group.

Perform the following:

1. Log in to the Jamf console.
2. Select **Devices**.
3. Select **Static Device Groups**.
4. Select the group within which you want the device.
5. Click on **Assignments** and **Edit**.
6. Select the desired device(s) and **Save**.

This figure shows the list of devices for a given static device group.



Mobile Devices > Static Device Groups > SampleGroup	
Mobile Device Group	Assignments
Filter Re	1 - 4 of 4
	NAME
<input type="checkbox"/>	QA's iPhone
<input type="checkbox"/>	CS's iPod touch
<input type="checkbox"/>	QA's iPhone
<input checked="" type="checkbox"/>	Device Team 10.3.3

Configuring Device Application Auto-Activation

The McAfee MVISION Mobile application for iOS can automatically activate. The process is the following sections.

iOS Activation

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

This configuration is performed within Jamf. During the add application step, there is a configuration option. As another alternative, you can edit the application after the application is added.

Configuration Key	Value Type	Configuration Value
MDMDeviceID	String	\$UDID
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).

NOTE: The configuration keys are case sensitive if they are specified in the XML.

About App Configuration

For the app configuration, you can use the app configuration generator which generates a starting PLIST file for you.

Set the PLIST XML value in the field under the **App Configuration** tab. This shows an example PLIST XML value.

```
<dict>
  <key>JSS_URL</key>
  <string>https://mvision.jamfcloud.com</string>
  <key>JSS_ID</key>
  <string>$JSSID</string>
  <key>defaultchannel</key>
  <string>https://acceptor.mcafee-mvision-mobile.com/srx</string>
  <key>MDMDeviceID</key>
  <string>$UDID</string>
  <key>tenantid</key>
  <string>sample-tenant</string>
</dict>
```

Device Actions and Remediation

The McAfee integration with Jamf provides a way to block access to company data such as email and other services. If a threat is detected on a device and that threat has an MDM action of 'Inform EMM', then MVISION Mobile sends the new mobile threat level of that device to Jamf. The mobile threat level of the device is the highest threat event classification that is pending for that device, also known as the risk posture in the Jamf console.

When the risk posture of 'Critical' matches, then the device has a high mobile threat level, and this makes the device non-compliant.

Then navigate to the Policy page in MVISION Mobile Console and select the MVISION Mobile Console group you want to target. For each threat classification that you want Jamf 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' as well, and the Mobile Threat Level of the device is adjusted accordingly.

Available Device Actions

The available MDM actions for the Jamf MDM in the MVISION Mobile Console are the following:

- No Action
- Lock Device
- Erase Device
- Inform EMM

NOTE: *The default action is the 'Inform EMM' action.*

Synchronizing iOS Apps

For iOS, we retrieve the iOS app list through the configured MDM and evaluate if the apps are malicious or legitimate. In addition, the security and privacy risks associated with the app is provided, if the MVISION Mobile Advanced license has been purchased.

The following steps allow an administrator to see the iOS apps in the MVISION Mobile Console:

- The device is enrolled in the MDM and with MVISION Mobile.
- The user installs a new app on the device.
- The MDM sees the new app in the sample request update.
- MVISION Mobile sees the new app when the MDM sync is performed for that device.

NOTE: *The synchronization of the iOS profiles is not supported by this MDM.*