McAfee MVISION Mobile

Business Concierge

Integration Guide

January 2021

Contents

Preface

This document is an administrator's guide to providing integration with SOTI MobiControl 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 SOTI MobiControl MDM. The MVISION Mobile Console application provides threat protection to mobile devices. The system administrator sets policies for threats and the MDM configuration.

See "*MVISION Mobile Console Product Guide*" for more information.

Related Documentation

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

Overview

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

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

McAfee's MVISION Mobile application detects malicious activity and depending on the MDM platform, is able to take action locally. When MVISION Mobile is integrated with an MDM, protection actions can be performed by the MDM in addition to local MVISION Mobile actions, providing a very powerful protection tool.

This document outlines the integration with Softbank's Business Concierge Device Management system.

Prerequisite Requirements

Integration with Business Concierge Device Management requires a connection between the MVISION Mobile Console and the Business Concierge Device Management server. This is accomplished through configuration on the Business Concierge Device Management side and also in the MVISION Mobile Console.

The following table details specific requirements for the API connection and Business Concierge integration.

Item	Specifics
Business Concierge Device Management	Release 12.3 and later
Administrator Account in Business Concierge Device Management Console	Refer to the "Access to the Business Concierge Device Management Console" section.
Device and OS	iOS 9.0 and later 64-bit devices required (Android is not supported at this time.)
MVISION Mobile	Release 4.8.0 and later
Integration Protocol	Secure Sockets Layer (SSL) protocol
MVISION Mobile Console	Release 4.22 and later

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the Business Concierge Device Management console through API access. If users are removed, then they are removed from the MVISION Mobile Console. These changes do not remove any of the events associated with that user or device.

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 Business Concierge Device Management system and provides the commands to perform the action described.

Full MDM Synchronization

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

On-Demand Device Synchronization

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

Access to the Business Concierge Device Management Console

To begin Business Concierge Device Management integration, contact and request an administrator account. An administrator account provides the following:

- DM Code
- Login ID
- Password

NOTE: *Business Concierge Device Management is currently available for Japanese customers only through SoftBank.*

Configuration Steps

Configuration steps are performed on both the Business Concierge Device Management console side and the MVISION Mobile Console side. In setting up this integration configuration the following are supported:

- Manages the user lifecycle.
- Synchronizes devices and their associated users.
- Handles device and user management functions with the MDM console.

NOTE: *The Business Concierge Device Management APIs do not yet support multiple groups, so for now all devices must be chosen for synchronization. Any groups defined in the Business Concierge Device Management console do not show up in MVISION Mobile Console.*

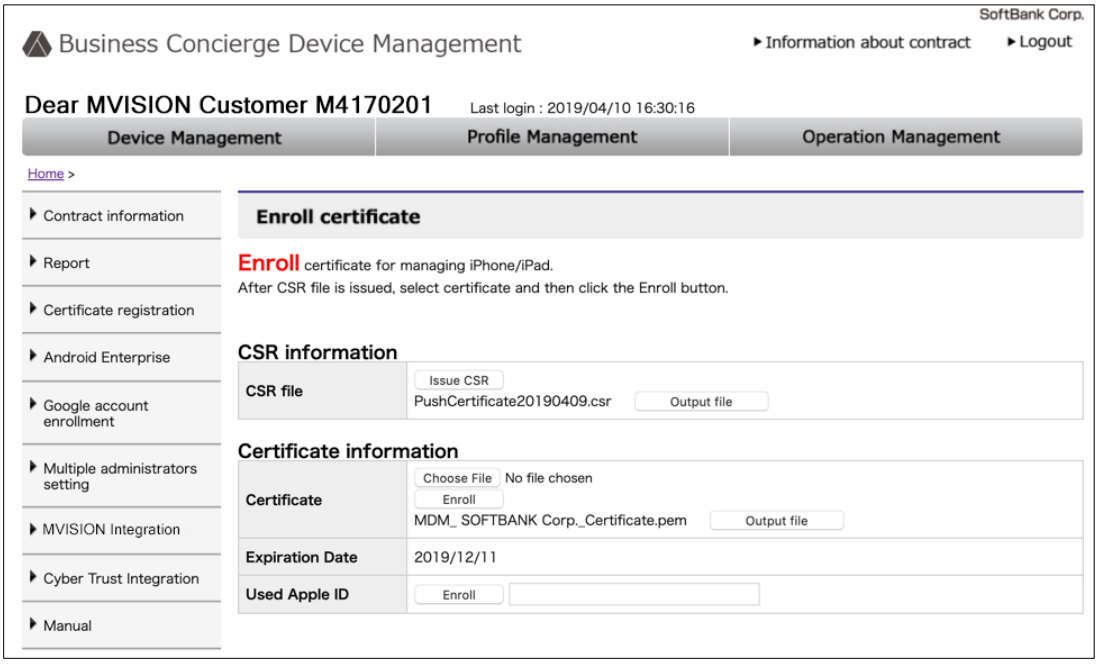
Certificate Configuration

This section details the steps for setting up the certificate in Business Concierge Device Management.

Perform the following steps:

1. Log in to the Business Concierge Device Management console.
2. Select **Information about Contract**.
3. Click **Certificate registration**.
4. Click **Issue CSR.** This generates a push certificate CSR file.
5. Click the **Output file** button under the CSR Information. This downloads the CSR file.
6. Then log in to the Apple Push Certificates Portal website: https://identity.apple.com/pushcert/
    a. Generate the certificate PEM file
    b. Download the PEM file.
7. In the Business Concierge Device Management console, under Certificate information, click on the **Choose File** button. Select the PEM file.
8. Click the **Enroll** button.

The figure shows the result of these steps.



Setting Email Addresses for Users Before Sync

When a user is created in Business Concierge Device Management, the user needs to be updated to provide the email address for synchronization with MVISION Mobile. New users do not initially have email addresses defined in Business Concierge Device Management.

To support synchronizing devices based on users, you must enter an email address in the user profile in Business Concierge Device Management. Otherwise, the default email address is assigned. This is in the format of '*tenant_name*-**user@qmpr.com**' where *tenant_name* is the tenant name in MVISION Mobile Console.

To update the user email address, perform the following steps:

1. Log in to Business Concierge Device Management.
2. Click **Device Management**.
3. Click **User Information**.
4. Click **User information list**.
5. Scroll through the list of users and select the user to modify.
6. Click **Change**.
7. Scroll down and update the email address for the 'Zimperium email address' field.
8. Click **Ok**.

Device Registration in Business Concierge Device Management

To integrate with the MDM, the end-user of the device needs to install the software on the device itself.

To set up device registration:

1. In the upper right, click **Information about Contract**.
2. Scroll down the page and see the section **Information for Device Registration**. This section has the URL that the user uses to register their device. It also includes the required login information. Ensure the **iPhone/iPad** option is selected.

iPhone/iPad	Android	4G Mobile	PC

Start date	2018/10/22
First start date	-

Information for Device Registration

Enrollment URL	http://stara.gbcdm.com/
DM code	M317020170
Enrollment ID	user106
Enrollment password	1780

3. Notify the user of the enrollment URL and the additional fields of DM code, Enrollment ID, and the Enrollment password. After the user opens the URL on the device, provides the authentication, and follows the prompts, the profile is installed. If MVISION Mobile is configured as a managed application, it is also installed on the device.

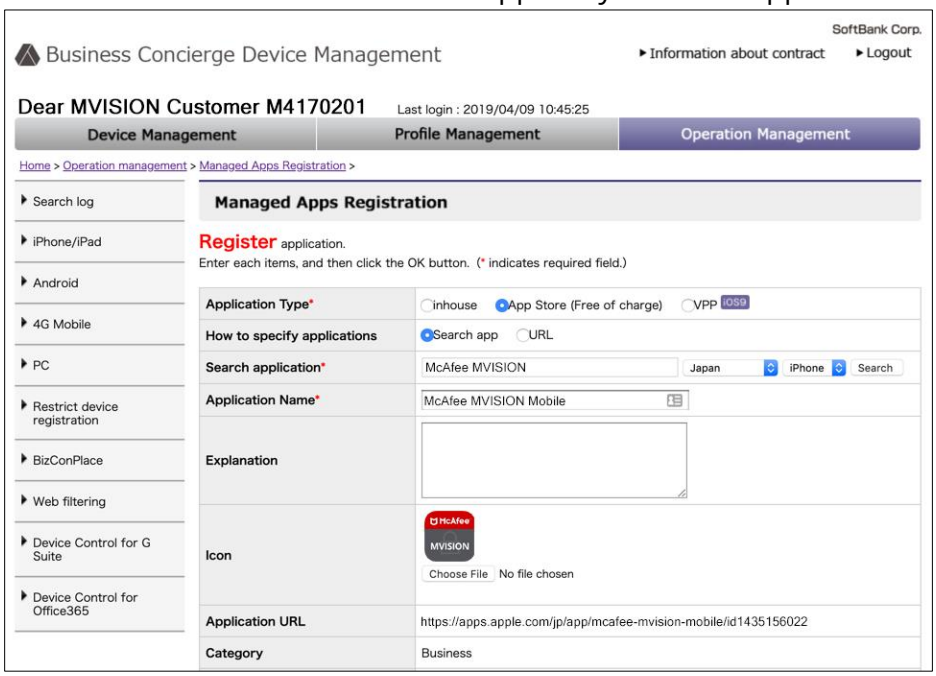
Set Up Device Application Deployment

This section details the steps for setting up the deployment of the device application in the Business Concierge Device Management system.

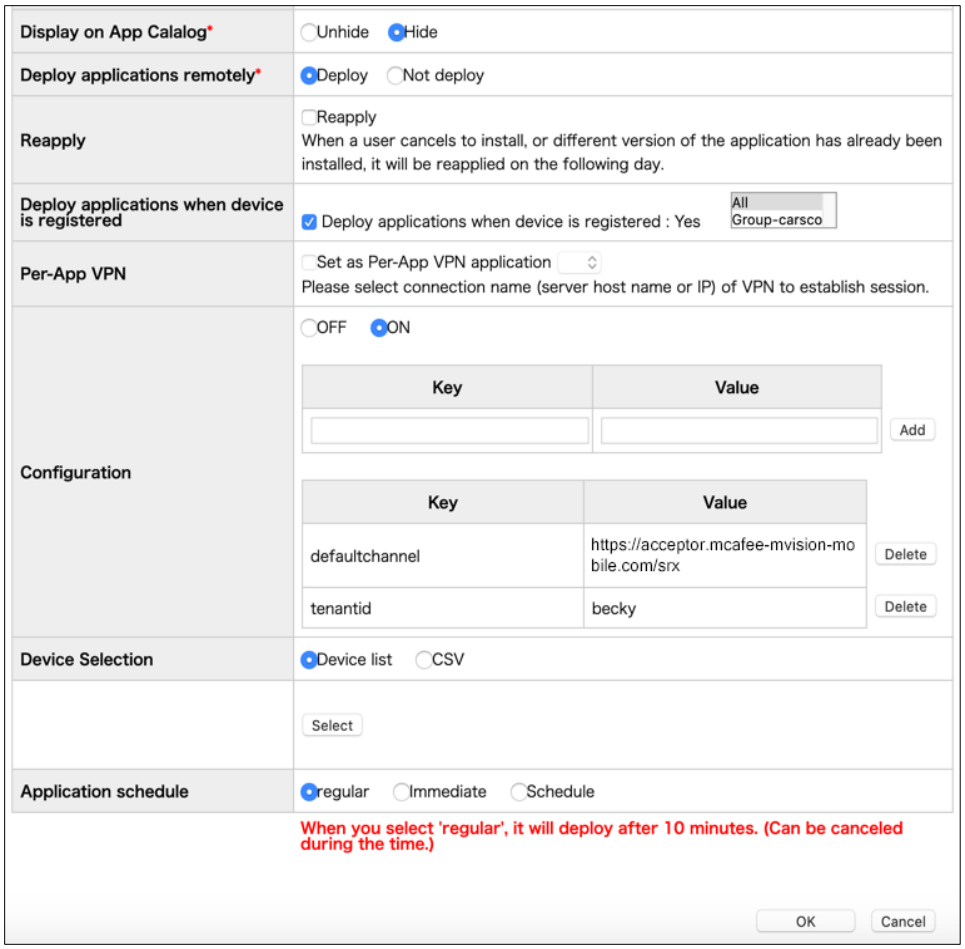
Initial Configuration in Business Concierge Device Management

You need to define the application under the Operation Management section as a managed app. This is defining what is pushed down to the registered devices. This step identifies the MVISION Mobile application from the Apple App Store. Perform the following steps:

1. Select **Operation Management**.
2. Click **iPhone/iPad**.
3. Click **Managed Apps Registration**.
4. Select the **App Store** under the Application Type.
5. Enter 'McAfee MVISION' as the search application input field value and click **Search**.
6. Select the McAfee MVISION Mobile app entry from the App Store list.



7. Set the Configuration toggle to 'ON' and set the auto-activation as described in section "Configuring Device Application Auto-Activation".
8. Under 'Device Selection', select either **Device list** or **CSV** to provide a list of devices. If you select 'Device list', then select the list of devices. If you select 'CSV', then upload a CSV file for the device list.
   NOTE: *Devices need to be enrolled in the Business Concierge Device Management system prior to selecting them in this step. Otherwise, you need to modify the managed app.*



9. Click **OK** and **OK** again to register.
   NOTE: *Some attributes on the managed application setup are not easily updated, so ensure that you set the configuration and the fields, as needed, before saving the registration. For example, If you need to change the configuration key values, you may need to remove and then re-add the managed application.*

Configuring Device Application Auto-Activation

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

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

This configuration is performed within the Business Concierge Device Management console. During the add managed application step there is a configuration option. Ensure this option is set to 'On'.

1. Use the values in the table for the configuration values.

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

NOTE: *The configuration keys are case sensitive. The usual device identifier field (such as UUID) is not in the configuration key list. The Business Concierge Device Management system populates this value itself internally.*

2. Choose **Configuration** and set it to 'Yes', and enter the 'Key' and 'Value' fields for the Configuration Keys.

This figure shows sample configuration values with the sample required configuration keys.

Configuration	Key	Value
	defaultchannel	https://acceptor.mcafee-mivision-mobile.com:443/srx
	tenantid	becky

Set Up User and Device Synchronization in MVISION Mobile Console

Determine the API URL, Access Key, and Secret Key

Before you can add the Business Concierge Device Management MDM in the MVISION Mobile Console, you need to have the following values from the Business Concierge Device Management system:

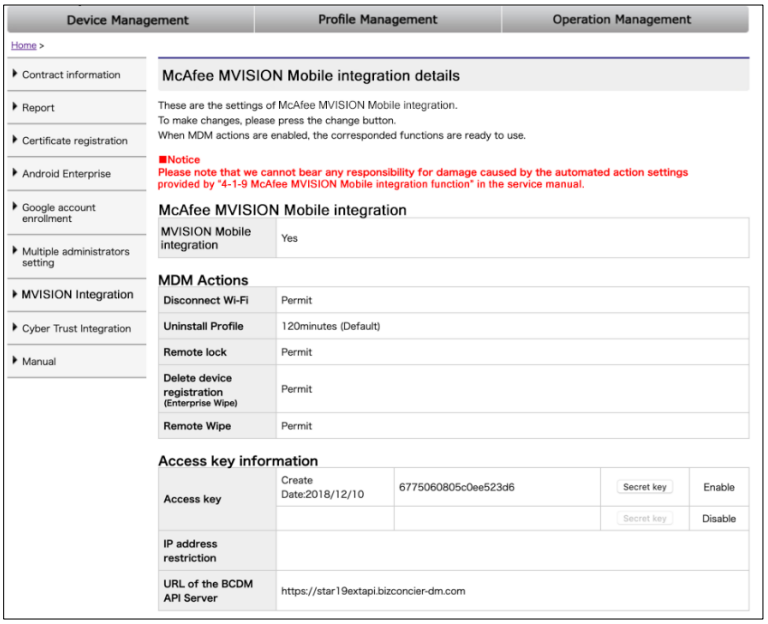
- API URL
- Access Key
- Secret Key (Password)

Perform the following steps:

1. In the upper right, click **Information about Contract**.
2. Select the **MVISION Integration** tab.
3. Note the data values in the section **Access key information** for the URL and the access key.
4. Click the **Secret Key** button and download the secret key provided in a CSV file.

   ***Note**: The API access key information is also on the initial screen display for the 'Information about contract' section, but the required API access information is under the Zimperium Integration tab.*

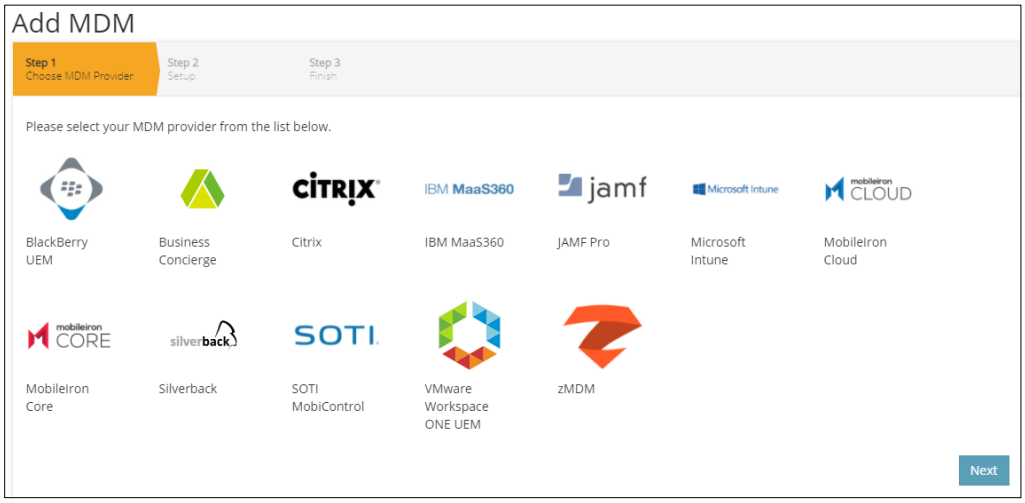
This figure shows an example of the access key information display under the Zimperium.



Add the MDM in MVISION Mobile Console

Perform the following steps:

1. Log in to MVISION Mobile Console and navigate to the **Manage** page.
2. Select the tab **Integrations**.
3. Click on **Add MDM** and select the Business Concierge Device Management icon and select **Next**.
   This figure shows the select of MDM icons.

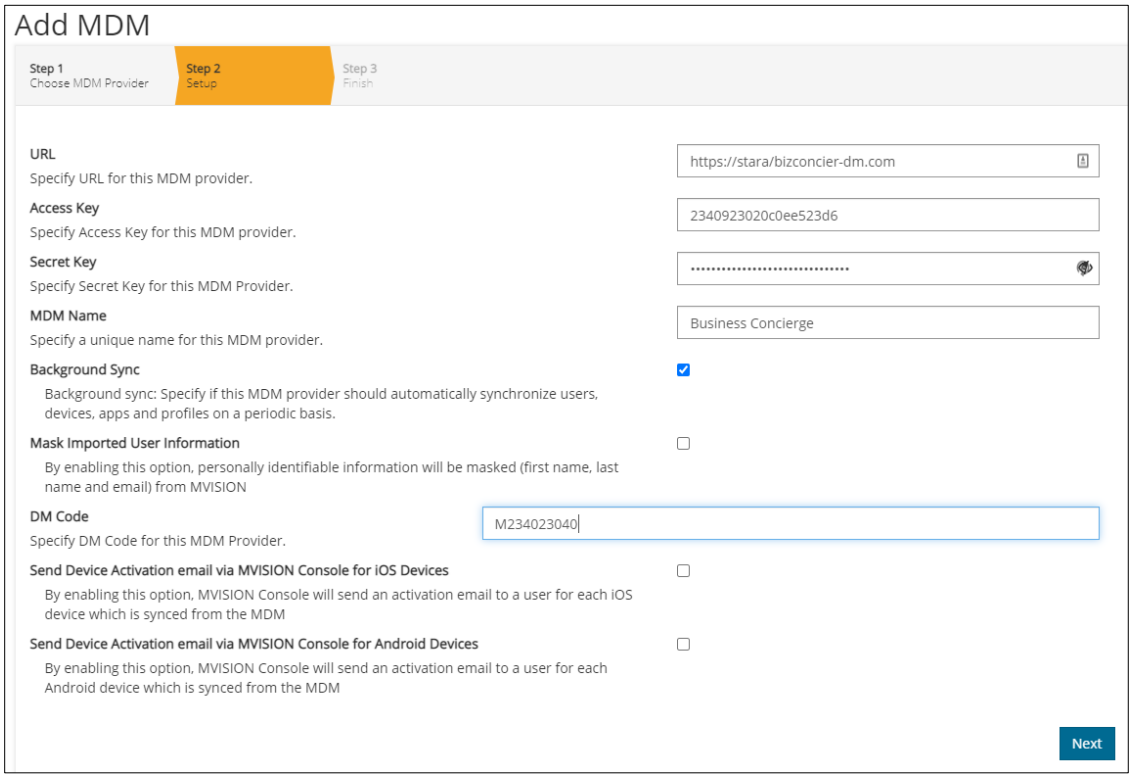


4. Enter the information for the Business Concierge Device Management integration in the table.

Item	Specifics
URL	This is the URL of the Business Concierge Device Management API server. You identified this string in the "Determine the URL, Access Key, and Secret Key" section. ***Note**: It is possible that this URL is not valid in a browser and can return a 404 error.*
Access Key	This is the access key provided by the Business Concierge Device Management console. You identified this string in the "Determine the URL, Access Key, and Secret Key" section.
Secret Key	This is the secret key provided by the Business Concierge Device Management console. You identified this string in the "Determine the URL, Access Key, and Secret Key" section.
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.

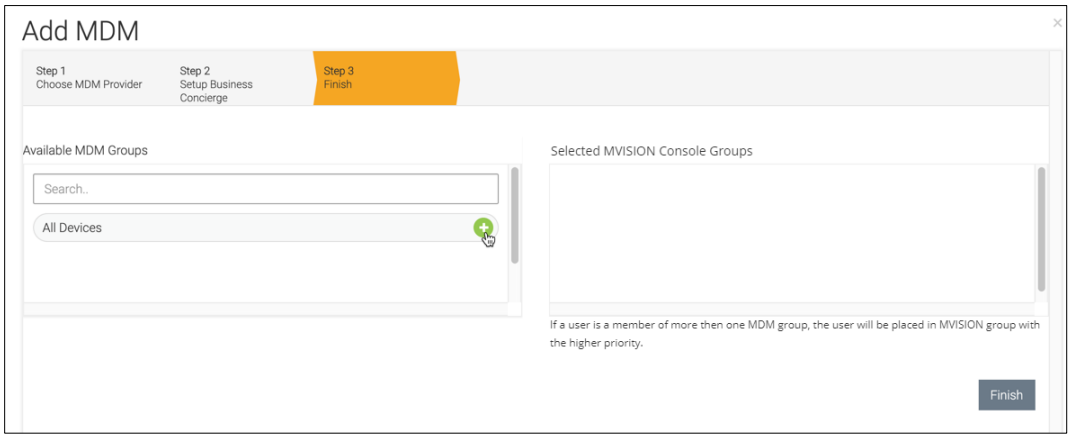
Background Sync	Check this box to ensure users/devices are synchronized.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, such as name or email address.
DM Code	This is the DM code value that is provided with your Business Concierge Device Management account.
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	Leave this checkbox unchecked.

This figure shows the screen with the input prompts for adding the MDM details.



5. Click **Next** and choose the 'All Devices' option with the plus-sign.

This figure shows the selection of all devices and the last step with the 'Finish' button.



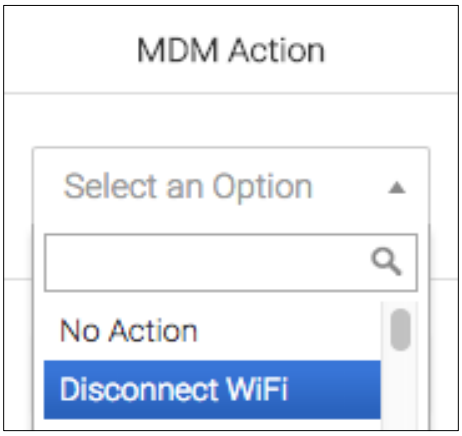
NOTE: *The Business Concierge Device Management APIs do not yet support multiple groups, so for now all devices must be chosen. Any groups defined in the Business Concierge Device Management console do not show up here.*

6. Click **Finish** to save the configuration and start the first synchronization.
7. You can verify the synchronization by navigating to the Devices page in the MVISION Mobile Console and verify the display. The device entries are greyed out until the user starts up MVISION Mobile and activates the app.
   NOTE: *The device apps and iOS profiles also synchronize if configured*.

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 API 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.

This figure shows a portion of an MDM Action dropdown on the Policies page for the Business Concierge Device Management group.



Available Device Actions

Business Concierge Device Management integration provides several MDM actions to push to the device. For example, choosing 'Disconnect Wi-Fi' causes the MVISION Mobile Console to notify Business Concierge Device Management to push a Wi-Fi profile to the device when the corresponding threat is detected. The device disconnects from the currently connected Wi-Fi network, removing it from the suspicious Wi-Fi network. Automatically, the profile is created automatically when a device is under attack. Then the profile is removed after a short period of time. (This only applies to iOS.)

For Business Concierge Device Management, the available MDM Actions are the following:

- No Action
- Lock Device
- Disconnect Wi-Fi
- Enterprise Wipe

The threat policy defines which action to take for each threat. The MDM Action 'Enterprise Wipe' removes the device from the Business Concierge Device Management console.

Managed App Details

The MVISION Mobile application is now published and installed on the registered devices. Your users have the auto-activated version of MVISION Mobile. You can monitor the status of the devices from the Business Concierge Device Management console.