



McAfee MVISION Mobile

BlackBerry Integration Guide

MVISION Mobile Console 4.23

June 9, 2019

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

Overview	4
BlackBerry UEM Enterprise Mobility Suite (MDM option)	4
Prerequisite Requirements	4
About MDM and MVISION Mobile Console Communication	4
Protection Methods	5
Configuration Steps.....	5
Basic Application Deployment	5
Synchronization.....	5
Auto Activation/Advanced Application Deployment.....	10
Granular Protection	13
BlackBerry Dynamics (Containerization Option).....	13
Prerequisite Requirements	13
About MDM and MVISION Mobile Console Communication	14
Protection Methods	14
MVISION Mobile App Device Actions	14
BlackBerry Dynamic MDM Actions	15
Configuration Steps.....	16
Basic Application Deployment	16
Synchronization.....	16
Auto Activation/Advanced Application Deployment.....	19
Granular Protection	21
Appendix A - UEM Messaging and Device Activation.....	22

Overview

BlackBerry currently maintains two products that McAfee integrates with, the Unified Endpoint Management Server (formerly known as BES) and BlackBerry Dynamics (formerly known as Good Dynamics). At this time while UEM can handle both products, this document details each in the following sections.

If you are using both UEM MDM and UEM Dynamics simultaneously, configure the firewall ports using the UEM Dynamics section.

Note: You need to review and configure McAfee MVISION Mobile App from both the UEM MDM and UEM Dynamics sections.

BlackBerry UEM Enterprise Mobility Suite (MDM option)

Prerequisite Requirements

Integration with UEM for MDM devices requires a connection between the McAfee MVISION Mobile Console and the UEM API server. This is accomplished via the Internet using SSL on TCP port 443 or 18084. Also, for an on-premise UEM management server, there must be an allowed path for the MVISION Mobile Console to connect to the API Server on port 443 or 18084.

The following table details specific requirements for the API connection:

Item	Specifics
UEM MDM enrolled device	UEM V12.4 Note: iOS App configuration is only supported in UEM V12.6+
API Administrator Account in UEM management console.	Proper Role defined in section below.
Access to certain TCP ports on the UEM Server	TCP/443 or 18084

Note: The MDM integration does not support the UEM Cloud version (SaaS management server) because it does not support the APIs needed for MDM integration. However, the MDM integration does support the on-premise UEM product.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console server is configured to share information with the UEM console through API access. When MVISION Mobile App 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 Cloud server. The Cloud server then reaches out to the proper UEM API Server and provide the commands to perform the action described.

Protection Methods

McAfee interacts with the UEM 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 device and delete only work data.

Configuration Steps

Basic Application Deployment

To deploy the MVISION Mobile App application through UEM, download both iOS and Android MVISION Mobile App from their respective public application stores.

To publish the MVISION Mobile App application from the public application store, create a new app from the App Store or Google Play Store and search for the appropriate MVISION Mobile App app. Or, you can use these links:

Login to UEM and navigate to Apps and choose to Add a new Internal app. Create a new Internal Application and upload the proper application file (IPA for iOS and APK for Android) to UEM. Assign the User Group to the application and publish.

At this point the application is now published and installed on the devices in the User Group assigned. Your users can now activate the application as described in the platform guides in the support portal. They need the activation link created in the MVISION Mobile Console to access the application, unless a synchronization is performed (with iOS or Android Enterprise).

Synchronization

Full MDM Synchronization

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

- **New Enrollments** - If we see additional users in the User Group(s) being used for synchronization, they are added along with their devices to MVISION Mobile Console.
- **Unenrolled Users** - If we see users removed, then they are removed from the MVISION Mobile Console. Doing this does not remove any of the events associated with that user or device.

On-Demand Device Synchronization

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

MVISION Mobile Console gets the identification information from MVISION Mobile App used for the authentication and matches it up with the proper customer for authentication. Once that happens, MVISION Mobile Console retrieves that device and user information from the MDM configured for that customer. MVISION Mobile App on that device is now authenticated and allowed to proceed. This type of synchronization adds devices over time as they are activated.

Prerequisites

For this to work correctly, MVISION Mobile App must be deployed as follows:

- **iOS:** Associate an app configuration with the MVISION Mobile App application that pushes down the **Tenant ID** and **Default Channel** to be used for the on-demand device sync. This is described in the section “Auto Activation/Advanced Application Deployment” below.
- **Android:** This requires Android for Enterprise for auto-activation. Use MVISION Mobile Console activation URLs for native Android. Contact your McAfee Customer Support Team for more information on this topic.

Synchronization Setup

To set up synchronization, perform the following steps:

- 1) Create a UEM administrator with the proper role access:
Navigate to: Settings/ Administrators/ Roles/ Add a role. Provide name, Description and select the following:

Directory access:

- Select either All company directories or Selected company directories as needed.

Group Management:

- All groups and users

User and Devices:

- View users and activated devices
 - Export user list
 - Manage devices
 - Disable workspace
 - Lock workspace
 - Lock device and set message
 - Delete only work data
 - Delete all device data
 - Specify work password and lock
 - Get device logs

Groups:

- View group settings
 - o Create and edit user groups
 - Assign user roles
 - o Add and remove users from user groups
 - o Delete user groups
 - o Create and edit device groups
 - o Delete device groups

Policies and Profiles:

- View VPN Profiles
 - o Create and edit VPN profiles
 - o Delete VPN profiles
- View compliance profiles
 - o Create and edit compliance profiles
 - o Delete compliance profiles
- Assign IT policies and profiles to users
- Assign IT policies and profiles to user groups
- Assign IT policies and profiles to device groups
- Rank IT policies and profiles

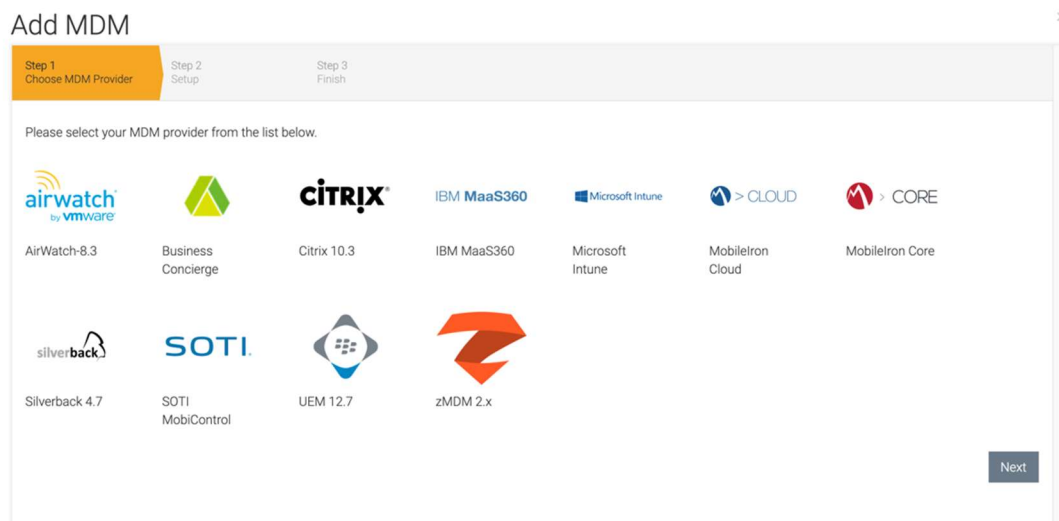
Apps:

- View apps and app groups

Restricted Apps:

- View restricted apps

- 2) Create one or more User Groups that contain the devices that you plan to protect, if you do not already have one. MVISION Mobile Console uses the user group(s) to synchronize users and devices.
- 3) Ensure TCP port 443 or 18084 is opened
- 4) Log in to MVISION Mobile Console and go to the **Manage** page. From there select **MDM**.
- 5) Click on **Add MDM** and select the UEM icon.



- 6) Enter information pertinent for the UEM integration list in the table.

Field	Description
URL	<p>URL of the UEM API Server. For example, append ':18084/SRP_ID' to the end of the URL, where <i>SRP_ID</i> is the Server Routing Protocol Identifier (SRP ID).</p> <p>This SRP ID can be found under your BlackBerry 'My Account' tab under servers. Each server has a different SRP ID. An alternative is to contact your BlackBerry representative for assistance. For instance:</p> <p>https://se-lab-uem2.zdtmdc.com:18084/S62887113</p>
Username	UEM Administrator created with the needed roles access.
Password	Password of the UEM Administrator created.
MDM Name	Internal name used to represent this MDM Integration in MVISION Mobile Console.
Sync User	Check this box to ensure users/devices are synchronized with the UEM User Groups chosen on the next page.
Set Synced user's password	Check this box to override the default password during user sync. (This field is only applicable to MVISION Mobile App Release 4.4 and earlier which has a username and password login.)
Synced user's password	The value of the password to use for each user when they are synchronized and the box for the 'Set synced user's password' is checked. (This field is only applicable to MVISION Mobile App Release 4.4 and earlier which has a username and password login.)
Mask Imported User Information	Check this box to mask personally identifiable information about the user, for instance, 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.

Add MDM

Step 1
Choose MDM Provider
Step 2
Setup UEM 12.7
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.

Sync users

Specify if this MDM provider should synchronise users.

Set synced users password

If you do not specify a password, a default value will be used

Synced users password

Specify the password for users synced from the MDM

Mask Imported User Information

By enabling this option, personally identifiable information will be masked (first name, last name and email) from the zConsole

Send Device Activation email via zConsole for iOS Devices

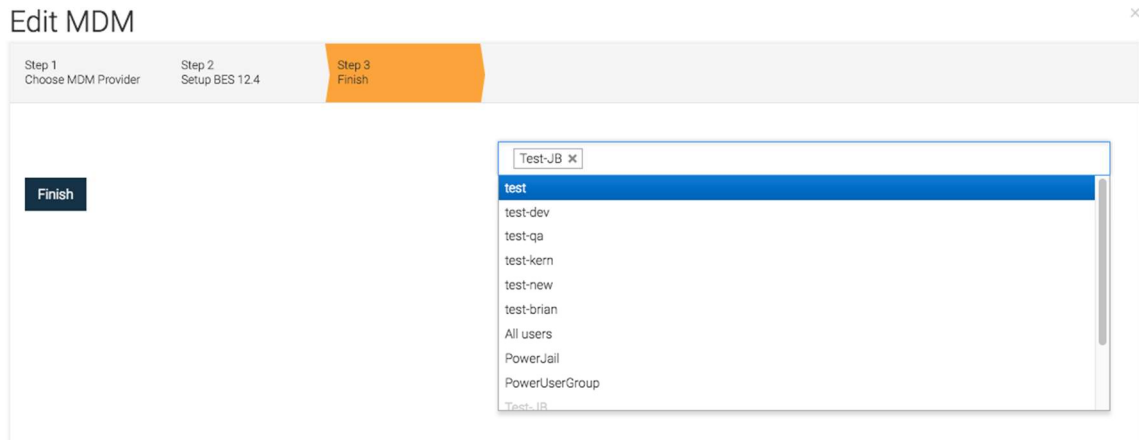
By enabling this option, zConsole will send an activation email to a user for each iOS device which is synced from the MDM

Send Device Activation email via zConsole for Android Devices

By enabling this option, zConsole will send an activation email to a user for each Android device which is synced from the MDM

Next

- 7) Click Next and choose the User Group(s) to synchronize. The available User Groups show up by clicking in the entry box. Click **Finish** to save the configuration and start the first synchronization.



- 8) The User Groups are retrieved, and user/device synchronization setup is completed.
- 9) You can verify this by going to the Devices or Users pages in the MVISION Mobile Console to see that they are displayed. The device entries are greyed out until the user starts up MVISION Mobile App and activates the app.

Auto Activation/Advanced Application Deployment

The McAfee MVISION Mobile App application in both iOS & Android Enterprise (Android for Work) can auto-activate. The process is different on each platform as described below.

iOS Activation

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

This configuration is done within UEM. During the add application step there is an option to define the add an App configuration:

Note: BlackBerry Dynamics does not use activation link enrollment.

1. If you have an app defined already, edit the app and scroll to the bottom. Click on the plus sign ('+') to add an App configuration with the key and the value.
- For MVISION Mobile App Release 4.8.0 and later use the values described in this table. There are additional notes for required changes to the keys and options if you are using MVISION Mobile App Release 4.7.x.

Configuration Key	Value Type	Configuration Value	Additional Notes

MDMDeviceID	String	%IOSUDIdentifier%	This configuration key value is 'uuid' for MVISION Mobile App Release 4.7.x.
tenantid	String	Contact your Customer Support Team.	
defaultchannel	String	Contact your Customer Support Team.	
tracking_id_1	String	(Optional) Use your desired identifier.	This key is supported in MVISION Mobile App Release 4.8.0 and later.
tracking_id_2	String	(Optional) Use your desired identifier.	This key is supported in MVISION Mobile App Release 4.8.0 and later.
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. Also, the "display_eula" key is supported in MVISION Mobile App Release 4.4.0 or later for iOS and MVISION Mobile App Release 4.7.0 or later for Android.

2. Click **Save**.
3. When assigning this app to a group, ensure to select the App Configuration to be used. See the sample setting below for the App configuration, 'DemoJon'.

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

Activation with UEM Messaging

UEM supports message templates where you can send a customized email to users. This is an optional activation method. See "[Appendix A - UEM Messaging and Device Activation](#)" section for information on how to set up these notifications.

Granular Protection

The McAfee integration with UEM adds the ability to lock the device or delete work data from the device. To choose these selections, navigate to Policy and view the current Mobile threat policy. Under the MDM Action column for the threat chosen, select either Lock Device or Delete only work data. When that threat is detected, the selected action is used.

BlackBerry Dynamics (Containerization Option)

The Dynamics Secure Mobility Platform in UEM provides additional ability to protect company intellectual property whether it is on a mobile device or inside the corporate intranet. BlackBerry can be alerted to malicious behavior on the device and take action to protect that data further.

BlackBerry Dynamics users can be synchronized with the assigned MVISION Mobile Console. MVISION Mobile App communicates to BlackBerry Dynamics what actions to use to protect the device in different situations/threats, these actions can be selected by the MVISION Mobile Console Administrator through the Policy page.

Prerequisite Requirements

Integration with BlackBerry Dynamics requires a connection between the McAfee MVISION Mobile Console and the BlackBerry UEM Dynamics API server. This is accomplished via the Internet using SSL on the TCP ports mentioned below.

The following table details specific requirements for the API connection.

Item	Specifics
BlackBerry Dynamics enrolled device	
Administrator Account in the BlackBerry Dynamics or UEM Management console.	Ensure the Administrator account has the role defined below.

Public SSL Certificate on BlackBerry Dynamics API Server	The SSL certificate is trusted externally.
Access to certain TCP ports on the UEM Server	TCP/18084 TCP/17433
Approval to run MVISION Mobile App for BlackBerry in a PoC	Navigate to the request URL provided below.

About MDM and MVISION Mobile Console Communication

The MVISION Mobile Console is configured to share information with the BlackBerry Dynamics console through API access.

When MVISION Mobile App 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 Cloud server. The Cloud server then reaches out to the proper BlackBerry Dynamics API Server and provides the commands to perform the action described for the affected device.

Protection Methods

McAfee is able to interact with the BlackBerry Dynamics Server through API's that provide the ability to modify device configurations securely over the internet. Three methods are used that provide granular protection capabilities.

MSIVISION Mobile App Device Actions

- MVISION Mobile App Device Actions
 - Android: If 'Disconnect WiFi' is selected under the Device Action column in the threat policy, when that threat is detected on an Android device, the Wi-Fi is disabled. The user can manually enable the Wi-Fi when they are out of the range of the suspect Wi-Fi network.
 - iOS: If 'Enable VPN' is selected under the Device Action column in the threat policy, when that threat is detected on an iOS device, the configured VPN is brought up. The user can manually bring the VPN down when they are out of the range of the suspect Wi-Fi network.

Device Action

☒ No Action
☐ Disconnect Wifi

☒ No Action
☐ Disconnect Wifi
☐ Enable VPN

BlackBerry Dynamic MDM Actions

The following are the MDM actions available in MVISION Mobile Console for each threat in the threat policy:

- **Lock Device**
This action locks access to the entire device and the user cannot access the device.
- **Delete only work data**
This removes the enterprise data associated with the BlackBerry for Access applications.
- **Block All Apps**
This blocks the use for each BlackBerry for Access application. In this case the app can continue to operate in the background. This is a lighter weight action than the lock action.
- **Unblock All Apps**
This unblocks the user so that they can use the BlackBerry for Access applications. When the application is started by the user, they are in their previous state of the application.
- **Lock All Apps**
This locks all applications running under the BlackBerry for Access workspace and requires the BlackBerry Dynamics Administrator to provide an unlock key that the user needs to enter per application. Users cannot interact with an app that is locked, and all data access for the app is stopped. This is a heavier weight action than the block action.
- **Unlock All Apps**
This unlocks the BlackBerry for Access applications. When an application is started by the user, an unlock key is required and they are in their initial state of the app.
- **Remove All Apps**
This removes the apps and the enterprise data associated with each BlackBerry for Access application. When the application is started by the user, they are in their initial state and the apps require activation.

Note: The block and unblock actions are supported for BlackBerry UEM Release 12.9 and later. The unlock action is supported for BlackBerry UEM Release 12.10 and later.

Configuration Steps

Basic Application Deployment

To deploy the MVISION Mobile App application through BlackBerry Dynamics, request a trial of MVISION Mobile App for BlackBerry via this URL: [https://apps.good.com/#/apps/com.McAfee.MVISION Mobile App](https://apps.good.com/#/apps/com.McAfee.MVISION%20Mobile%20App)

Both iOS and Android MVISION Mobile App for BlackBerry then show up in the BlackBerry Work Apps. Deploy these apps to the user groups required.

At this point the application is now published and can be installed from the BlackBerry Access App store on the device. Users can now activate the application as described in the platform guides in the Support Portal. The user needs the activation link created in the MVISION Mobile Console to access the application, unless a synchronization is performed (for iOS or Android Enterprise or Android for Work).

Synchronization

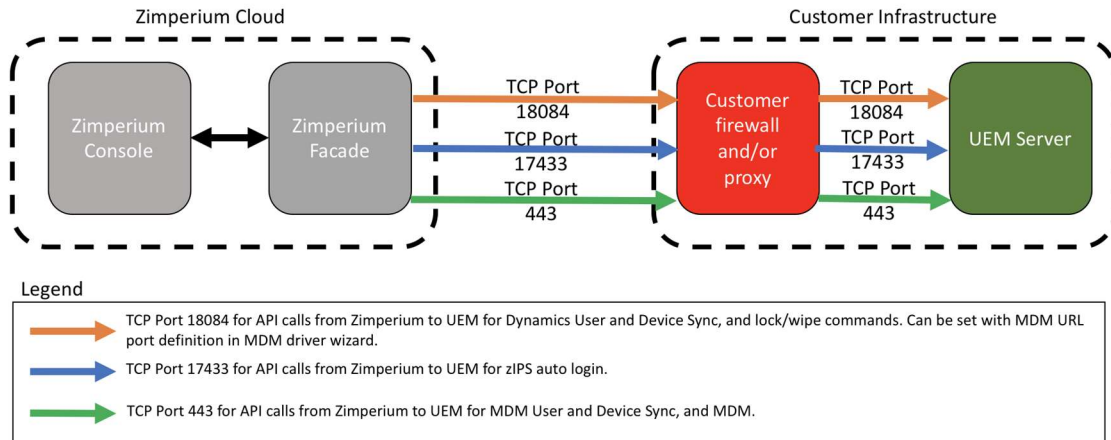
After the initial synchronization during the BlackBerry Dynamics Integration setup, devices are managed through a scheduled synchronization process that runs every four hours. If there are additional users, they are added and also their devices to MVISION Mobile Console. If there are users removed, then we remove them from the MVISION Mobile Console. Doing this does not remove any of the events associated with that device. Currently, all devices active on the BlackBerry Dynamics console are synchronized.

To set up synchronization, perform the following steps:

1. Create a BlackBerry Dynamics Administrator account with the role defined below:
 - a. Directory Access
 - i. All company Directories or Selected company directories as needed.
 - b. Policies and Profiles
 - i. View BlackBerry Dynamics compliance profiles
 - ii. View BlackBerry Dynamics profiles
 - iii. View BlackBerry Dynamics connectivity profiles
 - c. Settings
 - i. View Infrastructure settings
 1. View Servers
 - ii. View BlackBerry Dynamics settings
 1. View BlackBerry Dynamics app services
 2. View BlackBerry Dynamics server properties
 3. View BlackBerry Dynamics Direct Connect settings
 4. View BlackBerry Dynamics server jobs
 5. View BlackBerry Dynamics server cluster settings
 6. View BlackBerry Dynamics communication settings
2. This account is used for the synchronization.

- a. Create the user in the BlackBerry Dynamics console. In the User and Groups menu option click on the **Add Users** and follow the prompts.
 - b. Go to Administrators and edit the BlackBerry Dynamics Global Administrators role.
 - c. Click on members and add the user created in the previous steps to this role.
3. Ensure the following ports are opened inbound to the UEM Dynamics server:

UEM Dynamics



4. In the MVISION Mobile Console, create the MDM integration by following these steps:
 - a. Click **Manage** in the left frame.
 - b. Click **Add MDM**.
 - c. Choose the UEM icon.

- d. Enter the values specific to your integration and click **Next**.

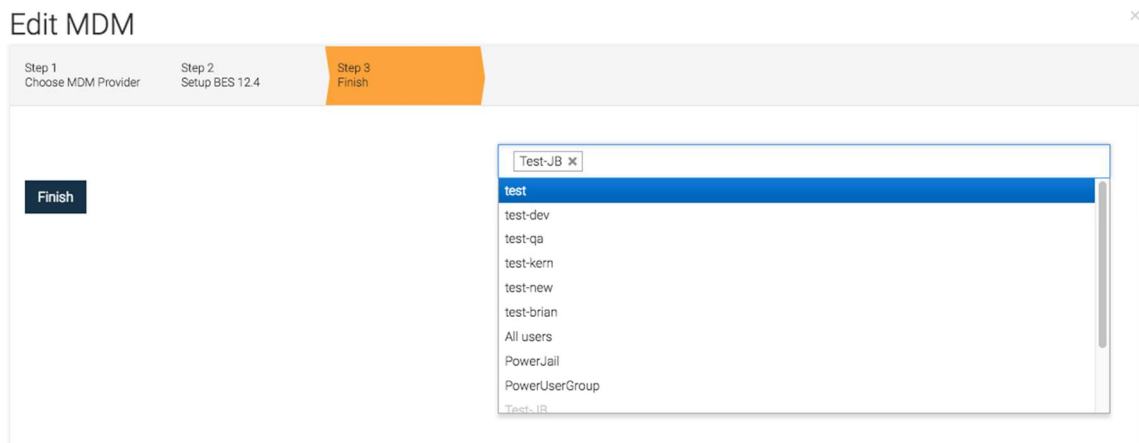
Add MDM

The screenshot shows the 'Add MDM' configuration interface, specifically Step 2: Setup UEM 12.7. The interface includes the following fields and options:

- URL:** A text input field for the MDM provider URL.
- Username:** A text input field containing 'user@example.com'.
- Password:** A password input field with masked characters and a toggle icon.
- MDM Name:** A text input field containing 'UEM 12.7'.
- Sync users:** A checkbox that is checked.
- Set synced users password:** A checkbox that is unchecked.
- Mask Imported User Information:** A checkbox that is unchecked.
- Send Device Activation email via zConsole for iOS Devices:** A checkbox that is checked.
- Send Device Activation email via zConsole for Android Devices:** A checkbox that is checked.
- Next:** A button at the bottom left to proceed to the next step.

- i. **URL:** Enter the URL to access the API server for your BlackBerry Dynamics Server. For example, append '**18084/SRP_ID**' to the end of the URL, where **SRP_ID** is the Server Routing Protocol Identifier (SRP ID). This SRP ID can be found in your BlackBerry 'My Account' tab under servers. Each server has a different SRP ID. An alternative is to contact your BlackBerry representative for assistance.
- ii. **Username:** Enter the Administrator account created previously.
- iii. **Password:** Enter the password for the Administrator account.
- iv. **MDM Name:** Name for this MDM integration internal to MVISION Mobile Console to be used for groups.
- v. **Sync users:** Check this box to enable the device and users to be synced from the BlackBerry Dynamics Server.
- vi. **Set synced users password:** By default, each user synchronized has the same password. To determine the password, take the McAfee environment name, change upper case letters to lower case and also change spaces to dashes. The password is the normalized environment name with "1234!" appended to the end. So "*McAfee Test*" becomes the string "*McAfee-test1234!*" If a different password is preferred, you can set it to a different value, by setting the next field. (This field is only applicable to MVISION Mobile App Release 4.4 and earlier which has a username and password login.)
- vii. **Synced users password:** If not using the default password. Then enter the desired password here. (This field is only applicable to MVISION Mobile App Release 4.4 and earlier which has a username and password login.)

- viii. **Mask Imported User information:** Check this box to mask personally identifiable information in the console such as name and email address.
 - ix. **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.
 - x. **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.
- e. Choose the user groups associated with this integration and click **Finish**.



- f. All active users and devices are now synced.

Users can now startup their MVISION Mobile App instance and they are able to activate given their activation link from MVISION Mobile Console.

Auto Activation/Advanced Application Deployment

The McAfee Android MVISION Mobile App for BlackBerry application can auto activate. This uses a BlackBerry Dynamics configuration. For MVISION Mobile App for BlackBerry Release 4.8.x and later use the values described in this table.

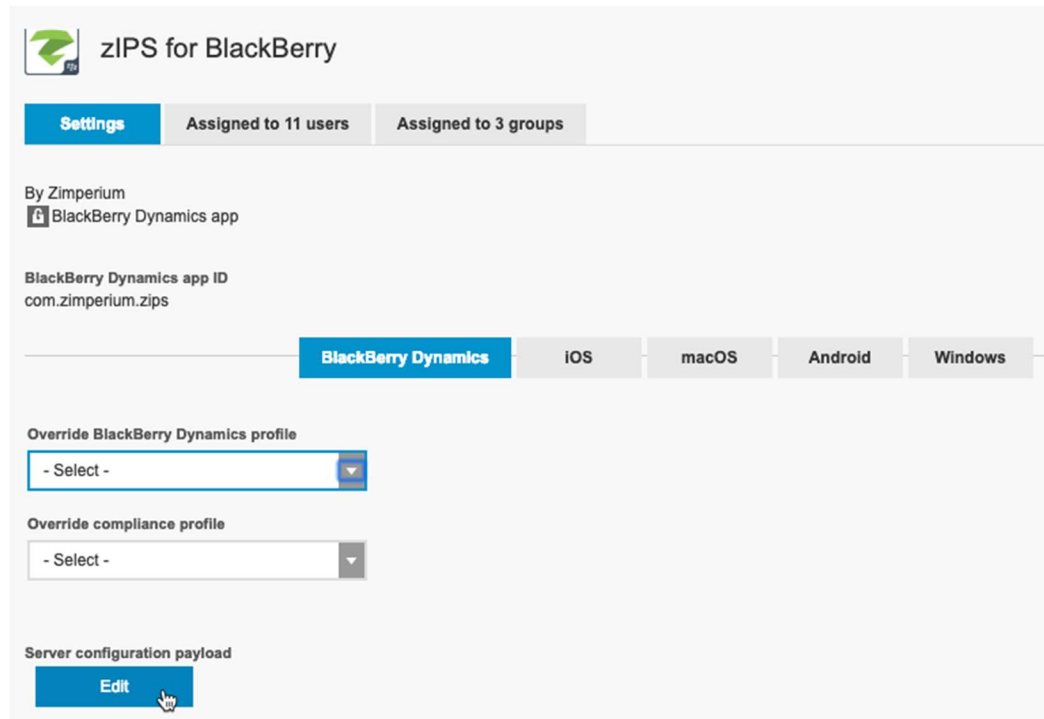
Configuration Key	Value Type	Configuration Value
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team

Note: The configuration keys are case sensitive.

Perform these steps to configure this functionality:

1. Login to the UEM console as a BlackBerry UEM administrator.
2. Click on **Apps** in the navigation menu.
3. Select the “MVISION Mobile App for BlackBerry” app from the list displayed.
4. Under the Settings tab, click the **Edit** button (or **Add** button) for Server Configuration Payload.


The figure shows the display for the Settings tab.



- 1) Set the configuration payload to provide the values for the tenantId and defaultchannel. This is a payload example in the format of the following:

```
{
  "tenantid" : "BB-demo" ,
  "defaultchannel": "https://sample-acceptor.McAfee.com/srx"
}
```

This figure shows a configuration payload set.

 zIPS for BlackBerry

Configuration payload

Specify the keys and values used to configure settings for the app. You must use the format that is required by the app developer (for example, JSON or XML).

```
{
  "tenantid": "BB-demo",
  "defaultchannel": "https://sample-acceptor.zimperium.com:443/srx"
}
```

Cancel

Save

Granular Protection

The McAfee integration with BlackBerry Dynamics provides the ability to perform different MDM actions. For the list of action, refer to the [“Protection Methods”](#) section.

An action can be selected as a response to a detection in the threat policy. To implement this, navigate to the Policy page in the MVISION Mobile Console. For the threat you want to deploy an action against, choose the action in the drop-down box for that threat.

In this threat policy example, this defines what MDM action should take place on the device when an ‘ARP Scan’ threat occurs. When your selections are complete, click on **Deploy** to push the new threat policy to MVISION Mobile App.

Note: When an action is taken such as ‘Lock All Apps’ or ‘Remove All Apps’, the MVISION Mobile App application is excluded from that set, so the MVISION Mobile App app protection continues.

Appendix A - UEM Messaging and Device Activation

BlackBerry supports messaging where you can send a customized email to users. This is an optional activation method. This details the steps to configure a message template to send an email after the user's device is successfully enrolled.

Note: This is only supported by UEM version 12.9 and later.

1. Click on **Settings**.
2. Click on **General Settings**.
3. Click on **Activation defaults**.
4. Click the checkbox for 'Send device activated notification'.

☒ Send device activated notification

To set up the customized email, perform the following steps:

1. Click on **Settings**.
2. Click on **General Settings**.
3. Click on **Email Templates**.
4. Set the email text for your preferences.

This is the specific device identifier variable.

MDM	MDM Device Identifier Variable
BlackBerry's UEM MDM	%IOSUDIdentifier%

Note: If you have an issue using the %IOSUDIdentifier% value, try the BlackBerry UEM variable for Android %DeviceIMEI%. BlackBerry UEM does not yet specifically support UUID value for Android.