McAfee MVISION Mobile

BlackBerry

Integration Guide

January 2021

Contents

Preface

This document is an administrator's guide to integration the MVISION Mobile Console with BlackBerry products.

Audience

The intended audience for this guide is a MVISION Mobile Console administrator. This guide helps administrators to provide integration with the BlackBerry MDM. The MVISION Mobile Console application provides threat protection to mobile devices. The system administrator sets policies for threats and the MDM configuration.

See "*McAfee 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

BlackBerry currently maintains two products that MVISION Mobile integrates with, which are the Unified Endpoint Management Server (formerly known as BES) and BlackBerry Dynamics (formerly known as Good Dynamics). This document details each in the following sections.

If both UEM MDM and UEM Dynamics are used simultaneously, configure the firewall ports according to the steps in the UEM Dynamics section.

NOTE: *Be sure to review and configure MVISION Mobile 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 MVISION Mobile Console and the UEM API server. This is accomplished via the Internet using SSL on TCP port 17433 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 17433 or 18084.

NOTE: *In order to connect to the On-premise UEM Management server without opening ports to the internet, a set up for the integration to the BlackBerry proxy can be used. Contact the McAfee Customer Success team for assistance in this setup.*

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 is defined in the section below.
Access to certain TCP ports on the UEM Server	TCP 18084 and 17433

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, MDM integration does support the on-premise UEM product.*

About MDM and MVISION Mobile Console Communication

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

Protection Methods

MVISION Mobile interacts with the UEM MDM through API's that provide the ability to modify device configurations securely over the internet. The basic methods to provide granular protection capabilities are to lock the device and delete only work data.

Configuration Steps

This section provides the configuration steps for the deployment of the basic MVISION Mobile application.

Basic Application Deployment

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

To publish the MVISION Mobile 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.

These links are also available from the Apple and Google Stores:

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

Login to UEM, navigate to **Apps,** and click **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 assigned User Group. The user activates the application, as described in the platform guides in the support portal. Users need the activation link created in the MVISION Mobile Console to access the application unless synchronization is performed (with iOS or Android Enterprise).

Synchronization

This section describes the steps for setting up the synchronization between the systems.

Full MDM Synchronization

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

- **New Enrollments**: If the new users in the User Group(s) are used for synchronization, they are added along with the devices to MVISION Mobile Console.
- **Unenrolled Users**: If the users are unenrolled, 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 pushed down to the device and attempts to start it prior to the device being synchronized with the MDM. When this situation occurs, MVISION Mobile Console performs an on-demand device synchronization when MVISION Mobile tries to log in, 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 that device and user information from the MDM configured for that customer. MVISION Mobile on that device is now authenticated and allowed to proceed. This type of synchronization adds devices over time as the devices are activated.

Prerequisites

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

- **iOS**: This requires associating an app configuration with the MVISION Mobile 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."
- **Android**: This requires Android for Enterprise for auto-activation. Use MVISION Mobile Console activation URLs for native Android. Contact the McAfee Customer Support Team for more information on this topic.

Synchronization Setup

To set up synchronization, perform these steps described in these sections.

Setting up the UEM Administrator

To set up and create a UEM administrator with the proper role access:

1. In the navigation panel, select **Settings**, select **Administrators**, then select **Roles**.
2. Click on the icon to add a role.
3. Enter the name and description.
4. Select the checkboxes for the following:
    a. Group Management
        i. All groups and Users
    b. User and Devices
    c. View users and activated devices
        i. Manage Devices
            a. Enable workspace

b. Lock workspace
c. Lock the device and set message
d. Unlock the device and clear password
e. Delete only work data from multiple devices
f. Enable Activation Lock
g. Disable Activation Lock

ii. Manage BlackBerry Dynamics apps
a. Lock app
b. Unlock app
c. Delete app data
d. Groups:

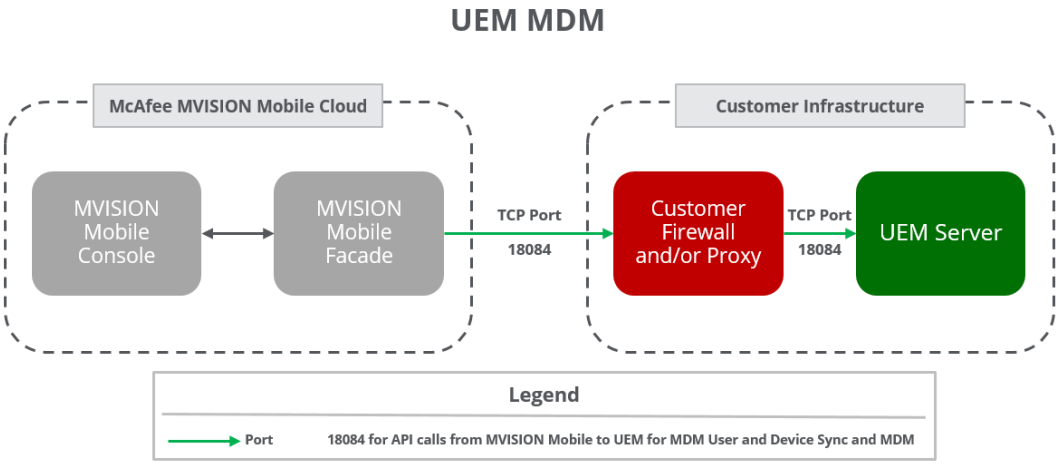
iii. View group settings
a. Create, assign, and edit user groups
b. Add and remove users from user groups
i. Delete user groups
ii. Create and edit device groups
iii. Delete device groups
c. Policies and Profiles
i. View VPN Profiles
a. Create and edit VPN Profiles
b. Delete VPN Profiles
c. View compliance profiles
ii. Create and edit compliance profiles
iii. Delete compliance profiles
iv. Assign IT policies and profiles to users
v. Assign IT policies and profiles to user groups
vi. Assign IT policies and profiles to device groups
vii. Rank IT policies and profiles
a. Apps:
i. View apps and app groups
ii. Delete apps and app groups
b. Restricted Apps:
i. View infrastructure settings
ii. View restricted apps
iii. Create restricted apps
iv. Delete restricted apps
c. Settings
d. View servers Directory Access (This may not be included by default if LDAP/Active Directory is not configured)

e. Select either all company directories or selected company directories as needed.

Setting up User Groups in UEM

Create one or more User Groups that contain the devices to protect, if one is not already selected. MVISION Mobile Console uses user groups to synchronize users and devices.

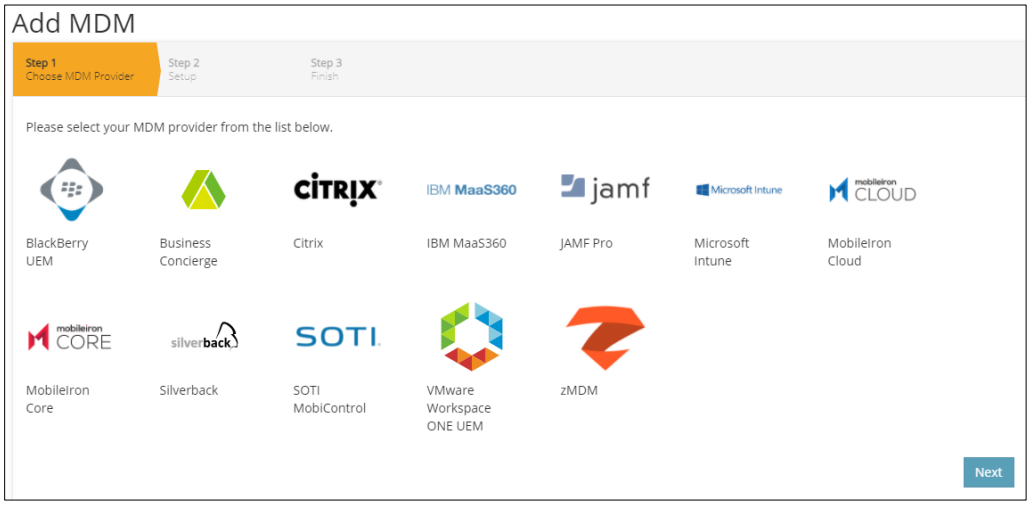
Ensure TCP port 18084 is open, as shown in this figure.



Setting up MVISION Mobile Console with MDM Integration

To set up the MDM integration in MVISION Mobile Console:

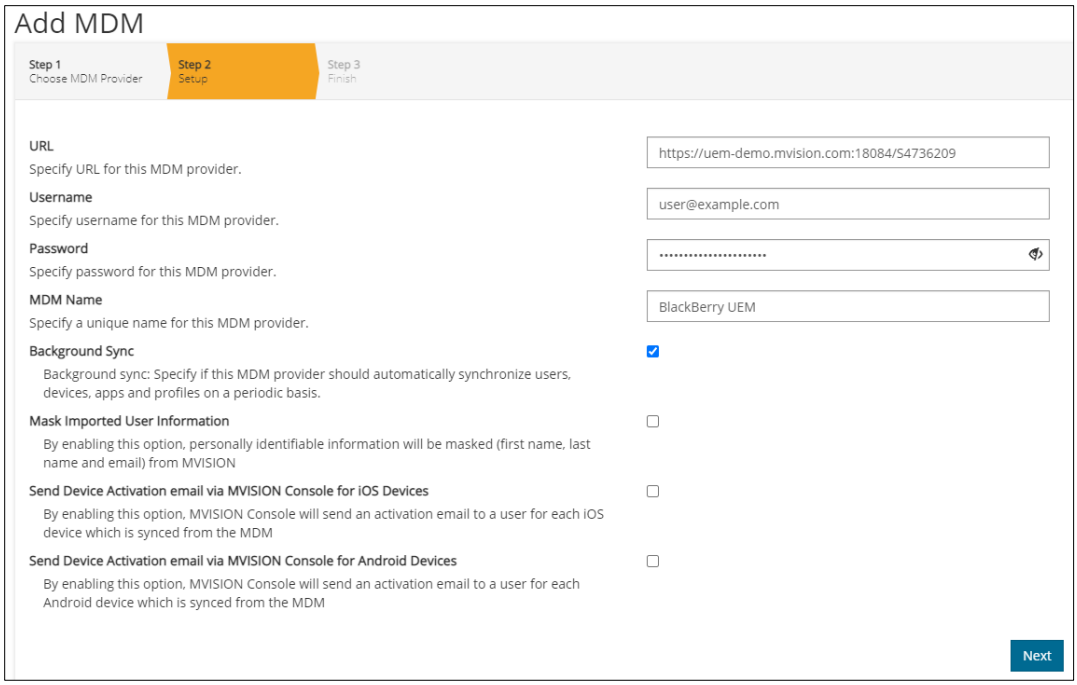
1. Log in to MVISION Mobile Console and go to the **Manage > Integrations**.
2. Click on **Add MDM** and select the UEM icon.



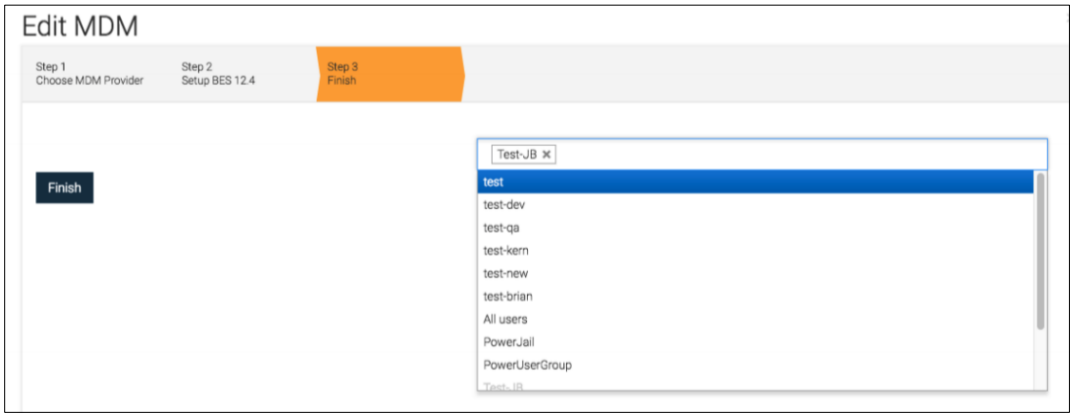
3. Enter information pertinent for the UEM integration list in the table.

Item	Specifics
URL	URL of the UEM API 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 under the user's BlackBerry 'My Account' tab under servers. Each server has a different SRP ID. An alternative is to contact the BlackBerry representative for assistance. For instance: https://se-lab-uem2.mvision.com:18084/S62887113
Username	UEM Administrator created with the needed roles access.
Password	The password of the UEM Administrator.
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.
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.

This figure shows an example window from the MVISION Mobile Console



4. Click Next and choose the User Group(s) to synchronize. The available User Groups show up by clicking in the entry box.



5. Click **Finish** to save the configuration and start the first synchronization.
6. The User Groups are retrieved, and the user/device synchronization starts.

This is verified by navigating to the **Device**s or **Users** pages in the MVISION Mobile Console to determine if they are displayed. The **Device** entries are greyed out and unavailable until the user starts MVISION Mobile and activates the app.

Auto Activation/Advanced Application Deployment

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

iOS Activation

McAfee's MVISION Mobile iOS 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 MVISION Mobile iOS without having to enter any credentials. The App configuration pre-programs MVISION Mobile iOS 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 an app is currently defined, edit the app and scroll to the bottom.
2. Click on the plus sign (+) to add an App configuration with the key and the value.
    a. Use the values described in this table. There are additional notes for required changes to the keys and options if using MVISION Mobile Release 4.8.x and higher.

Configuration Key	Value Type	Configuration Value	Notes
MDMDeviceID	String	%IOSUDIdentifier%	This configuration key value is 'uuid' for MVISION Mobile Release 4.8.x and up
tenantid	String	Retrieve from MVISION Mobile Console	Copy the value from the **Tenant ID** field on the MVISION Mobile Console **Manage** page under the **General** tab.
defaultchannel	String	Retrieve from MVISION Mobile Console	Copy the value from the **Default Channel** field on the MVISION Mobile Console **Manage** page under the **General** tab.
tracking_id_1	String	Use the desired identifier	(Optional) This is an optional tracking identifier.
tracking_id_2	String	Use the	(Optional) This is an optional tracking identifier.

		desired identifier	
display_eula	String	no	If this key is not used, the default displays the End User License Agreement (EULA). (Optional)

NOTE: *The configuration keys are case sensitive*.

3. Click **Save**.
4. When assigning this app to a group, ensure to select the App Configuration to be used.

Android Activation

Android Enterprise (Android for Work) users can use the managed app config for activations. The user must verify that the correct device identifier value is being passed for the configuration parameter. The recommended variables are the same set as the PLIST variables in the “iOS Activation” section.

NOTE: *Use the %DeviceIMEI% value for both MDM Device ID and UUID for Android Enterprise.*

For native Android devices, activations require the use of activation URLs. These are 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. These can be sent to end-users via the MVISION Mobile Console or the MDM.

See the "Appendix A - UEM Messaging and Device Activation" section for more information on sending users a customized email with the MDM.

To access activation links, go to the MVISION Mobile Console **Manage** page, and select the **Integrations** tab. After the MDM is 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 sends 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

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 the users 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.

Activation with UEM Messaging

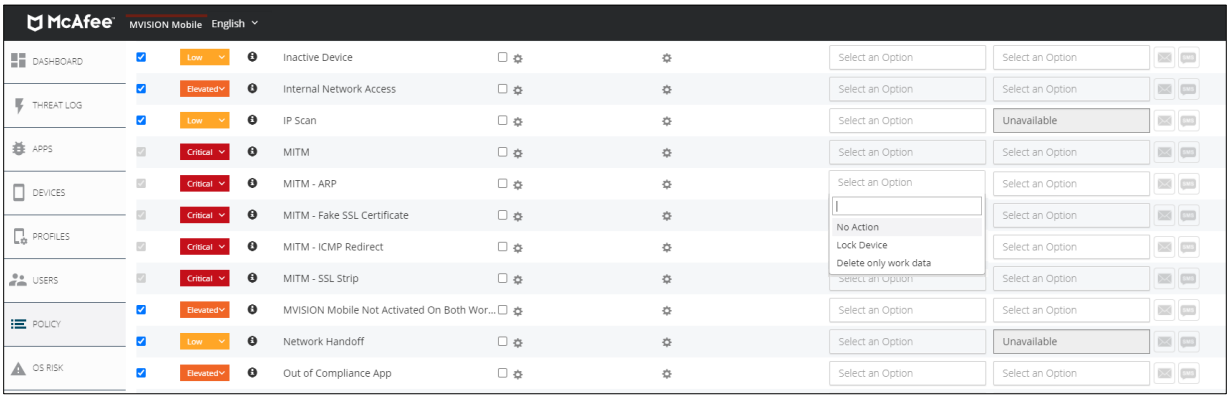
UEM supports message templates where the user sends a customized email to users. This is an optional activation method.

See the "Appendix A - UEM Messaging and Device Activation" section for information on how to set up these notifications.

Granular Protection

The MVISON Mobile integration with UEM adds the ability to lock the device or delete work data from the device. To choose these selections, in the navigation panel, select **Policy** and view the **Current Mobile Threat Policy**. Under the MVISION Mobile Console 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, as shown in the figure.



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 is alerted to malicious behavior on the device and takes action to protect that data further.

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

Prerequisite Requirements

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

This table details specific requirements for the 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 MVISION Mobile Certificate on BlackBerry Dynamics MVISION Mobile Server	The MVISION Mobile certificate is trusted externally.
Access to certain TCP ports on the UEM Server	TCP/18084 TCP/17433
Approval to run MVISON Mobile for BlackBerry in a PoC	Navigate to the request MVISION Mobile provided below.

NOTE: *To connect to the on-premise UEM Management server without opening ports to the internet, a set up for the integration to the BlackBerry proxy can be used. Contact the McAfee Customer Success team for assistance in this setup.*

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 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 server. The MVISION Mobile Console 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

MVISION Mobile interacts 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.

MVISION Mobile Device Actions

For these device actions, note that for:

- **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.
- **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.

BlackBerry Dynamic MDM Actions

These 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 action blocks the use of each BlackBerry for Access application. In this case, the app continues 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 application through BlackBerry Dynamics, request a trial of MVISION Mobile for BlackBerry via this URL:

https://apps.good.com/#/apps/com.zimperium.zips

Both MVISION Mobile iOS and Android 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 activate the application as described in the platform guides in the Support Portal. The user needs the activation link created in the MVISION Mobile to access the application unless 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, the user and the devices are added to the MVISION Mobile Console. If users are removed, then those users are disconnected 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.

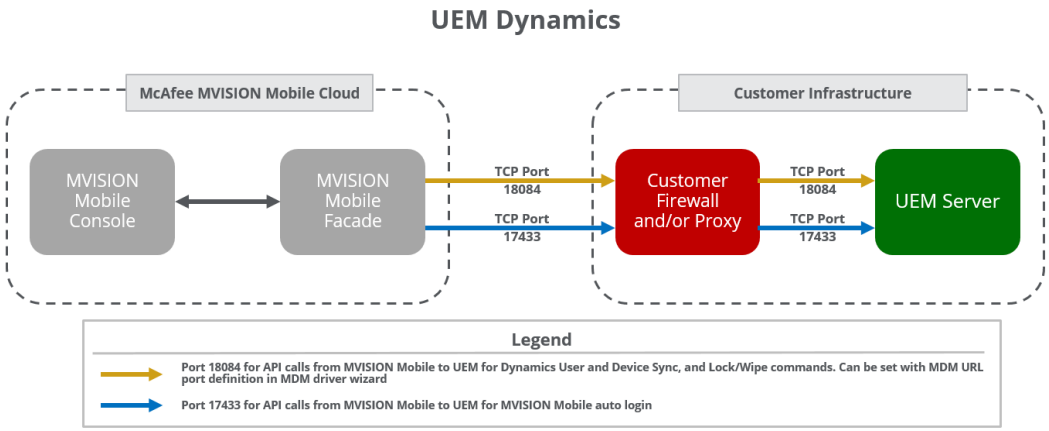
To set up synchronization:

1. Create a BlackBerry Dynamics Administrator account with the role with these authorizations.
2. Navigate to: **Settings**, then select **Administrators**, then select **Roles**.
3. Click on the icon to add a role.
   a. **Directory Access**: (This may not be included by default if LDAP / Active Directory is not configured):
      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

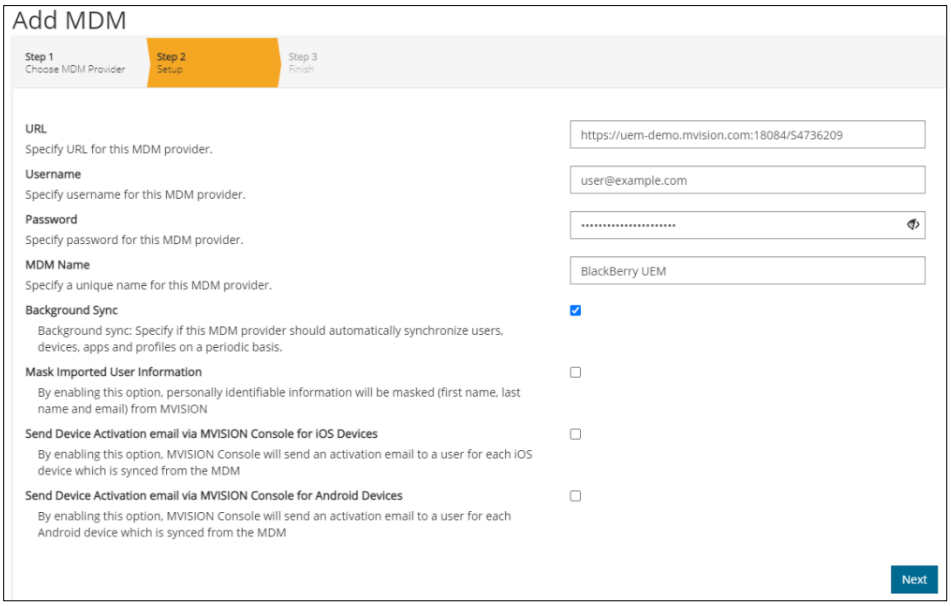
c. **Settings**:
i. View Infrastructure settings
a. View Servers
b. Lock workspace
ii. View BlackBerry Dynamic settings
a. View BlackBerry Dynamics app services
b. View BlackBerry Dynamics server properties
c. View BlackBerry Dynamics Direct Connect settings
d. View BlackBerry Dynamics server jobs
e. View BlackBerry Dynamics server cluster settings
f. View BlackBerry Dynamics communications settings

4. This account is used for 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 **Members** and add the user created in the previous steps to this role.
5. Ensure the following ports are opened inbound to the UEM Dynamics server:
   a. TCP Port 17433
   b. TCP Port 18084



6. In the MVISION Mobile Console, create the MDM integration by following these steps:
   a. Click **Manage** in the navigation menu and then **Integrations**.
   b. Click **Add MDM**.
   c. Choose the **BlackBerry UEM** icon.

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



i. **URL**: Enter the URL to access the API server for the 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 the user's BlackBerry 'My Account' tab under servers. Each server has a different SRP ID. An alternative is to contact the 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.

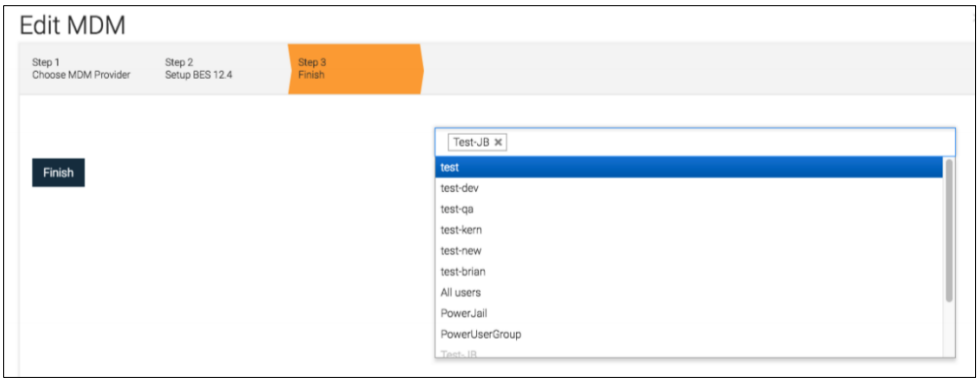
v. **Sync Users:** Check this box to enable the device and users to be synced from the BlackBerry Dynamics Server.

vi. **Mask Imported User information:** Check this box to mask personally identifiable information in the console such as name and email address

vii. **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.

viii. **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 start the MVISION Mobile instance, and the users are now able to activate given the activation link from MVISION Mobile Console.

Auto-Activation/Advanced Application Deployment

The MVISION Mobile Android for the BlackBerry application is capable of auto-activation. This uses a BlackBerry Dynamics configuration. For MVISION Mobile for BlackBerry Release 4.8.x and later use the values described in this table.

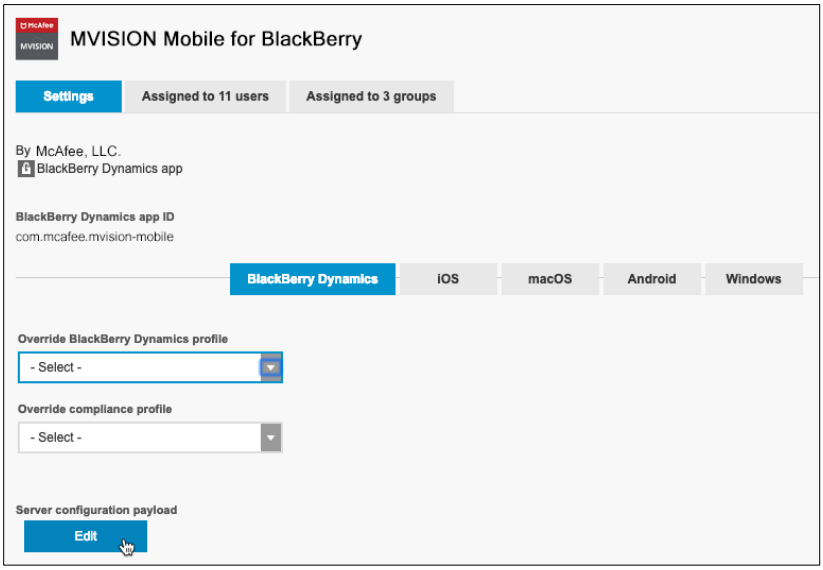
Configuration Key	Value Type	Configuration Value
tenantid	String	Copy the value from the **Tenant ID** field on the MVISION Mobile Console **Manage** page under the **General** tab.
defaultchannel	String	Copy the value from the **Default Channel** field on the MVISION Mobile Console **Manage** page under the **General** tab.

NOTE: *The configuration keys are case sensitive*.

Perform these steps to configure this functionality:

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

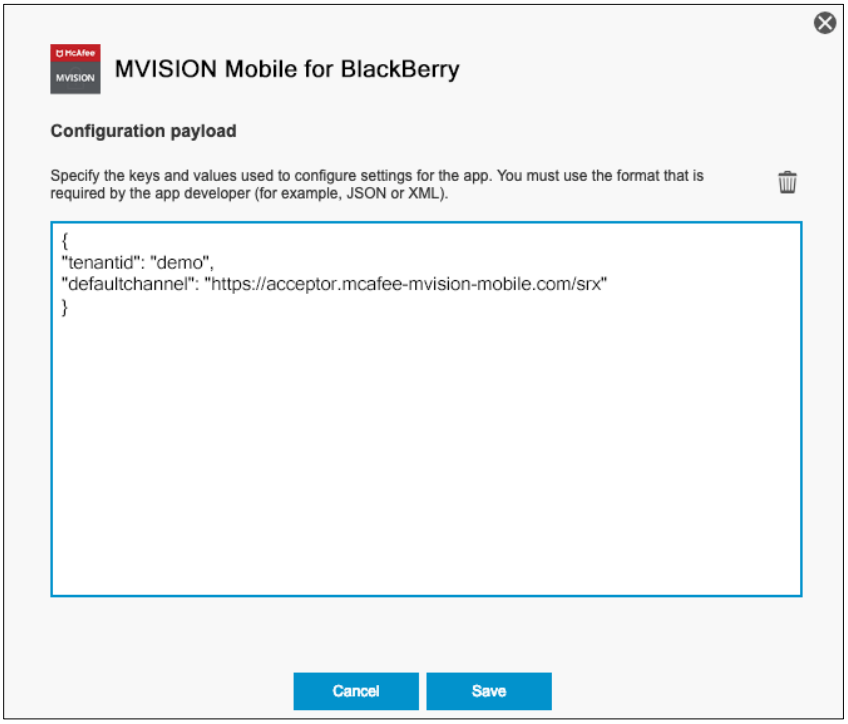
This figure shows the display for the Settings tab.



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": "demo",
"defaultchannel": "https://acceptor.mcafee-mvision-mobile.com/srx"
}
```

The figure shows a configuration payload set.

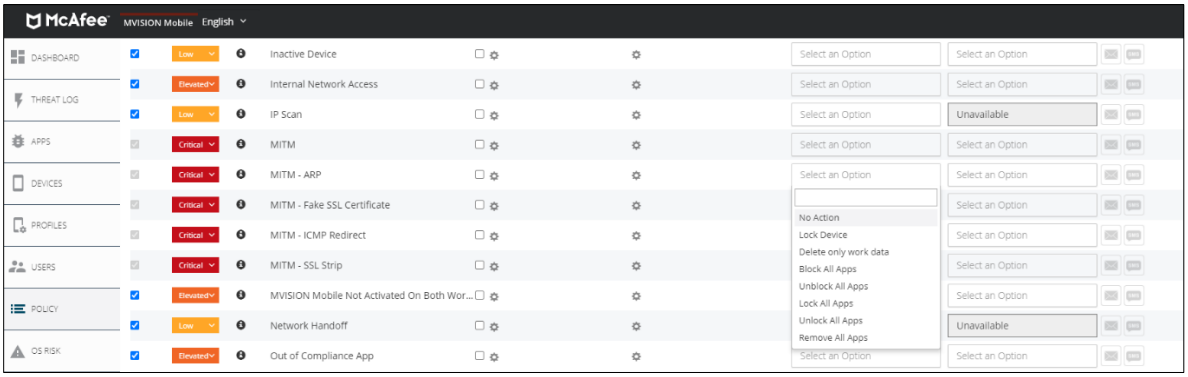


Granular Protection

The MVISION Mobile Console integration with BlackBerry Dynamics provides the ability to perform different MDM actions. For the list of actions, refer to the “Protection Methods” section.

An action is 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 to deploy an action against, choose the action in the drop-down box for that threat.

This figure shows an example list of MDM actions for a given threat



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

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

Appendix A - UEM Messaging and Device Activation

BlackBerry supports messaging where a customized email is sent to the users. This is an optional activation method. The following provides 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 **Settings**.
2. Click **General Settings**.
3. Click **Activation defaults**.
4. Click the checkbox for '**Send device activated notification**'.

To set up the customized email:

1. Click **Settings**.
2. Click **General Settings**.
3. Click **Email Templates**.
4. Set the email text for the user's preferences.

This is the specific device identifier variable.

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