Zimperium zConsole

MobileIron Integration Guide

zConsole Release 4.16

November 2018

Table of Contents

Preface

This document is a guide for integrating Zimperium products with the MobileIron Mobile Device Management (MDM).

Related Documentation

Zimperium support documentation is found in the Customer Portal at the following web site: http://support.zimperium.com.

Audience

The intended audience for this guide is a zConsole administrator. This guide helps administrators to provide integration with the MobileIron MDM. The zIPS application provides threat protection to mobile devices. The system administrator for zConsole sets policies for threats, and also monitors and manages the detected threats. See "Zimperium zConsole Configuration Guide" for more information.

New Features

Refer to the "Zimperium zConsole Release Notes" document for the list of new features in this release.

Document Update Log

Update Date	Release	Summary	Description
Feb 2018	4.8	MobileIron integrated MDM agent support	Configuration instructions to support the Integrated MobileIron Threat Defense.
May 2018	4.12	Made updates for zConsole 4.12	Updated information and versions for Cloud and MTD. Updated the admin roles needed for a MobileIron Cloud API user.
July 2018	4.13	Updated Requirements Section and Updated Information on Local on-device actions	- Updated the MobileIron MDM enrolled device Core minimum version from v8 to v9 - Added steps to configure MI on-device actions for Core.
October 2018	4.13	Updated Activation Details	- Updated the plist tables and added activation details. - Added Appendix A - MobileIron Messaging and Device Activation

			- Updated the MobileIron product name to align as “MobileIron Threat Defense”
November 2018	4.16	Include Support for MobileIron Spaces	Update the notes and screenshot on adding an MDM to include the MobileIron Spaces.

Overview

Integration with a Mobile Device Management (MDM) system is not required. However, when a MobileIron MDM is integrated, the zConsole provides the following:

- Synchronization of devices and their associated users into zConsole.
- MobileIron Threat Defense (MTD) or transparent user enrollment for zIPS if not using MTD.
- More granular and specific actions to protect data on the device and the device itself.

Zimperium zIPS detects malicious activity and depending on the platform, is able to take some defined actions locally. However, when zIPS is integrated with an MDM, actions can be performed by the MDM, providing a very powerful protection tool. MobileIron has built the zIPS z9 engine into their Core and Cloud MDM Agents via MobileIron Threat Defense. Therefore, zIPS is not required to effectively protect devices managed with MobileIron MDM. The MTD product is enabled on the MDM managed device and the agent enrolls with zConsole directly.

This provides the ability to perform local actions on the device at an MDM level without the need to have zConsole tell MobileIron to take some action. The actions happen locally on the device. (This is supported on MI Core today. MI Cloud is expected to support this as well in the future.)

The MobileIron Administrator can setup different workflows to handle different threats via a MobileIron TRM (Core only at this time) or via zConsole that the zConsole Administrator can choose through the Policy page.

For MobileIron Threat Defense on Core, when a threat is detected on the device, the Mobile@Work MDM Agent is notified locally on the device and perform the action on the device. For all others at this time, when a threat is detected, the zConsole instructs the MobileIron console to move the device to the chosen Label in the Threat Response Policy/Matrix (TRM). The workflow assigned to that Label determines the action that MobileIron takes on the device. The communication from the zConsole to the MobileIron console is performed securely with a MobileIron API call.

Requirements

Item	Specifics
MobileIron MDM enrolled device (Non Integrated)	Core: minimum v9 Cloud (Current SaaS version)
MobileIron Core with MobileIron Threat Defense	Core: v9.6.0.1 iOS Mobile@Work MDM Agent: v9.7.0

	Android Mobile@Work MDM Agent: v9.6.0 (Core v10.0.0.1 and Mobile@Work v10 are needed to support local MTD actions)
MobileIron Cloud with MobileIron Threat Defense	MobileIron Cloud Release 52 MobileIron Go for iOS Client: v3.2 MobileIron Go for Android Client: v2018.04.23
API Administrator Account in MobileIron management console.	Setup with the proper role defined in section below.

Architecture

Zimperium integrates with MobileIron MDM on different logical levels which are described in the "Zimperium zConsole Configuration Guide" available in the customer portal. Each level is addressed further on in this document with the specific configuration instructions. To achieve level 2 – 4 integrations, zConsole is configured to share information with the MobileIron console through API REST calls. When MTD/zIPS detects an event, it consults the current TRM resident on the device and if the action involves MobileIron, it is either performed locally or communicated to the zCloud server. The zCloud server then reaches out to the proper MobileIron API Server and provide the commands to perform the configured action.

MobileIron (MI) Core and MobileIron Cloud environments are configured differently and this guide details each configuration in separate sections. The key difference from a zConsole integration point of view is that MI Core manages devices and performs actions locally while MI Cloud instances manage devices and actions via device groups.

In addition, MI Core supports the integration of MobileIron Threat Defense directly in the Mobile@Work MDM Agent. This does not require zIPS on the device since the Mobile@Work agent has the Zimperium z9 engine built in, providing the same protection as zIPS. To enable and configure MobileIron Threat Defense in the Mobile@Work agent, see the section on MobileIron Core MDM - MobileIron Threat Defense.

MobileIron Core MDM with MobileIron Threat Defense

In this configuration, MobileIron Threat Defense, powered by the Zimperium Z9 engine is activated in the MobileIron Core Mobile@Work Agent. Since the engine is already built into the Mobile@Work Agent, zIPS does not have to be pushed down to the device. When a device enrolls in MI Core in this scenario, the MobileIron Mobile@Work Agent is configured with the activation code to enable the z9 engine and communicates with the proper Zimperium zConsole. The actions that can be taken in response to a threat are defined in the MI Console and are performed locally on the device.

The following sections describe the different configuration levels for MobileIron Core MDM with MobileIron Threat Defense.

Level 1: Basic Application Deployment

Since MobileIron Threat Defense is provided by the Mobile@Work Agent, the agent on the device needs to be updated with the activation code to enable the feature. This is done differently between iOS and Android but, in both cases, the same MobileIron Activation Code is required. This code is retrieved after the MobileIron Core MDM integration has been performed in the next step.

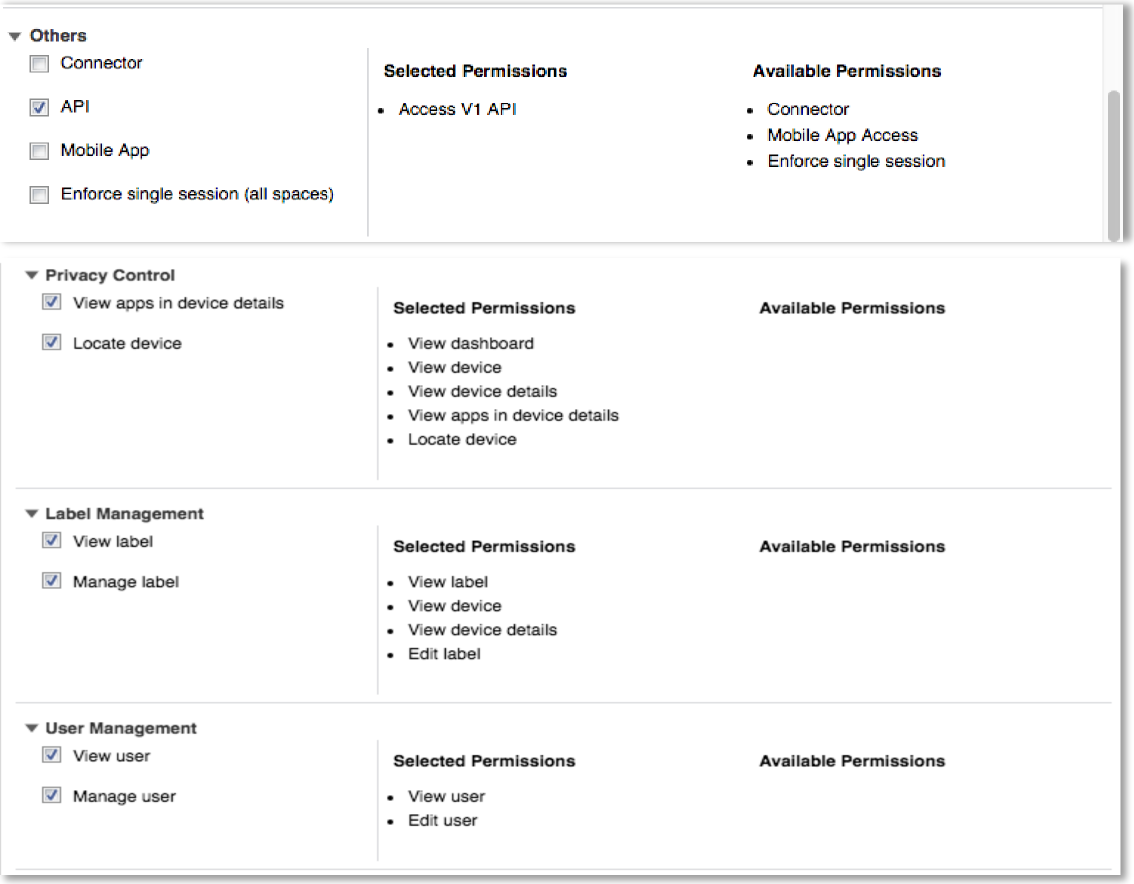
Level 2a: Device and User Synchronization

When device synchronization occurs, the zConsole requests certain information from the MobileIron MDM. That information is used to determine if suspicious profiles are installed on devices that are protected by zIPS as well as all applications on each device.
The information saved for each device includes:

- UUID, Device ID, Apps installed, and email address (if anonymous user functionality is not enabled).
- For zConsole, prior to release 4.13, serial number and IMEI are saved.

Setup User Synchronization

1) Create a MobileIron administrator with the proper API access.
   Navigate to: Devices & Users/ Users/ Add/ Add Local User.
   Then, Admin/ Click on the user and assign the Admin role below:



▼ Others

□ Connector

☑ API

□ Mobile App

□ Enforce single session (all spaces)

Selected Permissions

- Access V1 API

Available Permissions

- Connector
- Mobile App Access
- Enforce single session

▼ Privacy Control

☑ View apps in device details

☑ Locate device

Selected Permissions

- View dashboard
- View device
- View device details
- View apps in device details
- Locate device

Available Permissions

▼ Label Management

☑ View label

☑ Manage label

Selected Permissions

- View label
- View device
- View device details
- Edit label

Available Permissions

▼ User Management

☑ View user

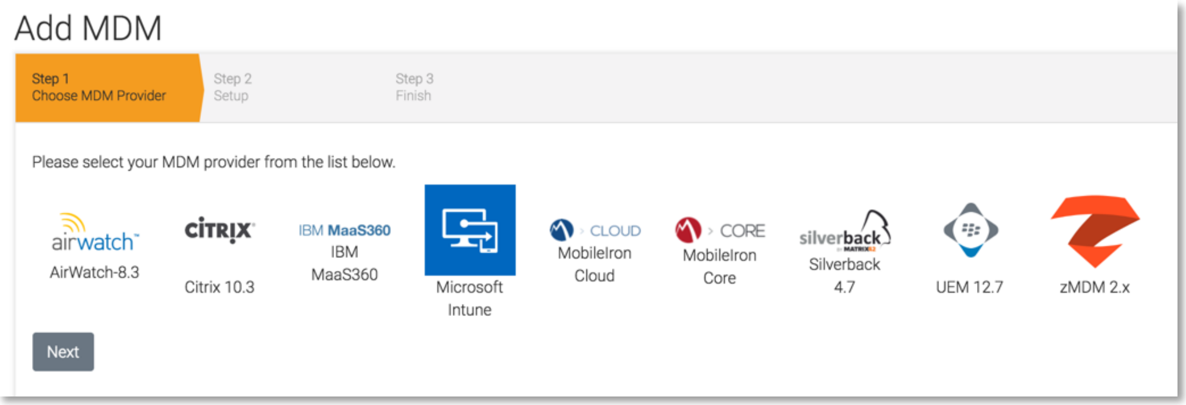
☑ Manage user

Selected Permissions

- View user
- Edit user

Available Permissions

2) Create one or more Labels that you plan to contain the devices that are to be protected if you do not have one that already exists. The zConsole application uses these label(s) to synchronize devices and associate users to zConsole.
3) Log into zConsole and navigate to Manage/ MDM.
4) Click **Add MDM** and select MobileIron Core.



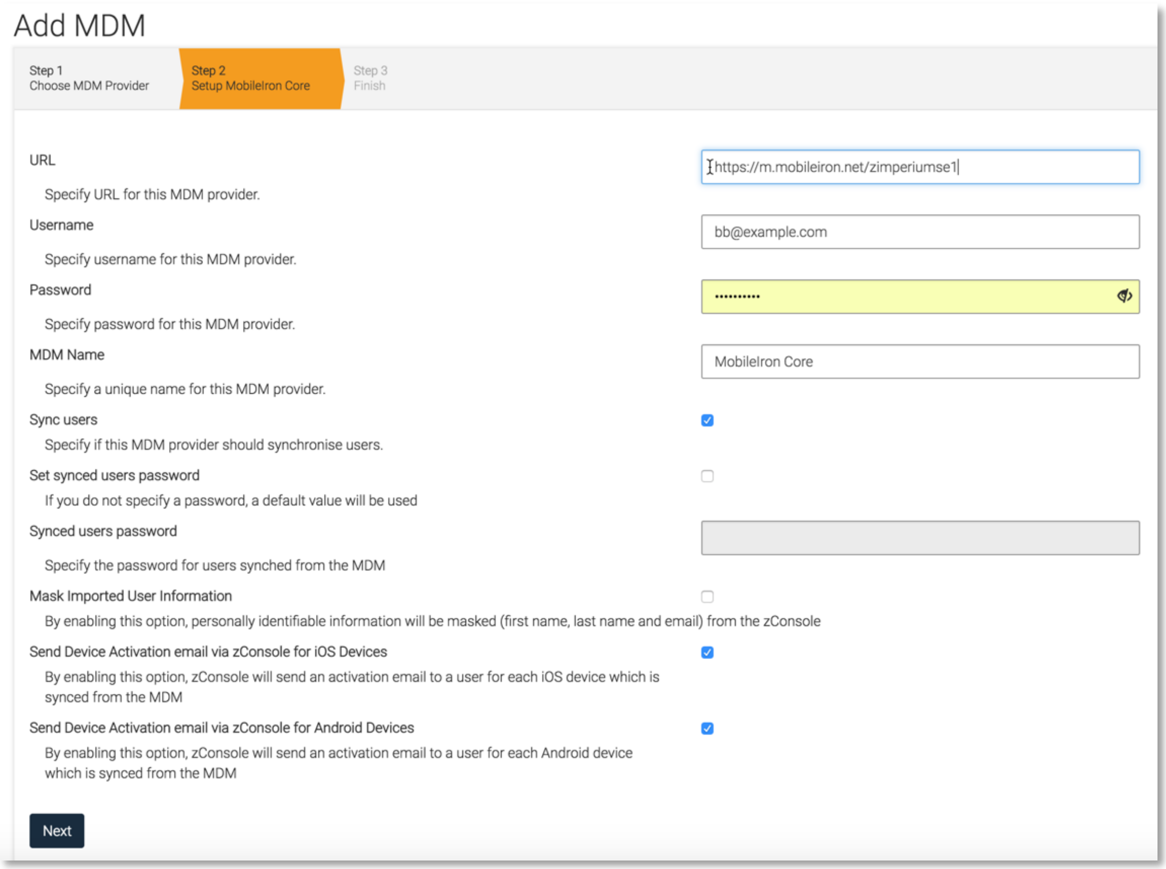
Add MDM

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

Please select your MDM provider from the list below.

5) Enter information pertinent for the MobileIron integration.

Item	Specifics
URL	URL of the MobileIron API Server
Username	MobileIron Administrator created with the API role access
Password	Password of the MobileIron Administrator
MDM Name	The name used in zConsole to reference this MDM integration. This is prepended to the group name to form the zConsole group name.
Sync Users	Check this box to ensure users/devices are synchronized with the MobileIron Labels chosen in the next page.
Set synced users password	Check this box to override the default password during user sync. If this is not checked a default password is computed as follows for all users that are synchronized: Start with the Zimperium environment name (this can be supplied by your Customer Success contact), change all uppercase letters to lowercase and also change all spaces to dashes. Then append "1234!" to the end. So, the value '*Zimperium Test'* becomes '*zimperium-test1234!'* This is for informational purposes only. The user does not need to know their credentials.
Synced users password	The override value of the password to use for each user when they are synchronized.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, for instance name or email address.
Send Device Activation email via zConsole 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	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 MobileIron Core

Step 3
Finish

URL: https://m.mobileiron.net/zimperiumse1

Specify URL for this MDM provider.

Username: bb@example.com

Specify username for this MDM provider.

Password: ••••••••••

Specify password for this MDM provider.

MDM Name: MobileIron Core

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 synched 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

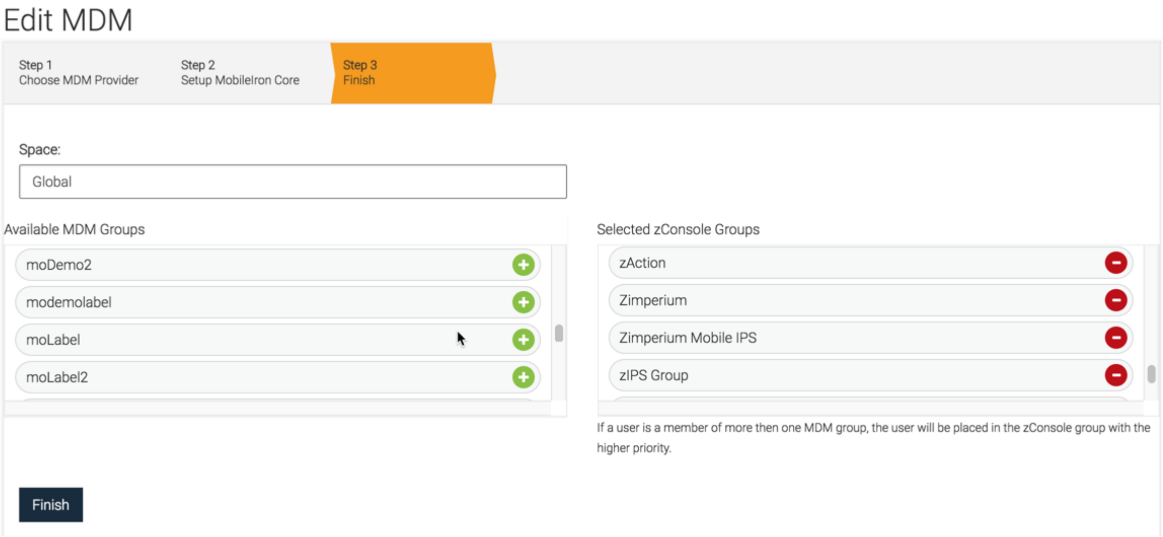
Send Device Activation email via zConsole for iOS Devices ☑

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

6) Click **Next** and choose the MobileIron Space. Then choose the groups to synchronize, then click **Finish**.



Edit MDM

Step 1
Choose MDM Provider

Step 2
Setup MobileIron Core

Step 3
Finish

Space: Global

Available MDM Groups	Selected zConsole Groups
moDemo2	zAction
modemolabel	Zimperium
moLabel	Zimperium Mobile IPS
moLabel2	zIPS Group

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

Note: Spaces are used to separate managed entities for the ease of administration, such as an organizational hierarchy. Now users can sync devices for MobileIron spaces, along with the default space.

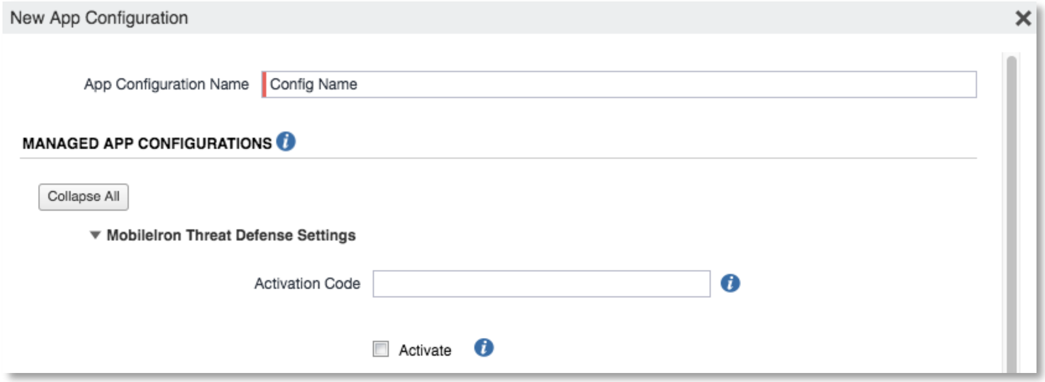
When more than one label is chosen the highest label in the list has the highest priority and so on down the list. If a device is present in more than one label, the label that applies is the highest label for the device.

7) Device and user synchronization starts.

Enable MobileIron Threat Defense

Now that a valid MobileIron MDM Integration has been setup, retrieve the activation code for MobileIron Threat Defense and apply it the Mobile@Work agent on the device.

1) Log into the zConsole and navigate to Manage/ MDM.
2) Locate the MobileIron that was just configured and copy the MobileIron Activation Code to your clipboard.
3) Log into the MobileIron Console.
4) Follow these steps for iOS devices:
    a) Navigate to Apps/ App Catalog.
    b) Locate the iOS Mobile@Work entry. If one does not exist add it from the App Store and associate the required labels.
    c) Click on the Mobile@Work app and **Edit**.
    d) Ensure that the following options are enabled:
        i) Allow conversion of app from unmanaged to managed (iOS 9 or later).
        ii) Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in.
        iii) Send installation or convert unmanaged to managed app request to quarantined devices.
    e) Under Managed App Configurations, click **Add+**



New App Configuration ✕

App Configuration Name: Config Name

MANAGED APP CONFIGURATIONS

▼ MobileIron Threat Defense Settings

Activation Code:

□ Activate

    f) Enter a name for this App Configuration.
    g) Click **Expand.**
    h) Enter the Activation Code.
    i) Enable Activate.
    j) Save the settings.

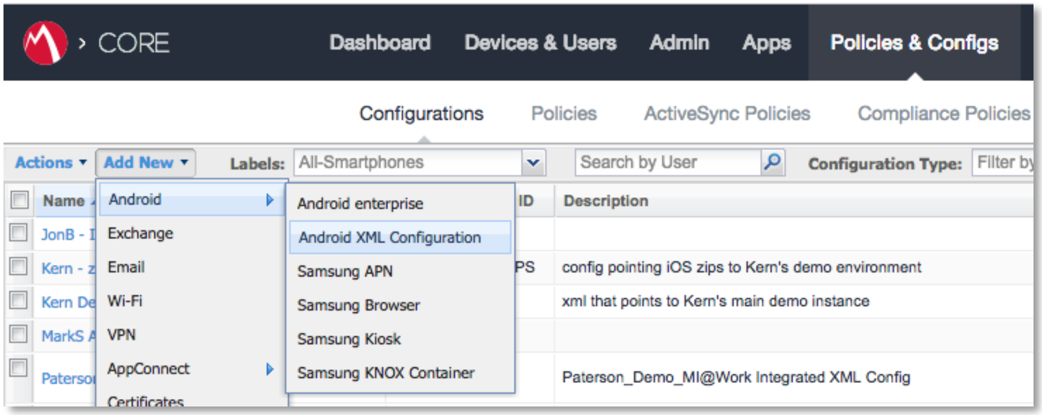
5) Follow these steps for Android devices:

   a) Create an XML file comprised of the following content:
   <?xml version="1.0" encoding="UTF-8"?><zimperium><token>insert activation token</token></zimperium>

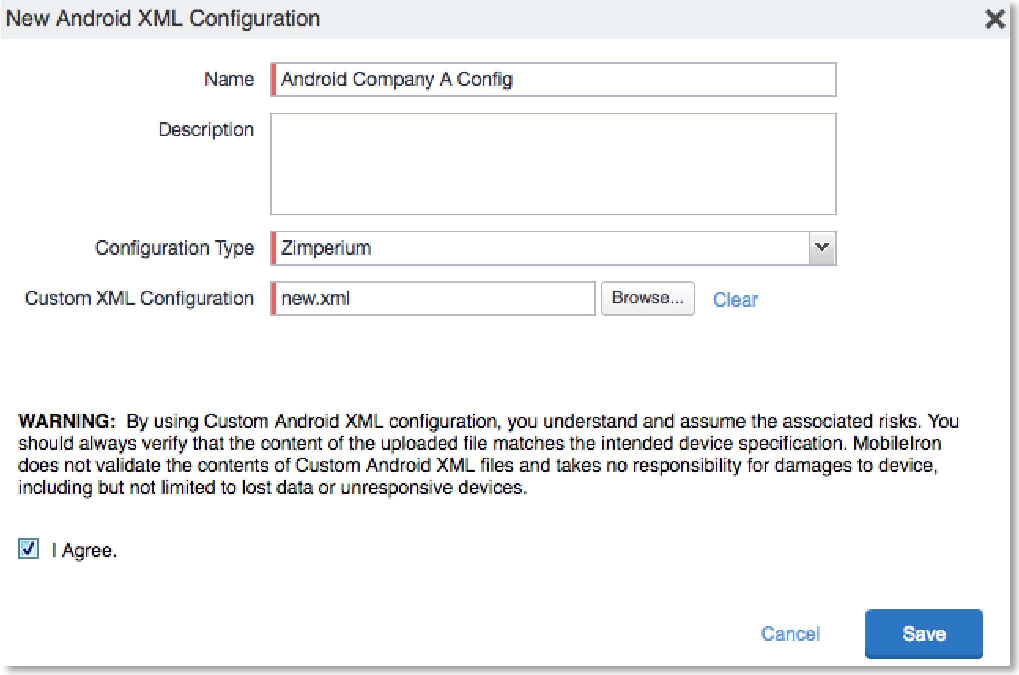
   b) Ensure there are no extra CR’s or LF’s in the file after it is saved.

   c) In the MobileIron console navigate to: Policies & Configs/ Configurations and click **Add New**.

   d) Click on Android/ Android XML Configuration.



   e) Enter a Name for this configuration.


New Android XML Configuration

Name: Android Company A Config

Description:

Configuration Type: Zimperium

Custom XML Configuration: new.xml

WARNING: By using Custom Android XML configuration, you understand and assume the associated risks. You should always verify that the content of the uploaded file matches the intended device specification. MobileIron does not validate the contents of Custom Android XML files and takes no responsibility for damages to device, including but not limited to lost data or unresponsive devices.

☑ I Agree.

   f) Provide a description.

   g) Choose Zimperium for the Configuration Type.

   h) Browse to the XML file created above and upload it.

i) Enable the ‘I agree’ checkbox, and then click **Save.**

j) Assign the required Labels to this new Android_XML Configuration.

At this point MobileIron Threat Defense is enabled for both iOS and Android. When a user enrolls their device, the Activation code is sent to the Mobile@Work agent and MobileIron Threat Defense starts to run.

The device shows up immediately in the zConsole in the default group and after the MDM Integration is automatically synchronized, it shows in the assigned group.

Level 3: Basic Protection

MobileIron Integration Level three does not apply. Proceed to level four.

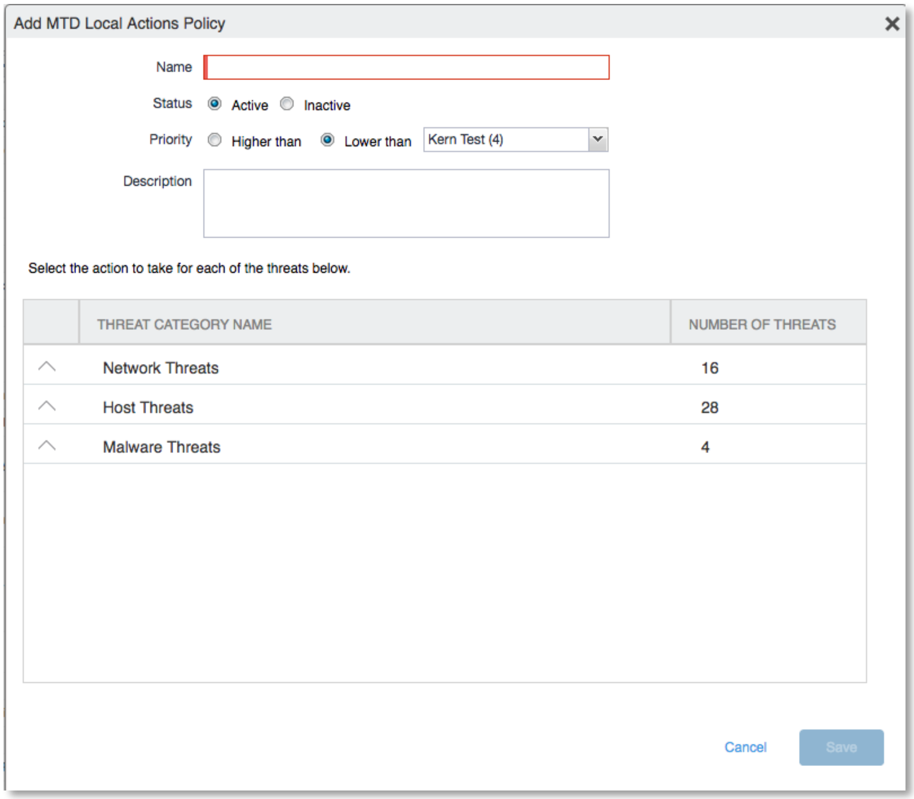
Level 4: Full Protection

The Zimperium integration with MobileIron provides the ability to perform actions directly on the device with no need for the round robin communication through the internet to the device. With MobileIron Threat Defense built into the Mobile@Work MDM agent, when a threat is detected, the agent is alerted by the MTD and takes defined actions locally. This provide a way to protect data on the device as well as the device itself when an attack occurs without having to go out to the internet.

To accomplish this, the MobileIron administrator simply sets up one or more MTD Local Action Policies via the MobileIron console. This provides a mechanism for notification to the user as well as required.

From the MobileIron console perform the following steps:

1) Navigate to Policies & Configs.
2) Navigate to Policies.
3) Click on Add New and choose MTD Local Actions.
4) Fill on the actions and notifications as required per the companies use case. A description of how to do this can be found in the MobileIron documentation set.



Add MTD Local Actions Policy ✕

Name

Status ● Active ○ Inactive

Priority ○ Higher than ● Lower than Kern Test (4)

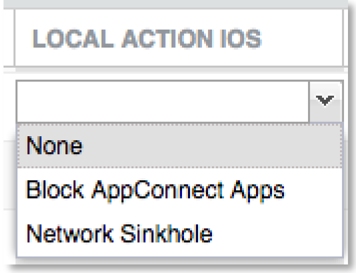
Description

Select the action to take for each of the threats below.

	THREAT CATEGORY NAME	NUMBER OF THREATS
^	Network Threats	16
^	Host Threats	28
^	Malware Threats	4

Cancel Save

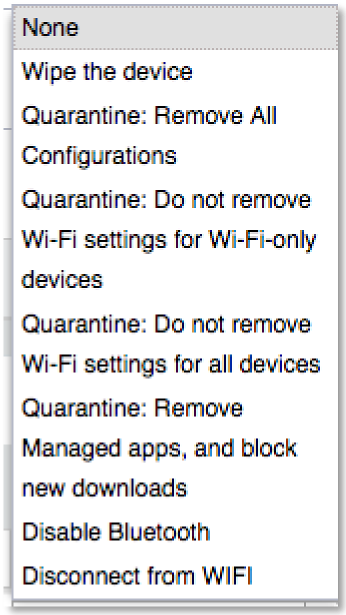
5) Options for iOS Actions include:



LOCAL ACTION IOS

- None
- Block AppConnect Apps
- Network Sinkhole

6) Options for Android Actions include:


None
Wipe the device
Quarantine: Remove All Configurations
Quarantine: Do not remove Wi-Fi settings for Wi-Fi-only devices
Quarantine: Do not remove Wi-Fi settings for all devices
Quarantine: Remove Managed apps, and block new downloads
Disable Bluetooth
Disconnect from WIFI

Select the desired option.

7) Click **Save**.
8) Assign the appropriate Label to this new Policy.

MobileIron Core Integration with zIPS

The following sections describe the different configuration levels for MobileIron Core Integration with zIPS.

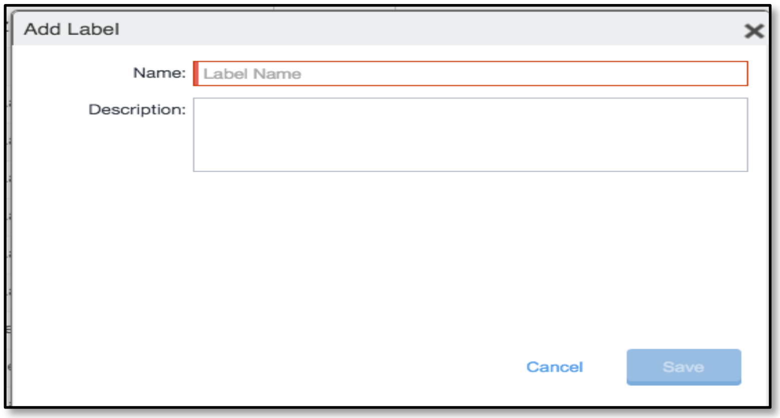
Level 1: Basic Application Deployment

If you are not using MobileIron Threat Defense, zIPS can be deployed. To deploy the zIPS application through MobileIron, ask your Customer Success Team at Zimperium for the iOS and Android version of zIPS. Or deploy via the public App Store for iOS and Play Store for Android.

Log into MobileIron Core. If no appropriate Label exists for the application deployment, create a Label. Create a new Internal Application and upload the proper application file (IPA for iOS and APK for Android) to MobileIron. Assign the Label to the application and publish.

Perform the following steps:

1) Create a Label to be assigned to devices that need to deploy zIPS.
    a. Device & Users/ Labels/ Add Label

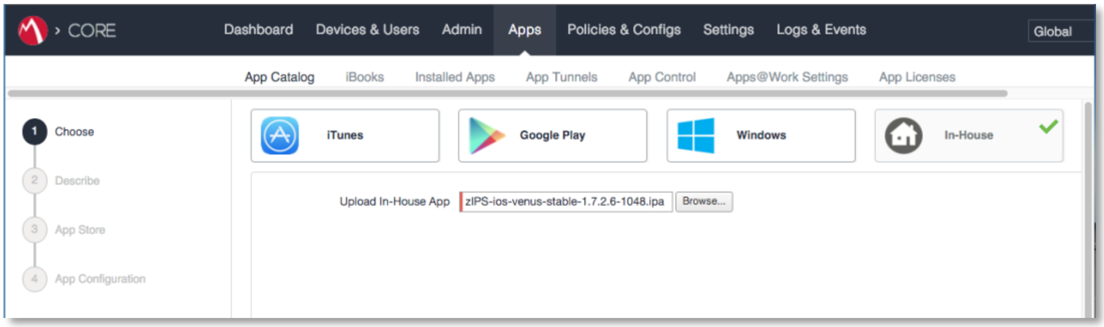


Name: Label Name

Description:

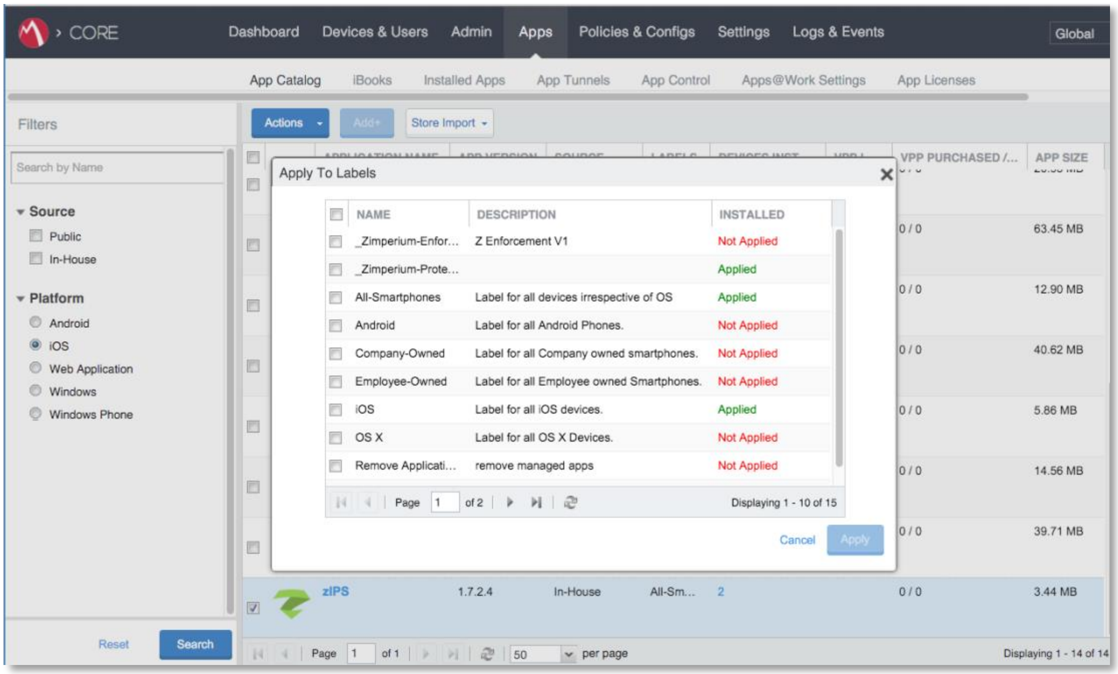
    b. Enter Label Name and short description
    c. Click **Save**

2) Upload and create zIPS application
    a. Apps/ Add+



Upload In-House App: zIPS-ios-venus-stable-1.7.2.6-1048.ipa

   b. Click **Next** and add/update information as needed in the next two screens and then click **Finish**.
   c. The application is now ready to be deployed.
3) Assign the label created in step 1) to this application.
   a. Click the radio button in front of the application just imported and click **Actions** and **Apply to Label**.



Apply To Labels

□	NAME	DESCRIPTION	INSTALLED
□	_Zimperium-Enfor...	Z Enforcement V1	Not Applied
□	_Zimperium-Prote...		Applied
□	All-Smartphones	Label for all devices irrespective of OS	Applied
□	Android	Label for all Android Phones.	Not Applied
□	Company-Owned	Label for all Company owned smartphones.	Not Applied
□	Employee-Owned	Label for all Employee owned Smartphones.	Not Applied
□	iOS	Label for all iOS devices.	Applied
□	OS X	Label for all OS X Devices.	Not Applied
□	Remove Applicati...	remove managed apps	Not Applied

Page 1 of 2 Displaying 1 - 10 of 15

Cancel Apply

   b. Choose the label created in step 1) and click **Apply**.
4) Assign this label to all devices that are required to be protected by zIPS
   a. Device & Users/ Devices.
   b. Click on the radio button next to all devices to be protected.
   c. Click **Actions** and then choose **Apply to Label**.
   d. Choose the Label to be applied and click **Apply**.

Level 2a: User Synchronization

To avoid having to create user credentials and the user management lifecycle, users and their devices can be synchronized through MDM integration. This allows all user management functions to be handled at the MDM console.

After the initial User Synchronization during the MDM Integration setup, users are managed through a scheduled synchronization process that runs every four hours. If we see additional devices in the label(s) being used for synchronization, we add them and their users to zConsole.

If we see devices removed, then we also remove them from the zConsole. Doing this does not remove their events logged since they have been created.

Ad-hoc MDM Synchronization

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

The zConsole application receives the identification information from zIPS used for the authentication and matches it up with the proper customer for authentication. Once that happens, zConsole retrieves that device and user information from the MDM configured for that customer. zIPS on that device is now authenticated and allowed to proceed. For this to work correctly, zIPS must be deployed as follows:

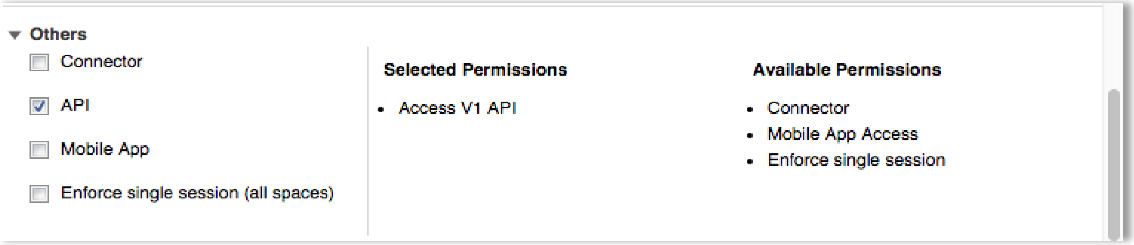
- **iOS**: Associate a plist file with the zIPS application that pushes down the fields used for the ad-hoc sync. This is described in the section “Level 2b: Auto Sign-in/Advanced Application Deployment” below.
- **Android**: Ad-hoc MDM synchronization for Android required the zIPS application to be modified. Contact your Zimperium Customer Support Team to set this up for Android.

When user synchronization occurs, the zConsole requests certain information from the MobileIron MDM. That information is used to determine if suspicious profiles are installed on devices that are protected by zIPS as well as all applications on each device. The information saved for each device includes:

- UUID, Device ID, Apps installed, and email address (if anonymous user functionality is not enabled).
- For zConsole, prior to release 4.13, serial number and IMEI are saved.

Setup User Synchronization

1) Create a MobileIron administrator with the proper API access.
   Navigate to: Devices & Users/ Users/ Add/ Add Local User.
   Then, Admin/ Click on the user and assign the Admin role below:



▼ Others

☐ Connector

☑ API

☐ Mobile App

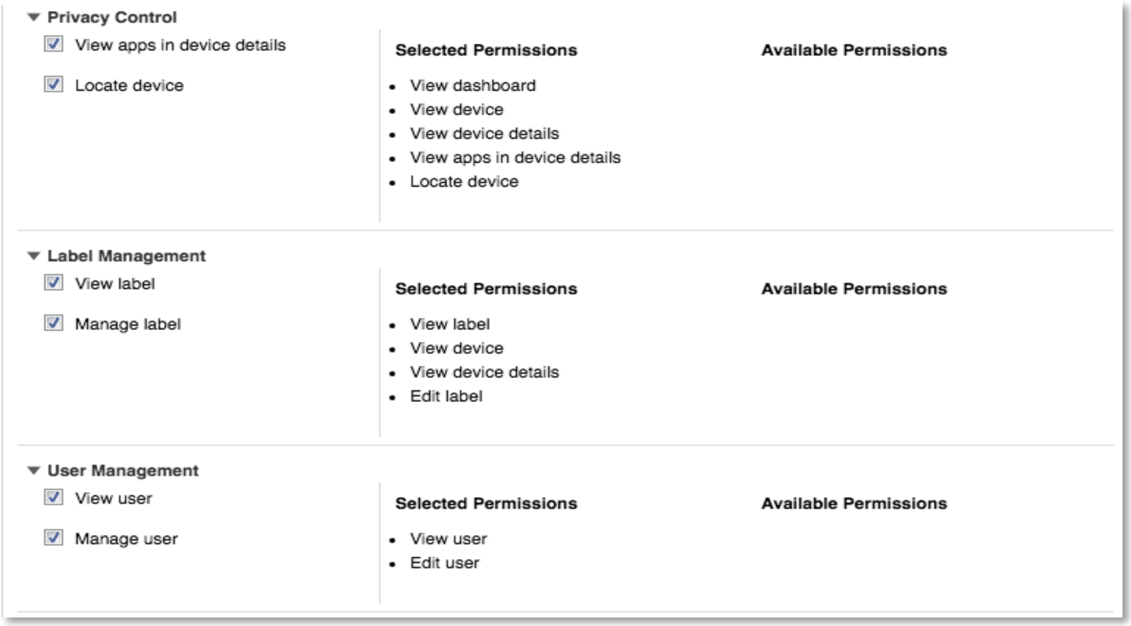
☐ Enforce single session (all spaces)

Selected Permissions

- Access V1 API

Available Permissions

- Connector
- Mobile App Access
- Enforce single session



▼ Privacy Control

☑ View apps in device details

☑ Locate device

Selected Permissions

- View dashboard
- View device
- View device details
- View apps in device details
- Locate device

Available Permissions

▼ Label Management

☑ View label

☑ Manage label

Selected Permissions

- View label
- View device
- View device details
- Edit label

Available Permissions

▼ User Management

☑ View user

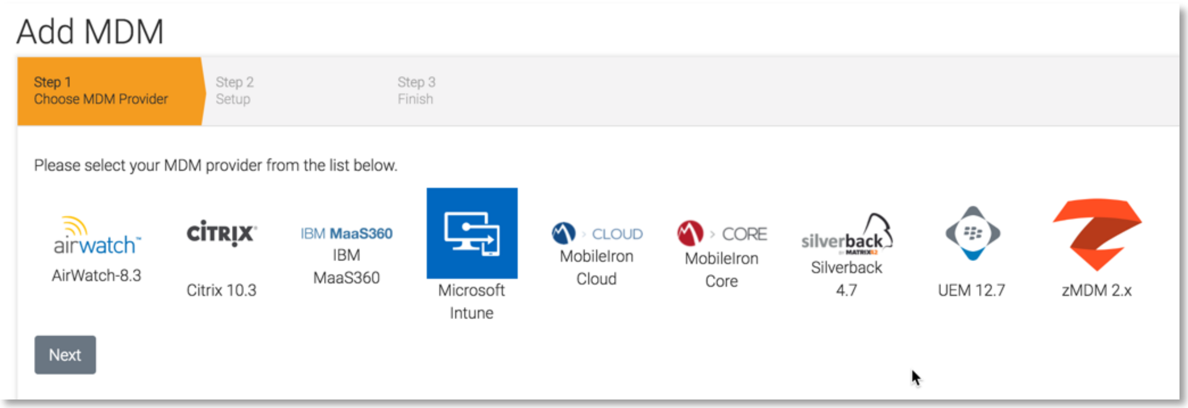
☑ Manage user

Selected Permissions

- View user
- Edit user

Available Permissions

2) Create one or more Labels that contain the devices that are protected if you do not have one that exists. The zConsole uses these label(s) to synchronize devices and their associated users.
3) Log into zConsole and navigate to Manage/ MDM.
4) Click **Add MDM** and select MobileIron Core.



Add MDM

Step 1
Choose MDM Provider

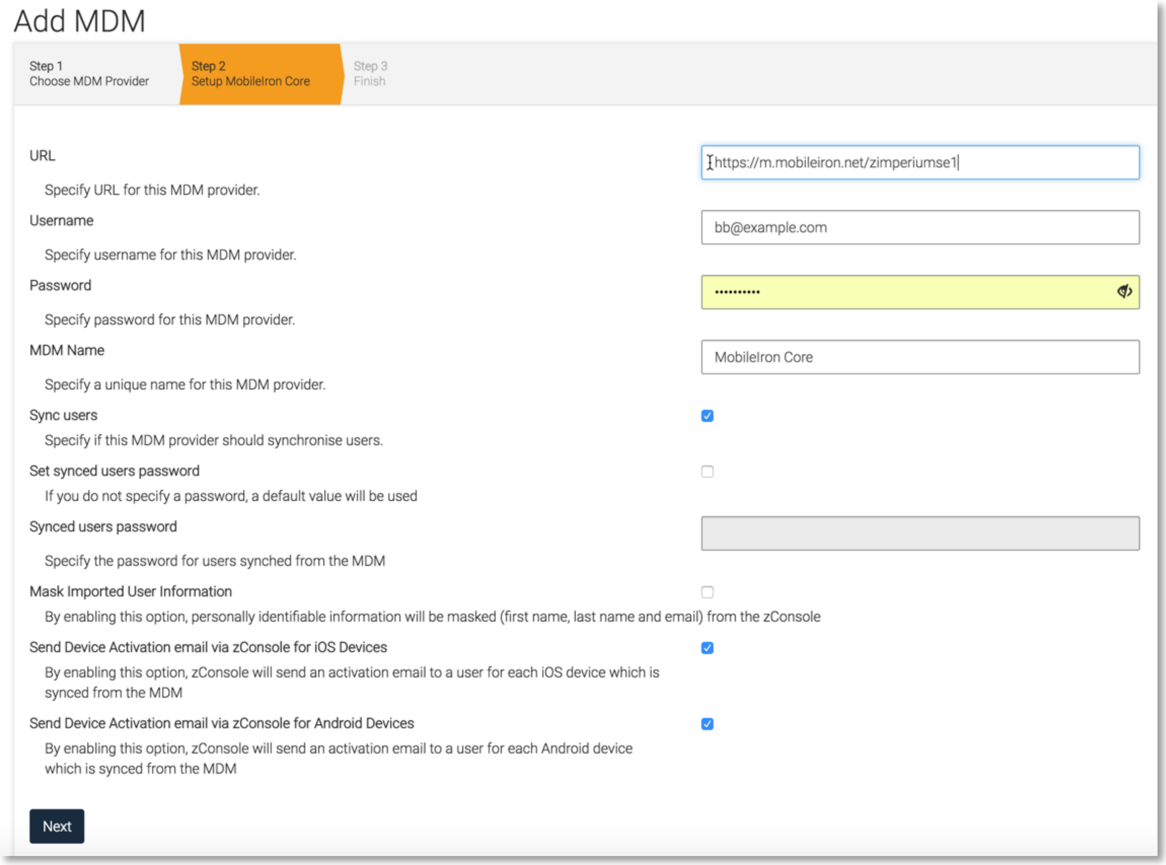
Step 2
Setup

Step 3
Finish

Please select your MDM provider from the list below.

5) Enter information pertinent for the MobileIron integration indicated in the table.

Item	Specifics
URL	URL of the MobileIron API Server
Username	MobileIron Administrator created with the API role access
Password	Password of the MobileIron Administrator
MDM Name	The name used in zConsole to reference this MDM integration. This is prepended to the group name to form the zConsole group name.
Sync Users	Check this box to ensure users/devices are synchronized with the MobileIron Labels chosen in the next page.
Set synced users password	Check this box to override the default password during user sync. If this is not checked a default password is computed as follows for all users that are synchronized: Start with the Zimperium environment name (this can be supplied by your Customer Success contact), change all uppercase letters to lowercase and also change all spaces to dashes. Then append the string “1234!” to the end. So, the value ‘*Zimperium Test’* becomes ‘*zimperium-test1234!’*
Synced users password	The override value of the password to use for each user when they are synchronized.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, for instance, name and email address.
Send Device Activation email via zConsole 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	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 MobileIron Core | Step 3 Finish

URL: https://m.mobileiron.net/zimperiumse1

Specify URL for this MDM provider.

Username: bb@example.com

Specify username for this MDM provider.

Password: ••••••••••

Specify password for this MDM provider.

MDM Name: MobileIron Core

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 synched 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

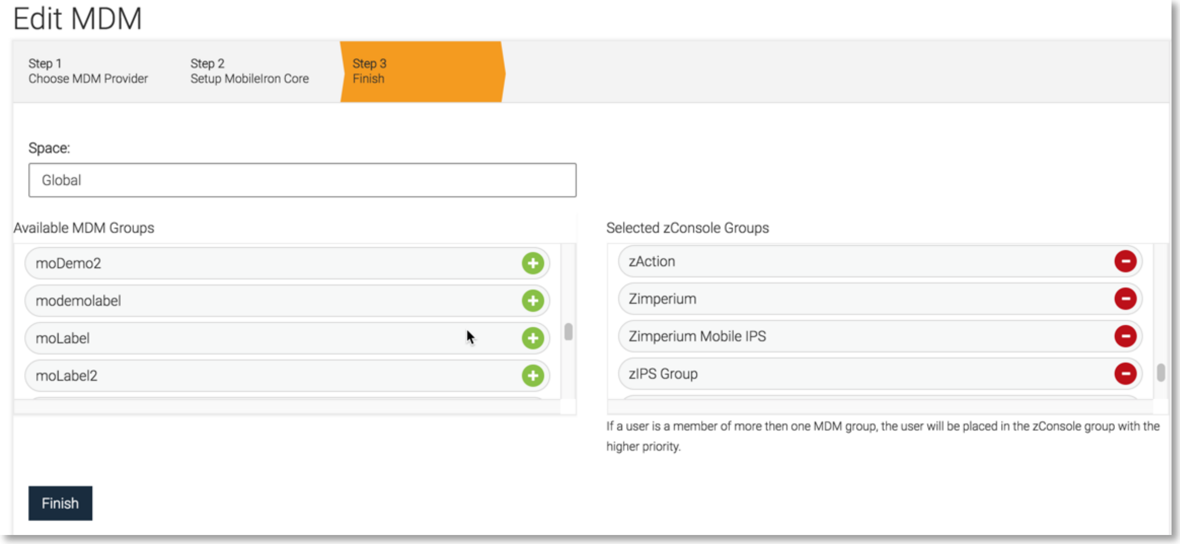
Send Device Activation email via zConsole for iOS Devices ☑

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

6) Click **Next** and choose the MobileIron Space. Then, choose the groups to synchronize, then click **Finish**.



Edit MDM

Step 1 Choose MDM Provider | Step 2 Setup MobileIron Core | Step 3 Finish

Space: Global

Available MDM Groups:

- moDemo2
- modemolabel
- moLabel
- moLabel2

Selected zConsole Groups:

- zAction
- Zimperium
- Zimperium Mobile IPS
- zIPS Group

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

Note: Spaces are used to separate managed entities for the ease of administration, such as an organizational hierarchy. Now users can sync devices for MobileIron spaces, along with the default space.

When more than one label is chosen the highest label in the list has the highest priority and so on down the list. If a device is present in more than one label, the label that applies is the highest label for the device.

7) Device and user synchronization now starts.
8) This can be verified by going to the Devices or Users pages in the zConsole to verify they are showing up. The device entries are greyed out until the user starts up zIPS and activates the applications.

Level 2b: Auto Sign-in/Advanced Application Deployment

The Zimperium zIPS application in both iOS and Android Enterprise (Android for Work) auto activate the user if MDM user synchronization has been configured. The process is different on each platform as described below.

iOS Activation

Zimperium's iOS zIPS application takes advantage the Managed Application Configuration when the app is pushed down to the device. This provides the best user experience, allowing the user to startup iOS zIPS without having to enter any credentials. The Managed Application configuration pre-programs iOS zIPS with this information.

This configuration is done within MobileIron. After adding the application:

- For zIPS Release 4.4.x and earlier, create a plist file that contains the information using variables as outlined in the table.

Configuration Key	Value Type	Configuration Value
serial (serial is not included in zConsole Release 4.13 or later)	String	$DEVICE_SN$
uuid	String	$DEVICE_UUID$
imei (imei is not included in zConsole Release 4.13 or later)	String	$DEVICE_IMEI$
wifimac	String	$DEVICE_MAC$

Note: The configuration keys are case sensitive.

For zIPS 4.4.x and earlier, the plist file is created as a text file in the following format using the variables in the above table.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList
1.0.dtd">
<plist version="1.0">
```

```
    <dict>
             <key>serial</key>
            <string>$DEVICE_SN$</string>
             <key>uuid</key>
            <string>$DEVICE_UUID$</string>
            <key>imei</key>
            <string>$DEVICE_IMEI$</string>
            <key>wifimac</key>
            <string>$DEVICE_MAC$</string>
    </dict>
</plist>
```

For iOS Ad-Hoc MDM sync to function properly, add these two new plist values.

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

- For zIPS Release 4.7 and later, create a plist file that contains the information using variables as outlined in the table.

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

Note: The configuration keys are case sensitive.

For zIPS 4.7 and later, the plist file is created as a text file in the following format using the variables in the above table.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList
1.0.dtd">
<plist version="1.0">
    <dict>
             <key>uuid</key>
            <string>$DEVICE_UUID$</string>
            <key>tenantid</key>
            <string>demo</string>
            <key>defaultchannel</key>
            <string>https://rx-demo.zimperium.com:443/srx</string>
    </dict>
</plist>
```

Add this plist file to MobileIron via the console:

1) Policies & Configs/ Configurations/ Add New/ iOS & OS X/ Managed App Config.
2) Select the file you just created above to upload.
3) Enter the bundle ID for the iOS app, com.zimperium.zIPS. (**Note**: If you are using the zIPS app from the Apple Play Store, use the bundle ID: com.zimperium.zIPS.appstore)
4) Click on the radio button by the new Managed App Configuration item.
5) More Actions/ Add to Label: Choose the label associated with the iOS zIPS app.

6) Click **Apply**.

Each time the iOS zIPS app gets pushed to a device it contains the information specified in the plist file. When the user clicks on the zIPS app, they automatically sign into the proper zConsole environment.

Android Activation

Android Enterprise (Android for Work) users can continue to use the managed app config for activations. You need to make sure you are passing the right device ID value for the configuration parameter. The variables are the same set as the plist variables in the "iOS Activation" section.

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

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

See the "Zimperium zConsole Configuration Guide" in the section "MDM Activation" 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 zIPS app being pushed to them.

Activation with MobileIron Messaging

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

Level 3: Basic Protection

MobileIron Integration Level three does not apply. Proceed to level four.

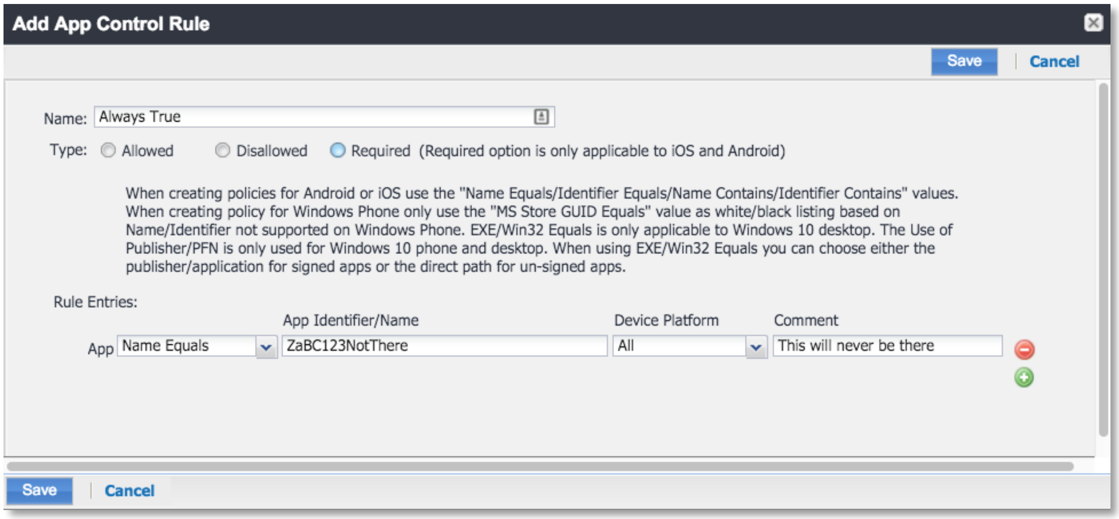
Level 4: Full Protection

The Zimperium integration with MobileIron provides the ability to apply a specific Label to the device within the customer's MobileIron environment. This allows the MobileIron administrator to define specific actions such as to quarantine a device, remove email access, assign a configuration or even unenroll a device (which happens automatically). To accomplish this, the MobileIron administrator needs to coordinate with the zConsole administrator what specific actions are needed and do the following configuration for each one with a unique label. MDM Integration with zConsole also has to be setup and functional.

This Label assigned to the device is pre-assigned to a Policy that is always evaluated as TRUE which activates a Compliance Action. The configuration involves the following:

- Building an App Control Rule
- Linking it to a Policy that is then configured to a Compliance Action.

1) Create a new App Control Rule that evaluates to be true so that whatever Policy it is used in, always runs when a device is assigned to it:
    a. Apps
    b. App Control
    c. Add (use the fields below to create a check for an application that does not exist)



Name: Always True

Type: ○ Allowed ○ Disallowed ● Required (Required option is only applicable to iOS and Android)

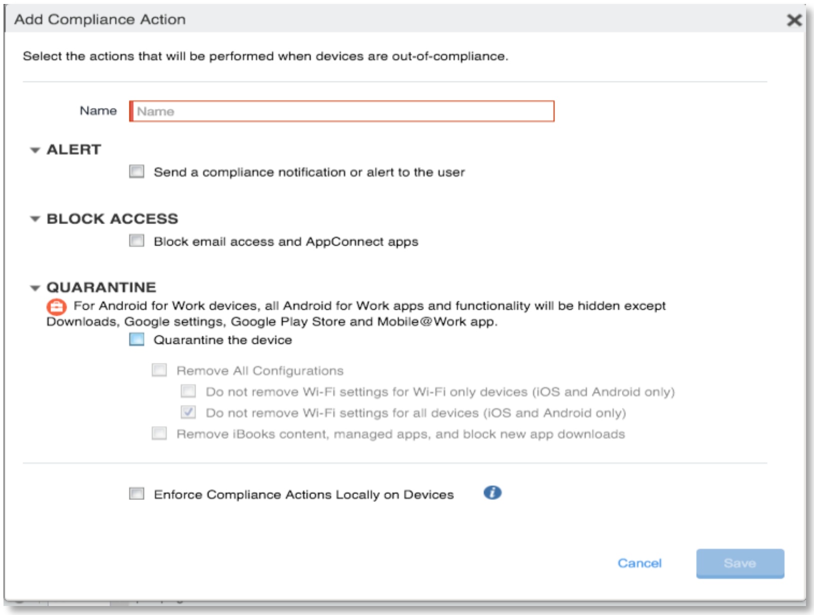
When creating policies for Android or iOS use the "Name Equals/Identifier Equals/Name Contains/Identifier Contains" values. When creating policy for Windows Phone only use the "MS Store GUID Equals" value as white/black listing based on Name/Identifier not supported on Windows Phone. EXE/Win32 Equals is only applicable to Windows 10 desktop. The Use of Publisher/PFN is only used for Windows 10 phone and desktop. When using EXE/Win32 Equals you can choose either the publisher/application for signed apps or the direct path for un-signed apps.

Rule Entries:

		App Identifier/Name	Device Platform	Comment
App	Name Equals	ZaBC123NotThere	All	This will never be there

    d. Save

2) Define a Compliance Action which affects the device under threat:
    a. Policies & Configs
    b. Compliance Actions
    c. Add+ (to add a new Compliance Action using the dialog box below)



Add Compliance Action ✕

Select the actions that will be performed when devices are out-of-compliance.

Name: Name

▾ ALERT

□ Send a compliance notification or alert to the user

▾ BLOCK ACCESS

□ Block email access and AppConnect apps

▾ QUARANTINE

For Android for Work devices, all Android for Work apps and functionality will be hidden except Downloads, Google settings, Google Play Store and Mobile@Work app.

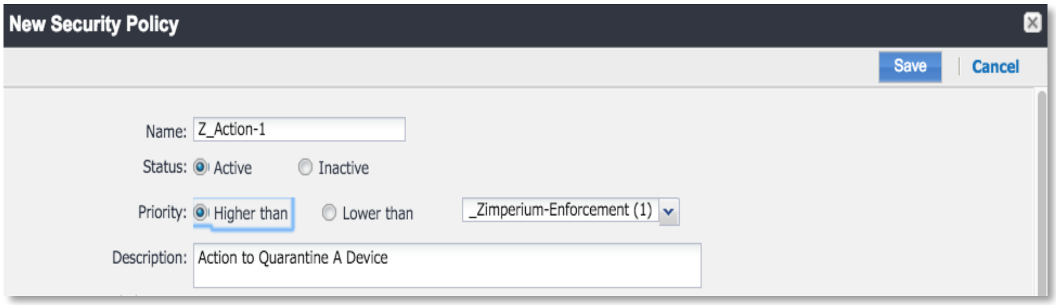
□ Quarantine the device

- □ Remove All Configurations
  - □ Do not remove Wi-Fi settings for Wi-Fi only devices (iOS and Android only)
  - ☑ Do not remove Wi-Fi settings for all devices (iOS and Android only)
- □ Remove iBooks content, managed apps, and block new app downloads

□ Enforce Compliance Actions Locally on Devices

  d. Save

3) Create a Policy that keys off of the App Control Rule:
   a. Policies & Configs
   b. Policies
   c. Add New (Choose Security form the drop-down list)
   d. Choose a name and ensure Active is checked.
   e. Enter a description for this Policy/Action



New Security Policy

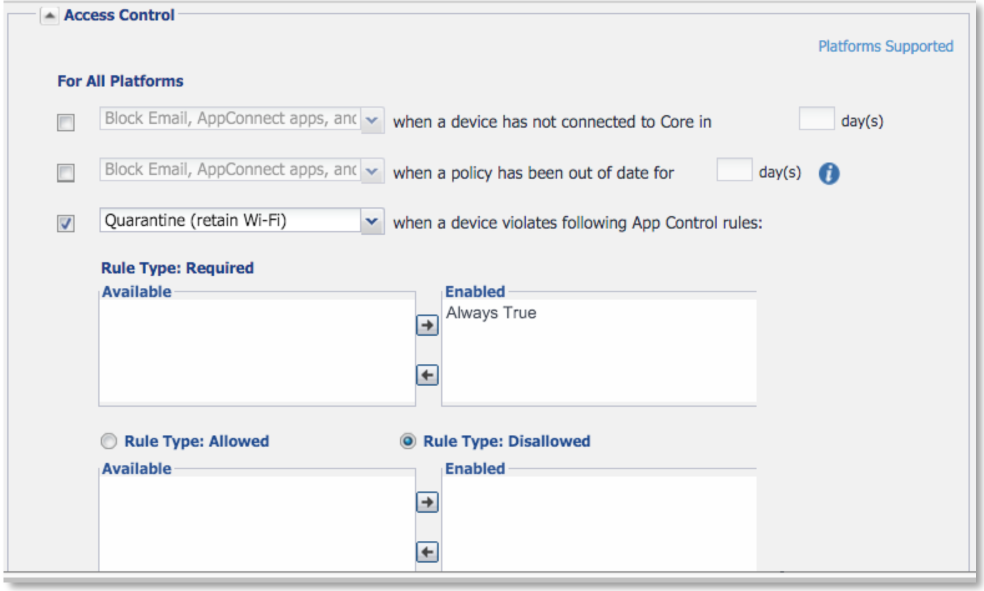
Name: Z_Action-1

Status: ● Active ○ Inactive

Priority: ● Higher than ○ Lower than _Zimperium-Enforcement (1)

Description: Action to Quarantine A Device

   f. Scroll down to Access Control
   g. Click on the radio button for “When a device violates the following App Control rules:”
   h. Choose the Compliance Action created earlier
   i. Choose the App Control rule “Always True” and move to the Enabled side



Access Control

Platforms Supported

For All Platforms

□ Block Email, AppConnect apps, anc when a device has not connected to Core in day(s)

□ Block Email, AppConnect apps, anc when a policy has been out of date for day(s)

☑ Quarantine (retain Wi-Fi) when a device violates following App Control rules:

Rule Type: Required

Available

Enabled: Always True

○ Rule Type: Allowed ● Rule Type: Disallowed

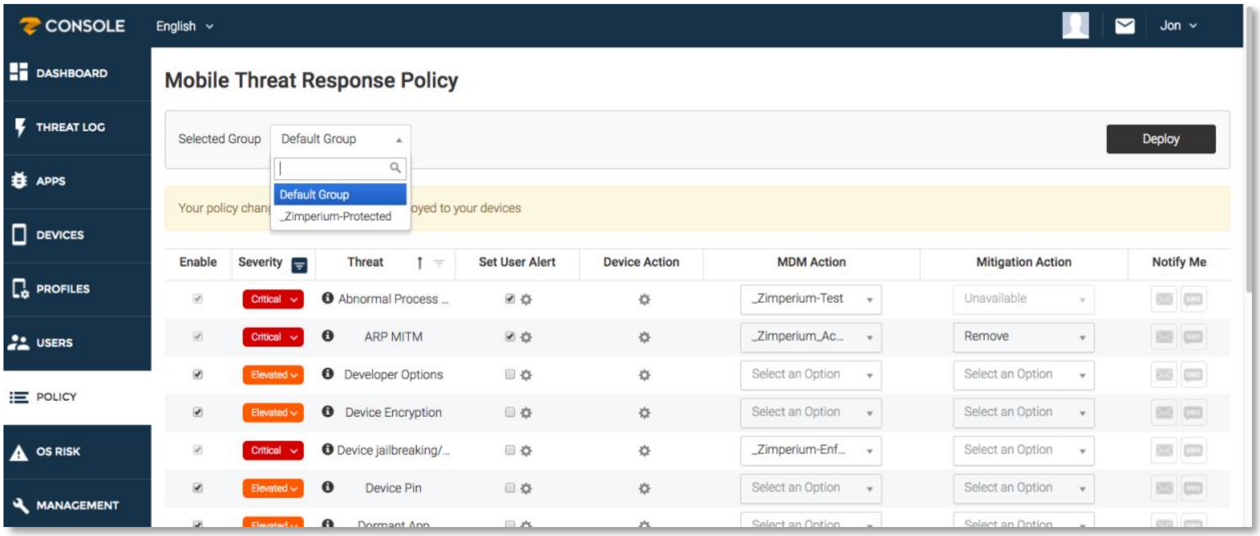
Available

Enabled

   j. Click **Save**

4) Assign a Label that is referenced in the zConsole Threat Response Policy/Matrix.
   a. Click the radio button in the front of this new Policy
   b. More Actions
   c. Apply to Label
   d. Choose the label to apply to this Policy that can be used in the zConsole (if needed you can create a new label)

This is now a new Action that can now be selected in the Threat Response Policy/Matrix such as shown under the MDM actions column below. An MDM sync might have to occur for this to be visible.



Mobile Threat Response Policy

Selected Group: Default Group

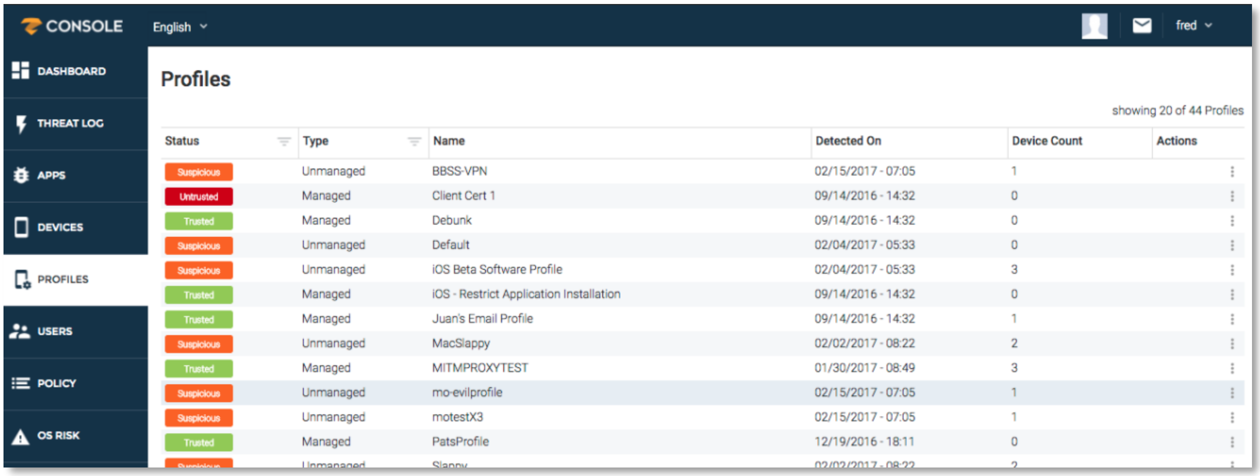
- Default Group
- _Zimperium-Protected

Your policy chan… …oyed to your devices

Enable	Severity	Threat	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
☑	Critical	Abnormal Process ...	☑ ⚙	⚙	_Zimperium-Test	Unavailable	✉ 💬
☑	Critical	ARP MITM	☑ ⚙	⚙	_Zimperium_Ac...	Remove	✉ 💬
☑	Elevated	Developer Options	□ ⚙	⚙	Select an Option	Select an Option	✉ 💬
☑	Elevated	Device Encryption	□ ⚙	⚙	Select an Option	Select an Option	✉ 💬
☑	Critical	Device jailbreaking/...	□ ⚙	⚙	_Zimperium-Enf...	Select an Option	✉ 💬
☑	Elevated	Device Pin	□ ⚙	⚙	Select an Option	Select an Option	✉ 💬
☑	Elevated	Dormant App	□ ⚙	⚙	Select an Option	Select an Option	✉ 💬

iOS Profiles (MobileIron Core)

Zimperium collects managed and unmanaged profiles through the MDM integration. These profiles are displayed in the Profiles page and any unmanaged profiles are defined as Suspicious.



Profiles

showing 20 of 44 Profiles

Status	Type	Name	Detected On	Device Count	Actions
Suspicious	Unmanaged	BBSS-VPN	02/15/2017 - 07:05	1	⋮
Untrusted	Managed	Client Cert 1	09/14/2016 - 14:32	0	⋮
Trusted	Managed	Debunk	09/14/2016 - 14:32	0	⋮
Suspicious	Unmanaged	Default	02/04/2017 - 05:33	0	⋮
Suspicious	Unmanaged	iOS Beta Software Profile	02/04/2017 - 05:33	3	⋮
Trusted	Managed	iOS - Restrict Application Installation	09/14/2016 - 14:32	0	⋮
Trusted	Managed	Juan's Email Profile	09/14/2016 - 14:32	1	⋮
Suspicious	Unmanaged	MacSlappy	02/02/2017 - 08:22	2	⋮
Trusted	Managed	MITMPROXYTEST	01/30/2017 - 08:49	3	⋮
Suspicious	Unmanaged	mo-evilprofile	02/15/2017 - 07:05	1	⋮
Suspicious	Unmanaged	motestX3	02/15/2017 - 07:05	1	⋮
Trusted	Managed	PatsProfile	12/19/2016 - 18:11	0	⋮
Suspicious	Unmanaged	Slappy	02/02/2017 - 08:22	2	⋮

The Profiles page filter contains the following:

Column	Description
Status	Display profiles that match the selected status of Trusted, Untrusted, Suspicious
Type	Display profiles that match the selection of Managed, Unmanaged
Name	Sort profiles based on their name
Detected On	Sort profiles by date/time that they were detected
Device Count	Sort profiles by number of devices they are installed on

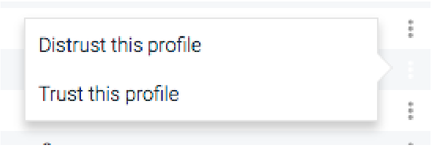
The Admin can modify the profile to either be trusted or distrusted. The lifecycle of an unmanaged profile detected by zIPS is the following:

1) After an MDM synchronization, qualify any new profiles.

2) Define which are MDM Managed and which are Unmanaged.

3) Set any Unmanaged Profiles to be suspicious and send an alert as defined in the Threat Response Policy/Matrix.

4) The Admin can then go to the Profiles page to find this unmanaged Profile. Click on the three dots to the right of the profile and select either **Trust this profile** or **Distrust this profile**. If Distrust is selected a new zIPS alert is created and the Threat Response Policy/Matrix is chosen.



MobileIron Cloud Integration with MobileIron Threat Defense

In this configuration, MobileIron Threat Defense, powered by the Zimperium z9 engine is activated in the MobileIron Core Mobile Go Agent. Since the engine is already built into the Mobile Go Agent, zIPS does not have to be pushed down to the device. When a device enrolls in MI Cloud in this scenario, the MobileIron Mobile Go Agent is configured with the activation code to enable the z9 engine and communicate with the proper Zimperium zConsole.

The following sections describe the different configuration levels for MobileIron Cloud Integration with MobileIron Threat Defense.

Level 1: Basic Application Deployment

Since MobileIron Threat Defense is provided by the Mobile Go Agent, the agent on the device needs to be updated with the activation code to enable the feature. This is done differently in iOS and Android. But in both cases, the same MobileIron Activation Code is required. This code can be retrieved after the MobileIron Cloud MDM integration has been performed in the next step.

Level 2a: User Synchronization

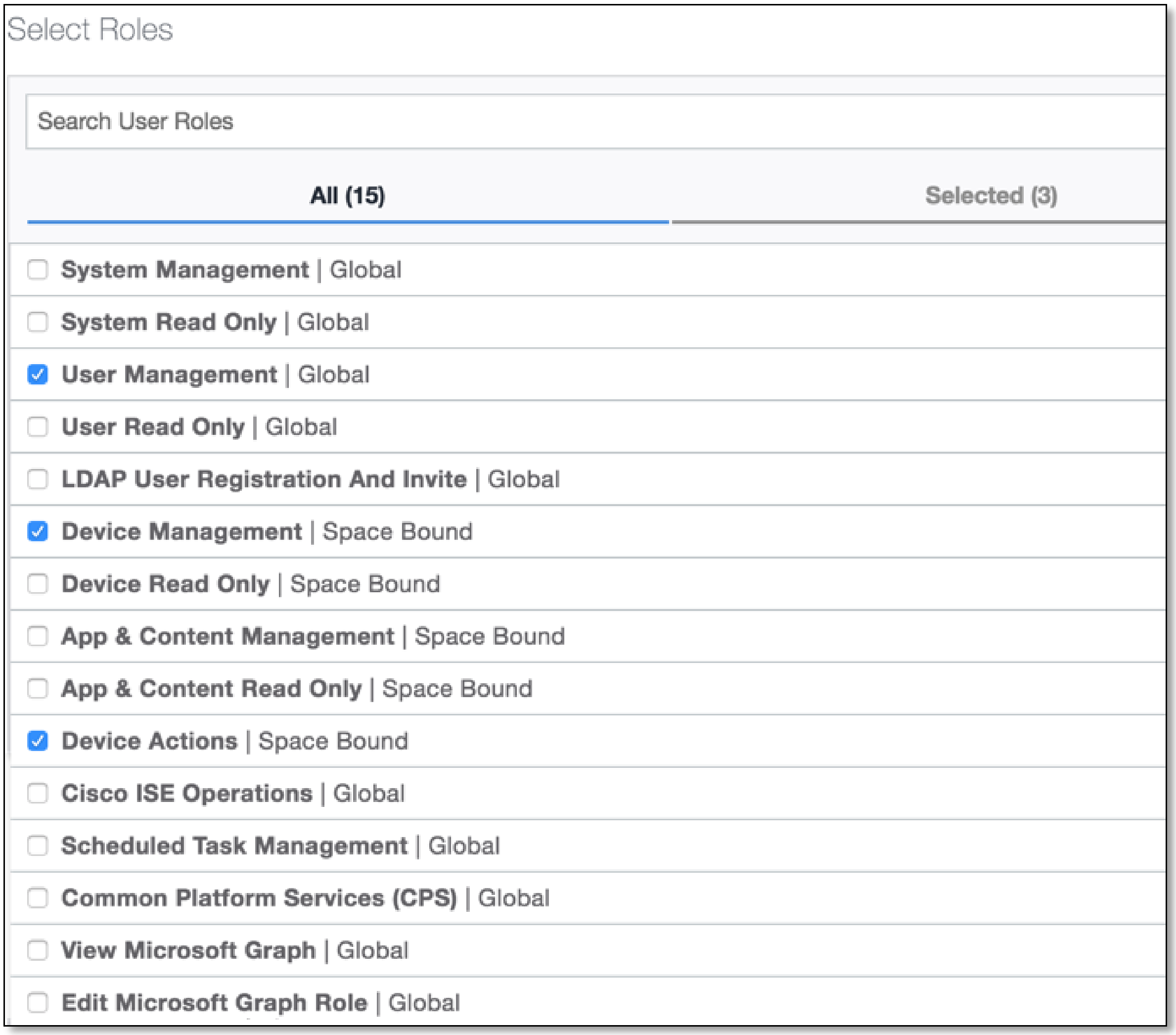
To avoid having to create user credentials and the user management lifecycle, users and their devices from selected device groups can be synchronized through MDM integration. This allows all user and device management functions to be handled at the MDM console.

After the initial User Synchronization during the MDM Integration setup, users are managed through a scheduled synchronization process that runs every four hours. If additional devices are in the device group(s) being used for synchronization, they are added along with their users to zConsole. If devices are removed, then they are also removed from the zConsole. Doing this does not remove their events logged since they have been created.

Setup User Synchronization

1. Create a MobileIron administrator with the proper API access.
    a. Navigate to: Users/ Users/ +Add/ Single User
    b. Enter the information for this new administrator and click **Done**.

2. Click on the new administrator and select the **Actions** drop-down. Select **Assign Roles**. Add the proper roles to the new administrator and click **Next**, and then click **Done**. For instance, add the following roles:
    - User Management
    - Device Management
    - Device Actions



Select Roles

Search User Roles

All (15) | Selected (3)

☐ **System Management** | Global

☐ **System Read Only** | Global

☑ **User Management** | Global

☐ **User Read Only** | Global

☐ **LDAP User Registration And Invite** | Global

☑ **Device Management** | Space Bound

☐ **Device Read Only** | Space Bound

☐ **App & Content Management** | Space Bound

☐ **App & Content Read Only** | Space Bound

☑ **Device Actions** | Space Bound

☐ **Cisco ISE Operations** | Global

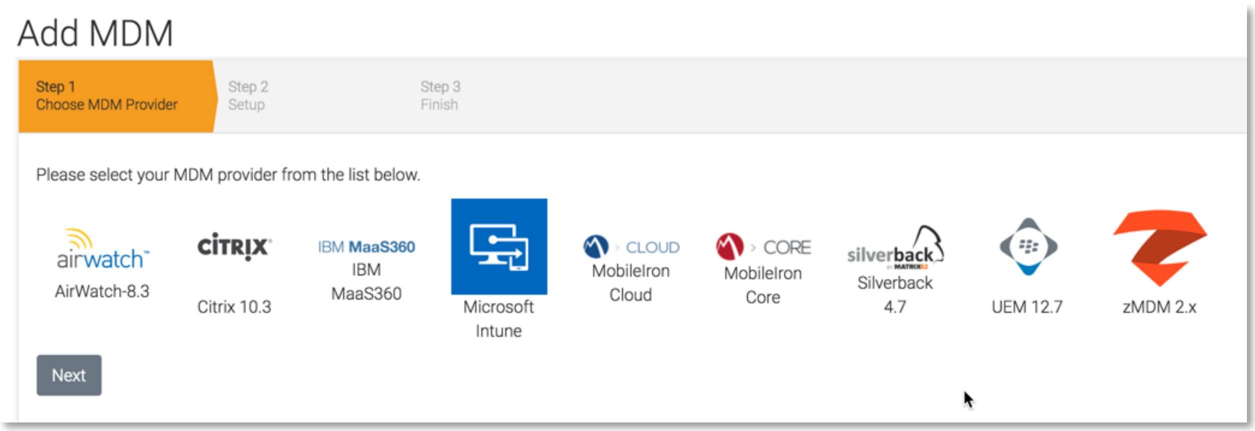
☐ **Scheduled Task Management** | Global

☐ **Common Platform Services (CPS)** | Global

☐ **View Microsoft Graph** | Global

☐ **Edit Microsoft Graph Role** | Global

3. Create one or more device groups that you plan to contain the devices that are protected, if a device group does not exist yet for this purpose. zConsole uses these device group(s) to synchronize devices and their associated users.
4. Log into zConsole and navigate to Manage/ MDM.
5. Click on **Add MDM** and select MobileIron Cloud.



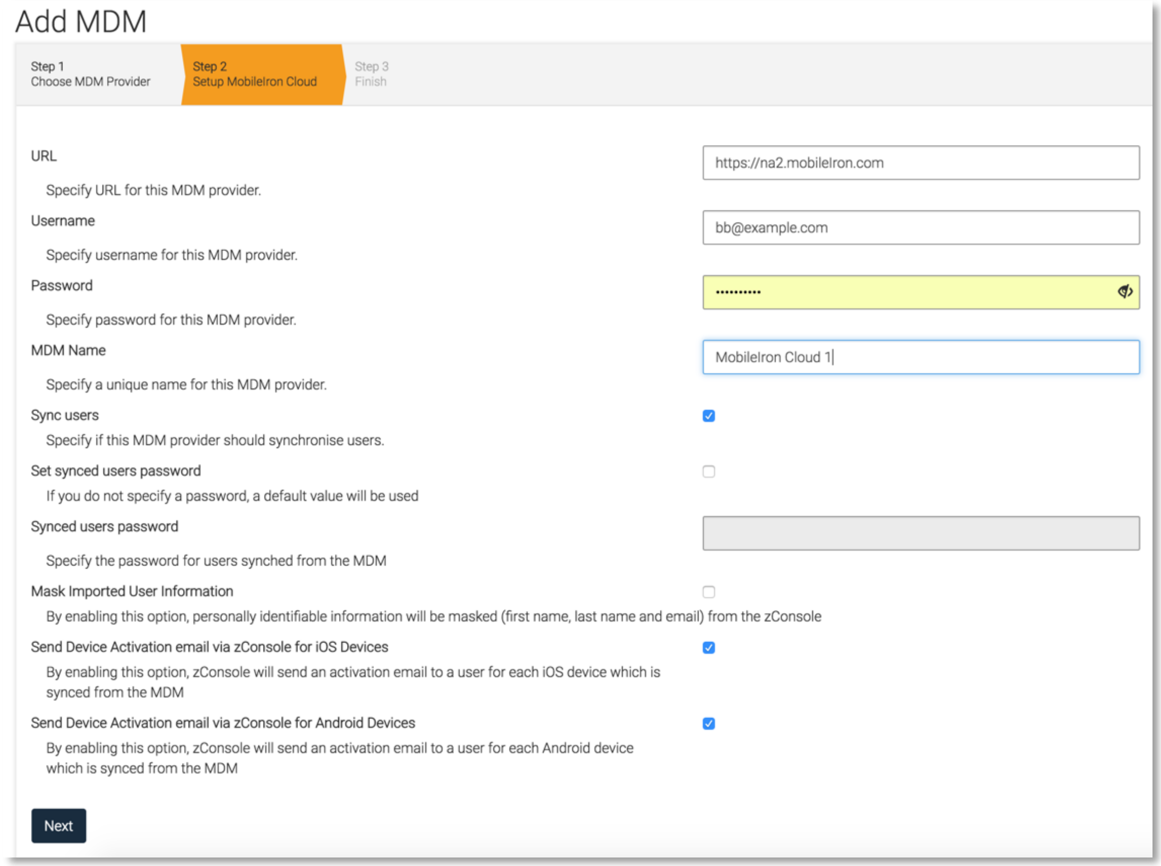
Add MDM

Please select your MDM provider from the list below.

6. Enter information pertinent for the MobileIron integration

Item	Specifics
URL	Url of the MobileIron API Server
Username	MobileIron Administrator created with the API role access
Password	Password of the MobileIron Administrator
MDM Name	The name used in zConsole to reference this MDM integration. This is prepended to the group name to form the zConsole group name.
Sync Users	Check this box to ensure users/devices are synchronized with the MobileIron Labels chosen on the next page.
Set synced users password	Check this box to override the default password during user sync. If this is not checked a default password is computed as follows for all users that are synchronized: Start with the Zimperium environment name (this can be supplied by your Customer Success contact), change all uppercase letters to lowercase and also change all spaces to dashes. Then append “1234!” to the end. So, the value ‘*Zimperium Test*’ becomes ‘*zimperium-test1234!*’
Synced users password	The override value of the password to use for each user when they are synchronized.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, for instance name or email address.
Send Device Activation email via zConsole 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	Check this box to send an email to the user for every Android device synced with the MDM.



Add MDM

URL
Specify URL for this MDM provider.
https://na2.mobileIron.com

Username
Specify username for this MDM provider.
bb@example.com

Password
Specify password for this MDM provider.
••••••••••

MDM Name
Specify a unique name for this MDM provider.
MobileIron Cloud 1

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

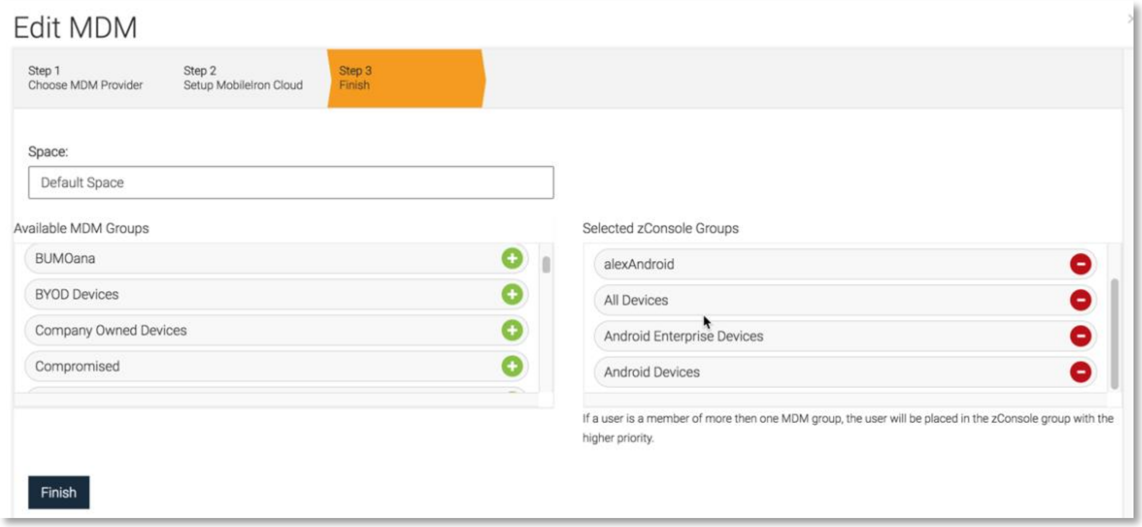
Synced users password
Specify the password for users synched from the MDM

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

7. Click **Next** and choose the MobileIron Space. Then, choose the groups to synchronize, then click **Finish**.



Space: Default Space

Available MDM Groups: BUMOana, BYOD Devices, Company Owned Devices, Compromised

Selected zConsole Groups: alexAndroid, All Devices, Android Enterprise Devices, Android Devices

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

> **Note**: Spaces are used to separate managed entities for the ease of administration, such as an organizational hierarchy. Now users can sync devices for MobileIron spaces, along with the default space.

When more than one device group is chosen the highest group in the list has the highest priority and so on down the list. If a device is present in more than one group, the group that applies is the highest group for the device.

8. Device and user synchronization now starts.
9. This can be verified by going to the Devices or Users pages in the zConsole to verify they are showing up. The device entries are greyed out until the user starts up zIPS and zIPS is activated.

Enable MobileIron Threat Defense

Now that a valid MobileIron MDM Integration has been setup, retrieve the activation code for MobileIron Threat Defense and apply it the Mobile Go agent on the device.

1) Log into the zConsole and navigate to Manage/ MDM.
2) Locate the MobileIron Cloud that was just configured and copy the MobileIron Activation Code to your clipboard.
3) Log into the MobileIron Console.
4) Perform the following steps for iOS devices:
    a) Navigate to **Apps** / **App Catalog**.
    b) Click on the **MobileIron Go** app link for iOS to open the app details page. (If the app is not listed, add it as a managed app from the App Store).
    c) Click on the **App Configurations** tab.

d) Click the plus sign next to the **iOS Managed App Configuration** to display the Configuration Setup page.
e) Provide a name for this entry.
f) Under the MobileIron Threat Defense Settings, enter the Activation Code (license token from Zimperium) and select the **Activate** option.

    Note: De-select the **Activate** option to disable MobileIron Threat Defense feature for the MobileIron Go app.

g) Select one of the following distribution options:
    - All Devices
    - No Devices (this is the default)
    - Custom

h) Click **Update**.
i) Navigate back to the **App Configurations** tab.
j) Click **Install on device**
k) Click **Install Application configuration settings**
l) Click **Edit**, scroll to the bottom of the screen and choose the option to Convert to Managed App.
m) Click **Update**.

5) Perform the following steps for Android devices:

a) Navigate to **Configurations**.
b) Click **+Add**.
c) Click **MobileIron Threat Defense**.
d) In the 'Create MobileIron Threat Defense Configuration' page, enter a name for the configuration.
e) (Optional) Enter a description.
f) In the Configuration Setup section, select the vendor **Zimperium**.
g) In the License Key field, enter your unique encrypted MobileIron Threat Defense activation code from Zimperium.
h) Click **Next**.
i) Select the **Enable this configuration** option.
j) Select one of the following distribution options:
    - All Devices
    - No Devices (this is the default)
    - Custom

k) Click **Done**.

At this point the MobileIron Threat Defense is enabled for both iOS and Android. When a user enrolls their device, the Activation code is sent to the Mobile Go agent and MobileIron Threat Defense starts to run.

The device shows up immediately in the zConsole in the default group and after the MDM Integration is automatically synchronized, and it shows in the assigned group.

Level 3: Basic Protection

MobileIron Integration Level three does not apply. Proceed to level four.

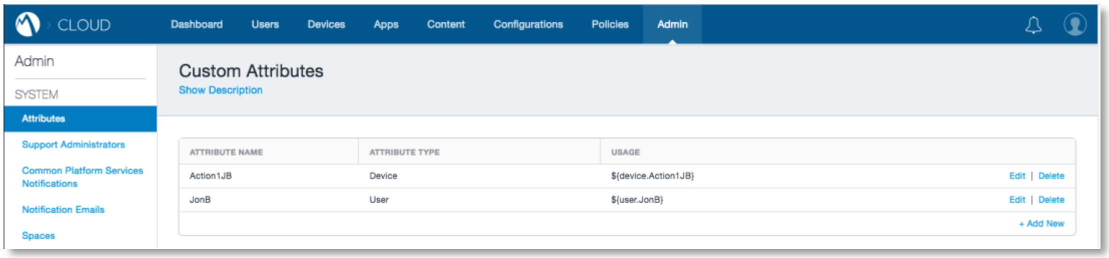
Level 4: Full Protection

The Zimperium integration with MobileIron provides the ability to apply a specific Device Group to the device within the customer's MobileIron environment. This allows the MobileIron administrator to define specific actions such as to quarantine a device, remove email access, assign a configuration or even unenroll a device (which happens automatically). To accomplish this, the MobileIron administrator needs to coordinate with the zConsole administrator the specific actions that are needed and do the following configuration for each one with a unique Device Group. MDM Integration with zConsole also has to be setup and functional.

The MobileIron Cloud integration contains one built in MDM action to Lock the device. The following steps are not needed for that action to be used.

When a device is under attack and the MDM action is set to some Device Group from the integrated MobileIron server, zConsole assigns the device to that device group via API calls. To set this up several configurations need to be done on the MobileIron Console:

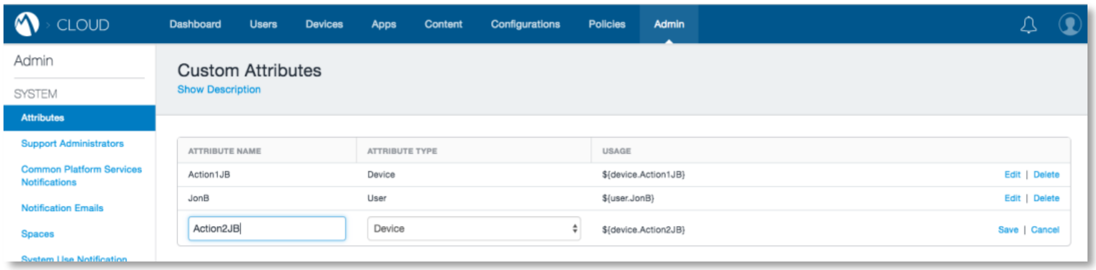
1) Log into the MobileIron Console
2) Navigate to the Admin page
3) Create a customer Device Attribute to be used to link the Device to the Device Group and Policy.
4) Click on the **+ Add New** option.



Custom Attributes

ATTRIBUTE NAME	ATTRIBUTE TYPE	USAGE	
Action1JB	Device	${device.Action1JB}	Edit | Delete
JonB	User	${user.JonB}	Edit | Delete
			+ Add New

5) Type the name of the new custom attribute and choose type **Device**. In the sample below the name is ‘Action2JB’. Click **Save**.



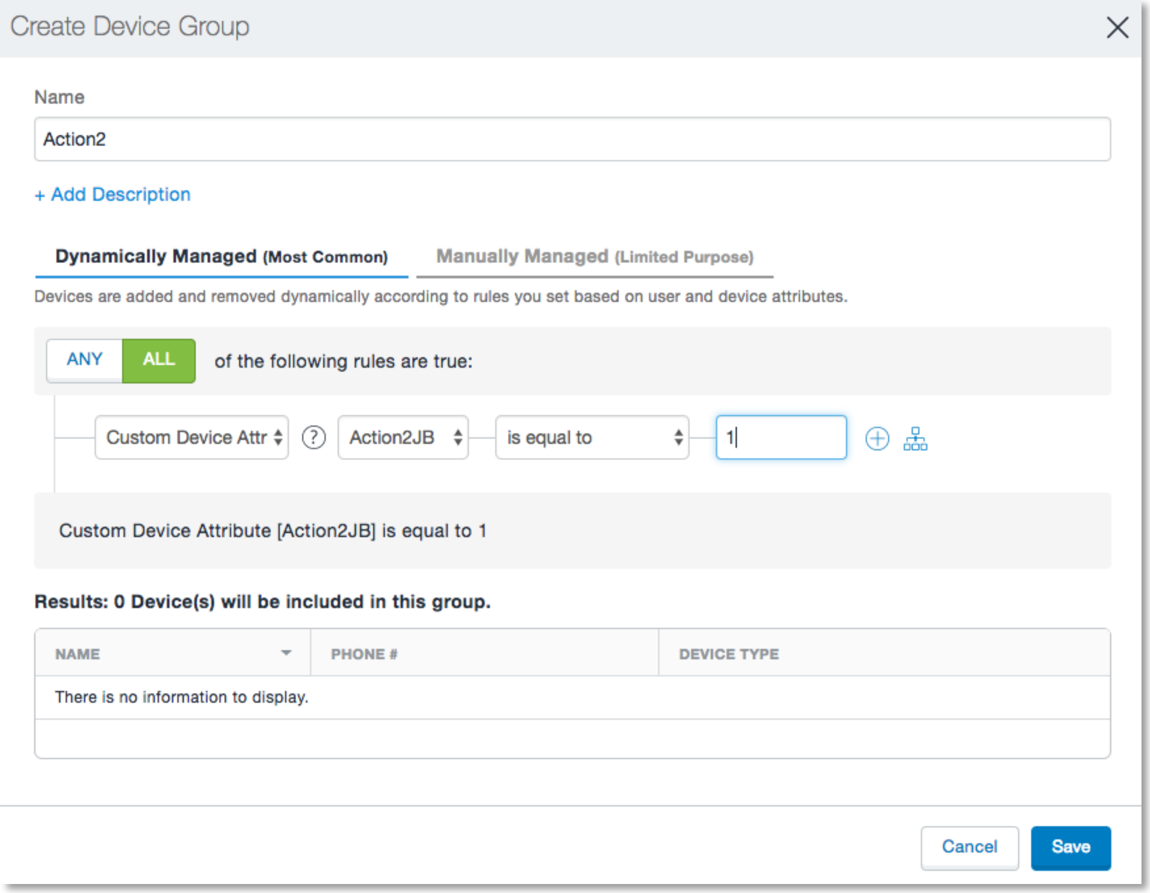
Custom Attributes

Show Description

ATTRIBUTE NAME	ATTRIBUTE TYPE	USAGE	
Action1JB	Device	${device.Action1JB}	Edit | Delete
JonB	User	${user.JonB}	Edit | Delete
Action2JB	Device	${device.Action2JB}	Save | Cancel

6) Create a dynamically managed Device Group based on the new Custom Device Attribute just created. navigate to Devices/ Device Groups. Click **+Add**.

7) Enter the new Device Group Name (This is the name that shows up in the TRM MDM actions column), Choose 'Custom Device Attribute' and then the new Custom Attribute just created with a value of '1'. Click **Save**.


Create Device Group

Name: Action2

+ Add Description
Dynamically Managed (Most Common)
Manually Managed (Limited Purpose)

Devices are added and removed dynamically according to rules you set based on user and device attributes.

ANY ALL of the following rules are true:

Custom Device Attr | Action2JB | is equal to | 1

Custom Device Attribute [Action2JB] is equal to 1

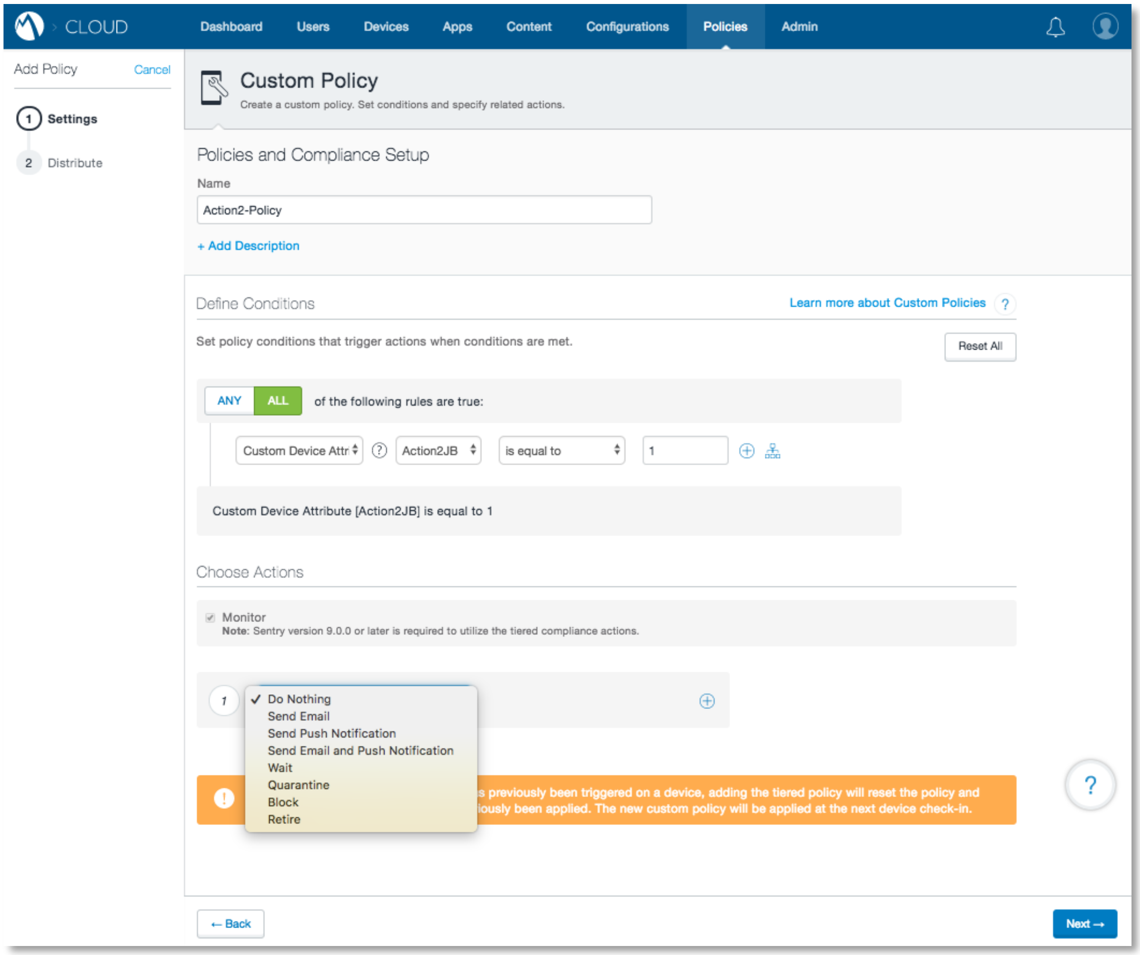
Results: 0 Device(s) will be included in this group.

NAME	PHONE #	DEVICE TYPE
There is no information to display.		

8) Create an Policy that is linked to the new Device Group just created that you plan to contain the action to carry out to protect the phone. Navigate to Policies and click the **+Add** option.

9) Choose a Custom Policy. Enter the Custom Policy name and choose the conditions, Any or All. This "Any" or "All" option does not matter as there is only one condition. Choose

‘Custom Device Attribute’, the new Custom Attribute name and the value entered previously, ‘1’. Then choose the actions to be executed as shown below. Click **Next**.



Custom Policy

Create a custom policy. Set conditions and specify related actions.

Policies and Compliance Setup

Name: Action2-Policy

Define Conditions

Set policy conditions that trigger actions when conditions are met.

ALL of the following rules are true:

Custom Device Attr | Action2JB | is equal to | 1

Custom Device Attribute [Action2JB] is equal to 1

Choose Actions

☑ Monitor
Note: Sentry version 9.0.0 or later is required to utilize the tiered compliance actions.

1
✓ Do Nothing
Send Email
Send Push Notification
Send Email and Push Notification
Wait
Quarantine
Block
Retire

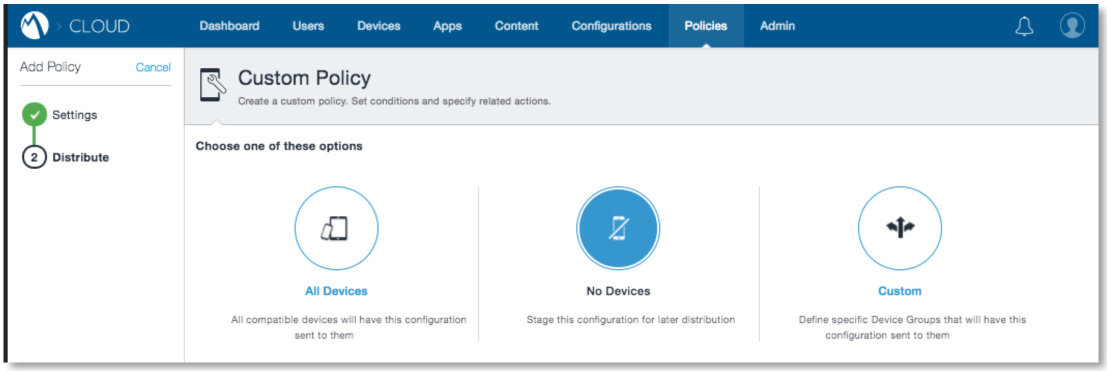
s previously been triggered on a device, adding the tiered policy will reset the policy and iously been applied. The new custom policy will be applied at the next device check-in.

The possible actions are:

- Send Email
- Send Push Notification
- Send Email and Push Notification
- Wait
- Quarantine
- Block
- Retire

For each option selected, an appropriate entry is displayed to enter more information, such as the text to be sent to the user if ‘Send Push Notification’ is chosen. More than one action can be chosen by clicking on the ‘+’ sign to add another action.

10) On the Distribution page, assign this policy to ‘No Devices’ and then click **Done**.



Custom Policy

Create a custom policy. Set conditions and specify related actions.

Choose one of these options

All Devices

All compatible devices will have this configuration sent to them

No Devices

Stage this configuration for later distribution

Custom

Define specific Device Groups that will have this configuration sent to them

11) Log into zConsole and perform an MDM sync to learn the new Device Groups. Navigate to MANAGE/ MDM. Click **Sync Now** and then **OK** for the MDM integration just modified.
12) The MDM actions column now include any new Device Groups created.

Actions assigned in the Threat Response Policy/Matrix happen automatically when the specific assigned threat is detected. For more information on this topic, see “Zimperium zConsole Configuration Guide” and the “MDM Capabilities Matrix” section in the Appendix.

MobileIron Cloud Integration with zIPS

The following sections describe the different configuration levels for MobileIron Cloud Integration with zIPS.

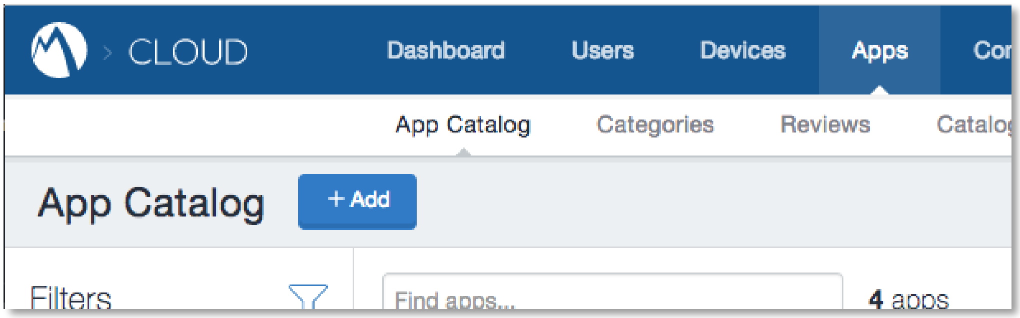
Level 1: Basic Application Deployment

To deploy the zIPS application through MobileIron, ask your Customer Success Team at Zimperium for the iOS and Android version of zIPS.

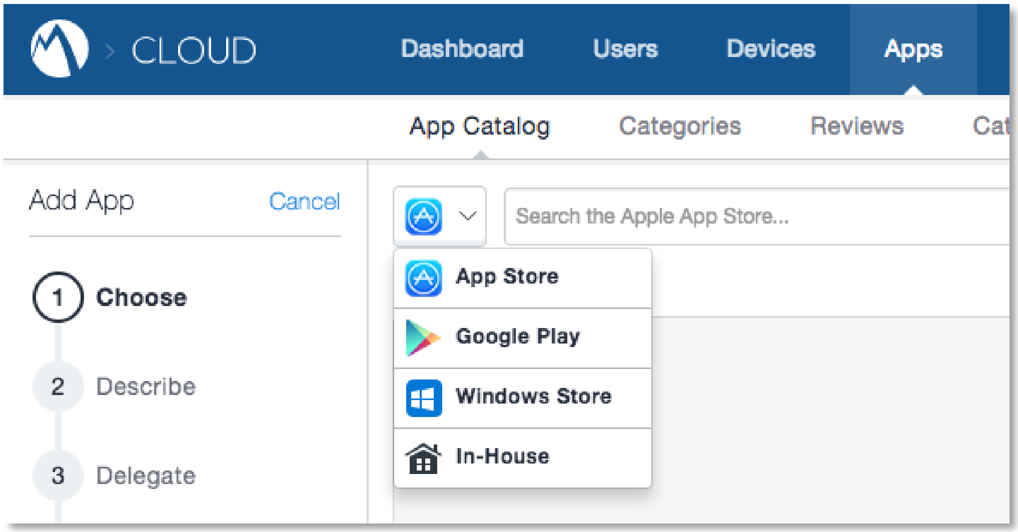
To deploy the zIPS app, log into MobileIron. Create a new In-House App and upload the proper application file (IPA for iOS or APK for Android). Distribute the app via your chosen method and publish.

Perform the following steps:

1) Navigate to Apps/ App Catalog/ +Add.

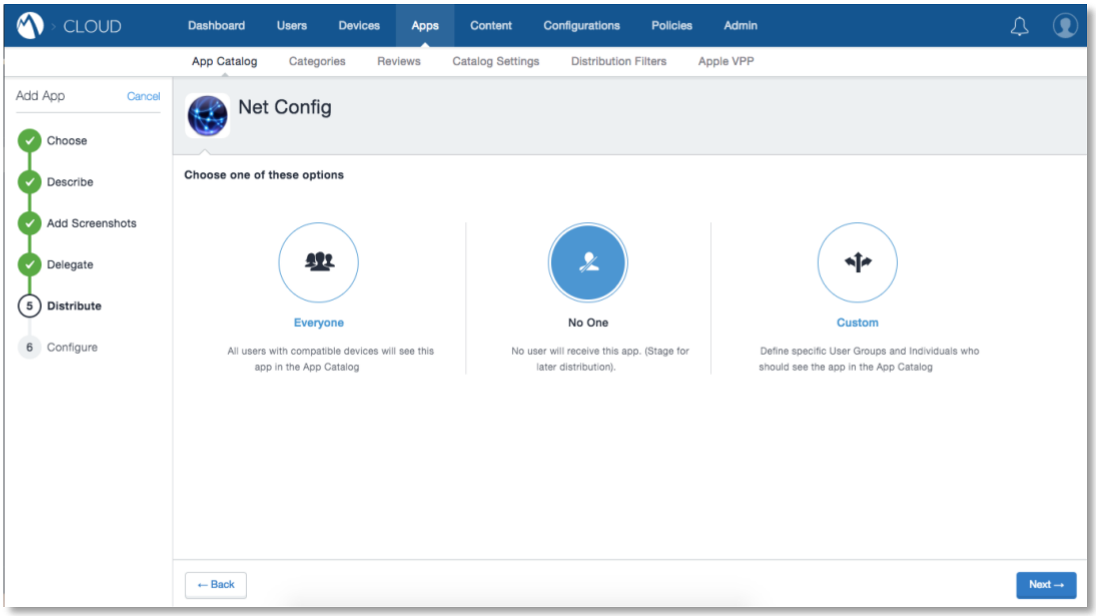


2) Choose ‘In-House’ from drop-down.



3) Drag the apps IPA or APK file to the page and click **Next→**

4) Add the app details such as name and category and click **Next→** until you get to the distribution options.



Choose one of these options

Everyone
All users with compatible devices will see this app in the App Catalog

No One
No user will receive this app. (Stage for later distribution).

Custom
Define specific User Groups and Individuals who should see the app in the App Catalog

5) Choose your distribution method and click **Next→**
6) Click **Done**

Level 2a: User Synchronization

To avoid having to create user credentials and the user management lifecycle, users and their devices can be synchronized through MDM integration. This allows all user and device management functions to be handled at the MDM console.

After the initial User Synchronization during the MDM Integration setup, users are managed through a scheduled synchronization process that runs every four hours. If additional devices are in the device group(s) being used for synchronization, they are added along with their users to zConsole. If devices are removed, then they are also removed from the zConsole. Doing this does not remove their events logged since they have been created.

Ad-hoc MDM Synchronization

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

The zConsole application gets the identification information from zIPS used for the authentication and matches it up with the proper customer for authentication. Once that happens, zConsole retrieves that device and user information from the MDM configured for that customer. zIPS on that device is now authenticated and allowed to proceed. For this to work correctly, zIPS must be deployed as follows:

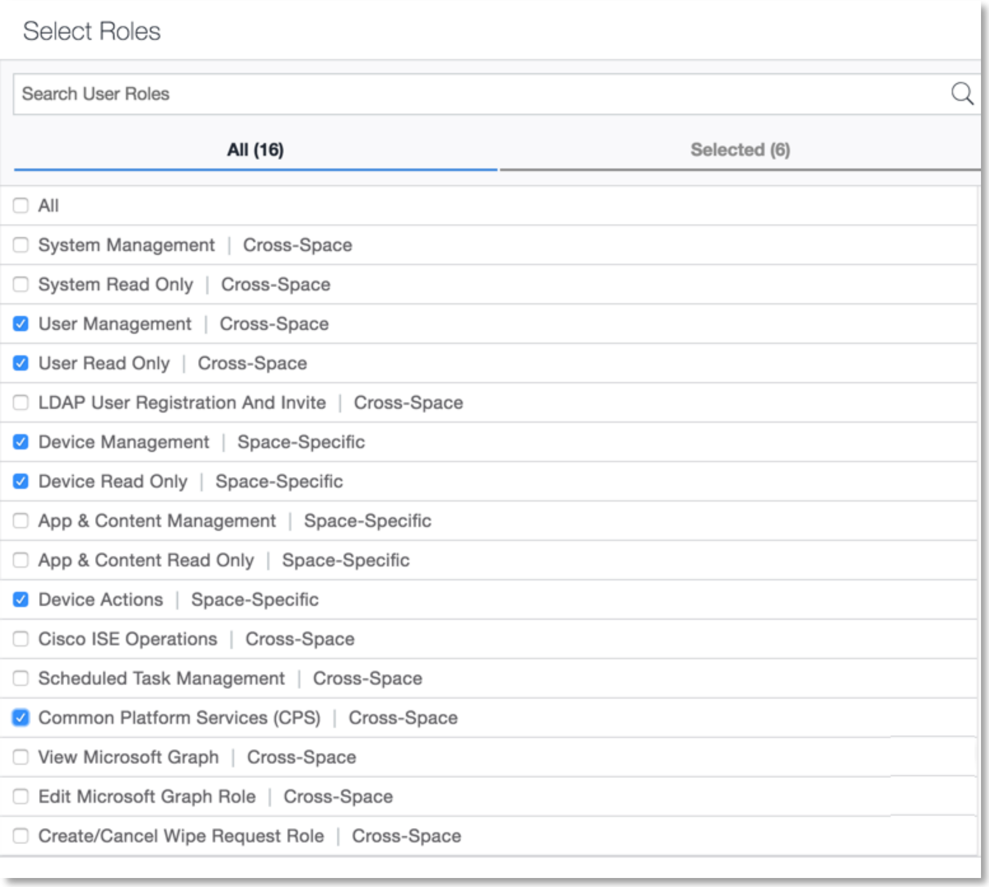
- **iOS**: Associate an App Configuration with the zIPS application that pushes down the fields to be used for the ad-hoc sync. This is described in the section "Level 2b: Auto Sign-in/Advanced Application Deployment" below.
- **Android**: Ad-hoc MDM synchronization for Android required the zIPS application to be modified. Contact your Zimperium Customer Support Team to set this up for Android.

When user synchronization occurs, the zConsole requests certain information from the MobileIron MDM. That information is used to determine if malicious apps are on the device. The information saved for each device includes:

- UUID, Device ID, Apps installed, and email address (if anonymous user functionality is not enabled).
- For zConsole, prior to release 4.13, serial number and IMEI are saved.

Setup User Synchronization

1) Create a MobileIron administrator with the proper API access.
    a) Navigate to: Users/ Users/ +Add/ Single User
    b) Enter the information for this new administrator and click **Done**.
2) Click on the new administrator and select the **Actions** drop-down. Select **Assign Roles**. Add the proper roles to the new administrator and click **Next**, and then click **Done**. For instance, add the following minimum roles:
    - User Management
    - Device Management
    - Device Actions
    - User Read Only
    - Device Read Only
    - Common Platform Services (CPS)



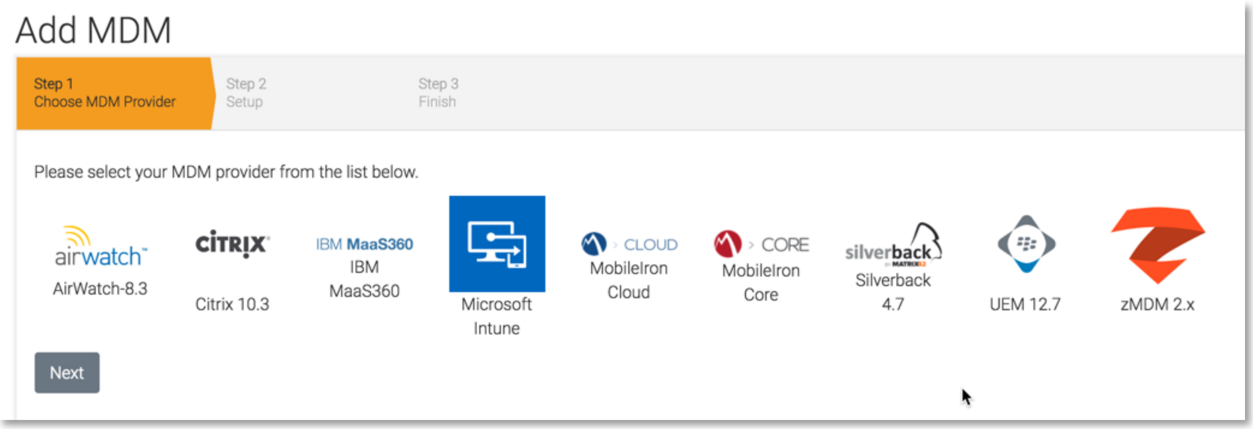
Select Roles

Search User Roles

All (16) | Selected (6)

☐ All
☐ System Management | Cross-Space
☐ System Read Only | Cross-Space
☑ User Management | Cross-Space
☑ User Read Only | Cross-Space
☐ LDAP User Registration And Invite | Cross-Space
☑ Device Management | Space-Specific
☑ Device Read Only | Space-Specific
☐ App & Content Management | Space-Specific
☐ App & Content Read Only | Space-Specific
☑ Device Actions | Space-Specific
☐ Cisco ISE Operations | Cross-Space
☐ Scheduled Task Management | Cross-Space
☑ Common Platform Services (CPS) | Cross-Space
☐ View Microsoft Graph | Cross-Space
☐ Edit Microsoft Graph Role | Cross-Space
☐ Create/Cancel Wipe Request Role | Cross-Space

3) Create one or more device groups that you plan to contain the devices that are protected, if a device group does not exist yet for this purpose. zConsole uses these device group(s) to synchronize devices and their associated users.
4) Log into zConsole and navigate to Manage/ MDM.
5) Click **Add MDM** and select MobileIron Cloud.



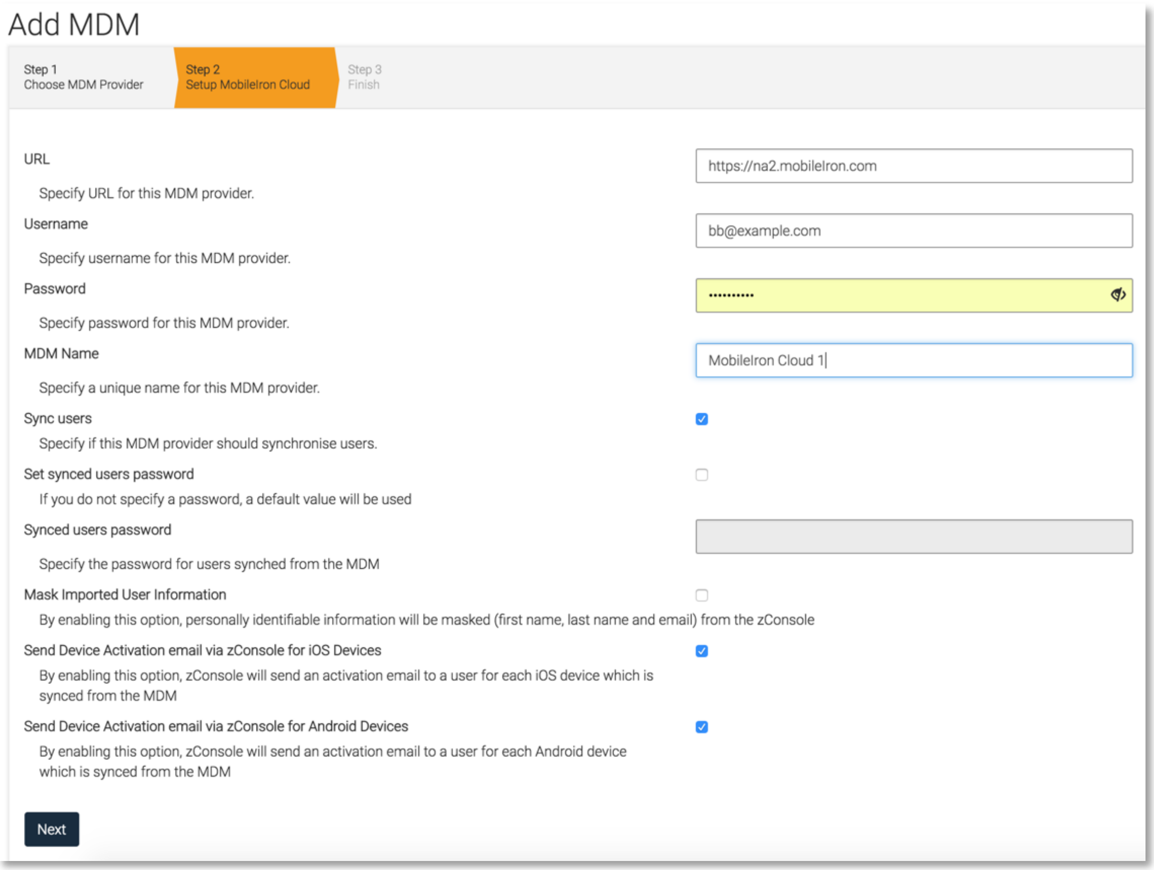
Add MDM

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

Please select your MDM provider from the list below.

6) Enter information pertinent for the MobileIron integration

Item	Specifics
URL	URL of the MobileIron API Server
Username	MobileIron Administrator created with the API role access
Password	Password of the MobileIron Administrator
MDM Name	The name used in zConsole to reference this MDM integration. This is prepended to the group name to form the zConsole group name.
Sync Users	Check this box to ensure users/devices are synchronized with the MobileIron Labels chosen in the next page.
Set synced users password	Check this box to override the default password during user sync. If this is not checked a default password is computed as follows for all users that are synchronized: Start with the Zimperium environment name (this can be supplied by your Customer Success contact), change all uppercase letters to lowercase and also change all spaces to dashes. Then append "1234!" to the end. So, the value '*Zimperium Test*' becomes '*zimperium-test1234!*'
Synced users password	The override value of the password to use for each user when they are synchronized.
Mask Imported Users Information	Check this box to mask personally identifiable information about the user when displayed, for instance name and email address.
Send Device Activation email via zConsole 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	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 MobileIron Cloud

Step 3
Finish

URL: https://na2.mobileIron.com

Specify URL for this MDM provider.

Username: bb@example.com

Specify username for this MDM provider.

Password: ••••••••••

Specify password for this MDM provider.

MDM Name: MobileIron Cloud 1

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 synched 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

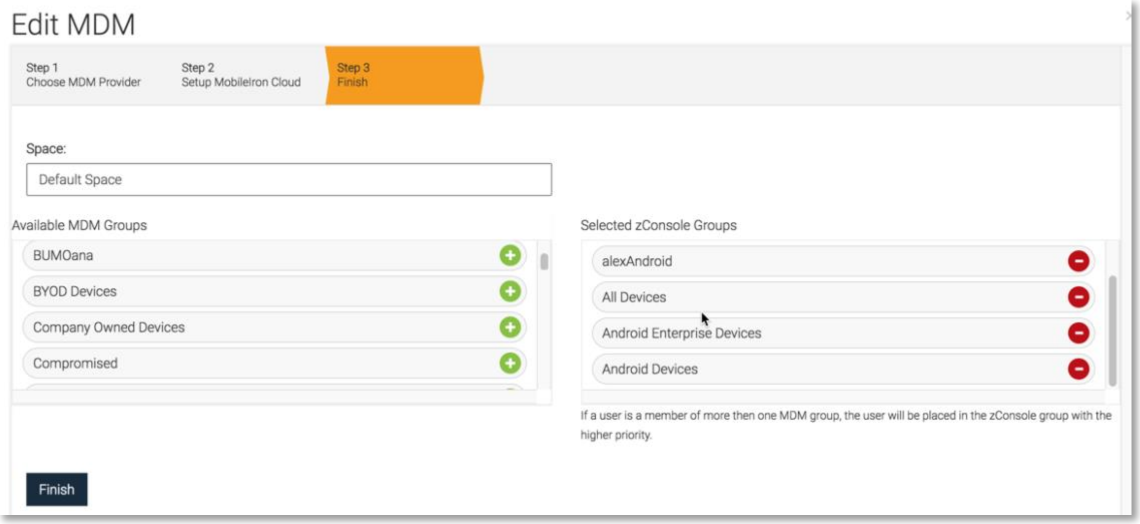
Send Device Activation email via zConsole for iOS Devices ☑

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

7) Click **Next** and choose the MobileIron Space. Then, choose the groups to synchronize, then click **Finish**.



Edit MDM

Step 1
Choose MDM Provider

Step 2
Setup MobileIron Cloud

Step 3
Finish

Space: Default Space

Available MDM Groups

- BUMOana
- BYOD Devices
- Company Owned Devices
- Compromised

Selected zConsole Groups

- alexAndroid
- All Devices
- Android Enterprise Devices
- Android Devices

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

Note: Spaces are used to separate managed entities for the ease of administration, such as an organizational hierarchy. Now users can sync devices for MobileIron spaces, along with the default space.

When more than one device group is chosen, the highest group in the list has the highest priority and so on down the list. If a device is present in more than one group, the group that applies is the highest group for the device.

8) Device/user synchronization now starts.
9) This can be verified by going to the Devices or Users pages in the zConsole to verify they are showing up. The device entries are greyed out until the user starts up zIPS and activates the application.

Level 2b: Auto Sign-in/Advanced Application Deployment

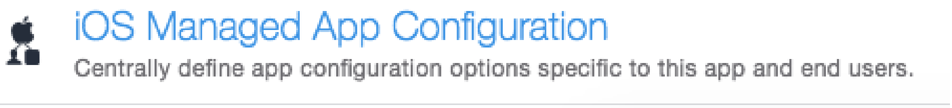
The Zimperium zIPS application for both iOS and Android Enterprise (Android for Work) auto activate the user if MDM user synchronization has been configured. The process is different on each platform as described below.

iOS Activation

Zimperium's iOS zIPS application takes advantage of the Managed Application Configuration when the app is pushed down to the device. This provides the best user experience, allowing the user to startup iOS zIPS without having to enter any credentials. The Managed Application configuration pre-programs iOS zIPS with this information.

This configuration is done within MobileIron:

1) Navigate to: Apps/ App catalog/ and find the iOS zIPS app to be modified.
2) Click on the app, navigate to the App Configurations tab and select iOS Managed App Configuration.



iOS Managed App Configuration

Centrally define app configuration options specific to this app and end users.

3) Click **Add** and enter a name for this configuration.
4) Add the configuration keys.

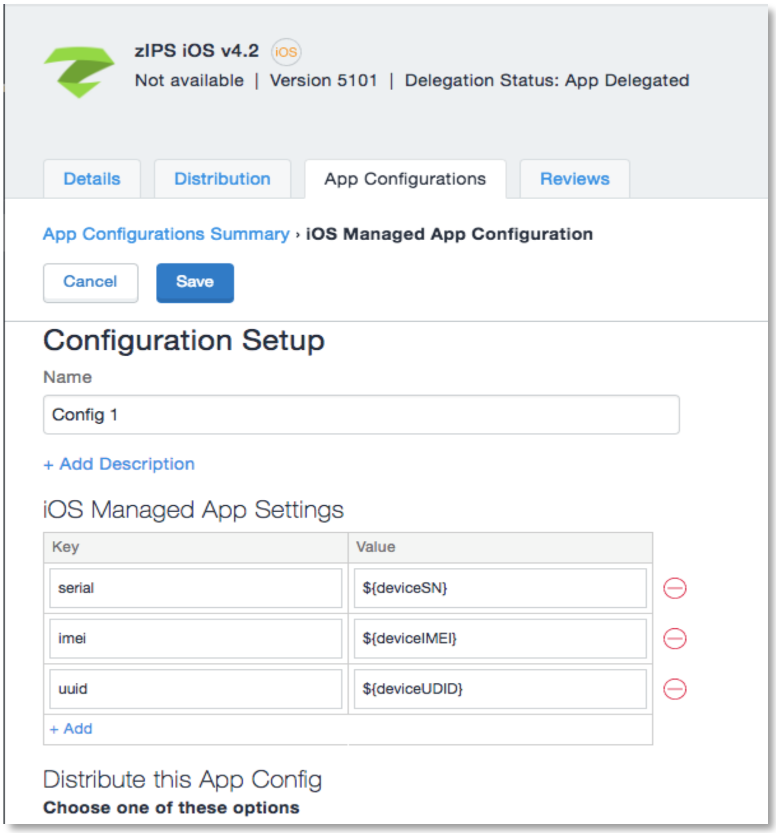
For zIPS Release 4.4.x and earlier the values are described in this table and figure.

Configuration Key	Value Type	Configuration Value
serial (serial is not included in zConsole Release 4.13 or later)	String	${deviceSN}
imei (imei is not included in zConsole Release 4.13 or later)	String	${deviceIMEI}

uuid	String	${deviceUDID}
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team

Note: The configuration keys are case sensitive.

This figure shows the Configuration Setup after adding some of the keys for zIPS Release 4.4.x and earlier.


zIPS iOS v4.2
iOS
Not available | Version 5101 | Delegation Status: App Delegated
Details
Distribution
App Configurations
Reviews
App Configurations Summary › iOS Managed App Configuration
Cancel
Save
+ Add Description
+ Add

Configuration Setup

Name: Config 1

iOS Managed App Settings

Key	Value
serial	${deviceSN}
imei	${deviceIMEI}
uuid	${deviceUDID}

Distribute this App Config

Choose one of these options

For zIPS Release 4.7 and later the values are described in this table.

Configuration Key	Value Type	Configuration Value
uuid	String	${devicePK}
tenantid	String	Contact your Customer Support Team
defaultchannel	String	Contact your Customer Support Team

Note: The configuration keys are case sensitive.

5) Click **Save.**

Each time the iOS zIPS app gets pushed to a device it contains the information specified in the plist file. When the user clicks on the zIPS app, they automatically sign into the proper zConsole environment.

Android Activation

Android Enterprise (Android for Work) users can continue to use the managed app config for activations. You need to make sure that you are passing the right device ID value for the configuration parameter. The variables are the same set as the plist variables in the "iOS Activation" section.

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

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

See the "Zimperium zConsole Configuration Guide" in the section "MDM Activation" 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 zIPS app being pushed to them.

Activation with MobileIron Messaging

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

Level 3: Basic Protection

MobileIron Integration Level three does not apply. Proceed to level four.

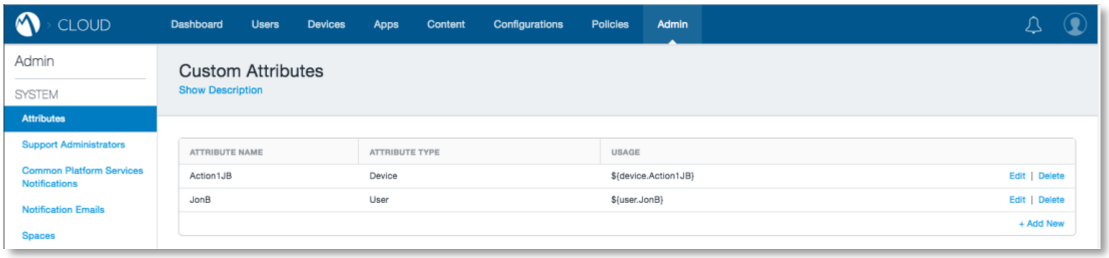
Level 4: Full Protection

The Zimperium integration with MobileIron provides the ability to apply a specific Device Group to the device within the customer's MobileIron environment. This allows the MobileIron administrator to define specific actions such as to quarantine a device, remove email access, assign a configuration or even unenroll a device (which happens automatically). To accomplish this, the MobileIron administrator needs to coordinate with the zConsole administrator the specific actions that are needed and do the following configuration for each one with a unique Device Group. MDM Integration with zConsole also has to be setup and functional.

The MobileIron Cloud integration contains one built in MDM action to Lock the device. The following steps are not needed for that action to be used.

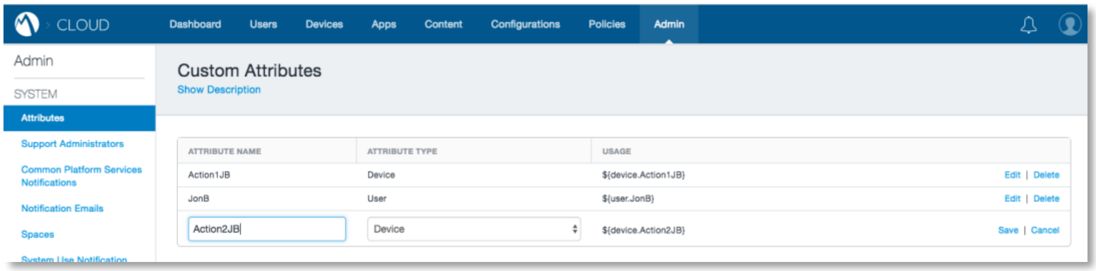
When a device is under attack and the MDM action is set to some Device Group from the integrated MobileIron server, zConsole assigns the device to that device group via API calls. To set this up several configurations need to be done on the MobileIron Console:

1. Log into the MobileIron Console.
2. Navigate to the Admin page.
3. Create a customer Device Attribute to be used to link the Device to the Device Group and Policy.
4. Click **+ Add New**.



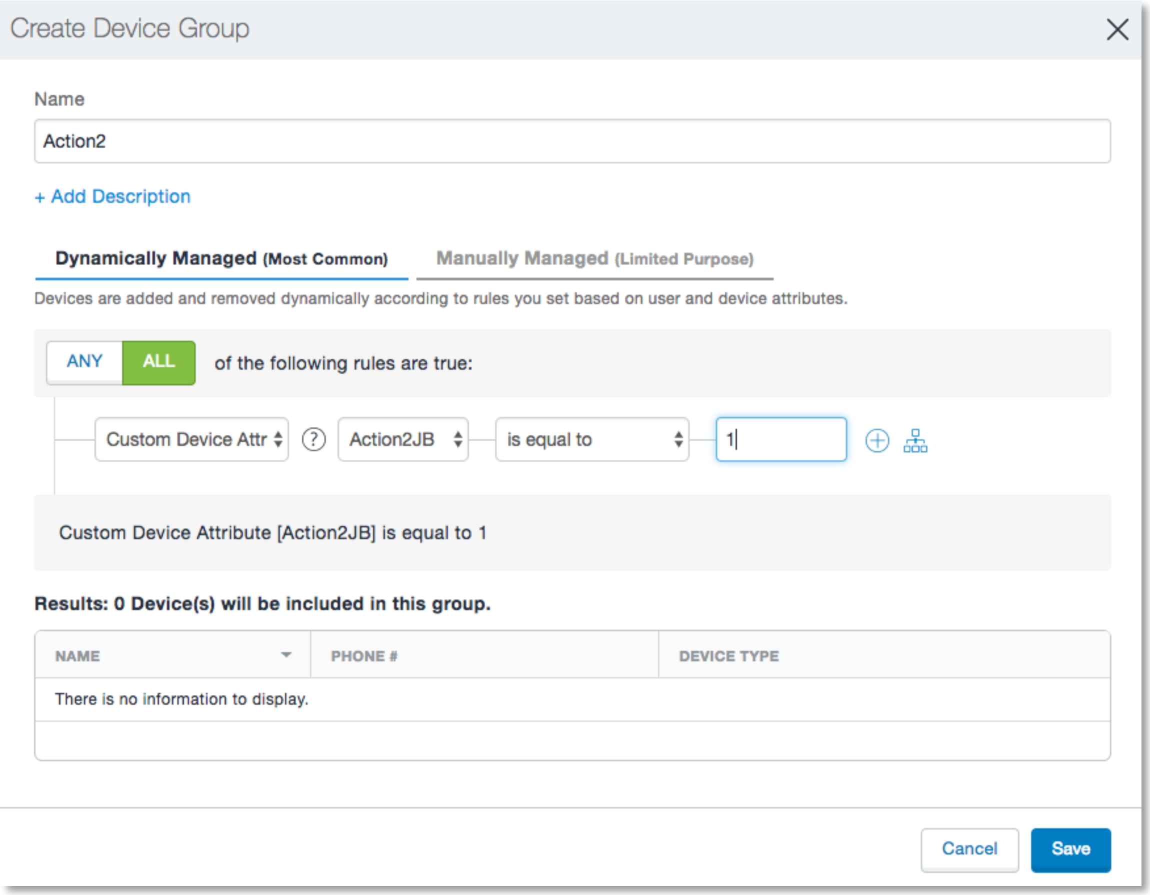
ATTRIBUTE NAME	ATTRIBUTE TYPE	USAGE	
Action1JB	Device	${device.Action1JB}	Edit | Delete
JonB	User	${user.JonB}	Edit | Delete
			+ Add New

5. Type the name of the new custom attribute and choose type **Device**. In the sample below the name is ‘Action2JB’. Click **Save**.



ATTRIBUTE NAME	ATTRIBUTE TYPE	USAGE	
Action1JB	Device	${device.Action1JB}	Edit | Delete
JonB	User	${user.JonB}	Edit | Delete
Action2JB	Device	${device.Action2JB}	Save | Cancel

6. Create a dynamically managed Device Group based on the new Custom Device Attribute just created. navigate to Devices/ Device Groups. Click **+Add**.
7. Enter the new Device Group Name. (This is the name that shows up in the TRM MDM actions column). Choose ‘Custom Device Attribute’ and then the new Custom Attribute just created with a value of ‘1’. Click **Save**.



Create Device Group

Name: Action2

+ Add Description

Dynamically Managed (Most Common) | Manually Managed (Limited Purpose)

Devices are added and removed dynamically according to rules you set based on user and device attributes.

ANY | ALL of the following rules are true:

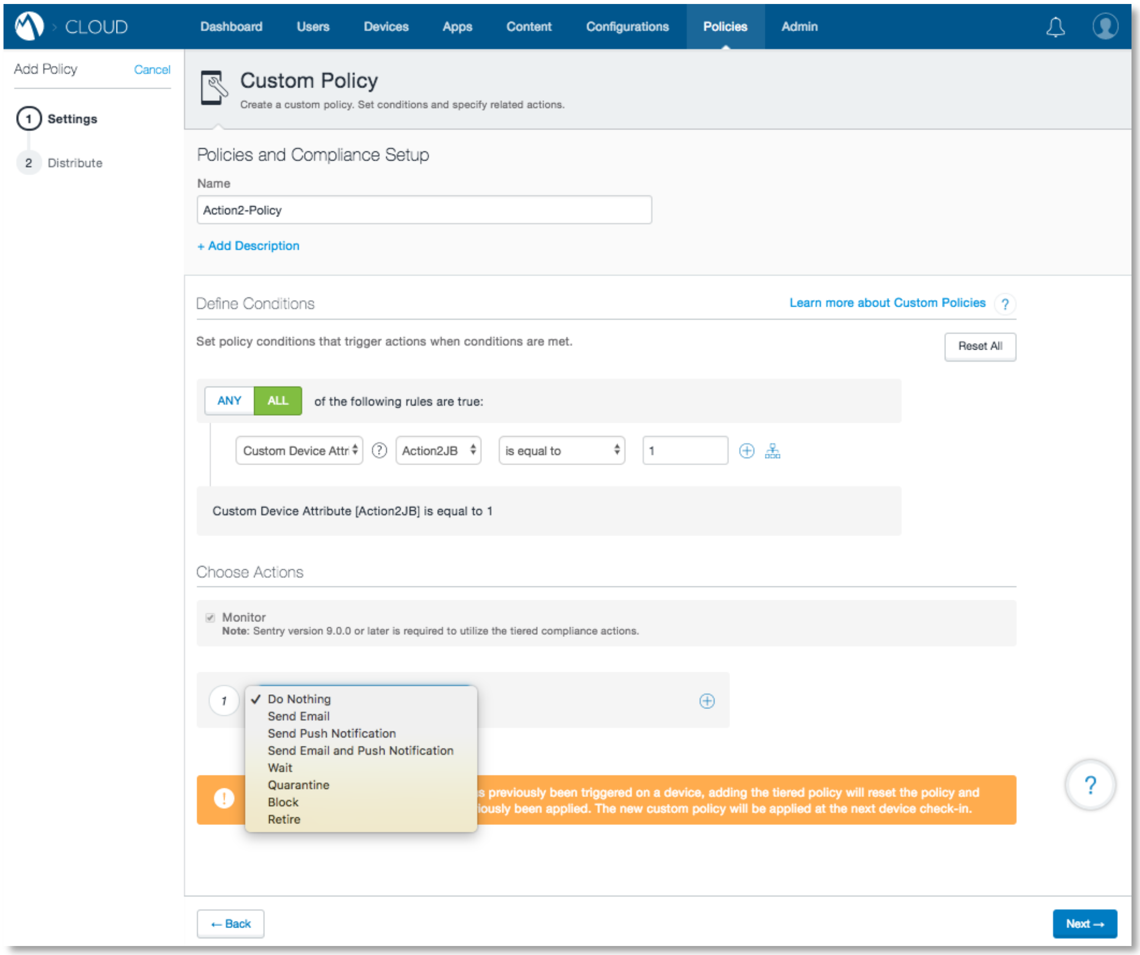
Custom Device Attr | Action2JB | is equal to | 1

Custom Device Attribute [Action2JB] is equal to 1

Results: 0 Device(s) will be included in this group.

NAME	PHONE #	DEVICE TYPE
There is no information to display.		

8. Create an Policy that is linked to the new Device Group just created that you plan to contain the action to carry out to protect the phone. Navigate to Policies and click **+Add**.
9. Choose a Custom Policy. Enter the Custom Policy name and choose the conditions, Any or All. This “Any” or “All” option does not matter as there is only one condition. Choose ‘Custom Device Attribute’, the new Custom Attribute name and the value entered previously, ‘1’. Then choose the actions to be executed as shown below. Click **Next**.



Custom Policy

Create a custom policy. Set conditions and specify related actions.

Policies and Compliance Setup

Name: Action2-Policy

+ Add Description

Define Conditions

Set policy conditions that trigger actions when conditions are met.

ANY | ALL of the following rules are true:

Custom Device Attr | Action2JB | is equal to | 1

Custom Device Attribute [Action2JB] is equal to 1

Choose Actions

☑ Monitor
Note: Sentry version 9.0.0 or later is required to utilize the tiered compliance actions.

1 ✓ Do Nothing

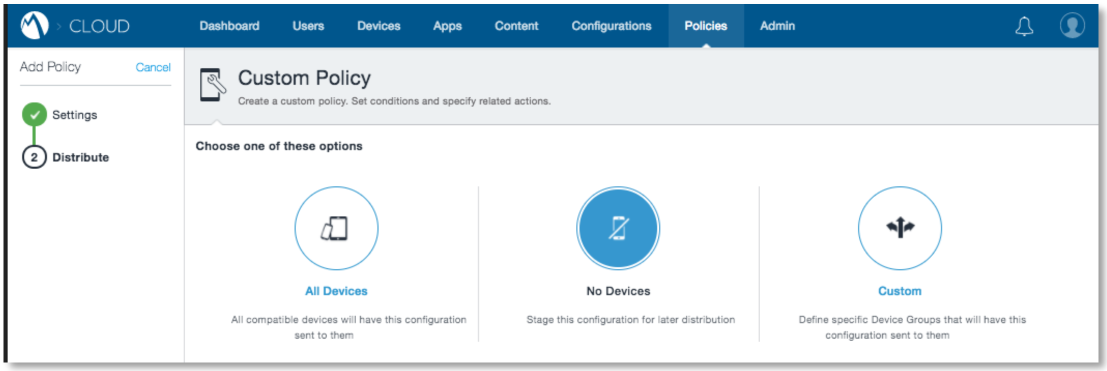
s previously been triggered on a device, adding the tiered policy will reset the policy and iously been applied. The new custom policy will be applied at the next device check-in.

The possible actions are:

- Send Email
- Send Push Notification
- Send Email and Push Notification
- Wait
- Quarantine
- Block
- Retire

For each option selected, an appropriate entry is displayed to enter more information, such as the text to be sent to the user if ‘Send Push Notification’ is chosen. More than one action can be chosen by clicking on the plus-sign (‘+’) sign to add another action.

10. On the Distribution page, assign this policy to ‘No Devices’ and then click **Done**.



Custom Policy

Create a custom policy. Set conditions and specify related actions.

Choose one of these options

All compatible devices will have this configuration sent to them

Stage this configuration for later distribution

Define specific Device Groups that will have this configuration sent to them

11. Log into zConsole and perform an MDM sync to learn the new Device Groups. Navigate to Manage/ MDM. Click on **Sync Now** and then **OK** for the MDM integration just modified.
12. The MDM actions column should now include any new Device Groups created.

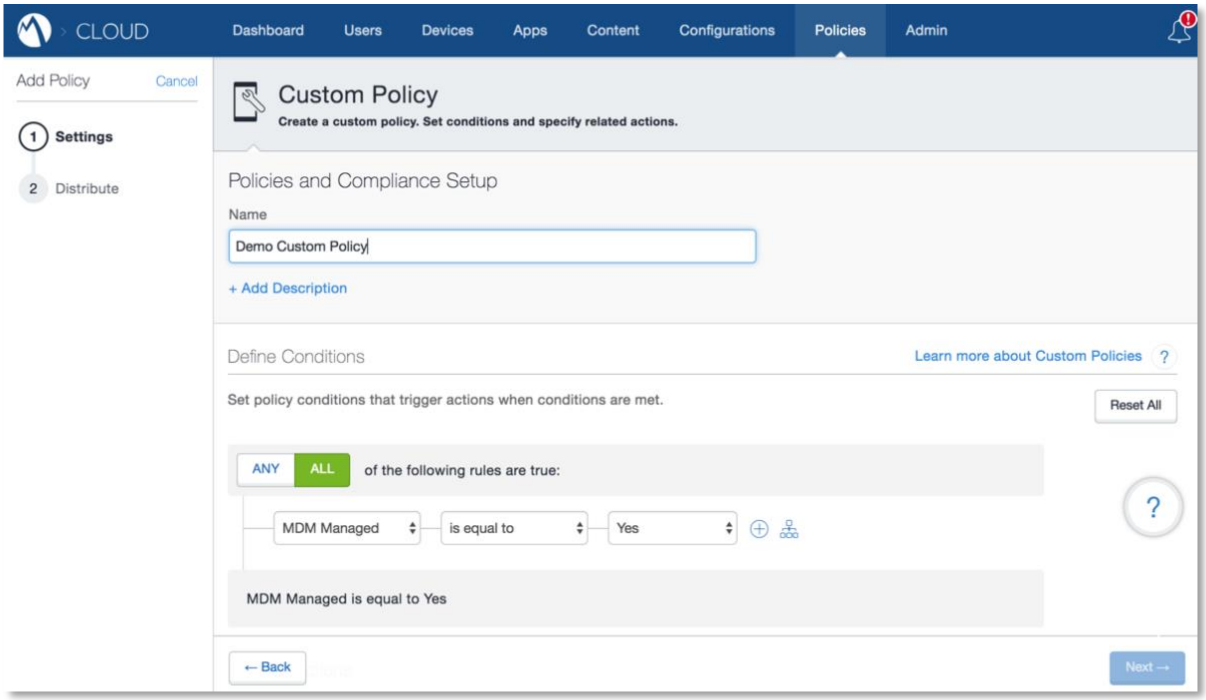
Actions assigned in the Threat Response Policy/Matrix happen automatically when the specific assigned threat is detected.

Appendix A - MobileIron Messaging and Device Activation

MobileIron Cloud 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.

Perform the following steps to set up an email after the user's device is enrolled.

1. Login to MobileIron Cloud at the following website: `https://na2.mobileIron.com`
2. Click **Policies** from the top menu.
3. Click **+Add** to add a new policy.
4. Select **Custom Policy**.
5. Give a name to your new policy and select the policy condition that the rule of 'MDM Managed' is set to 'Yes' and your policy looks like the figure below.



Custom Policy

Create a custom policy. Set conditions and specify related actions.

Policies and Compliance Setup

Name: Demo Custom Policy

Define Conditions

Set policy conditions that trigger actions when conditions are met.

ALL of the following rules are true:

MDM Managed | is equal to | Yes

MDM Managed is equal to Yes

6. Scroll down and click the **Send Email** action.

7. Provide the required email subject and the body text. Here's an example of the email text snippet with an HTML link for the activation link.

```
After you have installed the zIPS app, click the link below to activate
zIPS.
Activation Link:
<a href="https://activation.zimperium.com/activation?token=U2FsdGVkX183
.
.
.
bMGBnrSpI-kEIuvSE6olwZQREymFRi9h1VRMlFos&MDM_ID=${devicePK}">Click here
to activate zIPS</a>
```

Note: The activation URL has the MDM identifier of ${devicePK} added to the end of the URL and is in bold above.

8. Click the checkbox in the confirmation box.
9. Click **Next**.
10. Choose the option of which devices receive the email:
    - All Devices
    - No Devices
    - Custom
11. Click **Done**.

This table provides the specific device identifier needed for the MDM_ID field.

MDM System	MDM Device Identifier Variable
MobileIron Core	Core: $DEVICE_UUID$
MobileIron Cloud	Cloud: ${devicePK}

MobileIron supports messaging where you can tailor the MDM invitation email to a new user. This is changing the default email that the MDM sends. This details the steps to configure a message template to change the text for the MDM invitation email.

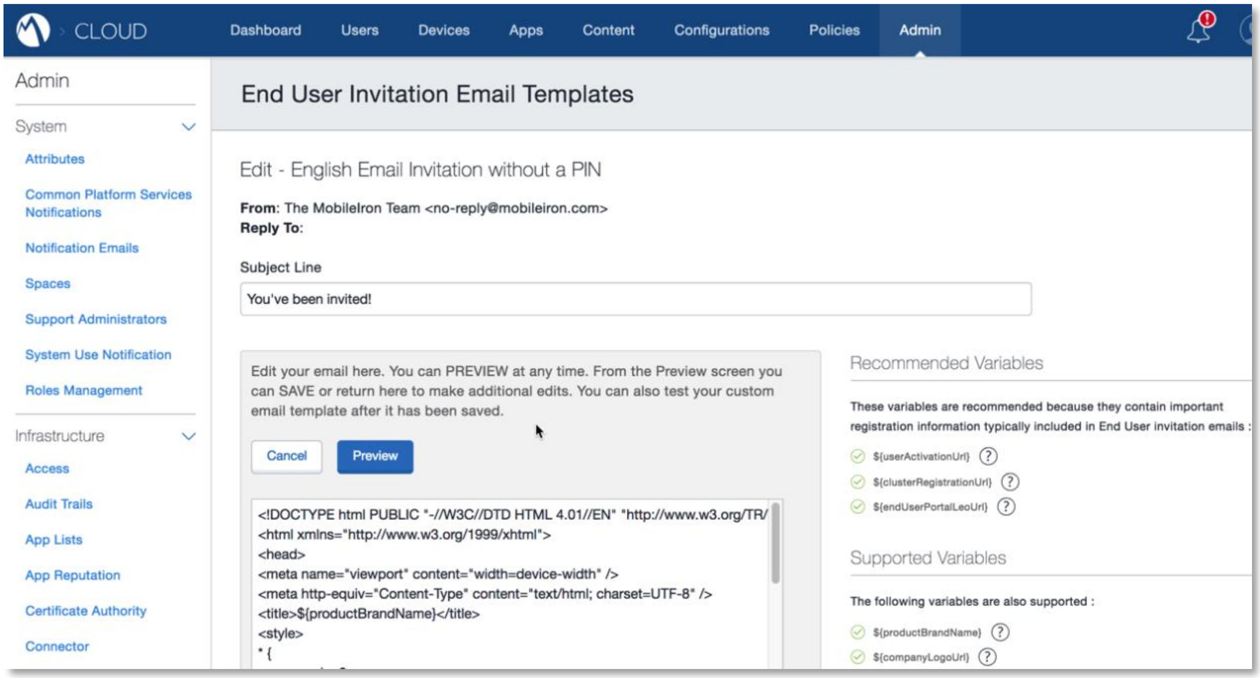
Perform the following steps to set up specific text for the invitation email to a new user.

1. Login to MobileIron Cloud at this website: https://na2.mobileIron.com
2. Click **Admin** from the top menu.
3. Click **Email Templates.**
4. Select **End User Invitation**.
5. Select the desired language/localization and edit the template text.
6. Provide the email subject text and body.

7. Click **Preview** and **Save** when complete.

   Note: This template does not have any device specific information.

This figure shows the editing of this template.



End User Invitation Email Templates

Edit - English Email Invitation without a PIN

From: The MobileIron Team <no-reply@mobileiron.com>
Reply To:

Subject Line

You've been invited!

Edit your email here. You can PREVIEW at any time. From the Preview screen you can SAVE or return here to make additional edits. You can also test your custom email template after it has been saved.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>${productBrandName}</title>
<style>
* {
```

Recommended Variables

These variables are recommended because they contain important registration information typically included in End User invitation emails :

- ✓ ${userActivationUrl} ?
- ✓ ${clusterRegistrationUrl} ?
- ✓ ${endUserPortalLeoUrl} ?

Supported Variables

The following variables are also supported :

- ✓ ${productBrandName} ?
- ✓ ${companyLogoUrl} ?