MobileIron Threat Defense Solution Guide for Core 10.6.0.0

Mobile@Work 10.6.0.0 for Android
Mobile@Work 12.2.0 for iOS

Revised: March 19, 2020

For complete product documentation see: MobileIron Core Product Documentation
## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 18, 2020</td>
<td>References to Zimperium website and documentation were removed.</td>
</tr>
<tr>
<td>March 19, 2020</td>
<td>zConsole configuration task &quot;Whitelisting a sideloaded app for Android devices&quot; was added to &quot;Using zConsole to monitor threats to Android devices&quot; in the section &quot;Using Zimperium management console (zConsole).&quot;</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision history</td>
<td>3</td>
</tr>
<tr>
<td>Contents</td>
<td>4</td>
</tr>
<tr>
<td>MTD features and enhancements in this release</td>
<td>8</td>
</tr>
<tr>
<td>VPN Sinkhole for iOS clients without user action</td>
<td>8</td>
</tr>
<tr>
<td>Longer default MTD wake-up interval</td>
<td>8</td>
</tr>
<tr>
<td>GDPR-enabled users have view and edit restrictions</td>
<td>9</td>
</tr>
<tr>
<td>MTD Local Actions threat names updated</td>
<td>9</td>
</tr>
<tr>
<td>App status on managed devices</td>
<td>9</td>
</tr>
<tr>
<td>Additional MTD Client features and updates</td>
<td>9</td>
</tr>
<tr>
<td>Android support for whitelisting a sideloaded App</td>
<td>9</td>
</tr>
<tr>
<td>Core to Cloud Mobile@Work migrations require user action</td>
<td>10</td>
</tr>
<tr>
<td>About MobileIron Threat Defense Solution</td>
<td>11</td>
</tr>
<tr>
<td>MobileIron Threat Defense Overview</td>
<td>11</td>
</tr>
<tr>
<td>Managing MTD via zConsole or Local Actions</td>
<td>13</td>
</tr>
<tr>
<td>MTD license determines functionality</td>
<td>14</td>
</tr>
<tr>
<td>MobileIron Threat Defense prerequisites</td>
<td>15</td>
</tr>
<tr>
<td>Configuring Privacy Policy</td>
<td>16</td>
</tr>
<tr>
<td>Creating an MTD admin</td>
<td>16</td>
</tr>
<tr>
<td>Adding MTD roles to the Core admin user</td>
<td>17</td>
</tr>
<tr>
<td>Enabling CPS messaging on MobileIron Core</td>
<td>18</td>
</tr>
<tr>
<td>Assigning an administrator to a space</td>
<td>20</td>
</tr>
<tr>
<td>Adding Core as your MDM server in zConsole</td>
<td>20</td>
</tr>
<tr>
<td>Allowing access to the App Gateway</td>
<td>21</td>
</tr>
<tr>
<td>External and Internet rules</td>
<td>22</td>
</tr>
<tr>
<td>Additional Firewall Rules</td>
<td>23</td>
</tr>
<tr>
<td>Enabling MobileIron Threat Defense for Mobile@Work devices</td>
<td>25</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>25</td>
</tr>
<tr>
<td>Creating an MTD activation configuration</td>
<td>26</td>
</tr>
<tr>
<td>Pushing new MTD activation configurations to existing devices</td>
<td>27</td>
</tr>
<tr>
<td>Android</td>
<td>27</td>
</tr>
<tr>
<td>iOS</td>
<td>27</td>
</tr>
<tr>
<td>Verify that MobileIron Threat Defense is working</td>
<td>27</td>
</tr>
<tr>
<td>Verify that MTD is working on a Device</td>
<td>27</td>
</tr>
<tr>
<td>Verify MTD on all devices</td>
<td>28</td>
</tr>
<tr>
<td>Defining Policies</td>
<td>29</td>
</tr>
<tr>
<td>Defining app control rules in Core</td>
<td>29</td>
</tr>
<tr>
<td>Defining an MTD security policy in Core</td>
<td>30</td>
</tr>
<tr>
<td>Creating event notifications in Core</td>
<td>31</td>
</tr>
<tr>
<td>Server-initiated mitigation and multi-tier compliance</td>
<td>34</td>
</tr>
<tr>
<td>Creating MTD labels in Core for Android and iOS devices</td>
<td>34</td>
</tr>
<tr>
<td>Creating and applying server-initiated multi-tier compliance actions</td>
<td>35</td>
</tr>
<tr>
<td>Quarantine Compliance Action</td>
<td>36</td>
</tr>
<tr>
<td>Tiered Compliance Action - 23 hours</td>
<td>36</td>
</tr>
<tr>
<td>Tiered Compliance Action - 4 hours</td>
<td>37</td>
</tr>
<tr>
<td>Configuring the zConsole Mobile Threat Response Policy</td>
<td>38</td>
</tr>
<tr>
<td>Enable</td>
<td>39</td>
</tr>
<tr>
<td>Severity</td>
<td>39</td>
</tr>
<tr>
<td>Threat</td>
<td>39</td>
</tr>
<tr>
<td>Set User Alerts</td>
<td>39</td>
</tr>
<tr>
<td>Set Device Action</td>
<td>40</td>
</tr>
<tr>
<td>MDM Action</td>
<td>40</td>
</tr>
<tr>
<td>Mitigation Action</td>
<td>41</td>
</tr>
<tr>
<td>Notifications</td>
<td>41</td>
</tr>
<tr>
<td>Updating Core Sync Policy</td>
<td>42</td>
</tr>
<tr>
<td>Configuring device scanning frequency for threat scan</td>
<td>42</td>
</tr>
<tr>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Mitigation and compliance using Local Actions</strong></td>
<td>44</td>
</tr>
<tr>
<td>Creating MTD Local Actions threat defense policy in Core</td>
<td>44</td>
</tr>
<tr>
<td>Creating compliance policy rules and groups</td>
<td>45</td>
</tr>
<tr>
<td>Threat types</td>
<td>45</td>
</tr>
<tr>
<td>Creating compliance policy rules</td>
<td>46</td>
</tr>
<tr>
<td>Creating compliance policy groups</td>
<td>47</td>
</tr>
<tr>
<td>Example: Creating an Out of Compliance Local Actions policy</td>
<td>48</td>
</tr>
<tr>
<td>Configuring the iOS sinkhole VPN local action</td>
<td>48</td>
</tr>
<tr>
<td>Threat category names and related threats</td>
<td>49</td>
</tr>
<tr>
<td>Network, device, and app threats available in Local Actions</td>
<td>50</td>
</tr>
<tr>
<td>Local Actions Network threats</td>
<td>50</td>
</tr>
<tr>
<td>Local Actions Device threats</td>
<td>52</td>
</tr>
<tr>
<td>Local Actions App threats</td>
<td>54</td>
</tr>
<tr>
<td>Editing an MTD Local Actions threat defense policy</td>
<td>54</td>
</tr>
<tr>
<td>Checking MobileIron Threat Defense status</td>
<td>55</td>
</tr>
<tr>
<td>Checking individual devices</td>
<td>55</td>
</tr>
<tr>
<td>Using Advanced Search</td>
<td>57</td>
</tr>
<tr>
<td><strong>Configuring Phishing Protection in Core</strong></td>
<td>58</td>
</tr>
<tr>
<td>Using a remote database to validate URLs</td>
<td>58</td>
</tr>
<tr>
<td>Anti-Phishing for iOS devices</td>
<td>59</td>
</tr>
<tr>
<td>How MobileIron Phishing Protection for iOS works</td>
<td>59</td>
</tr>
<tr>
<td>Enabling Phishing Protection in MobileIron Core</td>
<td>59</td>
</tr>
<tr>
<td>Anti-Phishing for Android and Android Enterprise devices</td>
<td>60</td>
</tr>
<tr>
<td>How MobileIron Phishing Protection for Android works</td>
<td>61</td>
</tr>
<tr>
<td>Phishing Protection Status</td>
<td>63</td>
</tr>
<tr>
<td>Device Details page</td>
<td>63</td>
</tr>
<tr>
<td>Using the Phishing Protection Dashboard to monitor enrollment</td>
<td>63</td>
</tr>
<tr>
<td>Updating the MTD Local Actions policy when new threat list is available</td>
<td>64</td>
</tr>
<tr>
<td><strong>Managing user privacy</strong></td>
<td>66</td>
</tr>
</tbody>
</table>
Managing EU users under GDPR .................................................................66
Enabling the GDPR Profile .........................................................................66
Assigning users to a GDPR profile ...............................................................67

Using Zimperium management console (zConsole) ........................................69
Configuring zConsole ..................................................................................69
General Settings .........................................................................................69
Managing Devices in zConsole ...................................................................71
General Display Filters ...............................................................................72
Using zConsole to monitor threats to Android devices ..................................73
Whitelisting a sideloaded app for Android devices .......................................74
Whitelisting an app prior to installation ......................................................74
Whitelisting an app after installation .........................................................74
Using zConsole to monitor threats to iOS devices .......................................75
Setting the Sinkhole action on iOS devices .................................................75

Administering Mobile@Work .......................................................................76
Logging and enhanced logging for iOS clients .............................................76
Sending Mobile@Work logs to MobileIron Support .....................................76
MTD Support for Android 10 .........................................................................77
MTD features and enhancements in this release

Each version of the MobileIron Threat Defense Solution guide contains all MTD features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, MobileIron releases new versions of the MTD guide as the features become fully available.

The following features and enhancements have been made to the MobileIron Threat Defense Solution in this release.

VPN Sinkhole for iOS clients without user action

Configure iOS sinkhole VPN protection without client user action. MTD admins can now configure sinkhole protection for iOS clients that will push an MTD virtual private network (VPN) to the client without user action. After upgrade to Core 10.6.0.0, a new default MTD VPN configuration is created and pushed silently to the device when a threat configured for Sinkhole action is discovered. The process works like this:

1. When a threat is detected on an iOS device, and a Network Sinkhole action is associated with this threat in the Local Actions configuration, the threat triggers the MobileIron Threat Defense VPN profile to isolate the device from the network, without user assistance.
2. While the Network Sinkhole action is active on the device, be aware of the following issues:
   - Attempts to reach Internet or other network destinations will fail.
   - Other threats may not be detected and displayed until the original threat (that caused the compliance action) is remediated.
   - The full list of threats may not display on the iOS device.
3. After the threat is remediated on the device, the VPN profile is disabled automatically, and network traffic is no longer affected by the sinkhole. At this point, browser traffic now succeeds.

For more information, see Configuring the iOS sinkhole VPN local action.

Longer default MTD wake-up interval

Previously, the MTD wake-up interval default was 15 minutes, which sometimes resulted in excessive battery usage for iOS clients. From Core version 10.6.0.0 through the most recently released version as supported by MobileIron, the MTD default wake-up interval is 60 minutes, which can be adjusted for your network.

For more information, see Enabling MobileIron Threat Defense for Mobile@Work devices.
GDPR-enabled users have view and edit restrictions

**Edit restrictions for GDPR-enabled users.** When the GDPR profile is enabled for a user, some functionality and edit rights in the Core Devices and Users pages are restricted. After upgrade to Core 10.6.0.0, GDPR-enabled users will see a banner across the top of the Admin portal, reminding them that these restrictions are in place.

For more information, see [Assigning users to a GDPR profile](#).

MTD Local Actions threat names updated

**Changes to the MTD Core Local Actions threat categories.** MobileIron Core previously used the threat category names Host threats, Malware threats, and Network threats for MTD Local Actions Policies. After upgrade to Core 10.6.0.0, the Core threat category names match those of the Mobile@Work client:

- Host threats changed to Device threats
- Malware threats changed to App threats
- Network threats (no change)

For more information, see [Creating compliance policy rules and groups](#).

App status on managed devices

**zConsole correctly lists the category type and management status of apps installed on managed devices.** MTD can evaluate Apps installed on a device by whatever means, and correctly categorize them. Previously, App management information was not reported to zConsole, so some apps were being incorrectly flagged. After upgrade to 10.6.0.0, the MobileIron API reports the status to zConsole.

For more information, see [How zConsole classifies installed Apps](#).

Additional MTD Client features and updates

The following features and updates affect MTD Mobile@Work clients.

**Android support for whitelisting a sideloaded App**

From Mobile@Work 10.6 and Core 10.6.0.0 through the most recently released version as supported by MobileIron, you can now whitelist a sideloaded app before or after it is installed on a device:

For more information, see [Whitelisting a sideloaded app for Android devices](#)
Core to Cloud Mobile@Work migrations require user action

When Android Mobile@Work clients migrate from Core to Cloud server, the user is prompted to re-enable MTD anti-phishing protection by setting the Mobile@Work client as the default browser from the Go interface, even if it has been configured previously.
About MobileIron Threat Defense Solution

Applicable to:

- Mobile@Work for Android client versions as supported by MobileIron Core.
- Mobile@Work for iOS client versions as supported by MobileIron Core.

MobileIron Core includes the ability to distribute activation tokens to enable MobileIron Threat Defense (MTD) technology integrated into Mobile@Work for Android and iOS clients. MobileIron Threat Defense protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications.

MobileIron Threat Defense monitors:

- **On the device level**: system parameters, configuration, firmware, and libraries to identify suspicious or malicious activity.
- **On the network level**: network traffic and suspicious connections to and from mobile devices.
- **On the app level**: leaky apps (potentially placing enterprise data at risk) and risky apps, through risk assessment and code analysis.

When this configuration is enabled in MobileIron Core and applied to the devices, the MTD libraries are enabled on the Mobile@Work clients. The MobileIron Threat Defense service can be deactivated on a device by excluding (undistributing) the MobileIron Threat Defense configuration from the device.

NOTE: MTD does not support macOS and Windows devices.

MobileIron Threat Defense Overview

The MobileIron Threat Defense Solution (MTD) consists of three components, as illustrated in the following figure.

- Mobile Device Management (MDM) server (MobileIron Core)
- MobileIron client application (Mobile@Work for iOS and Android)
- Management console (Zimperium management console (zConsole))
The Mobile Device Management (MDM) administrator is able to configure MobileIron Core to automatically install the required version of MobileIron client application, Mobile@Work for Android and iOS, deploy and enable an MTD Activation token on selected devices, and configure the components to interoperate to protect devices from mobile threats.

After an initial on-boarding, the list of workflows required to configure the MobileIron Threat Defense Solution are:

1. MobileIron Core provides an MTD Activation token to Mobile@Work clients on selected devices.
2. The threat defense functionality is enabled on selected devices.
3. The zConsole authenticates and establishes communication with MobileIron Core and synchronizes device parameters.
4. The administrator defines threat defense policies on the zConsole.
5. The administrator defines MTD local actions policies on Core.
6. MTD-enabled Mobile@Work clients check-in and begin communicating with zConsole and with Core.
7. MTD-enabled Mobile@Work clients periodically scan the device for threats and actions are taken in accordance with defined server-initiated and local action policies.
Managing MTD via zConsole or Local Actions

There are two ways to implement compliance actions using MobileIron Threat Defense. It is best practice to have one method, but you can use both methods.

- **Method 1**: Mitigation and multi-tier compliance using the Zimperium management console (zConsole) – The server-enforced method requires connection to MobileIron Core, and the policy can be set up for both server and mobile devices. For more information, see Server-initiated mitigation and multi-tier compliance.

- **Method 2**: Mitigation and compliance using Core Local Actions policy – Device-enforced local action compliance can be implemented using the MTD Local Actions policy. For more information, see Mitigation and compliance using Local Actions.

**NOTE**: In the event both server-initiated and local action policies are defined for the same threat, local MTD policy will take precedence and be executed immediately.

It is best practice to have both Local Actions configured in MobileIron Core, and a Threat Response Matrix (TRM) policy configured in zConsole, for a multi-layered, automated threat response to threats detected on mobile devices.

**Figure 2: MTD Solution**

- If mitigation is implemented using Local Actions, the threat is remediated based on the Local Actions configuration and does not need connection to Core or zConsole.

- If the device is connected to Core and zConsole (server-initiated), any threats detected on the device
informs the zConsole of threat status. zConsole instructs Core that a policy violation has been triggered. Core moves the compromised device to the appropriate label.

- When the threat is remediated on the device, the client passes this state change to the zConsole. The zConsole tells Core that the policy violation has been removed and to move the device back to the normal device group. Core will then restore the device back to normal operations.

**MTD license determines functionality**

MobileIron Threat Defense Solution has two types of licenses, which determine which features are enabled, and which are not. If you have an MTD+ license, all MobileIron MTD functionality is enabled, including advanced app analytics. Users with a standard MTD license will occasionally see an option that is greyed out, or is otherwise not accessible. If you find that you need MTD+ functionality, contact your MobileIron representative.
MobileIron Threat Defense prerequisites

Before you set up MobileIron Threat Defense, complete the following prerequisites:

1. Install MobileIron Core.
   See the “Core Installation” section in the On-Premise Installation Guide for information about how to install MobileIron Core.

2. Purchase an MTD license from MobileIron or a licensed partner. Zimperium licenses, for example, are not valid.

3. Complete the following prerequisites:
   See the MobileIron On-Premise Installation Guide for more information on required ports and firewall rules.
   - Port 443 in the firewall should be open
   - Allow access to the AppGateway URL
   - Allow access to the Voice network service (VNS) URL
   - Allow access to Apple Push Notification Service (APNS), and Firebase Cloud Messaging (FCM)
   - Obtain an MTD activation token
   - Have the fully-qualified domain name (FQDN) of the Core UEM server
   - Allow access to the App_Config_Spec_File repository URL
   - Allow incoming API calls and modify the ACL configuration for the specific source IPs


5. Obtain a Zimperium management console (zConsole) tenant. For both iOS and Android MTD implementations, contact your MobileIron representative to request your unique, encrypted MTD Activation token, or get it from the zConsole.

6. Request and upload a MDM certificate for iOS, if you have not already done so. In addition, you need to enable iOS MDM support and confirm MDM for an iOS device. For information, see the "Managing Mobile Device Management (MDM) certificates for iOS and macOS" section of the Getting Started with MobileIron Core.

   **NOTE:** If you are using only mobile application management (MAM)-only iOS devices, skip the MDM-related sections. For more information, see “Managing apps on MAM-only devices” in the MobileIron Apps@Work Guide

7. Update the device last check-in and policy update time in Core. See the "Managing device compliance checks" section in the MobileIron Core Device Management Guide.

8. Continue to Enabling MobileIron Threat Defense for Mobile@Work devices.
Configuring Privacy Policy

To configure the privacy policy to be applied to apps, perform the following procedure.

NOTE: The default Privacy Policy can be modified to collect All Apps.

2. Click Add New > Privacy. The New Privacy Policy dialog box opens.
   If there is already an existing privacy policy, the Modify Privacy Policy screen displays.
3. Enter the name of the policy and a description if needed.
4. In the Apps section, select All Apps.
5. Click to apply the All Smartphones label to the privacy policy.
6. Click Save.

NOTE: If you detect an unsecured Wi-Fi, but the quarantine action to remove the managed apps is not working, you may need to change the setting in the Apps field from App Catalog Apps to All Apps.

Creating an MTD admin

Before you configure the Zimperium management console (zConsole) for use with MobileIron Core, you need to create an MTD admin user, who will communicate with Core through the zConsole. MobileIron suggests creating a new admin user to manage MTD.

Procedure

1. In the Core Admin Portal, select Devices & Users > Users.
2. Click Add > Add new user.
   The Add New User dialog box opens.
3. Fill out the following fields:
   - User ID: Enter a meaningful User ID such as "mtdadmin."
   - First Name: Enter the first name of the mtdadmin user.
   - Last Name: Enter the last name of the mtdadmin user.
   - Display Name: Enter a name that will be displayed.
   - Password: Enter a password.
   - Confirm Password: Confirm the password.
   - Email: Enter the email address of the mtdadmin user.
4. Click Save.
Adding MTD roles to the Core admin user

Before you configure the zConsole for use with Core, you need to add MTD roles to the Core MTD admin user. These added MTD roles allow zConsole to communicate with Core using API calls that authenticate with this user to set privacy, label, compliance policy, and user management controls. For this procedure, use the same user ID, mtdadmin, and password that you set in Creating an MTD admin.

Before you begin

- Make sure port 443 is open bidirectionally to the internet on the firewall used to protect your trusted network.
- Obtain a username and password for the Zimperium management console (zConsole) service.
- Retrieve the MTD Activation token for MobileIron Threat Defense from your MobileIron representative or get it from the zConsole.

Procedure

1. In the Core Admin Portal, select Admin > mtdadmin. "mtdadmin" is the admin user name you will use to configure MDM in zConsole.
2. Select Actions > Edit roles.
3. In the list of roles, scroll down to:
   a. Privacy Control and select View apps and iBooks in device details and Locate device.
   b. Label Management and select View label and Manage label.
   c. User Management and select View user and Manage user.
   d. Other Roles and select Common Platform Services (CPS) and API.
4. Click Save.
Enabling CPS messaging on MobileIron Core

You run the MobileIron Core CLI program to enable Common Platform System (CPS) messaging. This procedure invokes a message broker, enables the Event Notification Service event notification feature, restarts the MobileIron server, and restarts Apache Tomcat (on MobileIron Core) to reload configurations.

**Note The Following:**

- The Messaging server listens to subscribing client requests over port 8883, and this port must be open for the service to function.
- If MobileIron Core is running in a High Availability configuration, please enable messaging on both primary and secondary nodes.

**Procedure**

To enable or disable CPS messaging, run the MobileIron Core CLI program as shown below:

```
host:~ host$ ssh miadmin@hostname
miadmin@hostname's password:
Last login: Thu May 4 13:43:48 2017 from 10.101.10.191
************************************************************
* MobileIron CORE CLI *
* *
* *
************************************************************
Welcome miadmin it is Thu May 4 13:49:39 UTC 2017
CORE(9.4.0.0-2388)@hostname> enable
Password:
CORE(9.4.0.0-2388)@hostname#configure terminal
Enter configuration commands, one per line.
CORE(9.4.0.0-2388)@hostname/config#activemq
Warning: Maintenance mode command.
Portal service will be stopped during this operation. Proceed? (y/n)y
Updating chkconfig...
Updating portal...
Starting ActiveMQ...
INFO: Loading '/mobileiron.com/programs/org.apache.activemq/bin/env'
INFO: Using java '/mobileiron.com/programs/com.mobileiron.platform.jre8/bin/java'
```
INFO: Starting - inspect logfiles specified in logging.properties and log4j.properties to get details

INFO: pidfile created: '/mobileiron.com/programs/org.apache.activemq/data/activemq.pid' (pid '22954')

Capturing tomcat metrics: [ OK ]

Stopping tomcat: [ OK ]

Starting tomcat: Using TOMCAT_ALLOCATION_MB=2048


Successfully enabled activemq

CORE(9.4.0.0-2388)@hostname/config#no activemq

Warning: Maintenance mode command.

Portal service will be stopped during this operation. Proceed? (y/n) y

Updating chkconfig...

Updating portal...

Stopping ActiveMQ...

INFO: Loading '/mobileiron.com/programs/org.apache.activemq/bin/env'

INFO: Using java '/mobileiron.com/programs/com.mobileiron.platform.jre8/bin/java'

ERROR: No or outdated process id in '/mobileiron.com/programs/org.apache.activemq/data/activemq.pid'

INFO: Removing /mobileiron.com/programs/org.apache.activemq/data/activemq.pid

Capturing tomcat metrics: [ OK ]

Stopping tomcat: [ OK ]

Starting tomcat: Using TOMCAT_ALLOCATION_MB=2048


MobileIron Threat Defense Solution Guide for Core | 19
Assigning an administrator to a space

After you have given the MTD administrator the needed roles, you need to assign the admin to a device space. For more information about assigning device spaces, see "Device Spaces" in the MobileIron Core Delegated Administration Guide.

Before you begin

Be sure you have added MTD roles to the Core admin user.

Procedure

1. In the Admin portal, select Admin > Admins.
2. In the To: field, select Authorized Users and enter the criteria in the Search by Name field to find the local user.
3. Click Enter to begin the search. From the search results, select a user, for example, "mtdadmin."
4. Go to Actions > Assign to space.
5. From the Space name field, select the space the local user will manage.
6. Click Save.

Adding Core as your MDM server in zConsole

You must add MobileIron Core as your MDM server in the Zimperium management console (zConsole) to enable MobileIron Threat Defense. After entering Core details such the URL and administrator user name and password, the zConsole synchronizes with Core. You can select the Core labels you want to use in zConsole, and the relevant users, devices, and apps from Core display in zConsole.

WARNING: Do not select any option that overwrites the password for your Core users.

Before you begin

- Locate the user name and password for the zConsole tenant you received from MobileIron after purchasing MobileIron Threat Defense Solution.
- Be sure you have completed Assigning an administrator to a space and Adding MTD roles to the Core admin user.
Procedure

1. Log in to your zConsole tenant with the credentials provided by MobileIron. The username and password defined for the MTD admin are required to establish communication with Core and synchronize the two servers.

2. Navigate to Manage > Integrations > Add MDM.

   NOTE: Mobile device management (MDM) is an older acronym for MobileIron Unified Endpoint Management (UEM).

3. Select MobileIron Core to add it to the zConsole as an MDM server.

4. Create your configuration using the following required information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the FQDN or externally accessible URL for your Core in secure hypertext protocol (HTTPS). For example: <a href="https://core.mydomain.com">https://core.mydomain.com</a></td>
</tr>
<tr>
<td>Username/Password</td>
<td>Enter an administrator user name and password for Core. The admin user should be assigned several roles, including API, as described in Adding MTD roles to the Core admin user.</td>
</tr>
<tr>
<td>MDM Name</td>
<td>Enter a name for Core.</td>
</tr>
<tr>
<td>Background sync</td>
<td>Select to specify that this MDM provider (Core) should automatically synchronize users, devices, apps, and profiles periodically.</td>
</tr>
</tbody>
</table>

5. Click Next.

6. In the last window, select the Core labels you want to use as zConsole groups. The list of zConsole groups is arranged in order of priority. Move a group name up or down to change its priority.

   NOTE: MobileIron recommends you create any new labels in the Core Admin portal before synchronizing zConsole with Core, otherwise the labels will not show up when this step is performed.

7. Click Finish.

8. Synchronize zConsole with Core. Make sure the synchronization is successful.

   NOTE: Whenever an MDM configuration is removed from zConsole, be sure to manually remove the MTD Activation token label in Core. If this is not done, the activation token remains assigned to a label in Core and Mobile@Work still displays "Enabled" for MTD.

Allowing access to the App Gateway

In order to create a MTD local action policy, you must grant MobileIron Core access to the App Gateway, so it can download threat definitions. See the following table for port information required for registering with the App
Gateway.

Before you begin

Be sure you have completed Adding Core as your MDM server in zConsole

External and Internet rules

The following table outlines the firewall rules required for Internet/Outside access for:

- MobileIron Core Appliance (physical or virtual) - All ports (except UDP) should be 'bi-directional' to allow information / data exchange between systems.
- Sentry Appliance (physical or virtual, ActiveSync / AppTunnel) - the Sentry must be able to resolve the Core hostname (via DNS lookup) or a hostfile entry must be added.

MobileIron Core Appliance and the Sentry Appliance items communicate with each other.

**TABLE 2. EXTERNAL AND INTERNET RULES**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from Internet/Outside to MobileIron Core</td>
<td>MobileIron Core is in the DMZ</td>
<td>Voice network service (VNS) gateway URL:</td>
</tr>
<tr>
<td></td>
<td>MobileIron Threat Defense scanning on iOS</td>
<td>Registration URL:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://appgw.mobileiron.com/api/v1/gateway/vns/organization">https://appgw.mobileiron.com/api/v1/gateway/vns/organization</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration URL:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://appgw.mobileiron.com/api/v1/gateway/vns/configuration">https://appgw.mobileiron.com/api/v1/gateway/vns/configuration</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Traffic from MobileIron Core to Internet/Outside</td>
<td>MobileIron Core is in the DMZ</td>
<td>Open ports 443 (HTTPS) and 2195, 2196, 2197 (TCP) between Core and Apple’s Apple Push Notification Service (APNS) network (17.0.0.0/8) for support of APNS for iOS devices. If you are not using iOS MDM, then this port is not required.</td>
</tr>
<tr>
<td></td>
<td>Apple APNS and MDM Services</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 2195, 2196, 2197</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 2196: feedback.push.apple.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 2197: api.push.apple.com (optional, alternative for HTTPS 443)</td>
</tr>
<tr>
<td></td>
<td>MobileIron Gateway</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td></td>
<td>support.mobileiron.com (199.127.90.0/23 ) for software update repository and upload of showtech log. Open HTTPS 443 to appgw.mobileiron.com, coresms.mobileiron.com, coreapns.mobileiron.com, clm.mobileiron.com,</td>
<td>HTTPS 443</td>
</tr>
</tbody>
</table>
TABLE 2. EXTERNAL AND INTERNET RULES (CONT.)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Port</th>
</tr>
</thead>
</table>
| Port                                             | api.push.apple.com, supportcdn.mobileiron.com, coregcm.mobileiron.com, and corefcm.mobileiron.com (199.127.90.0/23) for location/number lookup data, in-app registration, APNS/FCM/GCM messaging, licensing, and support for sending SMS.  
**a.mobileiron.net** for anonymized statistics collection. As the IP range for CDN sites (for example: supportcdn.mobileiron.com) may change from time to time, whitelist the domain name instead of the IP in the firewall if there is an option to do so. Otherwise, use support.mobileiron.com to download the updates instead of supportcdn.mobileiron.com. |               |
| AppConfig Community Repository                    | **https://appconfig.cdn.mobileiron.com**                                                                                                                                                                   | HTTPS 443     |

Additional Firewall Rules

The following table outlines additional firewall rules from the internal corporate network to the Internet.

- Organizations with local network-connected Wi-Fi must mirror the external firewall port configuration on their local DMZ firewall in order for Wi-Fi-connected devices to register and function day to day.
- MobileIron Sentry does not support connection pooling via load balancer. Turn off your load balancer’s connection pooling before deploying.

TABLE 3. ADDITIONAL FIREWALL RULES

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS (Wi-FiOnly) Devices</td>
<td>Open TCP 5223 to open 17.0.0.0/8 and allow iOS devices using corporate Wi-Fi to access the Apple APNS service. If you are not using iOS MDM, then this port is not required.</td>
<td>TCP 5223</td>
</tr>
</tbody>
</table>
|                          | **For devices on closed networks:**  
**ax.init.itunes.apple.com**: Current file-size limit for downloading apps over the cellular network.  
**ocsp.apple.com**: Status of the distribution certificate used to sign the provisioning profile.                                                                 |               |
| Android devices          | **To allow access to Google’s FCM or GCM service**: open TCP ports 5228, 5229, and 5230. FCM/GCM typically only uses TCP 5228, but it sometimes uses TCP 5229 and TCP 5230. FCM/GCM does not provide specific IPs, so you should allow your firewall to accept outgoing connections to all IP addresses contained in the IP blocks listed in Google’s ASN of 15169. For older devices, consider open HTTPS 443, as well. For Android enterprise: [https://www.googleapis.com/androidenterprise](https://www.googleapis.com/androidenterprise) | TCP 5228      
|                          | TCP 5229  
|                          | TCP 5230  
|                          | HTTPS 443 |
TABLE 3. ADDITIONAL FIREWALL RULES (CONT.)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://accounts.google.com/o/oauth2/token">https://accounts.google.com/o/oauth2/token</a></td>
<td>For Help@Work for Android: In general, TeamViewer will always work if Internet access is possible. As an alternative to HTTP 80, HTTPS 443 is also checked. It is also possible to open only TCP 5938 (required for mobile connections).</td>
<td></td>
</tr>
</tbody>
</table>

For the full list of ports, see the MobileIron Core On-Premise Installation Guide.

NOTE: When registering MTD for the first time, an Updating Configuration message displays prompting the device user: "Do you agree to allow your company to collect the list of apps on this device to report to the MobileIron Threat Defense service in order to protect your company’s data?" The device user must tap Agree. If not, the Mobile@Work registration will not work and the device user will need to re-register and agree.
Enabling MobileIron Threat Defense for Mobile@Work devices

This procedure is applicable to both Android and iOS devices.

Enabling MobileIron Threat Defense involves:

- Completing the prerequisites listed in Before You Begin.
- Obtaining your MTD Activation token.
- Creating a new MTD Activation Configuration.
- Apply label(s) to the configuration.

When this is done, the MTD Activation token is delivered to devices.

Note The Following:

- If you have an existing MTD Activation configuration, do not delete it. Install the new MTD Activation token first, and then optionally delete the old one.
- To be valid, the MTD license must be purchased from MobileIron or a licensed partner.

Before You Begin

Before you set up MobileIron Threat Defense, complete the following prerequisites:

1. Install MobileIron Core.
   See the "Core Installation" section in the On-Premise Installation Guide for information about how to install MobileIron Core.
2. Purchase a MobileIron Threat Defense license from MobileIron or a licensed partner.
3. Complete the following configuration tasks:
   See the On-Premise Installation Guide for more information on required ports and firewall rules.
   - Note the FQDN of the Core UEM server
   - Open Port 443 in the firewall
   - Allow access to the AppGateway URL
   - Allow access to the VNS URL
   - Allow access to APNS, FCS, GCM, etc.
- Allow access to the App_Config_Spec_File repository URL
- Allow incoming API calls and modify the ACL configuration for the specific source IPs

4. Upload your TLS (Transport Layer Security) trust certificate to Core (formerly called an MDM certificate). See the "Managing Certificates and Configuring Certificate Authorities" section of the MobileIron Core Device Management Guide.

5. Contact your MobileIron representative to request your unique, encrypted MTD Activation token, or get it from zConsole.

   NOTE: To be valid, the MTD license must be purchased from MobileIron or a licensed partner.

6. Request and upload an MDM certificate for iOS, if you have not already done so. In addition, you need to enable iOS MDM support and confirm MDM for an iOS device. For information, see the "Managing Mobile Device Management (MDM) certificates for iOS and macOS" section of the Getting Started with MobileIron Core.

   NOTE: If you are using only mobile application management (MAM)-only iOS devices, skip the MDM-related sections. For more information, see "Managing apps on MAM-only devices" in the MobileIron Apps@Work Guide

7. Update the device last check-in and policy update time in Core. See the "Managing device compliance checks" section in the MobileIron Core Device Management Guide.

8. Continue to Enabling MobileIron Threat Defense for Mobile@Work devices.

Creating an MTD activation configuration

Procedure

1. Log into zConsole and download the MobileIron MTD Activation Code.
2. In Core, go to Policies & Configs > Configurations.
3. Click Add New > MTD Activation. The Add MTD Activation Configuration dialog box opens.
4. Enter a name for the configuration.
5. (Optional) Click + Add Description to enter a description.
6. In the Configuration Setup section, make the following entries:
   - **Vendor**: Zimperium
   - **License Key**: enter your MobileIron Threat Defense activation code.
   - **Wake up Intervals (mins)**: 60 (the default) or set a higher interval.
7. Click Save. The Configurations page refreshes with the name of the new MTD Activation Configuration.
8. Apply a label to the MTD Activation Configuration. Upon next check-in, the new activation configuration is pushed to the device(s). See Creating MTD labels in Core for Android and iOS devices.
Pushing new MTD activation configurations to existing devices

Android

- For Mobile@Work 10.2.0.0, when the Android XML Configuration (zConsole) is pushed to the device and then the Administrator applies a label to the MTD activation configuration, upon the next device checkin, the MTD Activation token will take precedence.

- For Mobile@Work 10.1.0.0, when the Android XML Configuration (zConsole) is pushed to the device and then the Administrator applies a label to another MTD Activation Configuration, upon the next device checkin, the device user will see an error message stating that the license was already activated. The functionality will work, but it is advised you remove the old Android XML Configuration.

- In case of both Mobile@Work 10.1.0.0 client and Mobile@Work 10.2.0.0 client, if the first MTD Activation Configuration is pushed to the device and the Administrator applies a label to another MTD Activation Configuration, upon the next device checkin, the device user will see an error message stating that the license was already activated.

iOS

- For Mobile@Work 10.2.0.0, when the MTD Activation Configuration is pushed to the device and then the Administrator applies a label to the MTD Activation Configuration, the MTD Activation token will take precedence. You can optionally choose to delete the old configuration (Apps > App Catalog > select Mobile@Work > Edit > Managed App Configuration section.)

Verify that MobileIron Threat Defense is working

To verify that MobileIron Threat Detection is working, device users can review the Mobile@Work display, and administrators can perform a Force Device Check-in. You can also use zConsole to verify that the MTD Activation token(s) have been distributed to selected devices through the application of the correct label.

Verify that MTD is working on a Device

Administrators can verify that MobileIron Threat Detection is working by checking Devices in Core.

1. From MobileIron Core Admin Portal, go to Devices & Users > Devices.
2. Select the carat ^ next to the display name of the device you want to check. The device information displays.
3. In the Device Details tab, find MobileIron Threat Defense Status:
<table>
<thead>
<tr>
<th>Device type</th>
<th>Using client release</th>
<th>Device status message</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>Mobile@Work 10.2.0.0 client</td>
<td>&quot;Activated&quot;</td>
</tr>
<tr>
<td></td>
<td>Mobile@Work 10.4.0.0 client through the most recently released version as supported by MobileIron</td>
<td>&quot;Protected&quot;</td>
</tr>
<tr>
<td>Android</td>
<td>Mobile@Work 10.1.0.0 client</td>
<td>&quot;Activated threat scanning enabled&quot;</td>
</tr>
<tr>
<td></td>
<td>Mobile@Work 10.2.0.0 client through the most recently released version as supported by MobileIron</td>
<td>&quot;Protected&quot;</td>
</tr>
</tbody>
</table>

**Verify MTD on all devices**

To verify that MTD is working on all devices, administrators can perform a Force Device Check-in:

**Procedure**
1. From the MobileIron Admin Portal, click the **Devices** tab.
2. Select the devices that you want to check in.
3. From the menu, select **Force Check-in**.
Defining Policies

MobileIron Threat Defense uses policies to regulate the behavior of MTD-enabled devices. Each policy consists of a set of rules. You can create multiple policies for each policy type, but only one active policy of each type can be applied to a specific device.

Refer to the Getting Started with MobileIron Core for information on the most commonly used policy topics, such as:

- Default policies
- Security policies
- Privacy policies
- Lockdown policies
- Sync policies

The types of policies used by MobileIron Threat Defense include:

- MTD Local actions threat defense policies. See Mitigation and compliance using Local Actions.
- MTD security policies. See Defining an MTD security policy in Core.
- App control rules. See Defining app control rules in Core
- Phishing protection. See Configuring Phishing Protection in Core
- Event notifications. See Creating event notifications in Core.

Defining app control rules in Core

This server-initiated task creates an App Control rule that installs a non-existent app on the managed iOS or Android device, to enforce compliance actions on MTD-enabled devices by applying previously-defined labels.

Before you begin

Be sure you have completed Creating MTD labels in Core for Android and iOS devices.

Procedure

1. In the Core Admin Portal, select Apps > App Control.
2. Click the Add button.
3. Enter a descriptive name such as “Always True” in the Name field.
4. Select the radio button next to Required in the Type section of the page.

5. In the Rules Entries section, fill out the following fields:
   a. **App**: Select **Name Equals** from the pull down menu.
   b. **App Identifier/Name**: Add a bogus app identifier or name.
   c. **Device Platform**: Select **All** from the pull-down menu.
   d. **Comment**: Add a meaningful comment, such as "This app will never appear."

6. Click **Save**.

**Next steps**

Proceed to **Defining an MTD security policy in Core**.

### Defining an MTD security policy in Core

To define an MTD security policy in Core, you must create an MTD security policy for the labels you created in **Creating MTD labels in Core for Android and iOS devices**.

**Before you begin**

Be sure you have completed **Defining app control rules in Core**.

**Procedure**

1. In the Core Admin Portal, select **Policies & Configs > Policies**.
3. Enter a descriptive name in the **Name** field, such as MTD–Security Policy.
4. Change the **Status** to Active. Set the priority if needed.
5. Scroll down to the **Access Control** section.
6. Under **For All Platforms**, select the compliance action that you created in **Creating and applying server-initiated multi-tier compliance actions**, for the **when a device violates the App Control roles** field. (Quarantine, for example.)
7. In the Rule Type: Required section, move **Always True** to the Enabled column. (You created the rule type in **Defining app control rules in Core**.)
8. Scroll down to the For iOS devices section:
   a. Select **Quarantine** as the compliance action for the **when a compromised iOS device is detected** field.
   b. Select **Quarantine** for the **when device MDM is deactivated** field.
9. Scroll down to the For Android devices section, select **Quarantine** as the compliance action in the **when a compromised Android device is detected** field.
10. Click **Save**.
11. In the **Policies & Configs > Compliance Policies** page, select the check box next to the MTD security policy.

12. **Select Actions > Apply to Label.** This applies the threat label you configured in [Creating MTD labels in Core for Android and iOS devices](#) to the MTD security policy. (MTD–ExploitDetected, MTD–Malwareinfected, and MTD–NetworkThreat, for example)

**Next steps**

Proceed to [Creating event notifications in Core](#).

**Creating event notifications in Core**

You can create event notifications that the user will see on their Android or iOS device. Notifications are sent via push notification, SMS, or email, and only apply to app compliance policy violations.

In the context of MobileIron threat detection, notifications for server-initiated compliance events are governed and controlled by zConsole. When zConsole detects a non-compliant event, it generates a compliance action, and sends a message to the affected devices. This is a separate process from compliance notification for Local Actions policy.

**Before you begin**

Be sure you have completed [Defining an MTD security policy in Core](#).

**Procedure**

1. In the Core Admin Portal, select **Logs > Event Settings**.
3. Enter a descriptive name in the **Name** field, such as MTD – ExploitDetected.
4. Scroll down to the Security Policy Triggers section. Select the following fields under the App Control - All Platforms heading:
   a. Disallowed app found
   b. App found that is not in Allowed Apps list.
   c. Required app not found
5. For iOS devices, scroll down to the iOS section. Select the following fields:
   a. Disallowed iOS model found
   b. Disallowed iOS version found
   c. Compromised iOS device detected
   d. iOS Configuration not compliant
   e. Restored Device connected to server
f. iOS Location-Based Wakeups disabled by user

g. Device MDM deactivated (iOS 5.0 or later)

6. For Android devices, scroll down to the Android section. Select the following fields:
   a. Disallowed Android OS version found
   b. Compromised Android device detected
   c. Device administration not activated for DM client or agent
   d. Attestation Failed

7. For both iOS and Android devices, scroll down to the Actions section. Under the Alert Configuration heading, configure the following options:
   a. Select the radio button next to Limited under Maximum Alerts.
   b. Select the 1 day pull-down menu under Alert Every.
   c. Select None or User Only for the Send SMS field.
   d. Select User only or User + Admin for the Send Through Push Notification field.
   e. Move a label, such as "MTD-ExploitedDetected," from the Available to the Selected columns in the Apply to Labels field.

8. Click the Create button next to the Template field. The Add New Event Center Template dialog box opens. Enter the following fields:

   a. Enter a name for the template in the Name field. For example, use MTD-ExploitedDetected as a template name.

   b. Select a language with the pull-down menu for the Edit Template For field.

   ![Add New Event Center Template](image)

9. (Optional) In the Message field, enter text for alerts generated by violations of the compliance policy rule.
### TABLE 4. EVENT CENTER VARIABLES SUPPORT

<table>
<thead>
<tr>
<th>Type</th>
<th>Variables Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>$SEVERITY - The defined severity of the system event, for example, Information, Warning, or Critical.</td>
</tr>
<tr>
<td>Email Body</td>
<td>$PHONE_NUMBER - The phone number used by the device.</td>
</tr>
<tr>
<td>SMS</td>
<td>$USER_NAME - The display name of the user associated with the device.</td>
</tr>
<tr>
<td>APNS</td>
<td>$DEFAULT_POLICY_VIOLATION_MESSAGE - The hard-coded message associated with the policy violation that triggered the alert.</td>
</tr>
</tbody>
</table>

**NOTE:** Custom attribute variable substitutions are not supported.

10. Click **Save** to save the template. The New Policy Violations Event page displays.
11. Click **Save**.

**Next steps**

Proceed to [Configuring the zConsole Mobile Threat Response Policy](#).
Server-initiated mitigation and multi-tier compliance

The multi-tier compliance action format is a best practice for server-initiated mitigation and compliance via the zConsole. Before proceeding, some tasks need to be done:

- Delete any existing MTD labels
- Delete any existing MTD security policies
- Modify the default privacy policy to have no MTD-related app control rules

Server-initiated mitigation and compliance contains the following steps:

1. Creating MTD labels in Core for Android and iOS devices
2. Creating and applying server-initiated multi-tier compliance actions
3. Creating compliance policy rules and groups
4. Configuring the zConsole Mobile Threat Response Policy
5. Updating Core Sync Policy

NOTE: Both server-initiated and local compliance actions can exist concurrently – they are not mutually exclusive.

Creating MTD labels in Core for Android and iOS devices

You need to create several labels that will be applied to both Android and iOS devices. In the following procedure, create labels for malware infected, exploit detected, and network threat labels.

NOTE: If labels are created after initially configuring the zConsole and synchronizing it with Core, zConsole will need to be synchronized with Core again before the labels will appear in zConsole.

Before you begin

Be sure you have:

- Deleted any existing MTD labels
- Deleted any existing MTD security policies
- The Apps field in the Default Privacy Policy should be set to App Catalog Apps
Procedure

1. In the Core Admin Portal, select **Devices & Users**.
2. Select **Labels > Add Label**. The Add Label dialog box opens.
3. **Name** the label "MTD-Block," add an optional Description.
4. In the Type field, select the **Manual** radio button. This label can be applied to Elevated or Critical severity level threats within the Mobile Threat Response policies within zConsole.
5. Click **Save**.
6. Create a second label "MTD-Notification" and click the **Manual** radio button in the Type section. This label can be applied to Low or Normal severity threats within the Mobile Threat Response policies within zConsole.
7. Create a third label "MTD-Quarantine" and click the **Manual** radio button in the Type section. This label can be applied to Elevated or Critical severity level threats within the Mobile Threat Response policies within zConsole.
8. Create a fourth label called "MTD-Tiered Compliance 23 hours" and click the **Manual** radio button in the Type section. This label can be applied to Low, Normal, Elevated, or Critical severity level threats within the Mobile Threat Response policies within zConsole.
9. Create a fifth label called "MTD-Tiered Compliance 4 hours" and click the **Manual** radio button in the Type section. This label can be applied to Low, Normal, Elevated, or Critical severity level threats within the Mobile Threat Response policies within zConsole.

Creating and applying server-initiated multi-tier compliance actions

This section discusses how to create and apply compliance actions that are initiated by the Zimperium management console (zConsole). (For MTD local actions, see Creating MTD Local Actions threat defense policy in Core.) User devices can trigger a check-in with zConsole, but it is initiated by zConsole to Core and then Core sends a command to the device to do the check-in. This way, the devices are protected from zero-day malware, device, network and application threats without having to wait for the next scheduled check-in event. The compliance actions are evaluated during the client check-in event and the selected compliance actions are enforced on the client by MobileIron Core, when the device is determined to be non-compliant with policy.

**NOTE:** In order for the multi-tiered compliance actions feature to work, device users must have Mobile@Work 10.0.0.0 through the most recently released version as supported by MobileIron installed.

With custom compliance actions, you can create actions to better manage access control. With tiered compliance actions, you can customize them to include up to 4 levels of action to better manage compliance actions: Critical, Elevated, Normal and Low.

In addition to two existing compliance actions ("Block Email, App Connect apps and Send Alert" compliance action and the "Send Alert" compliance action, it is best practice to have three additional MTD-related compliance actions based on the threat severity level:
Before you begin

- Be sure that you have completed Creating MTD labels in Core for Android and iOS devices.
- Make sure there are two compliance actions created in Core: “Block Email, App Connect apps and Send Alert” compliance action and the “Send Alert” compliance action.

Quarantine Compliance Action

Procedure

1. In the Core Admin Portal, select Policies & Configs > Compliance Actions.
2. Click the Add+ button. The Add Compliance Action dialog box opens.
   a. **Name:** Enter "Quarantine."
   b. **Enforce Compliance Actions Locally on Devices:** Select the check box to enforce the compliance actions on the device.
3. In the Tier 1 section, fill out the following fields:
   a. **Alert:** Select the check box to send a compliance notification or alert to the device user.
   b. **Block Access:** Select the check box to block email access and AppConnect apps on the device. This selection does not apply to macOS devices.
4. Click the expand (+) button at the bottom of the dialog box. Tier 2 selections display.
   a. Select **Quarantine the device** to quarantine the device.
   b. Select **Remove All Configurations** to remove all configuration settings from an Android or iOS device.
   c. Select **Do not remove Wi-Fi settings for all devices (iOS, macOS, and Android only)** to allow all iOS and Android devices to maintain their connection to Wi-Fi.
   d. Select **Remove iBooks, content, managed apps, and block new app downloads** to remove iBooks, content and managed apps from these devices as well as to block downloads of new apps.
5. Click **Save**.

Tiered Compliance Action - 23 hours

1. Click the Add+ button. The Add Compliance Action dialog box opens.
2. **Name:** Enter "Tiered Compliance 23 hours."
3. **Enforce Compliance Actions Locally on Devices:** Select the check box to enforce the compliance actions on the device.
4. In the Tier 1 section, fill out the following fields:
a. **Alert**: Select the check box to send a compliance notification or alert to the device user.

b. **Block Access**: Select the check box to block email access and AppConnect apps on the device. This selection does not apply to macOS devices.

5. Click the **expand (+)** button at the bottom of the dialog box. Tier 2 selections display.
   a. Set the **Wait** time to 23 Hours.
   b. **Alert**: Select the check box to send a compliance notification or alert to the device user.
   c. **Block Access**: Select the check box to block email access and AppConnect apps on the device. This selection does not apply to macOS devices.

6. Click the **expand (+)** button at the bottom of the dialog box. Tier 3 selections display.
   a. Set the **Wait** time to 23 Hours.
   b. **Alert**: Select the check box to send a compliance notification or alert to the device user.
   c. **Block Access**: This section will be selected but read-only because the selection was made in Tier 2.
   d. Select **Quarantine the device** to quarantine the device; the section expands.
   e. Select **Remove All Configurations** to remove all configuration settings from an Android or iOS device.
   f. Select **Do not remove Wi-Fi settings for all devices (iOS, macOS, and Android only)** to allow all iOS and Android devices to maintain their connection to Wi-Fi.
   g. Select **Remove iBooks, content, managed apps, and block new app downloads** to remove iBooks, content and managed apps from these devices as well as to block downloads of new apps.

7. Click **Save**.

**Tiered Compliance Action - 4 hours**

1. Click the **Add+** button. The Add Compliance Action dialog box opens.

2. **Name**: Enter "Tiered Compliance 4 hours."

3. **Enforce Compliance Actions Locally on Devices**: Select the check box to enforce the compliance actions on the device.

4. In the Tier 1 section, fill out the following fields:
   a. **Alert**: Select the check box to send a compliance notification or alert to the device user.
   b. **Block Access**: Select the check box to block email access and AppConnect apps on the device. This selection does not apply to macOS devices.

5. Click the **expand (+)** button at the bottom of the dialog box. Tier 2 selections display.
   a. Set the **Wait** time to 4 Hours.
   b. **Alert**: Select the check box to send a compliance notification or alert to the device user.
   c. **Block Access**: This section will be selected but read-only because the selection was made in Tier 1.

6. Click the **expand (+)** button at the bottom of the dialog box. Tier 3 selections display.
a. Set the **Wait** time to 4 Hours.
b. **Alert**: Select the check box to send a compliance notification or alert to the device user.
c. **Block Access**: This section will be selected but read-only because the selection was made in Tier 1.
d. Select **Quarantine the device** to quarantine the device; the section expands.
e. Select **Remove All Configurations** to remove all configuration settings from an Android or iOS device.
f. Select **Do not remove Wi-Fi settings for all devices (iOS, macOS, and Android only)** to allow all iOS and Android devices to maintain their connection to Wi-Fi.
g. Select **Remove iBooks, content, managed apps, and block new app downloads** to remove iBooks, content and managed apps from these devices as well as to block downloads of new apps.

7. Click **Save**.

### Configuring the zConsole Mobile Threat Response Policy

The Threat Response Matrix (TRM) defines the actions that Zimperium management console (zConsole) takes upon detecting an event. Among the options are:

- Enable or disable detection of a specific threat classification
- Alert the user
- Define the text of the alert
- Set protection actions

**Before you begin**

- If you are setting up **Server-initiated mitigation and multi-tier compliance** be sure you have completed the procedures listed in [Creating compliance policy rules and groups](#)
- If you are setting up **Mitigation and compliance using Local Actions** be sure you have completed the procedure in [Creating optional additional compliance policies on zConsole](#)

After you modify these options, click **Deploy** to send, or sync, the new TRM to the devices currently logged in. When integrated and synced with MobileIron Core, each group used for integration is created as a group with its own TRM. Select which TRM to modify with the pull-down menu next to the **Selected Group** field. Only users and devices in the selected group receive the modified TRM. See below for a sample TRM.
**NOTE:** You must manually sync (deploy) zConsole with MobileIron Core. This aligns the labels in Core with the TRM settings.

**Enable**

The zConsole administrator has the option of disabling certain threat detections and, therefore, the collection of associated forensics. In the **Severity** column, you can disable the status of "Elevated" or "Lower" by clearing the radio button in the row of the event. This change is effective after selecting the **Deploy** button again.

After deploying / syncing with MobileIron Core, when a threat is detected, zConsole instructs Core to move the device to the chosen label in the Threat Response Policy / Matrix. The workflow assigned to that label determines the action that Core takes on the device. The communication from zConsole to Core is performed securely through a MobileIron API call.

**Severity**

The administrator has the option of changing the threat severity levels. This is useful for different business cases. The options are "Critical," "Elevated," "Low," and "Normal.

**Threat**

The threats listed in the **Threat column** represent the classes of threats that MobileIron Threat Defense detects. Threat classes are recognized by MTD, which is able to determine when a malicious event is happening.

**Set User Alerts**

Administrators cannot manage MTD alerts through zConsole. In order to implement and localize MTD alerts, please use Local Actions policy in Core. See Mitigation and compliance using Local Actions.
Set Device Action

Administrators can deploy device actions for Android and iOS devices on zConsole.

Procedure

1. From the MTD zConsole, navigate to the Policy > Threat Policy page.
2. Use the pull-down menu in the Selected Group field to display your configuration group.
3. Select the policy you want to modify.
4. From the Device Action column, click the settings icon for the selected row, and select an action. zConsole securely communicates with Core and applies the action.

5. To remove the device action, uncheck the action and click OK.

MDM Action

Administrators can enable server-enforced mobile device management (MDM) action items on the zConsole policies page.

Procedure

1. From the zConsole, navigate to the Policy > Threat Policy page.
2. Use the pull-down menu in the Selected Group field to display your Core configuration group.
3. Select the policy you want to modify.
4. From the MDM Action column, click the drop-down arrow on the selected row, and select an action. zConsole securely communicates with Core and applies the action.
5. To remove an action from occurring for a threat classification, change the threat MDM Action to No Action.

Mitigation Action

When a threat that was detected by zConsole has been remediated and is no longer posing a threat to the device, you can define specific actions that can be taken. For example, when a device is determined to be under a Man-in-the-Middle attack, it can be prevented from accessing various corporate resources. When the device is moved to a clean network, you can automatically allow the device to access those resources again.

The Mitigation Action column can be used to assign actions. To remove the action that was performed as a response to a threat that is now mitigated, choose Remove. This action removes the device from the group it was assigned to when the threat was detected.

Due to the nature of some threats, not all threat classifications can be mitigated. The following table provides possible mitigation actions for a threat.

**TABLE 5. POSSIBLE MITIGATION ACTIONS FOR A THREAT**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>All man-in-the-middle (MITM) threats</td>
<td>When the device connects to a different basic service set identifier (BSSID).</td>
</tr>
<tr>
<td>Root/Jailbroken</td>
<td>When the root flag on devices changes from true to false</td>
</tr>
<tr>
<td>EOP, system tampering, abnormal process activity</td>
<td>No mitigation, the only mitigation is to flash the device since it has been compromised</td>
</tr>
<tr>
<td>USB debugging</td>
<td>When USB debugging is enabled</td>
</tr>
</tbody>
</table>

Notifications

You can set up an email or SMS notification process for each specific threat. SMS notifications require the administrator’s telephone information to be set up in the User page of a given administrator. Each email or SMS contains an Event summary and a link to the actual event that can be viewed in a browser after login.

In this procedure, you configure the notifications and mitigation actions that apply to both iOS and Android devices.

**Procedure**

1. In the zConsole portal, select Policy. The Mobile Threat Response Policy page displays.
2. Use the pull-down menu in the Selected Group field to display your Core configuration group.
3. Click the Deploy button to deploy the policy on your devices.
- The **Threat** column displays the supported threat that can be detected by the client.
- The **Device Action** column displays the action taken after a threat is detected. This is an optional configuration.

**Related topics**

- Configuring zConsole

**Updating Core Sync Policy**

A final step in configuring mitigation and compliance is to make sure your sync policy is updated.

**Before you begin**

Be sure you have completed Server-initiated mitigation and multi-tier compliance or Mitigation and compliance using Local Actions.

**Configuring device scanning frequency for threat scan**

You can set the frequency for waking up iOS devices and running a threat scan.

**Procedure**

1. From the MobileIron Core Admin portal, go to **Policies & Configs > Policies**.
2. Click **Add New > Sync**. The **New Sync Policy** dialog box opens. If there is already an existing Sync policy the **Modify Sync Policy** screen will be displayed.
3. Enter the name of the policy and a description if needed.
4. (iOS only) Enter an **MTD wakeup interval** in minutes. This interval determines how often Mobile@Work wakes up and performs an MTD scan on iOS devices. The default wakeup interval is **15 minutes**. Setting this value to a low interval is more taxing on the device's battery than setting it at a higher interval.
   
   **NOTE:** If the default check-in interval results in excessive battery usage for iOS clients, select a higher wake up interval.
5. Click **Save**.
6. Apply the label **All Smartphones** to the policy.

**NOTE:** The **Client is always connected** option is only applicable for Android devices and does not apply to iOS devices. Selecting (enabling) this check box ensures continuous MTD scanning on Android devices.

**Next steps**

- Configuring zConsole
- Managing Devices in zConsole
Related topics

- For general instructions on creating a sync policy, see *Getting Started with MobileIron Core*.
- For instructions on iOS sync policy, see "iOS location-based wakeups interval and syncing with MobileIron Core" in the *MobileIron Core Device Management Guide for iOS*.
- For instructions on Android sync policy, see "Android notification sync policy" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*. 
Mitigation and compliance using Local Actions

You can create mitigation and compliance actions using Local Actions threat defense policy. This method does not require a connection to the server. The actions are applied locally on the device.

Core receives the threat definitions list from the App Gateway. The threat list is updated periodically, when new threats are identified or existing threats are removed. Before you begin, verify that Core is able to communicate with the App Gateway to obtain the latest threat list. The threat definitions file changes infrequently and an MTD audit log is created whenever a new version of the file becomes available.

NOTE: If you want to configure server-initiated compliance, see Server-initiated mitigation and multi-tier compliance.

Using Core MTD local actions policy to configure mitigation and compliance requires the following tasks:

1. Creating MTD Local Actions threat defense policy in Core.
2. Using zConsole to monitor threats to Android devices or Using zConsole to monitor threats to iOS devices.
3. Updating the MTD Local Actions policy when new threat list is available.
4. Configuring the zConsole Mobile Threat Response Policy
5. Updating Core Sync Policy.

Creating MTD Local Actions threat defense policy in Core

Using MobileIron Threat Defense Local Actions configurations, you can set specific local actions to be taken on supported iOS and Android devices when the MTD-enabled client detects a threat. The MTD local actions policy is enforced on devices, independent of the device being connected to and in communication with Core or the zConsole server. On the device, Mobile@Work enforces the policy locally.

Before you begin

Be sure you have completed MobileIron Threat Defense prerequisites.

Procedure

1. From the MobileIron Core Admin portal, select Policies & Configs > Policies > Add New > MTD Local Actions.
2. Enter the policy name into the Name field and an optional Description.
3. In the Status field, select Active to enable the policy. Select Inactive to disable the policy.
4. Specify the priority of this policy relative to other custom policies of the same type, to determine which policy Core applies if more than one policy is available. Select **Higher than** or **Lower than**, and then select an existing policy from the drop-down menu. For example, to give "Policy A" a higher priority than "Policy B," select “Higher than” and “Policy B.”

5. In the Threat category names and related threats table, click ^ to expand threat category, displaying all of the threats contained within that category. This selection controls which notifications are enabled on the device and which migration actions are taken locally on the device when a threat is detected.

6. Make your selections.

7. Click **Save** to save the policy.

**Creating compliance policy rules and groups**

**Before you begin**

Be sure you have completed Creating and applying server-initiated multi-tier compliance actions.

**Threat types**

Within MobileIron Threat Defense, there are three threat types. Within each type there are severity levels: Critical, Elevated, Normal, and Low. Altogether you have:

- **Device** – Critical, Elevated, Normal, and Low severity levels
- **Network** – Critical, Elevated, Normal, and Low severity levels
- **App** – Critical, Elevated, Normal, and Low severity levels

For each threat type, you create compliance policy rules based on the threat severity. As a best practice, you should have the following compliance policy rules:

- For Low and Normal threat types – use **Send Alert**
- For Elevated threat type – use **Block Access** and/or **Quarantine**
- For Critical threat type – use **Quarantine** or **Tier Compliance**:
  a. Block – notify
  b. Notification
  c. Quarantine – remove. If Low, send notification and let user decide what action to take.
  d. Tiered Compliance 23 hours
  e. Tiered Compliance 4 hours

Example of threat type implementation: user connects to hotel Wi-Fi

- Tier 1 - Notification - MTD alerts the device user "You just connected to unsecure Wi-Fi"
- Tier 2 - After 4 hours, MTD blocks the user's access to email and AppConnect apps.
- Tier 3 - MTD Quarantines and blocks the Wi-Fi; removes user's access to the company network.

Creating compliance policy rules

You will need to create compliance policy rules based on threat severity level.

Procedure

1. From the MobileIron Core Admin portal, select Policies & Configs > Compliance Policies.
2. Click the Compliance Policy Rule tab and then click Add+.
3. Enter "Block" in the Rule Name field.
4. Set the Status to Enabled.
5. (Optional) Enter a description of the rule, for example, "MTD Block Rule."
6. In the Condition expression field, enter this expression:
   
   ```
   ("common.platform" = "Android" OR "common.platform" = "iOS") AND "common.retired" = false AND "common.retired" = false
   ```
7. In the Compliance Actions field, select from the drop-down: Block Email, AppConnect apps, and Send Alert.
8. (Optional) In the Message field, enter text for alerts generated by violations of the policy rule.
9. Click Save. The Block rule displays in the Compliance Policy Rule tab.
10. Repeat steps 2-9 using the parameters below for creating additional compliance policy rules.

<table>
<thead>
<tr>
<th>Rule Name field</th>
<th>Condition expression field</th>
<th>Compliance Actions field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>(&quot;common.platform&quot; = &quot;Android&quot; OR &quot;common.platform&quot; = &quot;iOS&quot;) AND &quot;common.retired&quot; = false AND &quot;common.retired&quot; = false</td>
<td>Send Alert</td>
</tr>
<tr>
<td>Quarantine</td>
<td>(&quot;common.platform&quot; = &quot;Android&quot; OR &quot;common.platform&quot; = &quot;iOS&quot;) AND &quot;common.retired&quot; = false AND &quot;common.retired&quot; = false</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Tiered Compliance 23 hours</td>
<td>(&quot;common.platform&quot; = &quot;Android&quot; OR &quot;common.platform&quot; = &quot;iOS&quot;) AND &quot;common.retired&quot; = false AND &quot;common.retired&quot; = false</td>
<td>Tiered Compliance 23 hours</td>
</tr>
<tr>
<td>Tiered Compliance 4 hours</td>
<td>(&quot;common.platform&quot; = &quot;Android&quot; OR &quot;common.platform&quot; = &quot;iOS&quot;) AND &quot;common.retired&quot; = false AND &quot;common.retired&quot; = false</td>
<td>Tiered Compliance 4 hours</td>
</tr>
</tbody>
</table>

When you have finished, you should have five compliance policy rules displayed in the Compliance Policy Rule tab.
Creating compliance policy groups

Compliance policy groups are used to apply the group’s rules to devices matching the label.

Procedure

2. Click on the Compliance Policy Group tab and then click on Add+.
3. Enter "MTDBlock" into the Group Name field.
4. Keep the default Status of Enabled.
5. (Optional) Enter a description of the group name, for example, "MTDBlock."
6. In the Available Rules field, move the "Block" rule to the Selected Rules section. (Action is "Block Email, AppConnect apps, and Send Alert.")
7. Click Save. The MTDBlock group displays in the Compliance Policy Group tab.
8. Repeat steps 2-7 using the parameters below for creating additional compliance policy groups.

<table>
<thead>
<tr>
<th>Group Name field</th>
<th>Status</th>
<th>Rule Name</th>
<th>Action Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTDNotification</td>
<td>Enabled</td>
<td>Notification</td>
<td>Send Alert</td>
</tr>
<tr>
<td>MTDQuarantine</td>
<td>Enabled</td>
<td>Quarantine</td>
<td>Quarantine</td>
</tr>
<tr>
<td>MTDTiered23hours</td>
<td>Enabled</td>
<td>TieredCompliance23hours</td>
<td>Tiered Compliance 23 hours</td>
</tr>
<tr>
<td>MTDTiered4hours</td>
<td>Enabled</td>
<td>TieredCompliance4hours</td>
<td>Tiered Compliance 4 hours</td>
</tr>
</tbody>
</table>

When you have finished, you should have five compliance policy rules displayed in the Compliance Policy Group tab.
Example: Creating an Out of Compliance Local Actions policy

MTD+ customers can configure an app compliance policy that will protect client users from installing disapproved apps. Use this example task to create an Out of Compliance Local Actions policy, and others like it.

Before you begin
This feature is available only with an MTD+ license. See your MobileIron representative for more information.

Procedure

1. From the Admin portal, navigate to Policies & Configs > Policies page
2. Click Add New > MTD Local Actions. The Add MTD Local Actions Policy opens.
3. Enter a name, status (active or inactive), and optional description.
4. Click the upcarat for Malware Threats.
5. From the options, click Out of Compliance App
6. Select the local actions and notifications for the policy from the drop-down options.
7. Click Save.

Configuring the iOS sinkhole VPN local action

MTD Admins can configure an iOS sinkhole option to automatically redirect malicious client Internet traffic away from the Enterprise. From Core 10.6.0.0 through the most recently released version as supported by MobileIron, the MobileIron Local Actions configuration provides a Network Sinkhole option for iOS devices that can create and push a MobileIron Threat Defense VPN to client users immediately, without user confirmation.

NOTE: MobileIron recommends selecting the Network Sinkhole action ONLY for network-related threats. Use of Network Sinkhole action for device and application threats can result in disabling network connectivity to the device without the ability to restore network connectivity.

Procedure

1. From the MobileIron Cloud Configurations page, create or edit an MTD local action configuration.
2. From a threat in the Network Threats section, select Network Sinkhole from the Local Action iOS column.
3. Finish your configuration choices, and save the Local Actions configuration. The MobileIron Threat Defense VPN configuration displays in the Configurations page.

<table>
<thead>
<tr>
<th>MobileIron Threat Defense VPN</th>
<th>3 days, 2 hours ago by System</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Will auto install the sinkhole VPN profile on end users device which will get enabled if sinkhole local compliance action has been configured for a threat.</td>
<td>Distributed To:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS Devices</td>
</tr>
</tbody>
</table>

The VPN configuration cannot be edited. To remove the configuration, remove the Network Sinkhole options from the configuration.

4. Push the configuration to selected devices.
   a. From the Devices page, select the iOS devices.
   b. Click the Actions menu.
   c. Select Force Check-in. Confirm the choice.

### Threat category names and related threats

To select and configure a network, device, or app threat from the MTD Local Actions page, follow these general steps:

1. Click ^ to expand the threat category, displaying all of the threats contained within that category. This selection controls which notifications are enabled on the device and which migration actions are taken locally on the device when a threat is detected.

2. For Local Actions iOS, select Block AppConnect Apps or Network Sinkhole.
   
   **NOTE:** MobileIron recommends ONLY selecting the Network Sinkhole action for network-related threats. Use of Network Sinkhole action for device and application threats can result in disabling network connectivity to the device without the ability to restore network connectivity.

3. For Local Actions Android, select any one of the following:
   - 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 Wi-Fi

4. For Notifications, select Yes and No to enable or disable notifications, respectively.

5. To choose multiple threat actions, select the check box to the left of the threat. Click the Actions pull-down menu to select multiple actions for the threat.
For example, expanding the **Network Threats** section displays three columns: **Local Actions iOS**, **Local Actions Android**, or **Show Notification** columns. These are used to select an action that applies when a threat is detected on a device. The example below displays **Network Threats** as expanded, in the **Danger Zone Connected** row, the **Local Actions iOS** is set to Block Connected Apps and the **Local Actions Android** section is set to Quarantine: Remove Managed apps, and block new downloads.

![Network Threats Table]

**Network, device, and app threats available in Local Actions**

**NOTE:** To select all the actions, select the check box next to the **Name** field. This is a one time action and does not persist after the policy is saved.

**Local Actions Network threats**

The following Network threats are available in Mobile@Work Local Actions:

**TABLE 6. AVAILABLE NETWORK THREAT POLICIES**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Scan</td>
<td>A reconnaissance scan using the ARP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable for a network attack such as man-in-the-middle (MITM).</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Detected that the device connected to a captive portal network.</td>
</tr>
<tr>
<td>Danger Zone Connected</td>
<td>Danger Zone Connected provides device users with information on nearby Wi-Fi networks and their potential risk. If a iOS or Android device user does connect to a malicious Wi-Fi access point, the device user will be notified: “This device has connected to a Wi-Fi network where malicious attacks have been observed. It is recommended to disconnect immediately and use an alternative network.” In order to enable Danger Zone Connected, you must have the <strong>Enable the Danger Zone feature in zIPS</strong> check box selected (located in the <strong>management console &gt; Manage &gt; General tab</strong>.)</td>
</tr>
</tbody>
</table>
For Android release 9.0 through the most recently released version as supported by MobileIron, if the app developer does not add the Access_Coarse_Location permission, then the following zConsole functionality is not enabled:

- Network name and BSSID fields are not available for threat forensics information.
- Network threats are not mitigated.

If zConsole cannot get the BSSID from the device, then the Danger Zone Connection threat will not work.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Scan</td>
<td>A reconnaissance scan using the IP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable for a network attack such as MITM.</td>
</tr>
<tr>
<td>Internal Network Access</td>
<td>Detected application connecting to private, internal servers. It is uncommon for public applications to connect to internal servers. Public applications connecting to internal servers is considered suspicious behavior and should be investigated immediately for the possible threat of malware installed on the device and the risk of data leakage.</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-in-the-Middle attack where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.</td>
</tr>
<tr>
<td>MITM-ARP</td>
<td>Man-in-the-Middle attack using ARP table poisoning where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.</td>
</tr>
<tr>
<td>MITM-Fake SSL certificate</td>
<td>Man-in-the-Middle attack using fake certificate where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.</td>
</tr>
<tr>
<td>MITM-ICMP Redirect</td>
<td>Man-in-the-Middle attack using ICMP protocol where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.</td>
</tr>
<tr>
<td>MITM-SSL Strip</td>
<td>Man-in-the-Middle attack using SSL stripping that allows a hacker to change HTTPS traffic to HTTP so they can hijack traffic and steal credentials or deliver malware to the device.</td>
</tr>
<tr>
<td>Network Handoff</td>
<td>Network handoff allows a device to alter routing on a network, potentially allowing for a man-in-the-middle attack.</td>
</tr>
<tr>
<td>Rogue Access Point</td>
<td>Rogue Access Point exploits a device vulnerability to connect to a previously known Wi-Fi network by masking preferred/known networks.</td>
</tr>
<tr>
<td>Rogue Access Point: Nearby</td>
<td>Rogue Access Point exploits a device vulnerability to connect to a previously known Wi-fi network by masking a nearby network.</td>
</tr>
<tr>
<td>SSL/TLS Downgrade</td>
<td>SSL/TLS Downgrade force apps to use old encryption protocols. These protocols may be vulnerable to attacks that allow third parties to view encrypted information.</td>
</tr>
</tbody>
</table>
Mitigation

Detected

A Device

Existing

Device

Daemon

Developer

A

MobileIron

DNS Configuration

TABLE

The

Local

TABLE

Actions

Device threats

The following Device threats are available in Mobile@Work Local Actions:

Local Actions Device threats

The following Device threats are available in Mobile@Work Local Actions:

Available Network threat policies (Cont.)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Scan</td>
<td>A reconnaissance scan using the TCP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable for a network attack such as MITM.</td>
</tr>
<tr>
<td>UDP Scan</td>
<td>A reconnaissance scan using the UDP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable for a network attack such as MITM.</td>
</tr>
<tr>
<td>Unsecured WiFi Network</td>
<td>A unsecured Wi-Fi network is vulnerable for a network attack.</td>
</tr>
</tbody>
</table>

Available Device threat policies

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal Process Activity</td>
<td>Detected abnormal activity. User device is being monitored for any attacks.</td>
</tr>
<tr>
<td>App Tampering</td>
<td>Existing app libraries may have been modified, or a foreign library may have been injected into the app.</td>
</tr>
<tr>
<td>BlueBorne Vulnerability</td>
<td>MobileIron has detected this device is vulnerable to BlueBorne, an attack leveraging Bluetooth connections to penetrate and take control of targeted devices. To avoid any sort of risk from BlueBorne, it is highly recommended that the user turn off Bluetooth permanently until an update is available from the device manufacturer or wireless carrier. For those users that still require the use of Bluetooth, it is recommended that Bluetooth is turned off until it is needed and only in a trusted and secure area.</td>
</tr>
<tr>
<td>DNS Change</td>
<td>DNS Configuration change on the mobile device. If the DNS change happened in your own network to an unknown DNS server - it is likely to a MITM attempt.</td>
</tr>
<tr>
<td>Daemon Anomaly</td>
<td>Daemon Anomaly indicates abnormal system process activities which could indicate that the device has been exploited.</td>
</tr>
<tr>
<td>Developer Options</td>
<td>Developer Options is an advanced configuration options intended for development purposes only. When enabled, the user has the option to change advanced settings, compromising the integrity of the device settings.</td>
</tr>
<tr>
<td>Device Encryption</td>
<td>Device Encryption notifies an administrator when a device is not setup to use encryption to protect device content.</td>
</tr>
<tr>
<td>Device Pin</td>
<td>Device Pin notifies the administrator when a device is not setup to use a PIN code or password to control access to the device.</td>
</tr>
<tr>
<td>Device jailbreaking/rooting</td>
<td>Jailbreaking and rooting are the processes of gaining unauthorized access or elevated privileges on a system. Jailbreaking and rooting can potentially open</td>
</tr>
</tbody>
</table>
### Table 7: Available Device Threat Policies (Cont.)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security holes that may have not been readily apparent, or undermine the device’s built-in security measures.</td>
</tr>
<tr>
<td>EOP</td>
<td>A malicious process that results in the elevation of privileges on the mobile device, which allows the attacker to take full control of the device.</td>
</tr>
<tr>
<td>File system changed</td>
<td>A normal file system change.</td>
</tr>
<tr>
<td>Gateway Change</td>
<td>Gateway configuration change on the mobile device that can be indicative of sending traffic to a non-intended destination.</td>
</tr>
<tr>
<td>Proxy Change</td>
<td>Proxy configuration change on the mobile device that can be indicative of sending traffic to a non-intended destination.</td>
</tr>
<tr>
<td>SELinux Disabled</td>
<td>Security-enhanced Linux (SELinux) is a security feature in the operating feature in the operating system that helps maintain the integrity of operating system. If SELinux has been disabled, the integrity of the operating system may be compromised and should be investigated immediately.</td>
</tr>
<tr>
<td>Sideloaded App(s)</td>
<td>Sideloaded apps are installed independently of an official app store and can present a security risk.</td>
</tr>
<tr>
<td>Stagefright Vulnerability</td>
<td>Stagefright vulnerability indicates the device is on an OS patch version susceptible to compromise.</td>
</tr>
<tr>
<td>System Tampering</td>
<td>System Tampering is a process of removing security limitations put in by the device manufacturer and indicates that the device is fully compromised and can no longer be trusted.</td>
</tr>
<tr>
<td>USB Debugging Mode</td>
<td>USB Debugging is an advanced configuration option intended for development purposes only. By enabling USB Debugging, the user device can accept commands from a computer when plugged into a USB connection.</td>
</tr>
<tr>
<td>Unknown sources download config change</td>
<td>Allows user to download an app not in Google Play store.</td>
</tr>
<tr>
<td>Vulnerable Android Version</td>
<td>MobileIron has detected that the Android version installed on your device is not up-to-date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update the device's operating system immediately.</td>
</tr>
<tr>
<td>Vulnerable iOS Version</td>
<td>MobileIron has detected that the iOS version installed on your device is not up-to-date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update the device’s operating system immediately.</td>
</tr>
<tr>
<td>Vulnerable, non-upgradeable Android Version</td>
<td>MobileIron detected a device running a vulnerable Android version. However, the device is not eligible for an operating system upgrade at this time.</td>
</tr>
</tbody>
</table>
Local Actions App threats

The following App threats are available in Mobile@Work Local Actions:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable, non-</td>
<td>MobileIron detected a device running a vulnerable iOS version. However, the device is not eligible for an operating system upgrade at this time.</td>
</tr>
<tr>
<td>upgradeable iOS Version</td>
<td></td>
</tr>
</tbody>
</table>

Next steps

Proceed to either Using zConsole to monitor threats to Android devices or Using zConsole to monitor threats to iOS devices.

Editing an MTD Local Actions threat defense policy

This section addresses how to edit a MobileIron Threat Defense Local Actions policy.

Procedure

1. Select Policies & Configs > Policies
2. Select the check box next to the MTD policy that you want to edit. The Policy Details panel displays on the right of the page.
3. Click Edit. The Edit MTD Local Actions Policy dialog box opens.
4. Enter the changes.

5. To choose multiple threats actions, select the check box to the left of the threat and then use the Actions drop-down menu to select multiple actions for the threat.

6. Click Save.

Checking MobileIron Threat Defense status

To confirm MTD status from the Core admin portal for a particular device, use one of the following options:

- Checking individual devices
- Using Advanced Search

Checking individual devices

Procedure

1. Select Devices & Users > Devices, and click the carat (▲) next to the relevant device. The Device Details tab displays.

2. Scroll until you see MobileIron Threat Defense Status field and look at the value (see table below.)
### MTD Status on the Device Details Tab

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Definition</th>
<th>Location of Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected</td>
<td>MTD license activation successful. User device is protected.</td>
<td>User device and Core &gt; Device Details page.</td>
</tr>
<tr>
<td>Pending</td>
<td>MTD license key has been sent, awaiting confirmation from zConsole.</td>
<td>Core &gt; Device Details page (&quot;Pending&quot;)</td>
</tr>
<tr>
<td>License Key Error</td>
<td>License key error. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected due to a license key error.&quot;</td>
</tr>
<tr>
<td>License Not Activated</td>
<td>MTD license key to zConsole failed. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not because the license could not be activated.&quot;</td>
</tr>
<tr>
<td>Simulator Error</td>
<td>Internal error.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected due to a simulator error.&quot;</td>
</tr>
<tr>
<td>Connection Error</td>
<td>Connection error. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected due to a connection error.&quot;</td>
</tr>
<tr>
<td>License Expired</td>
<td>License has expired. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected because the license has expired.&quot;</td>
</tr>
<tr>
<td>Login Cancelled (Android only)</td>
<td>Too many logins. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected due to a cancelled login.&quot;</td>
</tr>
<tr>
<td>License Invalid</td>
<td>Invalid license key. The user device is not protected.</td>
<td>Core &gt; Device Details page (&quot;Error&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User device – &quot;MobileIron Threat Defense detected that your device is not protected&quot;</td>
</tr>
</tbody>
</table>
### Using Advanced Search

Using Advanced Search is helpful for searching through a large amount of devices.

**Procedure**

1. Select **Devices & Users > Devices**, and click the carat (^) next to the relevant device. The **Device Details** tab displays.
2. Click **All** to combine the criteria with a logical AND. Click **Any** to combine the criteria with OR.
3. In Field, type in MobileIron Threat Defense Status or select **Common Fields > MobileIron Threat Defense Status**.
4. Select an operator, such as **Equals**.
5. In the Select Type field, choose the Value to search on. The predetermined values that you can select are:
   - **Protected**: Indicates the MTD activation token has been sent to the device, the token is valid, MTD is activated and scanning is operating on the device.
   - **N/A**: Indicates that there is no MobileIron Threat Defense configuration on the device.
   - **Error**: Indicates the MTD activation token has been sent to the device but there were errors. Threat scanning is not enabled. See the table in **Device, Network, and App threats for iOS clients** for definitions of error messages.
   - **Unknown**: Indicates MTD Activation token accepted but the status of MTD scanning on the device is unknown. Not applicable to iOS devices.
6. Click **Search**. The results display in the bottom half of the screen.
Configuring Phishing Protection in Core

MobileIron Threat Defense Solution detects and prevents phishing attempts on MTD-enabled devices. Administrators can set up the anti-phishing capability in such a way that an unsafe URL gets blocked and the device user is prevented from accessing it. When a device user taps / clicks a malicious URL, access to the site is blocked with a pop-up message indicating that it contains malicious content that could steal sensitive or private content from the user device.

Phishing protection on MTD-enabled devices is enabled if:

- MTD is configured and enabled. See MobileIron Threat Defense prerequisites.
- The Anti-phishing Protection policy is enabled. See Enabling Phishing Protection in MobileIron Core.
- The MobileIron client is set as the default browser in the Settings app, as applicable, or the MobileIron client is chosen by the device user to handle the URL clicks.

If the anti-phishing policy is removed from Core, the policy will be uninstalled from the user's device and:

- **Android devices** - the URL intercepting activity will be disabled.
- **Android Enterprise** - the URL intercepting activity will be disabled and will be removed from the Device Policy Manager.
- **iOS devices** - the URL intercepting activity will be disabled.

If MobileIron Threat Defense configuration is removed after anti-phishing policy was applied to the device, the anti-phishing configuration will be considered non-compliant. In this case, Mobile@Work will report an "install error" to the server. If the device user taps on a URL, the scan result will return an error, but the user will be allowed to continue to the URL unprotected.

**NOTE:** The MobileIron Threat Defense Solution Anti-Phishing policy can show and track devices from Android version 7 through the most recently released version as supported by MobileIron. Earlier versions are not supported.

Using a remote database to validate URLs

This procedure is applicable to Android client devices.

By default, phishing policy is configured to use an on-device database for detecting phishing URLs. If you would prefer your Android devices to have access to a much larger, real-time updated database, you can configure this through the Zimperium management console (zConsole).
**Procedure**

1. Log in to the zConsole.
2. Navigate to Policy > Phishing Policy.
3. Select the device group you want in the policy.
4. Select these options:
   - Enable User-initiated URL Sharing
   - Enable content inspection on remote server
5. Deploy the changes.

**Anti-Phishing for iOS devices**

This section covers anti-phishing protection functionality for iOS devices.

**How MobileIron Phishing Protection for iOS works**

1. In the Admin portal, you create a MTD anti-phishing policy to ensure that device users will be blocked from visiting malicious URLs.
2. A notification is sent to users’ devices, stating that the MobileIron Phishing Protection has been enabled and the device user is invited to activate it on the device.
3. Users successfully enable MobileIron Phishing Protection on their devices. Content Blocker is applicable for URLs accessible from the Safari browser.
   
   **NOTE:** The administrator will be able to tell if the device user enabled the MobileIron Phishing Protection by checking the Device Details page in Core.
4. When the device user taps on a URL, the MobileIron Phishing Protection is triggered. Mobile@Work passes the URL to the Safari browser to display the URL. When the browser opens, the device displays a "Page Blocked by Content Blocker” page. This is applicable to whether a device user taps on a URL or if an app attempts to go to the malicious URL.
   
   **NOTE:** If the MTD Anti-Phishing policy does not exist, does not have a label applied to it, OR is inactive and the device user enables the MobileIron Content Blocker in the user’s selected browser, the client will not send any status to the server and will NOT block the malicious sites. While the MTD Anti-Phishing policy is in any of the above three states and the Content Blocker is enabled by the device user, the client will continue to display “Enabled” but will NOT block the sites.

**Enabling Phishing Protection in MobileIron Core**

**Procedure**

1. From the admin portal, go to Policy & Configs > Policies.
2. Click Add New > MTD Anti-Phishing.
3. In the Create Anti-phishing Protection Configuration dialog box, enter a name for the policy.
4. For status select Active. This is the default setting.
   NOTE: Only one active policy can be applied to a device.
5. Specify a priority for this policy, relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available.
6. Select Higher than or Lower than, then select an existing policy from the drop-down list.
7. (Optional) Enter a description.
8. Click Save.
9. Apply a label to the policy.
10. Create a compliance policy rule to ensure that device users enable MobileIron Phishing Protection. See Creating compliance policy rules and groups. Give the policy the following settings:
    a. Condition: MTD Anti-Phishing status / Equals / Not Enabled
    b. Regular Expression: "common.mtd_anti_phishing_status"="CLIENT_NOT_ENABLED"
       This expression makes the devices go out of compliance, and it triggers a compliance action that forces device users to enable MobileIron phishing protection.
11. Force device check in.
    To get the device back in compliance, device users will need to re-enable MobileIron as the default content blocker / URL handler. Device users tap on the MobileIron logo, and follow the provided instructions.

**Anti-Phishing for Android and Android Enterprise devices**

This section covers anti-phishing protection functionality for Android and Android Enterprise devices.

MobileIron tries to establish itself as the default URL interceptor to provide phishing protection so that it can scan the URL and block the URL if it is unsafe. On Android devices managed in MobileIron Core, phishing protection cannot be provided if the end-user types-in the URL in a browser directly.

NOTE: Although MobileIron clients implement phishing protection, if a third-party app opens a URL in its in-app browser, the MobileIron client cannot provide the phishing protection.

**Before you begin**

- Be sure that Android Enterprise is installed on Core. See “Setting up MobileIron Core for Android enterprise” in the **MobileIron Core Device Management Guide for Android and Android enterprise Devices**.
- An understanding about deployment models for Android devices and modes is necessary.
  - For information about Android deployment devices, see "Android Deployment Models" in the **MobileIron Core Device Management Guide for Android and Android enterprise Devices**.
  - For information about modes for Android enterprise devices, see "Android enterprise overview” in the **MobileIron Core Device Management Guide for Android and Android enterprise Devices**.
How MobileIron Phishing Protection for Android works

1. In the Admin portal, you create an MTD anti-phishing policy to ensure that device users will be blocked from malicious URLs.

2. Device users enable MobileIron Phishing Protection.
   a. **Android native and Android Knox**: A notification is sent to users’ devices stating that the MobileIron Phishing Protection has been enabled and the device user is invited to activate it on the device. During this process, the device user is asked to select a default browser. It is recommended the device user selects Mobile@Work as the default browser. The user’s choice of browser is saved in the device.

   **NOTE**: If the device user does not enable MobileIron Phishing Protection or the device is considered non-compliant, the end user will not be asked to set Mobile@Work as the default browser.

   b. **Android Enterprise**: MobileIron Phishing Protection is silently enabled on the user device with Mobile@Work set as the default browser.

   **NOTE**: To verify if a device user enabled MobileIron Phishing Protection, see Device Details page in MobileIron Core.

3. When the device user taps on a URL, MobileIron Phishing Protection is triggered. The default browser intercepts the URL, scans it, and if malicious, blocks it. Otherwise, the URL opens in an installed browser. Mobile@Work passes it on to an installed browser (if there is only one browser on the device) or a list of browsers displays (if there are multiple browsers on the device). The user’s choice of browser is saved in the device.

4. Refer to the table for a list of Android versions for default browser.

   **NOTE**: For Android 5.x devices, there is no default browser app settings.

<table>
<thead>
<tr>
<th>Device Mode</th>
<th>How to select MobileIron client as the default browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Admin mode</td>
<td><strong>Android 7.0+</strong>: User will be guided to select MobileIron client as the default browser app from the default apps settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Android 6.x</strong>: User will be guided to select MobileIron client as the default browser from the main Settings by searching and navigating from the default apps settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Android 5.x</strong>: User has to select MobileIron client from the list of browsers displayed by Android.</td>
</tr>
<tr>
<td>Work Profile (Profile Owner)</td>
<td><strong>Android Enterprise</strong>: MobileIron client will be set as the default browser. Only if it gets cleared from Settings, user will be prompted to set MobileIron client as the default browser.</td>
</tr>
<tr>
<td>(Android 5.0 through the latest version as supported by MobileIron)</td>
<td></td>
</tr>
</tbody>
</table>

MobileIron Threat Defense Solution Guide for Core | 61
<table>
<thead>
<tr>
<th>Device Mode</th>
<th>How to select MobileIron client as the default browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Device (Device Owner) (Android 5.0 through the latest version as supported by MobileIron)</td>
<td>For both device side and profile side, MobileIron client will be set as the default browser in Settings, except in Samsung devices. In Samsung devices, user has to explicitly choose MobileIron client as the default browser in the device Settings and work Settings. The work settings and device settings for the browser app are not in the same Settings page.</td>
</tr>
</tbody>
</table>
| Managed Device with Profile Owner (Android 8.0 through the latest version as supported by MobileIron) | MobileIron recommends distributing MobileIron Web@Work and enabling the following in the Global AppConnect policy for anti-phishing protection:  
  - **Allow Web** - If enabled, an unsecured browser can attempt to display a web page when a device user taps the page’s URL in a secure app.  
  - **Allow non-AppConnect apps to launch URL using Web@Work** - This will ensure that on URL clicks inside and outside the container, MobileIron client can intercept the URL for phishing protection and use the installed Web@Work to display the safe URLs. For more information, see the AppConnect section in the MobileIron Core product documentation. MobileIron Support credentials are required to access documentation in the Support Community. |
| AppConnect (Android 5.0 through the latest version as supported by MobileIron) |  |

After MobileIron client has been set or selected as the default browser to provide phishing protection:

**Kiosk** (Samsung devices from Android 5 to 8 and non-Samsung devices from Android 5 to 7) and **Kiosk Android enterprise Device Owner mode** (Android 5.0 through the latest version as supported by MobileIron): When URL clicks are inside the kiosk, if the URL is safe, it will display with browsers available in the kiosk mode. Kiosk mode remains active and functional if the phishing protection was enabled outside the kiosk and then removed while the device is in kiosk mode. Exiting in and out of kiosk mode keeps the phishing protection functional inside and outside the kiosk.

When a user taps a URL:

- If the URL is not safe, it will be blocked.
- If the URL is safe, MobileIron client will render the URL with the browser available or display a list of browsers for end user to choose to display URLs “Just Once” or “Always”.  
  - **Just Once** – MobileIron will continue to show a list of browsers if there are multiple browsers.  
  - **Always** – MobileIron client will save the selected browser. Next time, the saved browser package is used to render safe URLs.
NOTE: Once the user selects "Always" through the MobileIron client's list of browsers, the user cannot change the default browser for rendering safe URLs. As a workaround, install a new browser. On clicking the next safe URL, the user will be again shown a list of browsers, including the new browser.

Phishing Protection Status

MobileIron Phishing Protection requires device users to manually activate Phishing Protection. Admins can check on the anti-phishing status of devices from two places:

- Admin Portal > Devices and Users > Devices. See Device Details page.
- Admin Portal > Dashboard Devices. See Using the Phishing Protection Dashboard to monitor enrollment.

The MobileIron Phishing Protection status is available as a device attribute when creating custom policies. Administrators can set a rule in the custom policy using the status, so that actions can be taken against devices that do not have phishing protection enabled.

For more information, see the Policies and Configurations sections in the MobileIron Core product documentation. MobileIron Support credentials are required to access documentation in the Support Community.

Device Details page

After choosing Force Device Check in, you can verify that the anti-phishing policy is enabled on a given device by checking the device details for that device.

Procedure

1. From the MobileIron Core Admin Portal, select Devices & Users > Devices.
2. Click the carat (^) next to the relevant MTD-enabled device.
3. Under Device Details, MTD Anti-Phishing Status will also display the current status in one of the following values:
   - N/A – The MobileIron Phishing Protection configuration is not distributed by the admin or the configuration is not applied.
   - Enabled – Device users received a request from the administrator to manually activate MobileIron Phishing Protection and have done it.
   - Not Enabled – Device users received a request from the administrator to manually activate MobileIron Phishing Protection and have NOT done it.
   - Unknown – Device users have likely not set the device's default browser to Mobile@Work, and therefore, not enabled MobileIron Phishing Protection.

Using the Phishing Protection Dashboard to monitor enrollment

By using the Phishing Protection Dashboard, you can track how many users have enabled MobileIron phishing protection on their iOS and Android devices. This dashboard provides the following information:
- Total number of device users that have MobileIron phishing protection enabled
- Total number of device users that do NOT have MobileIron phishing protection enabled.

This feature is applicable on Android devices running OS 7 through the most recently released version as supported by MobileIron. Due to platform limitations, Core is not able to accurately track anti-phishing enablement status for devices running Android 6 and earlier OS versions.

Before you begin

You must have completed the following:

- Activated MobileIron Threat Defense
- Created a MobileIron Threat Defense policy
- Created an MTD Anti-Phishing policy

Procedure

1. In the MobileIron Core Admin portal, go to Dashboard > Devices.
2. Click Add.
   - The Add Chart dialog box opens.
3. Choose Devices by Phishing Protection Enabled in the Chart Type field and then click Add Chart.
4. The Devices by Phishing Protection Enabled chart displays on the dashboard (may need to scroll).
5. The pie chart indicates the following information: Enabled, Not Enabled, Unknown. See Device Details page for field definitions.
6. Clicking on a section of the chart opens the Device Details page, where you can view the status in the Phishing Protection Enablement column (Yes/No).
   - NOTE: If you add the MobileIron Phishing Protection chart in the dashboard and MTD is not activated, the chart will display “MobileIron Threat Defense not enabled.”

Updating the MTD Local Actions policy when new threat list is available

Zimperium management console (zConsole) provides the threat definitions list and the list is uploaded to the Apps Gateway. The list is updated when new threats are identified or existing threats are removed.

After you have configured an MTD Local Actions policy, applied label(s), and sent the configuration to the devices, you will need to update the MTD Local Actions policy with the new threat list. When it becomes available, the new threat list will contain deleted threats that were enabled previously.
Before you begin

Be sure you have completed either Using zConsole to monitor threats to Android devices or Using zConsole to monitor threats to iOS devices.

Procedure

1. In Core, select Policies & Configs > Policies.
2. Select the MTD Local Actions policy link and then select Edit. See Creating MTD Local Actions threat defense policy in Core for details.
3. Enter the changes and click Save.
Managing user privacy

MobileIron Threat Defense has policies and tools to provide elevated levels of privacy for MTD clients who require higher data privacy standards.

Managing EU users under GDPR

European Union (EU) members have additional data protection rights under the General Data Protection Regulation (GDPR) standard. The MobileIron GDPR profile protects member data from being exposed to integration partners, API developers and administrators.

- Enabling the GDPR Profile
- Assigning users to a GDPR profile

Enabling the GDPR Profile

Before you can assign the GDPR profile to a user, you must enable the feature in Core, and select which fields should be visible, and which should not.

Procedure

1. From the MobileIron Core Admin Portal, navigate to Settings > Users & Devices > GDPR profile.
2. Click GDPR Profile. The GDPR Profile page displays.
3. Click Enable GDPR Profiles to be assigned to users. The Default GDPR Profile options display. By default, all of the fields are selected.
4. Click the blue pencil in the upper-right corner to edit the profile defaults.
5. Disable GDPR for any fields that you do not want to hide by deselecting the check box for the field.
   Field options include:
   - User ID
   - Person Name
   - Email address
   - Phone Number
   - International Mobile Equipment Identity (IMEI)
   - Serial Number
   - Integrated Circuit Card ID (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Mobile Equipment Identifier (MEID)

NOTE: When hidden, the serial number and IMEI display as empty fields, the rest as asterisks: *****

6. Click Save.
Your GDPR profile elections display. In this example, the User ID will display in clear text, but the other fields will be hidden.

GDPR Profile

Assigning users to a GDPR profile

Once the GDPR profile is enabled, you must assign API users to it.

When the GDPR profile is enabled for a user, some functionality and edit rights in the Core Devices and Users pages are restricted. GDPR-enabled users will see an orange banner across the top of MobileIron Core, reminding them that these restrictions are in place.

**Figure 4. GDPR reminder banner**

GDPR profile enabled - Some functionality and edit rights are restricted. Contact your Administrator for more information

Procedure

1. From the MobileIron Core Admin Portal, navigate to Devices & Users > Users. The Users page displays.
2. Click the pencil icon to the left of the user name to edit the user profile. The Edit User dialog box opens.
3. Click Enable GDPR to assign a user to the GDPR profile.
4. Click **Save**.
   The Users page now displays **Yes** in the **GDPR Profile Enabled** column for users you have enabled.

5. Once GDPR has been enabled for an admin or API user, they will not be able to see device and user information. When they navigate to Devices & Users > Devices, the GDPR fields display as asterisks, or a blank field.
Using Zimperium management console (zConsole)

This section describes how to set up, configure, and use the zConsole for supported MobileIron Threat Defense activities.

**FIGURE 5. zConsole Threat Log**

![](image)

**Configuring zConsole**

The zConsole **Manage** page provides a way for you, acting as the administrator, to configure privacy and VPN settings for the environment, as well as a view to the audit logs that collect all activity on the active devices.

**General Settings**

The **Manage > General** tab provides basic information about the environment and an alternate location for modifying the selected language. It also provides the option to change the administrator password.
Here are specific configuration elements for the General tab:

- **Preferred Language:** Choose the language for the zConsole. The current options are English, Japanese or Hebrew.

- **Password Policy:** Define the following password requirements for the zConsole admin:
  - Minimum password length
  - Required password elements
  - Maximum repeating characters
  - Verify that the new password was not used in the past “X” passwords
  - Define how often the password must be changed
  - Define how many failed attempts prior to triggering an account lock
  - Define the account lock out time in minutes

- **Danger Zone Connected:** to enable Danger Zone, the *Enable the Danger Zone feature in zIPS* check box must be selected. Select **Save**.

- **Site Insight:** enable to check malicious URLs
  - **Android** - when enabled, URL requests are intercepted from non-browser apps to validate the requests are not malicious.
- **iOS** - when enabled, if a malicious URL is found, the iOS device user is alerted and actions are taken according to the settings in MTD.

### Managing Devices in zConsole

The Devices page displays the complete list of devices that are configured in this environment. Devices automatically appear in this page because an MTD-enabled new client has checked in. In addition, this page lists devices that are synchronized with MobileIron Core. The greyed out devices in the listing are devices that have synchronized with Core, but have not yet checked in.

The device information includes the following:

- **Risk Posture** (For example, Low, Elevated, Critical)
- **User**
- **Group**
- **OS** (Version of the device)
- **Upgradeable OS** (Yes, No, or N/A)
- **Device ID**
- **Model** (for example, iPhone, Nexus 5)
- **App Version** (of Mobile@Work)
- **Privileges** (for example, Rooted, Jailbroken, No Jailbroken)
- **Operational Mode** (Inactive, Active)
- **Last Seen** (Last date and time the device was seen by Mobile@Work, via check-in or from an event communication)

The Risk Posture of the device signals the highest level of a pending event seen for the device at the time of viewing. If the Risk Posture of the device is Elevated and a Critical event is detected, then the device has a new Risk Posture of Critical.
General Display Filters

Below is a list of the general display filters:

- **Profiles**: To display a list of iOS Devices that have specific profiles installed, click the Profiles option near the top of the screen and select the profiles of interest. A list of devices that have the selected profiles installed displays.

- **Apps**: To display a list of devices that have specific apps installed, click the Apps option near the top of the screen and select the apps of interest. A list of devices that have the selected apps installed displays.

- **Patch Date**: To display a list of devices that have a specific patch date, click the Patch Date option near the top of the screen and select the desired options. A list of devices that have the selected patch date displays.

The following table shows the columns included in the Devices page filter.

**TABLE 10. DEVICES PAGE FILTER**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Posture</td>
<td>Display devices that match the selected risk posture or postures</td>
</tr>
<tr>
<td>User</td>
<td>Display devices that match the selected user or users</td>
</tr>
<tr>
<td>Group</td>
<td>Displays the devices that match the selected management console groups</td>
</tr>
<tr>
<td>OS</td>
<td>Displays devices that match the selected OS versions</td>
</tr>
<tr>
<td>Upgradable</td>
<td>Displays devices that match the selected upgradable flag value</td>
</tr>
<tr>
<td>Device ID</td>
<td>Displays devices that match the selected device IDs</td>
</tr>
</tbody>
</table>
TABLE 10. Devices Page Filter (Cont.)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Name</td>
<td>Displays devices running the selected Mobile@Work app</td>
</tr>
<tr>
<td>App Version</td>
<td>Displays devices running the selected versions of the Mobile@Work app</td>
</tr>
<tr>
<td>Privileges</td>
<td>Displays devices that are jail-broken or rooted</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>This column displays the following:</td>
</tr>
<tr>
<td></td>
<td>Active: describes devices that are communicating on a regular basis to the</td>
</tr>
<tr>
<td></td>
<td>management console</td>
</tr>
<tr>
<td></td>
<td>Inactive: describes devices that have been active but are now not</td>
</tr>
<tr>
<td></td>
<td>communicating</td>
</tr>
<tr>
<td></td>
<td>Pending Activation: describes devices that have synchronized through</td>
</tr>
<tr>
<td></td>
<td>Core, but have not yet checked in.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Sorts by the date or time the filtered devices were last seen</td>
</tr>
</tbody>
</table>

You can export the listing(s) with the export icon. This export includes the filtered device list only and is downloaded as a CSV file via a link sent to the administrator’s email address.

**FIGURE 8. EXPORT AS CSV ICON**

![CSV Icon](image)

Clicking on a device opens the Device Details panel. Details about the device, including vulnerable configuration items and alerts, are displayed. At the bottom of the window are some actions and items that can display additional information about the device:

- To show threats for this device, click the **Show threats for this device** link. If no threats are available, the “No Threats detected for this device” message displays.
- Click **Logout** and choose the Mobile@Work application and a message that is sent to the user when completed.
- The **Device Info** option provides more specific information about the device such as the cell phone, carrier, and country information.

**Using zConsole to monitor threats to Android devices**

After configuring MobileIron Core as your MDM server in zConsole, and distributing Mobile@Work with MobileIron Threat Defense configured and activated, you can use zConsole to monitor threats to connected networks, apps, and devices. You will be able to view the following on zConsole:
- MTD-enabled devices that are registered with Core
- Networks
- Projected threat levels for devices and apps
- Core labels you selected during configuration, shown in zConsole as groups

NOTE: Every time you log in, zConsole generates a new MTD Activation token for Core that differs from the original MTD Activation token. Any new codes that zConsole generates are valid. The original code from MobileIron continues to be valid.

Related topics

Updating the MTD Local Actions policy when new threat list is available.

Whitelisting a sideloaded app for Android devices

If the Sideloaded App threat is enabled through the zConsole, when Mobile@Work for Android users install an app on their phone that wasn’t downloaded from the Windows App Store or Google Play Store (including Mobile@Work for Android), it triggers a "sideloaded app" threat. If a sideloaded app is approved for your organization and you want to whitelist (allow) it, you can configure this on the zConsole before or after it is installed on a device.

NOTE: If you chose not to whitelist UEM-managed apps through zConsole, Sideloaded App threats should not be bound to any compliance action.

Whitelisting an app prior to installation

Procedure

1. From the zConsole, click APPS.
2. Find an app that you want to whitelist.
3. Click the three-dot menu on the far right of the row, and select Allow / Deny.
4. From the Allow / Deny popup menu:
   a. Select Entire App Bundle, to prevent app threats from these apps displaying on client apps and in zConsole.
   b. Select ALLOW to whitelist the app.
5. Click Save to apply the changes.

Whitelisting an app after installation

Procedure

1. From the zConsole, click THREAT LOG.
2. Select the sideloaded app that you want to whitelist.
3. From the Actions menu, select **Whitelist App Developer**.
   Your selection is saved automatically.

**Using zConsole to monitor threats to iOS devices**

After configuring Core as your MDM server in zConsole, and distributing Mobile@Work with MobileIron Threat Defense, you can use zConsole to monitor threats to connected networks, managed iOS apps, and devices. You will be able to view the following on zConsole:

- Managed Core devices
- Managed apps on Core devices
- Networks
- Projected threat levels for devices and apps
- Core labels you selected during configuration, shown in zConsole as groups

Note The Following:

- Be sure you have completed **Creating MTD Local Actions threat defense policy in Core**.
- Every time you log in to zConsole, it generates a new MTD Activation token for Core that differs from the original MTD Activation token. Any new codes that zConsole generates are valid. The original code continues to be valid.

**Setting the Sinkhole action on iOS devices**

Of the three categories of MTD threats—device, network, and application—network threats can be mitigated using a sinkhole VPN profile in the MTD response policy. See **Creating MTD Local Actions threat defense policy in Core**

**NOTE:** MobileIron recommends that you select the sinkhole action only for network threats.

The process works like this:

1. When a threat is detected on the device and a Network Sinkhole action is associated with this threat in the MTD policy, the threat triggers the MobileIron Defender VPN profile to isolate the device from the network.
2. While the Network Sinkhole action is active on the device, be aware of the following issues:
   - Other threats may not be detected and displayed until the original threat that caused the compliance action to be taken is remediated.
   - The full list of threats may not display on the iOS device.
3. After the threat is remediated on the device, the VPN profile is disabled automatically and network traffic is no longer affected by the sinkhole. At this point, browser traffic now succeeds.

**NOTE:** If Core access to the App Gateway is blocked, the threat list is not displayed and the MTD local action policy cannot be created.

**Next Steps:** Proceed to **Updating the MTD Local Actions policy when new threat list is available**.
Administering Mobile@Work

This section includes information and tasks that MTD administrators may find helpful when troubleshooting Mobile@Work clients. We will be adding more information as the opportunity arises. For more MTD documentation, knowledge base articles, product bulletins, and forum groups, see https://help.mobileiron.com/s/product-detail?Id=a1s3400000240hOAAQ.

Logging and enhanced logging for iOS clients

If iOS device users experience issues with the Mobile@Work client, they can reproduce the issue and send the logs to their administrator. Enhanced Logging encrypts the logs for safe transport to the support Admin.

NOTE: This feature is for troubleshooting, and is disabled by default.

Sending Mobile@Work logs to MobileIron Support

Procedure

1. Open Mobile@Work.
2. Tap Settings.
3. To enable debug-level encrypted logging of your phone information, tap Enhanced Logging.
   If you do not require encryption, make sure Enhanced Logging is toggled off.
4. Reproduce the issue on the device.
5. Go back to Mobile@Work, and tap Settings > Send MobileIron Go Logs.
   Select a method to send the log information to MobileIron support. Options include email, SMS, AirDrop, and others.
6. Enter a support address and tap Send.
**MTD Support for Android 10**

MobileIron Threat Defense supports Android 10 OS with the following configuration caveats:

**Table 11. Expected behavior for new and upgraded Android 10 installations**

<table>
<thead>
<tr>
<th>Deployment mode</th>
<th>Expected behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>All modes</td>
<td>The local action <strong>Disconnect Wi-Fi</strong> cannot be applied to Android 10 devices.</td>
</tr>
<tr>
<td>Android enterprise modes (AE)</td>
<td>If location services are not enabled in Android enterprise mode, the threats <strong>Unsecured Wi-Fi</strong> and <strong>Rogue Access Point</strong> are not detected.</td>
</tr>
<tr>
<td>AE Profile Owner mode (PO)</td>
<td>During installation or upgrade of the client on Android 10, the user is prompted to turn on location services for both device and profile settings:</td>
</tr>
<tr>
<td></td>
<td>• If the user agrees, the app opens the device location service setting, so the user can enable it.</td>
</tr>
<tr>
<td></td>
<td>To complete the process, the user must manually navigate to the Profile settings to enable location services for the Profile.</td>
</tr>
<tr>
<td></td>
<td>• If the user does not enable the location services, <strong>Unsecured Wi-Fi</strong> and <strong>Rogue Access Point</strong> threats are not detected.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If <strong>Disallow share location</strong> is enabled in the <strong>PO lockdown</strong> config, this will block the user’s ability to turn on location services. Uncheck this feature to prompt the user to enable location services.</td>
</tr>
<tr>
<td>AE Work profile modes</td>
<td>Location settings are enabled without user action, allowing MTD detection of all network threats.</td>
</tr>
<tr>
<td>Device Owner (DO)</td>
<td></td>
</tr>
<tr>
<td>Managed device (COPE)</td>
<td></td>
</tr>
<tr>
<td>Device administrator mode (DA)</td>
<td><strong>Unsecured Wi-Fi</strong> and <strong>Rogue Access Point</strong> network threats cannot be detected for these devices.</td>
</tr>
<tr>
<td>Mobile application management mode (MAM)</td>
<td><strong>Unsecured Wi-Fi</strong> and <strong>Rogue Access Point</strong> network threats cannot be detected for these devices.</td>
</tr>
</tbody>
</table>

For full information about MobileIron support for Android devices, see the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*. 