MobileIron Threat Defense Solution Guide for Core 10.8.0.0

Mobile@Work 10.8.0.0 for Android
Mobile@Work 12.4.0 for iOS

Revised November 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>November 5, 2020</td>
<td>Incorporated review comments from MobileIron Professional Services.</td>
</tr>
<tr>
<td>November 19, 2020</td>
<td>Modified &quot;Assigning space and roles to an MTD administrator&quot; and added a known issue.</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>MTD features and enhancements for iOS devices</td>
<td>8</td>
</tr>
<tr>
<td>Advanced multi-level phishing protection</td>
<td>8</td>
</tr>
<tr>
<td>Mobile@Work sinkhole compliance VPN without user action</td>
<td>9</td>
</tr>
<tr>
<td>Risky link notifications display within client app</td>
<td>9</td>
</tr>
<tr>
<td>MTD wake-up interval increased to 60 minutes</td>
<td>9</td>
</tr>
<tr>
<td>Users can disconnect MobileIron anti-phishing VPN by connecting to a different VPN provider</td>
<td>10</td>
</tr>
<tr>
<td>MTD features and enhancements for Android devices</td>
<td>10</td>
</tr>
<tr>
<td>Additional network threats for Android devices</td>
<td>10</td>
</tr>
<tr>
<td>General MTD features and enhancements</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 through the Threat Management Console and local actions</td>
<td>12</td>
</tr>
<tr>
<td>MTD license determines functionality</td>
<td>13</td>
</tr>
<tr>
<td>MobileIron Threat Defense prerequisites</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Privacy policy</td>
<td>14</td>
</tr>
<tr>
<td>Creating an MTD admin</td>
<td>15</td>
</tr>
<tr>
<td>Assigning a space and roles to an MTD administrator</td>
<td>15</td>
</tr>
<tr>
<td>Enabling CPS messaging on MobileIron Core</td>
<td>16</td>
</tr>
<tr>
<td>Adding Core as your MDM server in Threat Management Console</td>
<td>17</td>
</tr>
<tr>
<td>Allowing access to the App Gateway</td>
<td>18</td>
</tr>
<tr>
<td>External and Internet rules</td>
<td>18</td>
</tr>
<tr>
<td>Additional Firewall Rules</td>
<td>20</td>
</tr>
<tr>
<td>Enabling MTD for Mobile@Work devices</td>
<td>22</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Creating an MTD activation configuration</td>
<td>22</td>
</tr>
<tr>
<td>Pushing new MTD activation configurations to existing devices</td>
<td>23</td>
</tr>
<tr>
<td>Android</td>
<td>23</td>
</tr>
<tr>
<td>iOS</td>
<td>23</td>
</tr>
<tr>
<td>Disabling MTD on MobileIron Core</td>
<td>23</td>
</tr>
<tr>
<td>Verify that MobileIron Threat Defense is working</td>
<td>23</td>
</tr>
<tr>
<td>Verify that MTD is working on a device</td>
<td>24</td>
</tr>
<tr>
<td>Verify MTD on all devices: force device check-in</td>
<td>24</td>
</tr>
<tr>
<td>Defining policies</td>
<td>25</td>
</tr>
<tr>
<td>Setting the MTD wake-up interval for iOS devices</td>
<td>25</td>
</tr>
<tr>
<td>Creating event notifications</td>
<td>25</td>
</tr>
<tr>
<td>Server-initiated mitigation and compliance</td>
<td>28</td>
</tr>
<tr>
<td>Creating MTD labels in Core</td>
<td>28</td>
</tr>
<tr>
<td>Creating and applying server-initiated multi-tier compliance actions</td>
<td>29</td>
</tr>
<tr>
<td>Quarantine compliance action</td>
<td>30</td>
</tr>
<tr>
<td>Tiered compliance action - 4 hours</td>
<td>30</td>
</tr>
<tr>
<td>Configuring the Threat Management Console Mobile Threat Response Policy</td>
<td>31</td>
</tr>
<tr>
<td>Set device action</td>
<td>33</td>
</tr>
<tr>
<td>MDM action</td>
<td>34</td>
</tr>
<tr>
<td>Mitigation action</td>
<td>34</td>
</tr>
<tr>
<td>Notifications</td>
<td>35</td>
</tr>
<tr>
<td>Updating Core sync policy</td>
<td>35</td>
</tr>
<tr>
<td>Configuring device scanning frequency for threat scan</td>
<td>35</td>
</tr>
<tr>
<td>Phishing protection for MTD devices</td>
<td>37</td>
</tr>
<tr>
<td>Advanced phishing protection for iOS devices</td>
<td>37</td>
</tr>
<tr>
<td>Enable Threat Management Console anti-phishing VPN</td>
<td>37</td>
</tr>
<tr>
<td>Enabling additional MTD anti-phishing protection</td>
<td>39</td>
</tr>
<tr>
<td>Anti-phishing for Android and Android Enterprise devices</td>
<td>40</td>
</tr>
<tr>
<td>How MobileIron phishing protection for Android works</td>
<td>41</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Device Details page</td>
<td>43</td>
</tr>
<tr>
<td>Additional Android phishing configuration tasks</td>
<td>44</td>
</tr>
<tr>
<td>Using a remote database to validate URLs</td>
<td>45</td>
</tr>
<tr>
<td>Using the Phishing Protection Dashboard to monitor enrollment</td>
<td>46</td>
</tr>
<tr>
<td>Updating the MTD Local Actions policy when new threat list is available</td>
<td>46</td>
</tr>
<tr>
<td><strong>Using the Threat Management Console</strong></td>
<td>48</td>
</tr>
<tr>
<td>Configuring Threat Management Console</td>
<td>48</td>
</tr>
<tr>
<td>General settings</td>
<td>48</td>
</tr>
<tr>
<td>Managing devices in Threat Management Console</td>
<td>50</td>
</tr>
<tr>
<td>General display filters</td>
<td>51</td>
</tr>
<tr>
<td>Using Threat Management Console to monitor threats on devices</td>
<td>53</td>
</tr>
<tr>
<td>Whitelisting a sideloaded app for Android devices</td>
<td>53</td>
</tr>
<tr>
<td>Whitelisting an app prior to installation</td>
<td>54</td>
</tr>
<tr>
<td>Whitelisting an app after installation</td>
<td>54</td>
</tr>
<tr>
<td><strong>Locally-initiated mitigation and compliance</strong></td>
<td>55</td>
</tr>
<tr>
<td>Creating MTD local actions in Core</td>
<td>55</td>
</tr>
<tr>
<td>Editing an MTD local actions policy</td>
<td>56</td>
</tr>
<tr>
<td>Threat category names and related threats</td>
<td>57</td>
</tr>
<tr>
<td>Network, device, and app threats available in Local Actions</td>
<td>58</td>
</tr>
<tr>
<td>Local Actions Network threats</td>
<td>58</td>
</tr>
<tr>
<td>Local Actions Device threats</td>
<td>60</td>
</tr>
<tr>
<td>Local Actions App threats</td>
<td>62</td>
</tr>
<tr>
<td>Creating compliance policy rules and groups</td>
<td>62</td>
</tr>
<tr>
<td>Threat types</td>
<td>62</td>
</tr>
<tr>
<td>Creating compliance policy rules</td>
<td>63</td>
</tr>
<tr>
<td>Creating compliance policy groups</td>
<td>64</td>
</tr>
<tr>
<td>Example: creating an out of compliance local actions policy</td>
<td>65</td>
</tr>
<tr>
<td>Setting the sinkhole action on iOS devices</td>
<td>66</td>
</tr>
<tr>
<td>Enable sinkhole VPN mitigation for iOS devices</td>
<td>66</td>
</tr>
</tbody>
</table>
Sinkhole mitigation by IP address, domain, or country ......................................................... 67
Checking MobileIron Threat Defense status ................................................................. 68
Checking individual devices ......................................................................................... 69
Using Advanced Search ............................................................................................. 71
Managing user privacy ............................................................................................... 72
   Managing EU users under GDPR ............................................................................ 72
   Enabling the GDPR profile .................................................................................... 72
   Assigning users to a GDPR profile ......................................................................... 73
Administering Mobile@Work .......................................................................................... 75
   Logging and enhanced logging for iOS clients ....................................................... 75
   Sending Mobile@Work logs to MobileIron Support ............................................... 75
   MTD support for Android 10 .................................................................................. 75
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 are a part of the MobileIron Threat Defense Solution for Core 10.8.0.0.

MTD features and enhancements for iOS devices

These features, updates, and enhancements are available for iOS devices in this release:

Advanced multi-level phishing protection

From Core 10.7.0.0 through the most recently released version as supported by MobileIron, advanced anti-phishing protection for MTD-enabled iOS devices can be pushed to devices without user action, independently of MTD Content Blocker. This advanced phishing tool provides full coverage against risky URLs. The configuration is pushed to the end user through an automatically enabled, on-device VPN. For full information, see Advanced phishing protection for iOS devices.

**Figure 1. Threat Management Console Phishing Policy Options**

Mobile phishing protection warns and protects users from accessing harmful sites/links.

- Enable phishing protection and activate zIPS URL sharing
- Local VPN For Phishing
  - Enable phishing protection and activate zIPS local VPN
  - Allow user control
  - Block detected phishing URLs
- Enable content inspection on remote server
NOTE: If Content Blocker is previously enabled on a device, it remains on the device even after Content Blocker is disabled.

Mobile@Work sinkhole compliance VPN without user action

MTD Administrators for iOS devices now have additional sinkhole configuration options to automatically redirect risky client Internet traffic away from the Enterprise without user action. Previously when a threat triggered a sinkhole, all network activity on the client was blocked. From Core 10.7.0.0 through the most recently released version as supported by MobileIron, you can designate IP addresses, Domains, and countries to be allowed or blocked on managed devices, using Threat Management Console Network Sinkhole Settings. See Sinkhole mitigation by IP address, domain, or country.

FIGURE 2. THREAT MANAGEMENT CONSOLE NETWORK SINKHOLE SETTINGS PAGE

Risky link notifications display within client app

When client users click on secure HTTP (HTTPS) phishing URLs, it is by design that the user notification appears within the app, and not on the browser.

MTD wake-up interval increased to 60 minutes

From version 10.7.0.0 through the most recently released version as supported by MobileIron, the MTD default wake-up interval for iOS devices is 60 minutes, which provides the best combination of battery life and threat detection. For more information, see "Sync Policies" in Getting Started with MobileIron Core.
Users can disconnect MobileIron anti-phishing VPN by connecting to a different VPN provider

Users who launch a device-level VPN app like PulseSecure or GlobalProtect from their device will disconnect the MobileIron anti-phishing VPN, which disables the anti-phishing solution on the device. The device user must navigate back to Settings > VPN settings and re-select MobileIron anti-phishing VPN to re-enable MTD anti-phishing protection.

### MTD features and enhancements for Android devices

These features, updates, and enhancements are available for Android and Android Enterprise devices in this release:

#### Additional network threats for Android devices

Three new network threats are included in Risky Wi-Fi threats for Android devices. You can enable threat notifications and apply MTD local actions when these threats are detected.

The threat types are:

- **ARP_MITM**: Protects against man-in-the-middle (MITM) attacks over address resolution protocol (ARP).
- **ICMP_REDIRECT_MITM**: Protects against redirect client-only MITM attacks over Internet control message protocol (ICMP).
- **SSL_STRIP**: Protects against the downgrading of your connection from secure HTTPS to insecure HTTP within the secure sockets layer (SSL).

These threats display in the Mobile@Work app Threat Defense home page, and the Threat Details page. Users see:

- Threat type: Risky Wi-Fi
- Description: Your data can be stolen and your device can be compromised
- Suggested action: Disconnect from this Wi-Fi immediately or turn off Wi-Fi on your device

For information on Mobile@Work support for Android devices, refer to MobileIron Core Device Management Guide for Android and Android enterprise Devices.

### General MTD features and enhancements

The following MTD general features, updates, and enhancements are available in this release:
About MobileIron Threat Defense Solution

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 removing the label that is associated with the MTD license configuration.

**Applicable to:**

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

**NOTE:** MTD does not currently 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** (Threat Management Console)
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 Threat Management Console authenticates and establishes communication with MobileIron Core and synchronizes device parameters.
4. The administrator defines threat defense policies on the Threat Management Console.
5. The administrator defines MTD local actions policies on Core.
6. MTD-enabled Mobile@Work clients check-in and begin communicating with Threat Management Console 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 through the Threat Management Console and local actions

Detected threats can be remediated through a combination of local- and server-initiated mitigation and compliance actions. Applied together, they provide the highest level of client threat protection.
- Server-initiated mitigation and compliance is done through the Threat Management Console.
- is done through the Admin Console.

The process works this way:

- 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 Threat Management Console.
- If the device is connected to Core and Threat Management Console (server-initiated), any threats detected on the device informs the Threat Management Console of threat status. Threat Management Console instructs Core that a policy violation has been triggered. Core assigns the compromised device to the appropriate label, which can trigger a custom enforcement workflow.
- When the threat is remediated on the device, the client passes this state change to the Threat Management Console. The Threat Management Console tells Core that the policy violation has been removed and removes the label that triggered a custom enforcement workflow from the device. Core then restores 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 Plus license, all MobileIron MTD functionality is enabled, including advanced app analytics. If you find that you need MTD Plus functionality, contact your MobileIron representative.
MobileIron Threat Defense prerequisites

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

- Configure MobileIron Core for managing devices.
- Obtain your MTD license.
- Obtain your Threat Management Console tenant credentials.
- Open port 8883 inbound from Threat Management Console to Core.
- Customers using Portal ACLs for IP Whitelisting to allow connections from the Threat Management Console to their Core for ports 443 or 8883 can use this information: MobileIron Threat Defense Management zConsole Requires Update to Firewall Rules to Avoid Service Interruption.

Configuring Privacy policy

You can modify the default Privacy Policy to apply to apps, or create a new policy if necessary. To configure the Privacy Policy to apply to apps, follow these steps:

Procedure

2. Choose one of the following options:
   - Select the existing default Privacy Policy and click the Edit button in the upper-right corner of the Policy Details section. The Modify Privacy Policy menu opens.
   - Click Add New > Policy. The New Privacy Policy menu opens.
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.

Tip: The default Privacy Policy can be modified to collect All Apps. 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 Threat Management Console for use with MobileIron Core, you need to create an MTD admin user, who will communicate with Core through the Threat Management Console. MobileIron suggests creating a new admin user to manage MTD.

NOTE: MobileIron recommends removing the User Portal role from the MTD admin. This role is automatically assigned to every local user.

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.

Next steps

Continue to Assigning an administrator to a space and Adding roles to the MTD admin user

Assigning a space and roles to an MTD administrator

Once you have created your MTD admin user, you must assign the admin to a device space, which limits his authority to that space, and assign the user appropriate roles. For more information about assigning device spaces, see "Device Spaces" in the MobileIron Core Delegated Administration Guide.

Before you begin

Be sure you have completed the steps for Creating an MTD admin.

Procedure

1. In the Admin portal, navigate to the Admin > Admins page.
2. Select the admin user to be the MTD administrator.
3. Click Actions > Assign to Space.

4. From the Select Space drop-down menu, select the space the local user will manage.
   
   NOTE: You must select a space for the MTD admin before the appropriate roles will appear. The default is no space is selected.

5. In the list of Admin Roles, scroll down to:
   
   a. Device Management and select Apply and remove device label.
   
   b. Privacy Control and select View apps and iBooks in device details and Locate device.
   
   c. Label Management and select View label and Manage label.
   
   d. User Management and select View user and Manage user.
   
   e. Other Roles and select Common Platform Services (CPS).

6. Click Save.

### Enabling CPS messaging on MobileIron Core

The Threat Management Console server integrates with MobileIron by using the Event Notification Service, which requires enabling CPS messaging. CPS messaging makes it possible for the Threat Management Console to receive notifications for changes on devices real time—for example for new device registrations or new app installs—instead of relying on the synchronization job that runs every 1-4 hours. These notifications will not be received by the Threat Management Console if messaging is not enabled. For more information, see “Using the Event Notification Service” in the MobileIron Event Notification Service and Common Platform Services API Guide.

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:

- Port 8883 needs to be open inbound from Threat Management Console to Core.
- If MobileIron Core is running in a High Availability configuration, enable messaging on both primary and secondary nodes.

### Procedure

To enable or disable CPS messaging, run the following commands in the MobileIron Core CLI:

```bash
hostname> enable
hostname# configure terminal
config# activemq
```
Adding Core as your MDM server in Threat Management Console

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

Before you begin

- Locate the user name and password for the Threat Management Console 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 Threat Management Console 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 Threat Management Console 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 roles to the MTD 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 Threat Management Console groups. The list of Threat Management Console 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 Threat Management Console with Core, otherwise the labels will not show up when this step is performed.

7. Click Finish.

8. Synchronize Threat Management Console with Core. Make sure the synchronization is successful.

   NOTE: Whenever an MDM configuration is removed from Threat Management Console, 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 Threat Management Console

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></td>
</tr>
<tr>
<td>Traffic from MobileIron Core to Internet/Outside</td>
<td>MobileIron Core is in the DMZ</td>
<td></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>
<tbody>
<tr>
<td>Apple APNS and MDM Services</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. HTTPS 443: api.push.apple.com TCP 2195: gateway.push.apple.com TCP 2196: feedback.push.apple.com TCP 2197: api.push.apple.com (optional, alternative for HTTPS 443)</td>
<td>HTTPS 443 TCP 2195, 2196, 2197</td>
</tr>
<tr>
<td>MobileIron Gateway</td>
<td><strong>support.mobileiron.com</strong> (199.127.90.0/23) for software update repository and upload of showtech log. Open HTTPS 443 to <strong>appgw.mobileiron.com</strong>, <strong>coresms.mobileiron.com</strong>, <strong>coreapns.mobileiron.com</strong>, <strong>clm.mobileiron.com</strong>, <strong>api.push.apple.com</strong>, <strong>supportcdn.mobileiron.com</strong>, <strong>coregcm.mobileiron.com</strong>, and <strong>corefcm.mobileiron.com</strong> (199.127.90.0/23) for location/number lookup data, in-app registration, APNS/FCM/GCM messaging, licensing, and support for sending SMS. <strong>a.mobileiron.net</strong> 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.</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td>AppConfig Community Repository</td>
<td><strong><a href="https://appconfig.cdn.mobileiron.com">https://appconfig.cdn.mobileiron.com</a></strong></td>
<td>HTTPS 443</td>
</tr>
</tbody>
</table>

### 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. <strong>For devices on closed networks:</strong> 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.</td>
<td>TCP 5223</td>
</tr>
<tr>
<td>Android devices</td>
<td><strong>To allow access to Google's FCM or GCM service:</strong> 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. <strong>For Android enterprise:</strong> <a href="https://www.googleapis.com/androidenterprise">https://www.googleapis.com/androidenterprise</a> <a href="https://accounts.google.com/o/oauth2/token">https://accounts.google.com/o/oauth2/token</a> <strong>For Help@Work for Android:</strong> 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>TCP 5228, TCP 5229, TCP 5230, HTTPS 443</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 MTD for Mobile@Work devices

This procedure is applicable to both Android and iOS devices.

Enabling MobileIron Threat Defense involves:

- Completing the prerequisites listed in MobileIron Threat Defense prerequisites.
- 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.

Creating an MTD activation configuration

Procedure

1. Log into Threat Management Console 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 and an optional description for the configuration.
5. In the Configuration Setup section, make the following entries:
   - **Vendor**: Zimperium
   - **License Key**: enter your MobileIron Threat Defense activation code.
6. Click Save. The Configurations page refreshes with the name of the new MTD Activation Configuration.
7. 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.
Pushing new MTD activation configurations to existing devices

Android

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

- For Mobile@Work 10.1.0.0, when the Android XML Configuration (Threat Management Console) is pushed to the device and then the Administrator applies a label to another MTD Activation Configuration, upon the next device check-in, 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 check-in, 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.

Disabling MTD on MobileIron Core

You can disable MTD and remove the MTD configuration from Mobile@Work devices in several ways:

- Remove the configuration from your device labels
- Delete the MTD configuration

Procedure

1. From the MobileIron Core, go to Policies & Configs > Configurations.
2. Click the check box for your Mobile Threat Defense Configuration.
   - To delete the configuration, click the Actions menu, select Delete, and confirm the delete.
   - To remove the config from your devices, click the Actions menu, select Remove from Label, select the labels from the list, and click Remove.

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 Threat Management Console 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: force device check-in

To verify that MTD is working on all devices, administrators can perform a **Force Check-in** for devices.

**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.

The types of policies used by MobileIron Threat Defense include:

- Mitigation and multi-tier compliance actions. See Server-initiated mitigation and compliance.
- MTD Local actions threat defense policies. See Locally-initiated mitigation and compliance.
- Phishing protection. See Phishing protection for MTD devices
- Sync policies. See Updating Core sync policy.
- Privacy policies. See Configuring Privacy policy.

Setting the MTD wake-up interval for iOS devices

You can adjust the default MTD wake-up interval for iOS devices from the Sync Policy menu in the Admin portal Policies & Configs > Policies page. Previously, the MTD iOS wake-up interval default was 15 minutes, which sometimes resulted in excessive battery usage for iOS clients. From version 10.7.0.0 through the most recently released version as supported by MobileIron, the MTD iOS default wake-up interval is 60 minutes, which can be adjusted for your network. For full instructions, see Sync policies in the Using default policies chapter of Getting Started with MobileIron Core.

Creating event notifications

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 Threat Management Console. When Threat Management Console 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>$SEVERITY - The defined severity of the system event, for example, Information, Warning, or Critical.</td>
</tr>
<tr>
<td>Email Body</td>
<td>$SEVERITY - The defined severity of the system event, for example, Information, Warning, or Critical.</td>
</tr>
<tr>
<td>SMS</td>
<td>$PHONE_NUMBER - The phone number used by the device.</td>
</tr>
<tr>
<td>APNS</td>
<td>$USER_NAME - The display name of the user associated with the device.</td>
</tr>
<tr>
<td></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 Threat Management Console Mobile Threat Response Policy.
Server-initiated mitigation and compliance

The multi-tier compliance action format is a best practice for server-initiated mitigation and compliance via the Threat Management Console.

Server-initiated mitigation and compliance contains the following steps:

1. Creating MTD labels in Core
2. Creating and applying server-initiated multi-tier compliance actions
3. Creating compliance policy rules and groups
4. Configuring the Threat Management Console 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

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 Threat Management Console and synchronizing it with Core, Threat Management Console will need to be synchronized with Core again before the labels will appear in Threat Management Console.

Procedure

1. In the Core Admin Portal, select Devices & Users.
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 Threat Management Console.
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 Threat Management Console.
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 Threat Management Console.

8. Create a fourth 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 Threat Management Console.

### Creating and applying server-initiated multi-tier compliance actions

This section discusses how to create and apply compliance actions that are initiated by the Threat Management Console. (For MTD local actions, see Creating MTD local actions in Core.) User devices can trigger a check-in with Threat Management Console, but it is initiated by Threat Management Console 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. This will allow the appropriate level of mitigation depending on risk/threat severity level: **Critical**, **Elevated**, **Normal** and **Low**.

By default, there are two existing compliance actions available – **Block Email**, **AppConnect Apps**, and **Send Alert**, and **Send Alert**. It is a best practice to create additional compliance actions that will be used specifically for MTD, for example:

- **MTD – Notify** (based on the "Send Alert" compliance action)
- **MTD – Block** (based on the "Block Email, App Connect apps and Send Alert" compliance action)
- **MTD- Quarantine** (see Quarantine compliance action)
- **MTD- Tiered Compliance 4 hours** (see Tiered compliance action - 4 hours)

**Before you begin**

- Be sure that you have completed Creating MTD labels in Core.
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.
   c. Select Quarantine the device to quarantine the device.
   d. Select Remove All Configurations to remove all configuration settings from an Android or iOS device.
   e. 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.
   f. 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.
4. Click Save.

Tiered compliance action - 4 hours

Procedure

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

7. Click the **expand (+)** button at the bottom of the dialog box. Tier 4 selections display.
   a. Set the **Wait** time to 4 Hours.
   b. Select **Quarantine the device** to quarantine the device; the section expands.
   c. Select **Remove All Configurations** to remove all configuration settings from an Android or iOS device.
   d. 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.
   e. 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.

8. Click **Save**.

### Configuring the Threat Management Console Mobile Threat Response Policy

The Threat Response Matrix (TRM) defines the actions that Threat Management Console takes upon detecting an event. Among the options are:

- Enable or disable detection of a specific threat classification
- Alert the admin
- Change the severity of a threat
- Set MDM actions and mitigation actions

After you modify these options, click **Deploy** to send, or sync, the new TRM to currently activated devices. When integrated and synced with MobileIron Core, each label used for integration I created as a group with its own TRM policy. 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) Threat Management Console with MobileIron Core. This aligns the labels in Core with the TRM settings.

### TABLE 5. THREAT RESPONSE POLICY OPTIONS

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>The Threat Management Console administrator has the option of disabling certain threat detections and, therefore, the collection of associated forensics. In the <strong>Severity</strong> 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 <strong>Deploy</strong> button again. After deploying / syncing with MobileIron Core, when a threat is detected, Threat Management Console 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 Threat Management Console to Core is performed securely through a MobileIron API call.</td>
</tr>
<tr>
<td>Severity</td>
<td>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.”</td>
</tr>
<tr>
<td>Threat</td>
<td>The threats listed in the <strong>Threat column</strong> 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.</td>
</tr>
<tr>
<td>Set User Alerts</td>
<td>Administrators cannot manage MTD alerts through Threat Management Console. In order to implement and localize MTD alerts, please use Local Actions policy in Core. See Locally-initiated mitigation and compliance.</td>
</tr>
<tr>
<td>Set Device Action</td>
<td>Administrators can deploy device actions for Android and iOS devices on Threat Management Console. See Set device action.</td>
</tr>
</tbody>
</table>
TABLE 5. THREAT RESPONSE POLICY OPTIONS (CONT.)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM action</td>
<td>Administrators can enable server-enforced mobile device management (MDM) action items on the Threat Management Console policies page. See MDM action.</td>
</tr>
<tr>
<td>Mitigation</td>
<td>When a threat that was detected by Threat Management Console 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. See Mitigation action.</td>
</tr>
<tr>
<td>Notifications</td>
<td>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. See Notifications.</td>
</tr>
</tbody>
</table>

**Set device action**

Administrators can deploy device actions for Android and iOS devices on Threat Management Console.

**Procedure**

1. From the MTD Threat Management Console, 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. Threat Management Console 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 Threat Management Console policies page.

Procedure

1. From the Threat Management Console, 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. Threat Management Console 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

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 6. 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

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

**Procedure**

1. In the Threat Management Console 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.

### 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 compliance or Locally-initiated mitigation and compliance.

**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.

**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 wakes up 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*.
Phishing protection for MTD devices

MobileIron Threat Defense Solution detects and prevents phishing attempts on MTD-enabled iOS and Android devices. When a user clicks on a risky URL, Mobile@Work blocks the site, and displays a pop-up message indicating that it contains risky content that could steal sensitive or private content from the user device.

To enable phishing protection on MTD-enabled devices, follow this workflow:

1. Configure and enable MTD on Core. See Enabling MTD for Mobile@Work devices.
2. (iOS only) Enable anti-phishing protection in Threat Management Console. See Advanced phishing protection for iOS devices.
3. Create an MTD anti-phishing configuration for managed Android devices and optionally, iOS devices. See Enabling additional MTD anti-phishing protection
4. Push the configuration to client devices.
5. (Android only) Have the user set MobileIron client as the default browser in the app Settings, or set MobileIron client to control URL clicks. See Additional Android phishing configuration tasks

Advanced phishing protection for iOS devices

From MobileIron Core 10.8.0.0 through the most recently released version as supported by MobileIron, you can enable Threat Management Console advanced phishing protection to MTD-enabled iOS devices without any client user action. This tool provides full coverage against risky URLs through an automatically enabled, on-device VPN.

**NOTE:** Anti-phishing configuration information displays only in English for this release. Other supported languages will be available in the next release.

Enable Threat Management Console anti-phishing VPN

**Procedure**

1. Log into Threat Management Console.
2. Click the **Policy** tab.
3. From the Policy page, click **Phishing Policy.** The phishing policy configuration page displays.
4. In the **Selected Group** field, select from the groups you created in Creating compliance policy rules and groups.

5. Select from the following options:

- **Enable phishing protection and activate zIPS URL sharing** - Enabled by default. Check this option to enable phishing protection.

  NOTE: Users who launch a device-level VPN app like PulseSecure or GlobalProtect from their device will disconnect the MobileIron anti-phishing VPN, which disables the anti-phishing solution on the device. The device user must navigate back to **Settings > VPN settings** and re-select **MobileIron anti-phishing VPN** to re-enable anti-phishing protection.

- **Local VPN for Phishing**

  - **Enable phishing protection and activate zIPS local VPN** - Enabled by default. Check this option to enable a local phishing VPN.

  - **Allow user control** - Disabled by default. This option cannot be enabled.

  - **Block detected phishing URLs** - Enabled by default. Check this option to block phishing URLs when they are detected on a device.

  NOTE: Do not disable Phishing Policy option "Block detected phishing URLs." If disabled, users will see a non-working notification.

- **Enable content inspection on remote server** - Enabled by default. This option allows the Threat Management Console to access a much larger database of blacklisted sites than the sites available on the device, providing multi-level protection.

6. Click **Deploy** to distribute the phishing protection policy to the selected device group.
Enabling additional MTD anti-phishing protection

You can create an MTD anti-phishing configuration for managed Android devices and optionally, iOS devices. The configuration applies URL Handler for Android devices, and on-device VPN and Content Blocker are options for iOS devices.

Procedure

1. Log in to MobileIron Core admin portal.
2. Go to Policy & Configs > Policies.
3. Click Add New > MTD Anti-Phishing. The Add MTD Anti-Phishing Policy page opens.

4. In the Add MTD Anti-Phishing Policy dialog box, enter a name for the policy.
5. For status select Active. This is the default setting.
6. Specify a priority for this policy, relative to the other custom policies of the same type. Select Higher than or Lower than, then select an existing policy from the drop-down list. This priority determines which policy is applied if more than one policy is available.
   
   NOTE: Only one active policy can be applied to a device.
7. (Optional) Enter a description.
8. In the iOS section, select from the following policy options:
   a. **Use on-device VPN to analyze malicious URLs** - This option auto-installs a VPN profile to managed clients without requiring end-user confirmation. Tapped links are checked against an on-device database of malicious URLs.
   b. **Enable Content Blocker anti-phishing** - The end user must enable this feature. When enabled, all network traffic is blocked when a phishing threat is detected. Once cleared, network traffic is again allowed.

9. In the Android section, **URL Handler** is enabled by default, and requires the end user to enable the feature.

10. Click **Save**.

11. Apply a label to the policy. See [Creating MTD labels in Core](#).

12. 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.

13. Force device check in.

---

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

You can configure anti-phishing protection 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.

**NOTE:** On Android devices managed in MobileIron Core, phishing protection cannot be provided if the end-user types-in the URL in a browser directly.

**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 select 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 the 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 a 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.
How to select MobileIron client as the default browser

<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>
</tbody>
</table>

- **Work Profile (Profile Owner)** (Android 5.0 through the latest version as supported by MobileIron)
  - Managed Device (Device Owner) (Android 5.0 through the latest version as supported by MobileIron)
    - **Android Enterprise**: 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.

- **Managed Device with Profile Owner (Android 8.0 through the latest version as supported by MobileIron)**
  - 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.

- **AppConnect (Android 5.0 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 documentation](#). MobileIron Support credentials are required to access documentation in the Support Community.

---

**See the following table for expected behavior after the MobileIron client has been set or selected as the default browser to provide phishing protection.**
### Table 8. Expected Client Behavior by Android Release

<table>
<thead>
<tr>
<th>Device Mode</th>
<th>Description</th>
<th>Expected behavior</th>
</tr>
</thead>
</table>
| Kiosk       | Samsung devices from Android 5 to 8 and non-Samsung devices from Android 5 to 7. | 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. |

| Kiosk Android enterprise Device Owner | Android 5.0 through the latest version as supported by MobileIron. | 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. |

### 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.
   - **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.

### Additional Android phishing configuration tasks

After MobileIron client has been set or selected as the default Android browser to provide phishing protection, some additional tasks may be needed.

#### TABLE 9. ADDITIONAL PHISHING CONFIGURATION TASKS

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AppConnect (Android 5.0+)</strong></td>
<td>In Android AppConnect container configuration, administrators should distribute Web@Work and enable the following lockdowns for the phishing protection:</td>
</tr>
<tr>
<td></td>
<td>- Allow Web</td>
</tr>
<tr>
<td></td>
<td>- Allow non-AppConnect apps to open URLs in Web@Work</td>
</tr>
<tr>
<td></td>
<td>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 Cloud product documentation. (MobileIron credentials are required to access documentation in the Support Community.)</td>
</tr>
<tr>
<td><strong>Kiosk Device Admin mode</strong> (Samsung devices from Android 5.x to 8.x and non-Samsung devices from Android 5.x to 7.x) and Kiosk Android enterprise Device Owner mode (Android 5.0+)</td>
<td>When URL clicks are inside the kiosk, if the URL is safe, it will be displayed 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.</td>
</tr>
</tbody>
</table>

When a user clicks 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. The end user is asked whether they want to use this browser **Just Once** or **Always**.
  - For **Just Once**, MobileIron will continue to show a list of browsers, if there are multiple browsers.
  - For **Always**, MobileIron client will save the selected browser, and use it to render safe URLs going forward.

**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.

**Using a remote database to validate URLs**

By default, phishing policy is configured to use an on-device database for detecting phishing URLs. If you prefer your devices to have access to a much larger, real-time updated database, you can configure this through the Threat Management Console. You can also set this option when configuring Advanced phishing protection for iOS devices.

**Procedure**

1. Log in to the Threat Management Console.
2. Navigate to Policy > Phishing Policy.
3. Select the device group you want in the policy.
4. Select these options:
   - Enable phishing protection and activate zIPS URL sharing
   - Enable content inspection on remote server

   **NOTE:** The option to allow user control of the phishing VPN is disabled.

5. Deploy the changes.
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

Threat Management Console 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 Using Threat Management Console to monitor threats on 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 in Core for details.
3. Enter the changes and click **Save**.
Using the Threat Management Console

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

Figure 5. Threat Management Console Threat Log

Configuring Threat Management Console

The Threat Management Console 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:

**TABLE 10. GENERAL TAB SETTINGS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description and actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company Information</strong></td>
<td>Enter your company information, including a contact email. Your plan type and activation date are populated automatically.</td>
</tr>
<tr>
<td><strong>Logged in user</strong></td>
<td>Enter the name, email address, system role, and password for the current user. Click <strong>Change password</strong> to open the Set Password menu. Click <strong>Save</strong> to retain your changes.</td>
</tr>
</tbody>
</table>
| **Set Password Policy** | 1. Click **Set Password Policy** to open the password policy menu.  
2. Define the password requirements for Threat Management Console users:  
   - Minimum password length  
   - Required password elements  
   - Maximum repeating characters  
   - Verify that the new password was not used in the past “n” 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  
3. Click **Save** to retain your changes. |
### Table 10. General Tab Settings (Cont.)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description and actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Language</td>
<td>Choose the language for the Threat Management Console. The current options are English, Japanese or Hebrew. Click <strong>Save</strong> to retain your changes.</td>
</tr>
<tr>
<td>Options for zIPS with root access</td>
<td>This feature is not supported for MTD clients.</td>
</tr>
<tr>
<td>Danger Zone</td>
<td>When this option is enabled, it alerts the user that they have connected to a Wi-Fi network that is in the Danger Zone database of possibly malicious websites. This option is disabled by default. Click <strong>Save</strong> to retain your changes.</td>
</tr>
<tr>
<td>Device Inactivity Configuration</td>
<td>This configuration controls how long the system waits before determining that a device is dormant:</td>
</tr>
<tr>
<td></td>
<td>1. <strong>Allowed Inactivity Time:</strong> The maximum time a device can be inactive before the device is entered into the warning timer, aka Grace Period. Enter a valid number in the left box, and choose <strong>Seconds</strong>, <strong>Minutes</strong>, or <strong>Hours</strong> in the right box.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Warning Interval (Grace Period):</strong> After the device exceeds the Allowed Inactivity Timer, it enters the grace period where it receives a warning. If more than one warning is required, enter a valid number in the left box to configure the interval between warnings, and choose <strong>Seconds</strong>, <strong>Minutes</strong>, or <strong>Hours</strong> in the right box.</td>
</tr>
<tr>
<td></td>
<td>3. <strong>Max Warnings:</strong> The number of warnings that can be sent to the device in the grace period. An entry of ‘0’ disables the grace period.</td>
</tr>
<tr>
<td></td>
<td>4. <strong>All Android devices use AFW/Enterprise:</strong> Click this box if all of your Android devices use Android enterprise (AE) or AE Work Profile mode. When enabled, it triggers a threat event if either of the client profiles (work or personal) exceeds the <strong>Allowed Inactivity Time</strong>.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Save</strong> to retain your changes.</td>
</tr>
</tbody>
</table>

### Managing devices in Threat Management Console

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)
- CVE (Common vulnerabilities and exposures)
- 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.

**FIGURE 7. EXAMPLE OF RISK POSTURE ON DEVICES**

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 11. 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>
<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>CVE</td>
<td>Display devices that include common vulnerabilities and exposures (CVE).</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>This column displays the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Active</strong>: describes devices that are communicating on a regular basis to</td>
</tr>
<tr>
<td></td>
<td>the management console</td>
</tr>
<tr>
<td></td>
<td><strong>Inactive</strong>: describes devices that have been active but are now not</td>
</tr>
<tr>
<td></td>
<td>communicating</td>
</tr>
<tr>
<td></td>
<td><strong>Pending Activation</strong>: 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 Threat Management Console to monitor threats on devices

After configuring MobileIron Core as your Mobile Device Management (MDM) server in the Threat Management Console, and distributing Mobile@Work with MTD, you can use Threat Management Console to monitor threats to connected networks, apps, and devices.

You use Threat Management Console to configure the following MTD threat management features:

- Advanced anti-phishing protection for iOS devices. See [Advanced phishing protection for iOS devices](#).
- Configurable sinkhole mitigation for iOS devices. See [Sinkhole mitigation by IP address, domain, or country](#).
- Whitelisting sideloaded apps for Android devices. See [Whitelisting a sideloaded app for Android devices](#).

You can view these MTD-related items on Threat Management Console:

- MTD-enabled devices that are registered with Core
- Managed apps on Core devices
- Networks
- Projected threat levels for devices and apps

### Whitelisting a sideloaded app for Android devices

If the Sideloaded App threat is enabled through the Threat Management Console, 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 Threat Management Console before or after it is installed on a device.

**NOTE:** If you chose not to whitelist UEM-managed apps through Threat Management Console, **Sideloaded App** threats should not be bound to any compliance action.
Whitelisting an app prior to installation

Procedure

1. From Threat Management Console, 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 Threat Management Console.
   b. Select **ALLOW** to whitelist the app.
5. Click **Save** to apply the changes.

Whitelisting an app after installation

Procedure

1. From Threat Management Console, 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.
Locally-initiated mitigation and compliance

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 compliance.

Locally-initiated mitigation and compliance includes the following tasks and options:

- Creating MTD local actions in Core
- Creating compliance policy rules and groups
- Setting the sinkhole action on iOS devices
- Checking MobileIron Threat Defense status

Creating MTD local actions 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 Threat Management Console 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 a 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.

**Editing an MTD local actions policy**

You can edit your MobileIron Threat Defense Local Actions policy to select new or alternative threat defenses.

**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**.
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, 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 12. 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: &quot;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.&quot; In order to enable Danger Zone Connected, you must have the Enable the Danger Zone feature in zIPS check box selected (located in the management console &gt; Manage &gt; General tab.) 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 Threat Management Console functionality is not enabled:</td>
</tr>
<tr>
<td>IP Scan</td>
<td>Network name and BSSID fields are not available for threat forensics information.</td>
</tr>
</tbody>
</table>
### TABLE 12: AVAILABLE NETWORK THREAT POLICIES (CONT.)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network threats are not mitigated.</td>
<td>If Threat Management Console cannot get the BSSID from the device, then the Danger Zone Connection threat will not work.</td>
</tr>
<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>
### Table 12. 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>

### Local Actions Device threats

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

### Table 13. 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>
<tr>
<td>Threat</td>
<td>Mitigation when the following events occur</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
</tbody>
</table>
Table 13. Available Device Threat Policies (Cont.)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Vulnerable, non-upgradeable iOS Version</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>
</tbody>
</table>

Local Actions App Threats

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

Table 14. Available App Threat Policies

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation when the following events occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Android App</td>
<td>A known risky app that attempts to take control of the user device in some manner (e.g. elevate privileges, spyware, etc.)</td>
</tr>
<tr>
<td>Suspicious Profile</td>
<td>A suspicious profile is a new profile introduced to the environment and is not explicitly trusted or untrusted. It is recommended that the Administrator review the Profile and mark the profile as trusted or untrusted.</td>
</tr>
<tr>
<td>Suspicious iOS App</td>
<td>A known and risky app that attempts to take control of the device in some manner (e.g. elevate privileges, spyware, etc.)</td>
</tr>
<tr>
<td>Untrusted Profile</td>
<td>An untrusted profile is a new profile installed on one or more devices and is deemed unsafe to have installed on user devices. An untrusted profile installed on devices could be used to control devices remotely, monitor and manipulate user activities, and/or hijack a users' traffic.</td>
</tr>
</tbody>
</table>

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:
MobileIron Threat Defense Solution Guide for Core 10.8.0.0

- **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 Compliance23hours</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 Compliance4hours</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

1. Select **Policies & Configs > Compliance Policies**.
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 Plus 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 Plus 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**.
Setting the sinkhole action on iOS devices

You can configure an iOS sinkhole option to automatically redirect risky client Internet traffic away from your network.

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, blocking all network traffic. See .

2. If, however, the Network Sinkhole settings in the Threat Management Console have also been configured to block or allow specific traffic, the VPN sinkhole profile will block or allow only the IP addresses, groups, or countries you specify. See Sinkhole mitigation by IP address, domain, or country.

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, blocked browser traffic now succeeds.

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.

Enable sinkhole VPN mitigation for iOS devices

Network threats can be mitigated using a sinkhole VPN profile in the MTD Local Actions policy. Once you enable the MTD Local Actions Network Sinkhole option, you can optionally specify specific IP addresses, domains, and countries through the Threat Management Console. See Sinkhole mitigation by IP address, domain, or country.

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.

Before you begin

- Make sure you have reviewed .

Procedure

1. From the MobileIron Core Policies & Configs > Policies 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 click **Save**. The Policy page displays, with your updated configuration.

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

4. To push this configuration to devices, select the configuration.

5. Click **Actions > Apply to Label**. The Apply to Label menu displays.

6. Select the device labels that will receive the configuration.

7. Click **Apply**. The configuration is pushed to labeled devices.

### Sinkhole mitigation by IP address, domain, or country

If you would like sinkhole protection to be applied to specific IP addresses, domains, and/or countries, use the Threat Management Console Network Sinkhole Settings to define them.

**NOTE:** MTD Sinkhole Local Actions must be enabled to deploy the Threat Management Console sinkhole. See [Enable sinkhole VPN mitigation for iOS devices](#). The Threat Management Console Sinkhole feature is optional, and MTD sinkhole will continue to work in either case.

**Before you begin**

Complete [Enable sinkhole VPN mitigation for iOS devices](#)

**Procedure**

1. Log into Threat Management Console.

2. Click the **Manage** tab.

3. Click **Network Sinkhole Settings**. The Network Sinkhole Settings page displays.
4. Choose whether the listed addresses should be allowed, or blocked.
   - Check **Block network access except ALLOW the IP address ranges/Domains below** - to allow the listed addresses.
   - Check **Allow network access except BLOCK the IP address ranges/Domains below** - to block the listed addresses.

5. Optional. Enter a valid IP address and associated IP mask in the IP Addresses field, and click the green plus icon \( + \) to add the address to the **Allowed/Blocked IP Addresses** list.

6. Optional. Enter a valid domain address (for example, www.example.com), and click the green plus icon \( + \) to add the address to the **Allowed/Blocked Domains** list.

7. Optional. Click the green plus icon \( + \) for each country you want to add to the **Allowed/Blocked Countries** list.

8. Click **Deploy** to apply the sinkhole options to the listed entities.

**Checking MobileIron Threat Defense status**

To confirm MTD status from the MobileIron 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.)

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Definition</th>
<th>Location of Error Message</th>
</tr>
</thead>
</table>
| Connection Error      | Connection error. The user device is not protected. | Devices & Users > Devices > Device Details page ("Error")
                                                          | User device – "MobileIron Threat Defense detected that your device is not protected due to a connection error." |
| License Expired       | License has expired. The user device is not protected. | Devices & Users > Devices > Device Details page ("Error")
                                                          | User device – "MobileIron Threat Defense detected that your device is not protected because the license has expired." |
| License Invalid       | Invalid license key. The user device is not protected. | Devices & Users > Devices > Device Details page ("Error")
                                                          | User device – "MobileIron Threat Defense detected that your device is not protected because the license is invalid." |
| License Key Error     | License key error. The user device is not protected. | Devices & Users > Devices > Device Details page ("Error")
                                                          | User device – "MobileIron Threat Defense detected that your device is not protected due to a license key error." |
| License Limit Exceeded| Maximum license count has been reached. The user device is not protected. | Devices & Users > Devices > Device Details page ("Error")
                                                          | User device – "MobileIron Threat Defense detected that your device is not protected due to a license key error." |
### Table 15. MTD status on the Device Details tab (Cont.)

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Definition</th>
<th>Location of Error Message</th>
</tr>
</thead>
</table>
| License Not Activated               | MTD license key to Threat Management Console failed. The user device is not protected. | Devices & Users > Devices > Device Details page (“Error”)  
User device – “MobileIron Threat Defense detected that your device is not protected because the license limit has been exceeded.”                                                                                     |
| Logged Out                          | User device is not protected due to a logout.                              | Devices & Users > Devices > Device Details page (“Error”)  
User device – “MobileIron Threat Defense detected that your device is not protected due to a cancellation.”                                                                                                               |
| Login Cancelled (Android only)      | Too many logins. The user device is not protected.                         | Devices & Users > Devices > Device Details page (“Error”)  
User device – “MobileIron Threat Defense detected that your device is not protected due to a cancelled login.”                                                                                                             |
| N/A                                 | • The MTD activation configuration is not assigned to the device  
• MTD has not been activated on the device                                 | Devices & Users > Devices > Device Details page (“N/A”)  
User device – This value has no equivalent on the client app.                                                                                                    |
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 Checking MobileIron Threat Defense status 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.

**TABLE 15. MTD status on the Device Details tab (CONT.)**

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Definition</th>
<th>Location of Error Message</th>
</tr>
</thead>
</table>
| Pending         | MTD license key has been sent, awaiting confirmation from Threat Management Console. | Devices & Users > Devices > Device Details page ("Pending")
|                 |                                                                           | User device – This value has no equivalent on the client app.                            |
| Protected       | MTD license activation successful. User device is protected.              | Devices & Users > Devices > Device Details page ("Protected")                           |
|                 |                                                                           | User device – "Protected"                                                                |
| Simulator Error | Internal error.                                                            | Devices & Users > Devices > Device Details page ("Error")                               |
|                 |                                                                           | User device – “MobileIron Threat Defense detected that your device is not protected due to a simulator error.” |

Using Advanced Search
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 9. GDPR reminder banner**

**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.
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 MobileIron MTD support page.

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:

Location services are required to detect network threats – Android 10 devices require that location services be on to configure Wi-Fi. Turning off location services impacts the client’s ability to identify network threats, including Unsecured Wi-Fi and Rogue Access Points. Irrespective of location permission status on the device, the critical network-based threats like MiTM, MiTM Fake SSL Cert, and Internal Network Access are still detected.

Note the expected location and Wi-Fi behavior for different modes of Android, described below.
### Table 16. 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>Disconnect Wi-Fi local action is disabled in all modes on Android 10 devices.</td>
</tr>
</tbody>
</table>
| **Android enterprise** (Profile Owner) | During installation or upgrade of MTD on Android 10, the device user is prompted to enable location services for both device and profile.  

**NOTE:** If **Disallow share location** is enabled in the **PO lockdown** config, this will block the user's ability to turn on location services. Uncheck this feature to prompt the user to enable location services.  

- If the user selects **GO TO SETTINGS**: Location service launches in Settings. When the user enables both location settings, configured network threats will be detected.  

  **NOTE:** If device-level location services are on, but profile services are off, MTD can't directly open to the Profile Services switch. The user will have to locate the switch.  

- If the user selects **NO**: Network threats will not be detected, although the MTD configuration is applied. |
| **Android enterprise** (Device Owner) | Location settings are enabled without user action, allowing Wi-Fi configurations and MTD detection of network threats. |
| **Device administrator** (DA) mode | Wifi APIs are not available for DA and mobile application management (MAM) modes, even if location services are enabled. So MTD cannot detect network threats for these devices. All configured non-network threats will be detected. |
| **Corporate owned, personally enabled** (COPE) mode | MTD requires that COPE devices running Android 10 have location enabled at all times, and currently cannot be disabled. |