MobileIron Threat Defense Solution Guide for Cloud 75

MobileIron Go 75 for Android

Revised: February 25, 2021

For complete product documentation, see:
MobileIron Cloud Documentation Home Page

Proprietary and Confidential | Do Not Distribute

Copyright © 2009 - 2021 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
February 12, 2021	Missing UI text commands replaced globally.
February 25, 2021	Added notes to Android anti-phishing topics that Tunnel 4.6.0 or higher is required.

Contents

MTD features, issues, and enhancements in Cloud 75

Each version of the MobileIron Threat Defense (MTD) 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 Cloud 75.

MTD features, issues, and enhancements for Android devices

The following MTD features, issues, and enhancements are available for Android and Android Enterprise devices in this release:

MobileIron Go client support for Zimperium 4.14.5 SDK

Android MobileIron Go clients support the latest Zimperium software development kit (SDK) 4.14.5, from MobileIron Go 75 through the most recently released version as supported by MobileIron. This feature resolved issues of expired certificates for on-premise Threat Management console and of whitelisting customer-defined SSIDs.

Blocked access to risky Wi-Fi networks in Airplane mode

The following Android Enterprise client devices—in which “Disconnect Wifi” is enabled as part of an Android device’s MTD Local Action configuration for “Unsecured Wi-Fi Network” threat—will be disconnected from risky Wi-Fi networks in Airplane mode, from Cloud 75 through the most recently released version as supported by MobileIron:

- Device owner (DO) mode: fully-managed company-owned device
- Corporate-owned, personally-enabled (COPE) mode: company-owned device with Work Profile

Users cannot be disconnected from risky Wi-Fi automatically in Airplane mode for devices in the following Android Enterprise modes:

- Work Profile on employee-owned device (PO) mode
- Work Profile on company-owned device (EPO) mode

Samsung devices in Android Enterprise Work Profile mode on Android 10 unable to disable risky Wi-Fi

When **Disconnect Wifi** had been enabled in an MTD Local Action configuration for network threats, a Samsung limitation prevents devices running MobileIron Go in Android Enterprise Work Profile mode on Android 10 from disabling risky Wi-Fi connections. This has been fixed by Samsung in Android 11.

MTD features, issues, and enhancements for iOS devices

There are no features, issues, and enhancements available for iOS devices in this release.

General MTD features, issues, and enhancements

There are no MTD general features, issues, or enhancements in this release.

About MobileIron Threat Defense Solution

Applicable to:

- MobileIron Go for Android client versions as supported by MobileIron Cloud.
- MobileIron Go for iOS client versions as supported by MobileIron Cloud.
- MobileIron AppStation client versions as supported by MobileIron Cloud.

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

MobileIron Threat Defense Solution 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.

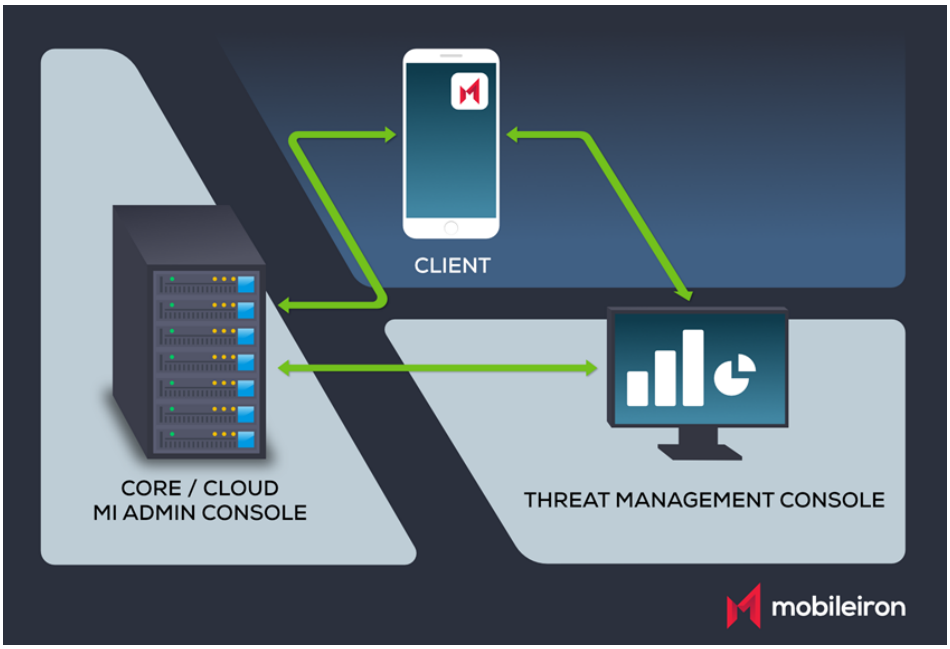
When this configuration is enabled in MobileIron Cloud and applied to the devices, the MobileIron Threat Defense Solution libraries are enabled on the MobileIron Go clients. The MobileIron Threat Defense Solution can be deactivated on a device by excluding (un-distributing) the MTD configuration from the device.

MobileIron Threat Defense overview

The MobileIron Threat Defense Solution consists of three components:

- **MobileIron Cloud Admin Console** to the Mobile Device Management (MDM) server
- **MobileIron Client Application** (MobileIron Go for iOS and Android and MobileIron AppStation)
- **Threat Management Console** (formerly referred to as zConsole)

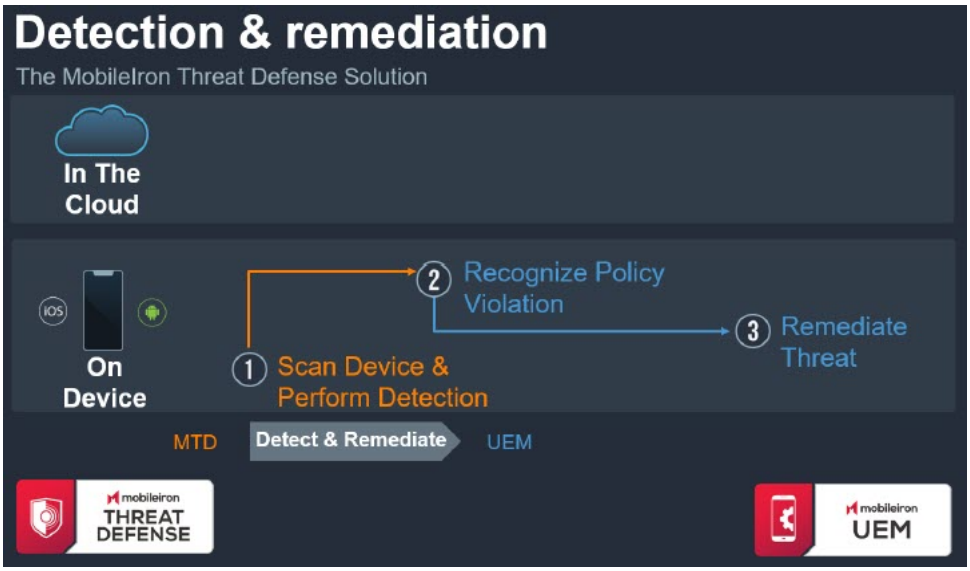
FIGURE 1. COMPONENTS OF MOBILEIRON THREAT DEFENSE SOLUTION



The MTD administrator can configure MobileIron Cloud to automatically install the required version of MobileIron client application, deploy and enable MTD on selected devices, and configure the components to protect devices from mobile threats.

After initial onboarding, the following workflow is required to configure the MobileIron Threat Defense Solution:

FIGURE 2. MTD WORKFLOW



1. MobileIron Cloud provides an activation code to MobileIron Go clients on selected devices. See MobileIron Threat Defense prerequisites.
2. MobileIron Threat Defense is enabled on selected devices. See Activating MobileIron Threat Defense.
3. The Threat Management Console authenticates and establishes communication with Cloud and synchronizes device parameters. For more information about Threat Management Console, see Using the Threat Management Console.
4. The administrator defines threat defense policies on the Threat Management Console. See Creating the Threat Management Console Threat Response Matrix.
5. The administrator defines MTD local actions configurations on the Admin Console. See Configuring MTD local actions for Cloud.
6. MTD-enabled MobileIron Go clients check in and begin communicating with the Threat Management Console and with Cloud.
7. MTD-enabled MobileIron Go 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.
- Locally-initiated mitigation and compliance 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 Cloud or Threat Management Console.
- If the device is connected to Cloud and Threat Management Console (server-initiated), any threats detected on the device informs the Threat Management Console of threat status. Threat Management Console instructs Cloud that a policy violation has been triggered. Cloud 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 Cloud that the policy violation has been removed and removes the label that triggered a custom enforcement workflow from the device. Cloud 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, do the following:

1. Obtain a Threat Management Console tenant license from Zimperium.
2. For both iOS and Android MTD implementations, contact your MobileIron representative to request your unique, encrypted MTD Activation token, or download it from the Threat Management Console.

   NOTE: You must purchase a MobileIron Threat Defense license from MobileIron or a MobileIron partner. Zimperium licenses purchased from other sources are not valid for activation through this page.
3. Ensure that the correct MobileIron Go client apps are installed for devices on which you want MTD to run.
4. Continue to Activating MobileIron Threat Defense.

Creating the MTD API user and assigning roles

Before you configure Threat Management Console for use with MobileIron Cloud, you need to create an MTD application program interface (API) user and assign a few roles. This API user will be the Cloud user you use in the Threat Management Console to communicate with Cloud. MobileIron suggests creating a new user to manage MTD.

Creating a new API user

Procedure

1. In the Admin Console, select **Users**.
2. Click **+ Add** > **API user**. The Add API User dialog page opens.
3. Enter the following details:
   - **Username**: Enter a meaningful User ID, such as "MTDAPIuser."
   - **Email**: Enter an email address for your MTD API user.
   - **First Name**: Enter a first name for your MTD API user.
   - **Last Name**: Enter a last name for your MTD API user.
   - **Display Name**: Enter a display name, for example, "MTD API Admin."
   - **Password**: Enter a password.
   - **Confirm Password**: Confirm the password.

4. Deselect the **Cisco ISE Operations** option.
5. Click **Done**.

Assigning roles to the API user

After you have added an API user, you need to assign MTD-specific roles to it.

Before you begin

Complete Creating a new API user before applying roles.

Procedure

1. From the Admin Console, go to **Users.**
2. Select the new API user you created previously.
3. Click **Actions.**
4. From the User details page, select **Assign Roles**.
5. Select the following roles:
   - **App & Content Management**
   - **App & Content Read Only**
   - **Device Actions**
   - **Device Management**
   - **Device Read Only**
   - **Common Platform Services (CPS)**
   - **System Read Only**
   - **User Read Only**
6. Click **Next.**
7. If the selected roles are "space bound," then select Spaces for all the space-bound roles.
8. Review the summary of the assigned roles.
9. Click **Done.**

Adding Cloud as your MDM server in Threat Management Console

You must add MobileIron Cloud as your Mobile Device Management (MDM) server in Threat Management Console to enable MobileIron Threat Defense. After entering Cloud details such as the URL and administrator user name and password, Threat Management Console synchronizes with Cloud. You can select the Cloud custom attributes you want to use in Threat Management Console. The relevant users, devices, and apps from Cloud are shown in the Threat Management Console.

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

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 assigned an API administrator with appropriate roles.

Procedure

1. Log in to your Threat Management Console with the credentials provided by MobileIron. The username and password defined for the MTD admin are required to establish communication with Cloud and synchronize the two servers.
2. Navigate to **Manage** > **Integrations** > **Add MDM**.
3. Select **MobileIron Cloud** to add it to the Threat Management Console as an MDM server.
4. Enter the following required information:

Item	Description
URL	Enter the FQDN or externally accessible URL for your Cloud in secure hypertext protocol (HTTPS). For example: `https://na2.mobileiron.com`
Username/Password	Enter an administrator username and password for Cloud. The admin user should be assigned several roles, including API, as described in Creating the MTD API user and assigning roles on page 13.
MDM Name	Enter a name for your Cloud.
Background sync	Select to synchronize users between Cloud and Threat Management Console.

5. Click **Next**.
6. In the last window, select the Cloud custom attributes 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 custom attributes in the Admin Console before synchronizing the Threat Management Console with Cloud, otherwise the custom attributes will not show up when this step is performed.
7. Click **Finish**.
8. Synchronize the Threat Management Console with Cloud. Make sure the synchronization is successful.

NOTE: Whenever MDM information is removed from the Threat Management Console, be sure to manually disable or remove the MobileIron Threat Defense Activation configuration from MobileIron Cloud.

Enabling the iOS significant location change service

The significant location change (SLC) service offers a power-friendly alternative, delivering location updates to Go clients only when the user's position changes by a significant amount within a specified period. If this service is enabled, then on location change, the MobileIron Go app wakes up in the background and checks in.

Before you begin

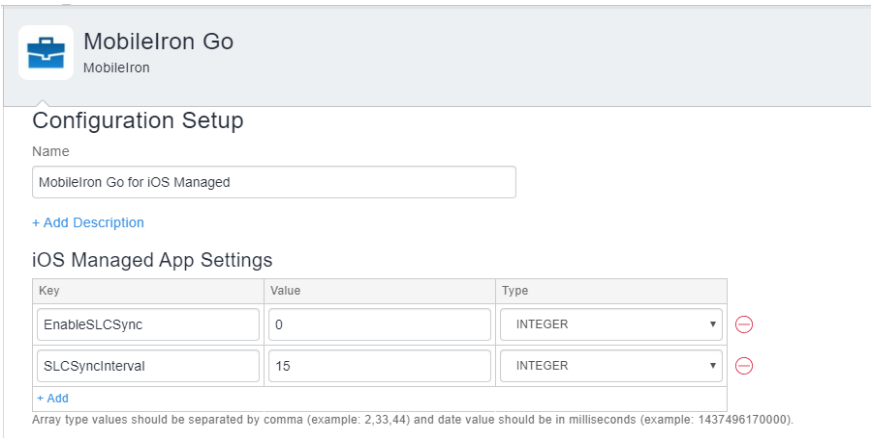
Verify that the MobileIron Go for iOS app is installed, and at least one iOS app is in the catalog. See the "App Catalog" section of the *MobileIron Cloud Administrator Guide*.

Procedure

To enable the significant location change service:

1. Log in to MobileIron Cloud Admin Console.
2. Go to **Apps > App Catalog**. The Apps page opens.
3. Click the **App Configurations** tab.
4. Click **+** next to iOS Managed App Configuration to display the Configuration Setup page to add a new configuration, OR
   Click **iOS Managed App Configuration** to edit an existing configuration.
5. Click **Add** to add a new configuration OR
   Click the name of an existing configuration and click **Edit.**
6. Under iOS Managed App Settings, click **+Add** to add the following key-value pairs:
   - **EnableSLCSync** - Enter **1** to enable SLC sync or **0** to disable SLC sync (default).
   - **SLCSyncInterval** - Enter an integer. If this key-value pair is not configured, the default value of 15 minutes applies.

   FIGURE 3. ENABLE THE SIGNIFICANT LOCATION CHANGE SERVICE



7. Click **Save** for a new configuration OR
   click **Update** for an existing configuration.

NOTE: If the SLCSyncInterval key is set to a value, the significant-change location sync will happen only if the previous check-in was earlier than the specified interval.

Activating MobileIron Threat Defense

When you have completed the MTD prerequisites, you can activate MobileIron Threat Defense Solution for your managed devices.

Before you begin

Retrieve your unique encrypted MobileIron Threat Defense activation code from your MobileIron representative.

Procedure

1. From the Admin Console, go to **Configurations.**
2. Click **+Add.**
3. Click **Mobile Threat Defense Activation.**
4. In the **Create Mobile Threat Defense Configuration** page, enter a name for the configuration.
5. (Optional) Enter a description.
6. In the Configuration Setup section, select the vendor **Zimperium.**
7. In the **License Key** field, enter your unique encrypted MobileIron Threat Defense activation code.
8. In the **Wake up Intervals (mins)** field, keep the default value of **60 minutes**, or set a higher or lower value. Note that more frequent wake-up times may result in unacceptable battery usage for iOS clients.
9. Click **Next.**
10. Select the **Enable this configuration** option.
11. Select one of the following distribution options:
    - **All Devices**
    - **No Devices** (default)
    - **Custom**
12. Click **Done.**

NOTE: For help activating MTD on Apple Automated Device Enrollment or International Roaming Expert Group (IREG) enrolled clients, see the knowledge-based article Allow MTD-activation of devices using Mobileiron Go client when app has been suspended or killed on the MobileIron support website.

Deactivating MobileIron Threat Defense

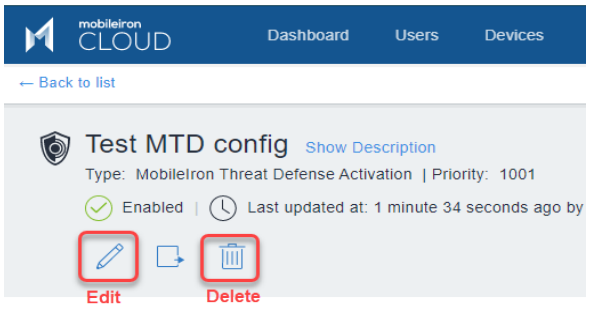
You can disable MTD and remove the MTD configuration from MobileIron Go devices in several ways:

- Disable the configuration
- Remove the configuration from your devices
- Delete the MTD configuration

Procedure

1. From the Admin Console, go to **Configurations.**
2. Click the name of your MobileIron Threat Defense Activation Configuration from the list to open the description.

FIGURE 4. EDIT OR DELETE MTD CONFIGURATION



To **delete** the configuration:

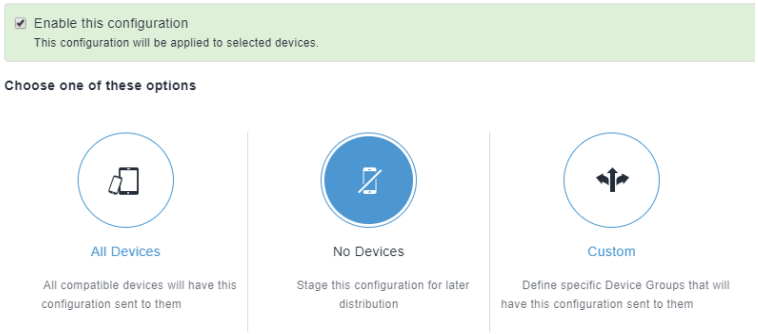
a. Click the garbage can icon and confirm the delete.

To **disable** the configuration:

a. Click the pencil icon to edit the configuration.

b. Click **Next** to go to the Distribution page.

FIGURE 5. DISABLE THE CONFIGURATION



a. Uncheck **Enable this configuration**.

b. Click **Done**.

To **remove** the configuration from your devices:

a. Click the pencil icon to edit the configuration.

b. Select **No Devices** from the Distribution page.

c. Click **Done**.

Disabling MTD on a MobileIron Go device

You can disable MobileIron Threat Defense Solution on a device with MobileIron Go client by removing the MobileIron Threat Defense configuration as follows:

1. Log in to Admin Console.
2. Go to **Devices.**
3. Click a device name to view the details page.
4. Go to **Configurations.**
5. Select the MobileIron Threat Defense configuration to be disabled.
6. Click **Exclude.**

When an MTD-enabled device is retired:

- If there is a single device in a device group on Cloud, the device is retired from MobileIron Cloud. On sync, the device remains on Threat Management Console.
- If there are multiple devices in a device group on Cloud, the device is retired from Cloud. On sync, the device is deleted on Threat Management Console.

Server-initiated mitigation and compliance

You can configure server-initiated multi-tier mitigation and compliance for managed MobileIron Go devices through the Threat Management Console. It is a best practice to apply server-initiated policies in parallel with local action policies for best coverage.

Before proceeding, perform the following tasks:

- Delete old custom attributes
- Delete old custom policies
- Delete old device groups
- Retire previously registered devices

Server-initiated mitigation and compliance includes the following actions:

1. Creating MTD custom attributes
2. Creating compliance policy rules and device groups
3. Creating the Threat Management Console Threat Response Matrix

Creating MTD custom attributes

You need to create several custom device attributes that will be applied to both Android and iOS devices. In the following procedure, create custom attributes based on threat severity.

NOTE: If you create custom attributes after you have configured the Threat Management Console and synchronized it with MobileIron Cloud, you will need to re-synchronize the Threat Management Console with Cloud before the custom attributes will appear in Threat Management Console policies.

Before you begin

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

Procedure

1. In the MobileIron Cloud Admin Console, go to **Admin > Attributes**.

   NOTE: Enter attribute names in lower case.

2. Create the custom attribute **mtdnotify**:
   a. Click **Add New**. The **Attribute Name** and **Attribute Type** fields are displayed.
   b. Select the default, **Device** as the attribute type.
   c. Name the custom attribute **mtdnotify**.
   d. Click **Save** to monitor and notify.

   This custom attribute can be applied to Low or Normal severity threats for MTD policies within the Threat Management Console.

3. Create a second custom attribute called **mtdblock**:
   a. Click **Add New**.
   b. Select **Device** as the attribute type.
   c. Name the custom attribute **mtdblock**.
   d. Click **Save** to monitor and notify.

   This custom attribute can be applied to Elevated or Critical severity threats for MTD policies within the Threat Management Console.

4. Create a third custom attribute called **mtdquarantine**:
   a. Click **Add New**.
   b. Select **Device** as the attribute type.
   c. Name the custom attribute **mtdquarantine**.
   d. Click **Save** to monitor, notify, and quarantine.

   This custom attribute can be applied to Elevated or Critical severity threats for MTD policies within the Threat Management Console.

5. Create a fourth custom attribute called **mtdtiered4hours**:
   a. Click **Add New**.
   b. Select **Device** as the attribute type.
   c. Name the custom attribute **mtdtiered4hours**.
   d. Click **Save** to monitor and notify, wait for 4 hours, block, wait for another 4 hours, and quarantine.

   This custom attribute can be applied to Low, Normal, Elevated, or Critical severity threats for MTD policies within the Threat Management Console.

   TIP: You can create more attributes for hours other than 4 hours.

Creating compliance policy rules and device groups

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

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

For each threat type, you create compliance policy rules based on the threat severity. Each of the policy types have a predefined condition, with the exception of custom policies, that determines when a device is not compliant. The administrator can choose from a list of compliance actions to be taken against violating devices.

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**:
  - Block - notify
  - Notification
  - Quarantine - remove. If Low, send notification and let user decide what action to take.
  - Tiered Compliance 23 hours
  - Tiered Compliance 4 hours

IMPORTANT: If a policy has previously been triggered on a device, adding the tiered policy will reset the policy and any compliance actions that had previously been applied. The new custom policy will be applied at the next device check-in.

Example

A managed MobileIron Go user connects to hotel Wi-Fi:

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

Creating standard policies

You can choose from a wide array of Cloud policy templates, that you can use or modify to create robust compliance policies. As an example, let's set up a policy to restart an iOS device if the jail-breaking policy is violated.

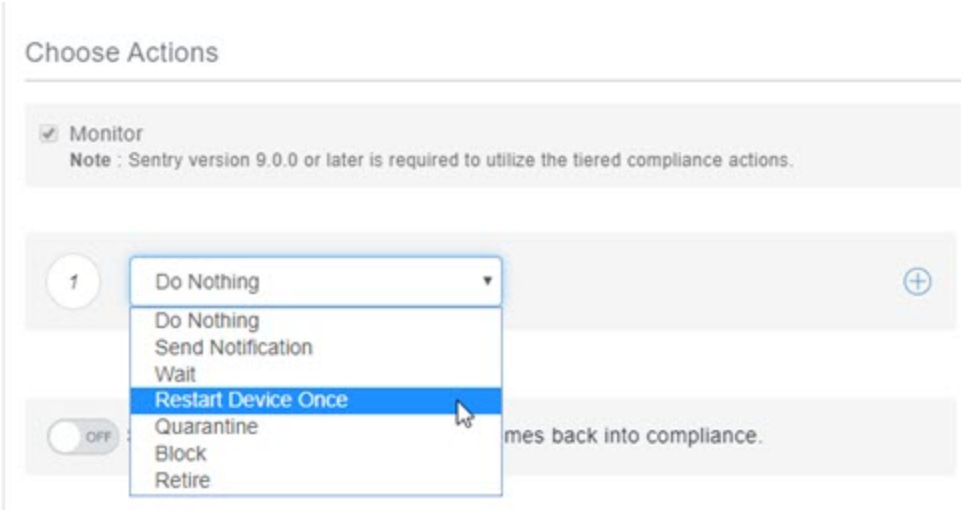
NOTE: For reference and other information about these options, see Policy > Adding a custom policy in the *MobileIron Cloud Administrator Guide*.

Procedure

1. From MobileIron Cloud Admin Console, click **Policies**. The Policies page displays.
2. Click **+Add** for policy options. The Choose Policy Type page displays.
3. Click **Compromised Devices**. The Compromised Devices menu displays.
4. Give the policy a useful name in the **Name** field. Add an optional description, if you desire.
5. From the **Choose Actions** section, click **Monitor** to configure tiered compliance actions.

   NOTE: Sentry version 9.0.0 or later is required to utilize the tiered compliance actions.
6. In the first **Actions** field, select an option from the menu:

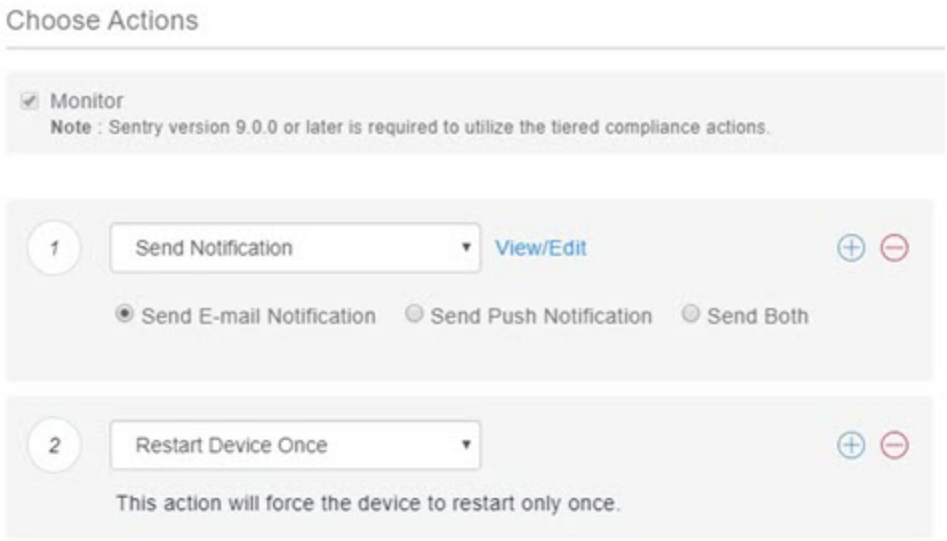
   FIGURE 6. TIERED COMPLIANCE ACTION MENU



   - **Do Nothing** (the default) – Take no action.
   - **Send Notification** – Follow the prompts to create a warning email.
   - **Wait** – Select the waiting time in minutes, days, or hours.
   - **Restart Device Once** – When a device goes out of compliance, the device is restarted. This will bring some devices back into compliance.
   - **Quarantine** – Configure default and optional quarantine actions.
   - **Block** – Uses Sentry to block managed devices from accessing email and AppConnect-enabled applications. Sentry version 9.0.0 or later is required to utilize the block action.
   - **Retire** – Retires the device. This action cannot be undone.

   For example, you might want your first action to be an email or text message to the user. So select **Send Notification**, and configure your message.
7. To add more compliance levels, click the plus (+) icon to the right of the action. To delete any level, click the red minus (–).
8. For the second action, select **Restart Device Once**. No configuration for this option is needed.

FIGURE 7. RESTART DEVICE ONCE OPTION TO LIMIT NOTIFICATIONS



9. Click **Yes, I understand**... after you read how these policies will affect devices.
10. Click **Next**. The Distribute page displays.
11. Select a distribution option.
12. Click **Done**. The policy is pushed to devices at the next check-in.

Creating custom policies

This section discusses how to define and create compliance actions using custom policies based on the MTD custom attributes. The compliance actions are evaluated during the regularly scheduled client check-in event, and the selected compliance actions are enforced on the client by MobileIron Cloud when the device is determined to be non-compliant with policy.

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 four levels of action to better manage compliance actions: Critical, Elevated, Normal, and Low.

Procedure

1. In MobileIron Cloud Admin Console, go to **Policies.**
2. Click **+ Add**.
3. Select **Custom Policy.**
4. Enter **mtdnotify** as the policy name.
5. Under Conditions, select **Custom Device Attribute.**
6. Select **mtdnotify** from the drop-down box and set the condition **is equal to** 1.
7. Under Choose Actions, select **Monitor** and **Send Email and Push Notification.**

8. Under Email Message fields, enter your preferred subject and body text.
9. Under Push Notification, enter your preferred message text.
10. Click **Yes, Next,** and **Done.**
11. Repeat this procedure to add the following policies (and any other custom policies you create) :

Policy Name	Custom Device Attribute	Attribute
mtdblock	mtdblock	• Monitor • Send Email and Push Notification • Block
mtdquarantine	mtdquarantine	• Monitor • Send Email and Push Notification • Quarantine
mtdtiered4hours	mtdtiered4hours	• Monitor • Send Email and Push Notification • All compliance actions

Creating device groups

You can create and match device groups with custom policies you have created.

Procedure

1. In the MobileIron Cloud Admin Console, go to **Devices > Device Groups.**
2. Click **+ Add**.
3. Enter **mtdNotify** as the device group name.
4. Under Dynamically Managed groups, select **Custom Device Attribute.**
5. Select **mtdnotify** from the drop-down box and set the condition **is equal to** 1.
6. Click **Save.**
7. Repeat this procedure to add the following device groups (and any other custom device groups you create):

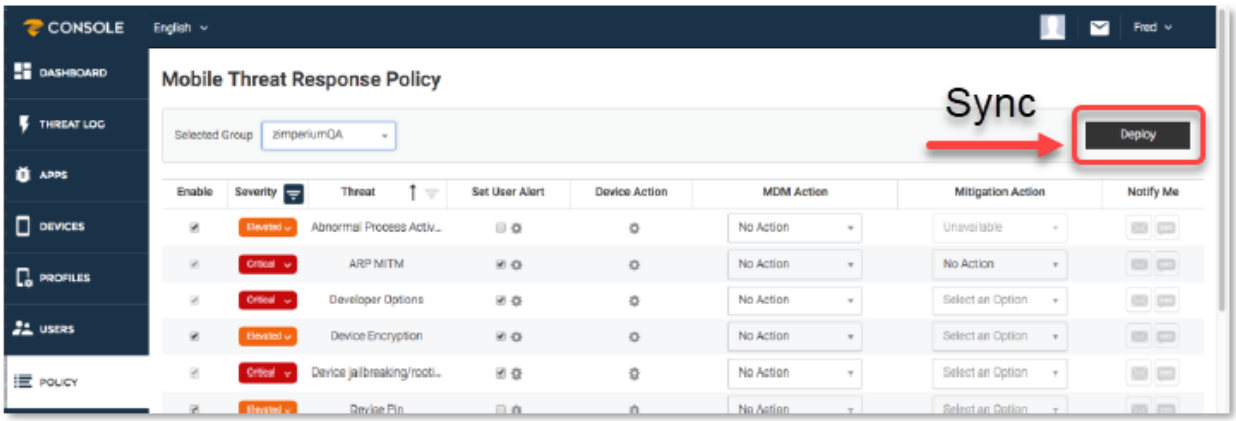
Device Group Name	Custom Device Attribute
mtdBlock	mtdblock
mtdQuarantine	mtdquarantine
mtdTiered4hours	mtdtiered4hours

Creating the Threat Management Console Threat Response Matrix

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

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

FIGURE 8. THREAT MANAGEMENT CONSOLE EXAMPLE MOBILE THREAT RESPONSE POLICY



Before you begin

If you are setting up server mitigation and compliance, complete Server-initiated mitigation and compliance . If you are setting up local mitigation and compliance, complete the procedures listed in Configuring MTD local actions for Cloud.

Configuring TRM notification and mitigation actions

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, select **Policy**. The Mobile Threat Response Policy page opens.
2. Use the pull-down menu in the **Selected Group** field to select a Cloud configuration group you set up in Creating compliance policy rules and device groups.
3. Configure the available options. See Configuring TRM notification and mitigation actions.
4. Click **Deploy** 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.

After you modify these options, click **Deploy** to send/sync the new TRM to the devices currently logged in. When integrated /synced with MobileIron Cloud, each group used for integration is created as a group with its own TRM. Select which TRM to modify with the pull-down menu next to the **Selected Group** field. Only users and devices in the selected group receive the modified TRM. See below for a sample TRM.

NOTE: You must manually sync (deploy) the Threat Management Console with MobileIron Cloud. This aligns the custom attributes in Cloud with the TRM settings.

TRM Configuration Options

The following TRM threat response policy options are available:

TABLE 2. TRM CONFIGURATION OPTIONS

Option by Column	Description
Enable Click to enable	**Enable or disable threat detections** The Threat Management Console administrator has the option of disabling certain threat detections and, therefore, the collection of associated forensics. In the **Severity** column, you can disable the status of "Elevated" or "Lower" by clearing the radio button in the row of the event. This change is effective next time you click **Deploy**. After deploying /syncing with MobileIron Cloud, when a threat is detected, the Threat Management Console instructs Cloud to move the device to the chosen custom attribute in the TRM. The workflow assigned to that custom attribute determines the action that Cloud takes on the device. The communication from the Threat Management Console to Cloud is performed securely through a MobileIron API call.
Severity Select one of four levels	**Severity threat levels** Administrators have the option of changing the threat severity levels. This is useful for different business cases. The options are "Critical," "Elevated," "Low," and "Normal."
Threats auto-populated	**Threat classes detected** The threats listed in the **Threat column** represent the classes of threats that MTD detects. Threat classes are recognized by MTD, which is able to determine when a malicious event is happening.
Set User Alert	**Enable or disable user alerts**.

TABLE 2. TRM CONFIGURATION OPTIONS (CONT.)

Option by Column	Description
Click the gear to open.	NOTE: Administrators cannot manage MTD alerts through the Threat Management Console. In order to implement and localize MTD alerts, use the **Show Notifications** option in the MTD Local Actions configuration in MobileIron Cloud.
Device Action Click the gear to open.	Select from these menu options to enable device actions on Threat Management Console: Android: • Disconnect Wifi • Network Sinkhole • Disable Bluetooth iOS • Network Sinkhole • Disable Bluetooth Samsung Knox • Use Android Actions • Disable App • Uninstall App • Block App • Isolate from Network • Data Loss Prevention
MDM Action Click the gear to open.	When an actionable threat is detected, you can define what actions to take, through the MobileIron Cloud Admin Console. The custom attributes you created in Creating MTD custom attributes will populate this column, but you can't modify them from Threat Management Console.
Mitigation Action Select an option	When a threat that was detected by the 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. 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**.

TABLE 2. TRM CONFIGURATION OPTIONS (CONT.)

Option by Column	Description
	This action removes the device from the group it was assigned to when the threat was detected. **Possible mitigation actions for a threat** Due to the nature of some threats, not all threat classifications can be mitigated. The following list provides possible mitigation actions for a threat when the trigger action occurs. • **All man-in-the-middle attacks (MITM)**—When the device connects to a different BSSID. • **Root/Jailbroken**—When the root flag on devices changes from true to false. • **EOP, system tampering, abnormal process activity**—No mitigation, the only mitigation is to flash the device because it has been compromised. • **USB debugging**—When USB debugging is enabled.
Notification (Notify Me) Click an icon	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 log-in.

Phishing protection for MTD devices

MobileIron Threat Defense Solution detects and prevents phishing attempts on MTD-enabled iOS and Android devices using a multi-layered approach. The following quick reference table identifies the primary anti-phishing options for MTD devices in this release:

TABLE 3. MTD ANTI-PHISHING OPTIONS FOR CLOUD 75 RELEASE

Anti-phishing option	Supported platforms	Key characteristics	For more information
Threat Management Console Phishing Policy			
Enable phishing protection and enable URL sharing	iOS and Android	Enables Threat Management Console phishing functions and activates URL sharing.	See Enable Threat Management Console anti-phishing VPN.
Local VPN for Phishing		Enables phishing protection through a local VPN and blocks detected phishing URLs.	
Enable content inspection on remote server		Checks links against a larger, remote database.	
MTD Anti-phishing Protection Configuration			
Content Blocker	iOS	Blocks all network traffic when a phishing threat is detected. iOS client user must enable.	See Enabling additional MTD anti-phishing protection
URL Handler	Android	Intercepts the URL on the default browser, scans it, and if malicious, blocks it. Android client user must enable.	
Use VPN to analyze malicious URLs	iOS	Checks links against an on-device database.	
	Android	Checks links against an on-device database. **Requires**: MI Tunnel app 4.6.0 through the latest version as supported by MobileIron.	See Enabling additional MTD anti-phishing protection, then Android anti-phishing using MobileIron Tunnel app

TABLE 3. MTD ANTI-PHISHING OPTIONS FOR CLOUD 75 RELEASE (CONT.)

Anti-phishing option	Supported platforms	Key characteristics	For more information
	Android Enterprise	Checks links against an on-device database. **Requires**: • MI Tunnel app 4.6.0 through the latest version as supported by MobileIron. • App configuration for Tunnel.	See Android anti-phishing using MobileIron Tunnel app, then Creating an MI Tunnel app configuration for AE devices
MTD general			
MobileIron Tunnel configuration	Android	Pushed to Android users as needed. System configuration. Not editable.	See About the MobileIron Tunnel Configuration.

Advanced phishing protection for managed devices

From MobileIron Cloud 75 through the most recently released version as supported by MobileIron, you can enable Threat Management Console advanced phishing protection to MTD-enabled iOS and Android devices without any client user action. This tool provides full coverage against risky URLs through an automatically enabled VPN.

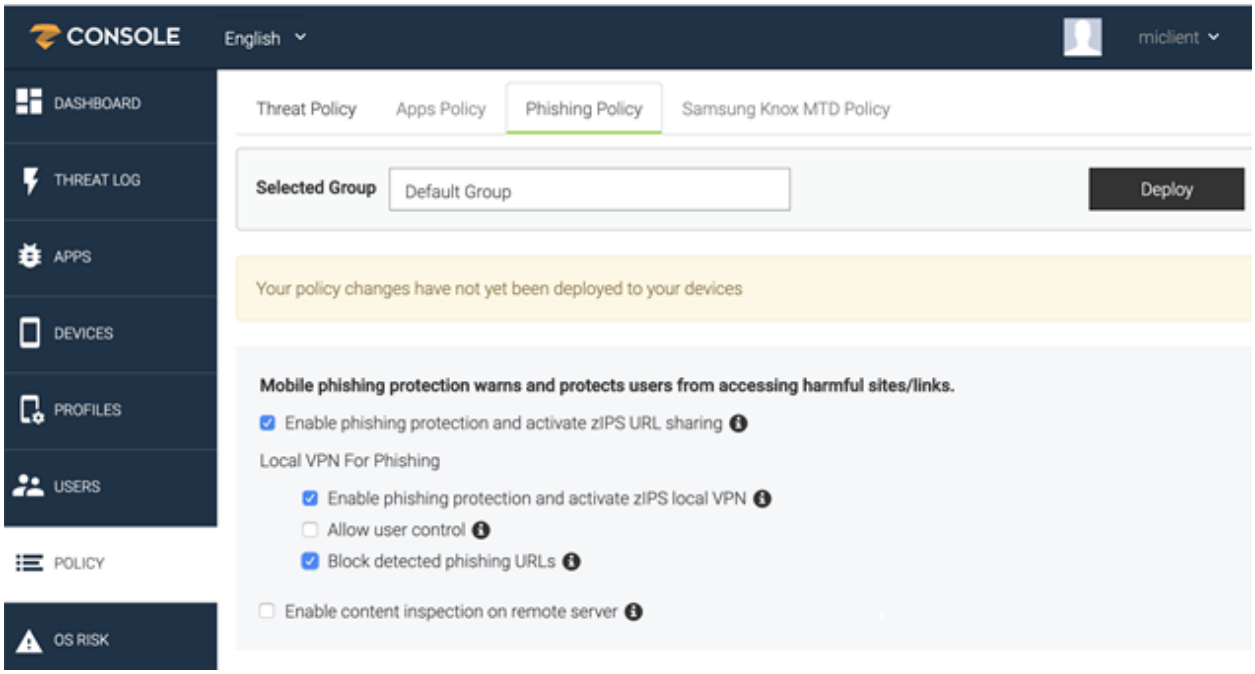
NOTE: MTD anti-phishing for Android devices requires Tunnel 4.6.0 through the latest version as supported by MobileIron.

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.

FIGURE 9. THREAT MANAGEMENT CONSOLE PHISHING POLICY PAGE



4. In the **Selected Group** field, select the group to receive phishing protection.
5. Select from the following options:

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

     NOTE: Users who launch a device-level VPN app such as 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** - Disabled 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 multilevel protection.

6. Click **Deploy** to distribute the phishing protection policy to the selected device group. For iOS clients, anti-phishing is enabled.
7. For Android clients, proceed to Android anti-phishing using MobileIron Tunnel app.

Enabling additional MTD anti-phishing protection

You have the option to enable additional MTD anti-phishing protections for managed Android and iOS devices:

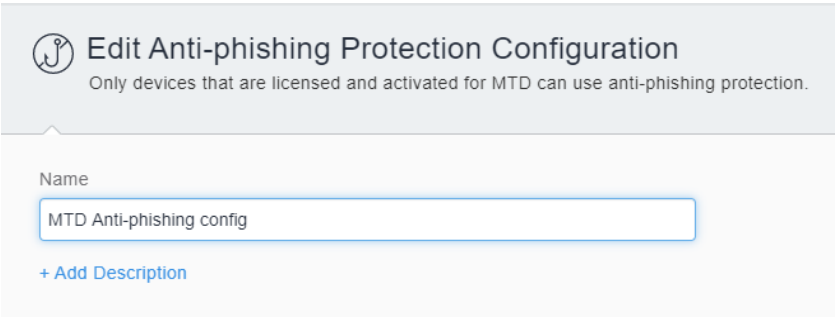
- **On-device VPN to analyze malicious URLs** – This option uses VPN to provide anti-phishing protection without requiring end-user confirmation. Tapped links are checked against an on-device database of malicious URLs.
- **Content Blocker** – (iOS devices) This option blocks all network traffic when a phishing threat is detected. Once cleared, network traffic is again allowed. The end user must enable this feature.
- **URL Handler** – (Android devices) When the device user taps on a URL, the MobileIron phishing protection intercepts the URL on the default browser, scans it, and if malicious, blocks it. Otherwise, the URL opens. See Understanding URL Handler.

These additional anti-phishing configurations can be used in conjunction with Threat Management Console anti-phishing policies.

Procedure

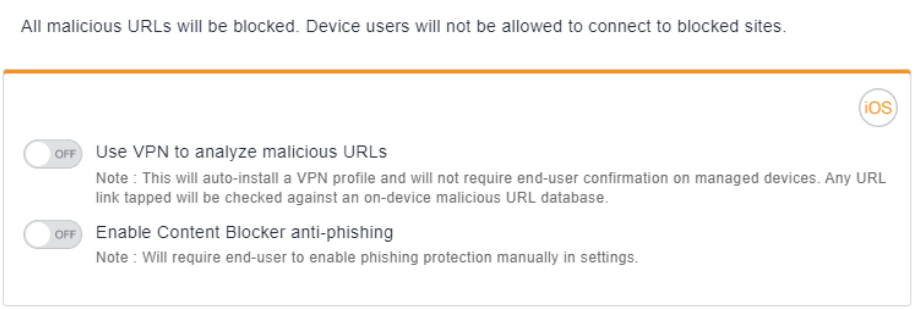
1. Log in to MobileIron Cloud Admin Console.
2. Go to **Configurations.**
3. Click **+Add.**
4. Click **Anti-phishing Protection**. The Create Anti-phishing Protection Configuration menu opens.

FIGURE 10. OPENING AN MTD ANTI-PHISHING CONFIGURATION



5. In the Create Anti-phishing Protection Configuration page, enter a **Name** for the configuration.
6. (Optional) Click **+Add Description.**
7. In the **iOS** section, select from the following options:

FIGURE 11. IOS MTD ANTI-PHISHING OPTIONS

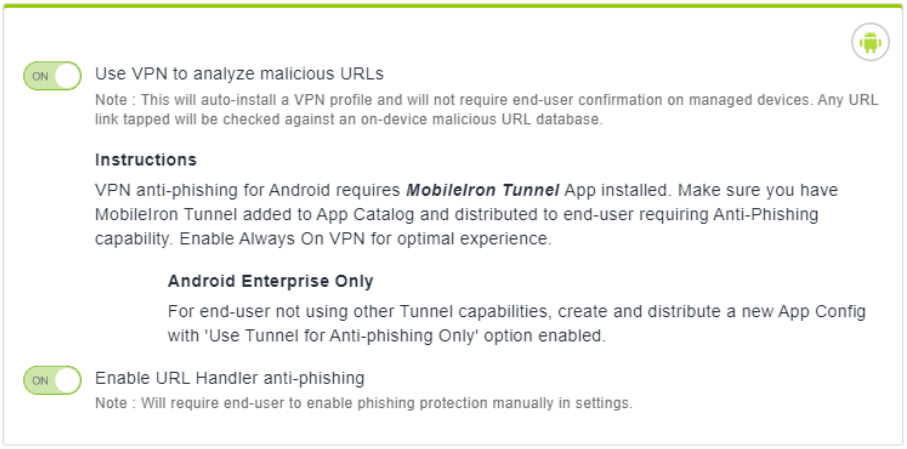


a. **Use on-device VPN to analyze malicious URLs**

b. **Enable Content Blocker anti-phishing**

8. In the **Android** section, select from the following configuration options:

FIGURE 12. ANDROID MTD ANTI-PHISHING OPTIONS



a. **Use 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 URL Handler anti-phishing**. See Understanding URL Handler.

9. Click **Next.**

10. Select the **Enable this configuration** option.

11. Select one of the following distribution options:

- **All Devices**
- **No Devices (default)**

- **Custom**

12. Click **Done.**

NOTE: Content Blocker anti-phishing will not work on iOS devices that have "Popups in Safari not allowed" enabled in their iOS device settings. Distribute an iOS restriction configuration with "Block pop-ups" disabled, and verify that this restriction is disabled on client devices.

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 managed 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.

Android anti-phishing using MobileIron Tunnel app

Once you have Advanced phishing protection for managed devices for Android devices through the Threat Management Console, you will need to provision Android clients with the MobileIron Tunnel app, to provide a VPN pathway. See Deploying MobileIron Tunnel app to Android and Android Enterprise devices.

NOTE: MTD anti-phishing for Android devices requires Tunnel 4.6.0 through the latest version as supported by MobileIron.

Android Enterprise (AE) clients need an additional app configuration with **Use Tunnel for Anti-phishing Only** option enabled. This permits anti-phishing for end users not using other Tunnel capabilities. See Creating an MI Tunnel app configuration for AE devices.

Before you begin

- Verify that you are running the MobileIron Tunnel app 4.6.0 through the latest version as supported by MobileIron.
- Complete the task Advanced phishing protection for managed devices.

Deploying MobileIron Tunnel app to Android and Android Enterprise devices

Procedure

1. In the MobileIron Cloud portal, go to **Apps >App Catalog**.
2. Find the app in the Google Play Store.
3. Click the app entry.
4. Accept permissions on behalf of Android Enterprise users.
5. Click **Next**.
6. Select a distribution option.
7. Expand **Advanced Options & App Configuration**.
8. Use the following guidelines to complete the options:

TABLE 4. AVAILABLE APP SETTINGS

Setting	Description
Install on Device	Select this option to start installation immediately after registration. The user will be prompted to confirm installation of the app except when the device is a Samsung Knox device and the silent installation option below has been selected.
Do not show app in end user App Catalog	Select this option if you do not want the user to see the app in the app catalog on the device.
Silently install on Samsung Knox devices	Select this option if you do not want the user prompted to confirm installation on Samsung Knox devices.
Set App Install Priority	For Android Enterprise apps you can prioritize downloading of specific apps before other apps. For example, you can prioritize the download of Tunnel and Email apps before other noncritical apps. The following are the available priority level options: • **High** • **Medium** (selected by default)

TABLE 4. AVAILABLE APP SETTINGS (CONT.)

Setting	Description
	• **Low** This setting is applicable for In- House, Public, Private and Web apps. The in-house apps are installed via the client and the public and private are installed via Google. The app priority is applied only to those apps that are installed via the same channel.
Install only when connected to Wi-Fi	Select this option to install the app only when the device is connected to the Wi- Fi.
Install only when charging	Select this option to install the app only when the charging of the device is in progress.
Install only when idle	Select this option to install the app only when the device is in idle (not actively used by the user).

9. Click **Next**.
10. Select a promotion option.
11. Click **Done**.

Next steps

To complete Android anti-phishing for Android Enterprise clients, continue to Creating an MI Tunnel app configuration for AE devices.

Related topics

For more information about the App Catalog, see "Managing mobile apps for Android" in the *MobileIron Apps@Work Guide*.

Advanced phishing protection for managed devices

Creating an MI Tunnel app configuration for AE devices

The final step to enable anti-phishing protection on Android Enterprise (AE) devices is to create and push an app configuration file for MobileIron Tunnel to AE devices.

Before you begin

Complete the following tasks before you begin:

- Advanced phishing protection for managed devices
- Android anti-phishing using MobileIron Tunnel app

Procedure

1. From the MobileIron Cloud **Apps > App Catalog** page, open the **MobileIron Tunnel** app.
2. Click the **App Configurations** tab. The **Managed Configurations for Android** page opens.
3. Enter a name for this Tunnel app configuration, and an optional description.
4. Under **MobileIron Threat Defense Settings**, click **Use Tunnel for Anti-phishing Only**.

   NOTE: VPN anti-phishing requires that the Tunnel app configuration is installed on the device. Select this option if no other Tunnel-related functionality is being used, and distribute the app to users who need anti-phishing.
5. Distribute the app to Android Enterprise devices.

About the MobileIron Tunnel Configuration

A default MobileIron Tunnel configuration (MI Tunnel config) is available from Cloud 74 through the latest release as supported by MobileIron. If an Android device does not have a tunnel configuration distributed, the server will push the default MI Tunnel config when needed.

NOTE: MI Tunnel config is generated by the system and is always available. It is not editable.

Understanding URL Handler

You can configure URL Handler anti-phishing protection for Android and Android Enterprise devices with or without the anti-phishing VPN option. 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 Cloud, URL Handler cannot provide anti-phishing protection if the end user types the URL into a browser manually.

1. In Cloud, you create an MTD anti-phishing configuration to ensure that device users will be blocked from malicious URLs.
2. Device users enable MobileIron URL Handler 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 MobileIron Go 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 MobileIron Go as the default browser.

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

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

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. MobileIron Go 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.

TABLE 5. DEFAULT BROWSER ACTION BY ANDROID RELEASE

Device Mode	How to select MobileIron client as the default browser
Device Admin mode	**Android 7.0 through the latest version as supported by MobileIron**: User are guided to select MobileIron client as the default browser app from the default apps settings.
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 is set as the default browser. The user is only prompted to set MobileIron client as the default browser if the setting becomes disabled.
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.

TABLE 5. DEFAULT BROWSER ACTION BY ANDROID RELEASE (CONT.)

Device Mode	How to select MobileIron client as the default browser
	• **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 6. EXPECTED CLIENT BEHAVIOR BY ANDROID RELEASE

Device Mode	Description	Expected behavior
Kiosk	Samsung devices from Android 5.0 to 8.0 and non-Samsung devices from Android 5.0 to 7.0.	When URL clicks are inside the kiosk, if the URL is safe, it will display with browsers available in the kiosk mode. Kiosk mode remains active and functional if the phishing protection was enabled outside the kiosk and then removed while the device is in kiosk mode. Exiting in and out of kiosk mode keeps the phishing protection functional inside and outside the kiosk. When a user taps a URL: • If the URL is not safe, it will be blocked. • If the URL is safe, MobileIron client will render the URL with the browser available or display a list of browsers for end user to choose to display URLs “Just Once” or “Always”. ◦ **Just Once** – MobileIron will continue to show a list of browsers if there are multiple browsers. ◦ **Always** – MobileIron client will save the selected browser. Next time, the saved browser package is used to render safe URLs. NOTE: Once the user selects "Always" through the MobileIron client's list of browsers, the user cannot change the default browser for rendering safe URLs. As a workaround, install a new browser. On clicking the next safe URL, the user will be again shown a list of browsers, including the new browser.
Kiosk Android Enterprise Device Owner	Android 5.0 through the latest version as supported by MobileIron.	

Legacy Android phishing configuration tasks

These legacy Android clients require their users to select the MoblileIron client as the default browser, and some additional tasks.

TABLE 7. ADDITIONAL PHISHING CONFIGURATION TASKS

Task	Description
AppConnect (Android 5.0+)	In Android AppConnect container configuration, administrators should distribute Web@Work and enable the following lockdowns for the phishing protection: • Allow Web • Allow non-AppConnect apps to open URLs in Web@Work This will ensure that on URL clicks inside and outside the container, MobileIron client can intercept the URL for phishing protection and use the installed Web@Work to display the safe URLs. For more information, see the AppConnect section in the MobileIron Cloud product documentation. (MobileIron credentials are required to access documentation in the Support Community.)
Kiosk Device Admin mode (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+)	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.

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 the Device Details page to verify anti-phishing is enabled

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

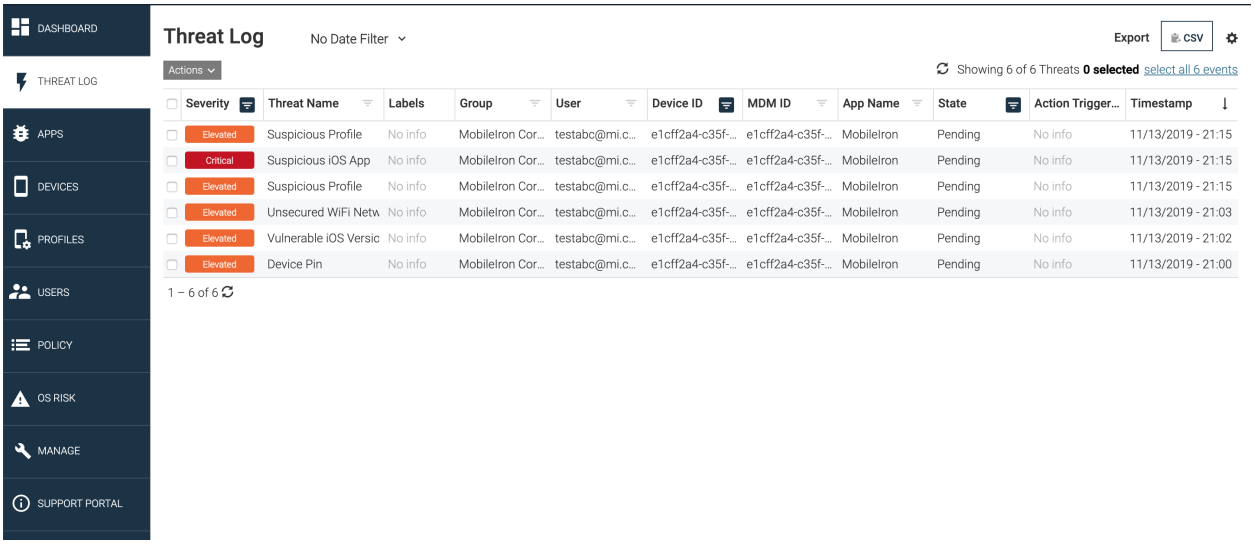
Procedure

1. From the MobileIron Cloud Admin Portal, select **Devices > 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 anti-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 anti-phishing protection and have enabled it.
   - **Not Enabled** – Device users received a request from the administrator to manually activate MobileIron anti-phishing protection and have NOT enabled it.
   - **Unknown** – Device users have likely not set the device's default browser to MobileIron Go, and therefore, not enabled MobileIron anti-phishing protection.

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 13. THREAT MANAGEMENT CONSOLE THREAT LOG



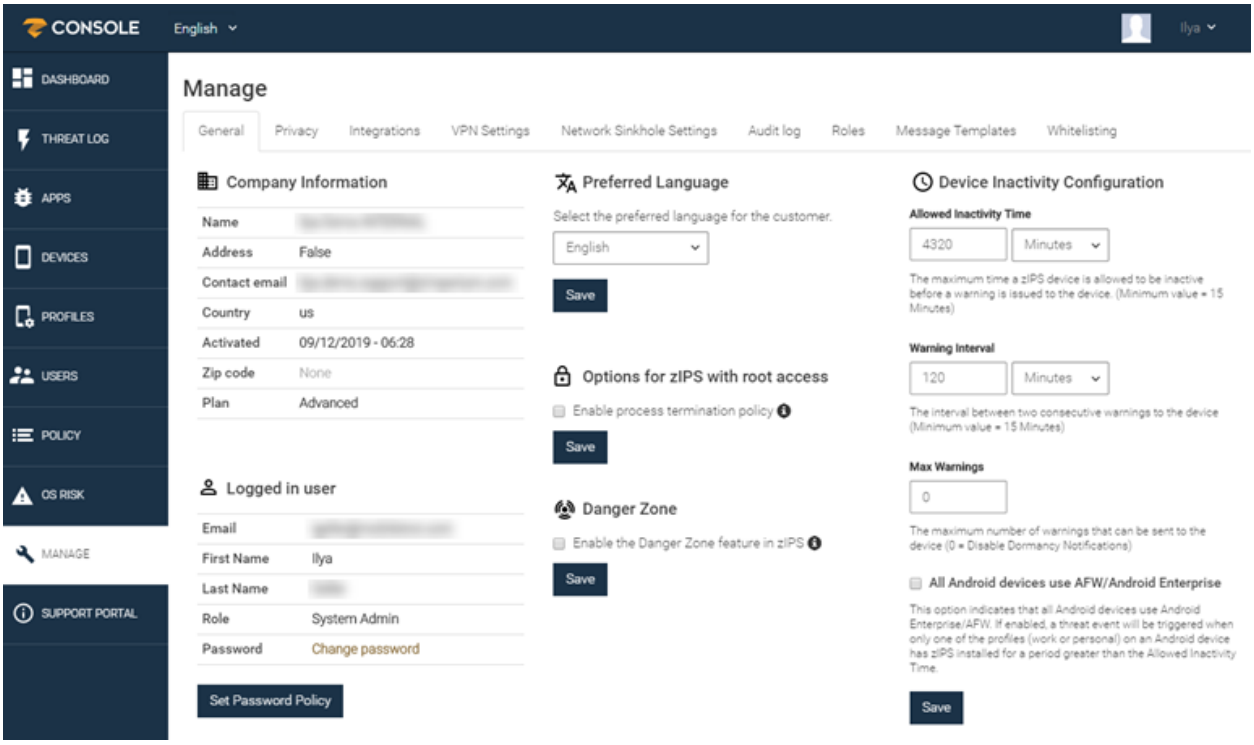
Configuring Threat Management Console

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.

FIGURE 14. THREAT MANAGEMENT CONSOLE > MANAGE > GENERAL TAB



Here are specific configuration elements for the General tab:

TABLE 8. GENERAL TAB SETTINGS

Section	Description and actions
Company Information	Enter your company information, including a contact email. Your plan type and activation date are populated automatically.
Logged in user	Enter the name, email address, system role, and password for the current user. Click **Change password** to open the Set Password menu. Click **Save** to retain your changes.
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 8. GENERAL TAB SETTINGS (CONT.)

Section	Description and actions
Preferred Language	Choose the language for the Threat Management Console. The current options are English, Japanese or Hebrew. Click **Save** to retain your changes.
Options for zIPS with root access	This feature is not supported for MTD clients.
Danger Zone	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 **Save** to retain your changes.
Device Inactivity Configuration	This configuration controls how long the system waits before determining that a device is dormant: 1. **Allowed Inactivity Time**: 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 **Seconds**, **Minutes**, or **Hours** in the right box. 2. **Warning Interval (Grace Period)**: 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 **Seconds**, **Minutes**, or **Hours** in the right box. 3. **Max Warnings**: The number of warnings that can be sent to the device in the grace period. An entry of '0' disables the grace period. 4. **All Android devices use AFW/Enterprise**: 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 **Allowed Inactivity Time**. Click **Save** to retain your changes.

Managing devices in Threat Management Console

In the Threat Management Console, the Devices page displays the complete list of devices that are configured in this environment. Devices appear automatically in this page when an MTD-enabled new client has checked in. In addition, this page lists devices that are synchronized with MobileIron Cloud. The disabled devices in the listing are devices that have synchronized with Cloud, but have not yet checked in.

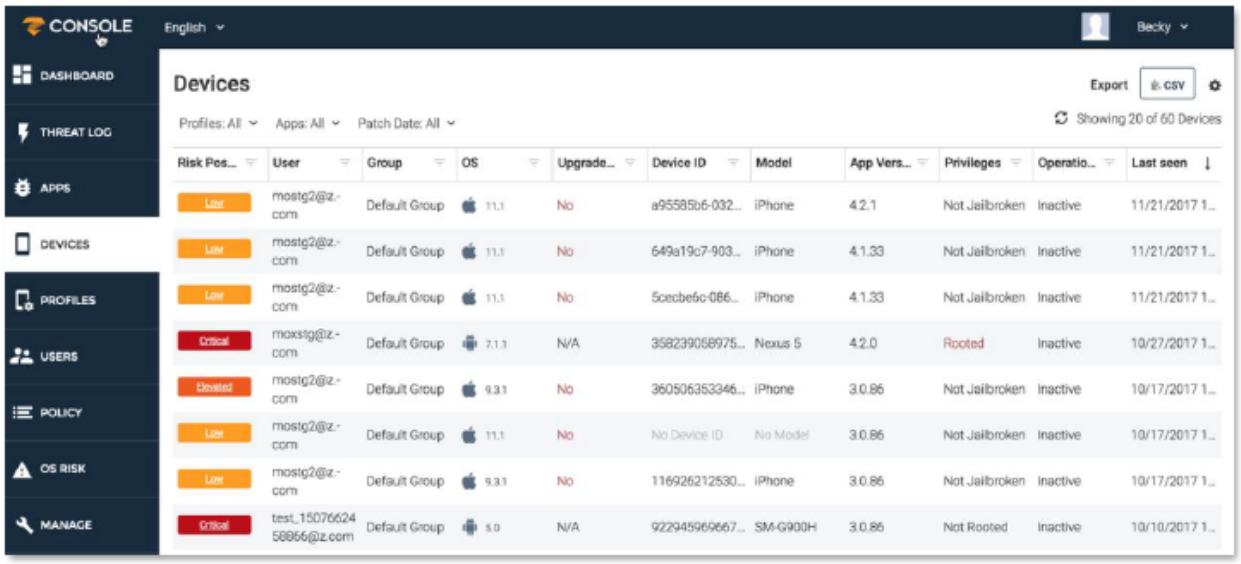
The device information includes the following:

- 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 MobileIron Go)
- Privileges (for example, Rooted, Jailbroken, No Jailbroken)
- Operational Mode (Inactive, Active)
- Last Seen (Last date and time the device was seen by MobileIron Go, 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 15. DEVICES IN THREAT MANAGEMENT CONSOLE



General display filters

Click one of the following options to filter your device list:

- **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 9. DEVICES PAGE FILTER CATEGORIES

Column	Description
Risk Posture	Displays devices that match the selected risk posture or postures
User	Displays devices that match the selected user or users
Group	Displays the devices that match the selected management console groups
OS	Displays devices that match the selected OS versions
Upgradable	Displays devices that match the selected upgradable flag value
Device ID	Displays devices that match the selected device IDs
App Name	Displays devices running the selected MobileIron Go app
App Version	Displays devices running the selected versions of the MobileIron Go app
Privileges	Displays devices that are jail-broken or rooted
Operational Mode	This column displays the following: **Active**: describes devices that are communicating on a regular basis to the management console **Inactive**: describes devices that have been active but are now not communicating **Pending Activation**: describes devices that have synchronized through Cloud, but have not yet checked in
Last Seen	Sorts by the date or time the filtered devices were last seen

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 16. EXPORT ICON (UPPER-RIGHT CORNER)

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 is displayed.
- The **Logout** function is not supported by MobileIron and won't work with MTD.
- 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 Cloud as your Mobile Device Management (MDM) server in the Threat Management Console, and distributing MobileIron Go 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 managed devices. See Advanced phishing protection for managed 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 Cloud
- Managed apps on Cloud 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 MobileIron Go for Android users install an app on their phone that wasn't downloaded from the Windows App Store or Google Play Store (including MobileIron Go 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 configure mitigation and compliance for managed MobileIron Go devices using the MTD Local Actions threat defense configuration. This method does not require a connection to the server. The actions are applied locally on the device. Local action policies can be applied in parallel with server-initiated policies for best practice coverage.

Mitigation and compliance using MTD local actions configuration includes the following actions:

- Configuring MTD local actions for Cloud
- Setting the sinkhole action on iOS devices

Configuring MTD local actions for Cloud

Using the MobileIron Threat Defense Local Actions configuration, you can set specific local actions to be taken on supported iOS and Android devices when the MTD-enabled client detects a threat. Local actions will only be taken on devices that are licensed and activated for MTD.

Before you begin

Be sure you have configured the items listed in Activating MobileIron Threat Defense.

Procedure

1. Log in to MobileIron Cloud.
2. Go to **Configurations**.
3. Click **+Add**.
4. Click **MobileIron Threat Defense Local Actions**.
5. In the Create MobileIron Threat Defense Local Actions Configuration page, enter a **Name** for the configuration.
6. Enter an optional **Description.**
7. In the Configuration Setup section, scroll to the category containing the threat you want to enable.
   - Network Threats
   - Device Threats
   - App Threats

   The number of threats are indicated for each threat category.
8. (Optional) Select specific threats and turn notifications on or off for them. To do so:

a. Expand the threat category.
b. Click the check box for the threats you want to configure. See the following tables for iOS and Android devices.
c. Threats with available actions for iOS clients will have a drop-down menu in the **Local IOS Action** category.
d. Threats with available actions for Android clients will have a drop-down menu in the **Local Android Action** category.
e. Click the **Show Notification** slider to the right of the action menus to enable notification for the threat.
f. (Optional) Select multiple threats and click the **Set Bulk Local Actions** to perform Local Android Action, Local iOS Action, or set Notification on or off. The total number of enabled local actions is displayed for your reference.

9. Click **Next.**
10. Select the **Enable this configuration** option, if it is not already enabled.
11. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
12. Click **Done.**

The following table lists the actions that are available for MTD threats on iOS devices:

TABLE 10. THREATS ON IOS DEVICES

Local Compliance Action	Definition
None	No action will be taken on the device.
Block Email Access and AppConnect Apps	• Disables email access. • Disables AppConnect-enabled applications and blocks the transfer of AppConnect data between Client and Cloud.
Network Sinkhole	Isolates the device from the network.

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.

The following table lists the actions that are available for MTD threats on Android devices:

TABLE 11. MTD THREATS ON ANDROID DEVICES

Local Compliance Action	Definition
None	No action will be taken on the device.
Wipe the device	Retires the device.
Quarantine - Remove all configurations	Removes configurations that provide access to corporate resources, such as certificates. Configurations that secure the device are not removed.
Quarantine - Do not remove Wi-Fi settings for Wi-Fi only devices	Removes configurations that provide access to corporate resources, such as certificates, with the exception of the Wi-Fi settings on Wi-Fi only devices. Configurations that secure the device are not removed.
Quarantine - Do not remove Wi-Fi settings for all devices	Removes configurations that provide access to corporate resources, such as certificates, with the exception of Wi-Fi settings on all devices. Configurations that secure the device are not removed.
Quarantine - Remove managed apps and block new downloads	Removes access to the company App Catalog and/or work apps.
Disable Bluetooth	Disables Bluetooth to the company App Catalog and/or work apps.
Disconnect from Wi-Fi	Disables Wi-Fi to the company App Catalog and/or work apps.

Editing an MTD local actions configuration

The threat detection list is updated when new threats are identified or existing threats are removed. To edit an MTD local actions configuration to update the threats, use the following procedure:

1. Log in to MobileIron Cloud.
2. Go to **Configurations.**
3. Select the check box next to the MTD configuration that you want to edit.
4. Click **Edit.** The Edit MobileIron Threat Defense Solution Local Actions Configuration page is displayed.
5. Click **^** next to Network, Device, or App Threats to edit the actions for a threat category. This selection controls which notifications are enabled on the device and which mitigation actions are taken locally on the device when a threat is detected. For more information about each threat, hover over the info icon next to the name of the threat.
6. (Optional) Select multiple threats and click the **Set Bulk Local Actions** to perform Local Android Action, Local iOS Action, or set Notification on or off. The total number of enabled local actions is displayed for your reference.
7. Click **Next.**
8. Select the **Enable this configuration** option if required.
9. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

10. Click **Done.**

Customizing local threat notification text

You can customize the local threat notification text for MobileIron Go devices through the Threat Management Console **Threat Policy** page. You also have the option to disable or re-enable the feature in the MTD Local Actions configuration.

Disabling or re-enabling custom local threat notifications

Custom local threat notifications are enabled and disabled from the Cloud **Configurations** page. This feature is enabled by default.

Procedure

1. From the Configurations page, create or open an MTD Local Actions configuration.
2. Click the check box below the Description: **Enable ability to customize end-user local notifications**.
3. **Save** the configuration.

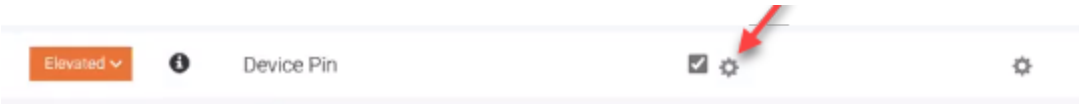
Customizing local threat notifications

Once custom end-user local notifications are enabled, you can customize the notification text that your device users receive, in any of the supported languages.

Procedure

1. From the Threat Management Console, go to Policy > Policies > **Threat Policy** page.
2. From the **Selected Group** drop-down menu, select the Group to receive the notification text.
3. From any enabled threat, click the **Set User Alert** check box, and click the Settings icon to open the **Alert User Message Configuration** page.

FIGURE 17. THE SETTINGS ICON FROM SET USER ALERT CHECK BOX



4. From the Alert User Message Configuration page, scroll to the enabled threat and enter the text, button label, and button link information for the alert you are customizing.

FIGURE 18. ALERT USER MESSAGE CONFIGURATION PAGE

- **Alert text field**: Enter the alert text you want your device users to see when a threat is detected.
- **Button Label**: This option is not supported.
- **Button Link**: This option is not supported.

5. Click **Submit**.
6. Click **Save & Deploy**.

The policy is pushed to the client group at the next check-in.

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 MobileIron Go Local Actions:

TABLE 12. AVAILABLE NETWORK THREAT POLICIES

Threat	Mitigation when the following events occur
ARP Scan	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).
Captive Portal	Detected that the device connected to a captive portal network.
Danger Zone Connected	Danger Zone Connected provides device users with information on nearby Wi-Fi networks and their potential risk. If an iOS or Android device user does connect to a malicious Wi-Fi access point, the device user will be notified: "This device has connected to a Wi-Fi network where malicious attacks have been observed. It is recommended to disconnect immediately and use an alternative network." **Procedure** To enable Danger Zone Connected: 1. Log into the Threat Management Console, and navigate to the **Manage > General** page. 2. Click **Enable the Danger Zone feature in zIPS**. NOTE: 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: • Network name and BSSID fields are not available for threat forensics information. • Network threats are not mitigated. If Threat Management Console cannot get the BSSID from the device, then the Danger Zone Connection threat will not work.
IP Scan	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.
Internal Network Access	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.
MITM	Man-in-the-Middle attack where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.
MITM-ARP	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.

TABLE 12. AVAILABLE NETWORK THREAT POLICIES (CONT.)

Threat	Mitigation when the following events occur
MITM-Fake SSL certificate	Man-in-the-Middle attack using fake certificate where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.
MITM-ICMP Redirect	Man-in-the-Middle attack using ICMP protocol where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device.
MITM-SSL Strip	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.
Network Handoff	Network handoff allows a device to alter routing on a network, potentially allowing for a man-in-the-middle attack.
Rogue Access Point	Rogue Access Point exploits a device vulnerability to connect to a previously known Wi-Fi network by masking preferred/known networks.
Rogue Access Point: Nearby	Rogue Access Point exploits a device vulnerability to connect to a previously known Wi-fi network by masking a nearby network.
SSL/TLS Downgrade	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.
TCP Scan	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.
UDP Scan	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.
Unsecured WiFi Network	A unsecured Wi-Fi network is vulnerable for a network attack.

Local Actions Device threats

The following Device threats are available in MobileIron Go Local Actions:

TABLE 13. AVAILABLE DEVICE THREAT POLICIES

Threat	Mitigation when the following events occur
Abnormal Process Activity	Detected abnormal activity. User device is being monitored for any attacks.
App Tampering	Existing app libraries may have been modified, or a foreign library may have been injected into the app.
BlueBorne Vulnerability	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.
DNS Change	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.
Daemon Anomaly	Daemon Anomaly indicates abnormal system process activities which could indicate that the device has been exploited.
Developer Options	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.
Device Encryption	Device Encryption notifies an administrator when a device is not setup to use encryption to protect device content.
Device Pin	Device Pin notifies the administrator when a device is not setup to use a PIN code or password to control access to the device.
Device jailbreaking/rooting	Jailbreaking and rooting are the processes of gaining unauthorized access or elevated privileges on a system. Jailbreaking and rooting can potentially open security holes that may have not been readily apparent, or undermine the device's built-in security measures.
EOP	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.
File system changed	A normal file system change.
Gateway Change	Gateway configuration change on the mobile device that can be indicative of sending traffic to a non-intended destination.
Proxy Change	Proxy configuration change on the mobile device that can be indicative of sending traffic to a non-intended destination.
SELinux Disabled	Security-enhanced Linux (SELinux) is a security feature in the operating feature

TABLE 13. AVAILABLE DEVICE THREAT POLICIES (CONT.)

Threat	Mitigation when the following events occur
	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.
Sideloaded App(s)	Sideloaded apps are installed independently of an official app store and can present a security risk.
Stagefright Vulnerability	Stagefright vulnerability indicates the device is on an OS patch version susceptible to compromise.
Suspicious Profile	Suspicious profiles identifies profiles that are untrusted or not explicitly trusted. MobileIron recommends that you review the profile and mark it as trusted or untrusted.
System Tampering	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.
USB Debugging Mode	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.
Unknown sources download config change	Allows user to download an app not in Google Play store.
Untrusted Profile	An untrusted profile is considered unsafe to install on your devices. An untrusted profile could be used to control devices remotely, monitor and manipulate user activities, and /or hijack traffic.
Vulnerable Android Version	MobileIron has detected that the Android version installed on your device is not up-to-date. The outdated operaing 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.
Vulnerable iOS Version	MobileIron has detected that the iOS version installed on your device is not up-to-date. The outdated operaing 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.
Vulnerable, non-upgradeable Android Version	MobileIron detected a device running a vulnerable Android version. However, the device is not eligible for an operating system upgrade at this time.
Vulnerable, non-upgradeable iOS Version	MobileIron detected a device running a vulnerable iOS version. However, the device is not eligible for an operating system upgrade at this time.

Local Actions App threats

The following App threats are available in MobileIron Go Local Actions:

TABLE 14. AVAILABLE APP THREAT POLICIES

Threat	Mitigation when the following events occur
Out of Compliance App	An app that is considered to be out of compliance with your corporate policy. When apps designated as "out of compliance" are detected on an MTD-enabled client device, the device user sees a threat warning and a request to remove the app from the device.
Suspicious Android App	A known risky app that attempts to take control of the user device in some manner (e.g. elevate privileges, spyware, etc.)
Suspicious iOS App	A known and risky app that attempts to take control of the device in some manner (e.g. elevate privileges, spyware, etc.)

Configuring an out of compliance Local Actions configuration

MTD Plus customers can configure an app compliance configuration that will protect client users from installing disapproved apps.

Before you begin

This feature is available only with an MTD Plus license. See your MobileIron representative for more information.

Procedure

1. From the MobileIron Cloud Admin Console, navigate to the **Configurations** page.
2. Click **+Add.** The Add Configuration page displays.
3. Optional: Enter "MobileIron Threat Defense Local Actions" in the Search Configurations field.
4. Click **MobileIron Threat Defense Local Actions**. The Create MobileIron Threat Defense Local Actions Configuration page displays.
5. Enter a name, and optional description.
6. Scroll down to **Malware Threats**, and click the upcarat to display the menu.
7. From the options, click **Out of Compliance App**.
8. From the first drop-down menu, select a local action for iOS clients. The options are:
   - None
   - Block email access and AppConnect apps
   - Network sinkhole
9. From the second drop-down menu, select a local action for Android clients. The options are:
   - None
   - Wipe the device

- Quarantine: Remove All Configurations
- Quarantine: Do not remove Wi-Fi settings for Wi-Fi-only devices
- Quarantine: Do not remove Wi-Fi settings for all devices
- Quarantine: Remove Managed apps and block new downloads
- Disable Bluetooth
- Disconnect from WIFI

10. Click the **Show Notification** slider if you want end users to see the notifications.
11. Click **Next**. Click the **Enable this configuration** switch if not already checked.
12. Choose one of the following options:
    - All Devices
    - No Devices
    - Custom
13. 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 Configuring MTD local actions for Cloud.
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 configuration. 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.

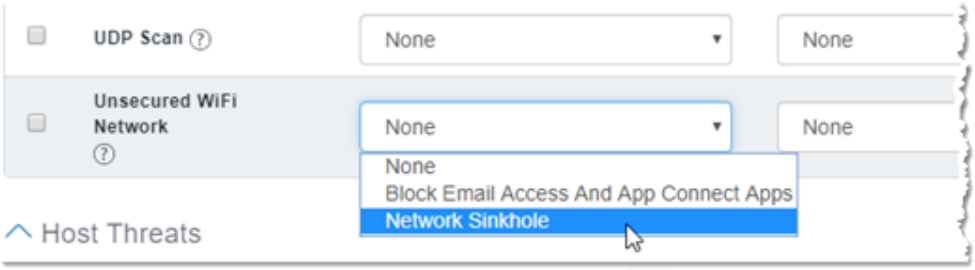
Before you begin

- Make sure you have reviewed Configuring MTD local actions for Cloud.

Procedure

1. From the MobileIron Cloud Configurations page, create or edit an MTD local action configuration.
2. From a threat in the Network Threats section, select **Network Sinkhole** from the Local Action iOS column.

FIGURE 19. NETWORK SINKHOLE OPTION IN ACTIONS MENU.



3. Finish your configuration choices, and click **Next**. The Configuration Distribution page displays.

   NOTE: The VPN configuration cannot be edited. To remove the configuration, remove the **Network Sinkhole** options from the configuration.
4. Click **Enable this configuration**.
5. Select the devices you want the configuration pushed to.
6. Click **Done** to push the configuration to the selected 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.

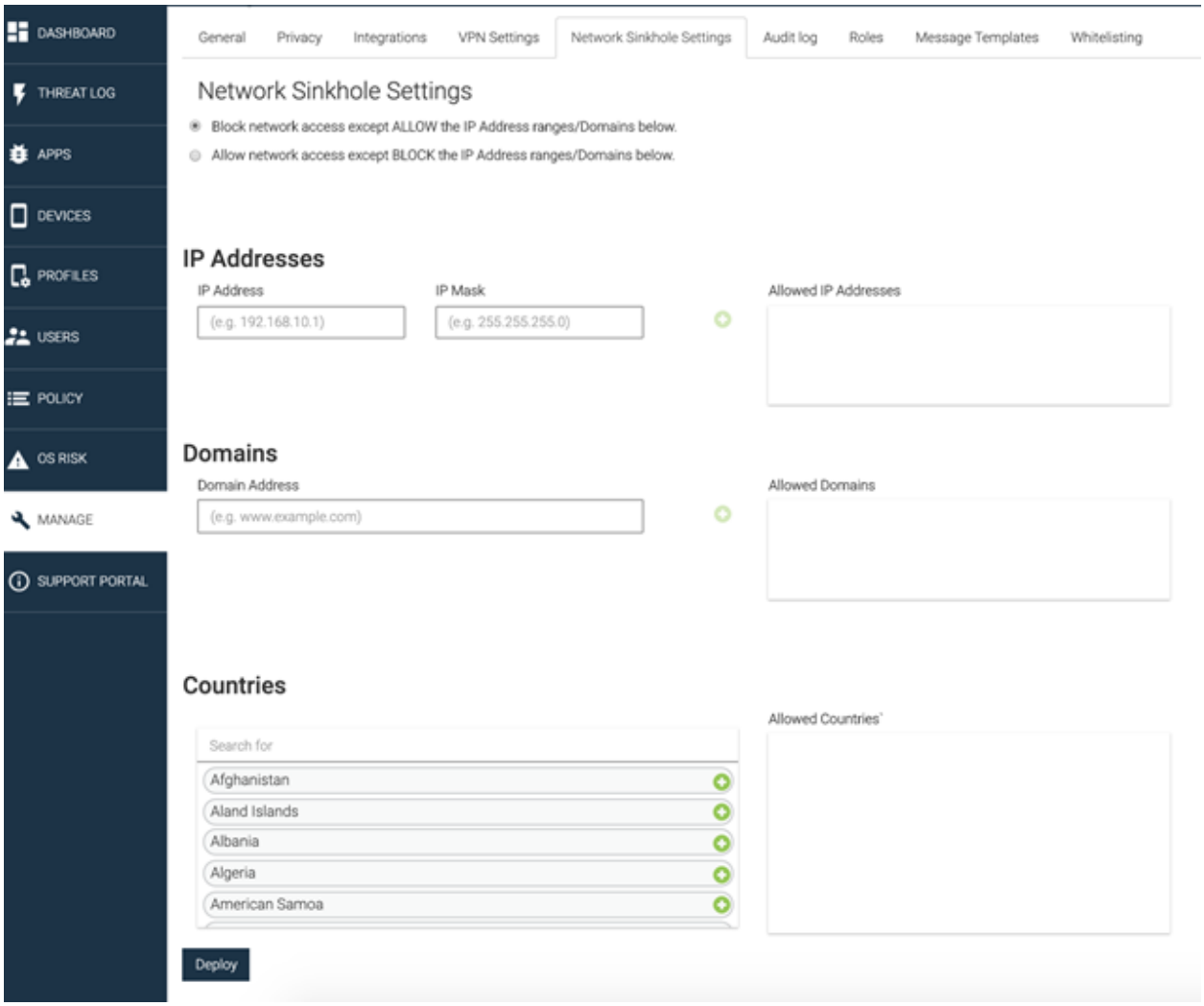
Before you begin

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.

FIGURE 20. NETWORK SINKHOLE SETTINGS IN THREAT MANAGEMENT CONSOLE



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.

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

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

Procedure

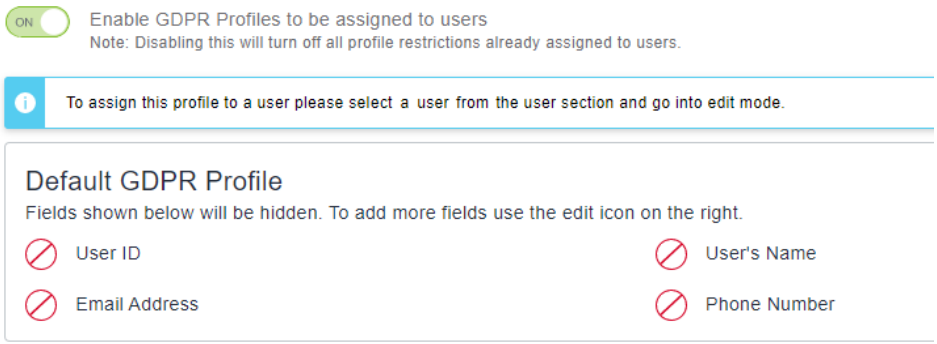
1. From MobileIron Cloud, navigate to **Admin > System > GDPR Profiles**. The GDPR Profile page displays.
2. Click **Enable GDPR Profiles to be assigned to users**. The Default GDPR Profile options display. By default, all of the fields are selected.
3. Click the blue pencil in the upper-right corner to edit the profile defaults.
4. 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
   - User's Name
   - Email Address
   - Phone Number
   - International Mobile Equipment Identity (IMEI)
   - Serial Number
   - Integrated Circuit Card ID (ICCID)

- International Mobile Subscriber Identity (IMSI)
- Mobile Equipment Identity (MEID)

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

5. Click **Save**.
   Your GDPR profile elections display, similar to this example.

FIGURE 21. GDPR PROFILE ELECTIONS

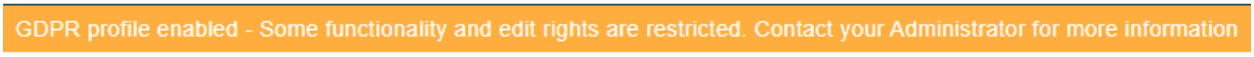


Assigning users to a GDPR profile

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 Cloud Devices and Users pages are restricted. GDPR-enabled users will see an orange banner across the top of MobileIron Cloud, reminding them that these restrictions are in place.

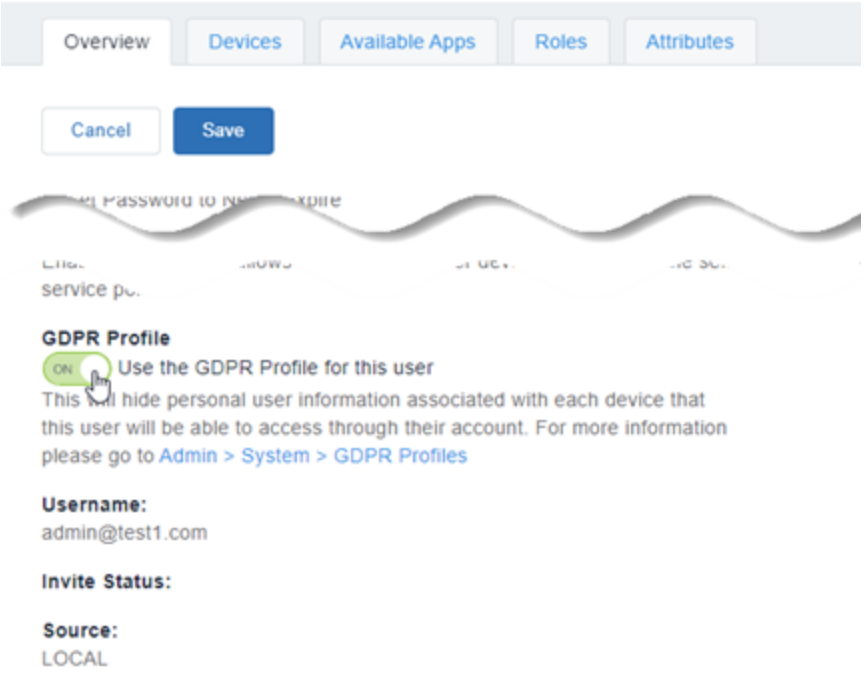
FIGURE 22. GDPR REMINDER BANNER



Procedure

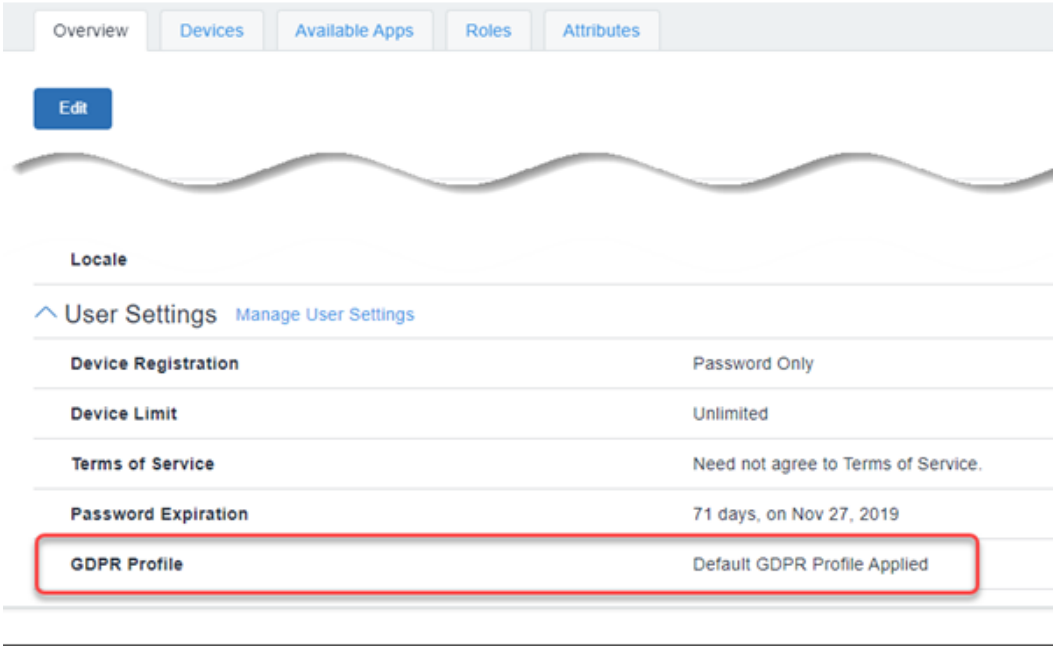
1. From the MobileIron Cloud portal, navigate to **Users > Users**. The Users page displays.
2. Select a user, click the three-dot menu for the row, then click **Details**. The User Information page displays.
3. Click **Edit**.
4. Scroll down to the **GDPR Profile** section. Click **Use the GDPR Profile for this user**.

FIGURE 23. USE THE GDPR PROFILE FOR THIS USER ENABLED



5. Click **Save**.
   GDPR Profile – Default GDPR Profile Applied now appears on the user's Edit User Details page, under **User Settings**.

FIGURE 24. CONFIRM THAT THE GDPR PROFILE HAS BEEN ENABLED



6. Once GDPR has been enabled for an admin or API user, they will not be able to see device and user information. The GDPR fields display as asterisks, or a blank field.

Administering MobileIron Go

This section includes information and tasks that MTD administrators may find helpful when troubleshooting MobileIron Go 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 MobileIron Go 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 MobileIron Go logs to MobileIron Support

Procedure

1. Open MobileIron Go.
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 MobileIron Go, 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:

If location services are not enabled in Android Enterprise mode, the threats **Unsecured Wi-Fi** and **Rogue Access Point** are not detected.

TABLE 15. EXPECTED BEHAVIOR FOR NEW AND UPGRADED ANDROID 10 INSTALLATIONS

Deployment mode	Expected behavior
All modes	The local action **Disconnect Wi-Fi** cannot be applied to Android 10 devices.
Android Enterprise (Profile Owner mode)	During installation or upgrade of the client on Android 10, the user is prompted to turn on location services for both device and profile settings: • If the user agrees, the app opens the device location service setting, so the user can enable it. To complete the process, the user must manually navigate to the Profile settings to enable location services for the Profile. • If the user does not enable the location services, **Unsecured Wi-Fi** and **Rogue Access Point** threats are not detected. 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.
Android Enterprise (DO and COPE modes)	For Android Enterprise Device Owner (DO) and Corporate Owned Personally Enabled (COPE) modes, Location settings are enabled without user action, allowing MTD detection of all network threats.
Device administrator (DA mode) **Mobile application management** (MAM mode)	**Unsecured Wi-Fi** and **Rogue Access Point** network threats cannot be detected for these devices.