MobileIron Core 10.6.0.0 Device Management Guide

for Android and Android enterprise Devices

March 4, 2020

For complete product documentation see:
MobileIron Core Product Documentation Home Page

Contents

Android Deployment Models

MobileIron Core supports these deployment models for Android devices that are registered to Core:

- Android enterprise devices
- Android devices using the device administrator
- Android MAM-only devices
- AppConnect for Android devices
- Samsung Knox Workspace devices

NOTE: Different devices can have each of these deployment models.

Android enterprise devices

Android enterprise is Google's program for supporting Android devices for enterprise. Android enterprise enables devices to have separate private and work profiles in BYOD deployments, and enables administrators to have broader control over enterprise owned and provisioned devices. MobileIron Core supports Android enterprise.

Related topics

- Setting up MobileIron Core for Android enterprise
- "Managing Mobile Apps for Android enterprise" in the *MobileIron Apps@Work Guide*

Android devices using the device administrator

In this deployment model, Mobile@Work has Android device administrator privileges. With these privileges, MobileIron Core is the Mobile Device Management (MDM) server for a registered device. As the MDM server, MobileIron Core, with help from Mobile@Work, can enforce many MDM features, such as device password requirements, device encryption requirements, lockdown requirements, Samsung-specific features, and more. MobileIron Core can also performs Mobile App Management (MAM) on the devices.

Android MAM-only devices

In this deployment model, MobileIron Core provides only Mobile App Management (MAM) features for a registered device. Core supports app installations using Apps@Work and most policies and configurations. However, because Mobile@Work does not have device administrator privileges, Core provides no MDM features to the device.

Related topics

"Managing apps on MAM-only devices" in the *MobileIron Apps@Work Guide*

AppConnect for Android devices

AppConnect for Android is MobileIron's solution that containerizes apps to protect data on registered Android devices. Each AppConnect-enabled app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable. Because each user has multiple business apps, each app container is also connected to other secure app containers, This connection allows the AppConnect-enabled apps to share data, like documents.

MobileIron Core supports AppConnect for Android only on:

- devices using the device administrator
- MAM-only devices

MobileIron Core does not support AppConnect for Android on:

- Android enterprise devices
- Samsung Knox devices

Related topics

MobileIron Core AppConnect and AppTunnel Guide

Samsung Knox Workspace devices

MobileIron Core supports Samsung Knox Workspace devices. Samsung Knox Workspace provides a secure container for corporate apps within a device.

Note The Following:

- You cannot deploy Samsung Knox Workspace and Android enterprise containers on a device at the same time.
- MobileIron Core does not support using both Samsung Knox Workspace and AppConnect apps on the same device.

Related topics

Samsung Knox Settings

Wear OS by Google

Mobile@Work for Android utilizes the Google Wear OS app as a companion app for Android phones and tablets. The Wear OS app works with Mobile@Work in Android enterprise deployments for Work managed device (DO) mode. The Wear OS app can be used by administrators to track the presence and inventory of apps on Wear OS devices in a corporate environment.

In Core, the Devices & Users page displays the information gathered from the watch, in addition to displaying all watches paired with the local device. If the connection to the Wear OS device is not established up to 1 week, Core will purge the data from the Device Details page > Wear OS tab. Mobile@Work will not display watches paired with remote devices.

NOTE: Mobile@Work for Android (phone) receives Wear OS data from the Wear OS device (watch) and the Android system tends to cache this data for an unknown time frame. There is a possibility that the true value of the "Wear OS Client Installed" field in Device Details > Wear OS tab is delayed for several hours.

Procedure

1. Create a Wear OS policy (see Working with Wear OS device policies.)
2. View the paired watch in the Device Details page > Wear OS tab. (see Viewing paired watch information .)
3. Search for watch information in Advanced searching.
4. Removing paired watch information.

Viewing paired watch information

Once you have a Wear OS policy in place, the Device Details page displays information about the Wear OS device that is connected to a mobile phone. This feature is applicable to Work managed device (DO) mode.

Procedure

1. Select **Devices & Users > Devices**.
2. Select the device. The device details display below.
3. Select the **Wear OS** tab. The Wear OS device details and application inventory display.

TABLE 1. WEAR OS TAB

Item	Description
Last Check-in Time	Lists the time stamp of the last time the Wear OS app checked in. The value field is updated when the device checks in.
Android Wear Make	Displays the make of the Wear OS device.
OS version	Displays the OS of the Wear OS device.

TABLE 1. WEAR OS TAB (CONT.)

Item	Description
Model	Displays the model of the Wear OS device.
Brand	Displays the brand of the Wear OS device.
Serial Number	The serial number of the watch. The value of this item is blank if the device user has not granted permission on the watch app.

Below the initial Wear OS information, a table displays the name of the app, its version number and the app's identifier.

Removing paired watch information

When the Mobile@Work client is erased (wiped) from the phone, the Wear OS data (including policies) stored in Core is purged after a specific time frame, only if the device is retired and the purge data setting is active. For example, if the device is retired and the "Delete Retired Device" field is set for 1 day, the data is purged from the Wear OS tab after 1 day the device is retired. Administrators can change the purge time frame (1-365 days) in Settings >Users & Devices > Delete Retired Devices.

Related topics

Working with Wear OS device policies

Setting up MobileIron Core for Android enterprise

MobileIron Core supports Android enterprise devices.

Android enterprise Overview

Android enterprise is Google's program for supporting Android devices for enterprise. Android enterprise enables devices to have separate private and work profiles in BYOD deployments, and enables administrators to have broader control over enterprise owned and provisioned devices. MobileIron Core supports Android enterprise. This supports requires you to perform setup tasks with Google, MobileIron (help.mobileiron.com), and the MobileIron Core Admin Portal.

Modes for Android enterprise devices

Android enterprise devices that are registered with MobileIron Core are in one of the following Android enterprise modes:

- **Work Profile mode:** An Android enterprise device is in Work Profile mode when it has a *work profile*. The device is typically privately owned (BYOD). Corporate data and apps are secured in the *work profile*, while the user's private data and apps are in the separate *personal profile*. MobileIron Core has administrative control over the work profile. For more information see https://developers.google.com/android/work/requirements/work-profile.
- **Work Managed Device mode:** An Android enterprise device that is in Work Managed Device mode is typically corporate-owned. The device has a single profile with corporate data and apps. This mode is only available on factory installed devices. If a device with this mode on it is wiped it will no longer be in Work Managed Device mode. MobileIron Core has administrative control over the device, with more lockdown features available than for device using a work profile. For more information see: https://developers.google.com/android/work/requirements/work-managed-device.
- **Managed Device with Work Profile mode:** An Android enterprise device in this mode is an enterprise-owned device with personal data separate from the rest of the phone. It has a small client installed on it to

separate personal data from the rest of the phone. This mode is only available on factory installed or factory reset devices. If a device in this mode is wiped it will no longer be in Work Managed Device mode. This mode requires:

- Mobile@Work 9.7 for Android through the most recently released version as supported by MobileIron.
- Android 8.0 through the most recently released version as supported by MobileIron.
- A managed Google Play account
- If the account is enrolled with Google Domain, the device will be registered in the Work Managed Device mode.

NOTE: In Android developer documentation, "work profile" is referred to as "profile owner" and "work managed device" is referred to as "device owner".

Requirements for using Android enterprise

To enable Android enterprise for your enterprise and use it with MobileIron Core, you need:

- A Google account that is not tied to Managed Google Accounts. That is, any Google account that is not managed by an enterprise can be used for enrolling with Android enterprise.
  - access to Google Play on Android devices and Core
  - access to these URLs through outbound HTTP proxy:
  - https://accounts.google.com/o/oauth2/token
  - https://www.googleapis.com

  See Outbound HTTP Proxy Set Up in the On-Premise Installation Guide.

Requirements for using an Android enterprise device in work profile mode

To enable an Android enterprise device in work profile mode, the following is required:

- an Android enterprise-capable device, running Android 5.0 through the most recently released version as supported by MobileIron, with the Mobile@Work for Android app installed

  NOTE: The Mobile@Work app on Android devices shows whether the device is Android enterprise-capable in the Settings > About > Product Details tab. Google provides a list of Android enterprise-capable devices here: https://enterprise.google.com/android/.
- if using managed Google Play Accounts, MobileIron Core automatically generates a Google User based on the UUID of the user.
- an Android enterprise setting on MobileIron Core (**Policies & Configs > Configurations**) applied by label to the device

Requirements for using an Android enterprise device in work managed mode

To enable an Android enterprise device in work managed mode, all the Requirements for using an Android enterprise device in work profile mode are necessary. In addition, for work managed mode devices, you must enroll

devices with either NFC, QR code, “afw#” tokens, or Google’s Zero-Touch. For more information, see Provisioning an Android enterprise device.

Requirements for using an Android enterprise device in Managed Device with Work Profile mode

To enable an Android enterprise device in Managed Device with Work Profile mode, all the Requirements for using an Android enterprise device in work profile mode and Requirements for using an Android enterprise device in work managed mode are necessary. In addition, for devices in this mode, you must select **Enable Managed Device with Work Profile on the devices** on the Android enterprise setting.

Enabling Android enterprise

To enable MobileIron Core to provide Android enterprise features, you must perform setup steps with Google, MobileIron Support, and MobileIron Core. You will associate a managed Google Play Account with MobileIron Core. Note that this procedure does not share your enterprise’s user names or email addresses with Google.

Depending on if you are a new or upgrading customer, the app distribution settings are different. If you are a new customer, the app distribution is set to per device by default. You cannot change this setting. For upgrading customers, you have a choice between apps distribution per user or per device. Also for upgrading customers, app distribution per user is selected by default. Many users have multiple devices. If a user has multiple devices, when app distribution is set per device then you can make a different set of apps available on each device.

Procedure

1. Log into help.mobileiron.com**.**
2. Click **Android enterprise Enrollments.**
3. Click **Create New Android enterprise Enrollment**.
   The screen **Android enterprise Setup - Step 1** displays.
4. Click **Begin**.
   Do not click **Alternate Setup Method**. If you used the alternate setup method in the past, see Using the alternative method to set up Android enterprise.
   After clicking **Begin**, the screen **Android enterprise Setup - Step 2** displays.
5. Use the radio buttons to select a brand that matches the Core you are using.
6. Click **Submit**.
7. The Bring Android to Work page displays. Click **Sign In**.
8. Sign in with a Google account.
9. Click **Get Started**.
10. Enter your Organization details: name and agree to the **managed Google Play agreement.**
11. Click **CONFIRM**.

12. Click **COMPLETE REGISTRATION**.
13. The **Android enterprise Enrollment** page displayed in help.mobileiron.com.
    Click **Download Google JSON Enrollment file.**
    The downloadService JSON file is downloaded.
    Store it in an accessible file location for later use, such as if you need to enable Android enterprise on another MobileIron Core.
14. Log into the MobileIron Core Admin Portal and go to **Services > Google**.
15. Upload the JSON file. Use the browse button to navigate to the JSON file you downloaded earlier in this procedure and click **Connect**.
    The Google Play App Catalog dialog box opens with this warning message: If more than one Core instance is publishing the Google Play layout, you will be sending redundant (possibly conflicting) layouts to Google. This does NOT affect the distribution of apps, only the layout visible in Google Play. To use a Custom Layout in the Google Play store see "Distributing your enterprise apps in the Google Play App catalog or in Apps@Work" in the *MobileIron Apps@Work Guide.* This step is optional.
16. Go to **Policies & Configs > Configurations > Add New > Android > Android enterprise** to go to the New Android enterprise setting dialog box.
17. Enter a Name and Description.
18. To make devices that this setting applies to be in Managed Device with Work Profile mode, select **Enable Managed Device with Work Profile on the devices**.
19. Ignore **Auto update Mobile@Work app on the devices**. This option is no longer applicable. Using Google Play on the device, a user can specify that apps should be updated automatically. Click **Save**.
20. Apply the Android enterprise setting to a label that is also applied to Android enterprise-capable devices. For example, apply this setting to the built-in **Android** Label, or a custom label that is defined using the filter "android.afw_capable = true". For more details about labels, refer to the *Getting Started with MobileIron Core.*

For information on the other fields on the Android enterprise setting, see:

- Enabling run-time permissions for Android enterprise apps
- Adding a Google account to an Android enterprise managed device
- Enabling an Android enterprise VPN client to be always on
- For more information, see VPN clients deployed either inside or outside Knox Workspace on page 234.
- Refer to the *MobileIron Apps@Work Guide.*

Related topics

- Impact of removing the Android enterprise setting from a device
- Removing Android enterprise

Impact of Android enterprise setting to devices that are not Android enterprise-capable

There is no impact to devices that are not Android enterprise-capable to have the Android enterprise setting applied. Some devices might become Android enterprise-capable in the future, if the carrier upgrades the device's firmware.

To view the status of the Android enterprise setting for a device:

- Go to **Devices & Users > Devices**.
- Open the device details for the device.
- Click the **Configurations** tab.
- Look for the Android enterprise setting. The **Status** column displays:
  - **Pending**: The device has not yet confirmed that it has received the setting.
  - **Applied**: The setting is applied.
  - **Sent**: The device is not Android enterprise-capable; the setting is ignored by Mobile@Work.

Determining if a device is Android enterprise-capable

You can check if a device is Android enterprise capable by doing the following:

- On the device, open Mobile@Work. Tap the menu, and tap **Settings > About > Product Details**. Look for Android Enterprise (AFW) Support and see if its value is **Yes**.
- Once the device is registered, on MobileIron Core go to **Devices & Users > Devices** page. Find the device and click the caret next to the display name to view the **Device Details.** Look for the "Android enterprise Capable" row. The value is true if the device is capable.

Enabling run-time permissions for Android enterprise apps

You can specify whether run-time permissions are automatically accepted or denied for Android enterprise apps, or whether the device user is prompted to accept run-time permissions when each app requests them. You make this choice in the Android enterprise setting. The choice you make applies to all Android enterprise apps on devices that receive the Android enterprise setting, based on the labels on the devices and the setting.

However, you can also specify run-time permissions for each permission for each app in the app's settings in the MobileIron Core App Catalog. The run-time permissions setting for the app in the App Catalog overrides the run-time permissions setting in the Android enterprise setting.

NOTE: The run-time permission settings are supported only on Android 6.0 through the most recently released version as supported by MobileIron.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations.**
2. Select an Android enterprise setting.

3. Click **Edit**.
4. Select **Enable Runtime Permissions.**
   The choices for run-time permissions display.
5. Select a run-time permission setting.
   - **User Prompt**: The device user is prompted to accept or deny each run-time permission that each app requests when it launches. This behavior also applies if you do not select **Enable Runtime Permissions.**
   - **Always Accept**: The run-time permissions are automatically accepted for each app when it launches. The device user is not prompted.
   - **Always Deny**: The run-time permissions are automatically denied for each app when it launches. The device user is not prompted.
6. Click **Save**.

Related topics

"Features specific to Android enterprise devices" in the *MobileIron Apps@Work Guide*.

Adding a Google account to an Android enterprise managed device

As an administrator, you can add an additional Google account to an Android enterprise managed device. This action enables you to control which Google account can be added to the Android enterprise account. This account can only be administered or modified by you, the device administrator. The device user cannot modify or remove the added account or add another account to the managed profile.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations.**
2. Select an Android enterprise setting.
3. Click **Edit**.
4. Select **Add Google Account** check box in the **For Android 6.0 and higher only** section.
   A Google Account field displays.
5. Enter the name of a Google Account you want to add.
   The added account must be an account with a Google domain. The name can include any of the following Core substitution variables listed in the information popup next to the field. For example, you can enter:
   - $USER_CUSTOM1$
   - $LAST_NAME$.$FIRST_NAME$@mycompany.com
   - $DISPLAY_NAME$@mycompany.com
6. Go to **Policies & Configs > Policies** and select the lockdown policy for this device.
7. Uncheck the **Allow the user to create and modify accounts** option if it is checked.

Searching for devices that are registered as Android enterprise devices

The Device Details pane for a device indicates the registration status of Android enterprise devices. These values are:

- **Work Profile**
- **Work Managed Device**
- **Managed Device with Work Profile**

You can use advanced search to find devices with the registration statuses of interest to you, and create dynamic labels for those sets of devices, if desired.

Related topics

Searching for Devices

Enabling an Android enterprise VPN client to be always on

You can specify an Android enterprise VPN client as an Always-On client.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select an Android enterprise setting.
3. Click **Edit**.
4. Select the **Always-On VPN** check box to display the **App Identifier** drop-down menu.
   The drop-down menu lists only apps that are configured to be installed as Android enterprise apps.
5. Select a VPN app to apply the Always-On setting.
6. Click **Save**.

Note The Following:

The Android enterprise setting displays in Device Details as Partially Applied with an error message in the following cases:

- The selected app is not installed on the device.
- The selected app is installed on the device, but it is not a VPN app, or it is a VPN app that does not support Always-On.

For Samsung Knox VPN settings, see KNOX VPN Support on page 233.

Moving in-house apps to a Knox v3 Workspace

You can move your in-house apps to a Knox v3 Workspace.

Procedure

1. Go to **Policies & Configs** > **Configurations**.
2. Select **Add New** > **Android** > **Android enterprise**. The New Android enterprise (all modes) Setting dialog box is displayed.

3. Select the check box next to the **Move In-house app into workspace** field. Then the **Package Names** field is displayed.
4. Use the drop-down menu next to the **Package Names** field to select an app name.
5. Click **Save**.

For more information, see VPN clients deployed either inside or outside Knox Workspace on page 234.

Requiring a password for accessing the work profile

Typically, a password for an enterprise work profile should not be the same as the device password; however, some devices allow the two passwords to be the same.

Within the Work Challenge section, having the “Block unified password” option selected will force the device user to enter a password twice – first to unlock the device, second to unlock the work profile. (Using the "Block unified password" field helps disable the use one lock option on the device to force device users to specify a security challenge for apps running in the work profile.) This feature is supported on devices using Android 7 through the most recently released version as supported by MobileIron.

- For devices using Mobile@Work 10.1.0.0 for Android and Android 9.0 through the most recently released versions as supported by MobileIron, select **Block unified password (device and work profiles)** in the Android enterprise setting. This option appears when you select the **Work Challenge** option.
- For other devices, distribute an Android enterprise setting with a work challenge configuration that has stricter requirements than the device passcode settings on the security policy for the devices. For example, stricter requirements include increasing the minimum password length in the **Minimum Password Length** field or increasing the number of complex characters in the **Minimum Number of Complex Characters** field.

  For more information, see step 15 in the procedure below.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations.**
2. Select an Android enterprise setting.
3. Click **Edit**.
4. In the For Android 7.0 and higher only section, select the **Work Challenge** check box. When a work challenge is set, the administrator can block device passcode matching the work profile. This is to enforce separate work and device passwords so that device users do not unlock the work profile at the same time as unlocking the device.

   The Password fields display for configuring your work challenge requirements.
5. Select the Password Type:
   - **Simple PIN:** Includes repeated characters, or ascending/descending characters, for example, 123 or CBA.
   - **Complex PIN**: Select **On** to include numbers that are not repeated and should not be in a sequence, for example, 1234, 2468, 9876. An example of repeating digits is 4444.

- **Alphanumeric**: At least one letter and one number is required.

6. Set **Minimum Password Length** to the minimum password length ranging from 1 to 16 numbers or characters.
7. Set **Maximum Inactivity Timeout** to the maximum time allowed for the device to be inactive before the user must reenter the work challenge to access the work profile. This may be set to **Never** to prevent timeout.
8. Use **Minimum Number of Complex Characters** to set the minimum number of complex characters required in the password. Complex characters are special characters that are not numbers or letters, such as !, *, and #.
9. Set the **Maximum Password Age** to the number of days until the user must change the work challenge.
10. Set **Maximum Number of Failed Attempts** to the maximum number of attempts to enter the correct password in one login. The default value for failed attempts is 10. When the maximum number of attempts is reached, the work profile is retired.
11. Set **Password History** to how many old work challenge passwords are stored so that the device user cannot repeat them.
12. Select **Block Fingerprint** to prevent a device user from using a fingerprint to replace the work challenge password.

    NOTE: Both the **Block Iris Scan** and **Block Face unlock** fields require either a Samsung device running Samsung OS 7.0 through the most recently released version as supported by MobileIron or a non-Samsung device running Android 9.0 through the most recently released version as supported by MobileIron.

13. Select **Block Iris Scan (Android 9 or Samsung only)** to prevent a device user from using an iris scan to replace the work challenge password.
14. Select **Block Face unlock (Android 9 or Samsung only)** to prevent a device user from using a face scan to replace the work challenge password.
15. Select **Block unified password (device and work profiles)** - by selecting this option, the administrator forces the device user to set a secondary password for the work profile. The system shows the security challenge when the user attempts to open any work apps. This feature is supported on devices using Android 7 through the most recently released version as supported by MobileIron. If this field is de-selected (default), then the device user can use the same password for unlocking the device and the work profile.

Impact of removing the Android enterprise setting from a device

Removing the Android enterprise setting from a device causes the device to become retired.

The Android enterprise setting can be inadvertently removed from a device if:

- the setting is applied to a dynamic label instead of a built-in label, and
- the device is dynamically removed from the label for any reason, or
- the Android enterprise setting is manually removed from a label shared with a device.

Removing the setting from the device causes the following to happen:

TABLE 2. REMOVING ANDROID ENTERPRISE SETTING

Android enterprise status	If Android enterprise setting is removed:
work profile	• Core shows the device as registered, but the device no longer has the Mobile@Work app nor work profile and cannot communicate with Core. (This is similar to the state that occurs if a user manually removes Mobile@Work from a device.) • User can re-register the device. The user must re-enable Mobile@Work through the Google Play store.
device owner mode	• The device becomes unregistered and performs a factory reset. • The device can be re-registered at a later time.

Related topics

Removing an Android enterprise configuration causes device to retire

Configuring the security policy for Android enterprise devices

Most security policy settings for Android enterprise devices are the same as the settings for other Android devices. However, note that a few settings in the security policy are specific to Android enterprise devices. These settings are:

- **Block notifications on lock screen** (Android enterprise work managed devices only)
- **Allow only redacted notifications on lock screen** (for Android enterprise work profile devices only)
- **Bypass Factory Reset Protection** (Android enterprise work managed devices only)

Also in the security policy, you specify compliance actions for various security violations. When a compliance action includes quarantine, on Android enterprise devices, all Android enterprise apps and functionality are hidden except for Downloads, Google Play Store, and the Mobile@Work app.

When configuring Zebra OTA (Over-the-Air) service, only for Work managed Zebra devices is supported.

Related topics

- "Security policies" in *Getting Started with MobileIron Core*
- "Add Compliance Action table" in *MobileIron Core Device Management Guide for Android and Android enterprise Devices*

Configuring the lockdown policy for Android enterprise devices

You can configure the lockdown policy to apply lockdown settings to Android enterprise devices. Whether a lockdown policy field applies to an Android enterprise device depends on the Android enterprise mode that the

device is registered in. The modes -- Work Profile Mode, Work Managed Device Mode, and Managed Device with Work Profile Mode -- are described in the Android enterprise Overview .

NOTE: For Android enterprise Work Profile and Work Managed Device modes, only the camera and phone are included in the package identifier. Enable all system apps by logging into the Admin Portal and going to **Policies & Configs > Policies > Add New > Lockdown**.

Related topics

"Lockdown policies" in *Getting Started with MobileIron Core*

Removing Android enterprise

This section addresses the removal of Android enterprise-related items.

Removing an Android enterprise configuration causes device to retire

When you enroll an Android device on a dynamic label using Android for Work with Work profile mode, Work managed device mode, and Managed device with Work profile (COMP) mode and later modify the label criteria to exclude the device, the following occurs:

- the device's client configuration is removed
- the device becomes retired and displays in the Retired Device's Dashboard.

This is applicable to Android Enterprise devices in all modes:

- Device Owner mode - in this mode, a retire causes a factory reset
- Profile Owner mode
- Managed device with Work profile mode (COPE)
- Device Owner with Work Profile mode

Removing the Android enterprise account in Core

You can remove the Android enterprise account from MobileIron Core, severing Core's connection with Google. This removal causes devices to retire when they check in.

Procedure

1. In the MobileIron Core Admin Portal, go to **Services > Google.**
2. Under **Android enterprise** click **Remove** to open the **Remove Account** dialog.
3. If you wish to remove the Android enterprise account with Core, click the check box for "I understand" and then click **Remove**.

MobileIron Core will retire Android enterprise devices when they next check in.

Removing your managed Google Play account

You can remove your managed Google Play account if you no longer need it.

Procedure

1. Login to help.mobileiron.com.
2. Select Android enterprise Enrollments.
3. Click on your managed Google Play Account.
4. The **Android enterprise Enrollment Detail** screen displays.
5. Click **Delete**.

Registering Devices

A device is available for management by MobileIron Core after it has been registered by a device user or administrator.

The topics in this section include the following advanced topics:

- Registration methods
- Terms of service
- Visual privacy
- Invite users to register
- In-app registration for iOS and Android
- Registering Android devices
- Web-based registration for Android devices
- ActiveSync device registration
- Managing the Android enterprise device life cycle
- Provisioning an Android enterprise device
- Managing operators and countries
- Specifying eligible platforms for registration
- Setting the registration PIN code length for device user registration
- Customizing registration messages
- Configuring the default ownership for newly registered devices
- Disabling analytics data collection

Refer to the *Getting Started with MobileIron Core* for the most commonly used registration topics, such as:

- Single device registration
- Bulk device registration
- Tracking registration status
- Restricting the number of devices a user registers
- Registration considerations

Registration methods

Registering a device designates it for management by MobileIron Core.

Before you begin

Setting the registration PIN code length for device user registration

The following registration methods are available:

- Admin invites users to register
- In-app registration for iOS and Android
- Registering Android devices
- Registration methods
- Users register additional devices
- Admin registers ActiveSync devices
- Registration methods
- Registering Android devices via web portal (MIRP)
- Registering Samsung devices using Samsung Knox Mobile Enrollment

You can also register Android devices using the MobileIron Provisioning app. See Provisioning an Android enterprise device

The process resulting from these methods may vary by device OS.

Admin invites users to register

For users who are mobility savvy and do not require significant assistance, you can send an invitation and enable them to register their own phones. You can send an invitation to multiple users from the Users Management screen. The invitation includes instructions on how to log into the user portal to register phones.

The user needs to know the following information for the device:

- phone number (if any)
- country
- platform

Related topics

Invite users to register

In-app registration for iOS and Android

One way to reduce the load on IT personnel is to instruct iOS and Android users to download the MobileIron app directly from the App Store on iTunes or from Google Play and initiate registration from within the Mobile@Work app.

For iOS devices

1. Go to **Settings > System Settings > iOS > MDM** and select the Send email to user and notification to client if MDM profile is not installed check box.
2. Device users of iOS 12.2 and later will need to download Mobile@Work, manually navigate to Settings view and download the MDM profile.
3. Device users then complete the registration process by responding to registration prompts. If Core detects that the MDM profile has not yet been installed, upon the next device check-in, Mobile@Work will display a notification asking the device user to re-enroll.

NOTE: In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Mobile@Work app is running. Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". MobileIron recommends device users to enable tracking. This change applies to all versions of iOS 13 through the latest version as supported by MobileIron. Mobile@Work for iOS does not track device users' location without consent.

Administrator tasks

- This feature depends on access to the MobileIron Gateway; therefore, the corresponding port must be properly configured. See the Pre-Deployment Checklist in the *On-Premise Installation Guide* for details. The User Portal role must be assigned to the user.
- To auto-populate the MobileIron Core server name during registration, the following setup is required:
  - The user associated with the device must be known as an LDAP user or defined as a local user.
  - To auto-populate based on the device phone number, see Auto-populating the MobileIron Core server name based on email address on page 56 for details.
  - To auto-populate based on the email address, you must register your VSP with MobileIron.
- Schedule email reminders, see Customizing registration messages on page 73

Registering Android devices

As with other types of devices, you can configure whether you want Android device users to enter a password, PIN, or both during registration. This can be done with managed and un-managed Android devices.

NOTE: If upgrading to Core 10.6.0.0, and you have your Device Registration set to a specific authentication setting (Password, Registration PIN or Password and Registration PIN), the setting will be retained as a default. If you are registering devices for the first time using Core 10.6.0.0 or later as supported by MobileIron, the default setting is Password.

Before you begin

Setting the registration PIN code length for device user registration

Procedure

1. Upload the APK file for Mobile@Work for Android to a secure server. This server must be accessible to device users.
2. For unmanaged Android devices:
   a. Go to **Settings > System Settings > Users & Devices > Device Registration**.
   b. In the In-App Registration Requirement field, select one of the following:
      - **Password** - device user will be required to enter username and password.
      - **Registration PIN** - device user will be required to enter a registration PIN.
      - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.
   c. Click **Save**.
3. For Zero Touch and Samsung Knox Android managed devices:
   a. Go to **Settings > System Settings > Users & Devices > Device Registration**.
   b. In the Zero Touch and Samsung Knox Mobile Enrollment field, select one of the following:
      - **Password** - device user will be required to enter username and password.
      - **Registration PIN**- device user will be required to enter a registration PIN.
      - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.
   c. Click **Save**.

   For more information, see Provisioning Android enterprise devices using Zero Touch and Registering Samsung devices using Samsung Knox Mobile Enrollment
4. For all other managed Android device types, in the Managed Devices/Device Owner (afw#, QR code, NFC) field, select one of the following:
   - **Password** - device user will be required to enter username and password.
   - **Registration PIN** - device user will be required to enter a registration PIN.
   - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.

   Click **Save**.

   For more information on registering using afw# token, QR code or NFC bump, see Provisioning an Android enterprise device.
5. In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
6. Click **Register**.

   The Registration Instructions dialog box opens.
7. Copy the Registration PIN for sending to the device user. If you are intending to send an email invitation to device users, you can skip this step.
8. Set up the email invitation template. See Customizing registration messages

9. Send the email invitation to device users. Core will automatically add the Registration PIN within the invitation.
10. Once the device user has registered, monitor devices for status in **Devices & Users > Devices**. The Android Automated Enrollment field lists the values as appropriate for the type of Android setup:
    - Google Zero Touch
    - Knox Mobile Enrollment
    - Non Zero Touch AE Enrollment

    NOTE: The Android Automated Enrollment field is valid for Core 10.6.0.0 through the latest version as supported by MobileIron. If an "Unknown" value displays, it indicates a previous version of Core was used and the "In-App Registration Requirement" field in **Settings > System Settings > Users & Devices > Device Registration** was used. It can also mean that an old client was used with Core version 10.6.0.0 or later.

Users register additional devices

Once a device has been registered, an authorized user can use the user portal to register additional devices without administrative help. This is often used with adding devices for users who do not require assistance.

Prerequisites

- Users must have the **User Portal** role assigned, with the **Device Registration** option enabled.
- The user needs to know the following information for the device:
  - phone number (if any)
  - country
  - platform

Related topics

Self-service User Portal

Admin registers ActiveSync devices

If you have a MobileIron Sentry configured, then you can see the devices that are connecting to your ActiveSync server. To incorporate these devices into your MobileIron Core inventory, you can use the Register button in the ActiveSync Associations screen. This is often used with devices accessing email via ActiveSync.

Prerequisites

- MobileIron Sentry must be installed and configured.
- The user (local or LDAP) associated with the device must be available for selection at the time of registration.
- For iOS, Android, and Windows devices, the User Portal role must be assigned to the user.

- You need to know the following information for the device:
  - phone number (if any)
  - country code
  - platform

Related topics

ActiveSync device registration

Registration via user portal

The user portal can be used to streamline the registration process. See Self-service User Portal on page 437 for more information.

Registering Android devices via web portal (MIRP)

Administrators who use web portals (such as the BYOD Portal) to initiate registrations can provide a URL in the web portal to help device users register Android devices with little or no typing. Users just download Mobile@Work from Google Play and then tap the URL in the web portal from the device. Tapping the URL launches the Mobile@Work app and populates the registration screen with the available information, such as the username. The information that is available depends on the web portal being used.

The URL is based on the MobileIron Registration Protocol (MIRP). The link you provide on the web portal must have the following format:

mirp://<Core URL><parameters>

The following parameters are available:

- user: The username for the device user.
- pin: The PIN generated for this user for PIN-based registration.

Examples:

- mirp://mycore.mycompany.com&user=android&pin=1234
  If you have configured MobileIron Core for PIN-only registration, device users will be automatically registered without having to enter any credentials.
- mirp://mycore.mycompany.com&user=android
  Device users will be prompted to enter credentials to complete registration. The credentials include either a PIN or password, depending on how you configured Core.

Note The Following:

- The ampersand character is reserved. If you require an ampersand in a field value, it must be URL-escaped to a character code (i.e.,%26).
- Unsupported parameters will be ignored.

Registering Samsung devices using Samsung Knox Mobile Enrollment

MobileIron Core supports using the Samsung Knox Mobile Enrollment process to register qualified Samsung devices with MobileIron Core.

Using Samsung's Knox Mobile Enrollment process, once the process is set up, qualified devices are automatically enrolled and registered to MobileIron Core when the end user activates the device for the first time.

Requirements

- A CSV file that provides a list of device IMEI numbers or serial numbers, and optionally:
  - a username
  - a registration PIN and/or password
    If you configured registration to use a PIN, include a PIN in the registration file. If you configured registration to use a password, include a password. If you configured registration to use both a password and a PIN, include only one of them in the CSV file. You configure the registration requirements on the Admin Portal at:
    Settings > System Settings > User & Devices > Device Registration > Zero Touch and Samsung Knox Mobile Enrollment.

  NOTE: If username or PIN or password is not in the CSV file, the user must provide them.

- A Samsung Knox account and use of the Samsung Knox Mobile Enrollment portal
- Samsung Knox devices (see Samsung portal for a list of qualified devices)

NOTE: Mobile@Work for Android is automatically installed during the enrollment process.

Benefits

- Bulk enrollment of devices: No user interaction is required to download the Mobile@Work app. The app is installed automatically as part of the enrollment process. No access to Google Play is required.
- No need for users to enter credentials (unless desired); credentials are populated in the background.
- Auto-Enrollment: Once a device is enrolled into an UEM/MDM via Samsung's mobile enrollment process, the MDM software is always be imposed even if the device is erased, inadvertently or maliciously, until you remove the device from the Samsung Knox Mobile Enrollment portal or retire
- Choice of enrollment options: you can choose to enroll the device using NFC bump, a URL, or automatic activation when a device is first powered on.
- Multiple Core (or MobileIron Cloud) servers can participate in the program.

Instructions

Complete instructions for setting up and using the Samsung Knox Mobile Enrollment portal with MobileIron Core are available in the MobileIron knowledge base article, here:

Samsung Knox Mobile Enrollment with MobileIron Quick Start Guide

Related topics

You can also register Android devices using the MobileIron Provisioning app. See Provisioning an Android enterprise device

Terms of service

You can optionally define terms of service text to be displayed to users during:

- device registration on iOS, macOS, Android, and Windows devices
- logging into AppConnect apps on iOS and Android devices

Device users must accept the terms of service before they can continue with registration or with accessing AppConnect apps.

You can search for users by terms of service acceptance and date of acceptance. You can create one terms of service agreement for each supported language. The same terms of service text is used for both registration and AppConnect app access.

Regarding terms of service during registration:

- Presenting the terms of service is part of the registration process when using Mobile@Work. Users must accept the terms of service agreement in order to complete registration.
- Configuring a terms of service agreement or updating it applies only to users who register after you complete the configuration. Previously registered users do not accept the terms of service agreement. However, you can require existing users to accept the terms of service agreement by retiring their devices and requesting them to re-register.
- If both custom terms of service and the privacy policy are enabled, users will have to accept the privacy policy first.

Regarding terms of service for accessing AppConnect apps:

- In addition to providing the terms of service text, you must enable terms of service on the AppConnect global policy.
- Also on the AppConnect global policy, you indicate whether:
  - users must accept the terms of service each time they are prompted for their AppConnect passcode or biometric authentication. If you update the terms of service text for a user's language, the user sees the updated text on all subsequent AppConnect logins.

  - the user must accept the terms of service only once. However, if you update the terms of service text for a user's language, on the next AppConnect login, the user is prompted once more to accept the terms of service.
- If you delete the terms of service, but do not disable it on the AppConnect global policy, users continue to be prompted to accept the terms of service with whatever the last terms of service text was.
- For information about enabling terms of service when logging into AppConnect apps, see "Configuring the AppConnect global policy" in the *MobileIron Core AppConnect and AppTunnel Guide*.

Creating a terms of service agreement

Before you begin

Set up the system default language as described in Setting the system default language .

If there is no terms of service available in the primary language of a given device, or if more than one agreement is defined for more than one device language on a device, the terms of service agreement defaults to the system default language.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Scroll down to the **End User Terms of Service** section.
3. Click **Add+**.
4. Select the language for the terms of service.
5. For **Type**, select **System** for iOS, macOS and Android devices. Select **AAD enrollment** for Windows devices.
6. Enter the text for the terms of service.

   You can adjust the editor to use rich or plain text by clicking the Source Edit icon.
7. Click **Save**.
8. Optionally, repeat steps 3 through 6 to add a terms of service agreement for each supported language, and for Windows devices versus iOS, macOS, and Android devices.

Note The Following:

- To edit a terms of service agreement, click the **Edit** link next to the relevant language.
- To delete a terms of service agreement, click the **Delete** button next to the relevant language.

Searching for devices by terms of service agreement criteria

You can search for devices based on whether users have agreed to the terms of service, and the date on which terms of service were accepted.

The following table describes the searchable criteria related to terms of service. Corresponding fields are displayed on each device's Device Details tab.

TABLE 3. SEARCHABLE CRITERIA FOR TERMS OF SERVICE

Criterion	Description
Terms of Service Accepted	A false value means the user did not accept the terms of service at registration, which means the device was registered before a terms of service agreement was required, or a terms of service agreement was never configured. A true value indicates the device user accepted the terms of service agreement at registration.
Terms of Service Accepted Date	Filters for the exact time users accepted the terms of service agreement at registration. This search is useful if you want to locate the version of the terms of service agreement accepted by a specific user for a particular device.
AppConnect Terms of Service	The value **DECLINED** means the user did not accept the terms of service for using AppConnect, which means the device user logged into AppConnect before a terms of service agreement was required, or a terms of service agreement was never configured. The value **ACCEPTED** indicates the device user accepted the terms of service agreement when logging into AppConnect.
AppConnect Terms of Service Date	Filters for the exact time users accepted the terms of service agreement when logging into AppConnect. This search is useful if you want to locate the version of the terms of service agreement accepted by a specific user for a particular device.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Click **Advanced Search**.
3. Add one or more of the search rules regarding terms of service.
   a. From the **Field** drop-down list, select the field of interest:
      - **Common Fields > Terms of Service Accepted**.
      - **Common Fields > Terms of Service Accepted Date**.
      - **Common Fields > AppConnect Terms of Service**.
      - **Common Fields > AppConnect Terms of Service Date**.
   b. Provide the appropriate value:
      - **Terms of Service Accepted**: Select **true** or **false** in the **Select Value** field.
      - **Terms of Service Accepted Date**: Enter the number of units in the **Value** field and select the units (such as days, weeks, or months) in the **Date** field.
      - **AppConnect Terms of Service**. Enter **ACCEPTED** or **DECLINED** in the **Value** field
      - **AppConnect Terms of Service Date**. Enter the number of units in the **Value** field and select the

units (such as days, weeks, or months) in the **Date** field.

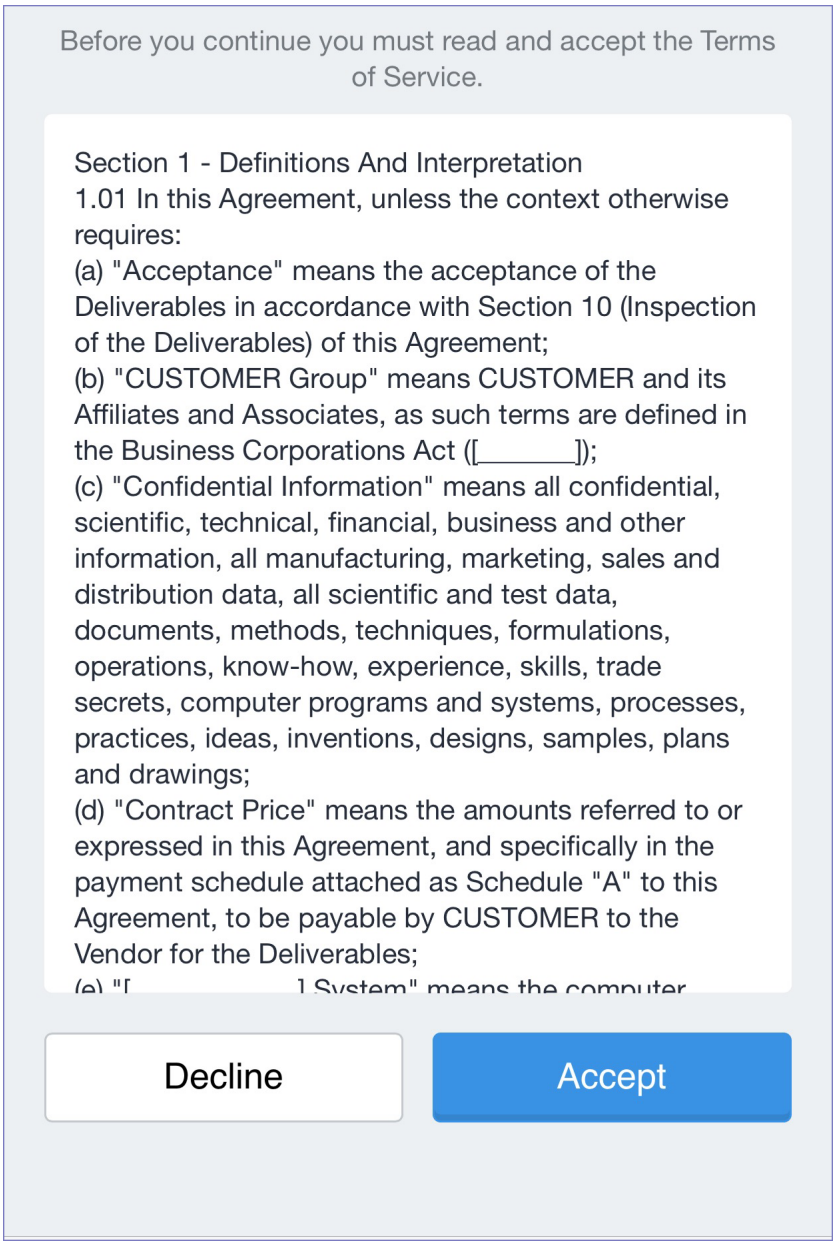
The search criteria you selected are displayed in the search field.

4. Click **Search**.
5. The results are displayed.
6. Optionally, save your search to a label by clicking **Save to Label**.
7. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.

Terms of Service for users

Device users can easily scroll through and accept an administrator-defined terms of service agreement in their web browser or Mobile@Work client, as in the following example.

FIGURE 1. TERMS OF SERVICE FOR USERS



Visual privacy

MobileIron Core allows you to display privacy information to device users.

Visual privacy describes to users what device information is collected and why, and what actions administrators can take on the device, based on MobileIron Core settings. Additionally, MobileIron Core notifies users when changes are made to the privacy policy or MDM profile settings.

Users view the visual privacy information during registration, when they must accept the privacy policy.

Enabling visual privacy for devices

When enabled, end-users will be able to learn more about the privacy of their data. Mobile@Work will show what content stays private on the device, what information is collected and why, and what actions the IT administrator can take on the debice, according to the settings on the server. This can help reduce end-user questions and concerns.

Procedure

1. Go to **Settings** > **System Settings > Users & Devices > Registration**.
2. Select **Enable privacy settings in Mobile@Work**.
3. Click **Save**.

Invite users to register

This feature is supported on macOS devices.

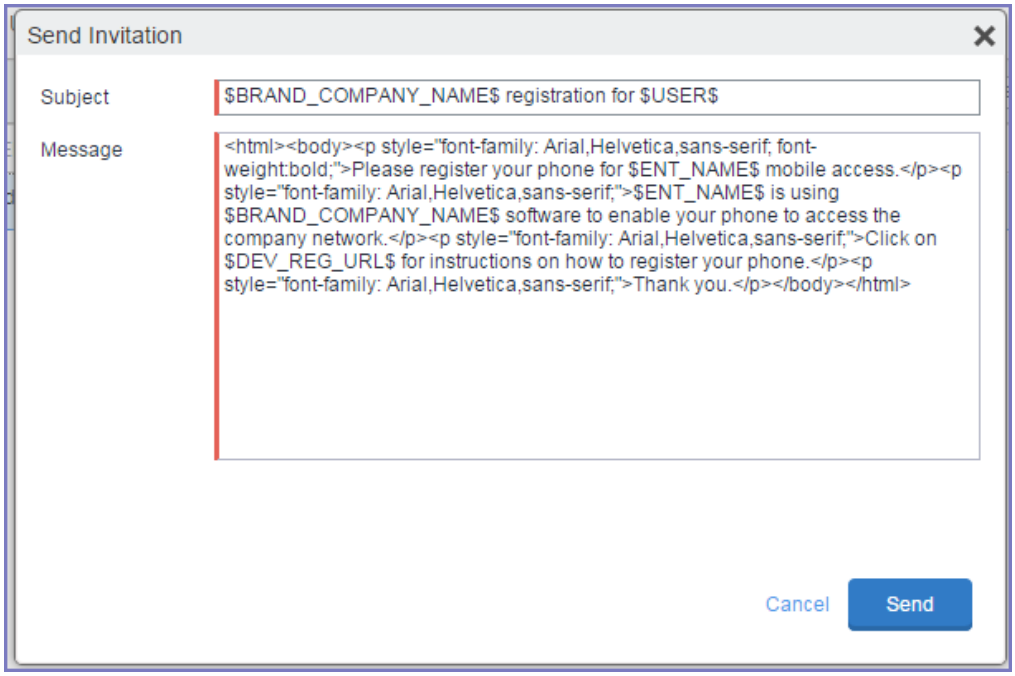
Administrators can invite users to perform self-service registration through the user portal. See Self-service User Portal for information on this self-service user portal. The administrator sends invitations that provide the instructions necessary to complete the registration process.

NOTE: Language-specific templates are not currently available for invitations.

See Registration methods for points to consider before using this registration method.

Procedure

1. Go to **Devices & Users > Users**.
2. Select the type of user accounts you want to work with:
   a. Select **Authorized Users** from the To drop-down list to select from local user accounts.
   b. Select **LDAP Entities** from the To drop-down list to select users from the configured LDAP server.
3. Click the check box next to each user you want to invite.
4. Click **Actions** and then click **Send Invitation**.



5. Review the default text for the invitation and make any changes.
   The text is displayed here with HTML markup. The user will receive the formatted version.
6. Click **Send**.

What the user sees

This registration method results in user notification via email. The email contains instructions for registering devices via the user portal. See Self-service User Portal for information on what the user is expected to do to complete the registration process.

In-app registration for iOS and Android

You can ask Android users to download Mobile@Work from Google Play and register by themselves.

Procedure

1. Make sure that the user has a user record (local or LDAP) available in MobileIron. See “Managing Users” in Getting Started with MobileIron Core.
2. Instruct the user on downloading the app and registering. The user will need the following information:
   - user name
   - password and/or Registration PIN
   - server (and the port number, if you did not use the default port number for TLS)

See Registration methods on page 42 for points to consider before using this registration method.

What the user sees

NOTE: For iOS 12.2 through the most recently released version as supported by MobileIron, when doing the iReg and in-app registration of the MDM profile, the device user experiences a different registration process.

After downloading and installing Mobile@Work, the device user must register with MobileIron Core by entering their user name, password, and server details.

NOTE: In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Mobile@Work app is running. Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". MobileIron recommends device users to enable tracking. This change applies to all versions of iOS 13 through the latest version as supported by MobileIron. Mobile@Work for iOS does not track device users' location without consent.

If a customized terms of service agreement has been defined on MobileIron Core, users will need to accept the agreement before registering with Core.

Auto-populating the MobileIron Core server name during registration

Auto-populating the MobileIron Core server name streamlines the registration process and eliminates the need for the user to type it. You can auto-populate the Core server address based on the device phone number or the email address.

NOTE: This feature is not supported for devices with Android v6.0 and above.

Auto-populating the MobileIron Core server name based on email address

To auto-populate the server name based on the device user's email address, you only need to register your MobileIron Core with MobileIron. Additional configuration on Core is not required.

Users must enter their full email address when prompted to enter their user name in the registration screen. MobileIron matches the email domain to the appropriate MobileIron Core and populates the registration screen with the correct server name.

Registering your MobileIron Core with MobileIron

To register your MobileIron Core, open a ticket on the MobileIron Support portal and provide the following information:

- your company name (e.g. MobileIron)
- your email domain (e.g. mobileiron.com)
- your MobileIron Core hostname for on-premise Core, or m.mobileiron.net:<appropriate port number> for Connected Cloud.

Auto-populating the MobileIron Core server name based on the phone number

You can also auto-populate the MobileIron Core server name based on the device's phone number. The following setup is required:

- Core access to the MobileIron Gateway. Configure the required ports. See the "Changing Firewall Rules" section in the *Installation Guide* for details.
- Enable server name look up in the Admin Portal on the **Settings > System Settings > Users & Devices > Device Registration** page.

To enable server name lookup:

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration**.
2. Select **Enable Server Name Lookup**.
3. Click **Save**.

Note The Following:

- Because this feature relies on a mobile number, it does not apply to iOS devices.
- The mobile number must also be present on the SIM in order for the **Enable Server Name Lookup** option to work.
- Registering MobileIron Core with MobileIron is not required.

Registering an Android device with Mobile@Work

After the Mobile@Work app is installed on your device, complete registration as a corporate user.

Procedure

1. Tap the Mobile@Work app icon.
   A permissions notice page is displayed to tell the user that they are about to be asked for permission to allow access to their device if you are installing Mobile@Work on Android 6.0 through the most recently released version as supported by MobileIron for the first time.
2. Select **OK**.
3. The next page asks to Allow MobileIron to make and manage phone calls from the device. This is mandatory for registration. If you click Deny, then you will be sent to TURN ON screen to Open Settings.
4. Click **Allow** to display the Settings screen of the Android device.
5. Click **Permissions**.
6. Enable Phone permissions.
7. If you visited the Setting screen, use the Android Back key to go back to the Mobile@Work registration page.
8. Click **Next**.

9. After the device admin mode is activated at a later stage, a Samsung device automatically enables all the listed permissions automatically (Contacts, Location, SMS and Phone).
10. Enter your corporate email address or server URL.
11. Click **Next**.
12. Read the Privacy Statement and click **Continue**.
13. Enter your username and password for your corporate account.
14. Click **Sign In**.
    If you are using a non-Samsung device you will be asked to proceed with Permissions if you did not enable Location permission.
15. Click **Continue**.
16. Allow MobileIron to access this device's location (optional for non-Samsung devices). If you do not grant location permission, the administrator cannot perform location related operations for the device.
    Click **Allow**.

Requiring device identifiers for enrollment

You have the option to make the collection of a device's hardware identifiers such as the IMEI number and the phone number optional before the device is enrolled. If you disable **Require device identifiers for enrollment,** the enrollment will still proceed, but the client will not collect the device identifier data. The device would be a "PDA" device such as a tablet.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration.**
2. Select **Require device identifiers for enrollment**.
   This is supported on devices using Android 6.0 through the most recently released version as supported by MobileIron.
3. Click **Save**.

NOTE: Phone number lookup is supported on devices in Device Owner mode and using Android prior to Android 6.0.

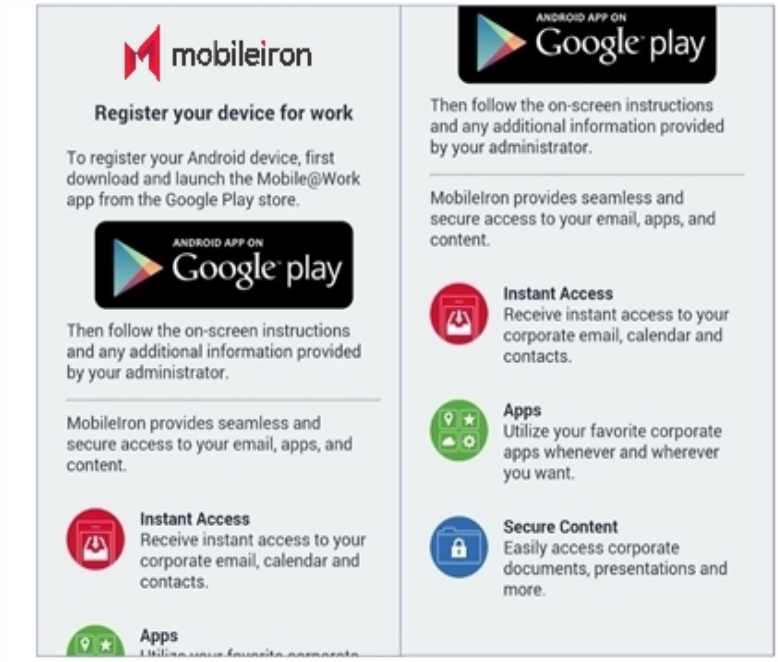
Web-based registration for Android devices

You can instruct users to register with MobileIron Core through the web. Users enter the URL of the server with forward slash "go" appended to the end of the URL, which takes them through a guided web-based registration process. Device users must still install Mobile@Work to complete the registration process.

Procedure

1. Make sure the user has a user record (local or LDAP) available in MobileIron. See "Managing Users" in Getting Started with MobileIron Core.

2. Instruct the user on downloading the app and registering. The user will need the following information:
   - user name
   - password and/or Registration PIN
   - server (and the port number, if you did not use the default port number for TLS)
3. Instruct the user to register with the MobileIron Core server at the following URL:
   https://<fully-qualified domain name for Core>/go
   The following pages are displayed, instructing the device user to download Mobile@Work for Android from Google Play:



4. Instruct the user to tap the **Google play** button so as to download Mobile@Work.
5. Instruct the user to follow the on-screen instructions in Mobile@Work, entering the user credentials and server name in the space provided.

Registering a device with Mobile@Work

After the Mobile@Work app is installed on your device, complete registration as a corporate user.

Procedure

1. Tap the Mobile@Work app icon.
   A permissions notice page is displayed to tell the user that they are about to be asked for permission to allow access to their device if you are installing Mobile@Work on Android 6.0 through the most recently released version as supported by MobileIron for the first time.
2. Select **OK**.

The next page asks to Allow MobileIron to make and manage phone calls from the device. This is mandatory for registration. If you click Deny, then you will be sent to TURN ON screen to Open Settings.

3. Click **Allow** to display the Settings screen of the Android device.
4. Click **Permissions**.
5. Enable Phone permissions.
   If you visited the Setting screen, use the Android Back key to go back to the Mobile@Work registration page.
6. Click **Next**.

   NOTE: After the device admin mode is activated at a later stage, a Samsung device automatically enables all the listed permissions automatically (Contacts, Location, SMS and Phone).
7. Enter your corporate email address or server URL.
8. Click **Next**.
9. Read the Privacy Statement and Click Continue.
10. Enter your MobileIron credentials.
11. Click **Sign In**.
    If you are using a non-Samsung device you will be asked to proceed with Permissions if you did not enable Location permission.
12. Click **Continue**.
    Allow MobileIron to access this device's location (optional for non-Samsung devices). If you do not grant location permission, the admin cannot perform location related operations for the device.
13. Click **Allow**.

ActiveSync device registration

The **ActiveSync** view displays the devices that are accessing ActiveSync. This view is populated only if you have a MobileIron Sentry configured. From this view, you can decide to register selected devices.

See Registration methods for points to consider before using this registration method.

Procedure

1. Go to **Devices & Users > ActiveSync**.
2. Select a device to be registered.
3. Click **Actions > Register**.
4. See “Single device registration” in the *Getting Started with MobileIron Core* for instructions on completing the registration process.

Managing the Android enterprise device life cycle

Managing the life cycle of an Android enterprise device includes the following steps:

- Provisioning a work managed for Android enterprise device
- Registering a work managed for Android enterprise device
- Migrating devices to Android enterprise
- Preventing automatic migration
- Migration effects on a device
- Quarantine on Android enterprise devices
- Retiring an Android enterprise device
- Wiping an Android enterprise device
- Locking an Android enterprise device
- Unlocking an Android enterprise device

Related topics

Removing Android enterprise

Provisioning a work managed for Android enterprise device

Provisioning is necessary only for work managed devices. You can provision factory reset Android devices using one of these methods:

- the MobileIron Provisioner app, which uses the NFC bump method.
- an afw# token
- Android Zero Touch

Once provisioned, a work managed device can register with MobileIron Core as usual.

Related topics

Provisioning an Android enterprise device

Registering a work managed for Android enterprise device

To register an Android enterprise-capable device, the user follows the same registration process as for any Android device. The registration process detects if MobileIron Core and the device are Android enterprise-capable, and performs the correct registration steps automatically.

To register an Android enterprise-capable device to have an Android enterprise work profile (as opposed to being registered as a regular Android device), the following must be in place:

- Core has been set up for Android enterprise as described in Enabling Android enterprise. To confirm the setup, go to **Services > Google**. In the **Android enterprise** section you should see **Account Settings:** information with **Status: Connected**.
- The **Android enterprise setting** is applied to an appropriate label.

The user follows the registration process in the Mobile@Work app.

Once registered, to verify that the device is using Android enterprise:

- on a device with a work profile, check that the Mobile@Work app appears with the Android enterprise badge
- on a work managed device that was provisioned, look for the Google Play store icon, which will show the Work version of the store.

Related topics

In-app registration for iOS and Android

Migrating devices to Android enterprise

"Migrating" refers to the actions devices take when they are already registered and running Mobile@Work and an update to MobileIron Core or Mobile@Work takes effect. This section describes migration and what to expect.

Migration does not apply to work managed devices, because such devices are enabled for Android enterprise after factory reset. Migration applies only to device that are not in work profile mode, yet.

A registered device may migrate to an Android enterprise profile (assuming Core has Android enterprise enabled, u and the device has the Android enterprise setting applied to it) when the following occurs:

- the device becomes Android enterprise-capable after it receives a firmware update from the carrier
- Core is newly enabled for Android enterprise.

In these migration scenarios, the Android devices begin their migration to use work profile automatically.

Preventing automatic migration

When all the conditions required to enable Android enterprise are met, a device will automatically migrate to use the work profile. If you want to prevent a device from automatically migrating, ensure the device does not have the **Android enterprise setting** applied.

NOTE: If you applied the **Android** label to the **Android enterprise setting**, then all Android devices potentially have the setting, and all Android enterprise-capable devices be will be automatically migrated. If this is not desired, do not use the **Android** label for this configuration.

Migration effects on a device

The following changes occur on a registered device when it is migrated to work profile:

1. User is prompted to uninstall all secure apps and in-house apps.

   NOTE: The migration will not continue until the user completes this step or there are no secure or in-house apps installed.

2. All managed configurations are removed, except for Wi-Fi configurations.
   As when a device is retired, no personal certificates are removed.
3. The Android enterprise work profile is created.
4. The Mobile@Work app icon appears with the Android enterprise badge.
5. Configuration steps appear as needed.

Quarantine on Android enterprise devices

When an Android enterprise device is quarantined (with all configurations removed) due to a compliance violation, the following changes are made on the device:

TABLE 4. ANDROID ENTERPRISE QUARANTINE BEHAVIOR

Android enterprise mode	"Quarantine app when device is quarantined" field is selected (checked)	"Quarantine app when device is quarantined" field is de-selected (not checked)
• Work profile mode • Work managed device mode • Managed device with Work profile mode NOTE:	• All the apps in the Work profile are hidden, except: - Google Play - Mobile@Work - Downloads • Contacts are hidden. • The Wi-Fi configurations are kept or removed, based on the quarantine settings.	Users will still see the app on the device.

NOTE: The quarantine behavior of individual Android enterprise apps is controlled by setting the configuration of each Android enterprise app in the App Catalog.

For more information, see "Adding in-house apps for Android" section or the "Adding an Android enterprise public app using the app wizard in the Core Admin Portal" section in the *MobileIron Apps@Work Guide*.

Retiring an Android enterprise device

When an Android enterprise device gets the **Retire** command, the following behavior occurs:

TABLE 5. ANDROID ENTERPRISE RETIRE BEHAVIOR

Android enterprise status	Retire behavior
work profile	• The work profile is removed. • All apps, data, and contacts in the work profile are removed. • A user can re-register a retired device by re-enabling Mobile@Work through Google Play.
work managed device	The device is reset to factory settings. (Note: Retire and Wipe have the same effect.) The device can be re-provisioned by an administrator.

Related topics

Removing an Android enterprise configuration causes device to retire

Wiping an Android enterprise device

When an Android enterprise device gets the **Wipe** command, the following behavior occurs:

TABLE 6. ANDROID ENTERPRISE WIPE BEHAVIOR

Android enterprise status	Wipe behavior
work profile	• The work profile is removed. (No changes are made to any apps or data on the personal profile.) • All apps, data, and contacts in the work profile are removed. • A user can re-register a wiped device by re-enabling Mobile@Work in Google Play.
work managed device	The device is reset to factory settings. (Note: **Retire** and **Wipe** have the same effect.) The device can be re-provisioned by an administrator.

Locking an Android enterprise device

The **Lock** command locks the screen of an Android enterprise device. To lock the device:

1. Go to **Devices & Users > Devices**.
2. Select the device.
3. Click **Actions > Lock.**
   For work managed devices, the Lock command locks the entire device. The user must enter the device password to unlock the device.

For work profile devices, the Lock command locks the work profile if a Work Challenge was set (Android 7.0 through etc). TODO from Jackie: Add what happens on pre-Android 7.0 devices. Adrian needs to provide this info.

Unlocking an Android enterprise device

The **Unlock** command unlocks the screen of an Android enterprise device. Before unlocking Samsung devices running in Device Administrator mode, the password must be reset in the DevicePolicyManager resetpassword() API. For unlocking devices with Knox licenses, administrators will need to make sure the Knox license is activated (Samsung General Policy in Policies & Configs) and then reset the password. This is applicable to Android 7 through the latest version as supported by MobileIron.

To unlock the device:

1. Go to **Devices & Users > Devices**.
2. Select the device.
3. Click **Actions > Unlock Device.**

The following table shows unlock support on Android enterprise devices:

TABLE 7. SUPPORT FOR UNLOCKING THE DEVICE PASSCODE ON ANDROID ENTERPRISE DEVICES

Android device	Prior to Android 7.0	Android 7.0 through the most recently released version as supported by MobileIron
Android enterprise work managed devices	Supported	Supported
Android enterprise work profile devices	Not supported	Supported

Provisioning an Android enterprise device

Administrators register Android enterprise devices, by registering a “work profile” and by provisioning “work managed” devices on a master device.

- Register a “work profile” device by following the regular registration process to install Mobile@Work.
- Provision “work managed” devices using a master device that is running the Provisioner app. For details, see the following sections.
  - Provisioning Android enterprise devices using a QR code or NFC bump
  - Provisioning Android enterprise devices using an afw# token
  - Provisioning Android enterprise devices using Zero Touch

Related topics

In-app registration for iOS and Android

Provisioning Android enterprise devices using a QR code or NFC bump

To provision Android enterprise devices using QR code or NFC bump you will need to download and install the MobileIron Provisioner app from Google Play on the master device.

Requirements to provision an Android enterprise device

To provision an Android enterprise device to be a work managed device, you need to:

- Ensure the required **Android enterprise Configuration** must be defined and applied to a recommended label.
- Enable Android enterprise on the server.
- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Managed Devices / Device Owner (afw#, QR code, NFC)" field set to Password, Registration PIN or Password and Registration PIN.
- Have an NFC-capable Android device (only if NFC is used) to serve as the master, with the Provisioner app installed.
- Have Android enterprise-capable devices to provision.

Enabling the Android beam for use with NFC bump

Procedure

1. Go to **Settings** on the device.
2. Go to **Networks** > **Wireless Networks.**
3. In the **Connectivity section** select **Share & connect**.
4. Slide the **NFC** switch to **On**.
5. Slide the **Android Beam** switch to **On**.

NOTE: The steps to enable the Android beam and NFC may vary on different devices.

Provisioning Android enterprise devices to become work managed devices

Procedure

1. Using the Android master device, download the **MobileIron Provisioner** app from Google Play and install the app.
2. Launch MobileIron Provisioner on the master device.

3. Select **NFC** or **QR code** for the Provisioning method.
4. Tap **App for Provisioning**, and choose the client app to be installed on the provisioned device:

Select this client app:	To register with this EMM server:
Mobile@Work	MobileIron Core
MDM	Deutsche Telekom Core
Vodafone Mobile@Work	Vodafone Core

5. Fill out the remaining fields in the MobileIron Provisioner app. Some fields may auto-populate if a supported Wi-Fi type is present. The Wi-Fi fields are not shown if QR code is selected. Use these guidelines:

Field	Value
Select app for provisioning	Mobile@Work
Time Zone	Enter the time zone to be configured on the device
Locale	Enter the locale to be configured on the device
Enable All System Apps	Click the check box to enable all system apps
Wi-Fi Network SSID	Enter the Wi-Fi SSID the target device is to use
Wi-Fi Security Type	Enter the Wi-Fi security type
Wi-Fi Password	Enter the password for the Wi-Fi
Bulk Enrollment	Bulk enrollment is optional along with the hostname and username. Optionally click the Quick Start check box to use Quick Start feature. If a username is entered or Quick Start is checked, then a hostname is required.

6. Tap **Continue**.
7. If you selected **NFC**,tap **Continue**. The screen **Bump the devices!** appears on the master device. Continue with the NFC Bump section below.
8. If you selected QR code, the screen Scan this QR code! appears on the master device. Continue with the QR Code section below.
9. Configure NFC Bump.
   a. Confirm that the target device is displaying the Android Welcome screen.
   b. Press the master device back-to-back with the target device to initiate an NFC transfer. If the NFC transfer succeeds, the target device may make a sound, and then proceed to downloading the client app. If a Wi-Fi connection cannot be established, or if the device is unable to download the client app, the device will automatically do a factory reset.

c. If you hear the sound or see a screen other than the Welcome screen, you can decouple the devices. This typically takes a few seconds. If the device is not encrypted, it will start the encryption process before continuing.

d. You can continue to provision additional devices by “bumping” the devices to the master device. The target device must be showing the Welcome screen, and the master device must be showing the “Bump the devices!” screen.

10. Configure QR Code provisioning.

a. Confirm that the target device is displaying the Android Welcome screen.

b. Tap the Android Welcome screen on the target device 6 times on the same place on the screen.

c. You will be prompted to configure a WiFi network so the setup wizard can download a QR code reader to the target device.

d. After the QR code reader is downloaded, the camera is launched.

e. Hold the target device a few inches above the master device until the QR code is scanned successfully. The setup wizard will then proceed to download the client app. If it is unable to download the client app, it will automatically do a factory reset.

f. You can continue to provision additional devices by scanning the QR code on the master device. The target device must have a camera ready to scan, and the master device must show the “Scan this QR code!” screen.

g. The QR code can also be exported by tapping the Share icon. The options offered for exporting will vary by device.

Provisioning Android enterprise devices using an afw# token

You can provision an Android enterprise device in Device Owner mode using an afw# token instead of using the NFC bump or QR code methods. This method enables you to sign on a device with a token in the form afw#mobileiron.core which facilitates an automatic installation of the Mobile@Work client and provisioning in Device Owner mode.

NOTE: Device Owner mode is supported on devices provisioned with Managed Google Play Accounts, using Android 6 through the most recently released version as supported by MobileIron. For details see the Android EMM Developers guide: https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Before you begin

- You must be enrolled with an Android enterprise account.
- The device must be Android enterprise-capable.
- The device must use Android 6 through the most recently released version as supported by MobileIron.
- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Managed Devices / Device Owner (afw#, QR code, NFC)"

field set to Password, Registration PIN or Password and Registration PIN.

- You must have an Android enterprise token for MobileIron Core or a client branded token such as:
  - MobileIron Core: **afw#mobileiron.core**
  - Deutsche Telekom: **afw#telekom.mi**
  - Vodafone: **afw#vodafone.mi**
- You must have a new or factory reset device.

Procedure

1. Power on the device and enter your WI-FI password.
   Your device may prompt you for a different password.
2. In the **Verify your account** screen enter your Android enterprise token. Click **Next**.
3. On the **Google Services** screen click **Install**.
4. Accept the Terms and Conditions.
5. On the Setup work device screen click **Next**.
   The Mobile@Work client downloads and installs on the device. The device now enters Device Owner mode.

Provisioning Android enterprise devices using Zero Touch

For information on Android Zero Touch provisioning, see the Android Zero Touch Provisioning Guide.

Note The Following:

- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Zero Touch and Samsung Knox Mobile Enrollment" field set to Password, Registration PIN or Password and Registration PIN.

Zero Touch enrollment with custom attributes

Administrators can specify certain custom device attributes at the time of initial provisioning. This works with the MobileIron Provisioner app, QR code, KNOX Mobile Enrollment (KME) and Zero Touch (ZT) for devices in Work managed device mode (DO) or corporate-owned personal-enabled (COPE) mode. It also works with all modes of registration, including PIN based and password based registration.

At initial registration and during any check-in, these custom attributes are passed on to Core to categorize the device and place it in the correct group and assign the correct labels. The client sends property (customAttributes) consisting of the device custom attribute keys (variable name) and values that client wants Core to set for that device. The client also sends to Core updated values with the existing keys for the (customAttributes) key. If the client does not send a (customAttributes) key, the existing custom attributes values will not change.

Zero Touch enrollment with custom attributes is supported for custom attributes of type: String, Boolean, and Integer. The Provisioner App only supports String type.

NOTE: It is the responsibility of the administrator to make sure that the custom attributes are setup correctly in Core beforehand and match what is being sent by the Provisioner app or Zero Touch portal.

Use Case examples

Example - BOOLEAN

- Attribute Name – COPE
- Attribute Description – Enabled COPE Mode
- Value Type – Boolean
- Variable Name – True

Example - INTEGER

- Attribute Name – OrgID
- Attribute Description – Organization ID
- Value Type – Integer
- Variable Name – 3456

Example - STRING

- Attribute Name – AEmode
- Attribute Description – Android Enterprise Mode
- Value Type – String
- Variable Name – DO

For information on how to set custom attributes, see Adding custom attributes to users and/or devices.

Managing operators and countries

MobileIron provides a default list of operators for users to select from during registration. You can enable or disable operators to determine whether they appear in the list of operators displayed during registration of US devices and other devices having a country code of 1.

For non-US devices, country selection is an important part of the registration process. MobileIron also provides a default list of countries enabled for registration purposes. You may need to adjust this list to enable additional countries.

This section explains how to customize displayed operators and countries.

Enabling operators

Enabling an operator displays it in the list of operators presented to users during registration.

Procedure

1. In the Admin Portal, go to **Services >Operators**. By default, the Operators screen shows only Enabled operators.
2. Select **Disabled** or **All** from the **Status** drop-down.
3. Click the check box next to each operator you want to enable.
4. Click **Actions > Enable**.

Enabling additional countries for registration

A subset of countries are enabled for device registration by default. You should check this list and determine if any of your users have home countries not represented in the default list.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration.**
2. Scroll to the **Countries for Registration** section.
3. Select countries from the **Disabled Countries** list.
4. Click the arrow button to move them to the **Enabled Countries** list.
5. Click **Save**.

Disabling operators

Disabling an operator removes it from the list of operators presented to users during registration.

Procedure

1. In the Admin Portal, go to **Services >Operators**.
2. By default, the **Operators** screen shows only Enabled operators.
3. Click the check box next to each operator you want to disable.
4. Click **Actions > Disable**.

Filtering operators

You can use filters to display only those operators you want to work with in the Operators screen. You can:

- Search for a specific operator
- Display operators by country
- Display operators by status

Searching for an operator

Procedure

1. Enter a portion of the operator's name in the **Search by Name** field.
2. Click the search icon to display the matching operators.
3. Click the x that appears in the search field to return to the default display.

Displaying operators by country

To narrow the list of operators by country, select a country from the **Country** drop-down list.

Displaying operators by status

To display operators by status, select from the **Status** drop-down list. The following options are available:

- Enabled
- Disabled
- All

Specifying eligible platforms for registration

In some cases, you may want to exclude from registration all devices of a particular platform. For example, if corporate policy dictates that a particular device platform will not be supported, you may want to prevent users from selecting the platform during self registration. Likewise, you may want to prevent help desk personnel from mistakenly registering the unsupported platform in the Admin Portal.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Scroll to the **Platforms for Registration** section.
3. In the **Enabled Platforms** list, select the platform you want to exclude.
   Shift-click platforms to select more than one.
4. Click the left arrow button to move the selected platforms to the **Disabled Platforms** list.
5. Click **Save**.
   All methods of registration now exclude the selected platforms.

Setting the registration PIN code length for device user registration

This feature is supported on Android, iOS and macOS devices.

By default, device users must enter a password to register a device. You have the option to require a MobileIron-generated Registration PIN in place of or in addition to the password.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Select a **Registration PIN code Length,** which is the minimum length for the PIN (6-12 characters).
3. Click **Save**.

For setting Android registration authentication, see Registering Android devices.

For iOS and macOS registration authentication, see Registering iOS and macOS devices through the web

Limit for failed attempts to enter a registration password

After the sixth failed attempt to enter a registration password, MobileIron Core locks the device user's account for 30 seconds. The device user sees a message stating that the account is locked and will be released after the specified interval.

Customizing registration messages

This feature is supported on iOS, macOS, Windows, and Android devices.

The registration process is a critical part of deployment. You can customize the registration messages involved in this process by editing the registration templates. Registration templates enable you to specify content and basic formatting using HTML markup.

MobileIron sends multiple messages related to registration:

- registration SMS
- registration email and reminder email
- post registration email

These messages may vary by:

- platform
- language

In addition, messages may vary by device type:

- phones
- PDAs

To accommodate this range of messages:

- Separate registration templates are provided for each language/platform combination.
- Each registration template contains separate text for each registration message type.
- Each registration template contains separate text for phones and PDAs.
- For when Core discovers device users that have not downloaded the MDM profile, reminder email scheduling capabilities are provided

Viewing registration templates

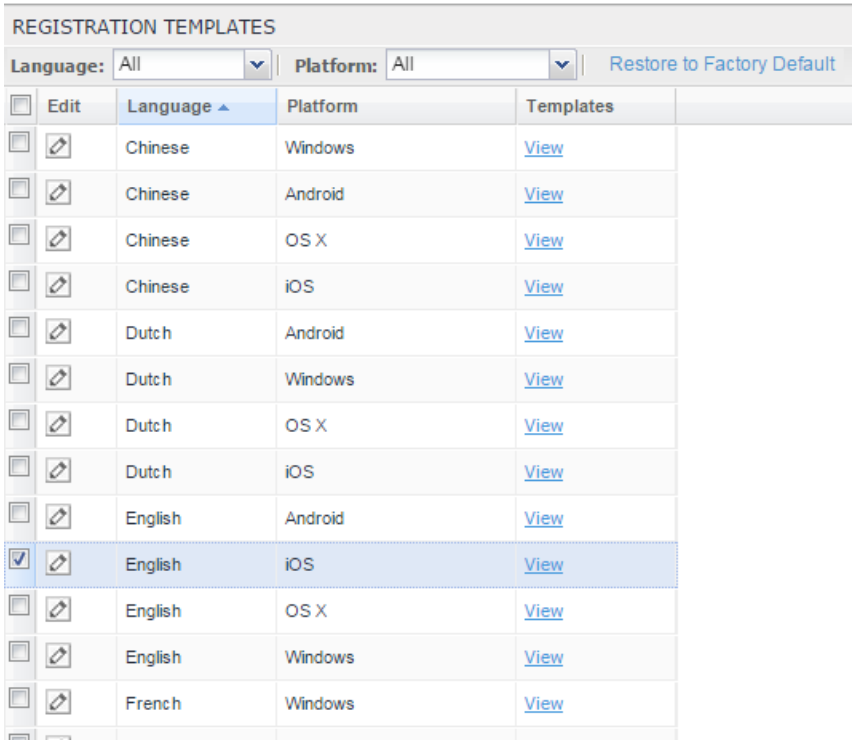
To view MobileIron message templates:

1. In Admin Portal, click **Settings > Templates**.
2. Select **Registration Templates**.
3. Click the **View** link for the template you want to view.

Editing registration messages

To edit registration messages:

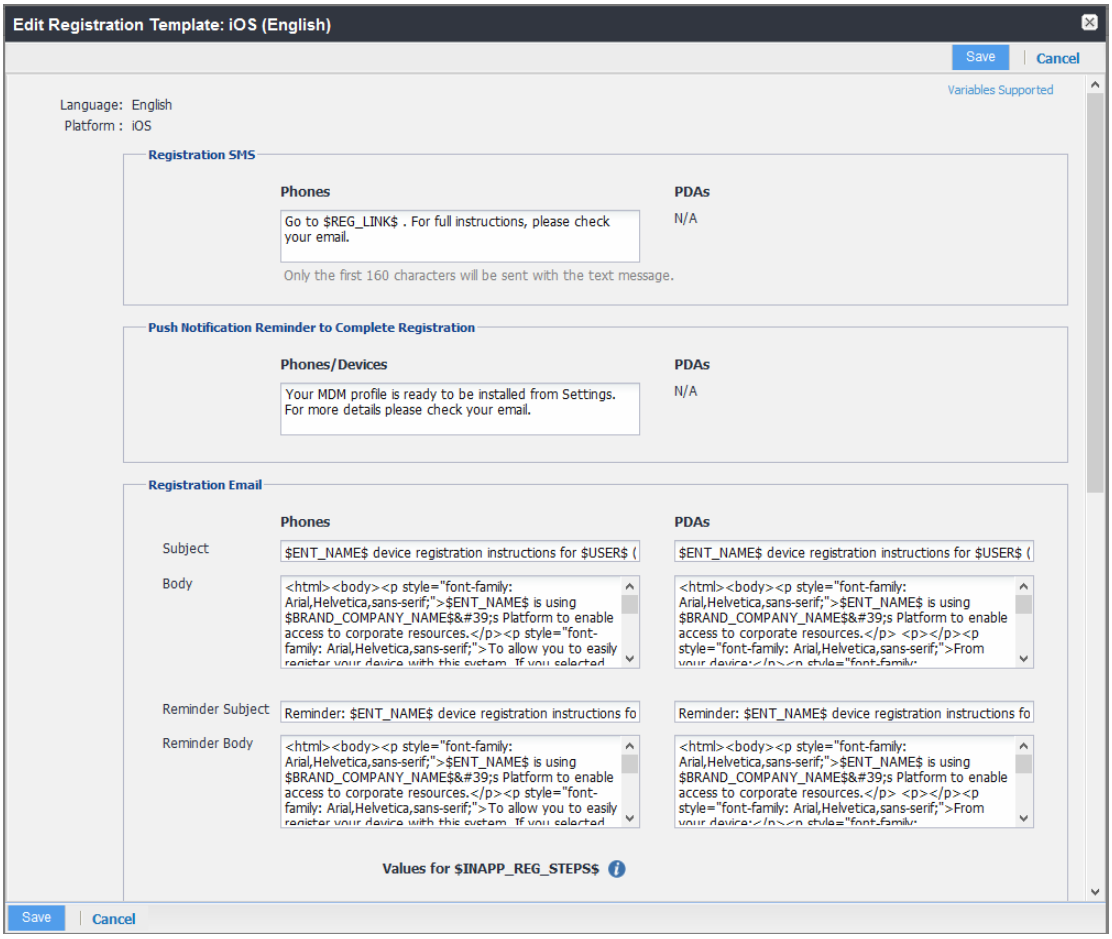
1. In Admin Portal, select **Settings > Templates > Registration Templates**.
2. Select the template you want to edit and click the **Edit** pencil icon.



   Registration messages are displayed with the HTML markup that provides the basic formatting for the content.

3. Make changes to the displayed registration messages.

NOTE: Do not add the <head> html tag in the registration template fields.



4. Click the **Variables Supported** link in the right corner of the dialog box to display a guide to the supported variables. See Using variables in registration messages on page 75 for additional details.
5. Click **Save**.

Next steps

Customizing registration messages

Using variables in registration messages

Each field in a registration template has a set of supported variables, most of which are required. Supported and required variables also differ by OS. Use the following variables to guide your customization. You can also click the Variables Supported link to display this information. **All variables except $BRANDING_COMPANY_NAME$ are also required in the specified field.**

Registration message variables

The following table gives the of variables used in types of registration messages.

TABLE 8. VARIABLES USED IN DIFFERENT TYPES OF REGISTRATION MESSAGES

Type	Supported Variables
Registration SMS, Phone	REG_LINK
Registration Email	
Registration Email, Subject (Phone)	ENT_NAME, $USER, $PHONE$
Registration Email, Subject (PDA)	ENT_NAME, $USER, $PHONE$
Registration Email, Body(Phone)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Registration Email, Body(PDA)	ENT_NAME, $BRAND_COMPANY_NAME$, REG_LINK, $INAPP_REG_STEPS$
Registration Email, Reminder Subject (Phone)	ENT_NAME, $USER$, $PHONE$
Registration Email, Reminder Subject (PDA)	ENT_NAME, $USER$, $PHONE$
Registration Email, Reminder Body (Phone)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Registration Email, Reminder Body (PDA)	ENT_NAME, $BRAND_COMPANY_NAME$, REG_LINK, $INAPP_REG_STEPS$
Values for $INAPP_REG_STEPS$	
Server	$SERVER_URL$
Username	$USER_ID$
PIN	$PASSCODE$, $PASSCODE_TTL$
Post-Registration Email	
Post Registration Email, Subject (Phone)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Post Registration Email, Subject (PDA)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Post Registration Email, Body (Phones)	$PHONES$, $BRAND_COMPANY_NAME$

Variables used inside registration messages

The following table gives the description of variables used inside registration messages.

TABLE 9. DESCRIPTION OF VARIABLES USED INSIDE REGISTRATION MESSAGES

Variable	Description
$BRAND_COMPANY_NAME$	An internal variable.
ENT_NAME	The name of the organization using MobileIron Core to secure the device. See the field **EnterpriseName** in **Settings > System Settings > General > Enterprise**.
$INAPP_REG_STEPS$	Combines $SERVER_URL$, the user's LDAP password, $PASSCODE$, and $USER_ID$.
$PASSCODE$	The registration PIN generated for the device by Core.
$PASSCODE_TTL$	The number of hours that the registration PIN remains valid. See the field **Passcode Expiry** in **Settings > System Settings > Users & Devices > Registration.**
$PHONE$	The phone number associated with the device.
REG_LINK	The URL that users access to complete the registration process (i.e., https://server name:port/a/ for Androidhttps://server name:port/v/passcode for Windows and other platforms).
$SERVER_URL$	The MobileIron Core server address used for registration.
$USER$	The name of the user associated with the device, as displayed in MobileIron Core.
$USER_ID$	The user ID for the user associated with the device, as defined in the user account on Core.

Filtering registration messages

In the Registration Templates page, you can filter registration messages by:

- language
- platform

Procedure

1. If you want to restrict the templates displayed based on language, select the preferred language from the **Language** list.
2. If you want to restrict the templates displayed based on device platform, select the preferred platform from the **Platform** list.

Restoring registration messages to default content

To restore a registration message to the default content provided by MobileIron:

1. In the **Settings > Registration Templates** page, select the template you want to restore.
2. Click **Restore to Factory Default**.

Configuring the default ownership for newly registered devices

By default, all newly registered devices are configured as company-owned. You can change this default setting to employee-owned (and back) on the Registration page.

Alternatively, you can change the ownership of a device after registration by:

- selecting **More** > **Change Ownership** in the User Portal. For more information, see About changing device ownership in the user portal on page 440.
- selecting **Devices & Users** > **Devices** > **Actions** > **Change Ownership** in MobileIron Core.

Procedure

1. In MobileIron Core, go to **Settings > System Settings > Users & Devices > Registration**.
2. For the **Default ownership for a newly registered device** setting, select the relevant radio button:
   Company owned
   OR
   Employee owned
3. Click **Save**.

Disabling analytics data collection

MobileIron collects data to analyze the use of MobileIron Core to help us provide customer support, perform bug fixes, improve product functionality and reliability and fulfill obligations to our customers. You can view details about data collected in our product privacy notice: https://www.mobileiron.com/en/legal/product-privacy.

The data is collected from:

- Mobile@Work
- Apps@Work

Procedure

1. In MobileIron Core, go to **Settings > System Settings > General > Analytics**.
2. Select the **Disable data collection from Mobile@Work and Apps@Work** check box.

3. Click **Save**. A confirmation dialog opens.
4. Click **Yes** to confirm or **No** to cancel and allow analytics data collection.

Searching for Devices

The **Devices** page in the Admin Portal, offers both basic and advanced searching features. The basic search features provide a way to find devices or users using a limited set of criteria. The Advanced search features allow you to create complex search queries using the full set of available criteria. You can also apply advanced search criteria to a new or existing/unassigned or existing/unused label.

The topics in this chapter include the following advanced topics:

- Basic searching
- Advanced searching
- Using the query builder
- Using a manually edited search expression
- Using both the query builder and manual editing
- Negative operators with advanced search
- Clearing an advanced search
- Searching for retired devices
- Searching for blocked devices
- Saving a search criterion to a label

Refer to the *Getting Started with MobileIron Core* for the most commonly used topics for managing devices, such as:

- Using the Dashboard
- Creating custom attributes
- Deleting retired devices

Basic searching

You can quickly search for devices based on the following criteria:

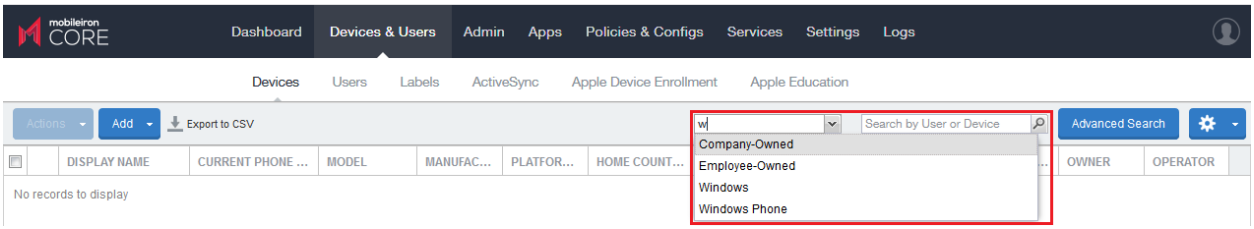
- Label
- User Principal/ID
- User Email Address
- User First/Last Name

To search by label, you can:

- select the appropriate label name from the **Labels** list.
- enter the initial letters of the label name in the **Labels** list.

  The list changes to show only label names containing the letters you entered.

FIGURE 2. SEARCH BY LABEL



To search by the other criteria, select any label in the **Labels** list then use the following syntax in the **Search by User or Device** field:

- uid:<User Principal/ID>
- mail:<User Email Address>
- name:<User First/Last Name>

NOTE: The prefixes mail: and name: are optional. All others are required. For example, to find the devices registered with the email address jdoe@mobileiron.com, you can enter the following:
mail:jdoe@mobileiron.com
or just
jdoe@mobileiron.com

Advanced searching

As data sets get larger, it is increasingly important to have a powerful search. You can use advanced search to build complex queries using the full set of available criteria. You can also create a new label using the advanced search criteria.

To access advanced search:

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Click the **Advanced Search** button located at the top right, above the table to display the query builder.
4. Enter search criteria using the query builder, or type the search expression directly. See Device field definitions.
5. Click **Search**. Verify your results.
6. (Optional) Click **Save to Label** button. This will save your new search query as a new label and in **Devices & Users > Labels**, you can utilize this new label as a filtered label.

7. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.

Searchable fields

To see the complete list of searchable fields in the query builder:

1. Click **Field** to see the categories
2. Click **Expand All**.

The fields are organized alphabetically into the following categories for convenience:

- Device fields: apply to device type based on their operating system.
- OS-specific fields: apply to devices of the selected platform.
- User fields: apply to the device's user, including LDAP fields for groups and custom attributes.

Device field definitions

This section covers the device field definitions found in the **Devices & Users > Devices** page. They also display in the Advanced Search field on the same page.

TABLE 10. DEVICE FIELD DEFINITIONS

Device Type	Field	Description
Android Fields	Admin Activated	True / false if device activated by admin.
	Android Automated Enrollment (This field is valid for Core 10.6.0.0 through the latest version as supported by MobileIron.)	Once automated Android registration is completed, the following values display: • Google Zero Touch • Knox Mobile Enrollment • Non Zero Touch AE Enrollment - this is for Managed Devices / Device Owner types (afw#, QR code, NFC) • Unknown - this value displays if versions before Core 10.6.0.0 were used. This means the "In-App Registration Requirement field in Settings > System Settings > Users & Devices > Device Registration was used. It can also mean that an old client was used with Core version 10.6.0.0 or later.
	Android Client Version Code	Version code of the client.
	Android for Work Capable	True if the device is Android enterprise capable, otherwise false.

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Attestation	Result of Samsung Attestation.
	Brand	Brand of the device.
	C2DM Token	C2DM token of the device if present, otherwise blank.
	Code Name	Code name of the Mobile@Work client
	Developer Mode	True if the Android device has Developer mode enabled, otherwise false. This is reported on all Android device configurations and also on KNOX.
	Device	Brand name of device, for example, Mako.
	Device Encryption Status	Device encryption status.
	Device Roaming Flag	True if the device is roaming, otherwise false.
	File encryption	True if the Android device has enabled file encryption, otherwise false. This is reported on all Android device configurations and also on KNOX.
	GCM/FCM Token Present	GCM token of the device if present, otherwise blank.
	Google Device Account Present	True if the device has a Google Device Account (eg: Android enterprise), false otherwise.
	ICCID	Integrated Circuit Card Identifier number.
	Kiosk Enabled	True if the device is kiosk enabled, otherwise false.
	Manufacturer OS Version	Manufacturer OS version.
	MDM Enabled	True if MDM is enabled, otherwise false.
	Media Card Capacity	Amount of memory capacity of the media / SD card.
	Media Card Free	Amount of free memory on the media / SD card.
	Multi MDM	Indicates true/false.
	OS API Level	The Android OS API level. See https://developer.android.com/studio/releases/platforms for more details. This number is used so administrators can use a numerical

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		comparison of OS versions.
	OS Build Number	OS build number.
	OS Update Path	OS Update Path.
	OS Update Status	OS Update Status.
	OS Version	Lists the OS version of the device.
	Password/PIN Days Before Expiring	Represents the number of days before the password / PIN will expire. This numerical value is controlled by the Security policy's Maximum Password Age field value. This field is a dynamic field, its value decreases every day by 1 until the password / PIN is renewed. At renewal, the value returns to the original number stated in the Maximum Password Age field and starts a new daily count-down. See Working with default policies.
	Platform Flags	Internal string representing the capabilities of the Mobile@Work application.
	Registration Status	Registration status of the device.
	SafetyNet Enabled	True if SafetyNet is enabled, false otherwise.
	SafetyNet Exception	SafetyNet exception during error.
	SafetyNet Status	SafetyNet status if enabled and no error.
	SafetyNet Timestamp	Timestamp of when last SafetyNet check was run.
	Samsung Carrier Code	Samsung Carrier code.
	Samsung E-FOTA Capable	True if the device supports Samsung E-FOTA, false otherwise.
	Samsung KNOX Version	Knox version, if present.
	Samsung Model Number	Samsung Model Number.
	Samsung SAFE Version	Samsung Safe Version.
	Screenlock PIN Change Prompt – Showing	Indicates if device user was prompted to change the device's screen lock password / PIN and the device user skipped the prompt. Values are:

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		• Unknown - If coming from an older client device, value is unknown. • True - Indicates the PIN is to expire in 7 days or less. • False - (default) Indicates the device user is not being prompted to change the password / PIN (it has not reached its 7-day expiration window.) The value listed stays until the device user successfully changes the password /PIN on the device. See Working with default policies.
	Secure Apps Enabled	True if Secured Apps / AppConnect is enabled, otherwise false.
	Secure Apps Encryption Enabled	True if Secured Apps Encryption is enabled, otherwise false.
	Secure Apps Encryption Mode	Type of Secured Apps / AppConnect Encryption.
	Security Detail	Reason for security failure if it occurs.
	Security Patch Level	Security Patch Level string or timestamp.
	Security Patch Level Date	Date of the Security Patch Level of the OS.
	Security Reason	Reason device is considered jailbroken.
	USB Debugging	True if USB debugging is enabled, otherwise false.
	Wear OS Client installed	True only if one or more paired-watches have Mobile@Work installed on the Wear OS device.
	Wear OS Device is Paired	True if one or more Wear OS device is paired to device via Bluetooth.
	Zebra Build Fingerprint	Fingerprint of the firmware build currently present on the Zebra device.
	Zebra Device Build Id	Current Build ID of the Zebra device.
	Zebra Device System Update	• **Unknown** - Not supported by client or OS version • **Current** - The most current update is installed. Applicable to Android 8 through the most recently released version as supported by MobileIron. Applicable to Zebra 6 through the most recently released version as supported by MobileIron.

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
		• **Pending** - The client has accepted a system update configuration, but the update is not yet downloaded or installed. Applicable for Zebra 6 through the most recently released version as supported by MobileIron. • **Downloading** - An update is being downloaded. Applicable for Zebra 6 through the most recently released version as supported by MobileIron. • **Available** - An update is available (Android 8 through the most recently released version as supported by MobileIron) or downloaded (Zebra 6 through the most recently released version as supported by MobileIron) but is not yet installed.
	Zebra OTA Capable	True if the device supports Zebra OTA (Over The Air), otherwise false.
	Zebra Patch Version	The version of firmware for the Zebra device to be upgraded to. This is the target firmware version of the firmware applied to the Zebra device through firmware policy.
Common Fields	APNS Capable	Only true if there is an APNS token for the Mobile@Work client, otherwise false.
	AppConnect Terms of Service	True/false for if the AppConnect Terms of Service was accepted.
	AppConnect Terms of Service Date	Represents the date/time the AppConnect Terms of Service was accepted.
	Background Status	True if iOS background status is enabled, otherwise false.
	Battery Level	Percentage of battery left.
	Block Reason	A list of reasons why the device is blocked.
	Blocked	True if the device is blocked, otherwise false.
	Cellular Technology	GSM, CDMA, or blank if the device does not support cellular.
	Client Build Date	The build date of the client, if registered with Mobile@Work client.
	Client Id	The unique client ID if the device was registered with

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		Mobile@Work client.
	Client Last Check-in	Date/Time of last check-in.
	Client Migration Status	Status of Mobile@Work client migration from Core to Cloud (true/false).
	Client Name	The name of the client, if registered with Mobile@Work client.
	Client Version	The version of the client, if registered with Mobile@Work client; otherwise, false.
	Cloud Migration Status	Status of device migration from Core to Cloud (true/false).
	Comment	A field that the admin uses to add their own comments for the device.
	Compliant	True if the device is in compliance, otherwise false.
	Creation Date	The creation date of this device record.
	Current Country Code	Current country code of the device.
	Current Country Name	Current country name of the device.
	Current Operator Name	Short name of the cellular carrier, if there is a cellular service.
	Current Phone Number	Current phone number of device, if the device has cellular service.
	Device Admin Enabled	True if device admin (Android) is enabled, otherwise false.
	Device Encrypted	True if the device is encrypted, otherwise false.
	Device is Compromised	True if the device is compromised, for example, jailbroken.
	Device Locale	Locale of the device.
	Device Owner	Company or Personal.
	Device Space	Name of the space the device belongs to.
	Device UUID	Unique ID of the device generated from Core.
	Display Size	Size of device's display.
	EAS Last Sync Time	Exchange ActiveSync last sync time.

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
	Ethernet MAC	Ethernet MAC ID.
	Home Country Code	Home (Initial) country code of the device.
	Home Country Name	Home country name of the device.
	Home Operator Name	Home Operator Name.
	Home Phone Number	Home Phone Number.
	IMEI	IMEI (International Mobile Equipment Identity) number.
	IMSI	ISMI (International Mobile Subscriber Identity) number.
	IP Address	Current IP address of the device.
	Language	Language of the device.
	Last Check-in	Last check-in time of the device.
	Manufacturer	Manufacturer of the device.
	MDM Last Check-in	Last MDM check-in time of the device.
	MDM Managed	True if the device is MDM managed, otherwise false.
	Memory Capacity	Memory capacity of the device.
	Memory Free	Amount of free memory in the device.
	MobileIron Threat Defense Status	MobileIron Threat Defense Status.
	MobileIron Tunnel App Installed	True / false if the MobileIron Tunnel app was installed.
	Model	Model of the device.
	Model Name	Model name of the device.
	Modified Date	Date/Time for last updates to device details.
	MTD Anti-Phishing Status	MTD Anti-Phishing Status.
	Non-compliance Reason	Reason why the device is not in compliance.
	OS Version	OS version number string.
	Passcode	Contains registration PIN for a preregistered device, empty if

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
		none exists.
	Passcode Expiration Time	The expiration time for the registration pin for a prereigstered device, empty if none exists.
	Platform	Operating system of the device.
	Platform Name	Operating system and OS version of the device.
	Processor Architecture	Architecture of the processor for the device.
	Quarantined	True if the device is quarantined, false otherwise.
	Quarantined Reason	Reason for quarantined, empty if the device is not quarantined.
	Registration Date	Registration date of the device.
	Registration IMSI	Registration of ISMI (international mobile subscriber identity) number.
	Registration UUID	Unique ID when registering from the client.
	Retired	True if the device is retired, otherwise false.
	Roaming	True if the device is roaming, otherwise false.
	SD Card Encrypted	True/faise if SD card is encrypted.
	Security State	Security state of the device.
	Serial Number	Serial number of the device.
	Status	Status of the device.
	Storage Capacity	Total storage capacity, in bytes, of the device.
	Storage Free	Number of bytes of free storage on the device.
	Terms of Service Accepted	True if the End user Terms of Service was accepted, otherwise false.
	Terms of Service Accepted Date	Date for when the End User Terms of Service was accepted, otherwise blank.
	Wi-Fi MAC	Wi-FI MAC address of the device.

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
iOS Fields	Activation Lock Bypass Code	Code to bypass activation lock.
	Activation Lock is Enabled	True if Activation Lock is enabled on the device, otherwise false. Applicable to iOS.
	APNS Token	Mobile@Work client APNS wakeup token. Applicable to iOS.
	Apple Device Mac Address	iPhone (media access control address) MAC address. Applicable to iOS and OS X.
	Apple Device Version	iPhone version code. Applicable to iOS and OS X.
	Apple OS Update Product Key	Available OS update product key. Applicable to iOS and macOS.
	Apple OS Update Product Version	Available OS update product version. Applicable to iOS and macOS.
	Apple OS Update Status	OS update status. Applicable to iOS and macOS.
	Bluetooth MAC	Bluetooth MAC address. Applicable to and OS X.
	Build Version	MDM build version. Applicable to iOS and OS X.
	Carrier Settings Version	Carrier settings version. Applicable to iOS.
	Current Mobile Country Code	Current mobile country code. Applicable to iOS.
	Current Mobile Network Code	Current mobile network code. Applicable to iOS.
	Data Protection	Applicable to iOS.
	Data Roaming Enabled	True if device is data roaming enabled, otherwise false. Applicable to iOS.
	DEP Device	True if the device is a DEP device, otherwise false. Applicable to iOS, macOS, and tvOS.
	DEP Enrolled	True if the device is DEP enrolled, otherwise false. Applicable to iOS.
	Device Locator Service is Enabled	True if device locator service is enabled, otherwise false. Applicable to iOS.

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Device Name	Name of the device. Applicable to iOS and OS X.
	Do Not Disturb is in Effect	True if Do Not Disturb is enabled, otherwise false. Applicable to iOS.
	Force Encrypted Backup	True if backups are forced to be encrypted, otherwise false. Applicable to iOS.
	Full Disk Encryption Enabled	True if full disk encryption is enabled, otherwise false. Applicable to macOS 10.9+.
	Full Disk Encryption Has Institutional Recovery Key	True if full disk encryption has institutional recovery key, otherwise false. Applicable to macOS 10.9+.
	Full Disk Encryption Has Personal Recovery Key	True if full disk encryption has personal recovery key, otherwise false. Applicable to macOS 10.9+.
	Hardware Encryption Caps	Hardware encryption capabilities. Applicable to iOS.
	iCloud Backup is Enabled	True if Cloud backup is enabled, otherwise false. Applicable to iOS.
	iOS Background Status	True if iOS background status is enabled, otherwise false. Applicable to iOS.
	iOS ICCID	Device's integrated circuit card identifier number. Applicable to iOS.
	IT Policy Result	Applicable to iOS.
	iTunes Store Account Hash	iTunes Store Account Hash.
	iTunes Store Account is Active	Ttrue if iTunes Store Account is active, otherwise false. Applicable to iOS.
	Languages	Language of the device. Applicable to tvOS.
	Last Acknowledged Lock PIN	PIN to unlock a locked macOS device. Applicable to macOS.
	Last Acknowledged Wipe PIN	PIN to proceed after wiping a macOS device. Applicable to macOS.
	Last iCloud Backup Date	Last iCloud backup date. Applicable to iOS.

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
	Last MTD Sync Time	Last MTD check-in time. Applicable to iOS.
	Locales	Locale of the device. Applicable to tvOS.
	macOS User ID	macOS user ID. Applicable to OS X.
	macOS User Long Name	macOS user's long name. Applicable to OS X.
	macOS User Short Name	macOS user's short name.Applicable to OS X.
	Maximum Resident Users	Only for use with iOS Education Shared iPads. Tells the device how many users will have their data cache on the device. When the device reaches this number, the next logged-in user that is not already present will be cached and one of the cached users will be removed from the cache (up to Apple which user.) Applicable to iOS.
	MDM Lost Mode Enabled	True if MDM Lost Mode is enabled, otherwise false. Applicable to iOS.
	MDM Service Enrolled	True if the device is was enrolled via MDM Service (non-over air DEP), otherwise false. Applicable to iOS.
	MEID	Mobile Equipment Identity Number.
	Modem Firmware Version	Modem firmware version. Applicable to iOS.
	Network Tethered	True if the device was reported as currently network tethered, otherwise false. Applicable to macOS.
	Organization Info	Organization for the device. Applicable to iOS.
	Passcode Compliant	True if passcode is in compliance, otherwise false. Applicable to iOS.
	Passcode Compliant with Profiles	True if passcode is compliant with rules specified from profiles. Applicable to iOS.
	Passcode Present	True if Passcode is present on device, otherwise false. Applicable to iOS.
	Personal Hotspot Enabled	True if Personal Hotspot is enabled, otherwise false. Applicable to iOS.
	Product Code	iPhone Product code. Applicable to iOS and OS X.

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
	Product Name	Product name. Applicable to iOS and OS X.
	Security Reason Code	Security reason code. Applicable to iOS.
	SIM Label 1, 2, 3	SIM label associated to the phone number.
	SIM MCC 1, 2, 3	SIM card mobile country code associated to the phone number.
	SIM MNC 1, 2, 3	SIM card mobile network code associated to the phone number
	SIM Phone Number 1, 2, 3	The phone number associated with the SIM card / eSIM.
	SIMs	• Lists the number of SIMs associated to the device. This includes embedded SIMs (eSIM) and physical SIMs. • There can be multiple SIMs associated with the eSIM. • For eSIMs in iPhone XS, iPhone XS Max, or iPhone XR with iOS 12.1 or later through the most recently released version as supported by MobileIron.
	Subscriber Carrier Network	SIM card subscriber carrier network. Applicable to iOS.
	Subscriber MCC	SIM card mobile country code. Applicable to iOS.
	Subscriber MNC	SIM card mobile network code Applicable to iOS.
	Supervised	True if the device is MDM supervised, otherwise false. Applicable to iOS.
	UDID	iPhone unique device identifier. Applicable to iOS and OS X.
	Voice Roaming Enabled	True if voice roaming is enabled, otherwise false. Applicable to iOS.
	VPN IP Address	VPN IP address. Applicable to iOS and tvOS.
	Wakeup Status	Device Wakeup status.
User Fields	Display Name	The display name of the device user.
	Email Address	Device user's email address.
	First Name	Device user's first name.
	Last Admin Portal Login Time	Date of admin's last log in into Core.

TABLE 10. DEVICE FIELD DEFINITIONS(CONT.)

Device Type	Field	Description
	Last Name	Device user's last name.
	LDAP > Attribute Distinguished Name	The Attribute Distinguished Name for an LDAP user.
	LDAP > Groups > LDAP Group Distinguished Name	LDAP Users who are members of an LDAP group with a specific group distinguished name.
	LDAP > Groups > Name	LDAP Users who are members of an LDAP group with a specific group name.
	LDAP > LDAP User Distinguished Name	The LDAP distinguished Name of the user.
	LDAP > LDAP User Locale	An LDAP User who are members of a specific locale.
	LDAP > Principal	Value of the attribute specified as the User ID in the LDAP server configuration.
	LDAP > upn	Value of the attribute specified as the User Principal Name in the LDAP server configuration.
	LDAP > User Account Control > Account Disabled	Indicates whether the LDAP user account is disabled (true/false).
	LDAP > User Account Control > Locked Out	Indicates whether the LDAP user account is locked out (true/false).
	LDAP > User Account Control > Password Expired	Indicates whether the LDAP user 's password has expired (true/false).
	LDAP > User Attributes > custom1	The value of the LDAP user attribute is defined in **Services > LDAP**.
	LDAP > User Attributes > custom2	The value of the LDAP user attribute is defined in **Services > LDAP**.
	LDAP > User Attributes > custom3	The value of the LDAP user attribute is defined in **Services > LDAP**.
	LDAP > User Attributes >	The value of the LDAP user attribute is defined in **Services > LDAP**.

TABLE 10. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	custom4	
	LDAP > User Attributes > memberOf	The value of the LDAP user attribute is defined in **Services > LDAP**.
	SAM Account Name	The security account name. This was the login name for earlier versions of Windows.
	User ID	The LDAP user ID.
	User UUID	The LDAP Universally Unique Identifier.

For **Windows** field definitions, see https://docs.microsoft.com/en-us/windows/client-management/mdm/healthattestation-csp.

Using the query builder

To use the query builder:

1. Select a field on which to search. **Hint**: you can type a few letters of the field name to see a short list of matching fields, or press **Expand All** within the field list to see all the fields.
   For example, if you select **Status**, the search engine provides only values available for **Status**.
2. Select an operator, such as **Equals**.
3. Click in the **Value** field to enter a value you want to search.
4. Some fields have predetermined values that you can select.
5. Select additional fields and criteria as needed.
6. Click **All** to combine the criteria with a logical AND or click **Any** to combine the criteria with OR.
7. Click **Search** to display the matching devices and their owners.

NOTE: To include retired devices in the results, uncheck the check box to the left of the **Search** button.

Using a manually edited search expression

To enter a search expression directly into the expression field:

1. Type or paste the search criteria into the expression field. The automatic syntax check displays a status icon next to the expression field. A green icon indicates that the syntax is correct, and a red icon if incorrect.
2. When the syntax is correct, click **Search** to display the matching devices and their owners.

Using both the query builder and manual editing

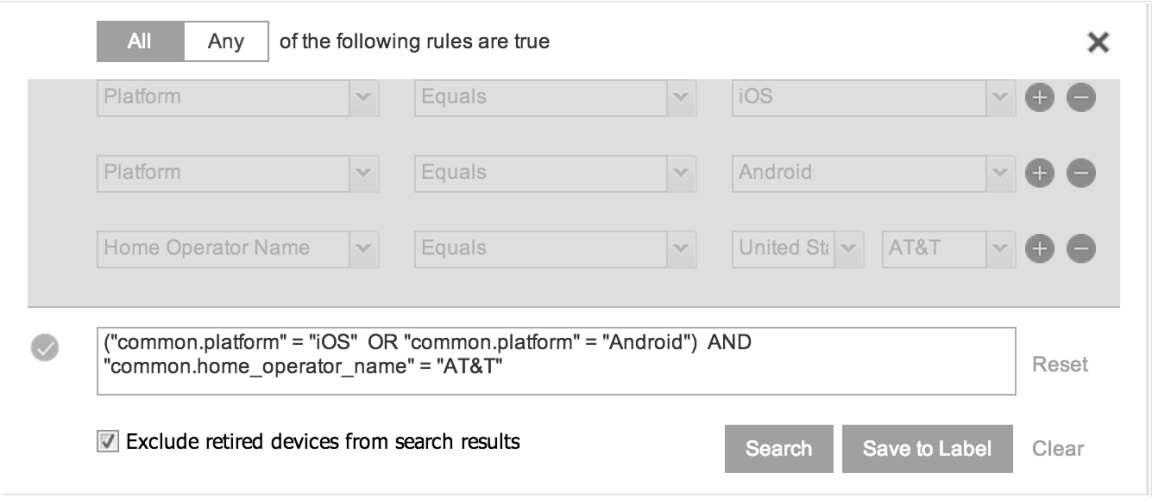
Use the query builder to start an expression, look up field syntax, and select predetermined values. Then, edit the expression directly as needed.

1. Select fields and criteria.
2. Click **All** to combine multiple criteria with a logical AND or **Any** to combine multiple criteria with OR. You can manually edit individual logical operators in the expression field.
3. In the expression field, edit the expression directly.
4. For example, you can add parentheses, change logical operators, or manually edit field names or values.
5. The automatic syntax check displays a status icon next to the expression field. A green icon indicates that the syntax is correct, and a red icon if incorrect.
6. When the syntax is correct, click **Search** to display the matching devices and their owners.

Once you manually edit the expression, the query builder is covered with a gray box to indicate it no longer represents the current state of the expression. Click the **Reset** link to remove your manual edits and continue using the query builder.

Example: Find all iOS or Android devices that use AT&T as their service operator.

FIGURE 3. SERVICE OPERATOR IN QUERY BUILDER



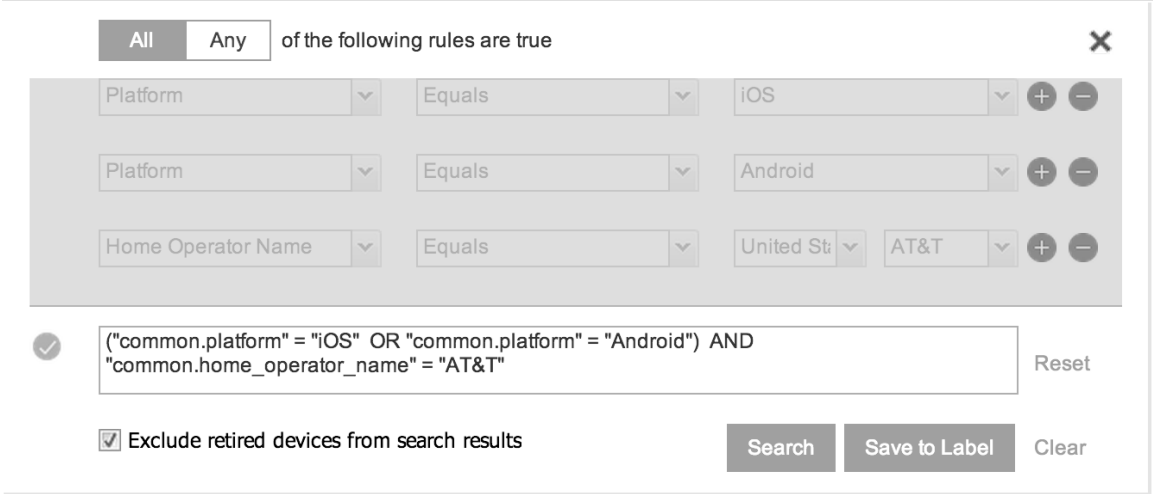
Build the expression to match the above example.

1. Click **Advanced Search** to open the query builder.
2. Select **Platform** in the first field, select **Equals** for the operator, then select **iOS** as the platform.
3. Click the plus icon to add another row for criteria.
4. Select **Platform**, **Equals**, and **Android** as the field, operator, and platform value, respectively.

5. Click the plus icon to add a third row for criteria.
6. Select **Home Operator Name** for the field and **Equals** for the operator.
   Notice that the value field adjusts automatically to display service operator values by country.
7. Accept the first value field and select **AT&T** in the second value field.

Manually edit the expression.

1. Replace the first **AND** with **OR**.
   The syntax is checked automatically as you type. Note a red icon indicating incorrect syntax while you edit the expression.
2. Add parentheses around the phrase to read:
   ```
   ("common.platform" = "iOS" OR "common.platform" = "Android") AND
   “common.home_operator_name” = “ATT&T”
   ```
   Note a green icon indicating correct syntax has replaced the red icon. Your advanced search will look the same as the original image (see below).



   To revert to the original expression without your manual edits, click the **Reset** link to the right of the expression.
3. Click **Search** to display the matching devices and their owners.

Negative operators with advanced search

Using negative operators enables you to create filters that exclude devices instead of including them. For example, you can search for:

- Devices that use any platform other than iOS
- Devices with a current country code other than US

TABLE 11. NEGATIVE OPERATORS WITH ADVANCED SEARCH

Operator	Action	Example
Does not equal	Returns a list of devices that do not match the criteria specified in the value field for the selected field.	Select: • **Home Country Name** as the field • **Does not equal** in **Operator** • **United States** in **Country Name** The search returns a list of devices that do not have United States as their home country name.
Does not contain	Returns a list of devices that do not contain the string specified in the selected field. • Used only with strings. • Available only in the expression field.	Select or enter: • Go to **Common Fields** and select **Device Space**. • In the expression field, enter: does not contain • Place the cursor between the two quote marks in the expression field and enter: **Global** The search returns a list of devices that are not assigned to the **Global** space.

Examples for advanced search with negative operators

To display a list of devices that have countries other than the United States as the assigned home country, create an advanced search expression that provides the necessary information.

1. Go to **Device & Users > Devices.**
2. Click the large magnifying glass icon located at the top right to initiate an advanced search.
3. In **Field**, select **Common Fields**.
4. Select **Home Country Name**.
5. Select **Does not equal** from the list in **Operator**.
6. Select **United States** from the list of countries in **Country Name**.
7. Click **Search**.
8. **Optional:** To save the search to a label, click **Save to Label** and then provide an existing label name or a new label name and description.
9. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.

Suppose you want to list users within an LDAP group that have a Home Country Code other than the United States (US).

To create the advanced search expression that provides the needed list:

1. Go to **Device & Users** > **Devices**
2. Click the large magnifying glass icon located at the top right to initiate an advanced search.
3. In the expression field enter the following, including quote marks:
   “user.ldap.groups.name” = “Corp_Users” AND “common.home_country_code” != “US”
4. Click **Search**.
5. **Optional:** To save the search to a label, click **Save to Label** and then provide a new label name and description.
6. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.

Clearing an advanced search

- In the advanced search, click the **Clear** link, or
- Apply a different search by entering a basic search.

Closing the advanced search query builder does not clear the search.

Searching for retired devices

By default, retired devices are excluded from search results. To include them, uncheck the Exclude Retired Devices From Search Results check box, located to the left of the Search button in advanced search.

To find only retired devices:

1. Uncheck the check box to exclude retired devices
2. Select the following in the advanced search query builder:
   - Field: **Retired**
   - Operator: **Equals**
   - Value: **true**
3. Click **Search**.

The matching records are displayed.

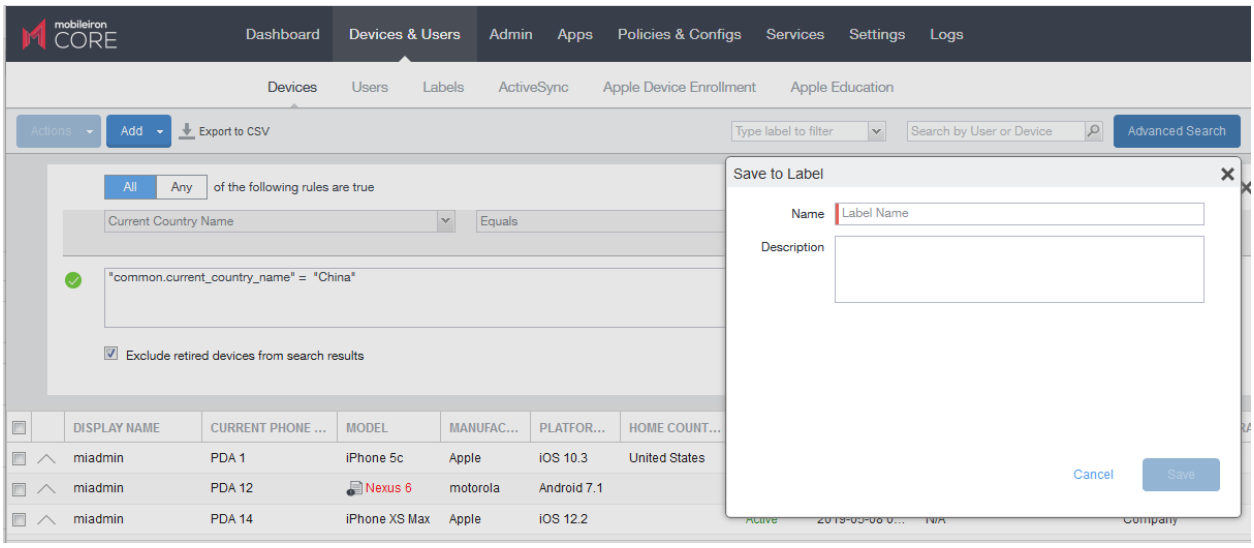
Searching for blocked devices

You can search for devices for which the status field value is **Blocked**, which means that the device is blocked from accessing the ActiveSync server. However, the **Status** column does not show the value **Blocked**. Instead, the ActiveSync Association view shows this information. See “Viewing ActiveSync associations” in the *MobileIron Sentry Guide.*

Saving a search criterion to a label

Once you create a search criterion, you can save it to a label. Click the **Save To Label** button in advanced search to create a new label using the search criterion. Type a new label name in the **Label** field and type a description. The new filter label is created with the advanced search criterion applied.

FIGURE 4. SAVING A SEARCH CRITERION TO A LABEL



If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.

Securing Devices

Securing devices is at the heart of MobileIron Core. The topics in this chapter include the following advanced topics:

Refer to the *Getting Started with MobileIron Core* for the most commonly used topics for managing devices, such as:

- Displaying device assets
- Restricting the number of devices a user registers

Registration-related features and tasks

The following table summarizes features and tasks related to registration.

TABLE 12. REGISTRATION-RELATED TASKS

Feature	Description	Use Case
Reprovisioning a device	Restarts the MobileIron provisioning process for the device	Troubleshooting incomplete registration
Retire	Ends the registration (and MobileIron management) for a device	Moving devices out of inventory

Reprovisioning a device

Select **Re-provision Device** to restart the MobileIron provisioning process without repeating the whole registration process. For example, you might want to do this if the initial attempt was interrupted, leaving the registration in the Pending state.

NOTE: This action applies only to devices in the Pending or Verified state. To reinstall the MobileIron Client for devices in the Active state, you can either restore from a backup snapshot or retire the device and re-register it. To reinstall the MobileIron Client for devices in the Wiped state, you must re-register the device.

Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Select **Actions > Re-provision Device**.
4. The same registration settings are used.

Using self service security features

Users can perform lock, unlock, wipe and retire functions on devices on which they are registered from the new **My Devices** page on the device.

Procedure

1. Open the Mobile@Work app on the device.
2. Click the menu icon in the upper left corner of the landing page.
3. Click **My Devices.**
4. You are prompted to login. Login is required when accessing the page for the first time.
5. Click **Continue**.
   A list of the devices on which the user is registered is displayed on the **My Devices** page.
6. Select the device. The **Device Details** page is displayed.
7. Choose to **Lock Device** or **Unlock Device**.
   When **Lock Device** or **Unlock Device** is selected the user is prompted to enter their password and confirm the action.
8. Click the menu icon on the upper right to select **Wipe** or **Retire** the device.
   When **Wipe** or **Retire** is selected the user is prompted to enter their password and confirm the action.

Retiring a device

Retiring a device archives the data for that device and removes the configurations and settings applied by MobileIron Core (no personal information or settings on the device are impacted). The entry for the device no longer appears in the **Device & Users** page (unless you specifically search for retired devices), and the user is notified that the software has been removed.

If the retired device is also in the ActiveSync Association view, it remains there. However, because the device is retired, it can no longer access the ActiveSync server. You can manually remove the device from the ActiveSync Association page. See “Removing ActiveSync phones” in the MobileIron Sentry Guide.

Retiring an Android device means the device user cannot access any AppConnect apps or data. For details, see the MobileIron Core AppConnect and AppTunnel Guide.

If you have duplicate devices, see Managing Duplicate Devices.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Click **Actions > Retire**.
   The **Retire** dialog appears.
4. In the **Retire** dialog, confirm the user and device information and enter a note.
5. Click **Retire**.
   The user receives notification of the action.

To see a list of retired devices, see “Searching for retired devices” in the *Getting Started with MobileIron Core.*

Deletion of retired devices

As device users leave your enterprise or change to new devices, more and more devices in the MobileIron Core database are retired. When you retire a device, MobileIron Core un-registers it and no longer manages or secures the device. All the configurations and settings that Core had applied to the device are removed. The device can no longer access enterprise data or apps.

However, MobileIron Core retains retired devices in its database. Deleting these devices from the database improves Core performance and frees up disk space. Although Core also provides a web services API and a CLI command to delete retired devices, using the Admin Portal display is easier. It also provides an easy way to automatically delete retired devices every day.

With this Admin Portal display, you can:

- Easily navigate to the list of retired devices.
- Delete devices that have been retired for more than a specified number of days.
- Configure Core to automatically delete retired devices daily, weekly, or monthly.

NOTE: You can use this display only if you are assigned to the global space **and** you are assigned the admin role **Delete retired device**. Otherwise, the actions on this display are disabled.

When Core deletes retired devices due to your actions on this display, it records **Delete Retired Device** events in the audit log. Personal data related to retired devices can be deleted by deleting the local user. However, LDAP users cannot be permanently deleted unless the LDAP server or group has been deleted, in which case the LDAP users become local users and can be deleted. If a user is deleted on the LDAP server, the user is automatically removed from MobileIron Core during the next LDAP sync.

Deleting retired devices by threshold

A common task, although not necessarily a daily task, is deleting retired devices. Deleting these devices from the database improves Core performance and frees up disk space.

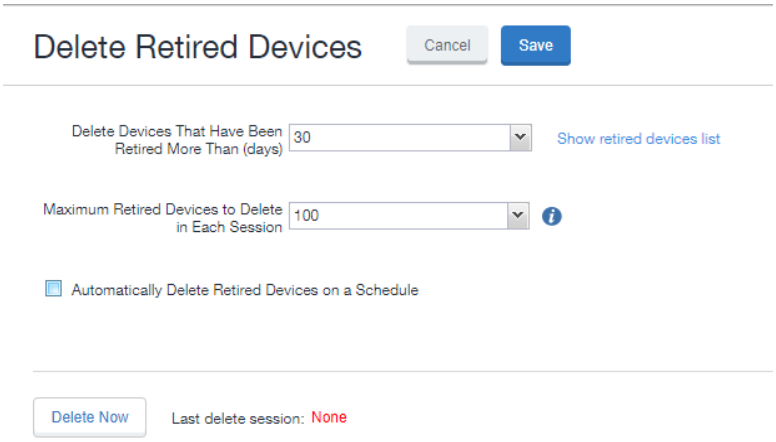
Prerequisites

Make sure you are assigned the required admin role. To delete retired devices, you must be:

- assigned to the global space
- assigned the admin role **Delete retired device**

Procedure

1. From the Admin Portal, go to **Settings > System Settings**.
2. Select **Users & Devices > Delete Retired Devices**.



3. Optional. Select the number of days after which retired devices should be deleted, or accept the default of 30 days.
4. Optional. Select the maximum retired devices to delete in each session, or accept the default of 100 devices.
5. Optional. Click **Delete Now** to delete the retired devices that meet the new criteria.
6. Click **Save** to save the configuration.

NOTE: If **Delete Now** is disabled, only an administrator who is a "super administrator" can assign you to the global space and assign the **Delete retired device** admin role to you. The procedure for the super administrator and definition of a super administrator are in Assigning an administrator the role to delete retired devices on page 106.

Deleting retired devices by schedule

You have the option to delete retired devices at daily, weekly, or monthly intervals.

Procedure

1. From the Admin Portal, go to **Settings > System Settings > Users & Devices > Delete Retired Devices**.
2. Optional. Select the number of days after which retired devices should be deleted, or accept the default of 30 days.
3. Optional. Select the maximum retired devices to delete in each session, or accept the default of 100 devices.
4. Click **Automatically Delete Retired Devices on a Schedule**. The Delete Schedule Configuration menu displays.
5. Select the **Weekly** or **Monthly** radio button, or accept the **Daily** default. Additional fields display.

   a. **Daily** - Select the hour you want the process to run.
   b. **Weekly** - Select the day and the hour you want the process to run.
   c. **Monthly** - Select the hour you want the process to run on the first day of the month.
6. Click **Save** to keep the configuration. The retired devices that match or exceed the threshold at the scheduled time will be deleted.

Assigning an administrator the role to delete retired devices

If you are a super administrator, you can assign another administrator the capability to delete retired devices. You are a super administrator if you are:

- assigned to the global space.
- assigned the role **Manage administrators and device spaces**.

Procedure

1. In the Admin Portal, go to **Admin > Admins**.
2. Select an administrator.
3. Select **Actions > Edit roles**.
4. For **Admin Space**, select **Global**.
5. Select the **Device Management** role **Delete Retired device**.
6. Click **Save**.

Managing Duplicate Devices

Before Core version 10.6, duplicate devices with an "active" state were retired. From Core version 10.6 through the latest version as supported by MobileIron, administrators can set duplicate active devices to the “Unknown” status by selecting Enable managing duplicate devices.

Core also supports Daily, Weekly and Monthly options for scheduling this feature.

Procedure

1. In the Admin portal, go to **Settings > System Settings**.
2. Expand **Users & Devices** and then click **Manage Duplicate Devices**.
   The Manage Duplicate Devices page displays.
3. Select **Enable managing duplicate devices**.
   The page expands to display more options.

   NOTE: To disable this feature, simply de-select this field.
4. Make your settings using the guidelines below.
5. Click **Save**.

TABLE 13. MANAGING DUPLICATE DEVICES SETTINGS

Item	Description
Scan Schedule Frequency	Select the appropriate radio button and make the setting: • **Daily** - Select the time of the scan of the duplicate device. This is the time on the Core server. • **Weekly** - Select the day and time of the of the duplicate device. This is the time on the Core server. • **Monthly** - Select the time of the scan of the duplicate device to occur on the first day of the month. This is the time on the Core server.
Device Action	Select one option: • Retire the old device - (default) • Mark the old device as "Unknown"

Related topics

Retiring a device

Security-related features and tasks

The following table summarizes the features and tasks related to security.

TABLE 14. SECURITY-RELATED FEATURES AND TASKS

Feature	Description	Use Case
Lock	Forces the user to enter a password before accessing the device	Dealing with lost and stolen devices
Unlock	Reverses the Lock function	Accessing the device when the passcode has been forgotten or reassigning the device to a different user NOTE: For security reasons, it is inadvisable to execute this command on lost or stolen devices.
Unlock AppConnect Container	Unlocks the AppConnect container (clears the AppConnect passcode)	The device user has forgotten the AppConnect passcode.
Device Encryption Status	Displays the encryption status of the device in the Device Details tab.	Dealing with lost and stolen devices.
Android Security Patch level	Displays the Android Security patch level of the device in the Device Details tab.	Enables an admin to verify that the deployed devices have the latest Android security patches.
Wipe	Removes content and settings to return the device to factory default settings.	Dealing with lost and stolen devices Preparing a device for a different user
Cancel Wipe	Attempts to cancel a wipe action for devices.	Reversing an inadvertent Wipe command. NOTE: Wipe cannot be reversed after it completes.
Block AppTunnels	This feature is not supported on Android devices.	
Lost	Flags a device as lost	Dealing with lost and stolen devices
Found	Flags a device as found	Dealing with lost and stolen devices
Locate	Reports the last known location for a device	Dealing with lost and stolen devices
Reset PIN	This feature is not supported on Android, iOS, or macOS devices.	

Lock

Locking a device forces the user to enter a password to access the device and prevents the user from reversing this restriction. The user is informed of this action via email. If the user has set a password for the device, then that password must be entered. Locking an Android device also causes the device user to be locked out of AppConnect apps. For details, see the MobileIron Core AppConnect and AppTunnel Guide.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Select **Lock** from the **Actions** menu.

NOTE: If the Mobile@Work app on the selected device is currently connected, then this action will be applied immediately. If the Mobile@Work app is not currently connected, then MobileIron Core attempts to complete the operation by means of the operator's SMTP service. If SMTP is used, it may take more time to execute the operation, and the time required may vary by operator.

Unlock

Unlocking the device passcode is supported as follows:

TABLE 15. SUPPORT FOR UNLOCKING THE DEVICE PASSCODE ON ANDROID DEVICES

Android device	Prior to Android 7.0	Android 7.0 through the most recently released version as supported by MobileIron
Android enterprise work managed devices	Supported	Supported
Android enterprise work profile devices	Not supported	Supported
Android (not using Android enterprise)	Supported	Not supported Unlock is not supported because these versions of Android do not allow a command to change the device passcode.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Click **Actions > Unlock**.

Unlock behavior on Android:

- The Unlock command causes Mobile@Work for Android to attempt to remove the existing passcode from an Android device. If the attempt is successful, the user will be able to access the device with the default Swipe.
- On some devices, the Mobile@Work attempt to remove the passcode on an Android device fails. When the attempt fails, Mobile@Work sets the passcode to "0000".
- If the Administrator forces a password reset Mobile@Work client itself will try to unlock the device if possible, or the user can unlock the device using the default password, 0000. The user is forced to change that password to one that conforms to password requirements defined in the Security policy. This applies to devices in Device Admin or Device Owner using an OS older than Android 7 through the most recently released version as supported by MobileIron or Profile Owner supporting Work Challenge using Android 6 through the most recently released version as supported by MobileIron. User of Android 6 device in Profile Owner without Work Challenge support may unlock with “0000” (the default) password as well, but is not forced to change the password.
- Android enterprise Work Managed mode-registered devices that are in kiosk mode move out of kiosk when you send the UNLOCK command from Core. This only happens when the password is mandatory as per the Security Policy on Core.
- For Android enterprise devices, see Unlocking an Android enterprise device.

Unlock AppConnect container

To unlock the AppConnect container (clear the AppConnect passcode):

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Select **Actions > Android Only > Unlock AppConnect Container**.

Encryption

The encryption status for a device is now reported on the device details tab.

To check the encryption status of a device:

1. Log into the Admin Portal.
2. Go to **Device & Users** > **Devices > Device Detail**.
   The device encryption status displays as Activating, Active, Active Per User, Active Default Key, Inactive, Unsupported, or None.

Android Security Patch level

The security patch level of an Android device is reported on the device details tab. This is available on Android devices using Android 6 through the most recently released version as supported by MobileIron.To check the security patch level of an Android device:

1. Go to **Device & Users** > **Devices.**
2. Select an Android device.
3. Use the drop-down menu to configure search rules to find the patch level.
4. In the first drop-down menu, select **Security Patch Level**.
5. Use the other fields to define your search.
6. Optionally, select the **Exclude retired devices from search** results check box.
7. Click **Search** or click **Save to Label**.
   If you click **Save to Label** and Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see Best practices: label management.
8. Go to **Device & Users** > **Devices** > **Device Detail**.
   The **Security Patch Level** displays in the **Device Details** tab.

Wipe

NOTE: This feature can also be used on SD cards, for most devices.

When wiping a device, MobileIron Core informs the user of this action via email.

WARNING: Wiping a device returns it to factory defaults, which can result in loss of data.

Required Role: The Device Management: Wipe device role is required to use this feature.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device to be wiped.
3. Click **Actions > Wipe**.
4. Optionally, select either or both of the following options:
   - **Preserve data plan (iOS 11 and later devices only)**. Select this option to retain the data plan on devices running iOS 11, if one exists.
   - **Skip Proximity Setup (iOS 11.3 and later devices only)**. Select this option to skip the proximity setup pane in the iOS Setup Assistant.
5. Click **Wipe**.

NOTE: If the Mobile@Work app on the selected device is currently connected, then this action will be applied immediately. However, if the Mobile@Work app is not currently connected, then MobileIron Core will attempt to complete the operation by means of the SMTP configuration.

Cancel Wipe

Cancel Wipe attempts to cancel a wipe command for one or more devices. The ability to cancel a device wipe action helps you avoid mistakes that can be difficult and costly to fix.

A device wipe action does not take effect until the device checks in with MobileIron Core. Using **Cancel Wipe**, you may be able to stop the wipe action.

Cancel Wipe is supported for Android devices with status: **Wipe pending.**

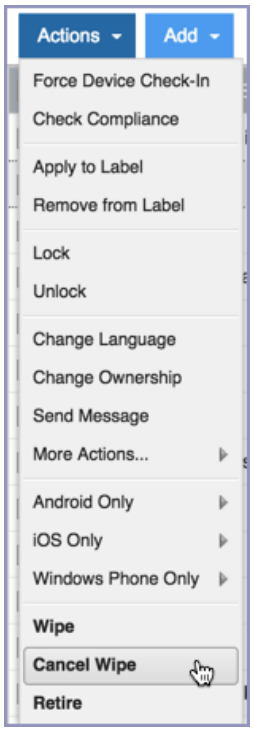
A successful **Cancel Wipe** action sets the device state to **Active**.

For Android devices, the device status must be **Active** or **Wipe pending** to use **Cancel Wipe**.

To cancel a device wipe action for Android devices:

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Check the status of the devices for which you need to cancel the device wipe.

   NOTE: For Android devices with status **Wiped**, you cannot cancel the device wipe action.
3. For Android devices with status **Wiped**, you cannot cancel the device wipe action.
4. Select devices with status **Wipe pending** that you do not want to wipe.
5. Click **Actions > Cancel Wipe**.



If the **Cancel Wipe** action is successful, the device state is set to **Active**, and the device can check in to MobileIron Core and receive updates.

If one or more of the selected devices changed from **Wipe Pending** to **Wiped** after you checked device status, a message displays indicating that these devices were wiped.

Selective Wipe

The Selective Wipe command is no longer supported, however, the functionality is available using the following methods:

- Selective wipe of email is accomplished through security compliance actions, removing the device from the associated label, or retiring the device.
- For Exchange through integration with selected devices and email apps.

Block AppTunnels

NOTE: This feature is not supported on Android devices.

Lost

When a user reports a lost device, you can set its status to **Lost**. Setting this status does not have a functional effect on the phone. It just flags the phone as lost for tracking purposes and to ensure that it appears in the Lost Phones screen.

Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Select **Actions > Lost** from the **Actions** menu.
4. In the displayed dialog, confirm the user and device information and enter a note.
5. Click **Lost**.
   The entry for this device will appear with a status of “Lost.” Use the Found action to undo this status. See Found on page 113

Found

If a user reports that a lost phone has been found, you can use the Found action to remove the Lost indicator from the entry for the phone. Setting this status does not have a functional effect on the phone.

Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Select **Actions > Found** from the **Actions** menu.
4. In the displayed dialog, confirm the user and device information and enter a note.
5. Click Found to return the entry for this device to **Active** status.

Locate

Android devices use both cell towers and GPS to locate the device. On Android 6.0 devices, Location Permissions must be granted to the app at runtime.

Most registered phones can be located on a map using cell tower IDs. When locating a device via cell tower IDs, Mobile@Work records tower data until the next time data is synchronized between Mobile@Work and MobileIron Core. See “Sync policies” in *Getting Started with MobileIron Core* for information on changing the Sync Interval setting. Using the Force Device Check-in in the Admin Portal or in Mobile@Work will result in immediate synchronization.

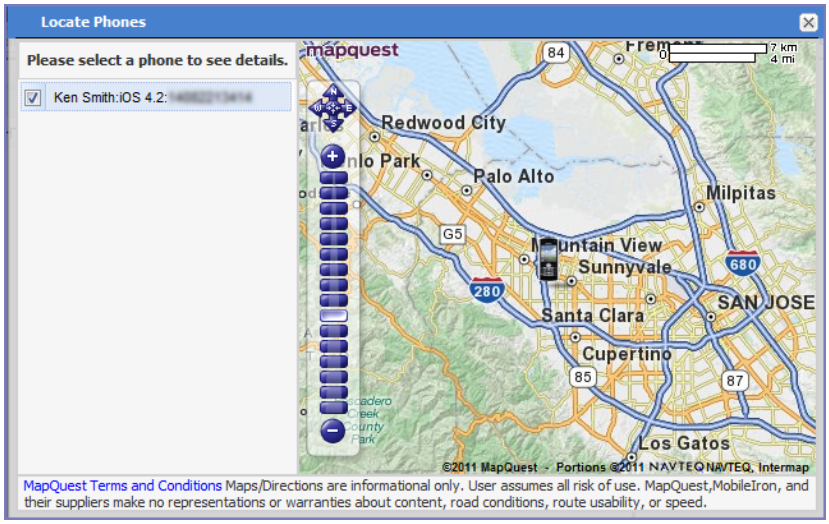
Required role

The **Privacy Control: Locate device** role is required to use this feature.

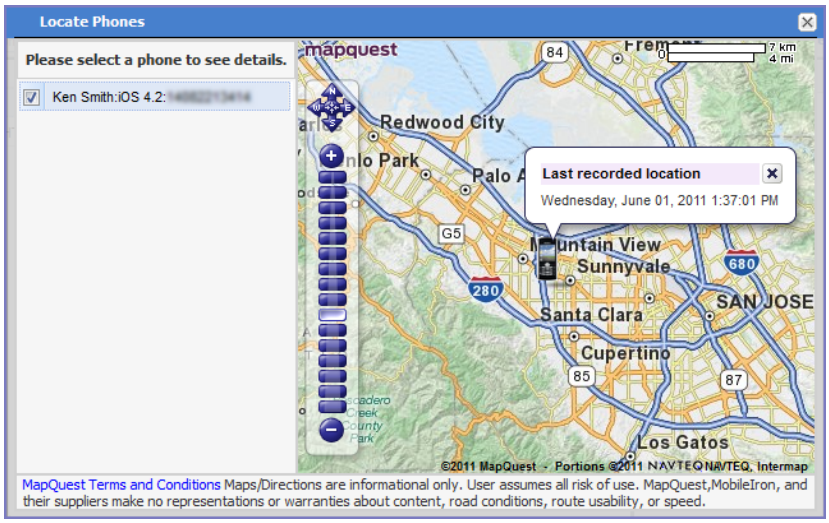
Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Click **Actions > Actions > Locate** to display the last known location of the phone.

   NOTE: To ensure that old and misleading location information is eliminated, location data expires after 72 hours.



4. Click the phone icon on the map to display the date on which the location information was collected.



Reset device PIN

NOTE: This feature is not supported on Android devices.

Force Device Check-In

You can use the **Force Device Check-in** feature to force the device to connect to the MobileIron Core. You might use this feature if Mobile@Work has not connected for some time, or you want to override a long sync interval to download updates.

You can use this feature to troubleshoot MobileIron operations.

NOTE: Both the **Force Device Check-in** option on the Admin Portal and the Mobile@Work for Android update the policies and settings related to AppConnect. The app check-in interval on the AppConnect global policy does not apply to Android devices.

Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Click **Actions > Force Device Check-in**.
4. The **Force Device Check-In** dialog appears.
   In the dialog, confirm the user and device information and enter a note.
5. Click **Force Device Check-in**.

Setting up background check-ins with APNs

This feature is not supported on Android devices.

Managed iBooks

This feature is not supported on Android devices.

Personal hotspot on/off switch

This feature is not supported on Android devices.

Using Custom APN with Samsung devices

Your device uses the APN or Access Point Name settings to set up a connection to the gateway between the carrier's network and the internet. You can configure a custom APN on Samsung devices in Work managed device mode (DO) and Managed device with work profile mode (COMP) for cellular data network access. Multiple APN's can be set up for each Samsung device, but only one configuration is allowed per APN.

To enter the custom setting for APN:

1. Go to **Policies & Configs** > **Configurations** > **Add New** >**Android** > **Samsung APN**.
2. In the New Samsung APN Setting dialog box, enter the values.
   Settings with fields marked in red are required.
3. Click **Save**.

Custom Configuration support for Zebra devices

You can deploy a custom configuration for your Zebra devices using XML configuration files from Zebra's StageNow software. The custom XML configuration file is uploaded to Core as a text file, and applied to a label. This XML configuration is then pushed to the Zebra device. To deploy the XML configuration file:

1. Go to **Policies & Configs > Configurations > Add New > Android > Android XML Configuration** to display the New Android XML Configuration page.
2. Enter the **Name** and **Description** of the configuration.
3. In the Configuration Type field, select **Zebra**.
4. Click **Browse** to navigate to and select the XML configuration file.
5. Read the warning and select the **I Agree** check box.
6. Click **Save**.

NOTE: XML configuration files is supported on Zebra 4.4 devices. For more information on Zebra devices and Stage Now software go to: https://www.zebra.com/us/en.html.

MobileIron Core supports Android remote control of Zebra devices with TeamViewer. For more information, see knowledge base article Support for Help@work on Zebra devices for Core.

Reporting on managed devices

MobileIron provides a Web Services API that enables you to create reports for many aspects of your managed devices. See the MobileIron API documentation for information. You can create reports in the following ways:

- Exporting records to CSV
- Using APIs for reporting
- For details, refer to the **Feature Usage** and **Get Last Sync Time and State of ActiveSync Devices** sections in the *MobileIron Core v2 API Guide.*

Exporting records to CSV

The enhanced Export to CSV feature provides access to numerous additional device attributes that were previously unavailable. The attributes are organized into platform-specific groups to make it easy to report on the relevant attributes for the devices you're working with.

Procedure

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Use the **Advanced Search** feature or select a label to filter the devices you are interested in. All of the devices in the table will appear in the exported file.
3. Click **Export to CSV** to open the **Export CSV Spreadsheet** dialog.
4. Select the information to export. The exported fields for each selection are listed below.
5. Click **Export**. to export the DeviceSearchResult.csv file is to your computer.

Export to CSV Field Options

Below describes what is contained inside a .CSV file.

TABLE 16. EXPORT TO CSV FIELD OPTIONS

Type	Supported Variables
Registration SMS (Phones)	REG_LINK
Registration Email	
Subject (Phones)	ENT_NAME, $USER$, $PHONE$
Subject (PDAs)	ENT_NAME, $USER$, $PHONE$
Body (Phones)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, $REG_LINK
Body (PDAs)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Reminder Subject (Phones)	ENT_NAME, $USER$, $PHONE$
Reminder Subject (PDAs)	ENT_NAME, $USER$, $PHONE$
Reminder Body (Phones)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Reminder Body (PDAs)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
$INAPP_REG_STEPS$	
Server	$SERVER_URL$
Username	$USER_ID$
Password	$PASSCODE$, $PASSCODE_TTL$
Post Registration Email	
Subject (Phones)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Subject (PDAs)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Body (Phones)	$BRAND_COMPANY_NAME$, $PHONE$
Body (PDAs)	$BRAND_COMPANY_NAME$, $PHONE$
Include Only Basic Device Information	User ID, Device UUID, Current Country Name, Current Operator Name, Current Phone Number, Device Owner, Display Name, Email Address, Home Country Name, Language, Last Check-In, Manufacturer, Model, Passcode, Passcode Expiration Time, Platform Name, Registration Date, Status

TABLE 16. EXPORT TO CSV FIELD OPTIONS(CONT.)

Type	Supported Variables
Include all device data, including the following options below.	(Select one or more options below)
User Attributes	User ID, Device UUID, account_disabled, Attribute Distinguished Name, custom1, custom2, custom3, custom4, Display Name, Email Address, First Name, Last Admin Portal Login Time, Last Name, LDAP Group Distinguished Name, LDAP User Distinguished Name, LDAP User Locale, locked_out, memberOf, Name, password_expired, Principal, sam_account_name, upn, User UUID NOTE: If defined in LDAP settings, custom attributes appear here also.
Common Device Attributes	User ID, Device UUID, APNS Capable, Background Status, Battery Level, Block Reason, Blocked, Cellular Technology, Client Build Date, Client Id, Client Last Check-in, Client Name, Client Version, Comment, Compliant, Creation Date, Current Country Code, Current Country Name, Current Operator Name, Current Phone Number, Device Admin Enabled, Device Encrypted, Device Is Compromised, Device Locale, Device Owner, Device Space, Display Size, EAS Last Sync Time, Ethernet MAC, Home Country Code, Home Country Name, Home Operator Name, Home Phone Number, IMEI, IMSI, IP Address, Language, Last Check-In, Manufacturer, MDM Managed, Memory Capacity, Memory Free, Model, Model Name, Modified Date, Non-compliance Reason, OS Version, Passcode, Passcode Expiration Time, Platform, Platform Name, Processor Architecture, Quarantined, Quarantined Reason, Registration Date, Registration IMSI, Registration UUID, Retired, Roaming, SD Card Encrypted, Security State, Serial Number, Status, Storage Capacity, Storage Free, Terms of Service Accepted, Terms of Service Accepted Date, Wi-Fi MAC
Android Attributes	User ID, Device UUID, Admin Activated, Android Client Version Code, Android enterprise Capable, Attestation, Brand, C2DM Token, Code Name, Device, Device Encryption Status, Device Roaming Flag, GCM/FCM Token Present, ICCID, Incremental, Kiosk Enabled, Manufacturer OS Version, MDM Enabled, Media Card Capacity, Media Card Free, Multi MDM, OS Build Number, OS Update Path, OS Update Status, Platform Flags, Registration Status, Samsung KNOX Version, Secure Apps Enabled, Secure Apps Encryption Enabled, Secure Apps Encryption Mode, Security Detail, Security Patch Level, Security Reason, USB Debugging

Managing Custom Attributes

This section addresses all components relating to custom attributes.

Assigning a custom attributes role

An administrator the assigned role of **Manage custom attributes**, can add, view, edit, search, or remove custom user or device attributes. Custom attributes is a role for the global admin space.

Procedure

1. Log into the Admin Portal.
2. Go to **Admin > Admins**.
3. Select an administrator to assign the custom attributes role.
   This role is for the Global admin space.
4. Select one of the following options for the selected administrator:
   - **Actions > Assign to Space > Global** if the global space has not been assigned
   - **Actions > Edit Roles** if the global space has been assigned
5. Scroll down to the **Settings and Services Management** section.
6. Click the **Manage custom attributes** option and click **Save**.

Adding custom attributes to users and/or devices

You can add up to 300 custom attributes for users and 300 custom attributes for devices.

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.
3. In the **Custom Device Attributes** section, click **Add+**.
4. Enter the information for the custom attribute for devices, including:

Field	Description
Attribute Name	Enter a name for the custom attribute.
Attribute Description	Enter a meaningful description for the custom attribute.
Value Type	Select one of three value types: boolean, integer or string. For information on Android Zero Touch custom attributes, see Zero Touch enrollment with custom attributes.
Variable Name	This field is read-only and displays the machine-generated name of the device that is used as a substitution variable in policies and configurations. For example, the substitution variable $USERNAME$ is replaced with the actual device username.
Actions	Click **Save**. The new custom device attribute is created and displays in the table.

5. (Optional) For Apple School Manager, click **Add+**and create a new Custom Device Attribute for device carts, for example, DeviceCartName, and choose the string value type. Remember this custom attribute name as you will need it when you turn on Apple Education in Core.
6. In the **Custom User Attributes** section, click **Add+**.
7. Referring to the table above, enter the information for the custom user attributes.
8. Click **Save**. The new custom user attribute is created and displays in the table.
9. (Optional) Repeat the steps, as needed.

Viewing custom attributes available for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.
3. View all available custom attributes for users and/or devices.
   Search for the attribute, if necessary, to see all available attributes.

Viewing custom attributes assigned to users

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Users**.
3. Locate a single user and expand the details.
4. Click the **Custom Attributes** tab.

Viewing custom attributes assigned to devices

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Devices**.
3. Locate a single device and expand the details.
4. Click the **Custom Attributes** tab.

Editing custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.
3. Locate the attribute you want to edit.
   Search for the attribute, if necessary.
4. Click in the **ATTRIBUTE DESCRIPTION** field and modify the description.
   This field has a 255 characters limit.
5. Click **Save**.

Searching for custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.
3. Enter the search criteria for the name or description.

Exporting a log of the custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Logs**.
3. Scroll down the list of filters to **Custom Attributes**.
4. Click the number link of the custom attributes to display the complete list in the details pane.
5. Click **Export to CSV** to export all records to a single file.

Deleting custom attributes from users and/or devices

You can delete an attribute if it has only been assigned to a user or a device. An attempt to delete a custom attribute assigned to a label will prompt an error message that provides a list of labels to which it has been assigned.

Procedure

1. Log into the Admin Portal.
2. Select **Settings > System Settings > Users & Devices > Custom Attributes**.
3. Locate the attribute you want to remove.
   Search for the attribute, if necessary.
4. Click **Delete**.

Setting custom attribute values for device or users

Setting custom attribute values for device or user requires **Edit custom device attribute values** and **Edit custom user attribute values** roles.

To set custom attributes for devices:

1. Log into Admin Portal.
2. Select **Devices & Users > Devices**.
3. Check the box next to one or more devices.
4. Click **Actions > Set Custom Attributes**.
5. Set the value for attributes and click **Save**.
   You can also clear the value for an attribute by checking the **Clear Value** box and save.

To set custom attributes for users:

1. Log into Admin Portal.
2. Go to **Devices & Users > Users**.
3. Check the box next to one or more users.
4. Click **Actions > Set Custom Attributes**.
5. Set the value for attributes and click **Save**.
   You can also clear the value for an attribute by checking the **Clear Value** box and save.

   NOTE: If you choose a single device or user when setting attribute values, the current attribute values are displayed. If you choose multiple devices or users, the current attribute values are not displayed.

Applying custom attributes to labels

Applying custom attributes to labels, requires **Label Management** permissions.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Labels**.
3. Click **Add Label > Filter**.
4. Locate the attribute using one of the following options:
   - Search for it in the **Field**, **Operator**, or **Value** fields.
   - Expand **Field** > **Custom Attributes > Device Attributes**.
   - Expand **Field** > **Custom Attributes > User Attributes**.

   For more information about field definitions, see Device field definitions.
5. Complete the criteria.
6. Click **Save**.

Pushing label attribute changes to devices and users

Changing attribute values for a user or device label does not trigger an automatic update. If you have changed the attribute values for a label, by default, changes will take effect:

- **For devices**: the next time the device checks in
- **For users**: the next scheduled LDAP sync

If you want the changes to go into effect immediately, take the following action:

- **For devices**: force a device check-in. See Force Device Check-In.
- **For users**: force an LDAP sync. See "Synchronizing with the LDAP server" in Getting Started with MobileIron Core.

Managing Policies

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

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

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

The topics in this chapter include the following advanced topics:

- Working with default policies
- Importing and exporting policies
- Viewing policy status and platform support
- Proactive password security policy
- Device log encryption on Android devices
- Sync policies and battery use
- Work Schedule policy
- Country changes and alerts
- Android devices and the Client Is Always Connected option
- Working with Samsung Android kiosk policies
- Working with Android Quick Setup policies
- Working with Samsung general policies
- Notifications of changes to the privacy policy
- Exporting the devices in the WatchList

Related topics

For information on MobileIron Threat Defense, including the MTD Local Actions policy, see the *MobileIron Threat Defense Solution Guide for Core.*

Working with default policies

Default policies are the policies applied to a device automatically when it is registered. Default policy values are also used as a starting point when you create a custom policy. MobileIron provides the values for each default policy specification. It is recommended that you create your own policies. You can use the settings in the default policies as a starting point. If you do edit a default policy's values (not recommended), those new values become the starting point when you create a new custom policy.

Unlike configurations, a device can have only one policy of each type.

MobileIron Core provides defaults for the following policy types:

- Security (Refer to *Getting Started with MobileIron Core* for details.)
- Privacy (Refer to *Getting Started with MobileIron Core* for details.)
- Lockdown (Refer to *Getting Started with MobileIron Core* for details.)
- Sync (Refer to *Getting Started with MobileIron Core* for details.)
- ActiveSync (See "Working with ActiveSync policies" in the .)
- AppConnect global policy (Refer to the *MobileIron Core AppConnect and AppTunnel Guide.)*

NOTE: You cannot delete default policies.

The default settings for each policy type are listed in the section for each type.

Setting an alert that a device's PIN change request was skipped

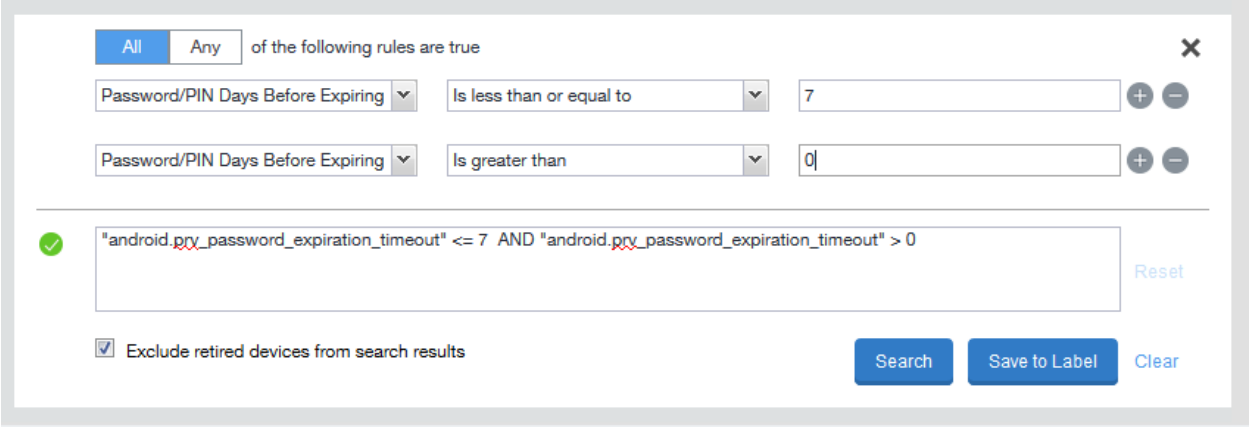
You can set an alert to have the device user change the password / PIN. You can also identify devices that have prompted the device user to change the password / PIN but the device user skipped the prompt.

Procedure

1. In your security policy, indicate the value in the Maximum Password Age field the number of days a password is valid for. See to*Getting Started with MobileIron Core*for details.
2. Create a compliance action with the desired number of days (1,2,3…up to 7) that the administrator wants to give as a grace period before taking a compliance action. For example, if the the administrator wants to have immediate effect, the value would be 7 (days.) If the administrator wants to give a grace period of 5 days, the value would be 2 (days.). See Adding custom attributes to users and/or devices.
3. Using Advanced searching, create a search that searches for devices that are less than 7 days (for example) of the device's password expiration date. Utilize the Android > Password/PIN Days Before Expiring field as part of your search criteria.

   NOTE: If the Maximum Password Age is 0, that means the PIN is set to never expire. When this happens, it means the Screenlock PIN Change Prompt – Showing value will always display as false and the Password/PIN Days Before Expiring displays as 0. Thus, the compliance policy cannot be a simple rule of just Password/PIN Days Before Expiring > Is

less than or equal to > 7. It needs to be Password/PIN Days Before Expiring > Is less than or equal to > 7 and Password/PIN Days Before Expiring > Is greater than > 0 (see below).



4. Click **Save to Label**.

   Apply the saved search to the appropriate labels (**Actions > Apply to Labels**).
5. To view the results, go to Device Details page and in the Details tab, view the values for the following fields:

- **Screenlock PIN Change Prompt - Showing** - Indicates if device user was prompted to change the device's screen lock password / PIN and the device user skipped the prompt. Values are:
  - Unknown - If coming from an older client device, value is unknown.
  - True - Indicates the PIN is to expire in 7 days or less.
  - False - (default) Indicates the device user is not being prompted to change the password / PIN (it has not reached its 7-day expiration window.)

  The value listed stays until the device user successfully changes the password /PIN on the device.
- **Password/PIN Days before expiring field** - represents the number of days before the password / PIN will expire. This numerical value is controlled by the Security policy's Maximum Password Age field value. This field is a dynamic field, its value decreases every day by 1 until the password / PIN is renewed. At renewal, the value returns to the original number stated in the Maximum Password Age field and starts a new daily count-down.

Importing and exporting policies

You can import and export policies from one deployment of MobileIron Core to another. Topics in this section include:

- Exporting policies or configurations
- Importing policies or configurations

NOTE: This feature is supported when importing or exporting policies or configurations between Core instances that are running the same version.

Exporting policies or configurations

Exporting policies and configurations help reduce errors when you have multiple instances of MobileIron. You can export a configuration .json file for an existing policy, modify it, then import it to another policy. The export/import features allow you to do this.

Procedure

1. Select **Policies & Configs** > **Policies** or **Policies & Configs** > **Configurations**.
   All available policies are listed in the policies table.
   All available configurations are listed in the configurations table.
2. Select a single policy or configuration to export.
   You can sort, as necessary, to find the one you want to export.
3. Click **Export** to create an export .json file.
   No application-related information is captured when exporting a policy or configuration.
4. Enter an export password and confirm it in the two password fields.
   This password encrypts sensitive configuration data during export (including passwords and certificates). The same password is required to import the exported data to another MobileIron Core server.
5. Check **Remember password for this session** if you want to re-use the password during a session.
   A session is defined as the length of a single login. The session ends when you log out or when you have been logged out by the system.
6. Locate the .json file, open, modify, and save it, as necessary.

   NOTE: Review this file before reusing it as values are not verified before importing them. For instance, If a security policy .json file has a minimum password length of 2000, the imported profile will have a minimum password length of 2000 and, when pushed to devices, it will enforce all the devices to have such a big password. The encrypted hash of the sensitive data is displayed in the .json file, but the sensitive data is not displayed in plain text format in the .json file.

Importing policies or configurations

Importing policies and configurations help reduce errors when you have multiple instances of MobileIron. You can export a configuration .json file for an existing policy, modify it, then import it to another policy. The export/import features allow you to do this.

Procedure

1. Select **Policies & Configs** > **Policies** or **Policies & Configs** > **Configurations**.
2. Click **Import** to locate a saved exported .json file.

3. Enter the name of the file or click **Browse** to locate it.
4. Enter the password created when the file was exported.
   See Step in Exporting policies or configurations on page 128.
5. Check **Remember password for this session** if you want to re-use the password during a session.
   A session is defined as the length of a single log-in. The session ends when you log out or when you have been logged out by the system.
6. Read the warning message and click the **I Agree** check box.
7. Click **Import** to add the new policy to the policy table.
   If you import a policy that already exists, you can override the policy or cancel the import. If an exported policy has child object/s (such as app control rules and compliance actions), MobileIron creates them during import. If the child objects already exist, they are overridden.

Viewing policy status and platform support

For any given device, you can view the status of a policy you have applied to that device, such as Pending, Sent, or Applied. For any given policy, you can view a list of supported platforms, such as Android, iOS, and Windows.

Topics in this section include:

- Displaying policy status
- Displaying supported platforms for policies

Displaying policy status

The Device Details pane on the **Device & Users > Devices** page displays status for the following tasks:

- apply lockdown policies
- apply security policies

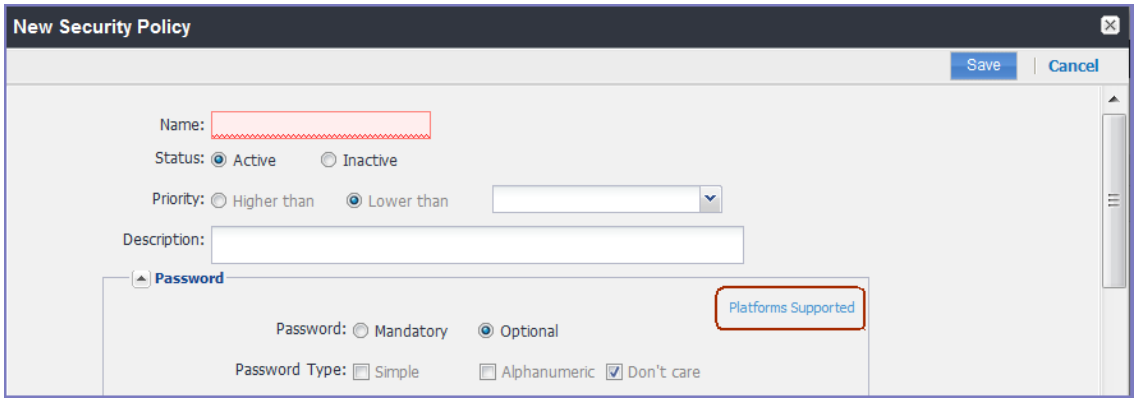
The categories of status you will see in the **Policies** tab are:

- **Pending**: The process of applying the policy has been started.
- **Sent**: The policy has been successfully sent to the device.
- **Applied**: MobileIron Core has confirmed that the verifiable settings appear to have been applied to the device. For Android devices, expand the **DETAILS** section of the Policies tab to see the verifiable results for Security and Lockdown policies.
- **Partially Applied**: One or more settings may have been rejected by the device. This can mean that the feature is not supported by the device. For Android devices, expand the **DETAILS** section of the Policies tab to see the verifiable results.

Displaying supported platforms for policies

To clarify which policies are supported on specific platforms, “Platforms Supported” links are included in the policy dialogs. For example:

FIGURE 5. PLATFORMS SUPPORTED LINK



Each link displays a table outlining the platform support for each policy feature.

Proactive password security policy

When certificates are applied to the device as certificate settings, certificate enrollment settings, or via a Wi-Fi configuration, Mobile@Work proactively applies a password policy that meets the Android OS certificate installation requirements.

With the proactive password policy, Mobile@Work prompts the user to create a screen lock for their device, even if MobileIron Core does not enforce a privacy policy.

Device log encryption on Android devices

Log files can be emailed by using the **Send Log** option in Mobile@Work for Android. You can choose whether the log files are encrypted when they are provided to the email app. The choice affects the log files of the following:

- Mobile@Work for Android
- Secure Apps Manager
- AppConnect-enabled apps (including what the app logs and what the AppConnect wrapper around the app logs)

The security policy for a device contains the option for choosing whether the emailed log files are encrypted. The default setting is to **not** encrypt the files.

By default, encrypted log files can be decrypted only by MobileIron Technical Support. If you want to encrypt the log files using your own certificate, see Encrypting device logs with your own certificate.

NOTE: Regardless of the device log encryption setting, the log files never include passwords, certificate content, license information, or other sensitive authentication data.

By encrypting the emailed log files, you improve security because the data is readable only by MobileIron Technical Support when using the default encryption, or by your own enterprise when using your certificate for encryption. Since emailing logs for troubleshooting is a common practice, you typically choose to encrypt the logs.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the security policy for the appropriate devices.
3. Click **Edit**.
4. In the **Data Encryption** section. for **Device Log Encryption**, select **On**.
5. Click **Save**.

Sync policies and battery use

If users note significant battery impact on their devices after installing the MobileIron client (Mobile@Work), consider reviewing and optimizing your sync policies.

Work Schedule policy

This policy allows administrators to set work schedules for device users. After the scheduled work time, users are blocked from accessing specified apps and services, which include:

- Exchange Active Sync services
- AppConnect-enabled apps
- Managed apps that use MobileIron Tunnel on Sentry

After the scheduled work time-period, users are unable to open any of these apps or services. In its place, users see a message indicating that access is not available. Message can vary, depending on the app or service they attempt to use. The policy starts and ends after the next scheduled sync following the specified start time and duration period.

This section contains the following procedures:

- Adding a Work Schedule policy
- Applying a Work Schedule policy

- Managing a Work Schedule policy
- Setting up Work Schedule policy notifications

Adding a Work Schedule policy

Use this procedure to add a policy that sets a work schedule and blocks apps and services outside of the scheduled time.

NOTE: Enforcement of this policy requires Standalone Sentry 9.0.0.

Procedure

1. Log into the Admin Portal.
2. Select **Policies & Configs > Policies > Add New > Work Schedule**.
3. Enter the policy name in the **Name** field.
4. Select **Active** to enable the schedule.
   Select **Inactive** to disable the policy.
5. Select **Higher than** or **Lower than** in the **Priority** option, then select the other priority.
   This option is available only if you have two or more Work Schedule policies. Use it to select the priority on one policy over the other in cases of conflicts.
6. Use the drop down to select a **Timezone**, which defines the start and end times for the policy.
7. Set up the weekly work schedule.
   The policy treats unchecked days as a time period outside of the work schedule, blocking affected apps and services for that 24-hour period.
8. Click **Save** to add the policy to the **Policies** page.

Applying a Work Schedule policy

Core sends the policy to Sentry and Sentry enforces the policy. When you apply the policy to a label, any device associated with the selected label will receive the policy during the next sync between the Sentry and the device.

Procedure

1. Log into the Admin Portal.
2. Select **Policies & Configs > Policies**.
3. Select the work schedule policy.
4. Select **Actions > Apply to Label**.
5. Select one or more labels and click **Apply**.

Managing a Work Schedule policy

Use this procedure to modify or delete a work schedule policy.

Procedure

1. Log into the Admin Portal.
2. Select **Policies & Configs > Policies**.
3. Select the work schedule policy you want to manage.
   a. Click **Edit** to modify the work schedule, then click **Save**.
   b. Select **Actions > Delete** to delete the policy.

Setting up Work Schedule policy notifications

Use this procedure to modify or delete a work schedule policy.

Procedure

1. Log into the Admin Portal.
2. Select **Logs > Event Settings**.
3. Select **Add New > Device Status Event**.
4. Complete the form and check **Work schedule policy applied**.
   See the "Working with Events" section for details.
5. Click **Save**.

Country changes and alerts

Country changes are monitored by the MobileIron client. Assuming that the **Sync While Roaming** option is not set to **No Sync**, each country change causes Mobile@Work to send the change to MobileIron Core. If Mobile@Work can connect, then the **Event Center** generates the configured alerts, regardless of the sync interval. If connectivity is not established, then Mobile@Work generates a local alert, if configured.

Android devices and the Client Is Always Connected option

Android devices support the Client is Always Connected option on the sync policy. Enable this option only when FCM (previously GCM) cannot be used. These situations include:

- Regions and countries in which FCM is not available.
- Select commercial and government use cases.
- Devices which do not support FCM, such as the Amazon Kindle.

NOTE: Google shut down GCM service on May 29, 2019. GCM is replaced by Firebase Cloud Messaging (FCM). MobileIron Core 8.0 and Mobile@Work for Android 10.2.1.0 through the latest version as supported by MobileIron now use FCM. See Customer Notice - GCM Batch End of life.

MobileIron Core uses FCM to immediately send lock, unlock, retire, and wipe, commands to devices. You can also send notification messages to devices using FCM. With **Always Connected** option enabled, Core can send these commands and notification messages to the device at any time without using FCM.

MobileIron recommends that you enable **Always Connected** mode on a maximum of 5000 devices per Core instance. The reason is that the device generates a regular connection status check to Core when using **Always Connected** mode. This status check can impact the device as follows:

- It will cause a small increase in battery power consumption on the device.
- It will cause a small increase in bandwidth usage on the device, which sometimes is a concern when using cellular networks.

Enabling SafetyNet attestation on Android devices

In the MobileIron Core Admin Portal, you can enable Google SafetyNet attestation on Android devices to verify the integrity of the devices' software and hardware. This action provides Core with the devices' SafetyNet attestation status. With this status, you can:

- Take actions on untrusted devices.
- Deliver policies, configurations, and apps to only trusted devices.
- Assess whether the Mobile@Work app running on a device is valid, or if it is a malicious app pretending to be Mobile@Work.

This feature attests, or verifies, various information about the device. Specifically, this feature:

- certifies the manufacturer and model of devices
- provides information about Mobile@Work
- certifies the device is intact and has not been tampered with
- verifies that the Google Play version installed on the device supports SafetyNet

SafetyNet attestation works with any Android deployment, including work profiles, managed devices, and managed devices with work profiles. It also works when the device is in device admin mode.

If SafetyNet is enabled on the security policy of the device, Core initiates a SafetyNet attestation check when:

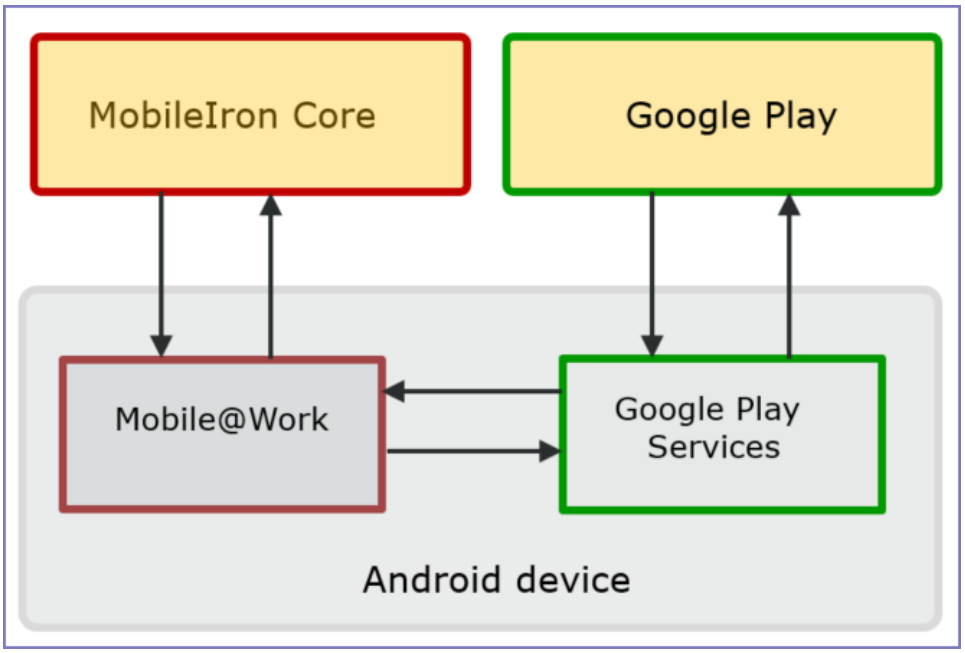
- the device has been rebooted or
- the last SafetyNet check was performed more than 24 hours ago.

NOTE: Safety attestation requires that the device is running Mobile@Work 10.1 for Android through the most recently released version as supported by MobileIron.

SafetyNet attestation flow

When MobileIron Core initiates a SafetyNet attestation check for a device, it sends a request to Mobile@Work. Mobile@Work requests Google Play Services to do the check, and Google Play Services communicates with Google Play. Google Play Services returns the results to Mobile@Work, which returns the results to Core. The following figure illustrates this flow.

FIGURE 6. SAFETYNET ATTESTATION FLOW



Setting SafetyNet attestation

To configure MobileIron Core to initiate SafetyNet attestation for devices, do the following.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Select a security policy and click **Edit**.
   Alternatively, create a new security policy by clicking **Add New > Security**.
4. Scroll down to the **Android** section.
5. Select "**Require Google SafetyNet Attestation**".
6. Click **Save**.

Related topics

"Security policies" in *Getting Started with MobileIron Core*

Basic integrity check and CTS profile verification

SafetyNet attestation provides two checks for the device:

- the basic integrity check
  Verifies that the device has not been tampered with.
- the Google Compatibility Test Suite (CTS) profile verification.
  Verifies that the device meets the requirements of a device that has passed Android compatibility testing.

SafetyNet attestation information in device details

In the Admin Portal, in the **Device Details** of a device at **Devices & Users > Devices**, you can view the following fields about SafetyNet attestation. You can also use these fields in Advanced Search, including creating labels.

TABLE 17. SAFETYNET ATTESTATION INFORMATION

Status on Device	Description
SafetyNet Enabled	Indicates whether the security policy applied to the device has SafetyNet enabled.
SafetyNet Exception	Indicates an exception occurred while running SafetyNet attestation on the device.
SafetyNet Timestamp	The date and time when Core last received a SafetyNet attestation response from the device.
SafetyNet Status	The results of the last SafetyNet attestation, described in the next table.

The following table explains the values of the SafetyNet Status field in a device's Device Details.

TABLE 18. SAFETYNET STATUS VALUES

Core Status	Description
Compatible	Core received a successful response, indicating a positive response to both the basic integrity test and the CTS profile verification.
Basic	Core received a successful response to the basic integrity check, but received a failed response to the CTS profile verification.
Fail	Core received a response, but received failed responses to basic integrity and CTS profile. This status indicates that a device is uncertified.
Unsupported	This status occurs when either: • Mobile@Work determines that SafetyNet attestation is not supported on the device. • The device is running a version of Mobile@Work for Android prior to Mobile@Work 10.1.

Core Status	Description
Unknown	Either Mobile@Work timed out waiting for results, or Core did not receive results in the acceptable time interval. Examples of legitimate reasons for an Unknown state are when a user is in airplane mode or has lost network connectivity. Therefore, be cautious about the actions you assign to devices that display this status.
Tampered Client	Core received a response that Mobile@Work is not valid, indicating the device has been tampered with.
Error	Either an exception occurred when calling SafetyNet or there was some other error.

Working with Windows Update policies

This feature is not supported on Android devices.

Working with Samsung Android kiosk policies

NOTE: Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.

NOTE: Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.

See Samsung Android kiosk policy on page 424 for information on configuring this policy.

Working with Android Quick Setup policies

The Android Quick Setup policy offers additional options for getting devices configured quickly:

- optional Device Administrator role for Mobile@Work
- cache registration password for Exchange and Wi-Fi configuration.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Click **Add New > Android > Android Quick Setup**.
3. Use the following guidelines to complete the form:

Action	Example
Name	Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type. **Tip:** Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.
Status	Select Active to turn on this policy. Select Inactive to turn off this policy. **Why:** Use the Status feature to turn a policy on or off across all phones affected by it. The policy definition is preserved in case you want to turn it on again.
Priority	Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select “Higher than” or “Lower than”, then select an existing policy from the drop-down list. For example, to give "Policy A" a higher priority than Policy B, you would select “Higher than” and “Policy B”. Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.

Action	Example
Description	Enter an explanation of the purpose of this policy.
Policy Parameters	Clear the **Device Administrator** option to complete registration without applying the Device Administrator role to the Mobile@Work app. Clearing this option streamlines the registration process by eliminating the need for the device user to approve granting the Device Administrator role. Clearing the option also disables the following features on the device: • Password requirements • Device encryption • Device lock/unlock • Wipe • Camera lock • Lockdown policies • Samsung Knox features • Samsung native email configuration • Samsung Knox container • Kiosk mode
Use registration password for	Select the Exchange and/or Wi-Fi check box to cache the registration password on the device for use in configuring the Exchange and/or Wi-Fi settings. Selecting these options streamlines the configuration process if you are using LDAP for authentication as part of the registration and Exchange/Wi-Fi configuration processes. Note that the password is cached in memory only. Terminating the app drops the password from memory.

4. Click **Save**.
5. Apply the policy to the appropriate labels (**Actions > Apply to Labels**).

Working with Samsung general policies

Use the Samsung general policy to manage Samsung Knox license keys on Samsung devices.

Upgrade Note: The Samsung Knox license key for Samsung Knox activation has been moved from the Samsung (Knox) Container policy (**Policies & Configs > Configurations**) to the Samsung General policy (**Policies & Configs > Policies**). If a license key is configured in the Container policy, then a new Samsung general policy is automatically created.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select **Add New > Android > Samsung General**.
3. Use the following guidelines to complete this form:

Item	Description
Name	Enter a unique name for the policy.
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.
Priority	Select Higher than or Lower than, then select an existing policy from the drop-down list. If you have multiple policies, use the Priority setting to select which policy gets applied. See “Prioritizing policies” in Getting Started with MobileIron Core.
Description	Enter a description for the policy.
Knox License Key	Enter the Samsung Knox license key **Important:** MobileIron Core does not validate the Knox license key. If the license key is invalid, AppConnect apps on the device cannot be used.
Knox Device Attestation Enabled	To enable attestation, first select the “I understand” check box, then select Knox Device Attestation Enabled. See also: Attestation support for Samsung Knox on page 140
Audit Collection Controls	Select Enable to enable event logging to the device logs on Samsung Knox devices. See Configuring audit collection controls for Samsung Knox devices.

4. Click **Save**.

Attestation support for Samsung Knox

In a BYOD environment, it is possible for employees to use rooted Android devices with customized firmware. An enterprise can validate a device’s integrity before it installs a Samsung Knox container on the device using the attestation feature.

The attestation feature requires Samsung Android devices that are attestation capable.

Attestation works by sending a challenge to the device to test its integrity. The device responds, and MobileIron Core returns its final verification. A device responds to the challenge in one of three ways:

- Correctly, resulting in attestation state of PASS
- Incorrectly, resulting in attestation state of FAIL
- No response, resulting in attestation state of UNKNOWN.

A device without attestation support does not respond. A device that supports attestation may also not respond, for example, if it has no network connectivity, or if it was compromised and sends no response.

An attestation challenge is sent to a device when the device checks-in with MobileIron Core, but not more frequently than once per hour. The attestation result determines whether a Samsung Knox container is removed, installed, or left unchanged. Additional compliance actions triggered by an attestation fail can be defined in a security policy.

NOTE: For all Samsung Android devices, whether or not they are attestation-capable, enabling attestation for the device removes a pre-existing Samsung Knox container from the device.

See Attestation behavior on the device for more details.

Configuring attestation on MobileIron Core

Before you begin

- You must have a Samsung Knox License Key to enable attestation.
- Samsung Android devices that support attestation are required to take advantage of this feature.

Recommendations

- For the best user experience, apply attestation to a new device deployment. If you enable attestation on a previously deployed device, any existing Samsung Knox container will be removed, and replaced only if the device passes the attestation challenge.
- MobileIron recommends enabling attestation in a homogeneous environment where all the devices are known to support attestation. For example, where all attestation-capable Samsung devices are corporate owned and assigned to an LDAP group.
- MobileIron strongly recommends against enabling attestation to groups of devices where attestation support is unknown or mixed.

Configuring attestation step-by-step

Follow these steps to enable attestation, create a related security policy with optional custom compliance actions, and assign the policy to devices.

Procedure

1. Create a label to use for attestation-related policies and devices:
   a. Go to **Device & Users > Labels.**
   b. Select **Add Label**. Name the label “Attestation Label”, for example.

2. Enable attestation in the Samsung General Policy:
   a. Go to **Policies & Configs > Policies**.
   b. Select **Add New > Android > Samsung General**. The **New Samsung General Policy** dialog appears.
   c. Enter the **Name**.
   d. Enter the **Knox License Key**.
   e. Read the **Caution** statement, and then select the “I understand” beneath it.
   f. Select **Knox Device Attestation Enabled**.
   g. Click **Save**.
3. Assign the Samsung General Policy to a label:
   a. Select the policy.
   b. Select **Actions > Apply to Label**.
   c. Select the desired label (for example, Attestation Label).
   d. Click **Apply**.
4. Optionally, create a custom compliance action to use in the attestation security policy:
   a. Go to **Policies & Configs > Compliance Actions**.
   b. Select **Add**.
   c. Select the actions to take if attestation fails.
   d. Click **Save**.
5. Create a security policy to define the consequences when attestation fails:
   a. Go to **Policies & Configs > Policies**.
   b. Select **Add New > Security.** The **New Security Policy** dialog appears.
   c. Enter a name. For example, “Attestation Security Policy”.
   d. Scroll down to **Access Control** and find the **For Android devices** section.
   e. Select the check box for “**when Samsung Knox device attestation fails**”.
   f. Choose the compliance action from the drop-down. If you created a custom compliance action for attestation, it appears as one of the options.
   g. Click **Save**.
6. Assign the Security Policy to a label:
   a. Select the policy.
   b. Select **Actions > Apply to Label**.
   c. Select the desired label (for example, Attestation Label).
   d. Click **Apply**.

7. Assign devices to the label with the attestation policies.
   a. Go to **Device & Users > Devices**.
   b. Select attestation-capable Samsung device(s).
   c. Select **Actions > Apply to Label**.
   d. Select the label with attestation policies (for example, Attestation Label).
   e. Click **Apply**.

WARNING: For all Android devices, Knox containers that were created before attestation is enabled are removed when the attestation policy is applied.

Attestation behavior on the device

A label that includes a Samsung Global Policy with the attestation feature enabled is applied to a device. MobileIron Core sends attestation challenges to the device periodically. The behavior of each device type is detailed below.

NOTE: Applying attestation to non-attestation capable devices is not recommended.

Android devices that are not attestation-capable

- Attestation state is reported as UNKNOWN in Device Details in the Admin Portal.
- Attestation state will always be UNKNOWN because the device is incapable of responding to an attestation challenge.
- Any existing Samsung Knox container is removed from the device.
- No new Samsung Knox container is installed.

Android devices that are attestation-capable

An attestation-capable device will respond to the attestation challenge. A challenge result can be PASS, FAIL, or UNKNOWN.

If the attestation result is PASS:

- Attestation state is reported as PASS in Device Details in the Admin Portal.
- For a new device deployment, a Samsung Knox container is installed.
- For an existing device which has a Knox container that was installed before attestation was enabled:
  - Pre-attestation Knox container is removed.
  - New Knox container is installed.
- For a device that previously passed, the Knox container remains unchanged.

If the attestation result is FAIL:

- Attestation state is reported as FAIL in Device Details in the Admin Portal.
- Samsung Knox container is removed.
- Additional compliance actions are taken based on the security policy in effect for the device, triggered by the “when Samsung Knox device attestation fails” condition.

If there is no response, the attestation result is UNKNOWN:

- Attestation state is reported as UNKNOWN in Device Details in MobileIron Core.
- If the device has previously passed attestation, it continues to function as if it has passed. The Knox container remains unchanged.
- If the device has not ever passed attestation, then:
  - Any pre-attestation Knox container is removed.

Configuring audit collection controls for Samsung Knox devices

The Samsung General Policy provides audit collection control settings. These settings control what audit events are logged to the device logs on Samsung Knox devices based on an event’s severity, outcome, and audit group. These settings impact logs collected on the Samsung device: logs made by the Samsung platform, as well as logs made by Mobile@Work.

You pull these device logs to MobileIron Core, and then can access them using the System Manager.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the Samsung General Policy that you are using.
3. Click **Edit**.
4. For **Audit Collection Controls**, select **Enable**.
5. For **Severity Rule**, select the severity level of events you want to collect. Only audit events of the chosen severity level or higher will be collected. For example, if you select **Error**, only **Error**, **Critical**, and **Alert** audit events will be collected. The severity levels are, from most severe to least severe, are:
   - Alert
   - Critical
   - Error (the default)
   - Warning
   - Notice
6. For **Outcome Rule**, select whether you want to collect only events indicating success, events indicating failure, or all.
7. For **Audit Groups**, select the groups of events you want to collect. Select one or more of **Security, System, Network, Events,** or **Application**. The default is that all of the groups are selected.

8. If you selected **Events** in the **Audit Groups** field, the **Audit Events** field is enabled. The possible individual events in the **Events** group are displayed in the **Audit Events** drop-down. Select the individual events that you want to collect.
9. In the **UID** section, click the + sign to add a UID. Each UID is an integer, defined by Samsung, for enabling Samsung-specific logging.
10. Click **Save**.

Related topics

Pull client logs for client devices

Working with Wear OS device policies

The Wear OS policy is used to send various Wear OS details to the server. If there isn't a policy in place or the watch app is not installed, then the Wear OS tab will not be displayed. If there is a policy and there are no watches paired to Mobile@Work, the Wear OS tab does not display. If there is a policy and the watch is paired (via Bluetooth) to the phone but the watch app is not installed on the watch, then Wear OS tab will not display. Once the policy has been implemented, the device continues to report watch details and inventory even when the device is quarantined.

NOTE: Mobile@Work for Android (phone) receives Wear OS data from the Wear OS device (watch) and the Android system tends to cache this data for an unknown time frame. There is a possibility that the true value of the "Wear OS Client Installed" field in Device Details > Wear OS tab is delayed for several hours.

Procedure

To create a new Wear OS policy:

1. Select **Policies & Configs > Policies**.
2. Click **Add New > Android > Wear OS policy**.
3. In the Add Wear OS Policy dialog box dialog box, use the guidelines to complete this form.
4. Click **Save**.
5. Apply the policy to a label.

TABLE 19. WEAR OS POLICY SETTINGS

Item	Description
Name	Enter a name for the Wear OS policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. You can have multiple active policies, and assign different labels to the various policies, but because only one policy is assigned to any given device, the highest-priority policy for a device is assigned.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the dropdown list. For example, to give Policy A higher priority than Policy B, you would select “Higher than” and “Policy B”.
Description	Enter an explanation of the purpose of this policy.
Collect Wear OS device details	• Enables (default) the collection of the device's Wear OS details to the server. • De-select to turn off the collection of Wear OS device details, including app inventory. NOTE: If the "Collect Wear OS device details" and "Collect Wear OS application inventory" fields are both selected, the collection of both device inventory and app inventory will occur.
Collect Wear OS application inventory	• Select to enable the collection of Wear OS application inventory. • De-select (default) to turn off the collection of Wear OS application inventory. Once this field is de-selected, old application inventory data will display in the Wear OS tab until the client explicitly sends a report to Core with no application inventory details or updated inventory details. NOTE: De-selecting this field will also de-select the "Collect Wear OS device details" field.

Related topics

Viewing paired watch information

Notifications of changes to the privacy policy

This feature is not available on Android devices.

Exporting the devices in the WatchList

The number in the **WatchList** field indicates the number of devices for which the configuration is still in queue.

To export the **WatchList**:

1. In the MobileIron Core Admin Portal, go to **Policies & Configs** > **Configurations**.
2. Click the number in the WatchList field for the configuration for which you want to export the WatchList. The Pending Devices window appears. The window displays a list of devices for which the configuration is queued.
3. Click Export to export the list of devices.
4. The list is downloaded as .CSV file.

Managing Compliance

MobileIron Core uses compliance policies to ensure that managed devices comply with security and administrator-defined compliance policies. Actions you define in policies, such as placing a device in quarantine, take effect when a device is non-compliant.

Refer to the following technical note for more information on compliance:

https://help.mobileiron.com/s/article-detail-page?Id=kA134000000QyFvCAK

The topics in this chapter include the following advanced topics:

- Managing device compliance checks
- Tiered compliance
- Compliance actions policy violations
- Viewing quarantine information
- Viewing configurations removed due to quarantine
- Custom compliance policies

Managing device compliance checks

Devices are checked for compliance with assigned policies each time they check in with MobileIron Core. In addition, Core checks all devices for compliance at regular intervals to detect out-of-compliance devices that have not checked in with Core.

Using MobileIron Core, you can:

- update device compliance status at any time
- set the timing for device compliance checks
- update the device last check-in and policy update time

NOTE: Core receives information regarding device compliance status and last check-in only after devices actually check-in with Core. While you can request a device check-in using the Admin Portal, many factors can affect whether a device actually checks in, such as network connectivity, or whether a device is switched on or off.

Setting the device compliance check interval

By default, all devices are checked for policy compliance every 24 hours. You can change the time between compliance checks. The Compliance Check Interval setting applies to compliance checks by the server only. Out of compliance conditions include:

- Device is out of contact for the time limit you set.
- Device's root detection logic has found an issue.
- Device Admin privileges have been lost.
- Device has been decrypted.
- Device OS version is below the expected version.

NOTE: It is best to run LDAP Sync and the compliance check at different times to avoid any potential Core performance problems.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Compliance Actions**.
2. Click **Preferences**.
3. In **Edit Compliance Preferences**, select one of the timings for **Compliance Check Interval** (2, 4, 8, 12 or 24 hours).

NOTE: Checking the compliance status of all devices every two or four hours may impact Core performance.

4. Click **Save**.

Updating device compliance status

You can manually request a device check-in to update device compliance status for one device, several devices, or all the devices registered to Core. Updating device compliance status enables:

- administrators to update the compliance status of any device without waiting for the scheduled compliance check to run
- users to return to productive work when a compliance check is resolved, rather than wait for the next scheduled compliance check
- administrators to update the following information about a device:
  - Last check-in, updated when the device checks in
  - Policy update time

Without the ability to update device status, the device in the following example could be locked for almost 24 hours after complying with the defined security policy:

- a device status is jailbreak when Monday's daily compliance check is done (the compliance check is set for 24 hours)

- the device is blocked when this status is detected, due to the defined security policy
- the device is brought back into compliance two hours after Monday's compliance check
- the user cannot use the device until the Tuesday daily compliance check is run 22 hours from the time the device is back in compliance

Procedure

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Select one or more devices to update.
3. Select **Actions > Check Compliance**.
4. A message is displayed, letting you know that the compliance check has begun.

NOTE: The compliance status of the chosen devices may not change for one to two minutes after selecting **Check Compliance**.

To update device compliance information for all devices:

1. In the Admin Portal, go to **Policies & Configs > Compliance Actions**.
2. Click **Check Compliance** to display a message asking if you want to update compliance status for all devices.
3. Click **Yes** to check compliance status for all devices or click **No** to cancel the action.

NOTE: The compliance status of the devices may not change for one to two minutes after selecting **Check Compliance**.

Compliance triggers and actions

Compliance actions, configured by the administrator, may be implemented locally on the device by Mobile@Work when certain system events have occurred that cause a compliance verification check, and only when the Enforce Compliance Actions Locally on Devices check box is selected for compliance action. Compliance verification checks also occur at the device check-in interval. Out of compliance conditions include:

- Out of Contact: the device has had no communication with the MobileIron Core server for greater than the time period selected which is specified in days.
- Compromised: the device is suspected to be rooted or an app has been installed for rooted devices.
- Device Admin lost: the device administration privileges have been revoked.
- Decrypted: it has been detected that the device is no longer encrypted
- OS Version: the version of the operating system on the device is below the expected version

Server compliance conditions and actions

Server compliance actions resulting from compliance conditions are listed in the table below.

TABLE 20. SERVER COMPLIANCE CONDITIONS AND ACTIONS

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
Wipe (Android only, when enabling Android custom ROM)	Wipe the device when it has been out of contact.	Wipe the device when the device has been compromised.	The device cannot be wiped when the administrator privileges have been removed.	Wipe the device when it has been detected that the device has been decrypted.	Wipe the device when the OS version is less than expected.
Alert • Android • iOS	Send an alert when the device is out of contact. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when the device has been compromised. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when administrator privileges have been removed. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when it has been detected that the device as been decrypted. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when the OS version is less than expected. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.
Remove Apps • Android • iOS Removal of apps is only possible if the MDM profile is sent by Core and is present on the device OR if the app settings have the "Remove app when device is quarantined of signed-out" check box selected.	Remove managed apps when the device is out of contact.	Remove managed apps when the device has been compromised.	Managed apps cannot be removed when administrator privileges have been removed.	Remove managed apps when the device has been decrypted.	Remove managed apps when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
Quarantine All • Android • iOS All Android enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Mobile@Work. (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	Remove all configurations when the device is out of contact.	Remove All configurations when the device has been compromised.	Remove All configurations when administrator privileges have been removed.	Remove All configurations when the device has been decrypted.	Remove All configurations when the OS version is less than expected.
Quarantine All Except Wi-Fi • Android • iOS • macOS (For Android enterprise apps, this is applicable only if the "Quarantine app when device is quarantined" check box is selected.)	Remove all configurations except for Wi-Fi.	Remove all configurations except for Wi-Fi when compromised.	Remove all configurations except for Wi-Fi when administrator privileges have been removed.	Remove all configurations except for Wi-Fi when the device has been decrypted.	Remove all configurations except for Wi-Fi when the OS version is less than expected.
Quarantine All Except Wi-Fi on Wi-Fi Only • Android • iOS • macOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	Remove all configurations except for Wi-Fi on Wi-Fi only devices.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when compromised.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when administrator privileges have been removed.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when the device has been decrypted.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
Block or retire AppConnect apps • iOS "Block" means blocking access to AppConnect apps.	not applicable	Block (unauthorized) or retire (unauthorize and wipe) AppConnect apps	not applicable	not applicable	not applicable

Local compliance conditions and actions

Local compliance actions do not apply to MobileIron Threat Defense functionality included with Mobile@Work clients. There are also no local compliance actions for Mobile@Work for macOS devices.

Local compliance enforcement actions resulting from compliance conditions are listed in the table below.

TABLE 21. LOCAL COMPLIANCE CONDITIONS AND ACTIONS

Situation	OS	Action
When the device can communicate with Core to perform a Compliance Check	**Alert** • Android • iOS	Send an alert when the device is out of contact. Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.
	Block AppConnect apps • Android • iOS	Blocks access to AppConnect apps.
	Quarantine • iOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations, managed apps and iBooks content are removed. New app downloads are disallowed.
	Quarantine • Android (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations and managed apps are removed. New app downloads are disallowed.
	Quarantine • Android Enterprise	All Android enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Mobile@Work.

Situation	OS	Action
When the device can NOT communicate with Core to perform a Compliance check	**Alert** • Android • iOS	Send an alert when the device is out of contact. Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.
	Block AppConnect apps • Android • iOS	Blocks access to AppConnect apps.
	Quarantine • iOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations, managed apps and iBooks content are removed. New app downloads are disallowed.
	Quarantine • Android (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations and managed apps are removed. New app downloads are disallowed.
	Quarantine • Android Enterprise	All Android enterprise apps and functionality are hidden, except Downloads, Google settings, Google Play Store, and Mobile@Work.
	Retire • Android Enterprise	The work profile is deleted or the managed device will be factory reset. NOTE: This action is not reversible.

Tiered compliance

Administrators can apply multiple compliance actions over time on violating devices using tiered compliance. The following example describes a possible 3-tiered compliance action:

1. Send device users a warning message that their device is out of compliance, and give them time to fix the violation.
2. If the device is violating the same policy 24 hours later, Core sends users a second message and blocks the device.

3. If the device continues to violate the same policy another 24 hours later, Core sends users a third message and quarantines the device.

The increasing penalties over time allow a user that is unintentionally violating a policy to get back under compliance before punitive measures are taken, rather than immediately pulling email configurations, for example, off the device and interrupting normal work flow.

NOTE: Tiers beyond the first one are only used by compliance policy rules, and are not used for security policies.

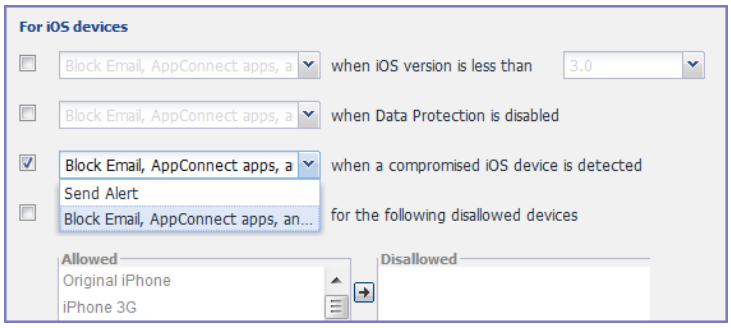
Tiered compliance behavior

- Tiered compliance checks do not run based on delay times. For example, if the delay time is 4 hours, Core does not automatically run a tiered compliance check after 4 hours. Instead, the next compliance check will occur in one of the following cases:
  - Device Check-in
  - Compliance check from the Devices page
  - Periodic compliance check (if the device has not checked in since the last periodic compliance check)
- If a device check-in or compliance check occurs during the interval between two tiers, Core will not take action based on the next tier. Core will only take action for the next tier after the delay time between tiers has elapsed.
- Delays between tiers are cumulative. For example, if the delay for tier 2 is 4 hours, and 8 hours for tier 3, then Core takes tier 3 action after 12 hours.

Compliance actions policy violations

You can assign compliance actions for security policy violations and for compliance policy violations. When you configure access control in either type of policy, you can select default compliance actions that are provided with MobileIron Core. You can also select custom compliance actions that you create.

FIGURE 7. COMPLIANCE ACTIONS POLICY VIOLATIONS



NOTE: To create the custom compliance actions, see Custom compliance actions.

Default compliance actions

The following table describes the default compliance actions:

TABLE 22. DEFAULT COMPLIANCE ACTIONS TABLE

Default compliance action	Description
Send Alert	Sends alert that you configured for the policy violation. To configure the alert, see Policy violations event settings on page 319.
Block Email, AppConnect Apps And Send Alert	• Sends alert that you configured for the policy violation. • Restricts access to email via ActiveSync if you are using a Standalone Sentry for email access. NOTE: If you manually block, allow, or wipe a device on the **ActiveSync Associations** page, blocking email access in a compliance action has no impact. The manual action overrides Core's automatic decision-making about access to email via ActiveSync. See "Overridding and re-establishing MobileIron Core management of a device" in the MobileIron Sentry Guide. • Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. • Unauthorizes AppConnect apps. AppConnect apps become unauthorized when the next device checkin occurs. When the device user tries to launch an AppConnect app, the Secure Apps Manager displays a small pop-up message with the reason the app is unauthorized. This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.
Customized compliance actions	These actions can contain 4 tiers of actions. Tiers 2-4 are only used in compliance policies; they are not used by legacy security policies. Security policies only perform the action defined in tier 1.

Custom compliance actions

You can customize the compliance actions that you want to take for the settings on the Compliance Actions page under Policies & Configs. After you create your customized compliance actions, the actions you created appear in a drop-down list in the **Access Control** section of your security policies.

Custom compliance actions enable you to specify combinations of the following actions:

- Send alert
- Block email access and AppConnect apps (includes blocking app tunnels)
- Quarantine: block email access, block app tunnels, block AppConnect apps, and wipe AppConnect app data

- Remove configurations (i.e., profiles)
- Specify exceptions for Wi-Fi-only devices

Once you create a set of these actions, you can select that set from the drop downs in the **Access Control** section of security policies.

Creating a compliance action

With custom compliance actions, you can create actions to better manage access control. With tiered compliance actions, you can customize them to include up to 4 levels of action to better manage compliance actions.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Compliance Actions**.
3. Click **Add+** to open the **Add Compliance Action** dialog box.
4. Select the appropriate fields as described in the Add Compliance Action table.

NOTE: If you have selected **Show** for the **Custom ROM Related Functions** in **Settings > System Settings > Android > Android Custom ROM**, then the wipe action is available. To enable wipe, first read and select the caution statement. You can then select **Wipe the device**. The wipe option applies to Android devices only.

5. If you want to add another set of actions, click the plus (+) button and select the fields, as necessary, to complete the second compliance action.
6. If you want to add another set of actions, click the plus (+) button and select the fields, as necessary, to complete the third compliance action.
7. Click **Save** to add the new compliance action for access control and compliance actions.
8. You can select them by going to:
   - **Policies & Configs > Policies >** policy > **Edit > Access Control** section (1 tier only).
   - **Policies & Configs > Compliance Policies > Add+ > Compliance Policy Rule > Compliance Actions** drop-down (1-4 tiers).

Add Compliance Action table

The following table describes the Add Compliance Actions options:

TABLE 23. ADD COMPLIANCE ACTION FIELDS

Item	Description
Name	Enter an identifier for this set of compliance actions. Consider specifying the resulting action so that the action will be apparent when you are editing a security policy.
Enforce Compliance	Select this to enable the Mobile@Work app to enforce compliance actions on

Item	Description
Actions Locally on Devices	the device for security violations without requiring action from Core. Core also continues to enforce compliance actions.
ALERT: Send a compliance notification or alert to the user	Select if you want to trigger a message indicating that the violation has occurred. Core sends alerts to users, administrators, or both. To configure the alert, see Policy violations event settings.
BLOCK ACCESS: Block email access and AppConnect apps	Selecting this option has the following impact to the device: • Restricts access to email via ActiveSync if you are using a Standalone Sentry for email access. NOTE: . • Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. This action blocks tunnels that AppConnect apps and iOS managed apps use. • Unauthorizes AppConnect apps. AppConnect apps become unauthorized when the next app checkin occurs. When launched, an AppConnect app displays a message and exits. Some iOS AppConnect apps that have portions that involve only unsecured functionality can allow the user to use only those portions. AppConnect apps become unauthorized when the next device check in occurs. When the device user tries to launch an AppConnect app, the Secure Apps Manager displays a small pop-up message with the reason the app is unauthorized. This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.
QUARANTINE: Quarantine the device (Select this check box to display the other Quarantine options.)	Selecting this option has the following impact to the device: • Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. This action blocks tunnels that AppConnect appsuse. • AppConnect apps are retired, which means they become unauthorized *and their secure data is deleted (wiped)*. AppConnect apps become unauthorized *and their data is wiped* when the next device checkin occurs. When the device user tries to launch an AppConnect app, the Secure Apps Manager displays a small pop-up message with the reason the app is unauthorized. This action impacts AppConnect apps, as well as third-party AppConnect for Android apps. • For Android enterprise devices, all Android enterprise apps and functionality are hidden, with these exceptions: Downloads, Google Play Store, and the Mobile@Work app. (Applicable only if the "Quarantine app when device is quarantined" check box is selected.) NOTE: In the App Catalog, the individual setting configured on each app takes precedence over this quarantined action. If the app

Item	Description
	config setting associated with the individual (specific) app is not selected to "Quarantine app when device is quarantined", then the app will be quarantined when the user device is quarantined.
QUARANTINE: Remove All Configurations and SaaS Sign-on Policy	Select to remove the following configurations: • Exchange • VPN • Wi-Fi • Docs@Work However, because of Android limitations, this action does not remove any certificates used in Certificate Enrollment, Certificate, and Wi-Fi configurations. These certificates are installed into the device's credential storage. Only the device user can remove them by using the Clear Credential Storage command in the Android Settings app on the device. Certificates used in Exchange and VPN configurations are removed because these certificates are stored in the respective apps. Also, certificates installed in a Samsung Knox device's credential store *are* removed.
QUARANTINE: Do not remove Wi-Fi settings for Wi-Fi only devices	Select if you want to retain the Wi-Fi configurations devices that do not have cellular access. Select this option to ensure that you can still contact these devices.
QUARANTINE: Do not remove Wi-Fi settings for all devices (iOS and Android only)	Select this option to retain the Wi-Fi configurations for any device, regardless of whether it has cellular access. You might select this option to preserve limited network access despite the policy violation.
QUARANTINE: Remove iBooks content, managed apps, and block new app downloads	Select this option to remove Managed Apps from the device and block access to Apps@Work when the device is not compliant. (Applicable only for Android enterprise apps and only if the "Quarantine app when device is quarantined" check box in the App Catalog is selected.)
Retire: Retire the Work profile or factory reset the managed device	Select to trigger a local retire action on an Android enterprise device. See the "Retiring an Android enterprise device" section in the Managing the Android enterprise device life cycle topic for the specific actions that are taken. This selection protects work profile data from data leakage by retiring the work profile on a personal device or performing a factory reset on a managed device. These actions are performed only locally on the device by Mobile@Work. Also, the Retire action is only visible when you select the **Enforce Compliance Actions Locally on Devices** check box and it is only available in tier 1. WARNING: This action cannot be reversed.

When the compliance action takes effect

When you first apply a security policy, several factors affect the amount of time required to communicate the changes to targeted devices:

- sync interval
- time the device last checked in
- battery level
- number of changes already queued
- whether **Enforce Compliance Actions Locally on Devices** is selected.

Once the change reaches the device, MobileIron Core checks the device for compliance. If the device is out of compliance, then the action is performed.

If the action for a security violation can be enforced locally on the device, and that option is selected in the Compliance Action dialog, then Mobile@Work initiates the compliance action without requiring contact with MobileIron Core.

Viewing quarantine information

Devices that have had configurations removed due to policy violations are considered quarantined. You can view quarantine information in the following places:

- **Device & Users > Devices** page
- **Policies & Configs > Configurations** page
- **Dashboard** page

Procedure

1. Go to **Device & Users > Devices**.
2. Click **Advanced Search**
3. Enter the search phrase: “common.quarantined” = true
4. Click **Search**.

To view information about an individual quarantined device:

1. Go to **Device & Users > Devices**.
2. Note devices that have been highlighted and appear with a quarantine icon.
3. Expand the device details for a quarantined device.
4. Click the **Configurations** tab in the device details panel to see which configurations have been removed due to quarantine.

Viewing configurations removed due to quarantine

You can view the configurations that MobileIron Core has removed due to quarantine on the Configurations page.

1. Go to **Policies & Configs > Configurations**.
2. Click a number link in the **Quarantined** column to display a list of devices that have had the configuration removed.

Dashboard page: Device by Compliance chart

To see how many devices are quarantined:

1. Go to **Dashboard**.
2. View the **Device by Compliance** chart. (If the chart is not visible, click **Add** to add it.)
3. To see a list of all quarantined devices, click the quarantined category.

Custom compliance policies

Core provides security policies for 10 static definitions to mark a device as non-compliant. These policies have limited customization options, but are a quick and easy way to begin to set up compliance policy rules. The Compliance Policies feature allows administrators to define their own criteria for marking devices non-compliant. They can combine dozens of device and user fields to create non-compliant matching criteria.

Compliance policy rules use the **Advanced Search** filter criteria to define non-compliant devices. Each compliance policy rule has a filter criteria and an associated compliance action object. Access compliance policies by selecting **Policies & Configs > Compliance Policies** from the Admin Portal.

Core uses custom device and user attributes to set up compliance policy rule conditions. These settings, listed under **Devices & Users > Devices > Advanced Search > User Fields > LDAP > User Account Control** in the Admin Portal, are:

- Account Disabled
- Locked Out
- Password Expired

Compliance policies are enforced by Core during device check-in.

The work flow to set up and use compliance policies is:

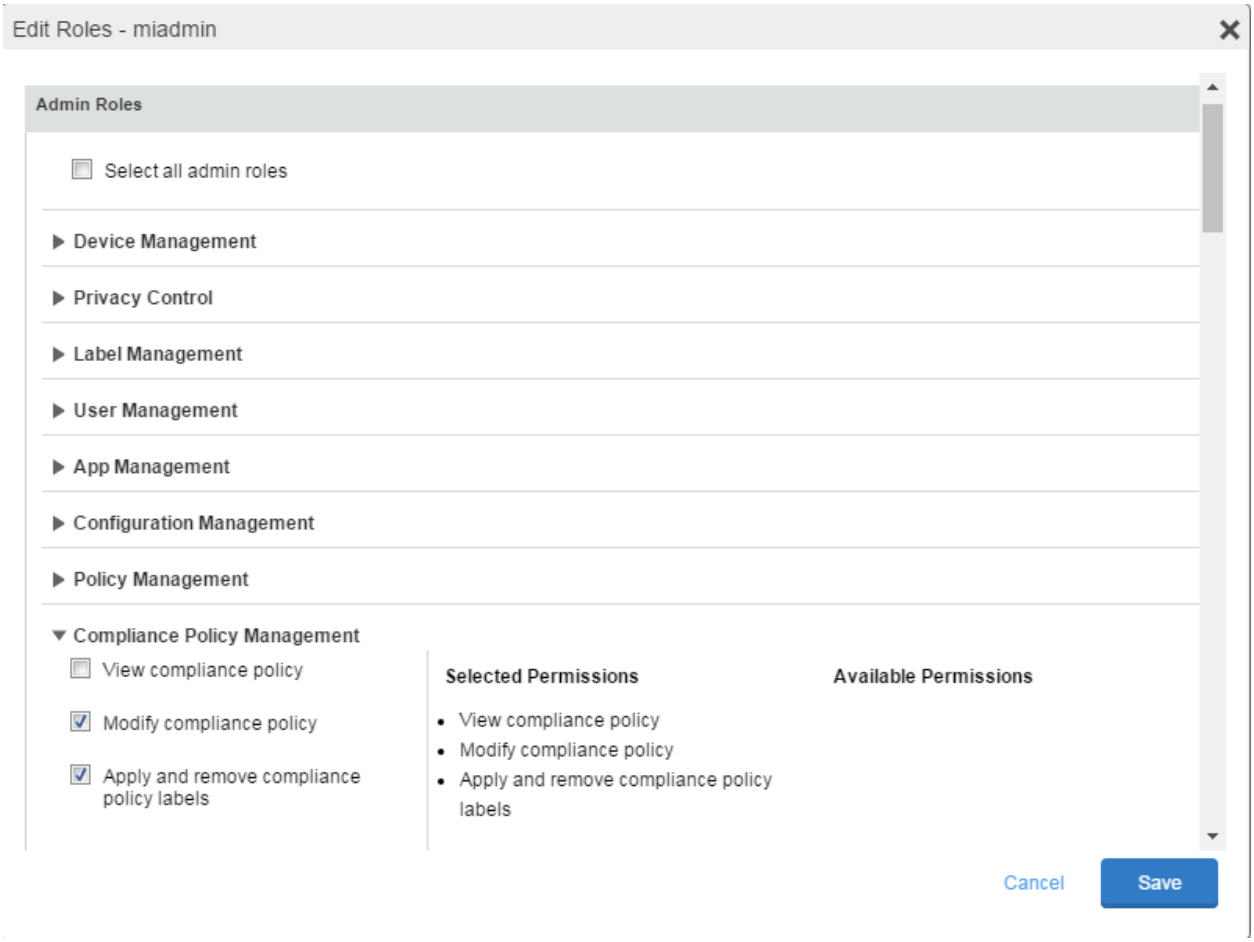
- Assigning compliance roles
- Managing compliance policy rules
- Managing compliance policy groups
- Device search fields for compliance rules

Assigning compliance roles

The following describes how to assign compliance roles.

Procedure

1. Log into the Admin Portal.
2. Go to **Admin > Admins**.
3. Select a user then click **Actions > Edit Roles**.
4. Select an Admin Space.
5. Scroll down the window to the **Compliance Policy Management** section.



6. Select one or more of the roles:
   - **View compliance policy**: Allows the selected user to view rules, groups, lists, and configuration.
   - **Modify compliance policy**: Allows the selected user to create, edit, and delete rules and groups.
   - **Apply and remove compliance policy labels**: Allows the selected user to add or remove groups from labels.
7. Scroll to the **Settings and Services Management** section.

8. Select **View settings and services**.
9. Click **Save**.

Managing compliance policy rules

Compliance policy rules are the building blocks in compliance policy groups used to manage device compliance. Administrators create compliance policy groups, add compliance policy rules to the groups, apply the groups to labels pushed to devices. Administrators can create a group with no rules or add compliance policy rules while creating the compliance policy group, if rules have already been created. They can also modify the group, including the name, description, and selected rules. This section describes:

- Creating compliance policy rules
- Substitution variables for compliance policy rules
- Viewing and modifying compliance policy rules
- Deleting compliance policy rules
- Searching for compliance policy rules

Creating compliance policy rules

A single rule can be in multiple compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies**.
3. Click **Compliance Policy Rule** tab and then click **Add+**.
4. Add a unique name in the **Rule Name** field.
5. Select the **Status** to **Enabled** or **Disable**.
6. Enter a description of the rule if desired.
7. Build a **Condition** using **Advance Search** to define non-compliance.

   NOTE: It is recommended to have one Condition set to include when Mobile@Work last checked in within the last 30 days. See the TIP below.

8. In the **Compliance Actions** field, select from the drop-down to use on devices matching the condition.
9. (Optional) In the **Message** field, enter text for alerts generated by violations of the policy rule.
   When configuring the message accompanying the compliance action, custom attributes (see Adding custom attributes to users and/or devices) and substitution variables can be inserted into the text. To do this, copy the appropriate variable (see the Substitution variable table) located to the right of the Message field and paste it into the text box. Before sending the message to the device, Core will replace the substitution variable to the actual value of the custom attribute for that device. For example, $FIRST_NAME$ would insert the first name of the target user into the message.

10. If you don't want the search results to include retired devices, select the **Exclude retired devices from search results** check box.
11. Click **Save**.

TIP: It is recommended to have a Compliance Policy Rule with one condition set to include when Mobile@Work last checked in with Core. This is helpful if you need assurance that Mobile@Work is running on devices (for example, for use in MobileIron Threat Defense).

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies**.
3. Click **Compliance Policy Rule** tab and then click **Add+**.
4. Enter *ClientLastCheckIn* in the **Rule Name** field.
5. Enter **Condition > All.**
6. Go to **Field** and type in "Client Last Check-In" or select **Common Fields > Client Last Check-In**.
   The regular expression is listed below; green check mark indicates regular expression is accepted.
7. Select **within the last** in the **Value** field; enter **30 days** in the remaining two fields.
8. Keep the default setting of **Exclude retired devices from search results**.
9. In the **Compliance Actions** field, select **Send Alert** from the drop-down.
10. Click **Save**.

Substitution variables for compliance policy rules

TABLE 24. SUBSTITUTION VARIABLES FOR COMPLIANCE POLICY RULES

Category	Substitution variable
Compliance policy rule customized message	The substitution variables are available for use in compliance policy rules for all devices. To use in a compliance action message, copy/paste the variable into the Message field. • CN • $CONFIG_UUID$ • $DEVICE_CLIENT_ID$ • $DEVICE_ID$ • $DEVICE_IMEI$ • $DEVICE_IMSI$ • $DEVICE_MAC$ • $DEVICE_PIVD_ACTIVATION_LINK$ • $DEVICE_SN$ • $DEVICE_UDID$ • $DEVICE_UUID$ • $DEVICE_UUID_NO_DASHES$ • $DISPLAY_NAME$ • $EMAIL$ • $EMAIL_DOMAIN$ • $EMAIL_LOCAL$ • $FIRST_NAME$ • $GOOGLE_AUTOGEN_PASSWORD$ • $ICCID$ • $LAST_NAME$ • $MI_APPSTORE_URL$ • $MODEL$ • $NULL$ • OU • $PASSWORD$ • $PHONE_NUMBER$ • $RANDOM_16$ • $RANDOM_32$ • $RANDOM_64$ • $REALM$ • $SAM_ACCOUNT_NAME$ • $TIMESTAMP_MS$ • $USERID$ • $USER_CUSTOM1$ • $USER_CUSTOM2$ • $USER_CUSTOM3$ • $USER_CUSTOM4$ • $USER_DN$ • $USER_LOCALE$ • $USER_UPN$

Viewing and modifying compliance policy rules

You can view or modify a compliance policy rule. Viewing a rule requires the View role and modifying a rule requires the Modify role.

You can modify a rule without removing it from an assigned group. For instance, you can change its status from Enabled to Disabled to troubleshoot it. When you modify a rule, the change is applied to all the groups that use the rule.

To view or modify a compliance policy rule:

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Rule**.
3. Select the name of the rule you want to modify and click **Edit**.
4. Modify details, as necessary, including disabling the rule.
5. Click **Save**.

Deleting compliance policy rules

To delete one or more compliance policy rules:

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Rule**.
3. Select the name of one or more rules to delete.
4. Click **Actions > Delete**.

Searching for compliance policy rules

To search for compliance policy rules:

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Rule**.
3. Enter a name in the search field.
4. Use one of the following filters:
   - All
   - Enabled
   - Disabled
5. Click **Search**.

Managing compliance policy groups

Compliance policy groups are applied to devices to manage device compliance. Administrators create compliance policy groups, add compliance policy rules to the groups, apply the group's rules to devices matching the label criteria.

Administrators can create a group with no rules or add compliance policy rules while creating the compliance policy group, if rules have already been created. They can also modify the group, including the name, description, and selected rules. This section describes:

- Creating compliance policy groups
- Modifying compliance policy groups
- Adding compliance policy rules to a group
- Applying compliance policy groups to labels
- Removing compliance policy groups from labels
- Deleting compliance policy groups
- Searching for compliance policy groups

Creating compliance policy groups

You can create a group without adding rules, which can be added later. One rule can be member of multiple groups.The following provides the steps to add one or more compliance policy rules to a compliance policy group.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies**.
3. Click **Compliance Policy Group** tab.
4. Click **Add+**. The Add Compliance Policy Group page displays.
5. Enter a unique name in the **Group Name** field.
6. Select Enabled in the **Status** field.
7. Move one or more rules from **Available Rules** to the **Selected Rules** list.
8. Click **Save**.

Modifying compliance policy groups

The following provides the steps to modify compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.

3. Select the name of the group you want to modify.
4. Modify details, as necessary, including the name, description, or to enable or disable the group.
5. Click **Save** in the **Details** section.
6. Click **Edit** in the Rules section.
7. Modify rules, as necessary, by adding or removing rules.
8. Click **Save** in the **Rules** section.

Adding compliance policy rules to a group

One rule can be a member of multiple groups. This procedure requires that you have already created one or more rule. See Creating compliance policy rules for details.

To apply a compliance policy rule to a compliance policy group:

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.
3. Double-click the name of the group to which you want to add one or more rules.
4. Go to the **Rules** section and click **Edit**.
5. Move one or more rules from the **Available Rules** list to the **Selected Rules** list.
6. Click **Save** in the **Rules** section.

Applying compliance policy groups to labels

Once a group (and its underlying rules) is assigned to devices, status of the devices are evaluated based on the conditions in the rules for compliance. Compliance Policy rules are evaluated against each device in the following ways:

- During device check-in
- Periodically, during the compliance policy check interval. This is set at **Policies & Configs > Compliance Actions > Preferences**.
- When a manual Check Compliance is initiated by the administrator. This can be set at **Policies & Configs > Compliance Actions > Check Compliance** or on the **Devices** page under **Actions**.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.
3. Select the name of the compliance policy group you want to apply to label.
4. Click **Actions > Apply to Labels**.
5. Select one or more of the labels.
6. Click **Apply**.

Removing compliance policy groups from labels

Once a group (and its underlying rules) is assigned to devices, status of the devices are evaluated based on the conditions in the rules for compliance. The following describes the steps to apply a compliance policy groups to one or more labels.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.
3. Select the name of the compliance policy group you want to remove from a label.
4. Click **Actions > Remove from Labels**.
5. De-select one or more of the labels.
6. Click **Apply**.
   After the next device check in, these changes will apply.

Deleting compliance policy groups

The following provides the steps to delete one or more compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.
3. Select the name of one or more groups to delete.
4. Click **Actions > Delete**.

Searching for compliance policy groups

The following provides the steps to search for compliance policy group.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies > Compliance Policy Group**.
3. Enter a name in the search field.
4. Use one of the following filters:
   - All
   - Enabled
   - Disabled
5. Click **Search**.

Device search fields for compliance rules

This section includes the compliance action objects the compliance policy rules use for device search fields. In addition to the fields listed in the below table, any Custom Device Attributes or Custom User Attributes that were added in **Settings > System Settings > Users & Devices > Custom Attributes** will also be available for searching.

The following table lists the available objects, including:

- Common fields
- Custom fields
- Android devices
- iOS devices
- Windows devices
- User fields (including LDAP fields)

TABLE 25. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES

Category	Compliance policy objects
Common	The following search fields are available for use in compliance rules for all devices: cellular_technology, client_name, client_build_date, client_version, creation_date, current_country_code, current_country_name, country_name, current_operator_name, carrier_short_name, current_phone_number, current_phone_number, data_protection_enabled, data_protection_reasons, device_admin_enabled, device_encrypted, device_is_compromised, eas_last_sync_time, ethernet_mac, home_country_code, home_country_name, home_operatory_name, home_phone_number, imei, imsi, language, last_connected _at, locale, location_last_captured_at, manufacturer, mdm_managed, mdm_tos_accepted, mdm_tos_accepted_date, model, model_name, os_version, owner, pending_device_passcode, pending_device_passcode_expiration_time, platform_name, platform, registration_date, registration_imsi, retired, roaming, security_state, status, uuid, wifi_mac_address
Android	The following search fields are available for use in compliance rules for all Android devices: admin_activated, attestation, afw_capable, brand, Client_version_code, device_roaming_flag, knox_version, manufacturer_os_version, mdm_enabled, multi-mdm, os_build_number, os_update_status, registration_status, samsung_dm, secure_apps_encryption_enabled, secure_apps_encryption_mode, security_detail, security_patch, usb_debugging, dpm_encryption_status
iOS	The following search fields are available for use in compliance rules for all iOS devices: BluetoothMAC, BuildVersion, CarrierSettingsVersion, Current MCC, Current MNC, DataRoamingEnabled, data_protection, forceEncryptedBackup, iCloud Backup Is Enabled, iOSBackgroundStatus, iPhone PRODUCT, iPhone VERSION,

TABLE 25. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES (CONT.)

Category	Compliance policy objects
	IsDeviceLocatorServiceEnabled, IsDEPEnrolledDevice, IsDoNotDisturbInEffect, IsMDMLostModeEnabled, IsMDMServiceEnrolledDevice, iTunesStoreAccountIsActive, ProductName, PasscodePresent, PasscodeIsCompliantWithProfiles, PasscodeIsCompliant, Personal Hotspot Enabled, SerialNumber, Supervised, SIM MCC, SIM MNC, Subscriber Carrier Network, Voice Roaming Enabled, osUpdateStatus,
Windows	The following search fields are available for use in compliance rules for all Windows devices: dm_client_version, wp_firmware_version, wp_hardware_version, wp_os_edition, health_data_issued, health_data_aik_present, health_data_dep_policy, health_data_bit_locker_status, health_data_boot_manager_rev_list_version, health_data_code_integrity_rev_list_version, health_data_secure_boot_enabled, health_data_boot_debugging_enabled, health_data_os_kernel_debugging_enabled, health_data_code_integrity_enabled, health_data_test_signing_enabled, health_data_safe_mode, health_data_win_pe, health_data_elam_driver_loaded, health_data_vsm_enabled, health_data_pcr0, health_data_sbcp_hash,
User	The following search fields are available for use in compliance rules user-related fields, including LDAP: email_address, user_id, attr_dn, dn, name, locale, principal, upn, account-disabled, locked_out, password_expired, custom1, custom2, custom3, custom4, <dynamically created custom user-attribute field name #1>, <dynamically created custom user-attribute field name #2>, <dynamically created custom user-attribute field name #3>, <dynamically created custom user-attribute field name #4>, <dynamically created user-attribute field names>

Managing Device Settings with Configurations

This section addresses the automation of major settings via configurations that can then be applied to a large inventory of different devices.

Management of device settings with configurations

Configuring major settings across a large inventory of different devices can mean a major daily time investment for IT personnel. You can automate this process by specifying and distributing configurations, previously called app settings. A configuration is a group of settings to be applied to devices.

The following table summarizes the device settings managed by MobileIron Core. Configurations are found on the **Policies & Configs > Configurations** page.

TABLE 26. DEVICE SETTINGS

Category	Configuration Type
Infrastructure	• Exchange • Email • Wi-Fi • VPN • Certificates • Certificate Enrollment
MobileIron AppConnect	• App Configuration

TABLE 26. DEVICE SETTINGS (CONT.)

Category	Configuration Type
	• Container Policy
MobileIron Features	• Docs@Work • Web@Work

Configurations page

A configuration (previously called app settings) is a group of settings that are applied to devices. Go to the **Policies & Configs > Configurations** page to create and manage configurations. It displays the following information for each configuration.

TABLE 27. CONFIGURATIONS PAGE OPTIONS

Field	Description
Name	Indicates a name for this group of settings.
Configuration Type	Indicates the kind of configuration.
Bundle/Package ID	If this configuration is links to a App Catalog entry, the Bundle/Package ID will display here.
Description	Displays additional information about this group of settings.
# Phones	Indicates the number of phones to which this group of settings has been applied. Click the link to display a list of the devices.
Labels	Lists the labels to which this group of settings has been applied.
WatchList	Displays the number of devices for which this group of settings is queued. Click the link to display a list of the devices.
Quarantined	Displays the number of devices that have had configurations removed due to policy violations. Click the link to display a list of the devices. See Creating a compliance action on page 157 for information on quarantining devices.

Required role: Administrator must have the **View configuration** role to access the Configurations page.

Default configurations

These configurations do not apply to Android devices.

Displaying configurations status

To see the status of configurations for each device:

1. Go to **Device & Users > Devices**
2. Select a device, and click the caret to open the device details
3. Click the **Configurations** tab.

The statuses you will see are:

- **Pending**: The process of applying the settings has been started.
- **Sent**: The settings have been successfully sent to the device.
- **Applied**: MobileIron Core has confirmed that the verifiable settings appear to have been applied to the device. Use the **View Details** button to see the verifiable results.
- **Partially Applied**: One or more settings may have been rejected by the device. This can mean that the feature is not supported by the device. Use the **View Details** button to see the verifiable results.
- **Update Pending**: The administrator has edited the setting in the Admin Portal. The process of applying the updated setting has begun.

Click the **View Details** button to see information on each configuration.

Adding new configurations

NOTE: Add new configurations through integration with selected devices and email apps plus MobileIron Sentry and ActiveSync.

To add new configurations:

1. Go to **Policies & Configs > Configurations**.
2. Click **Add New**.
3. Select the type of configuration you want to create.
4. Complete the displayed form for the configuration.
5. Click **Save**.
6. To push the configuration to devices, apply it to the appropriate labels. Select **Actions > Apply to Label**.

Editing configurations

NOTE: Add new configurations through integration with selected devices and email apps plus MobileIron Sentry and ActiveSync.

To edit configurations:

1. In the Configurations screen, select the configuration you want to edit.
2. Click **Edit**.
3. Make your changes.

4. Click **Save**.
   A pop-up displays.
5. Click **Yes** to continue.
   The configuration will be re-pushed to matching devices even you made no changes. However, if the only change made is to the description, the configuration will **not** be re-pushed to the devices.

Deleting configurations

NOTE: Add new configurations for Android devices through integration with selected devices and email apps plus MobileIron Sentry and ActiveSync.

To delete configurations:

1. In the Configurations screen, select the settings you want to delete.
2. Click **Delete**.

Exporting configurations

Export and importing setting configurations helps reduce errors when you have multiple instances of MobileIron. You can export a configuration .json file for an existing setting, modify it, then import it to another configuration.

To export a configuration:

1. Select **Policies & Configs** > **Configurations**.
   All available configurations are listed in the table.
2. Select a single configuration to export.
   You can sort, as necessary, to find the configuration you want to export.
3. Click **Export** to create an export configuration .json file.
   No application-related information is captured when exporting a configuration.
4. Locate the .json file, open, modify, and save it, as necessary.

   NOTE: Review this file before reusing it as values are not verified before importing them.

Importing configurations

To import a configuration:

1. Log into MobileIron Core.
2. Select **Policies & Configs** > **Configurations**.
3. Click **Import** to locate a saved exported configuration .json file.

4. Enter the name of the file or click **Browse** to locate it.
5. Read the warning message and click in the **I Agree** check box.
6. Click **Import** to add the new configuration to the configuration table.
   If you import a configuration that already exists, you can override the file or cancel the import.

Applying configurations to labels

Use labels to apply configurations to devices. Refer to the “Using labels to establish groups” section in the Getting Started with MobileIron Core for more information.

To apply a configuration to a label:

1. Select **Policies & Configs > Configurations** to display the configurations table with all available settings configurations.
2. Select the check box next to a configuration you want to apply to a label.
   Search for a configuration by entering the configuration name or description in the search box.
3. Click **Actions > Apply To Label**.
   Select the label.
4. You can search by label name or description to help find the label.
5. Click **Apply**.

Exporting the devices in the WatchList

The number in the **WatchList** field indicates the number of devices for which the configuration is still in queue.

To export the **WatchList**:

1. In the MobileIron Core Admin Portal, go to **Policies & Configs** > **Configurations**.
2. Click the number in the WatchList field for the configuration for which you want to export the WatchList.
   The Pending Devices window appears. The window displays a list of devices for which the configuration is queued.
3. Click Export to export the list of devices.
4. The list is downloaded as .CSV file.

Impact of changing LDAP server variables

A change to a LDAP server variable (such as $EMAIL$, $FIRST_NAME$, $LAST_NAME$, $DISPLAY_NAME$, $USER_UPN$, $USER_CUSTOM1, $USER_CUSTOM2, $USER_CUSTOM3$, or $USER_CUSTOM4$) now causes a setting that uses the variable to be re-pushed to the device. The impacted settings are:

- Exchange setting
- Email setting
- Wi-Fi setting
- VPN setting
- CalDAV setting
- CardDAV setting
- Subscribed calendar setting
- AppConnect app configuration
- Docs@Work setting

Configuring Email

This section addresses email account configuration, enabling S/MIME encryption and synchronizing account data.

Exchange settings

To specify the settings for the ActiveSync server that devices use, go to **Policies & Configs > Configurations**, then click **Add New > Exchange**. The ActiveSync server can be a Microsoft Exchange server, an IBM® Lotus® Notes Traveler server, Microsoft Office 365, or another server.

The Exchange configuration works:

- Through MobileIron Sentry and ActiveSync
- With Samsung Knox devices running the Samsung native email app and the Android versions listed in the Mobile@Work for Android Release Notes.

Note that AppConnect-enabled Email+ for iOS and Email+ for Android do not use an Exchange setting. Instead, you configure the email clients using an AppConnect app configuration.

Android enterprise email clients are configured using AppConnect app configurations. See Setting up Gmail with Android enterprise.

The following table describes the Exchange settings you can specify.

TABLE 28. EXCHANGE SETTINGS

Section	Field Name	Description
General	Name	Enter brief text that identifies this group of Exchange settings.
	Description	Enter additional text that clarifies the purpose of this group of Exchange settings.
	Server Address	Enter the address of the ActiveSync server.

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		If you are using Standalone Sentry, do the following: • Enter the Standalone Sentry's address. • If you are using Lotus Domino server 8.5.3.1 Upgrade Pack 1 for your ActiveSync server, set the server address to <**Standalone Sentry's fully qualified domain name**>/traveler. • If you are using a Lotus Domino server earlier than 8.5.3.1 Upgrade Pack 1, set the address to <**Standalone Sentry fully qualified domain name**>/servlet/traveler. • If you are using load balancers, contact MobileIron Professional Services. When using Integrated Sentry, set the server address to Microsoft Exchange Server's address. NOTE: When using Sentry, you can do preliminary verification of your Exchange configuration choices for the ActiveSync User Name, ActiveSync User Email, and ActiveSync Password fields. To do so, first set the server address to the ActiveSync server. After you have verified that users can access their email using this Exchange configuration, change the server address to the appropriate Sentry address. For more information about configuring Sentry, see the MobileIron Sentry Guide.
	Use SSL	Select to use secure connections. SSL is always used, regardless of whether this setting is selected.
	Use alternate device handling	Replaces the **Use Standalone Sentry** option. Use this option only under the direction of MobileIron Support.
	Domain	Specify the domain configured for the server.
	Google Apps Password	This check box only appears if you have configured a Google account with MobileIron Core, as described in Exchange settings on page 178. When linking to Google Apps, select this option to use

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		the Google Apps password to log in to the Google account you have configured to work with MobileIron Core. This password allows device users to access their mail, contacts, and calendar data on their managed devices. When selected, Core grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with MobileIron Core, as described in Synchronizing Google account data on page 185.
	ActiveSync User Name	Specify the variable for the user name to be used with this Exchange configuration. You can specify any or all of the following variables $EMAIL$, $USERID$, $PASSWORD$. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $USERID$ if your ActiveSync server is a Microsoft Exchange Server, and you use $EMAIL$ if your ActiveSync server is an IBM Lotus Notes Traveler server.
	ActiveSync User Email	Specify the variable for the email address to be used with this Exchange configuration. You can specify any or all of the following variables $USERID$, $EMAIL$,$SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $EMAIL$ in this field.
	ActiveSync User Password	Specify the variable for the password to be used with this Exchange configuration. You can specify any or all of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported.

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		Enter additional variables or text in the text box adjacent to the **Password** field. Entries in this text box are kept hidden and will not be visible to any MobileIron Core administrator. NOTE: All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. Valid variables are variables in the drop-down list.
	Identity Certificate	Select the Certificate Enrollment entry you created for supporting Exchange ActiveSync, if you are implementing certificate-based authentication. NOTE: When setting up email for devices with multi-user sign-in, the exchange profile must always use a user-based certificate. The user-based certificate will ensure secure access to email for all users. Using a device-based certificate can result in one user sending or receiving emails for another user. When configuring the user-based certificate, select the **Proxy enabled** and **Store certificate keys on MobileIron Core** options. This allows the user certificate and private key to be delivered each time they log in on the shared device.
	Password is also required	Specify whether to prompt device users for a password when certificate authentication is implemented. The password prompt is turned off by default. Once you specify an Identify Certificate, this option is enabled. Select the option if you want to retain the password prompt.
	Items to Synchronize	This feature is not supported.
	Past Days of Email to Sync	Specify the maximum amount of email to synchronize each time by selecting an option from the drop-down list. This setting works only with these email apps:

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		• Samsung Knox devices' native email app • Email+
	Move/Forward Messages to Other Email Accounts	This feature is not supported for Android devices.
S/MIME	Enable for Android and iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on devices running Android or iOS 9.3.3 or earlier.
S/MIME Signing		
	S/MIME Signing: Enable	This feature is not supported for Android devices.
	S/MIME Signing identity	This feature is not supported for Android devices.
	Signing Identity: User Overrideable	This feature is not supported for Android devices.
	S/MIME Signing: User Overrideable	This feature is not supported for Android devices.
S/MIME Encryption		
	Encryption by Default	This feature is not supported for Android devices.
	Encryption Identity	This feature is not supported for Android devices.
	Encryption Identity: User Overrideable	This feature is not supported for Android devices.
	Encryption by Default: User Overrideable	This feature is not supported for Android devices.
	Per-Message Encryption Switch	This feature is not supported for Android devices.
ActiveSync		Limited support for Android.
	Sync during	
	Peak Time	Select the preferred synchronization approach for peak times.This feature is not supported for Android devices.
	Off-peak Time	Select the preferred synchronization approach for off-peak times.This feature is not supported for Android devices.

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Use above settings when roaming	Specify whether to apply synchronization preferences while roaming.
	Send/receive when send	Specify whether queued messages should be sent and received whenever the user sends a message.
	Peak Time	
	Peak Days	Specify which days should be considered peak days.
	Start Time	Specify the beginning of the peak period for all peak days.
	End Time	Specify the end of the peak period for all peak days.
iOS 5 and Later Settings		These features are not supported for Android devices.
Android		
	Exchange App Priority	Drag and drop email configurations to specify which are allowed. Change the order of selected configurations to specify priority. If there are no email apps specified in the **Selected** column, then Mobile@Work uses the following provisioning priority: 1. Android Email+ (AppConnect-enabled) 2. Android Email+ 3. Native email app
General		
	Accept all SSL certificates: Enable	Enables device users to set Android devices to accept all SSL certificates. This setting applies to Android Email+ and Samsung Knox email and is intended for use when the MobileIron Sentry uses self-signed certificates. NOTE: Use caution when enabling this setting, as device users might unknowingly expose the device to attack.

TABLE 28. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Copy/Paste: Enable	Prevents use of the copy and paste commands in Android Email+.
	Allow access to secure info from outside container	Specify whether to publish contacts and calendar items to non-secure email clients running on the same device. For Secure Android Email+, you can allow access to both contacts and calendar.
	NitroDesk TouchDown	Enter the license key.
Samsung SAFE (Knox)	Supported on all Samsung Knox devices	
	HTML Email : Allow	Select this option to allow viewing of HTML email. This option is not enabled by default, which prevents rendering of HTML-based email.
	SmartCard Authentication: Enable	This feature is not supported.
	Windows 10 Desktop	This feature is not supported for Android devices.

Multiple Exchange Support for Android

Multiple Exchange mailboxes are supported for devices running Android versions no earlier than 4.0 or Samsung Knox 4.0 devices, using either Android Email+ or Samsung Native Email client apps. For Samsung Native Email client, Certificate Enrollment is not supported as the authentication method with multiple mailboxes.

The MobileIron Core administrator can configure and apply up to two Exchange settings for each device. Exchange settings are found in the Admin Portal under **Policies & Configs > Configurations**. When it receives the configuration, the device must be running Mobile@Work version 6.0 through the most recently released version as supported by MobileIron.

On the device, both mailboxes appear in a single email app. The email app is determined by 1) the email app's priority as specified in the Exchange Setting's **Exchange App Priority,** and 2) the email app's availability on the device. For example, if both Samsung Native Email and Email+ are available on the device, the app with the highest priority is used.

NOTE: Mobile@Work's **Options > Email Status** is not supported for multiple Exchange accounts.

Configuring POP and IMAP email settings (for iOS and macOS)

This feature is not supported for Android devices.

Synchronizing Google account data

You can synchronize email, contacts, calendar, and tasks with mail apps on devices managed by MobileIron Core. To enable synchronization, you need to authorize apps to use Google APIs for communication between servers without accessing user information. This requires a service account that makes API calls on behalf of an app, as well as credentials that authenticate the identity of the app.

You create these credentials in the Google Developers Console, and then upload the credentials both to the Google Admin Console and MobileIron Core. You can then configure an Exchange setting to synchronize Google email data (including email, contacts, calendar, and tasks) with managed devices. You can alternatively choose to synchronize only some email data, such as calendar and contacts only, or email alone.

The Exchange setting also allows you to control the Google Apps password through MobileIron Core.

Main steps

Synchronizing Google Apps data involves the following main steps:

- Using OAuth to enable access to Google APIs
- Uploading OAuth credentials to the Google Admin Console
- Linking Google Apps credentials with MobileIron Core
- Setting up your Exchange setting for access to Google Apps data
- Renewing the Google Apps password for a given set of users (optional)

Before you begin

You need a Google administrator account.

Review the following Google documentation:

- https://developers.google.com/admin-sdk/?hl=en_US
- https://support.google.com/googleapi/answer/6158857?hl=en
- https://support.google.com/googleapi/answer/6158849?hl=en#serviceaccounts

Using OAuth to enable access to Google APIs

You must login to the Google Developers Console to enable access to Google APIs from clients using OAuth.

For detailed information, see the Google documentation here:

- https://developers.google.com/identity/protocols/OAuth2
- https://developers.google.com/identity/protocols/OAuth2ServiceAccount

Following are the main steps of this procedure.

Main steps

1. Login to https://console.developers.google.com
2. In the Google Developers Console, create a new project.
3. Enable the Admin SDK and/or APIs.
4. Create credentials for the OAuth 2.0 client.
5. Create a consent form.
6. Enter the relevant information, as shown in the following table.

Item	Description
Application type	Select web application.
Name	Enter the name of the iOS app.
Authorized JavaScript origins	Enter JavaScript origins here or redirect URIs below (or both). Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).
Authorized redirect URIs	Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

7. Download the credentials in the form of a JSON file for the web client.

Uploading OAuth credentials to the Google Admin Console

You must now upload to the Google Admin Console the JSON file you created in Using OAuth to enable access to Google APIs on page 185. The JSON files contains the credentials you created for client access.

For detailed information, see the Google documentation here:

- https://developers.google.com/identity/protocols/OAuth2
- https://developers.google.com/identity/protocols/OAuth2ServiceAccount

Following are the main steps of this procedure.

Main steps

1. Go to https://admin.google.com and login with your administrator ID.
2. Enable API access.

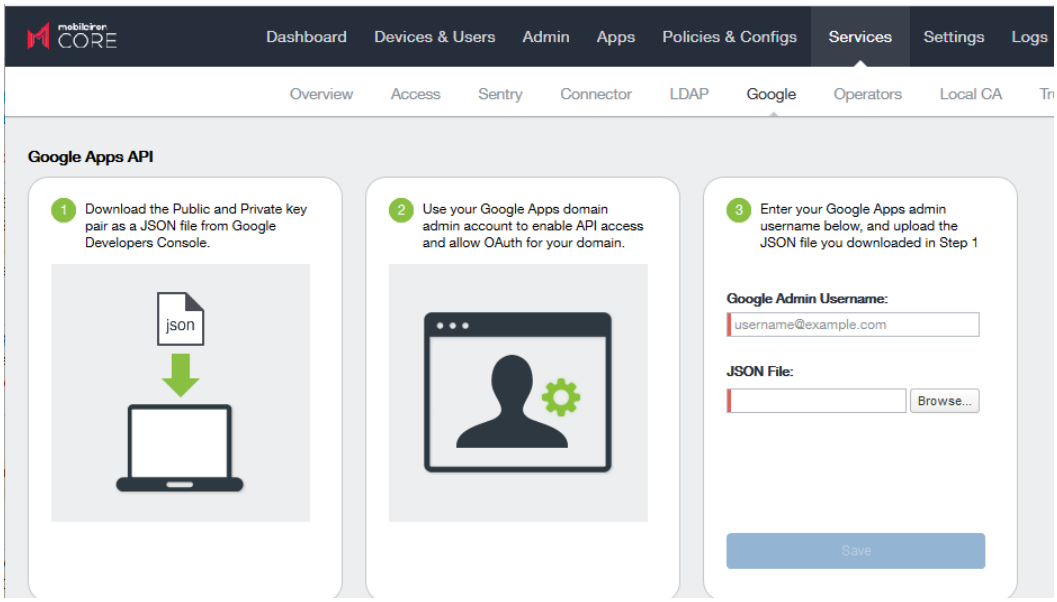
3. Enter the client name and API scope.
4. Authorize the JSON file so that clients may access it.

Linking Google Apps credentials with MobileIron Core

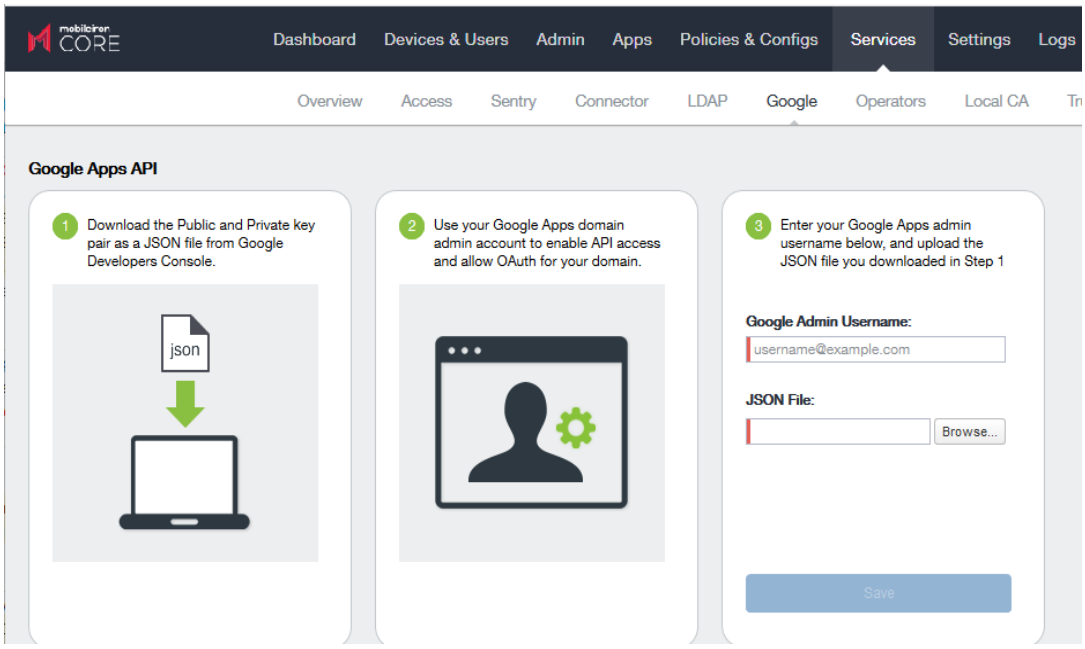
You must upload the JSON credentials file you downloaded from the Google Developers console to link your Google credentials with MobileIron Core. For more information, see Using OAuth to enable access to Google APIs on page 185.

Procedure

1. In the Admin Portal, go to **Services > Google**.
2. In the **Google Admin Username** field, enter your Google administrator email address.
3. Next to the **JSON File** field, click **Browse**.



4. Select the JSON file you downloaded from the Google Developers Console.
5. Click **Save**.
   The results are displayed on the lower left.



6. Go to **Settings > Preferences**.
7. Scroll down to the **Google Apps API** section.
8. Click **Password Settings**.
9. Configure password settings as follows:
   - Password length must be: Enter the minimum password length.
   - Require a password change every: Check the box and enter the number of days after which device users must change their password.

     NOTE: Password expiration and password length values should match whatever is configured in Google. For example, if you configured a 90 day expiration period in Google with a password length of 8 to 90, then you would configure the same expiration and password length values in MobileIron Core.
10. Click **Save**.
11. Optionally, view the Google Apps account status by clicking **View Account**.

Setting up your Exchange setting for access to Google Apps data

Create an Exchange setting to connect MobileIron Core to Google servers, such that device users will be able to access their email, calendar, and contacts. Apply the Exchange setting to the relevant labels, such that Core pushes the new setting to the correct devices. The Exchange setting must include the Google Apps Password flag, which tells Core to generate a Google Apps password and send it to Google servers.

When sending an event to a device, MobileIron Core checks whether the Google Apps Password flag is toggled on or off. If a Google Apps password is required, but the password has not yet been generated and sent to Google, then Core sends the password to Google first before sending the Exchange setting to the device.

If MobileIron Core cannot find a user on Google, Core logs an error, and does not push the Exchange setting again.

Under some circumstances, you may need to renew the Google Apps password. For more information, see Renewing the Google Apps password for a given set of users on page 190.

Note The Following:

- If you intend to distribute an AppConnect email app to devices, such as MobileIron Email+ for iOS, you must add the key email_password with a value of $GOOGLE_AUTOGEN_PASSWORD$ to the AppConnect app configuration for the email app. For more information, see "Configuring an AppConnect app configuration" in the *MobileIron Core AppConnect and AppTunnel Guide*.
- Set the Exchange Username field to $EMAIL$ when using $GOOGLE_AUTOGEN_PASSWORD$ in the Password field and when using Android enterprise managed configurations or AppConnect KVPs.

Procedure

1. In the Admin Portal go to **Policies & Configs > Configurations**.
2. Click **Add New > Exchange**.
3. In the Exchange Setting dialog box, enter the following:

Item	Description
General	
Name	Enter brief text that identifies this group of Exchange settings.
Description	Enter additional text that clarifies the purpose of this group of Exchange settings.
Server Address	Enter the address of the mail server, such as **m.google.com**. If you are using Standalone Sentry, do the following: • Enter the address of Standalone Sentry. • Go to **Services > Sentry** and edit your Standalone Sentry. In the **ActiveSync Server** field, enter **m.google.com**. • If you are using load balancers, contact MobileIron Professional Services. For more information about configuring Sentry, see the MobileIron Sentry Guide.
Use SSL	Select to use secure connections. NOTE: You must use SSL to link to Google Apps. SSL is always used, regardless of whether this setting is selected.
Google Apps Password	When linking to Google Apps, select this option to use the Google Apps

Item	Description
	password to log in to the Google account you have configured to work with MobileIron Core. This password allows device users to access their mail, contacts, and calendar data on their managed devices. When selected, Core grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with MobileIron Core, as described in Synchronizing Google account data on page 185.
ActiveSync User Email	Specify the variable for the email address to be used with this Exchange configuration. You can specify any or all of the following variables $EMAIL$, $USERID$, $PASSWORD$. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $EMAIL$ in this field.
Items to Synchronize	Select the items you want to synchronize with Google Apps: Contacts, Calendar, Email, Tasks.

4. Click **Save**.
5. Check the box next to the Exchange setting you created, and select **Actions > Apply To Label**.
6. Select the labels to which you want to apply the Exchange setting and click **Apply**.

Renewing the Google Apps password for a given set of users

If there is a communication error when sending a Google Apps password to Google, MobileIron Coresends the old password to the device. Core tracks the number of attempts to send updated passwords to Google. If it reaches the preset maximum number of attempts to contact Google servers, Core stops trying and the password is set to failure state. At this point, you must manually renew the Google Apps password.

You can renew the Google password for an individual user or a set of users on the Users page in the MobileIron Core Admin Portal. After you generate it, Core pushes the new password to Google when the device checks in.

Procedure

1. Go to **Devices & Users > Users**.
2. Select the user or users whose Google password you want to renew.
3. Select **Actions > Renew Google Apps Password**.
   The Admin Portal shows a dialog that lists the users whose Google Apps password you want to renew.
4. Click **Renew Google Apps Password**.
   The Admin Portal sends the request to renew the Google Apps password for the selected users.
5. Click **Close**.

Setting up Gmail with Android enterprise

You can deploy Gmail to Android enterprise devices if you have set up MobileIron Core for Android enterprise.

NOTE: If you want to set up MobileIron Email+ with Android enterprise, please see *MobileIron Email+ for Android enterprise*.

Add Gmail to the App Catalog on Core as you would any Android enterprise app. That is, in the Admin Portal, in **Apps > App Catalog,** add Gmail from Google Play. When adding it, be sure to select **Install this app for Android enterprise.**

When you add the Gmail app, its app configurations are displayed in the **Configuration Choices** section. Edit these choices according to the following table:

TABLE 29. GMAIL CONFIGURATION PARAMETERS

Settings	Description
Email Address	Enter substitution variables to define the email address. Typically, you enter $EMAIL$. You can also enter combinations of these variables, depending on your ActiveSync server requirements: $USERID$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$
Hostname or Host	Enter the host name of the mail server to use. Enter the fully qualified domain name of the Exchange server or the Standalone Sentry you are using.
Username	Use variables to define the username for the email account.
SSL Required	Select if you want secure communication using https: to the server that you specified for Exchange host.
Trust all certificates	Select only if you want the app to automatically accept untrusted certificates. Use this option only for debugging or development when working in a test environment.

TABLE 29. GMAIL CONFIGURATION PARAMETERS (CONT.)

Settings	Description
Login certificate alias	Enter the alias for the login certificate. The value should be a string alias representing a certificate with private key stored in the work profile keystore. For example: `$CERT_ALIAS:<certificate config name>$` NOTE: When a certificate alias is used with a password, Gmail does not send the certificate alias to the server and an "Unable to connect to server" error is displayed. This is a Google issue.
Default email signature	$USERID$
Default sync window	Use the Default sync window drop-down menu to select an interval in minutes for the device to sync with app or data updates.

Related topics

- Setting up MobileIron Core for Android enterprise
- "Deploying public Android enterprise apps" in the *MobileIron Apps@Work Guide*

Managing Wi-Fi Settings

This section addresses the Wi-Fi settings.

Wi-Fi settings

To configure wireless network access, in the Admin Console, go to **Policies & Configs > Configurations.** Click **Add New > Wi-Fi** to create a new configuration.

NOTE: Do not assign multiple Wi-Fi profiles to a device if the Network Name SSID (Service Set Identifier) differs only by case. For example, if one profile has an SSID value of "yourco" and another has an SSID of "YourCo," those two must not be assigned to the same device. Doing so will cause check-in problems, and full device details will not be properly recorded.

Android 10 devices

On Android 10 devices through the latest version as supported by MobileIron, upon installation or upgrade, device users can configure Wi-Fi and location settings in specific modes.

NOTE: Administrators are required to leave in all modes of deployment to enable Wi-Fi and MTD configurations to be successfully applied. This means having the Allow the user to turn on location sharing lockdown field selected (checked.)

The table below depicts the behavior changes in different configuration modes:

TABLE 30. WI-FI CHANGES IN SPECIFIC CONFIGURATION MODES

Item	Description
All modes	Disconnect Wi-Fi local action is disabled in all modes on Android 10 devices. For all modes of deployment, to enable Wi-Fi and MTD configurations to be successfully applied, the Allow the user to turn on location sharing lockdown field must be selected.
Work Profile mode (Android Enterprise)	Device users are requested to activate location for the device and for the Managed Profile. In order for administrators to update Wi-Fi and to have Mobile Threat Defense detect Wi-Fi-based threats, device users must activate location. If the device user chooses No, the device will be flagged with an unblocking error for non-compliance and Core will report a configuration error. Administrators will not be able to disable Wi-Fi through UEM configurations in Work managed device mode on Android 10 devices.
Work managed device mode (Android enterprise)	In the background, MobileIron will turn on the location services setting without device user intervention. Wi-Fi and MTD configurations should be successful with no errors. If there is no MTD configuration or a Wi-Fi configuration, the device user can switch location service on or off.
Device Administrator (DA) Mode	Wi-Fi configurations will not be supported and will show as Sent on the server with config error. MTD configurations will be still accepted for non-network threats but the Wi-Fi related threats will not work for Device Administrators and MAM. Administrators will not be able to disable Wi-Fi through UEM configurations in Device Administrator mode on Android 10 devices.
Kiosk mode	Administrators wanting users to enable/disable Wi-Fi but not connect to any other Wi-Fi network settings are not supported. Options available to administrators are: • Scenario 1 - Administrators wanting users to enable/disable Wi-Fi and connect to any available Wi-Fi will need to have the following settings in Kiosk mode: Lockdown settings: Allow Wi-Fi (de-selected) and Allow Wi-Fi to be configured (de-selected). Kiosk Mode Settings: Allow users to Access Wi-Fi Settings (selected). • Scenario 2 - Administrators wanting to block users from any Wi-Fi controls will need to have the following Lockdown settings: - Allow Wi-Fi (selected) - Allow Wi-Fi to be configured (selected).

Wi-Fi profiles and password caching

To make deployments easier, MobileIron offers the option of caching a user's Wi-Fi password. This option is turned off by default. Cached passwords are encrypted, stored on MobileIron Core, and used only for authentication. Note

that the password must match the LDAP password in order for this feature to be of use.

Wi-Fi network priority for Android devices

Within the Core user interface, you set the Wi-Fi network priority for Android devices in two places in the user interface. First, set the Lockdown policy option for Android Wi-Fi devices, then you can set the Wi-Fi configuration. The Lockdown policy option "**Always Connect Device to Managed Wi-Fi**" ensures that Android devices pro-actively connect to the highest priority managed Wi-Fi network in range. By enabling this field**i** in the Lockdown policy and using Wi-Fi priority settings, administrators can control which Wi-Fi network a device connects to. In addition, the Wi-Fi network configuration settings allow you specify a direct or automatic Wi-Fi connection to a Wi-Fi proxy setting, increasing the network security of your Wi-Fi devices. Both the Wi-Fi network priority and the **Always Connect Device to Managed Wi-Fi** lockdown policy option apply to *all* Android devices.

With **Always Connect Device to Managed Wi-Fi:**

- ENABLED: an Android device will always connect to the highest priority managed Wi-Fi network available, actively disconnecting from any unmanaged networks.
  - The Wi-Fi Priority value you set provides a preference for the highest priority network if multiple managed networks are available.
  - The connection to the managed Wi-Fi network is maintained as long as the signal is in range, even if a managed Wi-Fi network with a higher priority becomes available.
  - Exception: a newly received Wi-Fi configuration goes into effect after the current Wi-Fi connection disconnects.
- DISABLED: an Android device will connect to the highest priority Wi-Fi network as determined by Android.

Caution: When enabling **Always Connect Device to Managed Wi-Fi** in the Lockdown policy, because the device will actively connect to managed Wi-Fi SSID with the highest priority, if there is an error in the Wi-Fi configuration it is possible for the device to lose Wi-Fi access.

NOTE: When **Always Connect Device to Managed Wi-Fi** is enabled and a managed Wi-Fi network is in range, the user cannot override the Wi-Fi connection choice and cannot choose to connect to an unmanaged network.

Setting up enforced Wi-Fi network priority

First, set up the Lockdown policy to enable **Always Connect Device to Managed Wi-Fi** and apply the policy to the device.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Click **Add New > Lockdown**.
3. In the New Lockdown Policy dialog box, enter a **Name**.

4. Scroll down to the Android section. For **Always Connect Device to Managed Wi-Fi** , select **Enable**.
5. Fill out the rest of the Lockdown policy as needed.
6. Click **Save**.
7. Apply the policy to a label to assign it to the appropriate Android devices.

Next, provide values for network priority settings for all Wi-Fi configurations. From this menu, you can select a direct or automatic proxy server as well as specific servers to exclude.

In the MobileIron Core Admin Portal:

1. Go to **Policies & Configs > Configurations**.
2. Select an existing **Wi-Fi** configuration, and click **Edit** in the right-side panel.
3. Locate the **Android Settings** section in the dialog box.
4. For **Priority**, enter a number between 1 (lowest priority) and 100 (highest priority), inclusive, or leave it blank (default priority).

   NOTE: Devices use the priority that is provided when the Wi-Fi configuration is provisioned. Future changes to the priority value are not sent to the device.

5. Select an optional **Proxy Type** that is supported on Android 8.0 through the most recently released versions as supported by MobileIron. Use the pull-down menu to select from the following options:
   a. **None**: This is the default value, indicating that no proxy server is specified.
   b. **Direct**: Select to specify a direct connection to a proxy server. After you make this selection, the menu expands and the following fields are displayed:
      Host Exclusions List: Click **+** to enter one or more domains of traffic that will not be proxied. This setting applies to the URL traffic, but it does not apply to the proxy server.
      Proxy Server: Enter the host name or IP address of a proxy server.
      Proxy Port: Specify a proxy server port.
   c. **Auto**: Select to specify an automatic connection to the proxy server. After you make this selection, the following field is displayed:
      PAC URL: Enter the proxy auto-config (PAC) URL of the Wi-Fi proxy server. The PAC URL provides a mapping of URLs that the software uses to locate the proxy server automatically.
6. Click **Save**.
   The Wi-Fi configuration is now pushed to all devices that have the configuration's labels applied. The Priority designation applies to both newly provisioned and previously provisioned network settings.
7. Apply the Wi-Fi configurations to a label to assign them to the appropriate devices.

When the Wi-Fi configuration and the Lockdown policy as described are applied to a device, the highest priority Wi-Fi network is enforced.

Android 10 specific Wi-Fi settings

On Android 10 devices through the latest version as supported by MobileIron, upon installation or upgrade, device users can configure Wi-Fi and location settings in specific modes.

Note The Following:

- For all modes of deployment, to enable Wi-Fi and MTD configurations to be successfully applied, the Allow the user to turn on location sharing lockdown field must be selected.
- Administrators will not be able to disable Wi-Fi through UEM configurations in Work managed device mode and Device Administrator mode on Android 10 devices.
- Administrators are required to leave in all modes of deployment to enable Wi-Fi and MTD configurations to be successfully applied.

Wi-Fi configuration now requires end users to allow location services on the device. The behavior changes in different configuration modes and is documented in the table below.

TABLE 31. ANDROID 10 WI-FI SETTINGS

Item	Description
Work Profile mode (Android Enterprise)	Device users are requested to activate location for the device and for the Managed Profile. In order for administrators to update Wi-Fi and to have Mobile Threat Defense detect Wi-Fi-based threats, device users must activate location. If the device user chooses No, the device will be flagged with an unblocking error for non-compliance and Core will report a configuration error.
Work managed device mode (Android enterprise)	In the background, MobileIron will programmatically turn on the location services setting without device user intervention. Wi-Fi and MTD configurations should be successful with no errors. NOTE: If there is no MTD configuration or a Wi-Fi configuration, the device user can switch location service on or off.
Device Administrator (DA) Mode	Wi-Fi configurations will not be supported and will show as Sent on the server with config error. MTD configurations will be still accepted for non-network threats but the Wi-Fi related threats will not work for Device Administrators and MAM.
Kiosk Mode	Administrators wanting users to enable/disable Wi-Fi but not connect to any other Wi-Fi network settings are not supported. Options available to administrators are: • **Scenario 1:** Administrators wanting users to enable/disable Wi-Fi and connect to any available Wi-Fi will need to have the below settings in Kiosk. ◦ Lockdown settings > Allow Wi-Fi (de-selected)

TABLE 31. ANDROID 10 WI-FI SETTINGS (CONT.)

Item	Description
	◦ Lockdown settings > Allow Wi-Fi to be configured (de-selected) ◦ Kiosk Mode Settings > Allow users to Access Wi-Fi Settings (selected) • **Scenario 2:** Administrators wanting to block users from any Wi-Fi controls. ◦ Lockdown Settings > Allow Wi-Fi (selected) ◦ Lockdown Settings > Allow Wi-Fi to be configured (selected)

Using Wi-Fi priority values

Administrators can use the Wi-Fi priority feature to influence the network connections that devices make. The table below describes how to set Wi-Fi priorities to achieve the noted results.

TABLE 32. WI-FI PRIORITY VALUES

Desired outcome	Settings required
Allow any Wi-Fi connection, equally	(This is the default state.) For **Always Connect Device to Managed Wi-Fi** in Lockdown policy: **Disable** For Wi-Fi configuration: The **Priority** field is ignored
Ensure that managed Wi-Fi networks always get priority over non-managed networks; actively disconnect from unmanaged networks when a managed network is available. Do not allow users to override the Wi-Fi connection choice with an unmanaged network.	For **Always Connect Device to Managed Wi-Fi** in Lockdown policy: **Enable** For Wi-Fi configuration: set the **Priority** field for each Wi-Fi configuration. 1 = lowest, 100 = highest.

How an Android device chooses its Wi-Fi network

If a device has multiple Wi-Fi networks configured, then it will automatically connect to an SSID in the following priority order, assuming a signal is available:

1. a managed SSID with the highest priority as set by the administrator (if **Always Connect Device to Managed Wi-Fi** is enabled.)

2. an unmanaged SSID, (or a managed SSID if **Always Connect Device to Managed Wi-Fi** is disabled) as chosen by the Android operating system.

When multiple Wi-Fi networks have the same priority, the Android operating system typically prioritizes the most recently used SSID.

When the device receives a new highest-priority Wi-Fi configuration, the configuration takes effect after the current Wi-Fi connection is ended for any reason.

When multiple Wi-Fi signals become available

In Mobile@Work with the Lockdown policy setting **Always Connect Device to Managed Wi-Fi** set to Enable**,** an existing unmanaged Wi-Fi connection is pro-actively disconnected if a managed SSID signal comes into range.

For example, if a user connects to an unmanaged network, and walks into range of one or more managed networks, the device disconnects from the unmanaged network and connects to the highest-priority managed network.

With the Lockdown policy setting **Always Connect Device to Managed Wi-Fi** set to Disable, Wi-Fi connections are not actively disconnected. The next time the Wi-Fi connection is reestablished, Android will automatically choose the highest priority network.

Wi-Fi network manual override behavior

A user's ability to manually choose a Wi-Fi network depends on the **Always Connect Device to Managed Wi-Fi** setting in the Lockdown policy, as shown in the table.

TABLE 33. WI-FI NETWORK MANUAL OVERRIDE BEHAVIOR

Lockdown Policy Setting	Wi-Fi SSID manual override behavior
Always Connect Device to Managed Wi-Fi: Disable	A user can select and override a Wi-Fi SSID connection by connecting manually.
For **Always Connect Device to Managed Wi-Fi**: Enable	A user can attempt to select an SSID by connecting manually, however, if at any time a higher priority network is in range, the device disconnects from an unmanaged network and connects to the highest priority managed network. If the user manually connects to a managed network, the connection is maintained even if a higher priority managed network comes into range.

Wi-Fi authentication types

The fields that appear in the **New Wi-Fi Setting** dialog change based on values selected. The following tables describe the fields required **for each selection in the Authentication field**:

Open authentication

Use the following guidelines to set up Open authentication.

TABLE 34. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select Open.
Data Encryption	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Open authentication, the following encryption options are available: • Disabled • WEP
Network Key	WEP encryption Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	Re-enter the network key to confirm.
User Name	WEP Enterprise encryption Specify the variable to use as the user name when establishing the Wi-Fi connection. See Open authentication on page 200.
Password	WEP Enterprise encryption

TABLE 34. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any MobileIron Core administrator. Note The Following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See Open authentication on page 200.
Apply to Certificates	WEP Enterprise encryption Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config.
Trusted Certificate Names	WEP Enterprise encryption. If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	WEP Enterprise encryption. Select this option to let users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	WEP Enterprise encryption. Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • PEAP • TLS • TTLS You must select only one protocol. **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC).

TABLE 34. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	If you select TLS, then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.
Windows Settings	These features are not supported on Android devices.

Related topics

- Shared authentication
- WPA Enterprise authentication
- WPA2 / WPA3 Enterprise authentication
- WPA Personal authentication
- WPA2 / WPA3 Personal authentication
- Supported variables for Wi-Fi authentication

Shared authentication

Use the following guidelines to set up shared authentication:

TABLE 35. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select Shared.
Data Encryption	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Shared authentication, the following encryption options are available:

TABLE 35. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	• Disabled • WEP
Network Key	WEP encryption Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	Re-enter the network key to confirm.
User Name	WEP Enterprise encryption Specify the variable to use as the user name when establishing the Wi-Fi connection. See Shared authentication on page 202.
Password	WEP Enterprise encryption Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any MobileIron Core administrator. Note The Following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See Shared authentication on page 202.
Apply to Certificates	WEP Enterprise encryption Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config.
Trusted Certificate Names	WEP Enterprise encryption. If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as

TABLE 35. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	*.mycompany.com.
Allow Trust Exceptions	WEP Enterprise encryption. Select this option to let users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	WEP Enterprise encryption. Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • PEAP • TLS • TTLS You must select only one protocol. **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

Related topics

- Open authentication
- WPA Enterprise authentication
- WPA2 / WPA3 Enterprise authentication
- WPA Personal authentication
- WPA2 / WPA3 Personal authentication
- Supported variables for Wi-Fi authentication

WPA Enterprise authentication

Use the following guidelines to set up WPA Enterprise authentication:

TABLE 36. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA Enterprise.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Enterprise authentication, the following encryption options are available: • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See WPA Enterprise authentication on page 204.
Password	Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any MobileIron Core administrator. Note The Following: • If you specify $PASSWORD$, also enable Save User Password under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See WPA Enterprise authentication on page 204.
Apply to Certificates	Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config. Though this section allows multiple certificates to be configured, Android supports only one entry in this field. If more than one is configured, only one of them will be installed on the device. If more than one CA certificate is required to validate the Access Point Identity Certificate, they must be installed using separate Wi-Fi profiles.

TABLE 36. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Trusted Certificate Names	This feature is not supported on Android devices. If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	This feature is not supported on Android devices. Select this option to let users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	This feature is not supported on Android devices. Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • PEAP • TLS • TTLS You must select only one protocol. **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

Related topics

- Open authentication
- Shared authentication
- WPA2 / WPA3 Enterprise authentication
- WPA Personal authentication
- WPA2 / WPA3 Personal authentication
- Supported variables for Wi-Fi authentication

WPA2 / WPA3 Enterprise authentication

Use the following guidelines to configure WPA2 or WPA3 Enterprise authentication.

TABLE 37. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION

Item	Description
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: • WPA2 Enterprise • WPA2 Enterprise (iOS 8 or later except Apple TV) • WPA3 Enterprise (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA2 Enterprise authentication, the following encryption options are available: • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See WPA2 / WPA3 Enterprise authentication on page 207.
Password	Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any MobileIron Core administrator. Note The Following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. Valid variables are variables in the drop-down list.
Apply to Certificates	Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config. Though this section allows multiple certificates to be configured, Android

TABLE 37. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION (CONT.)

Item	Description
	supports only one entry in this field. If more than one is configured, only one of them will be installed on the device. If more than one CA certificate is required to validate the Access Point Identity Certificate, they must be installed using separate Wi-Fi profiles.
Trusted Certificate Names	This feature is not supported on Android devices.
Allow Trust Exceptions	This feature is not supported on Android devices.
Use Per-connection Password	This feature is not supported on Android devices.
EAP Type	Select the authentication protocol used: • PEAP • TLS • TTLS You must select only one protocol. **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

Related topics

- Open authentication
- Shared authentication
- WPA Enterprise authentication
- WPA Personal authentication
- WPA2 / WPA3 Personal authentication
- Supported variables for Wi-Fi authentication

WPA Personal authentication

Use the following guidelines to configure WPA Personal authentication.

TABLE 38. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA Personal.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

WPA2 Personal authentication

Use the following guidelines to configure WPA2 Personal authentication.

TABLE 39. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA2 Personal.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

Related topics

- Open authentication
- Shared authentication
- WPA Enterprise authentication
- WPA2 / WPA3 Enterprise authentication
- WPA2 / WPA3 Personal authentication
- Supported variables for Wi-Fi authentication

WPA2 / WPA3 Personal authentication

Use the following guidelines to configure WPA2 or WPA3 Personal authentication.

TABLE 40. WI-FI WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in MobileIron.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: • WPA2 Personal • WPA3 Personal (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Android devices.

Related topics

- Open authentication
- Shared authentication
- WPA Enterprise authentication
- WPA2 / WPA3 Enterprise authentication
- WPA Personal authentication
- Supported variables for Wi-Fi authentication

Supported variables for Wi-Fi authentication

You can use the following variables in fields that support variables.

- $PASSWORD$ (only supported in the password field)
- $EMAIL$
- $USERID$
- $DEVICE_MAC$
- $NULL$
- $USER_CUSTOM1$... $USER_CUSTOM4$ (custom fields defined for LDAP)

Custom attribute variable substitutions are supported.

Related topics

- Open authentication
- Shared authentication
- WPA Personal authentication
- WPA2 / WPA3 Personal authentication
- WPA Enterprise authentication
- WPA2 / WPA3 Enterprise authentication

Managing VPN Settings

This section addresses the VPN settings.

VPN settings overview

VPN is a technology that creates a secure network connection over a public network. A mobile device uses a VPN client to securely access protected corporate networks.

To use VPN:

- On the device, the user installs a VPN client app.

You determine how the user obtains the VPN client app. You can, for example, add the app as a Google Play Store app to the App Catalog. See “Managing Mobile Apps for Android” in the *Apps@Work Guide*.

NOTE: If the device receives the VPN setting before the user has installed the VPN client app, Mobile@Work displays an error message. The message instructs the user to install the VPN client app.

- Define a VPN setting in MobileIron Core.
- Apply labels to the VPN setting so that the VPN setting is sent to the appropriate devices.
- Depending on the type of VPN, additional set up steps may be required to complete the VPN configuration.

Mobile@Work uses the VPN client and the VPN setting to enable access to corporate networks.

Configuring new VPN settings

In the Admin Portal, go to **Policies & Configs > Configurations** and click **Add New > VPN** to configure VPN access.

The fields that appear in the **New VPN Setting** dialog box change based on values selected. The following sections describe the fields required for each selection in the **Connection Type** field. For MobileIron Tunnel support for Android, select **MobileIron Tunnel (Android)** in the Connection Type field.

PPTP

Use the following guidelines to configure PPTP VPN.

NOTE: iOS 10 and macOS Sierra no longer support PPTP for VPN.

TABLE 41. PPTP SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select PPTP.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.

TABLE 41. PPTP SETTINGS (CONT.)

Item	Description
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Encryption Level	Select **None**, **Automatic** or **Maximum** (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**: Password** or **RSA SecureID**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.

L2TP

Use the following guidelines to configure L2TP VPN.

TABLE 42. L2TP SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select L2TP
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes

TABLE 42. L2TP SETTINGS (CONT.)

Item	Description
	can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Shared Secret	The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Re-enter the shared secret to confirm.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**: Password** or **RSA SecureID**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.This field does not display if you selected RSA SecureID for authentication.
Proxy	Select Manual or Automatic to configure a proxy. If you select Manual, you must specify the proxy server name and port number. If you select Automatic, you must specify the proxy server URL.

IPSec (Cisco)

Use the following guidelines to configure IPSec (Cisco) VPN.

TABLE 43. IPSEC (CISCO) SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Connection Type	Select IPSec (Cisco).
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **None**, **Manual**, or **Automatic** to configure a proxy.

TABLE 43. IPSEC (CISCO) SETTINGS (CONT.)

Item	Description
	If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**:** Shared Secret/Group Name or Certificate.

TABLE 43. IPSEC (CISCO) SETTINGS(CONT.)

Item	Description
Group Name	Shared Secret/Group Name authentication. Specify the name of the group to use. If Hybrid Authentication is used, the string must end with “[hybrid]”.
Shared Secret	Shared Secret/Group Name authentication. The shared secret passcode. This is not the user’s password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Shared Secret/Group Name authentication. Re-enter the shared secret to confirm.
Use Hybrid Authentication	Shared Secret/Group Name authentication. Select to specify hybrid authentication, i.e., server provides a certificate and the client provides a pre-shared key.
Prompt for Password	Shared Secret/Group Name authentication. Specify whether the user should be prompted for a password when connecting.
XAuth Enabled	Specifies that IPsec XAuth authentication is enabled. Select this option if your VPN requires two-factor authentication, resulting in a prompt for the password. This option is enabled by default.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
Include User PIN	Certificate authentication. Select to prompt the user for a PIN.
VPN on Demand	Certificate authentication. Select to enable the VPN on Demand section. Click **Add New** to specify a domain or hostname and the preferred connection option.
Per-app VPN	This feature is not supported on Android devices.

IPSec (Blue Coat)

This feature is not supported on Android devices.

IKEv2 (Windows)

This feature is not supported on Android devices.

IKEv2 (iOS Only)

This feature is not supported on Android devices.

Samsung Knox IPsec

Samsung Knox IPsec is for Android devices with Samsung Knox only.

Samsung Knox IPsec is used for VPN access in the Samsung Knox container (Android Samsung Knox Container Settings on page 391). Use the following guidelines to configure Samsung Knox IPsec.

TABLE 44. SAMSUNG KNOX IPSEC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select Samsung Knox IPsec.
Server	Enter the IP address, hostname, or URL for the VPN server.
Backup Server	Enter the IP address, hostname, or URL for the fallback server to use in the event that the primary server is not available.
Authentication Type	Select the authentication method to use: Pre-Shared Key or Certificate.
Shared Secret	Pre-Shared Secret authentication. The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Pre-Shared Secret authentication. Re-enter the shared secret to confirm.
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
CA Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.

TABLE 44. SAMSUNG KNOX IPSEC SETTINGS (CONT.)

Item	Description
User Authentication	Select to enable user authentication as an additional factor.
Username	If User Authentication is selected, review the default variable to determine if it meets your needs. If it does not meet your needs, enter a different variable.
Password	If User Authentication is selected, review the default variable to determine if it meets your needs. default variable to determine if it meets your needs. If it does not meet your needs, enter a different variable.
IKE Version	Enter the Internet Key Exchange (IKE) version in use by your IPsec VPN server. IPsec uses the IKE to negotiate the protocols and algorithms used for the connection, and to generate the encryption and authentication keys.
Phase 1 Mode	If you selected IKE Phase 1, select the mode of operation in use by your IPsec VPN server: • Main: Has three two-way exchanges between the initiator and the receiver. • Aggressive: Fewer exchanges are made, and with fewer packets.
Group ID Type	Select the Group ID type your IPsec VPN server uses to authenticate to IKE peers.
Group Name	Enter the group name for your IPsec VPN server. This name corresponds to the value selected in Group ID Type.

Cisco AnyConnect (iOS only)

This VPN mode is for iOS devices only.

Cisco Legacy AnyConnect

Cisco AnyConnect is a universal app that can be used with Samsung Knox or with any Android device. This app can be used for all VPN modes:

- per-app inside the Knox container
- per-app outside the Knox container
- per-container (Knox)
- per-device (Knox)
- per-device (Android)

Users must remove old versions of the AnyConnect app before installing the new version.

Use the following guidelines to configure Cisco Legacy AnyConnect VPN.

TABLE 45. CISCO ANYCONNECT VPN SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select Cisco Legacy AnyConnect.
Samsung Knox	Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the **Samsung Knox** option. See: • Configuring VPN modes when VPN client is outside the Knox container on page 236 • on page 237
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This feature is not supported on Android devices. Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.

TABLE 45. CISCO ANYCONNECT VPN SETTINGS (CONT.)

Item	Description
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select Password or Certificate.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
Group Name	Specify the name of the group to use.
VPN on Demand	Certificate authentication. Select to enable the VPN on Demand section. Click **Add New** to specify a domain or hostname and the preferred connection option.
Per-app VPN	This feature is supported on Android devices with Mobile@Work 9.0.0.0 through the most recently released version as supported by MobileIron.
Provider Type	This feature applies to iOS and macOS devices only.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

Juniper SSL

The Juniper SSL VPN type supports Juniper SSL VPN definitions created in previous versions of MobileIron Core. Juniper SSL VPN definitions are routed to the Pulse Secure VPN client. Use the Pulse Secure SSL type for new VPN definitions.

Use the following guidelines to configure Juniper SSL VPN and Pulse Secure SSL VPN.

TABLE 46. JUNIPER SSL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select Juniper SSL.
Samsung Knox	Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the **Samsung Knox** option. See: • Configuring VPN modes when VPN client is outside the Knox container on page 236 • on page 237
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This feature is not supported on Android devices. Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.

TABLE 46. JUNIPER SSL SETTINGS (CONT.)

Item	Description
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use for authentication. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select **Password** or **Certificate**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.

TABLE 46. JUNIPER SSL SETTINGS (CONT.)

Item	Description
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN on Demand	Certificate authentication.
Per-app VPN	An additional license may be required for this feature. You cannot delete a per-app VPN setting that is being used by an app. Remove the per-app VPN setting from the app before you delete the setting. You can enable per-app VPN for an app when you: • add the app in the App Catalog. • edit an in-house app or an App Store app in the App Catalog. See the MobileIron Apps@Work Guide for information about how to add or edit apps.
Provider Type	This feature applies to iOS and macOS devices only.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

Pulse Secure SSL

The Pulse Secure SSL type replaces the Juniper SSL type.

Use the following guidelines to configure Pulse Secure SSL VPN.

TABLE 47. PULSE SECURE SSL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select Pulse Secure SSL.
Samsung Knox	Select this option to use per-app VPN (either inside or outside the Knox

TABLE 47. PULSE SECURE SSL SETTINGS (CONT.)

Item	Description
	Workspace) or per-container VPN. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the **Samsung Knox** option. See: • Configuring VPN modes when VPN client is outside the Knox container on page 236 • on page 237
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This feature is not supported on Android devices. Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy*

TABLE 47. PULSE SECURE SSL SETTINGS (CONT.)

Item	Description
	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use for authentication. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select **Password** or **Certificate**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN on Demand	Certificate authentication.
Per-app VPN	An additional license may be required for this feature. You cannot delete a per-app VPN setting that is being used by an app. Remove the per-app VPN setting from the app before you delete the setting. You can enable per-app VPN for an app when you: • add the app in the App Catalog. • edit an in-house app or an App Store app in the App Catalog. See the MobileIron Apps@Work Guide for information about how to add or edit apps.

TABLE 47. PULSE SECURE SSL SETTINGS (CONT.)

Item	Description
Provider Type	This feature applies to iOS and macOS devices only.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

F5 SSL

Use the following guidelines to configure F5 SSL VPN. This connection type is supported only on Android devices on which Samsung Knox is enabled.

TABLE 48. F5 SSL VPN SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select F5 SSL.
Samsung Knox	Always select this option. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the **Samsung Knox** option. See: • Configuring VPN modes when VPN client is outside the Knox container on page 236 • on page 237
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number.

TABLE 48. F5 SSL VPN SETTINGS (CONT.)

Item	Description
	If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select **Password** or **Certificate**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.

TABLE 48. F5 SSL VPN SETTINGS (CONT.)

Item	Description
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
VPN on Demand	Certificate authentication. Select to enable the VPN on Demand section. Click **Add New** to specify a domain or hostname and the preferred connection option.
Per-app VPN	This setting does not apply to Android.
Provider Type	This feature applies to iOS and macOS devices only.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

OpenVPN

Use this setting to configure Samsung “OpenVPN net.openvpn.knox.connect” for Samsung Knox devices. Contact Samsung to get the correct OpenVPN package. It is supported only on devices with the Samsung Knox option selected in the VPN setting.

Use the following guidelines to configure OpenVPN:

TABLE 49. OPENVPN SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select **OpenVPN**. Only fields relevant to OpenVPN are displayed.
Samsung Knox	Always select this option. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.

TABLE 49. OPENVPN SETTINGS (CONT.)

Item	Description
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the **Samsung Knox** option. See: • Configuring VPN modes when VPN client is outside the Knox container on page 236 • on page 237
Package Name	Applies to OpenVPN only. Provide the Android package name of the OpenVPN client app: net.openvpn.knox.connect
Server	Enter the IP address, hostname or URL for the VPN server.
Username	Specify the user name. The default is $USERID$. You can specify a different variable, for example $EMAIL$.
User Authentication	Click the radio button for **Password** or **Certificate** to specify user authentication type. If you select **Password**, specify the password to use. The default value is $PASSWORD$. You can specify a custom format, for example, $PASSWORD$_$USERID$. Other password formats available are: If you select **Certificate**, specify Password, and then provide the two other settings added to the page: Identity Certificate (required): Enter the identity certificate number. CA Certificate (optional): Select the CA Certificate from the list of available certificates. For more information, refer to the MobileIron Core Admin Guide.
Per-app VPN	Click Yes to set up per-app VPN inside the container, per-app VPN outside the container, and per-container VPN. To use per-app VPN, a Samsung General Policy with a valid Samsung Knox license is required.
Port	Applies to OpenVPN only. Enter the port number for the connection. (Required)
Protocol	Applies to OpenVPN only. Select from drop-down.
Cipher	Applies to OpenVPN only. Select from drop-down.
Packet Auth Digest	Applies to OpenVPN only. Select from drop-down.

Palo Alto Networks GlobalProtect

This feature is not supported on Android devices.

Custom SSL

Custom SSL does not apply to Android.

MobileIron Tunnel (for iOS and macOS)

This feature is not supported on Android devices.

MobileIron Tunnel (Android)

You can configure MobileIron Tunnel for use with Android. Before starting this procedure, make sure MobileIron Tunnel is installed on the Android device. For detailed information on how to set up MobileIron Tunnel for Android, see the *MobileIron Tunnel for Android Guide for Administrators*.

These instructions also include how to configure VPN chaining with MobileIron Tunnel. VPN chaining is the nesting of a VPN tunnel in another VPN tunnel for added security.

KNOX VPN Support

As part of MobileIron's support of Samsung Knox, Mobile@Work for Android together with MobileIron Core support the following Virtual Private Network (VPN) clients:

- Pulse Secure (previously called Junos Pulse) (SSL)
- F5 BIG-IP Edge Client (SSL)
- Cisco AnyConnect (SSL)
- OpenVPN (SSL)
- MobileIron Tunnel for Samsung Knox

Mobile@Work 9.0.0.0 for Android through the most recently released version as supported by MobileIron adds:

- Cisco AnyConnect (universal app for Android and for Samsung Knox)

MobileIron supports all of these VPN clients on Samsung Knox 2.0 through the most recently released version as supported by MobileIron.

Only Cisco AnyConnect and Pulse Secure are supported with other Android devices.

Basic Requirements to use Samsung Knox Features

To use any Samsung Knox Premium features that MobileIron supports, including VPN, the following are required:

- The user must have a Samsung Knox-capable mobile device.
- A Samsung General Policy with a Samsung Knox license key must be defined and applied to a label. To create this policy, in Core Admin Portal go to **Policies & Configs > Policies**. Select **Add New > Android > Samsung General**.
- The device must have the Samsung General Policy label applied.

VPN clients deployed either inside or outside Knox Workspace

VPN client apps are deployed either inside or outside the Knox Workspace (container). When deployed inside the container, the VPN client and its data are protected by the Knox security platform.

Whether the VPN client is deployed inside or outside the container depends on:

- the version of Mobile@Work on the device
- an option you set in the VPN setting

Mobile@Work 9.1 for Android

When a device is running Mobile@Work 9.1 for Android, you can set an option in the VPN setting to deploy the VPN client inside the container. The following VPN clients you can use with Samsung devices to deploy inside or outside the container are:

- Pulse Secure SSL (previously Junos Pulse)
- Cisco AnyConnect
- F5 SSL
- OpenVPN
- MobileIron Tunnel for Samsung Knox

The option in the VPN setting is called **Deploy inside Knox workspace. When you choose this option, be sure to add the VPN client app to the Apps** section of the Samsung Knox Container setting. MobileIron Tunnel for Samsung Knox is always deployed inside the container.

See also:

- Configuring VPN modes when VPN client is outside the Knox container on page 236
- on page 237

Prior to Mobile@Work 9.1 for Android

When a device is running a version of Mobile@Work prior to 9.1, the option in the VPN setting to deploy the VPN client inside the container **is not applicable**. The following table shows which VPN clients are deployed inside or outside of the Knox Workspace (container) when the device is running a version of Mobile@Work prior to 9.1:

Always deployed inside the container	Always deployed outside the container
• OpenVPN	• Pulse Secure SSL (previously Junos Pulse) • Cisco AnyConnect • F5 SSL

VPN Modes

For Android devices using the Samsung Knox Workspace, there are four VPN modes you can configure in MobileIron Core. They are:

Per-Device VPN

- If a VPN client is installed outside the Knox container:
  - all apps outside the container use the same VPN connection.
  - a per-device VPN does not apply inside the Knox container for Samsung Knox 2.0 through the most recently released versions as supported by MobileIron.
- If a VPN client is installed inside the Knox container, per-device VPN provides similar functionality to per-container VPN:
  - all apps inside the Knox container use the same VPN connection.
  - a per-device VPN does not apply to apps outside the Knox container.
- Available for all Android devices.

Per-Container VPN

- All apps inside the Knox container use the same VPN connection.
- Requires a Samsung Knox license.

Per-App VPN for apps inside of Knox Container

- Applies to individual apps inside a Knox container.
- Each app can be individually assigned to a VPN connection. We recommend using a single VPN profile from a single provider.(The new feature allows you to cross providers.)
- Any number of apps can share a single VPN connection. (Check this is true for the cross provider feature. It may only be one app.)
- Requires a Samsung Knox license. See Working with Samsung general policies on page 139.

Per-App VPN for apps outside of Knox Container

- Applies to apps outside of a Knox container (a Knox container may or may not be present.)
- Each app can be individually assigned to a VPN connection.
- Requires a Samsung Knox license.

All of these modes are supported by the following VPN clients on Samsung Knox devices:

TABLE 50. VPN CLIENTS

VPN Client Name	Appears in VPN Setting as Connection Type:
Pulse Secure (previously: Junos Pulse)	"Pulse Secure SSL" **Note:** The connection type "Juniper SSL" is only for VPN settings created in previous versions of MobileIron Core
F5 BIG-IP Edge Client	"F5 SSL"
OpenVPN	"OpenVPN"
Cisco AnyConnect	"Cisco AnyConnect"

The following VPN clients are supported for non-Samsung Android devices using per-device mode:

- Pulse Secure
- Cisco AnyConnect
- MobileIron Tunnel (Samsung Knox Workspace)

Configuring VPN modes when VPN client is outside the Knox container

If the VPN client is installed outside the Knox container, you can configure the VPN client to be used in one of these modes:

- per-device
- per-container
- per-app

In addition, you can configure a per app Android enterprise VPN within the Knox v3 workspace. See Creating per container and per app Android enterprise VPNs within the Knox v3 workspace.

The following table provides an overview of what you need to configure for each mode.

	per-device mode	per-container mode	per-app mode
Description	The VPN client configured for per-device use can be used by appropriately	The VPN client configured for per-container use can be used by any apps inside the	The VPN client configured for per-app use can be used only by apps specifically

	per-device mode	per-container mode	per-app mode
	labeled apps that are outside the Knox container.	Knox container.	configured to use it. The apps can be either inside or outside the Knox container.
VPN setting	Options in VPN setting: • **per-app VPN**: No • **Samsung Knox**: Select ONLY if using OpenVPN. • **Deploy inside Knox Workspace**: Not selected Apply label to VPN setting	Options in VPN setting • **per-app VPN**: Yes • **Samsung Knox**: Selected • **Deploy inside Knox Workspace**: Not selected Apply label to VPN setting	Options in VPN setting • **per-app VPN**: Yes • **Samsung Knox**: Selected • **Deploy inside Knox Workspace**: Not selected Apply label to VPN setting
App in App Catalog	• Apply label to app • **Per App VPN Settings** in app: not applicable	• App label is not applicable to VPN usage • **Per App VPN Settings** in app: not applicable	For apps outside the Knox container: • Apply label to app • **Per App VPN Settings** in app: set to VPN setting
Samsung Knox Container setting		• In the **App Settings** section, in the **VPN** field, select the VPN setting from the drop-down list. • In the **Apps** section, for a specific app, make no VPN selection. • Apply label to Samsung Knox Container setting	For apps inside the Knox container: • In the **Apps** section, for the specific app, select the VPN setting from the drop-down list. • In the **App Settings** section, in the VPN field, make no selection. • Apply label to Samsung Knox Container setting
Android enterprise	N/A	(Managed device with Work Profile mode) **Managed Device with Work Profile on the devices:** Selected **Enable Samsung Per-container VPN**: Selected	(Managed device with Work Profile mode) In the App Catalog, **Per App VPN by Label Only:** Selected (applicable for in-house apps only) **Install this app for Android Enterprise:** Selected

Creating per container and per app Android enterprise VPNs within the Knox v3 workspace

In Managed device with Work Profile mode, administrators can configure Knox VPN settings for per container and per app deployment devices to communicate with services securely. Within the Knox workspace, administrators can create per-app VPNs that they can assign to apps in the Apps catalog. Additionally, a special case of a per app deployment (MobileIron Tunnel + OpenVPN) supports VPN chaining, see "Configuring VPN chaining" procedure in *MobileIron Tunnel for Android Guide for Administrators*.

Managed device with Work Profile mode works with the following VPN connection types:

- Cisco AnyConnect
- F5 SSL
- Pulse Secure SSL
- OpenVPN
- MobileIron Tunnel (Samsung KNOX Workspace)

Note The Following:

These methods of configuring VPNs are not supported:

- Configuring VPNs via App restrictions and using Knox VPN APIs
- Support for device-wide VPN in Managed device with Work Profile mode

Android enterprise VPN is configured using a password and certificate-based credentials. KLM licenses must be applied.

Creating per container Android enterprise VPN with Knox 3 workspace

This section covers configuring Knox VPN settings for per container Android enterprise. The below procedure is applicable for Managed device with Work Profile mode for Android version 8.0.

Procedure

1. Register the device, in Work Profile mode, to Core using the procedure described in Setting the registration PIN code length for device user registration on page 72.
2. Create a Samsung General Policy. See Working with Samsung general policies.
3. Create a Android enterprise configuration.
   a. Click **Add New > Android > Android enterprise**.
      The New Android enterprise (all modes) Setting dialog box opens.
   b. Enter the Name and Description of the configuration.
   c. Select the **Enable Managed Device with Work Profile on the devices** check box.
   d. Click **Save**.

4. Apply the configuration to a device label.
5. Create a VPN configuration for Android enterprise.
   a. Click **Policies & Configurations > Configurations**.
   b. Select **Add New > VPN**. The Add VPN Setting dialog box opens.
   c. Select a Connection Type in the drop-down:
      - Cisco Legacy AnyConnect
      - OpenVPN
      - F5 SSL
      - Pulse Secure SSL
      - MobileIron Tunnel (Samsung KNOX Workspace)
   d. Select the **Samsung KNOX** check box.
   e. Select the **Deploy inside Knox Workspace** check box.
   f. Select the Per-app VPN **Yes** radio button.
   g. Click **Save**.
6. Apply the VPN configuration to a device label.
7. Edit the Android enterprise configuration.
   a. In the For Samsung Knox v3 (Android 8.0) section, select the **Enable Samsung Per-container VPN** check box.
   b. In the VPN Config Name field, select the VPN configuration you just created.
   c. Click **Save**.

In Devices & Users > Devices > Device Details page, the Managed Device with Work Profile displays your setting, for example, Workspace > Tunnel.

Creating per app Android enterprise VPN with Knox 3 workspace

This section covers configuring Knox VPN settings for per app Android enterprise. The below procedure is applicable for Managed device with Work Profile mode.

NOTE: Before you begin this procedure, follow the "Configuring VPN chaining" procedure in *MobileIron Tunnel for Android Guide for Administrators* to populate the **VPN Config Name** field.

1. Register the device, in Work Profile mode, to Core using the procedure described in Setting the registration PIN code length for device user registration on page 72.
2. Create a Samsung General Policy. See Working with Samsung general policies.
3. Apply the policy to a device label.
4. Add a new Android Enterprise app in the App Catalog, for example, Google Chrome.
   a. Click **Apps > App Catalog > Add** .
   b. In the Android Enterprise section, select the **Install this app for Android Enterprise** check box.

   c. Click **Save**.
5. Apply the app to a device label.
6. Create a VPN configuration for Android Enterprise.
   a. Click **Policies & Configurations > Configurations**.
   b. Select **Add New > VPN**. The Add VPN Setting dialog box opens.
   c. Select a Connection Type in the drop-down:
      - Cisco Legacy AnyConnect
      - OpenVPN
      - F5 SSL
      - Pulse Secure SSL
      - MobileIron Tunnel (Samsung KNOX Workspace)
   d. Select the **Samsung Knox** check box.
   e. Select the **Deploy inside Knox Workspace** check box.
   f. Select the Per-app VPN **Yes** radio button.
   g. **Save** the new configuration.
7. Import another app and install this app for Android enterprise. In the Per App VPN Settings section, select the new perApp VPN you created.

Next steps

Move Android enterprise in-house apps to inside Knox Workspace

Move Android enterprise in-house apps to inside Knox Workspace

Once you have set up VPN for Knox Workspaces, you can move in-house apps from outside of the workspace to inside the Knox workspace. This is applicable to:

- corporate-owned personal-enabled (COPE) mode on Android devices with an activated KNOX premium license.
- devices with Knox version 3.x and above only.

You cannot copy or move apps from the personal side of the device into corporate-owned personal-enabled (COPE) mode or Work Profile mode on Samsung devices. The in-house apps should be assigned to a device label so they can be installed in a personal (outside of the container) space. This Android enterprise-only capability allows you to move previously-installed in-house apps into the container (Knox V3 workspace) using whitelisting of apps in the Android Enterprise configuration. The app being moved must be whitelisted prior to moving inside the Knox workspace, see Android Samsung Knox Container Settings on page 391.

Procedure

This procedure is applicable for Android OS version 8.0 through the most recently released version as supported by MobileIron.

1. Complete the procedure in Creating per container Android enterprise VPN with Knox 3 workspace or Creating per app Android enterprise VPN with Knox 3 workspace.
2. Add a new Android Enterprise app in the App Catalog.
3. Apply the app to a device label.
4. If needed, force device check in.
5. In Policies & Configs > Configurations, **Edit** the Android enterprise configuration and select the **Move In-House app into workspace** check box.
6. In the Package Name field, select the name of the app or hold the Shift key down and select multiple apps.
7. Click **Save**.

On the device, the app is moved to the Knox Workspace. In the device's Settings > Workspace option, the Install apps option is disabled.

Remove Android enterprise apps from Knox Workspace

If the whitelist of apps is modified and an app is no longer listed inside the Knox workspace, that app will be moved back to the personal space. If the whitelist of apps is removed, all previously installed in-house apps will be moved back into the personal space.

Procedure

1. In **Policies & Configs > Configurations**, **Edit** the Android enterprise configuration.
2. In the Package Name field, de-select the name of the app or hold the Shift key down and de-select multiple apps.
3. Click **Save**.
4. Force device check in.

On the device, the app is moved out of Knox Workspace to the personal space.

Configuring VPN modes when VPN client is inside the Knox container

If the VPN client is installed inside the Knox container, you can configure the VPN client to be used in one of these modes:

- per-device, but when the VPN client is installed inside the Knox container, per-device mode is really another way to configure per-container mode. Apps outside the container cannot use the VPN client.
- per-container
- per-app

The following table provides an overview of what you need to configure for each mode.

	per-device mode	per-container mode	per-app mode
Description	The VPN client configured for per-device use can be used by any apps inside the Knox container. Therefore, per-device mode when the VPN client is inside the container ***is really a way of configuring per-container mode***.	The VPN client configured for per-container use can be used by any apps inside the Knox container.	The VPN client configured for per-app use can be used only by apps specifically configured to use it. The apps can be either inside or outside the Knox container.
VPN setting	Options in VPN setting: • **per-app VPN**: No • **Samsung Knox:** Selected • **Deploy inside Knox Workspace**: Selected Apply label to VPN setting	Options in VPN setting • **per-app VPN**: Yes • **Samsung Knox**: Selected • **Deploy inside Knox Workspace**: Selected Apply label to VPN setting	Options in VPN setting • **per-app VPN**: Yes • **Samsung Knox**: Selected • **Deploy inside Knox Workspace**: Selected Apply label to VPN setting
App in App Catalog	• App label is not applicable to VPN usage • **Per App VPN Settings** in app: not applicable	• App label is not applicable to VPN usage • **Per App VPN Settings** in app: not applicable	For apps outside the Knox container: • Apply label to app • **Per App VPN Settings** in app: set to VPN setting
Samsung Knox Container setting	• Include the VPN client in the **Apps** section. **Note:** Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container. • Apply label to Samsung Knox Container setting	• Include the VPN client in the **Apps** section. **Note:** Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container. • In the **App Settings** section, in the **VPN** field, select the VPN setting from the drop-down list. • In the **Apps** section, for a specific app, make no VPN selection. • Apply label to Samsung Knox Container setting	• Include the VPN client in the **Apps** section. **Note:** Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container. • For apps inside the container, in the **Apps** section, for the specific app, select the VPN setting from the drop-down list. • In the **App Settings** section, in the VPN field, make no selection. • Apply label to Samsung Knox Container setting

VPN Behavior on the Device

When a VPN setting is installed on a device, the following behavior is observed:

- The VPN client displays its VPN connection status in the notifications bar.
- For per-app VPN configurations, the connection is automatically established when the user opens an app or accesses data that requires the connection.
- For per-device VPN, the user must manually establish the connection through the VPN client app.

Disconnecting or attempting to remove VPN behaves as follows:

- A user cannot disconnect a per-app or per-container VPN connection manually. The connection is automatically disconnected if:
  - Device is removed from the label that provides VPN.
  - Device is retired.
- A user can disconnect a per-device VPN connection manually.
- A user cannot uninstall a VPN client on Samsung devices if a VPN connection exists using the client.

Usage Notes

For all VPN clients:

- Knox 1.2 supports using per-app VPN outside of the Knox container, but not inside. Per-device VPN works inside Knox 1.2 container.
- Knox 2.0 through the mostly recently released version as supported by MobileIron is required to use per-app VPN inside of the Knox container. Per-device VPN is not available inside these versions of the Knox container.

For the F5 BIG-IP Edge Client, Pulse Secure (previously Junos Pulse), OpenVPN, and Cisco AnyConnect:

- To use per-app VPN with Pulse Secure, F5 BIG-IP Edge Client, OpenVPN, or Cisco AnyConnect, you must select Samsung Knox in the VPN Settings. An invalid configuration can result if Samsung Knox is not selected.

For Juniper (Pulse Secure, previously Junos Pulse):

- For the Pulse Secure client, the user must accept the app's EULA before Mobile@Work can install the VPN setting.
- To use Pulse Secure for per-app VPN, a license is required from Juniper Networks that is applied to the VPN gateway.
- Mobile@Work supports the PulseSecure client, not the "Junos for Samsung" client.

Regarding migrating to Pulse Secure from Junos Pulse:

Only Mobile@Work 9.0.0.0 and prior prompts the device user to install Pulse Secure if the device is using the Junos Pulse VPN app. Otherwise, device users are not prompted, but can uninstall the Junos Pulse app and then install Pulse Secure. When Junos Pulse is uninstalled, the Junos Pulse configurations will be removed only if the device is running Mobile@Work 9.0.0.0 or prior.

If you prefer device users to be prompted to migrate, MobileIron recommends users stay on Mobile@Work 8.5 (8.5.0.0 through 8.5.0.3) until after they have upgraded to Pulse Secure. See the migration instructions in the following documents.

- "Junos Pulse to Pulse Secure Migration: Configuring a Custom SSL VPN Config in MobileIron Core": https://community.mobileiron.com/docs/DOC-1755
- "Action Required by September 30, 2015 to Support Junos Pulse VPN on Newly Enrolled iOS and Android Devices": https://community.mobileiron.com/docs/DOC-3097

Limitations for VPN connections and settings

- Per-container VPN for the Knox container cannot be combined with per-app VPN for apps inside the container. You must choose to use one VPN mode or the other.

  To do so, in the **New Samsung Knox Container Setting** dialog, you must either provide a VPN selection for individual apps in the **Apps** section, or provide a VPN selection in the **App Settings** section, but not both
- Mobile Iron recommends using a single VPN client and a single VPN connection per device.

How to set up VPN for apps both outside and inside the Knox container

In Knox 2.0 through the most recently released version as supported by MobileIron, when you install a VPN client outside of the Knox container, a per-device VPN does not provide VPN inside the Knox container. If you want VPN working for apps both inside and outside the Knox container when the VPN client is outside the Knox container, set up:

- a per-device VPN for apps outside of the container, and
- a per-container VPN for the apps inside of the container.

We recommend using the same VPN client for each. You will need to create a separate VPN setting for each, however. One VPN setting sets its per-app VPN option to yes, and the other sets it to no.

See Configuring VPN modes when VPN client is outside the Knox container on page 236.

Using certificates with VPN

When using certificates with VPN settings, depending on the VPN client, you will need to add the certificate in the VPN setting, and in some cases also assign the certificate to a label.

The following tables indicate the rules for each VPN client and certificate type.

VPN Client	Rules for User Authentication Certificates
Pulse Secure (previously: Junos Pulse), OpenVPN	Provide user authentication certificate in the VPN setting. Apply certificate to a label.
Mocana KeyVPN, F5 Big-IP Edge Client	Provide user authentication certificate in the VPN setting only. Do not apply certificate to a label.

VPN Client	Rules for CA (Root) Certificates
Pulse Secure (previously: Junos Pulse), F5 Big-IP Edge Client	Apply CA certificate to a label.
Mocana KeyVPN, OpenVPN	Provide CA certificate in the VPN setting only. Do not apply certificate to a label.

SonicWall Mobile Connect

Use the following guidelines to configure SonicWall Mobile Connect.

TABLE 51. SONICWALL MOBILE CONNECT SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	**Provide a description that clarifies the purpose of these settings.**
Connection Type	Select SonicWall Mobile Connect.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **None**, **Manual**, or **Automatic** to configure a proxy. If you select **Manual**, you must specify the proxy server name and port number. If you select **Automatic**, you must specify the proxy server URL.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Server	*Manual Proxy* Enter the name for the proxy server.
Proxy Server Port	*Manual Proxy* Enter the port number for the proxy server.
Type	*Manual Proxy* Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	*Manual Proxy* If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	*Manual Proxy* If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	The VPN will only proxy for the domain and domain suffixes specified here

TABLE 51. SONICWALL MOBILE CONNECT SETTINGS (CONT.)

Item	Description
	(`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
User Name	Specify the user name to use for authentication. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select **Password** or **Certificate**.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$.
Identity Certificate	Certificate authentication. Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.
VPN on Demand	Certificate authentication. Select to enable the VPN on Demand section. Click **Add New** to specify a domain or hostname and the preferred connection option.
Per-app VPN	Select **Yes** to create a per-app VPN setting. Per-app VPN is supported for devices running iOS 7 through the most recently released version of iOS as supported by MobileIron. You must update your VPN software to a version that supports iOS 7 features. An additional license may be required for this feature. You cannot delete a per-app VPN setting that is being used by an app. Remove the per-app VPN setting from the app before you delete the setting. You can enable per-app VPN for an app when you: • add the app in the App Catalog. • edit an in-house app or an App Store app in the App Catalog. See the MobileIron Apps@Work Guide for information about how to add or edit iOS apps.
Provider Type	

TABLE 51. SONICWALL MOBILE CONNECT SETTINGS (CONT.)

Item	Description
On Demand Rules (VPN on Demand, iOS 7 through the most recently released version of iOS as supported by MobileIron.) VPN On Demand rules are applied when the device's primary network interface changes, for example when the device switches to a different Wi-Fi network. Note the following: • A matching rule is not required. The Default Rule is applied if a matching rule is not defined. • If you select Evaluate Connection, a matching rule is not required. • You can create up to 10 On Demand matching rules. • For each matching rule you can create up to 50 Type and Value pairs.	
Add New Matching Rule	Click to add a new On Demand matching rule.
Action	Select one of the following actions to apply to the matching rule: • Connect • Disconnect • Allow • Ignore • Evaluate Connection
Add New	Click to add a new Type Value pair.
-	Click to delete either an On Demand rule, or a matching rule.
Matching Rules: For each matching rule to which the action is applied enter the type and value pair.	
Type	Select from one of the following key types: • DNS Domain • Interface Type • DNS Server Address • SSID • URL String Probe
Value	For each key selected, enter a value. DNS Domain—Enter a list of domain names to match against the domain being accessed. Wildcard '*' prefix is supported, e.g. *.example.com would match anything.example.com Interface Type—Enter either Wifi or Cellular. DNS Server Address—Enter a list of DNS servers to match against. All DNS servers have to match the device's current DNS servers or this match will fail. Wildcard '*' is supported, e.g. 1.2.3.* would match any DNS servers with 1.2.3. prefix. SSID—Enter a list of SSIDs to match against the current network. If the network is not a Wi-Fi network or if its SSID does not appear in the list, the

TABLE 51. SONICWALL MOBILE CONNECT SETTINGS (CONT.)

Item	Description
	match will fail. URL String Probe—Enter a URL to a trusted HTTPS server. This is used to probe for reachability. Redirection is not supported.
Description	Enter additional information about this matching rule.
Domain Action	Only appears if the Action is Evaluate Connection. Select one of the following Actions for the domain: • Connect if needed—The specified domains trigger a VPN connection attempt if domain name resolution fails. For example: The DNS server indicates that it cannot resolve the domain, or responds with a redirection to a different server, or fails to respond (timeout). • Never connect—The specified domains do not trigger a VPN connection attempt.
Action Parameters: Only appears if the Action is Evaluate Connection. Define the Evaluation Type and Value pair.	
Evaluation Type	Select the Evaluation type as one of the following: • Domain (Required) • Required DNS Server (only available with Connect if needed) • Required URL Probe (only available with Connect if needed)
Value	Enter the value for the evaluation type selected. Domain—Enter a list of domains for which this evaluation applies. Wildcard prefixes are supported, for example, *.example.com. Required DNS Server—Enter a list of IP addresses of DNS servers to use for resolving the domains. These servers do not need to be part of the device's current network configuration. If these DNS servers are not reachable, VPN is triggered. Either configure an internal DNS server or trusted external DNS server. Required URL Probe—Enter an HTTP or HTTPS (preferred) URL. The device to probes this URL using a GET request. The probe is successful if the DNS resolution for this server is successful. VPN is triggered if the probe fails.
Description	Enter additional information about this Evaluation Type and Value pair.
Default Rule: The default rule (action) is applied to a connection that does not match any of the matching rules.	
If none of the rules above match or if there is no rule defined, choose VPN connection to:	Select the action for the Default Rule.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

NetMotion Mobility VPN (iOS)

This VPN mode is for iOS devices only.

Managing Certificates and Configuring Certificate Authorities

This section addresses components related to managing certificates and certificate authorities.

Certificates overview

MobileIron is capable of distributing and managing certificates.

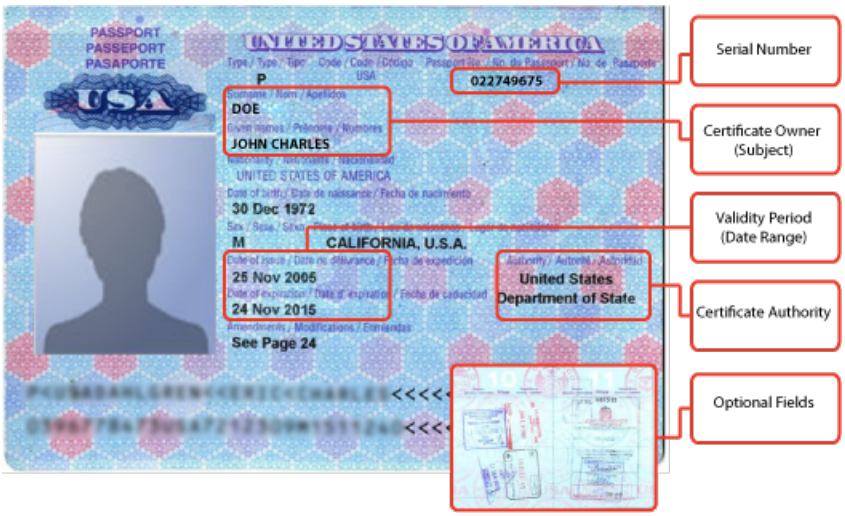
Certificates are mainly used for the following purposes:

- Establishing secure communications
- Encrypting payloads
- Authenticating users and devices

Certificates establish user identity while eliminating the need for users to enter user names and passwords on their mobile devices. Certificates streamline authentication to key enterprise resources, such as email, Wi-Fi, and VPN. Some applications require the use of certificates for authentication.

The following diagram compares a certificate to a passport:

FIGURE 8. COMPARING CERTIFICATES TO A PASSPORT



The certificate includes information that identifies the following information:

- the issuing certificate authority
- acceptable uses for the certificate
- information that enables the certificate to be validated.

The MobileIron solution provides the flexibility to use MobileIron Core as a local certificate authority, an intermediate certificate authority, or as a proxy for a trusted certificate authority.

Types of certificates

MobileIron uses the following types of certificates:

TABLE 52. CERTIFICATE TYPES

Certificate type	Description
Portal HTTPS	The identify certificate and its certificate chain, including the private key, that identifies MobileIron Core, allowing a client (such as a browser or app) to trust MobileIron Core. Typically, this certificate is the same certificate as the Client TLS and iOS Enrollment certificates. Core sends this certificate to the client as part of the TLS handshake over port 443 or 8443 when the client initiates a request to Core. NOTE: This certificate must be a publicly trusted certificate from a well-known Certificate Authority if you are using mutual authentication. **Related topics** "Certificates you configure on the System Manager" in the MobileIron Core System

TABLE 52. CERTIFICATE TYPES (CONT.)

Certificate type	Description
	Manager Guide
Client TLS	The identify certificate and its certificate chain, including the private key, that identifies MobileIron Core, allowing Mobile@Work for iOS and Android to trust MobileIron Core. Typically, this certificate is the same certificate as the Portal HTTPS and iOS Enrollment certificates. Core sends this certificate to Mobile@Work for iOS or Android as part of the TLS handshake over port 9997 when Mobile@Work initiates a request to Core. **Related topics** "Certificates you configure on the System Manager" in the MobileIron Core System Manager Guide
MobileIron Core server SSL	Can be either self-signed or third-party certificates. By default, Core generates self-signed certificates. You can use trusted certificates from third-party certificate providers such as Verisign, Thawte, or Go Daddy. Kerberos and Entrust certificates are also supported.
Sentry server SSL	Identifies the Sentry to the client and secures communication, over port 443, between devices and the Sentry.
Client identity	Verifies the identity of users and devices and can be distributed through Certificate Enrollment.

Samsung Knox devices and certificates managed by MobileIron Core

Certificates managed by MobileIron Core are automatically removed from a Samsung Knox device when the device is retired, or when the label that applied the certificate to the device is removed from the certificate.

Managing certificates issued by certificate enrollment configurations

MobileIron Core runs a process each day at 3:45 am that manages all certificates issued using certificate enrollment configurations.

Certificates have a limited lifetime that is defined when certificates are issued. When the certificate lifetime is within the expiry window (60 days, by default), MobileIron Core does not automatically renew the certificates. Only a forced manual renewal/creation is possible.

Re-issued certificates are sent to the managed device configuration and the expiring certificates become inactive. The inactive certificates are purged from the system once the certificates are expired or confirmed to be revoked.

Supported certificate scenarios

MobileIron supports the following certificate scenarios:

- MobileIron Core as a certificate authority
- Using MobileIron Core as a certificate proxy
- Using MobileIron Core as a certificate enrollment reverse proxy
- Kerberos constrained delegation

MobileIron Core as a certificate authority

You can configure MobileIron Core as a local certificate authority (CA) for the following scenarios:

- Core as an Independent Root CA (self-signed)—Configure Core as an independent root certificate authority if you are using a self-signed certificate. Use this option if your company does not have its own certificate authority and you are using Core as the certificate authority.
- Core as an Intermediate CA—Use this option when your company already has its own certificate authority. Using Core as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.

Using MobileIron Core as a certificate proxy

MobileIron Core can act as a proxy to a 3rd party CA by using APIs exposed by the 3rd party CA or the SCEP protocol to obtain certificates required by a Certificate Enrollment. This enables you to configure certificate-based authentication for devices.

Using Core as a certificate proxy has the following benefits:

- Certificate verifies Exchange ActiveSync, Wi-Fi and/or VPN connections, eliminating the need for passwords that are complex to manage
- MobileIron can manage certificates by checking status against a CA's CRL, deactivating revoked certificates and requesting replacement when certificates are about to expire
- MobileIron can detect and address certificate renewal and ensure that devices cannot reconnect to enterprise resources if they are out of compliance with company policies.
- Simplified enrollment with the following:
  - MS Certificate Enrollment
  - Entrust
  - Local CA
  - Symantec Managed PKI
  - User provided certificates
  - Open Trust
  - Symantec Web Services Managed PKI

The following applications are supported.

- ActiveSync is supported with Email+ and TouchDown
- VPN is supported on Android with Cisco AnyConnect .
- Wi-Fi.

The following certificates are supported for Android devices:

- Microsoft NDES Certificate Enrollment
- Entrust
- Local CA
- Symantec Managed PKI
- User provided certificates
- Open Trust
- Symantec Web Services Managed PKI
- Client-Provided certificates
- Client-provided certificates using the native SCEP client on iOS

For information about how to create certificate enrollment settings in MobileIron Core, see Certificate Enrollment settings on page 271.

Using MobileIron Core as a certificate enrollment reverse proxy

Identity certificates with Microsoft Certificate Enrollment are supported. A root or intermediate certificate from a trusted certificate authority (CA) is required, and you must set up MobileIron Core to act as a SCEP reverse proxy.

Windows devices originate the certificate request. When the Windows device requests a certificate, the MobileIron Core acts as a Certificate Enrollment reverse proxy and communicates with the Certificate Enrollment server to deliver the certificate to the device.

Kerberos constrained delegation

You can use Kerberos constrained delegation (KCD) for authenticating the device to the ActiveSync server, the app server, and to Sentry.

For detailed information about how to configure MobileIron to use Kerberos authentication, see, “Device and server authentication support for Standalone Sentry” in the MobileIron Sentry Guide.

MobileIron Core as a certificate authority

You can configure MobileIron Core as a local certificate authority for the following scenarios:

- **MobileIron Core as an Independent Root CA (self-signed)**—Configure MobileIron Core as an independent root certificate authority if you are using a self-signed certificate. Use this option if your company does not have its own certificate authority and you are using MobileIron Core as the certificate authority.
  See Configuring MobileIron Core as an independent root CA (Self-Signed) on page 257.
- **MobileIron Core as an Intermediate CA**—Use this option when your company already has its own certificate authority. Using MobileIron Core as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.
  See Configuring MobileIron Core as an intermediate CA on page 260.

Configuring MobileIron Core as an independent root CA (Self-Signed)

Configuring MobileIron Core as an independent root CA requires configuring your infrastructure to trust Core as an independent root CA.

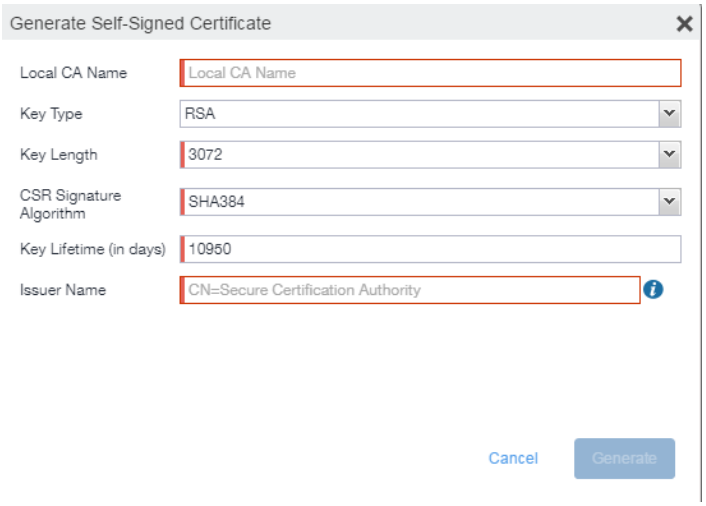
To configure MobileIron Core as an independent root CA, you must follow these basic steps:

1. Generate a self-signed certificate
   See Generating a self-signed certificate on page 257.
2. Create a local CA certificate enrollment setting for the self-signed certificate
   See Creating a local certificate enrollment setting on page 259.

Generating a self-signed certificate

To generate the self-signed certificate:

1. Log into the Admin Portal.
2. Go to **Services > Local CA**.
3. Select **Add > Generate Self-Signed Cert**.



4. Enter the following information.
   - **Local CA Name**: Enter a recognizable name to identify the self-signed certificate. This name will appear in the list of local certificate authorities in **Services > Local CA**.
   - **Key Type**: Specify the key type. The options are RSA (default) or Elliptical Curve.
   - **Key Length**: Specify the key length. The values are 2048, 3072 (the default), and 4096. The longer the key length, the more secure the certificate.
   - **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (default), and SHA512.
     - **Key Lifetime (in days)**: Enter number of days. The key will expire after the entered number of days.

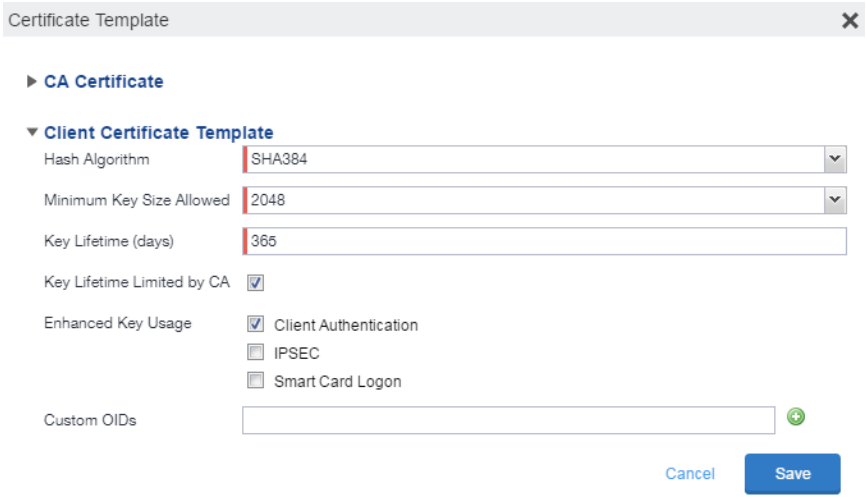
       The default is 10,950 days. MobileIron recommends 5 years or longer; 61 days is the minimum.
     - **Issuer Name**: Requires an X.509 name. For example, CN=www.yourcompany.com, DC=yourcompany, DC=com.

       The **Issuer Name** field uses an X.509 distinguished name. You can use one or more X.509 codes, separated by commas. The following table describes the valid codes for the Issuer Name field:

Code	Name	Type	Max Size	Example
C	Country/Region	ASCII	2	C=US
DC	Domain Component	ASCII	255	DC=company, DC=com
S	State or Province	Unicode	128	S=California
L	Locality	Unicode	128	L=Mountain View
O	Organization	Unicode	64	O=Company Name, Inc.
OU	Organizational Unit	Unicode	64	OU=Support
CN	Common Name	Unicode	64	CN=www.company.com

If you have a registered DNS name that you use to send SMTP mail, a best practice is to use the domain component convention and the DNS name for the certificate name.

5. Click **Generate**.



6. Configure the **Client Certificate Template**.

   Values depend on the purpose for the certificate and the requirements of your environment.

   - **Hash Algorithm**: The larger the hash number, the more secure. The options are SHA256, SHA384 (default), SHA512—part of the SHA2 secure hash algorithm family required for U.S. government applications. The number signifies the output bits.
   - **Minimum Key Size Allowed**: The longer the key length is, the more secure the certificate.
   - **Key Lifetime (days)**: 365 days or longer is recommended; 61 days is the minimum.
   - **Key Lifetime limited by CA**: Select to use the key lifetime specified for the self-signed CA. MobileIron recommends enabling this option. Enabling this option ensures that client certificate validity periods do not exceed the life time of the issuing CA certificate.
   - **Enhanced Key Usage**: When a certificate is presented to an application, the application can require the presence of an Enhanced Key Usage OID specific to that application. Leave these deselected if you do not have any applications that require additional OIDs.
   - **Custom OIDs**: If you are using this certificate for SSL authentication, enter the OID in this field.

7. Click **Save**.

   The newly created self-signed certificate will be listed in **Services > Local CA**.

Creating a local certificate enrollment setting

After you have generated the self-signed certificate, you need to create a local CA certificate enrollment setting for the self-signed certificate. Creating a local CA certificate enrollment setting enables proxy functionality so that MobileIron Core generates the certificates and caches the generated keys.

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations.**
3. Click **Add New > Certificate Enrollment > Local**.

For more information on configuring the settings, see Certificate Enrollment settings on page 271.

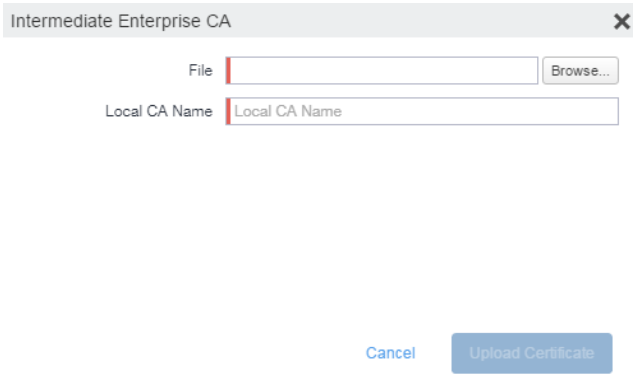
Configuring MobileIron Core as an intermediate CA

When you configure Core as an intermediate certificate authority, the managed device users can authenticate to servers within your company intranet; not just the MobileIron system.

After you get the certificate from your certificate vendor, you can add the certificates to MobileIron Core to create the intermediate certificate authority (CA).

Procedure

1. In the MobileIron Core Admin Portal go to **Services > Local CA**.
2. Click on **Add > Intermediate Enterprise CA**.



3. Click **Browse** and navigate to the combined file.
4. Click **Open**.
5. Enter a recognizable name in the **Local CA Name** field.
6. Click **Upload Certificate**.
   Your local certificate authority is now available to use. The local CA will be listed in **Services > Local CA**.

Mutual authentication between devices and MobileIron Core

MobileIron Core supports mutual authentication, which means that not only must the device trust MobileIron Core, but MobileIron Core must trust the device. Therefore, with mutual authentication, a registered device can continue to communicate with Core only if the device provides the right certificate to Core. Mutually authenticated communication between the device and MobileIron Core enhances security.

NOTE: A device authenticating to Core with a certificate is also known as certificate-based authentication to Core.

Scenarios that can use mutual authentication

The device can present a client identity certificate to MobileIron Core in the following cases:

TABLE 53. MUTUAL AUTHENTICATION USAGE BY PLATFORM

Platform	Mutual Authentication usage
iOS	• Mobile@Work for iOS device check-in • AppConnect for iOS check-in • iOS MDM device check-in • Apps@Work for iOS communication
macOS	• Mobile@Work for macOS device check-in • macOS MDM device check-in
Android	• Mobile@Work for Android device check-in, which includes AppConnect check-in • Apps@Work for Android communication
Windows 10	• Device check-in

NOTE: Mutual authentication is not possible at the time Mobile@Work registers with Core, because the device receives its identity certificate during the registration process.

Core port usage with devices, with and without mutual authentication

The following table summarizes MobileIron Core port usage for registration and further communication with devices. The port usage for some cases is different depending on whether mutual authentication is enabled.

TABLE 54. CORE PORT USAGE WITH DEVICES WITH AND WITHOUT MUTUAL AUTHENTICATION

	Without mutual authentication	With mutual authentication
Mobile@Work for iOS	9997	443
Mobile@Work for Android	9997	443
Mobile@Work for macOS	Not applicable. Mobile@Work for macOS always uses mutual authentication with Core.	443
iOS and macOS MDM agent provisioning and agent check-in	443	443
Windows 10	Not applicable. Windows 10 always uses mutual authentication with Core.	443

NOTE: Port 9997 is configurable in the System Manager in Settings > Port Settings > Sync TLS Port. However, changing the port is rare.

The mutual authentication setting on MobileIron Core

The setting on MobileIron Core to enable mutual authentication is in the Admin Portal in **Settings > System Settings > Security > Certificate Authentication.** Whether the setting is automatically selected on new installations and upgrades is described by the following table.

TABLE 55. SETTING FOR MUTUAL AUTHENTICATION ON NEW INSTALLS AND UPGRADES

	Setting to enable mutual authentication
New installations	Not selected. Mutual authentication is **not** enabled.
Upgrade from a previous version of Core in which mutual authentication was **not** enabled. Or Upgrade from a version of Core prior to Core 9.7.0.0 in which the Android mutual authentication setting was **not** enabled.	Not selected. Mutual authentication is **not** enabled.
Upgrade from a previous version of Core in which mutual authentication **was** enabled. Or Upgrade from a version of Core prior to Core 9.7.0.0 in which the Android mutual authentication setting **was** enabled.	Selected. Mutual authentication **is** enabled.

IMPORTANT: Once mutual authentication is enabled on Core, it cannot be disabled.

The mutual authentication setting impacts mutual authentication usage only on:

- Mobile@Work for Android
- Apps@Work for Android
- However, to enable mutual authentication for Apps@Work for Android:
  - You must also select **Certificate Authentication** for Apps@Work at **Apps > Apps@Work Settings > App Storefront Authentication**.
  - The device must be using Mobile@Work 10.2.0.0 for Android through the most recently released version as supported by MobileIron.
- Mobile@Work 9.8 for iOS through the most recently released version as supported by MobileIron
- iOS MDM
- macOS MDM

The mutual authentication setting has no impact on mutual authentication usage on:

- Versions of Mobile@Work for iOS prior to Mobile@Work 9.8

  These versions of Mobile@Work for iOS **never** use mutual authentication.
- Apps@Work for iOS

  Apps@Work for iOS uses mutual authentication if you select **Certificate Authentication** for Apps@Work at **Apps > Apps@Work Settings > App Storefront Authentication**.
- Mobile@Work for macOS

  Mobile@Work for macOS **always** uses mutual authentication.

- Windows 10 devices

  Windows 10 devices **always** uses mutual authentication.

When devices use mutual authentication

Whether devices use mutual authentication depends on:

- the device platform
- whether mutual authentication was enabled before upgrade
- whether mutual authentication is enabled after upgrade
- whether mutual authentication is enabled after a new installation
- for Mobile@Work for iOS, the version of Mobile@Work

The following table summarizes when devices use mutual authentication and the port they use in communication with MobileIron Core.

TABLE 56. CORE MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION

	New Core installation **or** **Core upgrade in which: MA setting was NOT enabled before upgrade**	**New Core installation in which you enable MA setting after installation.** **or** **Core upgrade in which: MA setting was NOT enabled before upgrade but you enable it after the upgrade.**	**Core upgrade in which:** **MA setting WAS enabled before upgrade**
Mutual authentication setting	Not enabled	Enabled	Enabled
Device client			
Android: Mobile@Work (all Mobile@Work versions that Core supports)	Port: 9997 MA: not used	Devices that register after enabling MA: • Port: 443 • MA: used Devices that were already registered: • Port: 9997 • MA: not used.	Port: 443 MA: used
iOS: Mobile@Work 9.8	Port: 9997 MA: not used	Devices that register after enabling MA: • Port: 443	Devices that register after enabling MA: • Port: 443

TABLE 56. CORE MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION (CONT.)

	New Core installation **or** **Core upgrade in which: MA setting was NOT enabled before upgrade**	**New Core installation in which you enable MA setting after installation.** **or** **Core upgrade in which: MA setting was NOT enabled before upgrade but you enable it after the upgrade.**	**Core upgrade in which:** **MA setting WAS enabled before upgrade**
through the most recently released version as supported by MobileIron		• MA: used Devices that were already registered: • Port: 9997 • MA: not used.	• MA: used Devices that were already registered: • Port: 9997 • MA: not used.
iOS: Mobile@Work versions prior to 9.8	Port: 9997 MA: not used	Port: 9997 MA: not used	Port: 9997 MA: not used
iOS: iOS MDM check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used.
macOS: Mobile@Work	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used
macOS macOS MDM agent check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used
Windows 10	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used

NOTE: On new MobileIron Core installations (not upgrades), if you enable mutual authentication **before any devices register**, you can disable port 9997 (in the System Manager in Settings > Port Settings > Sync TLS Port) because it is not used. If devices were registered before enabling mutual authentication, disabling the port causes those devices to not be able to check-in.

Mutual authentication identity certificate for MobileIron Core

You provide an identity certificate for MobileIron Core to use in mutual authentication in the Portal HTTPS certificate. You configure this certificate on the System Manager at **Security > Certificate Mgmt.** The certificate is the identify certificate and its certificate chain, including the private key, that identifies MobileIron Core, allowing

the devices to trust MobileIron Core. This certificate must be a publicly trusted certificate from a well-known Certificate Authority when using mutual authentication.

Mutual authentication client identity certificate

You enable mutual authentication for iOS and Android devices in the Admin Portal in **Settings > System Settings > Security > Certificate Authentication.** When enabling that setting, you specify a certificate enrollment setting. The certificate enrollment setting specifies how the identity certificate that the device will present to Core is generated.

By default, the certificate enrollment setting for mutual authentication is generated with Core as a local Certificate Authority (CA). Most customers use the default selection. However, if necessary due to your security requirements, you can instead specify a SCEP certificate enrollment setting that you create.

IMPORTANT:

- If you use a SCEP certificate enrollment setting for mutual authentication, you cannot use it for any other purpose. For example, you cannot use it in VPN or wi-fi configurations.
- If you use a SCEP certificate enrollment setting that uses an intermediate CA, make sure that all the intermediate CA certificates and the root CA certificate are included in MobileIron Core's trusted root certificates. See "Managing trusted certificates" in the Getting Started with MobileIron Core
- See:
  - Handling client identity certificate expiration for Android devices
  - Handling client identity certificate expiration for iOS devices

Handling client identity certificate expiration for Android devices

Mobile@Work 10.1 for Android handles the expiration of the client identity certificate used for mutual authentication between Mobile@Work for Android and MobileIron Core. In the Admin Portal, on the sync policy for the device, specify a renewal window for the certificate. The renewal window is a number of days prior to the certificate expiration. When Mobile@Work determines the renewal window has begun, it requests a new certificate from Core.

If Mobile@Work is out of contact with Core during the renewal window, but is in contact again within 30 days after the expiration, Mobile@Work requests a new certificate from Core.

If Mobile@Work is not in contact with Core either during the renewal window or within 30 days after the expiration, the device will be retired and will need to re-register with Core.

Mobile@Work versions prior to 10.1 do not support certificate expiration. When the certificate expires, the device user must re-register Mobile@Work.

Procedure

1. In the Admin Portal, go tos **Policies & Configs > Policies**.
2. Select the appropriate sync policy.
3. For **Mutual Certificate Authentication Renewal Window**, enter the number of days prior to the expiration date that you want to allow devices to renew their identity certificate. Enter a value between 1 and 60.

   NOTE: A blank value defaults to 60 days.
4. Click **Save**.
5. Click **OK**.

Handling client identity certificate expiration for iOS devices

Mobile@Work 11.1.0 for iOS handles the expiration of the client identity certificate used for mutual authentication between Mobile@Work for iOS and MobileIron Core version 10.3.0.0 through the most recently released version as supported by MobileIron. In the Admin Portal, on the sync policy for the device, specify a renewal window for the certificate. The renewal window is a number of days prior to the certificate expiration. When Mobile@Work determines the renewal window has begun, it requests a new certificate from Core.

If Mobile@Work is out of contact with Core during the renewal window, but is in contact again within 30 days after the expiration, Mobile@Work requests a new certificate from Core.

If Mobile@Work is not in contact with Core either during the renewal window or within 30 days after the expiration, the device will be retired and will need to re-register with Core.

Mobile@Work versions prior to 11.1.0 do not support certificate expiration. When the certificate expires, the device user must re-register Mobile@Work.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the appropriate sync policy.
3. For **Mutual Certificate Authentication Renewal Window**, enter the number of days prior to the expiration date that you want to allow devices to renew their identity certificate. Enter a value between 1 and 60.

   NOTE: A blank value defaults to 60 days.
4. Click **Save**.
5. Click **OK**.

Mutual authentication and Apps@Work

Both Apps@Work for Android and Apps@Work for iOS can use mutual authentication.

Apps@Work for iOS uses mutual authentication if you select **Certificate Authentication** at **Apps > Apps@Work Settings > App Storefront Authentication**. It does *not* depend on the mutual authentication setting at **Settings > System Settings > Security > Certificate Authentication.**

However, Apps@Work for Android uses mutual authentication only if you do both of the following:

- Select **Certificate Authentication** at **Apps > Apps@Work Settings > App Storefront Authentication**.
- Enable the mutual authentication setting at **Settings > System Settings > Security > Certificate Authentication.**

Related topics

- "Setting up Apps@Work for iOS and macOS" in the *MobileIron Apps@Work Guide*
- "Apps@Work in Mobile@Work for Android in the *MobileIron Apps@Work Guide*

Enabling mutual authentication for Apple and Android devices

The MobileIron Core mutual authentication setting enables mutual authentication for:

- Mobile@Work for Android
- Apps@Work for Android
  - You must also select **Certificate Authentication** for Apps@Work at **Apps > Apps@Work Settings > App Storefront Authentication**.
  - The device must be using Mobile@Work 10.2.0.0 for Android through the most recently released version as supported by MobileIron.
- Mobile@Work 9.8 for iOS through the most recently released version as supported by MobileIron
- iOS MDM
- macOS MDM

Note The Following:

- The setting is automatically enabled in the cases described in The mutual authentication setting on MobileIron Core.
- **After you enable mutual authentication, you cannot disable it.**

Before you begin

1. As discussed in in Mutual authentication client identity certificate, create a SCEP certificate enrollment setting if you do not want to use the default local certificate enrollment setting for mutual authentication. The SCEP setting must select the **Decentralized** option. For details, see Certificate Enrollment settings.

   NOTE: When you enable mutual authentication, change the certificate enrollment selection for mutual authentication ***before any more devices register***. Any devices already registered and using mutual authentication will not be able to check-in with Core. Those

devices will need to re-register with Core. Note that devices already registered but not using mutual authentication can continue to check-in.

2. If you are using iOS devices with the Apps@Work web clip using certificate authentication, change the **Apps@Work Port** field in the System Manager in **Settings > Port Settings**. MobileIron recommends port 7443. However, you can use any port except the port that the Admin Portal uses, which is either 443 or 8443, which you specify in the **MIFS Admin Port** field in the System Manager in **Settings > Port Settings**.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Security > Certificate Authentication.**
2. Select **Enable client mutual certification on Android client, iOS client and Apple MDM communication**.
3. In the **Certificate Enrollment Configuration** field, most customers use the default selection. Otherwise, select a SCEP certificate enrollment setting.
4. Click **Save**.

Related topics

- “Setting up Apps@Work for iOS and macOS” in the *MobileIron Apps@Work Guide*
- "Port settings" in the *MobileIron Core System Manager Guide*
- “Apps@Work for Android authentication to MobileIron Core” in the *MobileIron Apps@Work Guide*

Enabling TLS inspecting proxy support when using mutual authentication

Contact MobileIron Professional Services or a MobileIron certified partner to set up this deployment.

MobileIron Core can support a TLS inspecting proxy to handle HTTPS requests from your devices to MobileIron Core when using mutual authentication. For example, you can use a TLS offload proxy such as an Apache or F5 server. This proxy is also known as a Trusted Front End. It intercepts and decrypts HTTPS network traffic and when it determines that the final destination is MobileIron Core, it re-encrypts and forwards the traffic to Core. The devices that register to Core (using port 443) must send HTTPS requests to the TFE rather than to MobileIron Core. Also, the TFE must be provisioned with digital certificates that establish an identity chain of trust with a legitimate server verified by a trusted third-party certificate authority.

Related topics

"Advanced: Trusted Front End" in the *MobileIron Core System Manager Guide.*

Migrating Mobile@Work for Android to use mutual authentication

For devices that register after enabling mutual authentication, Mobile@Work uses port 443 for device check-ins. However, devices that were already registered continue to use port 9997. You can migrate Mobile@Work for Android from using port 9997 without mutual authentication to using port 443 with mutual authentication. The device users do not need to re-register with MobileIron Core.

Before you begin

Instruct Android device users to upgrade to Mobile@Work 10.1 for Android through the most recently released version as supported by MobileIron. Prior Mobile@Work releases do not support migration.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the sync policy for the devices that you want to migrate. Select **Edit**.
3. In the Modify Sync Policy dialog box, select **Migrate Mobile@Work Client**.
4. Click **Save**.
5. Click **OK**.

On the next device check-in, MobileIron Core will send the mutual authentication client identity certificate to the device. In all subsequent device check-ins, the device will use mutual authentication on port 443.

On that first device check-in, the device's **client migration status** changes to **Pending**. After Core has sent the mutual authentication client identity certificate to the device, the **client migration status** changes to **Success**. You can search on this value in the **Client Migration Status** field in **Advanced Search** on **Devices & Users > Devices**.

Related topics

When devices use mutual authentication

Certificates settings

Use a certificate setting to upload a trusted public key root certificate or certificate chain. If it is a certificate chain, it can include the root certificate or only intermediate certificates.

IMPORTANT: You cannot upload an identity certificate – a certificate that contains a private key – into a certificate setting. To upload an identity certificate to Core, use the certificate enrollment setting called single file identity.

You configure MobileIron Core to deliver the uploaded certificate or certificate chain to devices so that the devices can trust, for example, specific web services, email servers, or network components like VPN and Wi-Fi.

Two ways are available to deliver the certificate to a device:

- You reference the certificate setting from another Core setting, and apply the appropriate labels to the referencing setting. Only the following settings can reference a certificate setting:
  - An AppConnect app configuration, Web@Work setting, or Docs@Work setting can reference a certificate setting as the value of a key-value pair.

  - A Wi-Fi setting can reference a certificate setting in its **Apply to Certificates** field (used with specific authentication and data encryption values on the Wi-Fi setting).
- You want to deliver a trusted public key certificate directly to a set of devices, without referencing the certificate setting from another setting. In this case, label the certificate setting. This case is less common.

Note The Following:

- When upgrading from a MobileIron Core prior to Core 9.5.0.0, each certificate setting that contained an identity certificate is automatically converted to a single file identity certificate enrollment setting. Any settings that referenced the certificate setting refer to the new single file identity certificate enrollment setting.
- You cannot import a certificate setting from a MobileIron Core prior to Core 9.4.0.0 if the certificate setting contained an identity certificate. You must manually create a single file identity certificate enrollment setting.

Adding a certificate setting

Procedure

1. Log in to the Admin Portal.
2. Go to **Policies & Configs > Configurations**
3. Click **Add New > Certificates**.
4. Fill in the entries:
   - **Name**: Enter brief text that identifies certificate setting.
   - **Description**: Enter additional text that clarifies the purpose of this certificate setting.
   - **File Name**: Click **Browse** to select the X.509 certificate file (.cer, .crt, .pem, or .der) to upload to MobileIron Core. The certificate must be encoded as binary DER or ASCII PEM.
5. Click **Save**.

Label the certificate setting if you want to deliver the certificate directly to a set of devices, regardless whether it is referenced from another setting. If you are referencing the certificate setting from another setting, label the other setting.

Certificate Enrollment settings

Certificate enrollment settings are used as follows:

- As part of a larger process of setting up a certificate enrollment server to support authentication for VPN on demand, Wi-Fi, Exchange ActiveSync, AppTunnel and so on.
- To provide devices identity certificates that you uploaded to Core for the case when you want to provide the same identity certificate to many users' devices.

- To provide user-provided certificates to devices when end users use the MobileIron Core user portal to upload their identity certificates to Core.
- To specify that AppConnect apps on devices use derived credentials.

The available options are:

- **Blue Coat**: Select **Blue Coat** to create a Blue Coat certificate enrollment setting for integrating with the Blue Coat Mobile Device Security service.
- Client-Provided: Select **Client-Provided** if you want AppConnect apps to use derived credentials for authentication, digital signing, or encryption.
- **Entrust**: Select **Entrust** if you are using the Entrust Datacard certificate enrollment solution.
- **GlobalSign**: Select **GlobalSign** if you are using GlobalSign as the CA for certificate enrollment.
- **Local**: Select Local if you are using MobileIron Core as the CA.
- **OpenTrust**: Select **OpenTrust** if you are using the OpenTrust integration. See Certificate Enrollment settings on page 271.
- **Single File Identity: Select Single File Identity to upload an identity certificate for distribution to devices.**
- **SCEP**: Select **SCEP** for standard certificate-based authentication using a separate CA.

  NOTE: SCEP Configurations created before upgrading to Core 7.0.0.0 or later should be replaced with a new SCEP Configuration. Failure to do so might result in cert renewal failure from Core 9.4.0.0.

- **Symantec Managed PKI**: Select **Symantec Managed PKI** if you are using Symantec's Certificate Enrollment solution. See Certificate Enrollment settings on page 271" for more information.
- **Symantec Web Services Managed PKI**: Select **Symantec Web Services Managed PKI** if you are using the Symantec Web Services Managed PKI solution. See Certificate Enrollment settings on page 271 for more information.
- **User-Provided**: Select **User-Provided** if device users will upload their personal certificates. The user portal includes a certificate upload section for this purpose. A web services API is also available for you to upload user-provided certificates.

If Certificate Enrollment integration is not an option

If Certificate Enrollment integration is not an option for your organization, consider configuring MobileIron Core as an intermediate or root CA. See Certificate Enrollment settings on page 271 for more information.

Supported variables for certificate enrollment

The following variables are supported for the required and optional fields when configuring integration with supported Certificate Authorities (CA's):

- $EMAIL$
- $USERID$

- $FIRST_NAME$
- $LAST_NAME$
- $DISPLAY_NAME$
- $USER_DN$
- $USER_UPN$
- $USER_LOCALE$
- $DEVICE_UUID$
- $DEVICE_UUID_NO_DASHES$
- $DEVICE_UDID$
- $DEVICE_IMSI$
- $DEVICE_IMEI$
- $DEVICE_SN$
- $DEVICE_ID$
- $DEVICE_MAC$
- $DEVICE_CLIENT_ID$
- $USER_CUSTOM1$
- $USER_CUSTOM2$
- $USER_CUSTOM3$
- $USER_CUSTOM4$
- $REALM$
- $TIMESTAMP_MS$
- $RANDOM_16$
- $RANDOM_32$
- $RANDOM_64$
- $CONFIG_UUID$*

* This substitution variable works only for the values under the **Subject Alternative Names** section for the following configurations: Entrust, Local, SCEP, Symantec Managed KPI. It is used for Sentry certificate-based tunneling (CBT).

Certificate generation time

Certificate enrollment settings can be referenced from other settings on Core that require an identity certificate. Some settings that can reference certificate enrollment settings are Exchange settings, Email settings, Wi-Fi settings, VPN settings, AppConnect app configuration settings, Docs@Work settings, and Web@Work settings.

Most certificate enrollment settings cause an identity certificate to be generated. The identity certificate is generated at one of these times:

- Early generation
- On-demand generation

NOTE: Some certificate enrollment settings do not cause an identity certificate to be generated. Specifically, for user-provided certificate enrollment settings and single file identity certificate enrollment settings, the certificate is available on Core. For client-provided certificate enrollment settings, the certificate is available in Mobile@Work.

Early generation

Early generation occurs when you apply a label to a setting that references the certificate enrollment setting. Core generates identity certificates at this time for:

- Exchange settings for Android devices
- Email settings for Android devices
- Wi-Fi settings for Android devices
- VPN settings for Android devices
- AppConnect app configurations
- Docs@Work settings
- Web@Work settings

For each device that has the same label as the setting, Core generates an identity certificate for the device for *each* setting that references the certificate enrollment setting. Core delivers the identity certificate to the device at a later time when Core delivers the setting to the device. Core delivers a setting to a device when the device checks in with Core.

NOTE: After Core generates an identity certificate, if Core does not send the certificate to a device within 14 days, Core deletes the certificate from its file system. The certificate will be generated on-demand.

On-demand generation

On-demand generation occurs when MobileIron Core sends a setting that references the certificate enrollment setting to the device. On-demand generation occurs for all settings (that reference a certificate enrollment setting) that are not listed in the early generation list above. A setting, including the certificate, is delivered to a device when the device checks in with MobileIron Core.

Configuring a client-provided certificate enrollment setting

This section covers client-provided certificate enrollment settings.

Client-provided certificate enrollment settings are applicable only to iOS and Android devices.

Overview of client-provided certificate enrollment settings

Derived credentials are identity certificates derived from the certificates on a smart card. The derived credentials are stored on the device in Mobile@Work on iOS devices, and in Secure Apps Manager on Android devices. AppConnect apps on mobile devices can use derived credentials for these purposes:

- authentication to backend servers, such as email servers, web servers, or app servers
- digital signing
- encryption
- decryption of older emails for which the original encryption certificate has expired (iOS only)
- authenticating the user to Standalone Sentry when using AppTunnel with Kerberos authentication to the backend server

You create a client-provided certificate enrollment setting when you want an AppConnect app to use derived credentials for one of these purposes. You then refer to the client-provided certificate enrollment in the appropriate setting.

NOTE: The certificate enrollment setting is called *client-provided* because Mobile@Work for iOS or Secure Apps Manager for Android, known as *client* apps, provide the identity certificate to the AppConnect app.

Only the following settings can refer to a client-provided certificate enrollment setting:

- AppConnect app configuration
  It can refer to a client-provided certificate enrollment setting in:
  - the value in a key-value pair in its **App-specific Configurations** section
  - the identity certificate in its **AppTunnel Rules** section
- Web@Work setting
  It can refer to a client-provided certificate enrollment setting in:
  - the value in a key-value pair in its **Custom Configurations** section
  - the identity certificate in its **AppTunnel Rules** section
- Docs@Work setting
  It can refer to a client-provided certificate enrollment setting in:
  - the value in a key-value pair in its **Custom Configurations** section
  - the identity certificate in its **AppTunnel Rules** section

Make sure the version of Mobile@Work for iOS or the Secure Apps Manager for Android on the device supports client-provided certificate enrollment settings as shown in the following table:

Reference to the client-provided certificate enrollment setting	iOS: Mobile@Work prior to 8.5	iOS: Mobile@Work 8.5 and 8.6	iOS: Mobile@Work 9.0 through the most recently released version as supported by MobileIron	Android: All versions of Secure Apps Manager supported or compatible with MobileIron Core
In key-value pairs	Not supported	Supported	Supported	Supported
In AppTunnel rules	Not supported	Not supported	Supported	Not supported

Related topics

- *MobileIron Core Derived Credentials Guide*
- *MobileIron PIV-D Manager App for iOS Release Notes*
- *MobileIron PIV-D Entrust App for Android Release Notes*

Specifying a client-provided certificate enrollment setting

To specify a client-provided certificate enrollment setting:

1. Go to **Policies & Configs > Configurations**.
2. Select **Add New > Certificate Enrollment > Client-Provided**.

   In the New Client-Provided Certificate Enrollment Setting dialog box, use the following guidelines to specify your settings.

Item	Description
Name	Enter brief text that identifies this certificate enrollment setting.
Description	Enter additional text that clarifies the purpose of this certificate enrollment setting.
Select purpose	Select one of the following, depending on the intended use of the client-provided identity certificate: • **Authentication** • **Decryption** • **Encryption** • **Signing**
Provider	Select the derived credential provider.

3. Click **Save**.

Configuring an Entrust CA

MobileIron Core supports integration with the Entrust Administration Services (EAS). This integration allows MobileIron Core to work with Entrust to obtain certificates directly from the CA.

Entrust Prerequisites

The information in this section assumes the following:

- You have the URL for your Entrust server (received from Entrust).
- You have the Admin ID and password.

Procedure

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > Entrust**.
2. Use the following guidelines to specify the settings.
   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **API URL**: Enter the URL for your Entrust server (received from Entrust).
   - **Admin ID**: The credentials to log into the Entrust server.
   - **Admin Password**: Enter the Admin Password.
   - **Group**: The Entrust group associated with users. Custom attribute variable substitutions are supported.

     NOTE: If the profile you selected contains an iggroup variable, then the you must configure the same value here as well

   - **Key Usage**: Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.

     NOTE: When multiple certificates are returned by a DigitalID profile, the first one that matches the selected key usage flags is used. If none of the returned certificates match the selected key usage flags, an error is raised. Use the **Issue Test Certificate** feature to ensure the expected certificate is selected.

   - **Profile**: Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.

     Select a profile template from Entrust. Once you select this profile, more options (required and optional variables) are available to you based on the profile you select. Entrust refers to profiles as DigitalIDs.
   - **Profile Description**: Pre-populated based on the profile you select.
   - **Application Description**: Pre-populated based on the profile you select.
   - **Centralized**: Select to allow MobileIron Core to retrieve certificates on behalf of devices.

Decentralized: Select to let managed devices retrieve their own certificates.

This feature is supported on iOS devices only.

- **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Core.
  - If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.
- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.
- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **Entrust SCEP CA**:
- **URL**: Enter the URL of the Entrust SCEP CA.
- **Key Type**: Select RSA.
- **Key Length**: Select 1024 or 2048.
- **Subject Alternative Names table**: Enter a type and value. At run-time, these variables are resolved into user values. (See Configuring an Entrust CA on page 277 for more information.) Custom attribute variable substitutions are supported.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke an Entrust API Version 9 certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Entrust manager. When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Select **Actions > Revoke**.

Configuring a GlobalSign CA

MobileIron Core supports integration with GlobalSign as a certificate authority (CA) for certificate enrollment. This integration enables GlobalSign to perform the proxy tasks that would normally be performed by Core, allowing the

device to obtain certificates from the GlobalSign CA.

GlobalSign Prerequisites

The information in this section assumes that you have set up the following information with GlobalSign:

- A user name and password for MobileIron Core to use to access the GlobalSign server
- GlobalSign profiles
- Whether you want the generated certificates to have the enhanced key usage extension Encrypting File System (EFS)
- Whether you want the generated certificates to be the GlobalSign type “personal” or “department”

To specify GlobalSign settings:

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > GlobalSign**.
2. Use the following guidelines to specify the settings.
   - **Name**: Enter brief text that identifies this certificate enrollment setting.
   - **Description**: Enter additional text that clarifies the purpose of this certificate enrollment setting.
   - **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Core.

     If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.
   - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.
   - **Device Certificate**: Specifies that the certificate is bound to the given device.
   - **URL**: Enter the URL for the GlobalSign server. This field defaults to:

     https://system.globalsign.com/cr/ws/GasOrderService

     Typically, you only change this if you are working with a GlobalSign test environment.
   - **User Name**: The user name for MobileIron Core to use to access the GlobalSign server. Custom device and user attributes variable names are supported.
   - **Password**: Enter the password then re-enter to confirm. Custom device and user attributes variable names are supported.
   - **Profile**: Click **Refresh** to populate the drop-down list of profiles from GlobalSign. Then, select a profile.

     NOTE: You must enter a valid **User Name** and **Password** before clicking **Refresh**.
   - **Profile Description**: Pre-populated based on the profile you select.
   - **Application Description**: Pre-populated based on the profile you select.
   - **Product Code**: Select either **EPKIPSPersonal** or **EPKIPSDept**, depending on whether you want the generated certificates to be the GlobalSign type “personal” or “department”.

- **Certificate Expiration**: Specify when the generated certificate will expire.
- **EFS option**: Select this setting if you want the generated certificate to have the enhanced key usage extension Encrypting File System (EFS).

  Selecting this setting has no impact if the selected profile has disabled EFS.
- **Common Name**: Specify the Common Name to use in the generated certificate.
- **Organization Unit**: Specify the Organization Unit to use in the generated certificate.
- **E-Mail**: Specify the email address to use in the generated certificate.
- **Subject Alternative Names Value**: Enter a type and value. At run-time, these variables are resolved into user values. Add multiple SAN entries with corresponding values. Click **Add+**, select the SAN type (NT Principal Name) from the drop-down list, then select one of the available values. (See Configuring a GlobalSign CA on page 278 for more information.)

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a GlobalSign certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the GlobalSign server. When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Select **Actions > Revoke**.

Configuring MobileIron Core as the CA

This section describes how to configure MobileIron Core as the CA.

To specify local settings:

1. Go to **Policies & Configs > Configurations.**
2. Click **Add New > Certificate Enrollment > Local**.

3. Use the following guidelines to specify the settings.
   - **Name**: Enter brief text that identifies this group of settings. Example: Local Certificate Settings for Wi-Fi
   - **Description**: Enter additional text that clarifies the purpose of this group of settings.
   - **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

     If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

     Select this option for certificates used for email on devices with multi-user sign-in.
   - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

     Select this option for certificates used for email on devices with multi-user sign-in.
   - **Device Certificate**: Specifies that the certificate is bound to the given device.
   - **Local CAs**: Select the name of the self-signed certificate you generated.
   - **Key Type**: Specifies the key exchange algorithm used (typically RSA or elliptic curve).
   - **Subject**: Enter an X.509 name represented as an array of OIDs and values.

     See Configuring MobileIron Core as the CA on page 280 for more information.
   - **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select **None** from the drop-down list.
   - **Key Usage**: Specify acceptable use of the key (signing and/or encryption).
   - **Key Length**: Select a Key Length.

     The values are 1024, 1536, 2048 (the default), 3072, and 4096.
   - **CSR Signature Algorithm**: Select the signature algorithm.

     The values are SHA1, SHA256, SHA384 (default), and SHA512.
   - **Subject Alternative Names table**: Enter a type and value. At run-time these variables are resolved into user values.

     See "Configuring MobileIron Core as the CA on page 280" for more information.
4. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
5. Click **Save**.

NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a local certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

Configuring OpenTrust CA

MobileIron Core supports integration with the OpenTrust Mobile Provisioning Server (MPS). This integration enables OpenTrust to perform the proxy tasks that would normally be performed by Core. The following describes the configuration in Core.

Note The Following: Compatibility notes

- This integration does not support the pushing Certificate Authorities Bundles to devices, which is offered by OpenTrust.
- MobileIron Core supports one certificate per OpenTrust configuration. OpenTrust supports creating profiles having multiple credentials (called application in the OpenTrust context).

Before you begin

The information in this section assumes the following:

- You have the URL for your OpenTrust cloud instance.
- You have the client-side JSON connector identity certificate MobileIron Core will use to authenticate to the MPS.
- You have implemented a centralized OpenTrust cloud.
- You have created a Mobile Management Profile on MPS containing a single centralized credential.

Procedure

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > OpenTrust**.
2. Use the following guidelines to specify the settings:

   NOTE: Although optional fields are not required by OpenTrust, they are still used if present. Therefore, you must still specify the appropriate variable for each optional field. For example, the phone number might be an optional field because the tablets in your organization do not have phone numbers. However MPS might still use this information to request a certificate from the PKI server if it is present.

- **Name**: Enter brief text that identifies this group of settings.
- **Description**: Enter additional text that clarifies the purpose of this group.
- **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.
- If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices
- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.
- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **API URL**: Enter the URL for the OpenTrust server.
- **Certificate 1**: This is the name of the uploaded certificate.
- **Password 1** (Optional): This password is optional.
- **Add Certificate**: Click this link to add one or more certificates, as necessary.
- **Profile**: This is the MPS Mobile Profile to use for the integration. If you do not see an expected profile, then it most likely contains multiple credentials, a configuration that MobileIron Core does not currently support.
- **Profile Description**: This is pre-populated based on the profile you select.
- **Application Description**: This is populated automatically with the corresponding OpenTrust content associated with the selected profile.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a OpenTrust certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the OpenTrust manager. When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

Procedure

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

Configuring a single file identity certificate enrollment setting

Use a single file identity certificate enrollment setting to upload an identity certificate to MobileIron Core for distribution to devices. A typical use case for a single file identity certificate is using the certificate to authenticate devices to a network server, such as:

- Standalone Sentry
  When device authentication on Standalone Sentry is configured as Group Certificate, you typically distribute the same identity certificate to multiple devices.
- a Wi-Fi network component
  When you configure a Wi-Fi setting to use TLS or TTLS for its EAP type, you can distribute the same identity certificate to multiple devices.
- a VPN network component
  When you configure a VPN setting, depending on the type of VPN setting, you can use certificate-based authentication. For the authentication, you can distribute the same identity certificate to multiple devices.

You can upload either:

- An identity certificate.
  The certificate is a PKCS 12 certificate which contains exactly one private key. It is a .p12 or .pfx file. The file can optionally include the certificate chain. The certificate chain can include only intermediate certificates, or intermediate certificates through the root certificate. The root certificate is not necessary if it is from a well known certificate authority.
  You also provide the password for the identity certificate's private key.
- Multiple files, which include among them:
  - the private key and its password.
  - the public certificate.
  - the supporting certificates in the certificate chain. The root certificate is not necessary if it is from a well known certificate authority.
- Examples of combinations you can upload are:
  - a .p12 or .pfx file containing a an identity certificate and its private key and password, plus additional .pem files containing the intermediate certificates.
  - a .pem file containing the private key and password, a .pem file containing the public certificate, plus additional .pen files containing the intermediate certificates.

Procedure

1. Log in to the Admin Portal.
2. Go to **Policies & Configs > Configurations**
3. Click **Add New > Certificate Enrollment > Single File Identity**.
4. Fill in the entries:
   - **Name**: Enter brief text that identifies certificate enrollment setting.
   - **Description**: Enter additional text that clarifies the purpose of this certificate enrollment setting.

- **Certificate 1**: Click **Browse** to select the .p12 or .pfx file of the identity certificate, if you are uploading only one file.
- If you are uploading multiple files, select the file (.p12, .pfx, or .pem) that contains the private key.
- **Password 1**: Enter the password for the certificate's private key.

5. If you are uploading multiple files, click **Add Certificate** to add another file.
6. Fill in the entries:
   - **Certificate 2**: Click **Browse** to select the .pem file to upload to MobileIron Core. The certificate must be formatted as binary DER or ASCII PEM.
   - **Password 2**: The Password field is applicable only for the file that contains the private key.
7. Optionally, click **Add Certificate** to add another file**.**
8. Click **Save**.

After you save the single file identity certificate enrollment setting, you can view or change the certificate by editing the setting.

Configuring SCEP

This section describes how to specify settings that allow the device to obtain certificates from a CA using Simple Certificate Enrollment Protocol (SCEP).

To specify the SCEP settings:

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > SCEP**.
2. Use the following guidelines to specify the settings:
   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Centralized**: MobileIron Core retrieves certificates on behalf of devices. Core also manages the certificate lifetime and triggers renewals. See "SCEP proxy functions on page 288".

     NOTE: Select this option for certificates used for email on devices with multi-user sign-in.
   - **Decentralized**: Devices retrieve their own certificates.

     Use this feature if using the SCEP setting for mutual authentication. It is not supported for any other use cases with AndroidiOS and macOS devices. See Enabling mutual authentication for Apple and Android devices.

     This feature is not available for Android devices.
   - **Store keys on Core**:

     Specifies whether MobileIron Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices.

NOTE: Select this option for certificates used for email on devices with multi-user sign-in.

- **Proxy requests through Core**:
  This feature is not available for Android devices.
  When this option is enabled, Core acts as a reverse proxy between devices and the target certificate authority. This option is only available when **Decentralized** is selected.
- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

  NOTE: Select this option for certificates used for email on devices with multi-user sign-in.
- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **URL**: Enter the URL for the SCEP server.
- **CA-Identifier**: (Optional) Enter the name of the profile for SCEP servers that support named-profiles.
- **Subject**: Enter an X.509 name represented as a comma-separated array of OIDs and values. Typically, the subject is set to the user's fully qualified domain name. For example,
  C=US,DC=com,DC=MobileIron,OU=InfoTech or
  CN=www.mobileiron.com.
  You can also customize the Subject by appending a variable to the OID. For example, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$.
  For ease of configuration you can also use the $USER_DN$ variable to populate the Subject with the user's FQDN.
- **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select None from the drop-down list.
- **Key Usage**: Specify acceptable use of the key by signing.
- **Encryption**: Specify acceptable use of the key by encryption.
- **Key Type**: Specify the key type.
- **Key Length**: The values are 1024, 1536, 2048 (the default), 3072, and 4096.
- **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (default), and SHA512.
- **Finger Print**: The finger print of the CA issuing the root certificate.
- **Challenge Type**: Select **None**, **Microsoft SCEP**, or **Manual** to specify the type of challenge to use. The Challenge Type will depend on what the NDES server is configured to use.
- **Challenge URL**: For a Microsoft SCEP challenge type, enter the URL of the trustpoint defined for your Microsoft CA.
- **User Name**: Enter the user name for the Microsoft SCEP CA.
- **Password**: Enter the password for the Microsoft SCEP CA.

- **Subject Alternative Names Type**: Select NT Principal Name, RFC 822 Name, or None, based on the attributes of the certificate template. You can enter four alternative name types.

  NOTE: If this SCEP setting is for authenticating the device to the Standalone Sentry using an identity certificate: select NT Principal Name and select Distinguished Name for a second Subject Alternative Name

- **Subject Alternative Names Value**: Select the Subject Alternate Name Value from the drop-down list of supported variables. You can also enter custom variables in addition to and instead of the supported variables.

  NOTE: If this SCEP setting is for authenticating the device to the Standalone Sentry using an identity certificate: enter $USER_UPN$ for the value corresponding to NT Principal Name and enter $USER_DN$ for the value corresponding to Distinguished Name.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

   You cannot make changes to the saved SCEP settings. When you open a saved SCEP setting, the **Save** button is disabled.

   NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

X.509 Codes

The Subject field uses an X.509 distinguished name. You can use one or more X.509 codes, separated by commas. This table describes the valid X.509 codes:

TABLE 57. X.509 CODES

Code	Name	Type	Max Size	Example
C	Country/Region	ASCII	2	C=US
DC	Domain Component	ASCII	255	DC=company, DC=com
S	State or Province	Unicode	128	S=California
L	Locality	Unicode	128	L=Mountain View
O	Organization	Unicode	64	O=Company Name, Inc.
OU	Organizational Unit	Unicode	64	OU=Support
CN	Common Name	Unicode	64	CN=www.company.com

NOTE: If the SCEP entry is not valid, then you will be prompted to correct it; partial and invalid entries cannot be saved.

SCEP proxy functions

Choosing to enable SCEP proxy functions has the following benefits:

- A single certificate verifies Exchange ActiveSync, Wi-Fi, and VPN configurations
- There is no need to expose a SCEP listener to the Internet.
- MobileIron can detect and address revoked and expired certificates.

Configuring Symantec Managed PKI

Symantec Managed PKI support enables you to configure certificate-based authentication. Symantec Managed PKI is a source for certificates that you can reference in a variety of configurations, such as for Exchange, VPN, and AppConnect.

Prerequisites

- A valid Symantec Verisign Managed PKI account is required.
- (Optional) Get finger print from issuing CA for root certificate.
- One or more client certificate and password from CA.

Procedure

To specify the Symantec Managed PKI settings:

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > Symantec Managed PKI**.
2. Use the following guidelines to specify the settings:
   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Centralized**: MobileIron Core retrieves certificates on behalf of devices. Core also manages the certificate lifetime and triggers renewals. See “Using a proxy on page 289”.

     NOTE: Select this option for certificates used for email on devices with multi-user sign-in.
   - **Decentralized**: This feature is not available for Android devices.Devices retrieve their own certificates.
   - **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

     If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

     NOTE: Select this option for certificates used for email on devices with multi-user sign-in.
   - **Proxy requests through Core**: This feature is not available for Android devices.

- When this option is enabled, Core acts as a reverse proxy between devices and the target certificate authority. This option is only available when **Decentralized** is selected.

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

  NOTE: Select this option for certificates used for email on devices with multi-user sign-in.

- **URL Mode**: Specifies the mode and the corresponding URL supplied by Symantec.
- **CA-Identifier**: Required information supplied by Symantec.
- **Subject**: See Configuring Symantec Managed PKI on page 288 for more information.
- **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select **None** from the drop-down list.
- **Key Usage**: Use these options to indicate which key usage to request from the CA.
- **Key Type**: This is the Key Exchange algorithm: RSA or Elliptic Curve.
- **Key Size**: The values are 1024, 1536, 2048 (the default), 3072, and 4096.
- **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (the default), and SHA512.
- **Finger Print**: The finger print of Symantec Managed PKI.
- **Certificate 1**: Upload for the client authentication with the server.
- **Password 1**: This password is optional.Best used when certificate and password are in separate files.
- **Subject Alternative Names table**: Enter a type and value. At run-time these variables are resolved into user values. (See Configuring Symantec Managed PKI on page 288 for more information.)

  NOTE: The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI manager.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Using a proxy

Choosing to enable proxy functions has the following benefits:

- A single certificate verifies Exchange ActiveSync, Wi-Fi, and VPN configurations
- There is no need to expose a SCEP listener to the Internet.
- MobileIron can detect and address revoked and expired certificates.

Configuring Symantec Web Services Managed PKI

Integration with Symantec Web Services Managed PKI version 8.x enables you to configure certificate-based authentication. The following describes how to configure Symantec Web Managed PKI in MobileIron Core.

Before you begin

- Set up your account for Symantec Web Services Managed PKI with Symantec.
- Create an MDM (Web Service Client) profile in the Symantec PKI manager that you will use for the MobileIron integration.

  SeatID

  Be sure to include the Symantec SeatID as a required certificate profile field. In a Symantec Web Services Managed PKI environment, Symantec uses the SeatID to track the number of seats for billing purposes.

  To correctly track the number of seats, the SeatID value in the MobileIron Core SCEP settings must map to the value you created for the SeatID in the Symantec PKI Manager. For example, if the user's email address is used as the SeatID in Symantec PKI Manager, the Core SCEP settings should map the Core email address attribute to the Symantec SeatID.

  Core associates each issued Symantec certificate to a SeatID in the Symantec PKI Manager. If the SeatID does not exist, a new Symantec user account and SeatID is automatically created for the user at the time the certificate is requested.
- Gather the following items:
  - The server address for the Symantec Web Services Managed PKI.
    On MobileIron Core the default is set to pki-ws.symauth.com.
  - The Registration Authority (RA) certificate MobileIron Core will use to authenticate to the Symantec CA.

Procedure

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > Symantec Web Managed PKI**.
2. Use the following guidelines to specify the settings:

   NOTE: The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI manager.

   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Store keys on Core**: Specifies whether MobileIron Core stores the private key sent to each device. If you are using a Symantec profile that is set up to store keys on the Symantec server, you typically do not select this option.

     NOTE: If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices.

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

  The certificate is revoked when the user is removed from Core.

- **Device Certificate**: Specifies that the certificate is bound to the given device. Make sure the Symantec certificates are unique for each device.

  The certificate is revoked when the device is retired from Core.

a. **API URL**: Enter the server address for the Symantec Web Services Managed PKI (received from Symantec).

   The default is set to pki-ws.symauth.com.

   NOTE: Do not add https:// before the server name, and do not add path information after the server name.
   Only the hostname of the Symantec CA server should be provided.

- **Certificate 1**: Navigate and select the RA certificate you received from Symantec. This is usually a.p12 file. Enter the password for the certificate when prompted.
- **Password 1**: (Optional if certificate and password are stored in the same file.) Enter the password for the certificate.
- **Add Certificate**: Click this link to add one or more certificates, as necessary.
- **Profile**: This is the profile to be used for the integration. If you do not see an expected profile, then it most likely contains multiple credentials, a configuration that MobileIron Core does not currently support.
- **Profile Description**: This is pre-populated based on the profile you select.
- **Application Description**: This is populated automatically based on the selected profile.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

   NOTE: If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a Symantec Web Services Managed PKI certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Symantec Web Services Managed PKI manager. When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

Configuring a user-provided certificate enrollment setting

One user-provided certificate enrollment setting for each purpose

Configure a user-provided certificate enrollment setting for every purpose for which users can upload a certificate (PKCS 12 file) in the user portal. For example, consider a case in which users have three different purposes for providing certificates: S/MIME signing, S/MIME encryption, and authenticating to a backend server. In this case, you create three user-provided certificate enrollment settings.

You provide a display name for each user-provided certificate enrollment setting. The display name you choose is important because the device user sees it in two places:

- in the user portal when deciding what certificate to upload
- In the user portal, the display name is called “configuration”. The user’s selection associates the uploaded certificate with a user-provided certificate enrollment setting. The user can upload the same certificate, or different certificates, for each display name.
- in Mobile@Work for iOS, when Mobile@Work for iOS prompts the user for the private key password.
- Mobile@Work prompts for the password if a password was not required when the user uploaded the certificate to the user portal. Mobile@Work uses the display name to inform the user about which certificate to provide the password for. For details, see The private key password on page 293.

Note The Following:

- The PKCS 12 file must contain the certificate and one private key. MobileIron Core does not support PKCS 12 files with more than one private key.
- A web services MobileIron V2 API is also available for uploading user-provided certificates to Core and associating the certificates with a user-provided certificate enrollment setting.
- See the *MobileIron V2 API Guide.*
- The V1 API that uploaded user certificates to MobileIron Core is no longer available. If you used the V1 API to upload user certificates, Core will continue to use the certificates until either:
  - the user uploads a replacement in the user portal
  - you use the V2 API to upload a replacement

    Note that the V1 API associated the user certificate with a certificate type: All, WIFI, VPN, SMIMESIGNING, SMIMEENCRYPTION, EMAIL or EXCHANGE. Although Core still supports using these certificates and their associated type, the user portal does not display these certificates in the user portal.

Core stores the certificate and private key

When the user uploads a user-provided certificate in the user portal, the user uploads a PKCS 12 file. Core stores the file, which includes the certificate and its private key. Core does not remove the PKCS 12 file after delivering it to the user's device. Therefore, if the user registers another device, the PKCS 12 file is available to deliver to the additional device.

The private key password

In each user-provided certificate enrollment setting, you specify whether the user is required to provide a password for the certificate's private key. When a password is required, users must provide a password when using the user portal to upload a certificate associated with this certificate enrollment setting.

Important: Always require a password unless both of the following are true:

- The devices that will use the user-provided certificate are iOS devices running Mobile@Work 9.0 for iOS through the most recently released version as supported by MobileIron.
- The apps that will use the certificate are AppConnect apps.

When you do not require a private key password when the user uploads a certificate, Mobile@Work for iOS and an AppConnect for iOS app that uses the certificate behave as follows:

1. When the AppConnect app launches, control switches to Mobile@Work for iOS.
2. Mobile@Work prompts the device user for the private key password.
3. The device user enters the password.

   NOTE: If the device user exits Mobile@Work without providing the password, when the AppConnect app next launches, Mobile@Work unauthorizes the app, with the reason that the app is missing credentials.

4. Control returns to the AppConnect app.

Whether you require a password depends on your security requirements. If a password is required, Core stores the password along with the PKCS 12 file containing the certificate and private key. However, if your security environment requires limiting the password's storage to the device that uses the certificate, then do not require a password.

When the private key of a user-provided certificate is deleted

The private key of a PKCS 12 file, and password if provided, can be deleted from the Core file system. Whether you want the private key and password deleted from Core depends on your security requirements.

The following mechanisms are available to delete the private key and password:

- A user can delete the private key and password using the user portal.
- A web services API can delete the private key and password.

- You can specify in the Admin Portal that Core deletes private keys and passwords older than some number of days.

IMPORTANT: When the private key and associated password is deleted, Core retains the public certificate and maintains an entry in its certificate table so it can track where the certificate is used, when it expires and display information about it in the UI. Without the private key and associated password, Core is unable to use the identity certificate with any new certificate enrollments, AppConnect configuration and devices. Once the private key and associated password is deleted, the user-provided certificate must be uploaded again before it can be used.

Because the certificate without the private key is still available on Core, you can view information about the certificate, such as its expiration date. This information can help you manage devices still using the certificate.

Related topics

- Viewing, replacing, and deleting certificates in the user portal on page 457
- *MobileIron V2 API Guide*

Specifying the settings for a user-provided certificate enrollment setting

To specify the settings for a user-provided certificate enrollment setting:

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > User-Provided**.
2. Use the following guidelines to specify the settings:
   - **Name**: Enter brief text that identifies this setting.
   - **Description**: Enter additional text that clarifies the purpose of this setting.
   - **Display Name**: Enter the name that will appear on the user portal where device users upload their certificates. This name also appears in Mobile@Work if Mobile@Work prompts the device user for a certificate's private key password.
   - **Require Password**: This option requires the user to provide a password for the certificate's private key when uploading a certificate associated with this certificate enrollment setting.
   - **Important**: Always require a password except as described in The private key password on page 293.
   - **Delete Private Keys After Days**: Select the number of days after a user-provided certificate is uploaded to MobileIron Core after which Core deletes the private key and, if provided, its password, from Core.

     The default is **None**, which means Core does not delete the private key and its password.

     The default is **None**, which means Core does not delete the private key and its password.
3. Click **Save**.

Android shared-kiosk mode overview

For task-worker deployments, companies may offer dedicated Android devices that are customized for a specific user role. Depending on a user's profile, different apps and configurations may be presented on a device. For example, a user in a technical role may have a specific set of apps presented for their use, while another user in a maintenance role may have access to a different set of apps. For more details, see:

- Setting up the Android shared-kiosk mode
- Configuring the Android shared-kiosk mode
- User experience for staging and shared kiosk users
- Suggestions for configuring shared-kiosk mode

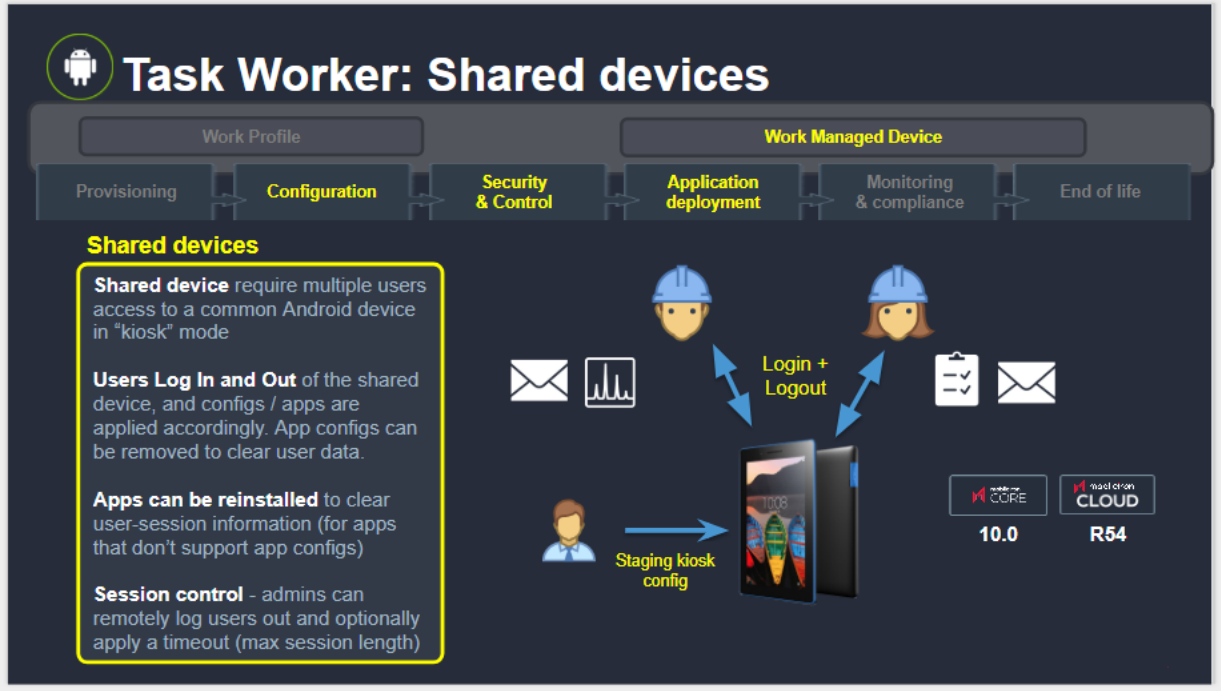
Setting up the Android shared-kiosk mode

NOTE: Samsung Kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead.

For task-worker deployments, companies may offer dedicated Android devices that are customized for a specific user role. Depending on a user's profile, different apps and configurations may be presented on a device. For example, a user in a technical role may have a specific set of apps presented for their use, while another user in a maintenance role may have access to a different set of apps. See the following sections:

The Android shared-kiosk mode acts as an app filter for different groups of users who share devices. A user who is logged in to the shared kiosk is only able to view the apps appropriate for their role. One of the main advantages to the shared-kiosk mode is that you can allow individual user groups access to different sets of apps from the same device. When a user logs out of an Android shared kiosk, their apps and user data, including history, are cleared from the display of the next user who logs onto the device. The shared kiosk requires connectivity to the Core for the user login and logout actions to take effect. In addition, the shared kiosk is only available to Android enterprise deployments with Managed Google Play accounts.

FIGURE 9. TASK WORKS IN ANDROID SHARED KIOSK MODE



The shared kiosk requires two types of users, a staging user and a shared kiosk user, and at least two policies that correspond to these users. The staging user is used to prompt the login screen to appear on a shared device. In effect, the staging user is the logged out device owner (default owner) when a shared user is not logged into the device. Also, the staging user is a special type of admin user who allows other users to login to the actual kiosk device. After the shared kiosk user logs in successfully, then the staging policy is replaced by a shared kiosk policy. The kiosk user has access to the apps installed on the device according to the policy assigned to it. Although you can create multiple shared kiosk policies, there is only one kiosk policy active on a kiosk device at a time. When the kiosk user logs out of the shared kiosk, the device reverts to the staging user and, consequently, the staging policy.

Since the staging user only has the ability to access the login page, you need to a create staging policy that is dedicated to this user. In contrast, the shared kiosk users are able to access the set of apps that you define in their policy. (Naturally, you also need to install the permitted apps on the shared kiosk devices.) The shared kiosk policy allows you to create a filter of permitted apps from all of the apps you have installed previously. You cannot directly upload apps into an Android-shared-kiosk-mode policy. Often you want to dedicate a shared-kiosk-mode policy to a type of shared kiosk user, or user group, depending on your organization. For example, a company may have day-shift and night-shift employees that have different roles and require access to separate sets of apps. In this case, you need to create a day-shift policy and a night-shift policy.

NOTE: Android shared kiosk only supports work-managed devices.

Configuring the Android shared-kiosk mode

To configure the Android shared-kiosk mode, you need to create a staging user role. Then you need to create one kiosk policy for the staging user as well as one or more policies for the shared kiosk users. For example, you can create one policy for managers and another one for employees. Within each policy, you can define the apps that the users, or user group, can access. Then you need to create and add a label to the device. Finally, you need to apply labels to both the staging and shared kiosk policies.

NOTE: You define user groups with a user group feature, such as LDAP. You cannot define user groups within the Android shared kiosk mode.

To configure the Android shared-kiosk mode, do the following:

1. Configuring a staging user
2. Creating a staging policy for the staging user
3. Creating a shared-kiosk-mode policy for the shared kiosk users
4. Creating and Adding labels to Android shared kiosk policies
5. Applying a label to the staging policy
6. Applying a label to a shared kiosk policy

Configuring a staging user

The first step in allowing users to access the Android shared-kiosk mode is to assign a user to the staging role. The staging user must have the same login as the person in your organization who registered MobileIron@Work during the initial setup of the software. Also, this user needs to have the Google Device Account role. MobileIron suggests that you make this user name easy to distinguish by using a name such as "staging-user."

NOTE: A Google Device Account applies only to Managed Google Play Accounts and **new** managed devices. The device account allows the staging user to enroll large numbers of managed devices, that is more than ten devices, without applying the limits imposed by Google.

Procedure

1. In Admin Portal, go to **Devices & Users**. Then select **Users**.
2. Select the check box next to a user.
3. From **Actions**, select **Assign Roles**. The **Assign Role(s)** screen displays.
4. Select the check box next to **Use Google Device Account (for Android enterprise device only)**.
5. Click **Save**.

Creating a staging policy for the staging user

You need to create a policy that is dedicated to the staging user. This policy is not active until you apply a label to the staging policy.

Procedure

1. In Admin Portal, go to **Policies & Configs > Policies**.
2. Click **Add New > Android > Android Kiosk Mode**.
3. In the New Android Kiosk App Setting Policy dialog box, enter a **Name** and **Description** for the policy.
4. Select **Active** for the **Status** field to enable this policy.
5. Scroll down to the Kiosk Settings section:
   - **Disable Quick Settings**
     If you select this option, the device does not display the system notification pull-down menu at the top of the shared kiosk screen.
     If you enable the following options, the settings are displayed as menu items in the shared-kiosk mode on the device.
   - **Allow User to Access WIFI Settings**. This is an optional setting.
   - **Allow User to Access Bluetooth Settings**. This is an optional setting.
   - **Allow User to Access Location Settings**. This is an optional setting.
   - Enter a 4 - 6 digit PIN in the **Kiosk Exit PIN** field.
     You can assign a pin to the staging user kiosk policy. However, it is not mandatory. Without a kiosk exit pin, the staging user cannot exit the kiosk mode .
   - Select the **Enable Shared Device**check box. This is a mandatory setting. By default, the **Enable Login (Only for Staging user)** radio button is selected. Check that this option is selected.
6. Scroll up to the Kiosk Branding section, customize the kiosk with a background color and background image if desired.
   - Use the pull-down menu below the **Background Color** field to select the background color of the kiosk screen.
7. Click **Save**.

Creating a shared-kiosk-mode policy for the shared kiosk users

You want to create one or more policies for the shared kiosk user who has access to the apps on the shared device based on their assigned policies. Each shared kiosk policy specifies a different set of apps available to the assigned user or user groups. For example, one policy could be for day-shift workers and a second one for night-shift workers. Also within these policies, you may want to configure branding to customize the device. This policy is not active until you apply a label to the shared kiosk policy.

NOTE: You need to install any apps that you wish to include in the kiosk using the App Catalog page before you begin this procedure. You cannot install apps from within the shared-kiosk -mode policy. You can only use the shared-kiosk -mode policy to setup which apps are displayed.

Procedure

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Android Kiosk Mode**.

3. Enter a **Name** and **Description** for the policy.
4. Select **Active** for the **Status** field to turn on this policy.
5. Scroll down to the Kiosk Settings section, select:
   - **Disable Quick Settings**
     If you select this option, the device does not display the system notification pull-down menu at the top of the shared kiosk screen.
     If you enable the following options, the settings are displayed as menu items in the shared-kiosk mode on the device.
   - **Allow User to Access WIFI Settings**. This is an optional setting.
   - **Allow User to Access Bluetooth Settings**. This is an optional setting.
   - **Allow User to Access Location Settings**. This is an optional setting.
   - Select the **Enable Shared Device** check box and then click the **Enable Logout** radio button. This is a mandatory setting.
   - Use the arrows next to the **Logout user if session exceeds** field to select the number of hours before a shared kiosk user is automatically logged out of the kiosk device. This is an optional setting.
6. In the **Choose Apps** section, select the app or apps that will be available to the shared kiosk user.

   NOTE: The built-in apps must be enabled in Device Owner mode. This may not be the case with all manufacturers.

   - Add the permitted apps to the **Kiosk Mode Allowed App** section.
   - Click **+Add** in the Built-in Apps to add apps such as the Built-in Camera or Built-In Dialer to the **Kiosk Mode Allowed Apps**.
   - Add apps from the **Built-in Apps** section by clicking **+Add**.
   - Add apps from the **App Catalog Apps** section by clicking **+Add**.
   - Add apps manually by entering a Package ID in the **Manually Add Apps with Package ID** field. Then click **+Add**.
     The order that the apps appear in the **Kiosk Mode Allowed Apps** section, reflects how they appear on the user screen. To change the position of an app on the screen, change its position in the **Kiosk Mode Allowed Apps** list by selecting it and dragging it up or down.

     NOTE: To hide an app, select an app in the **Kiosk Mode Allowed Apps** section and click the eye icon. To ensure the selected app is reinstalled when the user logs out, clearing user session and data, select the Enable force reinstall on Logout icon (which resembles a sheet of paper). You may want to select this icon for apps that contain sensitive data and for apps that do not support managed app configurations.
7. Scroll up to the Kiosk Branding section, customize the kiosk with a banner, background color, or background image as desired.
8. Click **Save**.

Creating and Adding labels to Android shared kiosk policies

After you create the staging policy and one or more shared kiosk policies, you need to create and add a filtered label to the policies to push the configuration to the target devices. You must create a label for the staging user and each of the shared kiosk users.

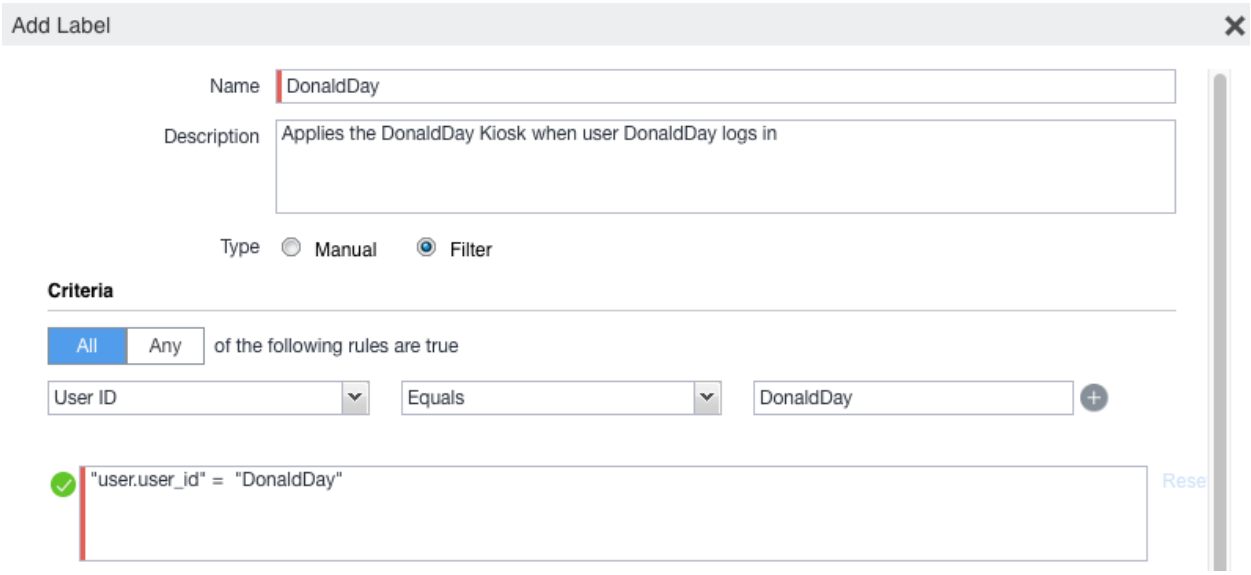
Procedure

1. Go to **Devices & Users > Labels**.
2. Click **Add Label**.The "Add a label" page is displayed.
3. Enter a name and description of the label.
4. Click the **Filter** radio button.
5. Create a rule for the label based on the type of user logged into the device. In the Criteria section, use the **Field**, **Operator**, and **Value** fields (or enter the rule in the **Type search expression here** field):
   - **Field**: Enter the user id as "user.user_id".
   - **Operator**: Enter "Equals" or some other operator to return a single username.
   - **Value**: Enter the user account name

     Here is an example of a rule for a staging user:

     "user.user_id" = "<StagingUsername>" AND common.retired = "false"

     See the following image for an example of a rule for a kiosk user:



     For more information about field definitions, see Device field definitions.
6. Click **Save**.
7. Apply this label to the related policy. See the following sections.

NOTE: The Display Name field on the "Add a label" page changes to reflect the user logged in. This is how the Filtered Label distinguishes which Kiosk Policy is applied.

Apply labels to Android shared kiosk policies

After you create the staging policy and one or more shared kiosk policies, you need to apply a label to the policies to push the configuration to the target devices.

NOTE: You must assign mutually exclusive labels to the staging and shared kiosk policies. In other words, the labels cannot resolve to a device that could be assigned to both policies at the same time. If that situation occurs, the policy with the higher priority is assigned to the device.

Applying a label to the staging policy

The label must contain local users or LDAP user group information (or some way of associating the target users). These are the users that will use the policy.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the check box next to the staging policy.
3. Select **Actions > Apply to Label**. The Apply to Label dialog box opens.
4. Select the check box next to the label.
5. Click **Apply**.

Applying a label to a shared kiosk policy

The label must contain local users or LDAP user group information. These are the users that will use the policy.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the check box next to the shared kiosk user policy.
3. Select **Actions > Apply to Label**. The Apply to Label screen dialog box opens.
4. Select the check box next to the label.
5. Click **Apply**.
6. If needed, repeat the procedure to assign an additional label to another shared kiosk policy.

User experience for staging and shared kiosk users

The staging and shared kiosk users have different user experiences when logging in and out of the kiosk. If you have defined a pin in the staging kiosk policy, the staging user has access to the Exit Kiosk menu command within **Settings**. However, the shared kiosk user has access to their permitted apps as well as to the **Logout Kiosk** command.

NOTE: Both the login and logout operations must be done when the device is online which allows a connection to the MobileIron Core server during these operations.

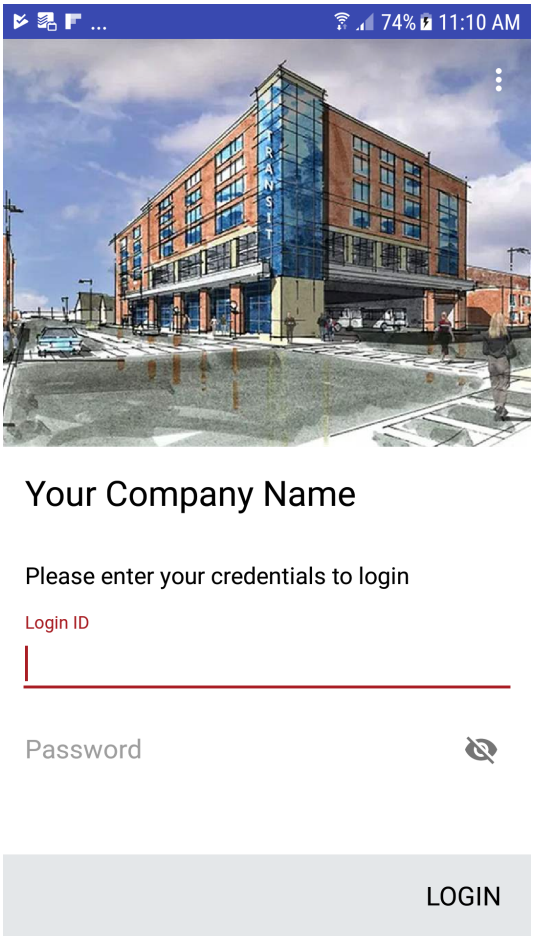
Staging user experience

Procedure

1. Click the **Mobile@Work** menu on the device and then select **Kiosk** to put the device into kiosk mode.The banner and background image are displayed on the screen of the staging user if they have been configured.
2. Click the **Settings** icon--the**Exit Kiosk** command as well as the **WIFI**, **Bluetooth**, and **Location Settings** options are displayed.
3. To exit the kiosk, select **Settings** icon and then select **Exit Kiosk**. Then you are prompted to enter a pin.
4. After you enter the pin, the shared kiosk mode is released and the Android home screen is displayed. See the following Android shared-kiosk login screen example.

NOTE: To re-engage in shared-kiosk mode, repeat step 1.

FIGURE 10. ANDROID SHARED-KIOSK LOGIN SCREEN EXAMPLE



Shared-kiosk mode user experience

Procedure

1. The staging login page is displayed.
2. Enter the shared-kiosk user credentials. It can take up to 30 seconds for the login to complete. Then the shared-kiosk screen is displayed. The **Settings** icon as well as the icons of the available apps are displayed on this screen. Any branding settings, such as banner, background color, or background image, are also displayed.
3. Use any of the allowed apps.(The shared kiosk user has access to at least one app.)
4. Click the **Settings** option, and then the **WIFI**, **Bluetooth**, and **Location Settings** options are displayed. along with the **Logout Kiosk** command.
5. To exit, select **Settings > Logout Kiosk** command. Then the staging login page is displayed on the device.

Monitor Android shared-kiosk mode

While you are setting up the shared-kiosk mode, you may want to verify which user, staging or shared, is logged into a device.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a shared-kiosk device.
3. Click the **Devices** panel to display users who are currently logged in. When a shared-kiosk user successfully logs in, the display name on the **Devices** panel is updated accordingly.

Suggestions for configuring shared-kiosk mode

As the administrator, you must ensure that the configuration for staging and shared kiosk users is accurate in regards to placing users in the correct user group. (The Core software cannot verify that a user is included in the correct group for your organization.) In addition, session control for shared-kiosk users is described.

NOTE: When a user who does not have shared kiosk permission logs into a kiosk, the user receives an error but stays in the staging user mode.

Configuration Example for shared-kiosk mode

See the following figure for an example of a configuration that employs a staging user as well as two shared-kiosk-mode user groups, "User Group "1 and "User Group 2".

FIGURE 11. ANDROID SHARED KIOSK MODE CONFIGURATION EXAMPLE

Configuration

	Staging User Presents Login screen, entry state.	**User Group 1** Set of users with unique set of apps and configs	**User Group 2** Set of users with unique set of apps and configs
User	Must set Device Account == TRUE	Any user on Core / Cloud	Any user on Core / Cloud
Device	Enrolled as Managed Device (Device Owner)		
Apps	Common set of apps distributed to all groups		
App configs	Null	App config per-user or per-group	App config per-user or per-group
Kiosk config / policy	Assigned with "Login" == TRUE	Assigned with "Logout" == TRUE Subset of apps; some apps may be "forced re-installed"	Assigned with "Logout" == TRUE Subset of apps; some apps may be "forced re-installed"

Session Control for shared kiosk devices

You can control the length of a user session in shared kiosk mode using two methods. Within the Suggestions for configuring shared-kiosk mode procedure, you can set the number of hours before a shared kiosk user is automatically logged out with the **Logout user** field. After the timeout period is reached, the device triggers a log out on the device and the device returns to the staging user.

Also, you can immediately force a shared kiosk user off the device by forcing a log out with the Shared Kiosk - Sign Out device command.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a shared-kiosk device.
3. Click **Actions > Android Only > Shared Kiosk - Sign Out**.

Working with Events

This section addresses the components related to The Event Center.

About events

The Event Center enables MobileIron administrators to configure events to specific alerts that can be sent to users, administrators, or both. Event types include:

- International Roaming Event
- SIM Changed Event
- Memory Size Exceeded Event
- System Event
- Policy Violations Event
- Device Status Event

An alert is a message sent via SMS, email, or through a push notification. You can select a predefined message template, or create a custom message to use for the alert.

For example, you can specify an SMS to be sent each time a user travels to a different country, informing the user that different rates may apply.

Events page

Use the **Logs > Event Settings** page in Admin Portal to manage the events you are interested in and the corresponding alerts you want to automate.

Required role

To edit settings on the **Event Settings** page, the administrator must have the **Manage events** role.

Managing events

The tasks that are common to all event types are:

- Creating an event
- Editing an event
- Deleting an event
- Ensuring the alert is sent to the correct recipients
- Applying the event to a label
- Setting alert retries
- Setting device push notifications
- Android notification sync policy

Creating an event

Procedure

To create an event, in the Admin Portal:

1. Go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select the type of event from the drop-down.
4. Complete the information for the selected event.
   Each event type has settings specific to the event type. See Event settings for information on the settings.
5. Click **Save**.

Editing an event

Procedure

To edit an event, in the Admin Portal:

1. Go to **Logs > Event Settings**.
2. Select the event you want to edit.
3. Click **Edit**.
4. Make your changes.
5. Click **Save.**

Deleting an event

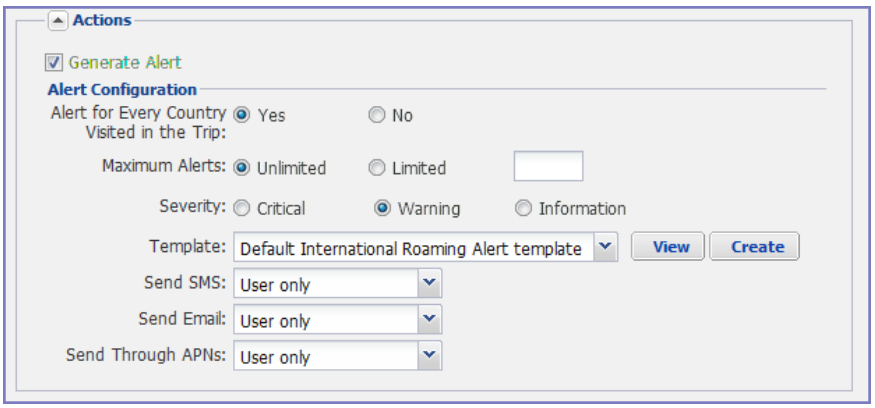
Procedure

To delete an event, in the Admin Portal:

1. Go to **Logs > Event Settings**.
2. Select the event you want to delete.
3. Click **Delete**.

Ensuring the alert is sent to the correct recipients

When you create an event, you designate recipients for the resulting alert. Each event type includes the alert configuration section shown in the following figure.

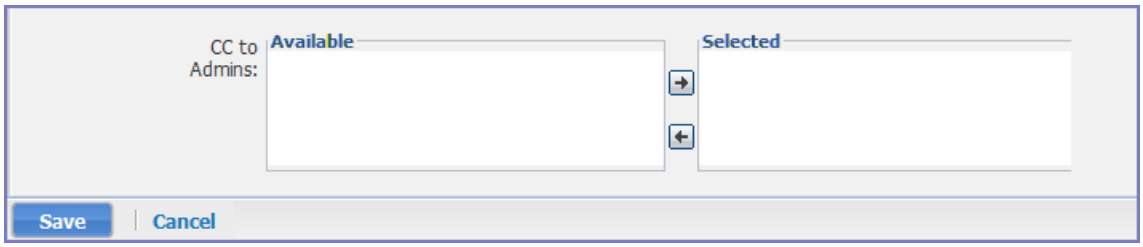


For each type of alert (i.e. SMS, email, and C2DM push notification), you can select to send the alert to one of the following:

- **None**
- **User only**
- **User + Admin**
- Admin only

If you select one of the Admin options, a **CC to Admins** section is displayed in the dialog box. This section displays a list of devices. Under the Available heading , select a device (or devices), that is associated with an email address that you want to notify, other than the device user. Core will send a notification to the email address associated with the device or devices that appear under the Selected heading.

FIGURE 12. CC TO ADMINS



NOTE: Only users who have registered devices can appear in the **Apply to Users** list.

Applying the event to a label

To specify the devices to which the event should apply, you select one or more labels when you create the event. The amount of time it takes to apply an event to a label depends on the number of devices identified by the label. Therefore, it may take some time for the label name to display as selected for the event.

Setting alert retries

You can specify the number of times MobileIron attempts to send an SMS alert or registration email.

Procedure

1. Enter the number of retries for SMS and registration email.
   Reminders are sent at 48-hour intervals until the number of reminders specified are sent, or the device is registered.
   For example, if you use the default for **Number of Retries for Email** (which is 2), an email is sent immediately after registration. If the device is not registered within 48 hours, a second email is sent. No other reminders are sent because you specified two reminders.
2. Click **Save**.

Setting MobileIron SMS, email, and push notifications

You can designate specific hours for the sending of SMS, email, and push notifications. The default notification time is 0300 (3 a.m.), which can be disruptive.

Procedure

To override the default notification schedule:

1. From the Admin Portal, go to **Settings > System Settings > General > Alert**.
2. Select the **Override Default Schedule SMS, Email, Push notification** check box. The section expands.
3. Enter the notification start time and end time, in UTC hours.

4. Select the days of the week when sending notifications are allowed.
5. Click **Save**.

Setting device push notifications

The Send Message feature provides device push notification support. The service enables you to:

- Check the validity and CRL of the certificate for every incoming request.
- Check for pending notifications for the device, if not maintain the connection for the configured time.
- Send a response if a pending event has been created.

NOTE: The notification pushed to the device might include an active URL. This URL can be opened in the Android client by clicking **GO TO LINK** in the notification.

Procedure

1. From the Admin Portal, go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Click **Actions > Send Message**. The **Send Message** dialog appears.
4. Select the **Push Notification** check box.
5. Click **Send Message**.

Android notification sync policy

The Android Notification Sync Policy allows you to specify the frequency and content of device updates.

Procedure

To set the Android Notification Sync Policy:

1. Go to **Policies & Configs > Policies**.
2. Click **Add New** > **Sync** to display the **New Sync Policy** dialog box.
   If there is already an existing Sync policy the **Modify Sync Policy** screen will be displayed.
3. Enter the name of the policy and a description if needed.
4. Enter the name of the ServerIP/Host Name.
5. Select the **Use TLS** check box.
6. Use the **Sync While Roaming** drop-down menu to specify what if any content is synced while the device is roaming.
7. Choose a type of notification using the **Android Notification Mechanism** drop-down menu.
8. Enter a **Hearbeat Interval** in minutes.
9. Enter a **Sync Interval** in minutes.
10. Enter an IOS Location-Based WakeUps Interval in minutes.

11. Enter a **MTD wakeup interval** in minutes. This interval determines how often Mobile@Work wakes up and scans a device. Settingt this value to a low interval, such as 5 minutes, is more taxing on the device's battery than setting it at a higher interval such as 30 minutes.
12. Click **Save**.

Event settings

Each event type has specific settings that need to be configured when you create or edit the event. This section describes the settings for each type.

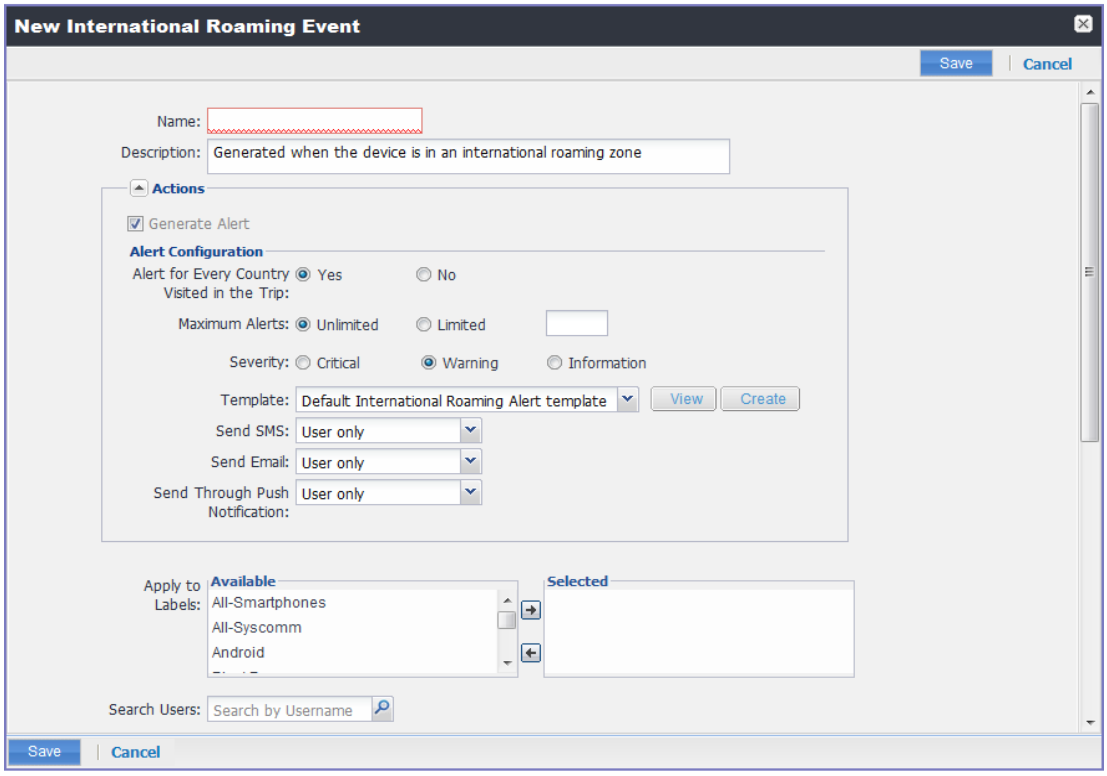
International roaming event settings

NOTE: International roaming detection is not supported for dual-mode devices (that is, devices that switch between GSM and CDMA).

Procedure

To create an international roaming event, in the Admin Portal:

1. Go to **Logs > Event Settings.**
2. Click **Add New**.
3. Select **International Roaming Event** from the drop-down menu. The New International Roaming Event dialog box opens.



4. Use the following guidelines to create an international roaming event:

Field	Description
Name	Identifier for this notification.
Description	Additional text to clarify the purpose of this notification.
Generate Alert	Turns on/off the alert defined for this event.
Alert for Every Country Visited in the Trip	Applies a compliance action for each country visited after the user leaves the home country.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for all countries within a given trip. If you select **Limited**, then you can specify the number of alerts to allow. Once the user returns to the home country, the count is returned to 0.
Severity	Specifies the severity defined for the alert: **Critical**, **Warning**, and **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See Customizing Event Center messages for information on creating a

Field	Description
	new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message via, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section displays. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Associate this event with the selected labels. See the “Using labels to establish groups” section in the *Core MobileIron Getting Started Guide* for more information.
Search Users	Enter the user ID to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with the selected users.
Search Admins	Enter the admin ID to find devices to which you want to apply this event.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the CC to Admins section appears. Use this section to specify administrative users who should receive the alert.

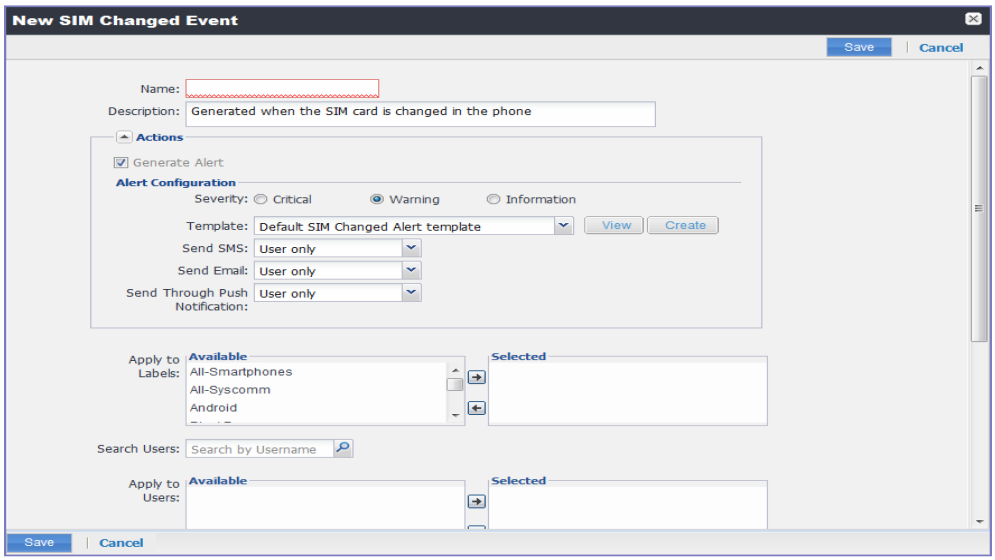
5. Click **Save**.

NOTE: If more than one international roaming event applies to a device, only the last one you edited and saved is triggered.

SIM changed event settings

To create a SIM changed event, in the Admin Portal:

1. Go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select **SIM Changed Event** from the drop-down menu. The New SIM Changed Event dialog box opens.



4. Use the following guidelines for creating a SIM changed event.

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this event.
Generate Alert	Turns on/off the alert defined for this event.
Severity	Specifies the severity defined for the alert: Critical, Warning, and Information.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See Customizing Event Center messages for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to

Field	Description
	the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Associate this event with the selected labels. See the “Using labels to establish groups” section in the *Core MobileIron Getting Started Guide* for more information.
Search Users	Enter the **user ID** to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with the selected users.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the **CC to Admins** section displays. Use this section to specify administrative users who should receive the alert.

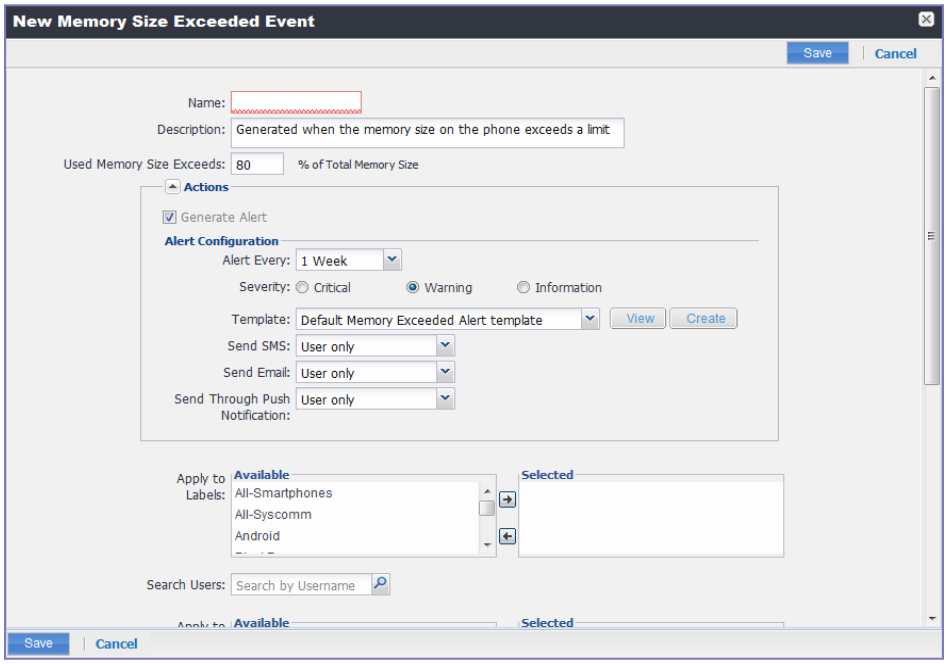
5. Click **Save**.

NOTE: If more than one SIM changed event applies to a device, only the last one you edited and saved is triggered.

Memory size exceeded event settings

To create a memory size exceeded event, in the Admin Portal:

1. Go to **Logs > Event Settings**.
2. Click **Add New.**
3. Select **Memory Size Exceeded Event** from the drop-down menu.



4. Use the following guidelines to create a memory size exceeded event:

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Used Memory Size Exceeds	Specifies the percentage of total memory that triggers the alert.
Generate Alert	Turns on/off the alert defined for this event.
Alert every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity defined for the alert: **Critical**, **Warning**, and **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See Customizing Event Center messages for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the

Field	Description
	Apply to Labels section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the admin, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Associate this event with the selected labels. See the “Using labels to establish groups” section in the *Core MobileIron Getting Started Guide* for more information.
Search Users	Enter the user ID to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with the selected users.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.

5. Click **Save**.

NOTE: Memory exceeded events are sent only once per week when the configured memory limit is reached. If more than one memory size exceeded event applies to a device, only the last one you edited and saved is triggered.

System event settings

A system event applies a compliance action when a component of a MobileIron implementation is not working. System alerts are intended for relevant administrators.

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.
2. Click **Add New**.

3. Select **System Event** from the drop down menu.
4. Use the guidelines in System event field description to complete the form:
5. Click **Save**.

System event field description

TABLE 58. SYSTEM EVENT FIELD DESCRIPTIONS

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Sentry (standalone and integrated) is unreachable	Applies a compliance action if MobileIron Core is unable to contact the MobileIron Sentry.
MobileIron gateway is unreachable	Select this option to send an alert if Core cannot connect to the MobileIron gateway.
LDAP server is unreachable	Select this option to send an alert if Core cannot connect to any of the configured LDAP servers.
DNS server is unreachable	Select this option to send an alert if Core cannot connect to one of the configured DNS servers.
Mail server is unreachable	Select this option to send an alert if Core cannot connect to the configured SMTP server.
NTP server is unreachable	Select this option to send an alert if Core connect to the configured NTP server.
Certificate Expired or Certificate Error	Select this option to send an alert for certificate expiration. An alert is sent 30 days before expiration and on the expiration date. Certificates supported include Admin Portal and device certificates.
Provisioning Profile Expired	This feature is not supported for Android devices.
SMTP Relay server is unreachable	Applies a compliance action if the configured SMTP relay (used for SMS archive) does not respond to a ping or SMTP ping.
SMTP Relay server error	Applies a compliance action if the configured SMTP relay (used for SMS archive) returns an error. The alert includes available details to enable troubleshooting.
System storage threshold has been reached	Applies a compliance action if the system storage threshold has been reached. Refer to *MobileIron Core System Manager Guide* for information on setting this threshold or manually purging the data.
Connector state events	Applies a compliance action if the health of the Connector changes. MobileIron defines a healthy connector as one that connects to the

TABLE 58. SYSTEM EVENT FIELD DESCRIPTIONS(CONT.)

Field	Description
	server at expected intervals and syncs successfully with the LDAP server. An alert is generated if a Connector changes from healthy to unhealthy, or from unhealthy to healthy.
Connector requires upgrade	Applies a compliance action if the automated upgrade of the Connector fails. This alert prompts you to manually upgrade the Connector.
Connector can not connect to LDAP server	Applies a compliance action if a configured LDAP server is no longer reachable.
Connector is unreachable	Applies a compliance action if the MobileIron server does not receive the expected response to the scheduled probe of the Connector. This alert generally indicates network problems.
Application update failed	Alerts the administrator that the Apps@Work or Bridge update for Windows failed. For more information, administrators can the server logs.
Android enterprise app requires new permission approval	Generates an alert if an Android enterprise app has new permissions that the administrator needs to approve in the App Catalog.
Mobile Threat Definition Update	Alerts administrators when a new version of the mobile threat definition is available. The notification includes any impacts to the existing MTD Local Action policies if threats were removed from the latest update.
Generate Alert	Turns on/off the alert defined for this event.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for a given event. If you select **Limited**, then you can specify the number of alerts to allow. By default, compliance is checked every 24 hours. See Managing Compliance and Creating an event for more information.
Alert Every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity defined for the alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See Customizing Event Center messages for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to**

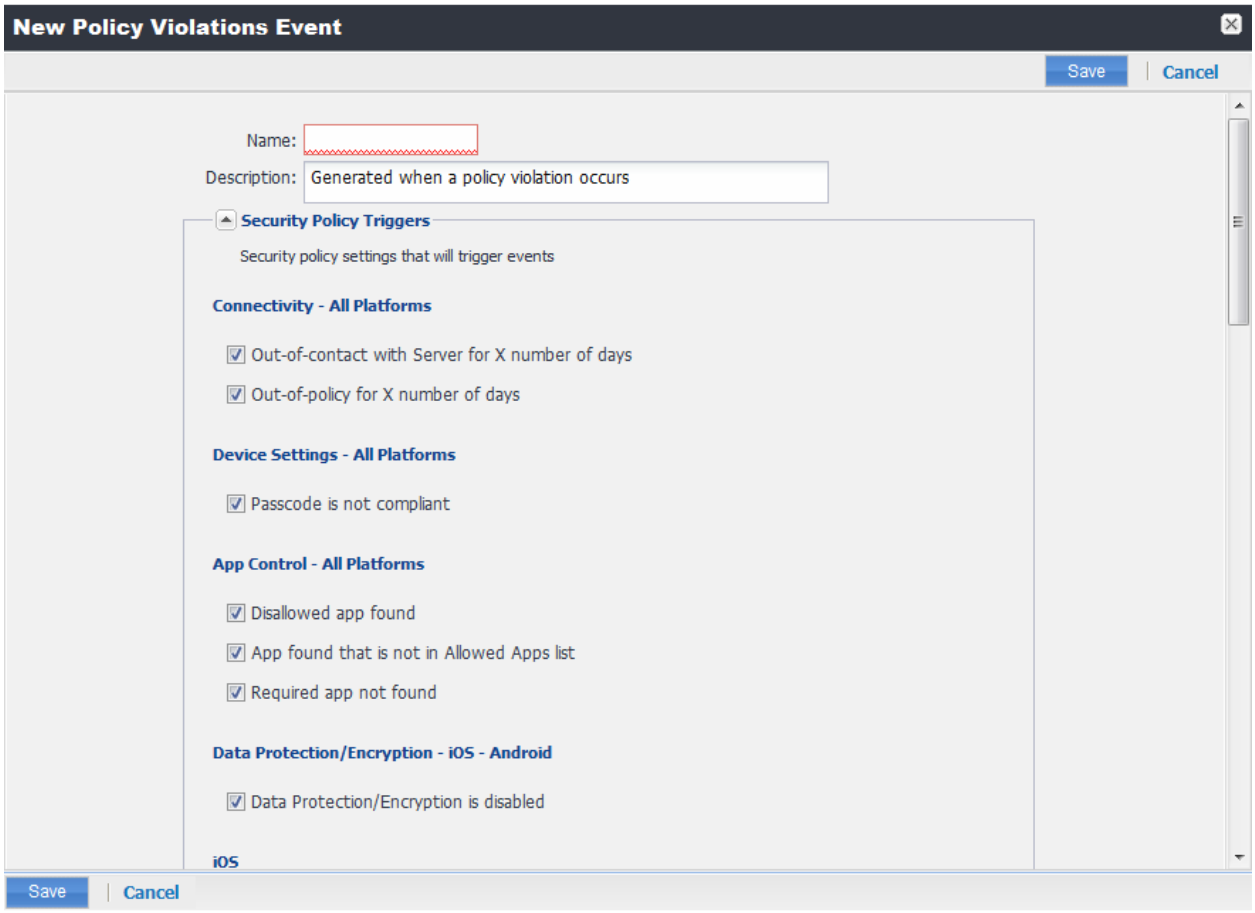
TABLE 58. SYSTEM EVENT FIELD DESCRIPTIONS(CONT.)

Field	Description
	Labels section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message via Android C2DM, and whether to send it to the user, administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the “Using labels to establish groups” section in the *Core MobileIron Getting Started Guide* for more information. NOTE: In most cases, if you do select a label, it should not be a label with broad coverage. System event alerts are usually not appropriate for device users.
Search Users	Enter the **user ID** to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.

Policy violations event settings

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select **Policy Violation Event** from the drop- down menu. The New Policy Violations Event dialog box opens.



4. Follow the guidelines in Policy violations event field description to complete the form.
5. Click **Save**.

NOTE: **Apply only one Policy Violations event to each device.** If more than one policy violations event applies to a device, only the last one you edited and saved is triggered. Therefore, do not create a separate policy violations event for each type of security policy violation.

In that one Policy Violations event, select all of the security policy settings that you want to trigger the event. Use the template variable $DEFAULT_POLICY_VIOLATION_MESSAGE in your message template to specify the security policy violation that triggered the event.

Policy violations event field description

The following table describes fields for configuring a policy violation event.

TABLE 59. POLICY VIOLATION EVENT FIELD DESCRIPTION

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Connectivity	
Out-of-contact with Server for X number of days	Select this option to send an alert when a device has been out of contact for the number of days specified in the Security policy assigned to it.
Out-of-policy for X number of days	Select this option to send an alert when a policy has been out of date for the number of days specified in the Security policy assigned to it.
Device Settings	
Passcode is not compliant	Applies a compliance action if a device is detected having a passcode that does not meet the requirements specified in the associated security policy.
App Control	
Disallowed app found	Applies a compliance action if an app that is specified as Disallowed is installed on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.
App found that is not in Allowed Apps list	Applies a compliance action if an app that does not appear on the list of allowed apps has been detected on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.
Required app not found	Applies a compliance action if an app that is specified as Required is not installed on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.
Data Protection/Encryption - iOS - Android	
Data Protection/Encryption is disabled	Applies a compliance action if an Android device has its Data Encryption feature turned off.
Security - Windows	
OS Build is less than the required OS build	Select this option to apply a compliance action if the device build is less than the OS build defined in the Security policy.
Last Hotfix is less than the required hotfix	Select this option to apply a compliance action if the device OS build is less than the hotfix build defined in the Security policy.
Last Hotfix installation date is out	Select this option to apply a compliance action if the device OS has not

TABLE 59. POLICY VIOLATION EVENT FIELD DESCRIPTION(CONT.)

Field	Description
of date	been updated in the time interval defined in the Security policy.
iOS	
Disallowed iOS model found	Select this option to apply a compliance action when a restricted iOS model is registered.
Disallowed iOS version found	Select this option to apply a compliance action when a restricted iOS version is registered.
Compromised iOS device	Select this option to apply a compliance action when a compromised iOS is registered or connects to the server. That is, an iOS device has been compromised by circumventing the operator and usage restrictions imposed by the operator and manufacturer.
iOS Configuration not compliant	Applies a compliance action if an iOS device does not have the expected security policy or app settings. This state may indicate that a setting was changed or was not applied successfully.
Restored Device connected to server	Applies a compliance action if a previously wiped device has been restored and attempts to connect through the MobileIron deployment.
MobileIron iOS App Multitasking disabled by user	Applies a compliance action if the device user disables multitasking for the MobileIron iOS app. Disabling multitasking increases the likelihood that a compromised device will go undetected for a significant period of time.
Device MDM deactivated (**iOS 5 and later**)	Applies a compliance action when the MDM profile on a managed iOS 5 device is removed.
macOS	
Disallowed macOS version found	Applies a compliance action if Core finds a registered device running a prohibited version of macOS.
Device MDM deactivated	Applies a compliance action if Core detects that MDM (Mobile Device Management) has been deactivated on a registered macOS device.
FileVault encryption disabled	Applies a compliance action if Core detects a registered macOS device with disabled FileVault encryption.
Android	
Disallowed Android OS version found	Applies a compliance action if an Android device having a disallowed OS version is detected. You can specify disallowed versions in the security policy.
Compromised Android device detected	Applies a compliance action if a modified Android device is detected. That is, an Android device has been compromised by circumventing the operator and usage restrictions imposed by the operator and

TABLE 59. POLICY VIOLATION EVENT FIELD DESCRIPTION(CONT.)

Field	Description
	manufacturer.
Device administrator not activated for DM client or agent	Generate an alert when a managed Android device is found to have no device administrator privilege activated for Mobile@Work or the Samsung DM Agent. NOTE: The Samsung DM Agent is not required on Samsung MDM 4.x, starting with Mobile@Work for Android version 5.9.
Actions	
Generate Alert	Turns on/off the alert defined for this event.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for a given event. If you select Limited, then you can specify the number of alerts to allow.
Alert Every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop down or click **Create** to create a new template. See Customizing Event Center messages on page 327 for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message via Android C2DM, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”,

TABLE 59. POLICY VIOLATION EVENT FIELD DESCRIPTION(CONT.)

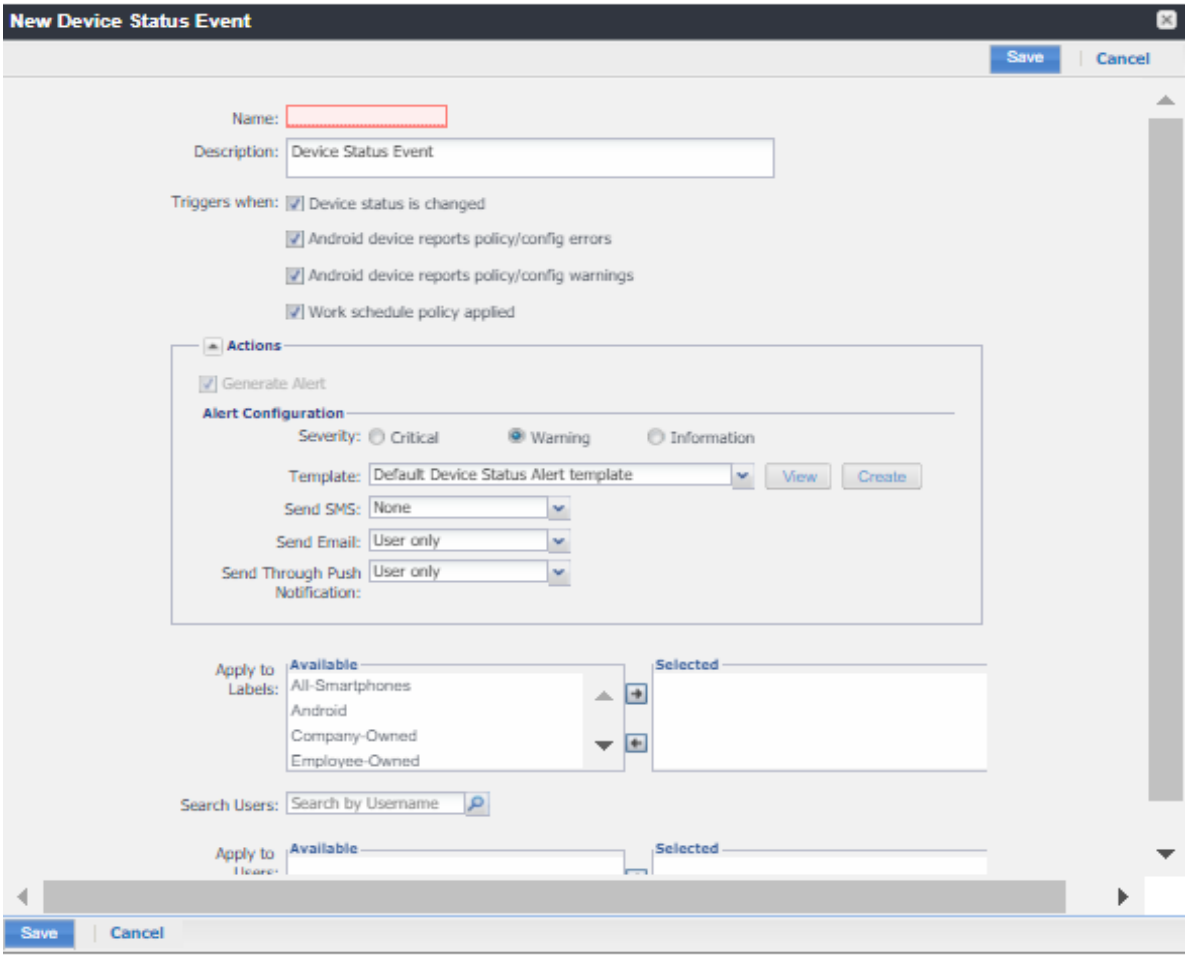
Field	Description
	then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the "Using labels to establish groups" section in the *Core MobileIron Getting Started Guide* for more information.
Search Users	Enter the user ID to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.
CC to Admins	If you selected "Admin only" or "User + Admin", then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.

Device status event settings

The device status event applies only to Android and iOS devices. The following describes the steps to create a device status event in the Admin Portal.

Procedure

1. Go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select **Device Status Event** from the drop-down menu. The New Status Event dialog box opens.



4. Use the following guidelines to complete the form:

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Triggers when	Specifies the conditions on the device that will trigger an alert: • Device status is changed (Android and iOS) • Android device reports policy/config errors • Android device reports policy/config warnings • Work schedule policy applied (Android and iOS)
Actions	
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.

Field	Description
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See Customizing Event Center messages for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the “Using labels to establish groups” section in the *Core MobileIron Getting Started Guide* for more information.
Search Users	Enter the user ID to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.

5. Click **Save**.

NOTE: If more than one device status event applies to a device, only the last one you edited and saved is triggered.

Related topics

Work Schedule policy

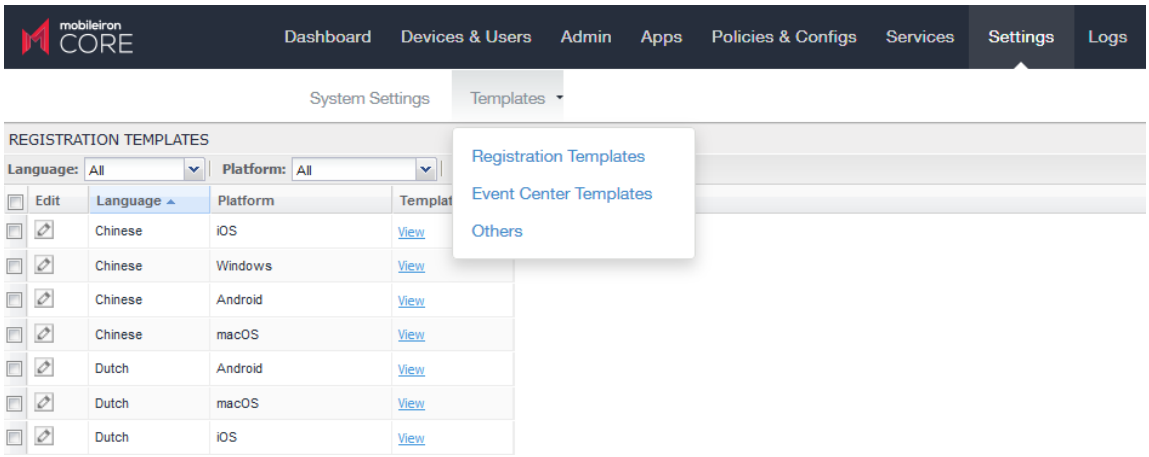
Customizing Event Center messages

The MobileIron Event Center sends emails, SMSes, and push notification messages based on triggering events. When you configure events, you can use the default message template or create a new one. Event Center templates enable you to specify content and basic formatting using HTML markup.

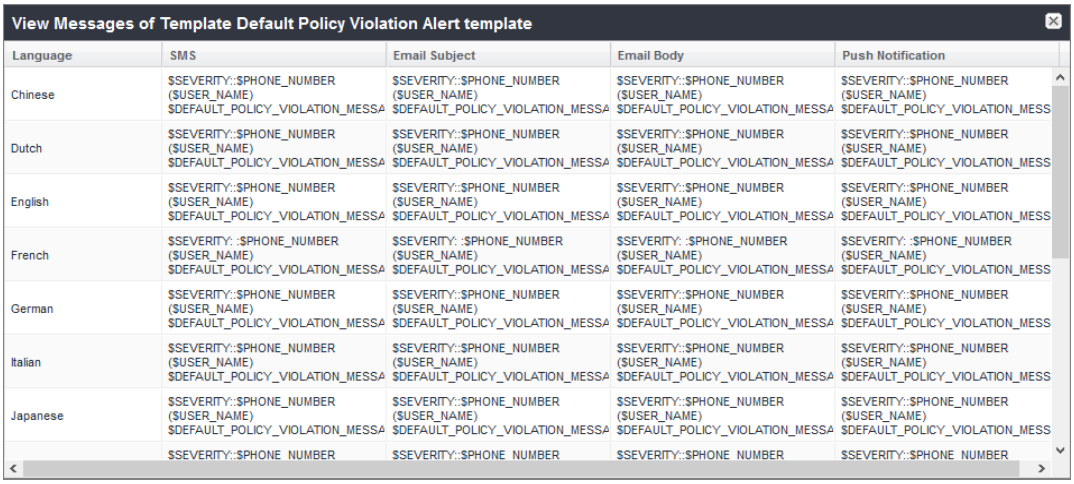
Displaying Event Center templates

To display Event Center templates:

1. In the Admin Portal, go to **Settings > Templates**.



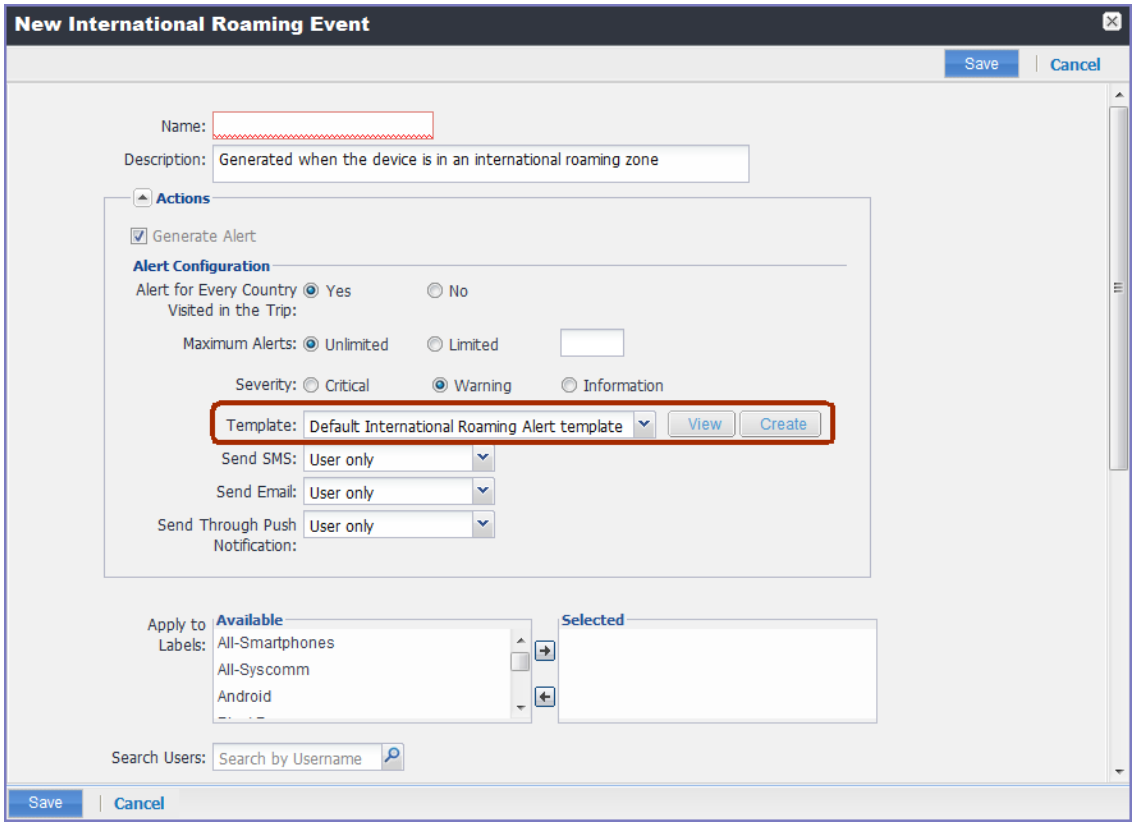
2. Select **Event Center Templates**.
   This list includes the default template for each Event Center type. Default templates are not editable.
3. Click the **View** link for the message template you want to view.



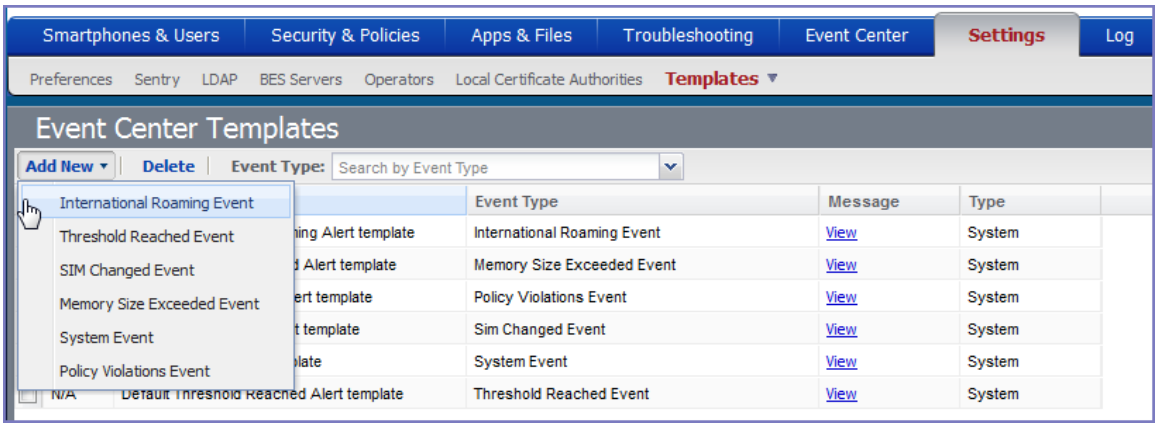
Adding custom Event Center messages

To add a custom Event Center message:

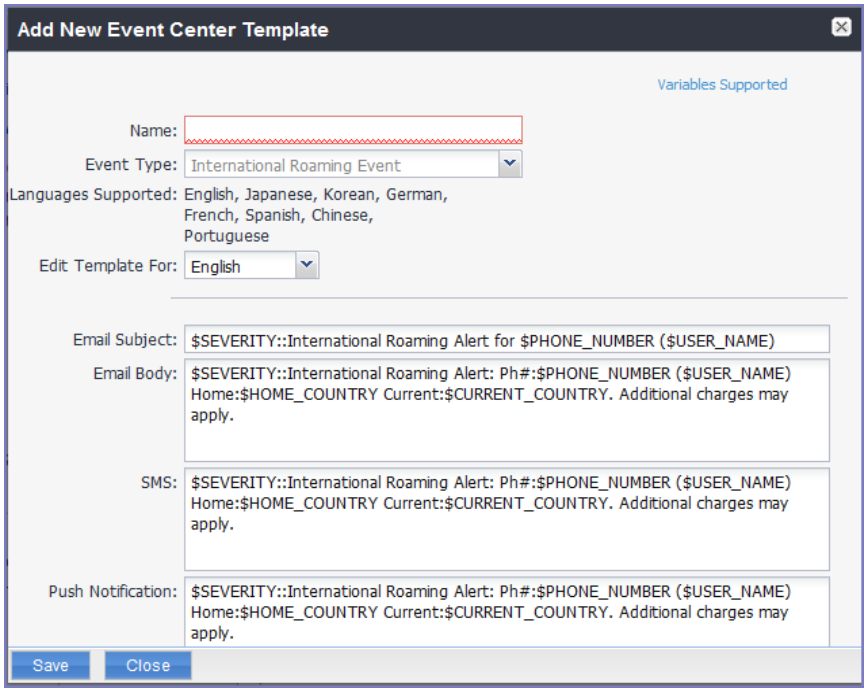
1. Either click the **Create** button in the event dialog or select the event type from **Settings > Templates > Event Center Templates > Add New**.
   The following figure shows the event dialog.



2. The following figure shows the Event Center Templates menu.



The dialog for the corresponding event type opens.



Event Center messages are displayed with the HTML markup that provides the basic formatting for the content.

3. In the **Name** field, enter a name for the template.
   The name must be unique for events of the same type.
4. In the **Edit Template for** field, select the language this template will be used for.
   Note that only those languages that have been enabled for the system will be displayed in this list.
5. Make changes to the displayed messages.
6. Click **Save**.

Using variables in Event Center messages

Supported and required variables for Event Center messages vary by the type of message. The following table summarizes these variables. You can also click the **Variables Supported** link to display this information. Note that, unlike variables used for registration variables, Event Center variables do not end with $.

TABLE 60. VARIABLES IN EVENT CENTER MESSAGES

Template Type	Required Variables
International Roaming	$CURRENT_COUNTRY $HOME_COUNTRY $PHONE_NUMBER $SEVERITY $USER_NAME
Threshold Reached	$PHONE_NUMBER $SEVERITY $THRESHOLD_ON $THRESHOLD_TYPE $THRESHOLD_UNIT $THRESHOLD_VALUE $USED_VALUE $USER_NAME
SIM Changed	$CURRENT_PHONE_NUMBER $NEW_PHONE_NUMBER $SEVERITY $USER_NAME
Memory Size Exceeded	$FREE_MEMORY_SIZE $MEMORY_SIZE_LIMIT $PHONE_NUMBER $SEVERITY $TOTAL_MEMORY_SIZE $USER_NAME
System Event	$DEFAULT_SYSTEM_MESSAGE $SERVER_IP $SERVER_NAME $SEVERITY
Policy Violation	$DEFAULT_POLICY_VIOLATION_MESSAGE $PHONE_NUMBER $SEVERITY $USER_NAME

Variable descriptions

The following table describes the variables used in Event Center messages.

TABLE 61. VARIABLE DESCRIPTIONS

Variable	Description
$CURRENT_COUNTRY	The country in which the device is currently located.
$CURRENT_PHONE_NUMBER	The phone number currently associated with the device in MobileIron Core, but not matching the phone number currently used by the device.
$DEFAULT_POLICY_VIOLATION_ MESSAGE	The hard-coded message associated with the policy violation that triggered the alert. NOTE: Due to the length limits of SMS and C2DM, the text might be truncated.
$DEFAULT_SYSTEM_MESSAGE	The third-party system message or error that triggered the alert.
$FREE_MEMORY_SIZE	The amount of free memory currently available on the device.
$HOME_COUNTRY	The home country of the device.
$MEMORY_SIZE_LIMIT	The threshold set for the device memory.
$NEW_PHONE_NUMBER	The phone number replacing the $CURRENT_PHONE_ NUMBER$ as a result of a SIM change.
$PHONE_NUMBER	The phone number used by the device.
$SERVER_IP	The IP address of the server triggering a system event alert.
$SERVER_NAME	The hostname of the server triggering the system event alert.
$SEVERITY	The defined severity of the system event, i.e., Information, Warning, or Critical.
$THRESHOLD_ON	The total used for calculations, i.e., International Roaming or Total Usage.
$THRESHOLD_TYPE	The type of usage measured, i.e., SMS, Data, or Voice.
$THRESHOLD_UNIT	The unit associated with the type of usage, i.e., minutes, messages, or MB.
$THRESHOLD_VALUE	The defined threshold value for this event, e.g., 1000 (voice minutes).

TABLE 61. VARIABLE DESCRIPTIONS (CONT.)

Variable	Description
$TOTAL_MEMORY_SIZE	The total memory reported by the device.
$USED_VALUE	The amount of memory currently used on the device.
$USER_NAME	The display name of the user associated with the device.

Specifying which template to use

When you create or edit an event, you specify which template to use for resulting alerts. To select a template:

1. Create or edit an event.
2. Select a template from the drop-down or click the **Create** button to create a new template.

Filtering Event Center messages

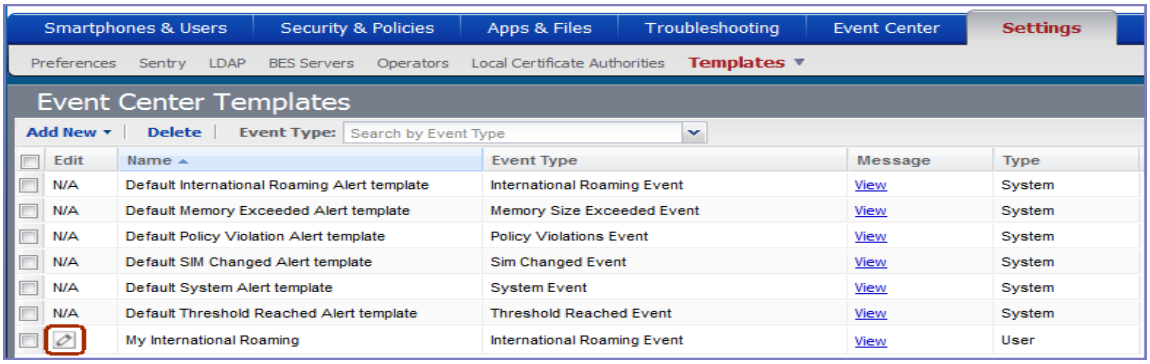
In the Event Center Templates page, you can filter messages by event type. Just select the preferred event type from the **Event Type** drop-down.

Editing Event Center messages

You can edit your custom Event Center templates. However, default Event Center templates are not editable.

To edit a custom Event Center template:

1. In Admin Portal, go to **Settings > Templates > Event Center Templates**.



2. Click the edit icon for the custom template you want to edit.
3. Make your changes.
4. Click **Save**.

Deleting Event Center messages

You can delete any of the Event Center messages you have created:

1. In Admin Portal, go to **Settings > Templates > Event Center Templates**.
2. Select the items you want to delete.
3. Click **Delete**.

Viewing and Exporting Events

Use the Events screen to track the events that have triggered alerts. To display the Events screen, go to **Logs > Events**.

Marking as Read or Unread

To enable tracking of which events have been noted and/or addressed by an administrator, you can mark an event as **Read**. Likewise, you can switch this flag back to **Unread**.

To set the Read/Unread flag:

1. Select one or more events.
2. Select **Read** or **Unread** or from the **Actions** menu.

Filtering events

You can display the events using the following filters:

TABLE 62. FILTERING EVENTS

Filter	Description
Read/Unread	Select **Read** or **Unread** from the **Show** drop-down list. To resume displaying all events, select **All**.
All	Select **All** to resume displaying all events.
Labels	Select the preferred label from the **Labels** drop-down to filter based on the label specified in the event.
User	Enter a user ID and click the search icon to filter based on the user IDs specified in the event.
Start Date/End Date	Select dates in the **Start Date** and **End Date** fields to filter events by date range.
Event Type	Select an event type from the **Type** drop-down to filter by event type.
Event Status	Select an event status from the status drop-down to filter based on the event's lifecycle state.

Event lifecycle and status

Events go through the following lifecycle:

Created -> Dispatch Pending -> Dispatching -> Dispatched

The following two failure states may also occur:

- Dispatch Failed: The process of generating the alert failed. This is usually the result of an SMTP problem. Check the SMTP configuration in System Manager, as well as the health of your SMTP server.
- Expired: Another event occurred that makes the alert obsolete, resulting in expiration before dispatch.

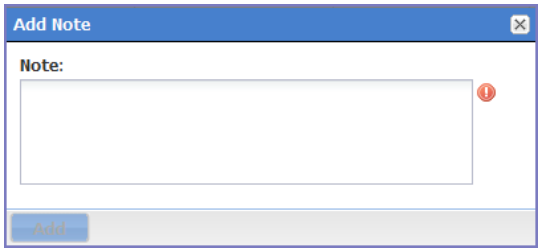
Exporting event history

To export a CSV file containing the currently displayed events on the **Logs > Events** page, click the **Export** button.

Adding a note

You can add a note to one or more events to help track the work that has been done in response. Each event can hold one note; adding another note replaces the existing note. To add a note:

1. Select one or more events.
2. Click **Actions > Add Note**.



3. Enter the text of the note.
4. Click **Add**.
5. Press F5 to refresh the screen and confirm that the note displays in the Note field for the selected events.

Troubleshooting MobileIron Core and devices

This section addresses troubleshooting various aspects of Core and devices.

About Core logs

As you oversee management and security of users, data and devices, you will need information about the actions and events that occur in your MobileIron Core instance. MobileIron Core logs many actions that can impact your Core instance, and provides the Audit Logs page for you to sort and view the logged information.

The following pages of logs, found in the Admin Portal under **Logs**, enable you to easily navigate through the MobileIron log entries to find the information you need.

- **Audit Logs**: for MobileIron device management entries
- **MDM Activity**: for Android MDM entries
- **Certificate Management**: for certificate-related entries

Note The Following:

- Logs are stored in the MobileIron Core file system, not in the MobileIron Core database. Therefore, the size of the logs does not impact Core performance.
- Core will show up to 1 million audit log records.

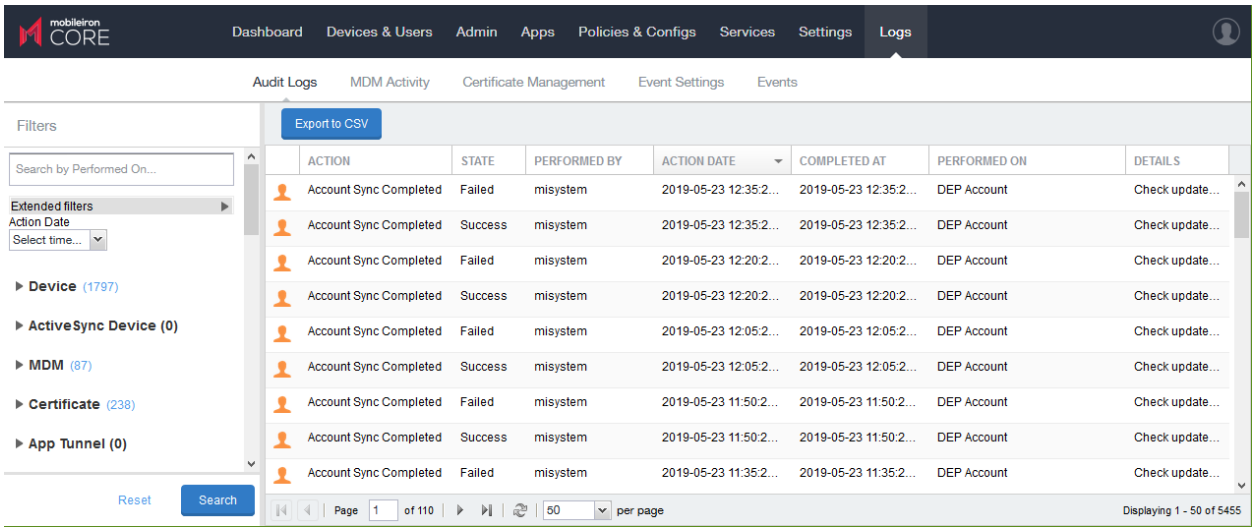
Audit logs

Using log entries, the Admin Portal tracks status and operations for each managed device. You can use log entries to confirm that actions were completed and to investigate problems.

The Audit Logs page includes panels that:

- enable you to filter through all events that Core has logged since the last time the logs were purged
- shows either the events recorded since the logs were last purged, or the events matching the criteria you specified in the Filters panel

FIGURE 13. AUDIT LOGS

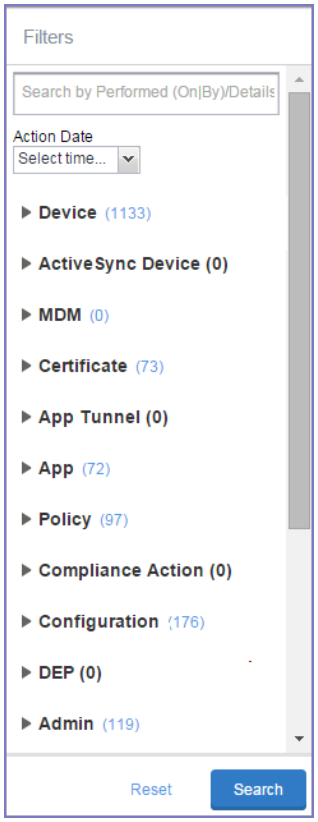


Searching the information in the audit logs

Procedure

To search the information that Core logs:

1. In Admin Portal, go to **Logs**.
   Core displays the Audit Logs page, which initially lists the events logged since the last time the logs were purged.
2. In the **Filters** panel, click on the number of events in a category to display only that category's events.
   For example, click the **72** next to **App**.



3. Alternatively, click to expand one of the information types that you want to view (for example, **App**).
4. Check the items within that category that you want to view (for example, **Add App** and **Install App**).
5. Repeat Step 3 and Step 4 for each category that you want to include in this search.
6. (Optional) To search for events involving a particular administrator, or actions that contain a specific word or phrase in the details, use the **Search by Performed (On|By)/Details** box in the Filters panel as follows:
   - enter the search string in the text box.
   - for example, to find events involving Mobile@Work, enter the text **Mobile@Work.**
7. (Optional) To limit the time frame of the actions, use the **Action Date** box (see Setting event time criteria in audit logs on page 337)
8. Click **Search**.
   The Audit Logs page shows all events matching your search criteria and time period. If you do not specify a time period, the default used is the period between the time you run the search and when the log data was last purged.
9. To reset all search criteria, click **Reset**.

Setting event time criteria in audit logs

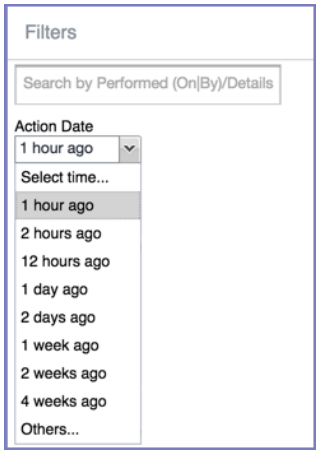
When you are working with audit logs, the default time frame for the events displayed is the time between the current time and the last time the logs were purged (for information about setting the log retention time, see

Specifying how long log information is saved). For example, if the logs were purged two weeks ago, the Audit Logs display all the events matching any criteria you set that occurred from two weeks ago to the current moment.

You can change the time frame of events you view in the **Filters** panel. You can select by time or date.

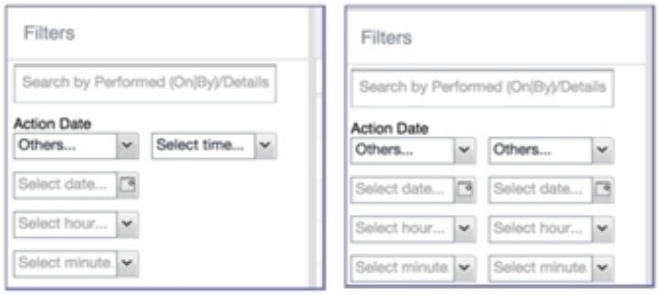
To specify a time frame for events you view from the audit logs:

1. In Admin Portal, go to **Logs**.
2. In the Filters panel, click the drop-down arrow in **Action Date**.



3. Select one of the times listed or **Others**.
   Selecting a time displays the events matching criteria you set, if any, for the time period from the last time the logs were purged until the time you specify.
   Any events that occurred between the specified time period and the current moment are not displayed. For example, if you select **1 hour ago**, no events that happened within the last hour are displayed.
4. If you select **Others**:
   - using the left column of time choices in Filters, you can specify an exact date, hour or minute (or any combination of these criteria) as one end of the time frame and use the date of the last audit log purge as the other end of the time frame
   - using the left and right columns of time choices in Filters, you can specify both the beginning and end of the time range.

   Use the following table to help you set the time range for your search.



Note The Following:

- When you set only one end of the time frame, the date or time you specify must be later than the last date the log data was purged. If the last log purge was May 13th, for example, May 12th would not be a valid date for selecting events.
- When you set both ends of the time frame, ensure that the time or date specified in the left column occurs before the time or date specified in the right column. For example, if you specify **1 hour ago** in the left column and **1 day ago** in the right column, Core will display a message asking you to reset your time criteria because 1 hour ago happens after 1 day ago.

TABLE 63. TIME CRITERIA SELECTION EXAMPLES

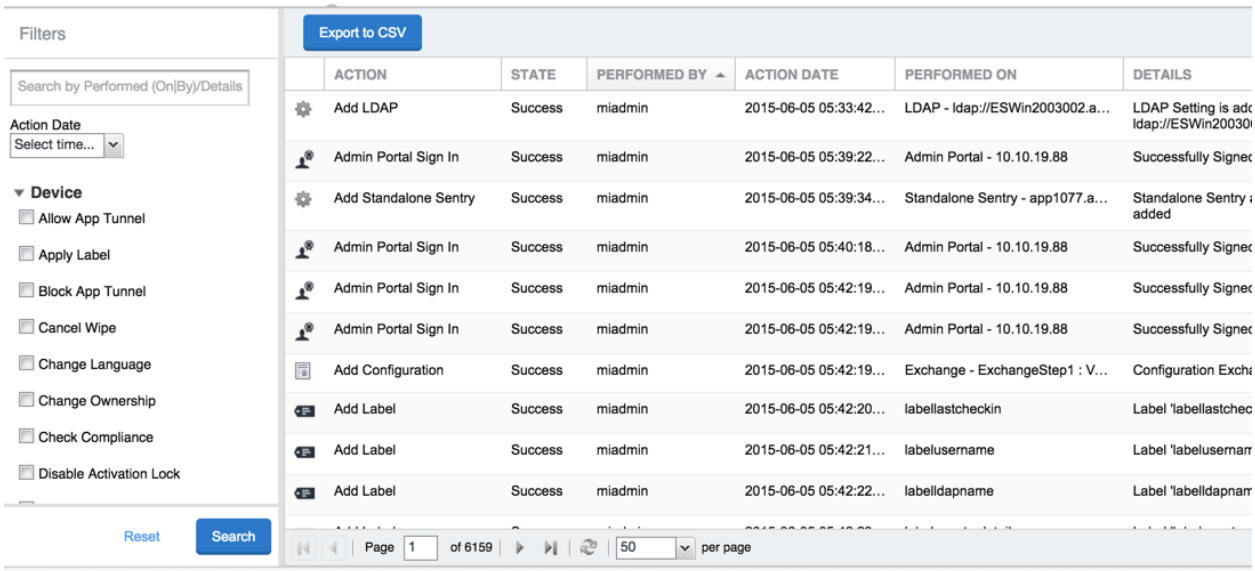
Time criteria selected	Value selected	Result
In the left column, select both: • **Others** • **Select date**	Click May 12th in the displayed calendar	Displays all events matching your criteria that occurred from the last audit log data purge until May 12th.
In the left column, select both: • **Others** • **Select hour**	Select 2AM from **the list of hours**	Displays all events matching your criteria that occurred from the last audit log data purge until 2AM of the current day.
In the left column, select both: • **Others** • **Select minute**	Select 15 from the list of **minutes**	Displays all events matching your criteria that occurred from the last audit log data purge until the 15th minute of the current hour.
In the left column, select: • **Others** • Select date In the right column, select: • a time interval from **Select time**	In the left column: • Select **April 10th** from the calendar In the right column: • Select **1 day ago**	Displays all events matching your criteria that occurred between April 10th and 24 hours ago.
In the left column, select: • **Others** • Select hour In the right column, select: • a time interval from **Select time**	In the left column: • Select **2AM** In the right column: • Select 1 hour ago	Displays all events matching your criteria for the time period that started at 2AM the morning of the current day and ended an hour ago.

Viewing audit log information

The Audit Logs page displays the information that MobileIron Core records for your Core instance. You specify what information is displayed on this page when you use the controls in the **Filters** panel of the page. See Searching the information in the audit logs for details.

To view the information that Core logs:

1. In Admin Portal, go to **Logs**.
   Core displays the Audit Logs page. The information panel displays:
   Action (for example, Admin Portal sign-in)



   - **State** (for example, **Success**)
   - **Performed By** (for example, **myadmin**)
   - **Action Date**
   - **Completed At**
   - **Performed On** (for example, **Admin Portal**)
   - **Details**
2. (Optional) Enter a number in **Page** to specify what page to view.
3. (Optional) Select a number from **per page** to specify how many records are displayed on a page.
4. (Optional) Click **Export to CSV** to export the records that match the current search criteria.

Specifying how long log information is saved

You specify how long log data is retained on your server. Determining how long to retain data is a balance between having data you need and having the available server resources to run your Core. The default value is 90 days.

To set how long log information is kept:

1. In System Manager, go to **Settings > Data Purge**.
2. In **Audit Logs Purge Configuration**, select the number of days Core retains log information.
3. Click **Apply**.

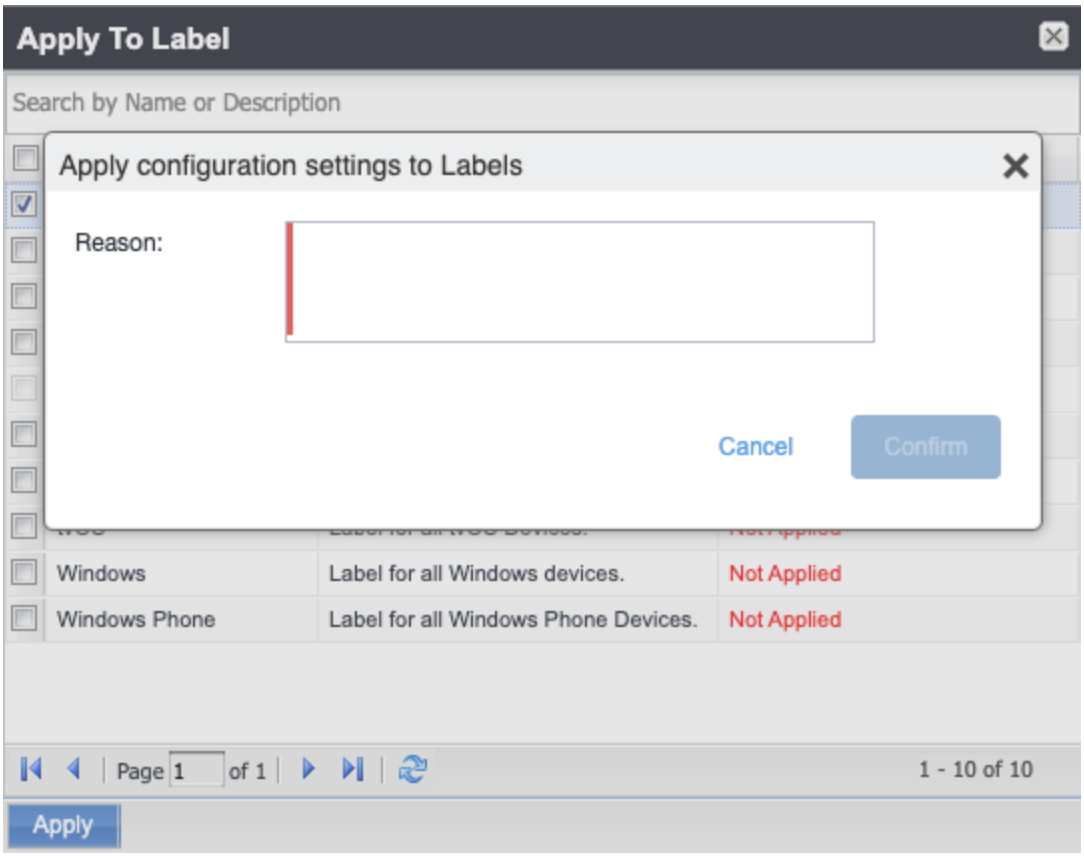
Audit log information

Several categories of information are available for you to view and audit. The category list, displayed on the left side of the Audit Logs page, includes:

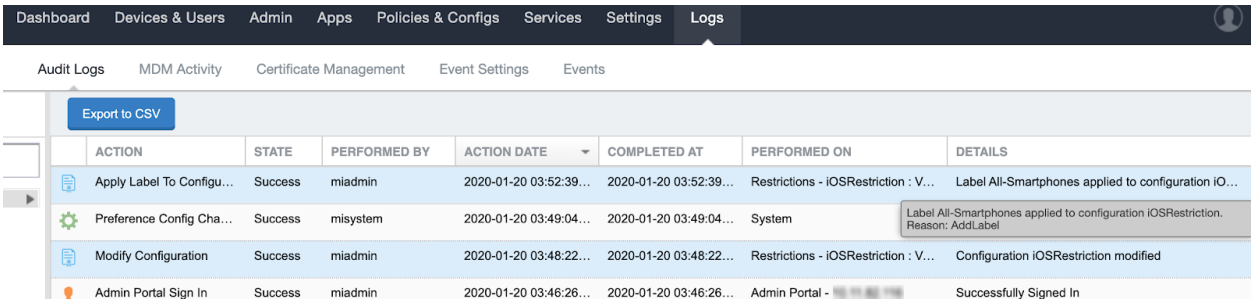
- **Device**
- **ActiveSync Device**
- **MDM**
- **Certificate**
- **App Tunnel**
- **App**
- **Policy**
- **Compliance Action**
- **Configuration**
- **DEP (Device Enrollment)**
- **Admin**
- **User**
- **LDAP**
- **Other**
- **Label**
- **Sentry**
- **AfW**
- **Custom Attributes**
- **Compliance Policy**
- **E-FOTA**
- **Migration**
- **MTD (MobileIron Threat Defense)**
- **Access Integration**
- **Derived Credential Provider**
- **Zebra FOTA**

Best practices: label management

If Notes for Audit Logs is enabled, whenever a change is made to a label, a text box displays for the administrator to provide a reason for the change.



Example text to enter would be a change ticket order number. This information then displays in the Audit logs, in the Details column as "Reason."



This affects the following label-related activities:

- Add/Edit/Delete/Save Label (Both filter and manual)
- In **Devices & Users > Devices > Advanced Search > Save to Label**
- Add/Edit/Remove Label to devices

- Add/Edit/Remove Label to configurations
- Add/Edit/Remove Label to policies
- Add/Edit/Remove Label to apps
- Add/Edit/Remove Label to iBooks

The Notes for Audit Logs feature is also applicable to any administrator-made changes to iOS and macOS restrictions.

To enable this feature, see "Setup tasks" in *Getting Started with MobileIron Core.*

Device events

Device events record device-related actions taken by an administrator in the Admin Portal.

To monitor device actions, select one or more of the logged device actions in the **Filters** panel:

- **Allow App Tunnel**: Manually allow app tunnels from the selected device.
- **Apply Label**: Associate an item with a label.
- **Apply Multiple Labels to One Device**: Associate an item with multiple labels.
- **Block App Tunnel**: Manually disallow app tunnels from the selected device.
- **Cancel Wipe**: Cancel an attempt to restore a device to factory defaults.
- **Change Language**: Change the language associated with a device.
- **Change Ownership**: Toggle device ownership between Employee and Company.
- **Check Available OS Update**:
- **Check Compliance**: Check device against compliance criteria.
- **Delete Retired Device**: Remove entry for a device that is not longer managed.
- **Device Location**:
- **Disable**:
- **Disable Activation Lock**: Turn off the activation lock feature for the selected iOS device.
- **Disable Data Roaming**: Turn off the ability to use data when the device is roaming.
- **Disable due to out of compliance**:
- **Disable Kiosk**: Exit kiosk mode on the designated Android device.
- **Disable KNOX Container**: Turn off the Samsung KNOX container feature for the selected device.
- **Disable Personal Hotspot**: Prevent the device user from using the personal hotspot feature.
- **Disable Voice Roaming**: Turn off the ability to make voice calls when the device is roaming.
- **Download Available OS Update**:
- **Enable**:
- **Enable Activation Lock**: Turn on the activation lock feature for the selected iOS device.

- **Enable Data Roaming**: Turn on the ability to use data while roaming for the selected iOS device.
- **Enable Kiosk**: Start kiosk mode on the designated Android device.
- **Enable KNOX Container**: Turn on the Samsung KNOX container feature for the selected device.
- **Enable MDM Lost Mode**: Enable lost mode for the selected iOS device.
- **Enable Personal Hotspot**: Allow the device user to use the personal hotspot feature.
- **Enable Voice Roaming**: Turn on the ability to make voice calls when the device is roaming.
- **Found**: Designate the selected lost device as found.
- **Install Downloaded OS Update**:
- **Install Help@Work**: Install the MobileIron Help@Work app.
- **Locate**: Retrieve the last known location for the selected device.
- **Lock**: Force the selected device to require a passcode for user access.
- **Lost**: Designate the selected device as lost.
- **MobileIron Bridge**: Create a configuration for the MobileIron Bridge application for Windows 10 Management.
- **Push Profile**: Prompt a manual distribution of profiles to the selected device.
- **Re-provision Device**: Restart the provisioning process for the selected device.
- **Reboot**: Reboot the selected Windows device.
- **Register Device**: Start the registration process for the selected device.
- **Remote Control**: Establish a remote control session (Help@Work) on the selected Android device.
- **Remote Display**: Establish a remote view session (Help@Work) on the selected iOS device.
- **Remove Device Attribute**: Remove an attribute from a device.
- **Remove Label**: Remove the association between the specified label and the selected item.
- **Remove Multiple labels from one device**: Remove the association between the specified labels and the selected item.
- **Request Derived Credential: Device user request in user portal for a derived credential.**
- **Request Unlock AppConnect Container** (Android only): Initiate unlock AppConnect container.
- **Request Unlock Device**: Initiate unlock device.
- **Request Unlock Passcode**: Initiate unlock passcode.
- **Resend Provision Message**: No longer supported.
- **Reset AppConnect Passcode:** Device user request in user portal to reset the AppConnect passcode.
- **Reset Password:**
- **Restart iOS Device**: Restart iOS device.
- **Reset PIN**: Generate a new registration PIN for the selected Windows device.
- **Retire**: End management of the selected device.
- **Send Activation Lock Bypass Code**: Send the bypass code to the selected iOS device.

- **Send Alert**: Send compliance alert to the selected device.
- **Send APNS message**: Launch a MobileIron client and authenticate against MobileIron Core.
- **Send Message**: Send SMS message to the selected device.
- **Set Device Attribute:** Set an attribute to a device.
- **Shutdown iOS Device**: Shutdown iOS device.
- **Sign In**: Launch a MobileIron client and authenticate against MobileIron Core.
- **Sign Out**: End session between the MobileIron client and MobileIron Core.
- **Substitution Variable Change**: Change a configuration due to a change in the value of a substitution variable.
- **Unlock AppConnect Container** (Android only): Begin unlock device and AppConnect container.
- **Unlock Device and AppConnect Container**: (Android only): Begin unlock device and AppConnect container.
- **Unlock Device Only**: Clear the passcode for the selected device.
- **Update Device Comment**: Change the Comment field in the record for the selected device.
- **Update OS Software:** Update iOS software.
- **Wakeup**: Force the device client to check in.
- **Windows License:** Alert administrators to upgrade the SKU of Windows 10 desktop devices. Options can be Windows 10 Pro to Enterprise or Windows 10 Education to Enterprise.
- **Wipe**: Return the device to factory default settings.

NOTE: Events beginning with **Request**, such as **Request Unlock Device**, are logged when an administrator clicks the corresponding command in the Admin Portal. The corresponding event without the word **Request**, such as **Unlock Device**, is logged when Core actually sends the request to the device. Core sometimes delays sending requests to regulate Core performance.

ActiveSync Device information

These events do not apply to Mac devices.

To monitor ActiveSync device actions, select one or more of the logged ActiveSync device actions in the **Filters** panel

- **ActiveSync Device Comment**: Add or change the comment associated with an ActiveSync device entry.
- **Add Correlation:**
- **Allow Device**: Allow a blocked ActiveSync device to access the ActiveSync server.
- **Assign ActiveSync Policy**: Apply an ActiveSync policy to the selected device.
- **Block Device**: Prevent the selected device from accessing the ActiveSync server.
- **Link To MI Device**: Associate an ActiveSync device with a device registered with MobileIron Core.
- **Remove**: End the association between the MobileIron Core device and the ActiveSync device record.

- **Remove Correlation:**
- **Revert ActiveSync Policy**: Restore the Default ActiveSync Policy to the selected device.

MDM events

MDM events indicate when a device takes an action due to a MobileIron Core request. These events pertain only to iOS and Mac devices unless otherwise noted.

To monitor these actions, select one or more of the logged MDM actions in the **Filters** panel.

- **Apply Redemption Code**: Apply Redemption Code: Use a Apple License code.
- **Clear Passcode**: Clear Passcode: Reset device passcode.
- **Device Lock**: Set screen lock on device.
- **Install Encrypted Sub-Profile:**
- **Install Managed Application**: Install a managed app.
- **Install MDM Profile**: Install the MDM profile on the device.
- **Install Provisioning Profile**: Install the provisioning profile for a managed app.
- **Lock Device (Android):** Lock an Android device.
- **Profile Change**: Change the profile on an iOS or Android device.
- **Remove Encrypted Sub-Profile:**
- **Remove Managed Application**: Uninstall a managed app.
- **Remove MDM Profile**: Remove the MDM profile from the device.
- **Remove Provisioning Profile**: Remove the provisioning profile for a managed app.
- **Settings**: Modify device settings.
- **Unlock Device (Android)**: Unlock an Android device and the AppConnect container on the device.
- **Unlock Device Only (Android)**: Unlock an Android device.
- **Wipe Device** (called **Erase Device** in the **MDM Activity** tab): Restore the iOS device to factory defaults.
- **Wipe Device (Android)**: Restore the Android device to factory defaults.

NOTE: This MDM log information is also provided in the **Logs > MDM Activity** tab.

Certificate events

To monitor actions involving certificates, select one or more of the logged certificate actions in the **Filters** panel.

- **Apply User Provided Certificate**: Use a certificate already provided by the user and sent to MobileIron Core.
- **Create Device Certificate**: Issue a device certificate.

- **Create User Certificate**: Issue a user certificate.
- **Delete User Provided Certificate**: Destroy certificate provided by the user via the self-service portal.
- **Device Certificate Expired**: Warn on a device certificate that is no longer valid due to expiration.
- **Device Certificate Renewal**: Re-enrolls a device certificate.
- **Reuse Device Certificate**: Use an existing device certificate.
- **Reuse User Certificate**: Use an existing user certificate.
- **Revoke Device Certificate**: Reclaim a device certificate.
- **Revoke User Certificate**: Reclaim a user certificate.
- **Upload User Provided Certificate**: Send certificate provided by the user via the self-service portal.
- **User Certificate Expired**: Warn on a user certificate that is no longer valid due to expiration.
- **User Certificate Renewal**: Re-enroll a user certificate.

NOTE: The contents of the **Logs > Certificate Management** shows information about certificates, such as their expiration dates. It allows you to take actions, such as re-enroll, remove, and revoke on the certificates.

App Tunnel events

To monitor actions involving app tunnels, select one or more of the logged app tunnel actions in the **Filters** panel.

- **Allow App Tunnel**: Permit the specified app tunnel.
- **App Tunnel Comment**: Add a comment on the selected app tunnel.
- **Block App Tunnel**: Do not allow the specified app tunnel.
- **Remove App Tunnel**: Delete the selected app tunnel configuration.

App information

To monitor actions involving apps, select one or more of the logged app actions in the **Filters** panel.

- **Add App**: Add an app to the app catalog.
- **Add App Control Rule**: Add an app control rule.
- **Add App Dependency**:
- **Add App Resource**: Add screenshots or icons for an app.
- **Apply Label to App**: Associate a label with an app.
- **Delete App Control Rule**: Remove an app control rule.
- **Edit App Control Rule**: Change one or more attributes of an app control rule.
- **Install App**: Send installation request for the selected app.
- **Manage VPP Labels**: Specify labels and account for Apple License app distribution.

- **Modify App**: Edit app catalog entry.
- **Remove App**: Delete entry from the app catalog.
- **Remove Label From App**: End the association between an app and a label.
- **Uninstall App**: Remove the app from the device based on managed app criteria.

Policy information

To monitor actions involving policies, select one or more of the logged policy actions in the **Filters** panel.

- **Activate Policy**: Set flag to make the selected policy active.
- **Add Policy**: Create a new policy.
- **Apply Label to Policy**: Associate a policy and a label.
- **Deactivate Policy**: Clear flag to make the selected policy inactive.
- **Delete Policy**: Delete a policy.
- **Export Policy**: Export a policy from MobileIron Core.
- **Import Policy**: Import a policy into MobileIron Core.
- **Modify Policy**: Change an attribute of an existing policy.
- **Modify Policy Priorities**:
- **Modify Policy Priority**: Change the priority for an existing policy.
- **Remove Label From Policy**: End the association between a policy and a label.

Compliance Action events

To monitor compliance actions, select one or more of the logged compliance actions in the **Filters** panel

- **Add Compliance Action**: Create a set of actions to be taken on devices that violate policies.
- **Delete Compliance Action**: Remove a set of actions to be taken on devices that violate policies.
- **Modify Compliance Action**: Make changes to a set of actions to be taken on devices that violate policies.
- **Modify Compliance Check Preferences**: Make changes to compliance preferences.

Configuration events

- **Add Configuration**: Create a new configuration.
- **Apply Label To Configuration**: Associate a configuration with a label.
- **Export Configuration**: Export a configuration from MobileIron Core.
- **Import Configuration**: Import a configuration to MobileIron Core.
- **Modify Configuration**: Change the settings in a configuration.
- **Remove Configuration**: Delete a configuration.

- **Remove Label From Configuration**: End the association between a configuration and a label.
- **Remove Labels From Configuration**: End the association between a configuration and multiple labels.

Admin events

- **Add Space**: Define a new delegated administration space.
- **Admin Portal Sign In**: Start an Admin Portal session.
- **Admin Portal Sign Out**: End an Admin Portal session.
- **Assign Space Admin**: Specify an administrator for a space.
- **Change Space Priority**: Set a different priority for a space.
- **Delete Space Admin**: Remove space admin access from the user.
- **Modify Space**: Make changes to rules that define a space.
- **Remove Admin From Space**: Remove the admin user from the space.
- **Remove Space**: Delete all rules that define a space and reallocate its devices.
- **Update Device Space**: Recalculate space rules to determine device membership.
- **User Locked Out**: Prevent administrator from further attempts at signing in after limit on authentication failures is exceeded.

User events

- **Add User**: Define a new MobileIron Core user.
- **Delete User**: Remove a MobileIron Core user.
- **Link to LDAP User**: Associate a local MobileIron Core user with an LDAP user.
- **Modify User**: Make changes to a user's attributes.
- **Modify User Role**: Make changes to the roles assigned to a user.
- **Re-sync with LDAP**: Synchronize LDAP data.
- **Remove User Attribute**: Remove an attribute from a user.
- **Renew Google Apps password**: Manually regenerate a user's Google Apps password.
- **Require Password Change**: Force a local user to change their MobileIron Core password.
- **Send Invitation**: Invite a user to register with MobileIron Core.
- **Set User Attribute**: Set an attribute for a user.
- **User Portal Sign In**: Start User Portal session.
- **User Portal Sign Out**: End User Portal session.

LDAP events

- **Add LDAP**: Integrate an LDAP server with MobileIron Core.
- **Delete Admin LDAP Entity**: Delete an Admin LDAP entity that has no roles.

- **Delete LDAP**: End the integration between an LDAP server and MobileIron Core.
- **Delete LDAP Entity**: Delete a user LDAP entity that has no roles.
- **Modify LDAP**: Make changes to the record for an integrated LDAP server.
- **Modify LDAP Preferences**: Make changes to the preferences for integrated LDAP servers.
- **Upload LDAP Certificate**: Add an LDAP certificate to MobileIron Core.

Other events

- **Application Started**: Start Core services.
- **Application Stopped**: Stop Core services.
- **Complete feature usage collection**: Complete the current run of feature usage collection.
- **Feature usage collection error**: Encountered error during collection.
- **Feature usage collection scheduling error**: Encountered scheduling error during collection.
- **Initiate feature usage collection**: Start feature usage collection.
- **Purge feature usage data**: Purge collected feature usage information.
- **Preference Config Changes**: Make changes to the settings under **Settings > System Settings** in the Admin Portal.
- **Retrieve feature usage data**: Start collecting feature usage data.
- **Retrieve feature usage data file list**: Start retrieval of the usage data file list.

Label events

- **Add Label**: Define a new label for MobileIron Core.
- **Delete Label**: Remove a label from MobileIron Core.
- **Modify Label**: Make changes to a label.
- **Save As Label**: Copy a label to a new label.

Sentry events

- **Add Integrated Sentry**: Establish a relationship between MobileIron Core and an Integrated Sentry.
- **Add Standalone Sentry**: Establish a relationship between MobileIron Core and a Standalone Sentry.
- **Delete Integrated Sentry**: End the relationship between MobileIron Core and an Integrated Sentry.
- **Delete Standalone Sentry**: End the relationship between MobileIron Core and a Standalone Sentry.
- **Disable Integrated Sentry**: Suspend the interaction between MobileIron Core and an Integrated Sentry.
- **Disable Standalone Sentry**: Suspend the interaction between MobileIron Core and a Standalone Sentry.
- **Edit Integrated Sentry**: Make changes to the settings for an Integrated Sentry.
- **Edit Standalone Sentry**: Make changes to the settings for a Standalone Sentry.
- **Enable Integrated Sentry**: Start the interaction between MobileIron Core and an Integrated Sentry.

- **Enable Standalone Sentry**: Start the interaction between MobileIron Core and a Standalone Sentry.
- **Manage Certificate**: Upload a certificate for Standalone Sentry.
- **Modify Sentry Preferences**: Make changes to the settings under **Services > Sentry**.
- **Regenerate Key**: Generate a new control key for attachment encryption.
- **Regenerate Attachment Encryption Control Key**:
- **Resync Integrated Sentry With Exchange**: Force Integrated Sentry to synchronize mailbox data with the Exchange server.

Android enterprise events

These events are only for Android devices.

- **Accept permissions for Android enterprise App**: Accept permissions on behalf of all users.
- **Apps@work setting modified**:
- **Connect Core to Android enterprise**: Establish binding between MobileIron Core and Android enterprise.
- **Disconnect Core from Android enterprise**: Remove binding between MobileIron Core and Android enterprise.
- **Save Restrictions for Android enterpise App**: Apply new or changed Android enterprise restrictions.
- **Sync Google Users with Cores**: Synchronize user data between Google and MobileIron Core.
- **Update catalog setting modified:**

Custom attributes events

- **Add Custom Attribute**: Create a new customer attribute definition.
- **Modify Custom Attribute**: Modify a customer attribute definition.

Compliance policy events

- **Add Compliance Policy Group**: Add a new compliance policy group.
- **Add Compliance Policy Rule**: Add a new compliance policy rule.
- **Apply Label to Compliance Policy Group**: Apply one or more labels to a compliance policy group.
- **Modify Compliance Policy Group**: Modify a compliance policy group.
- **Modify Compliance Policy Rule**: Modify a compliance policy rule.
- **Remove Compliance Policy Group**: Delete a compliance policy group.
- **Remove Compliance Policy Rule**: Delete a compliance policy rule.
- **Remove Label From Compliance Policy Group**: Delete one or more labels from a compliance policy group.

Audit Logs use cases

A wealth of information is available to you in the Audit Logs. Querying the events allows you to monitor your MobileIron system and resolve problems. You can run queries for one type of event, several types of events, or as many as you like. All you need to do is check the events you want to track, and then specify a time frame. The default time frame is the time between the last time the logs were purged and the current time.

For example:

- Use the certificate events to troubleshoot certificate issues. For example, query for certificates that have expired or have been revoked.
- Use the MDM events to troubleshoot MDM activity on devices. For example, query whether an MDM profile was removed, or whether a managed app was installed.
- Use the AppTunnel events to determine whether an administrator manually blocked or allowed AppTunnel on a device.
- Use the device events to determine activity taken on devices, such as unlocking the device, or deleting retired devices.
- Use the app events to determine whether an administrator has changed the app control rules in MobileIron Core. A change to app control rules can result in Core taking, or not taking, compliance actions such as blocking email on devices.

This section presents several scenarios and how you can use the audit logs to resolve the problems they present.

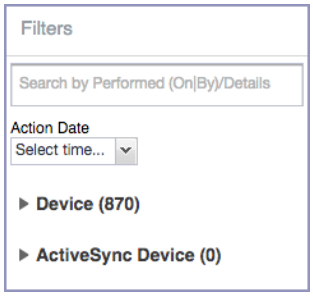
Personal information is wiped from devices

Suppose several of your users report that the personal information on their phones was wiped. How can you figure out how this happened? Using the audit logs, you can check the wipe actions recorded in the logs, and discover:

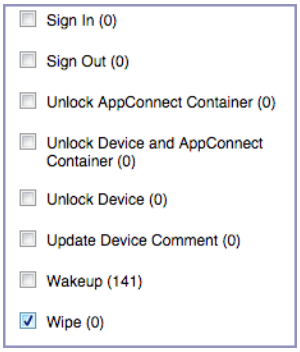
- who issued the Wipe commands
- when they occurred
- how many users are impacted

To resolve this problem:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect the device wipe(s) happened.
5. Open the **Device** events list.



6. Select **Wipe**.



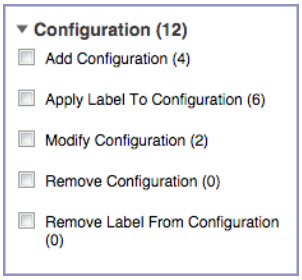
7. Click **Search**.
8. View the results of the search to determine:
   - when the devices were wiped
   - how many devices were wiped
   - which admin user issued the wipe commands

Users are prompted for email passwords when not necessary

Suppose you set up your Exchange policy to not require your users to provide a password when they log in to email, but your users are still prompted for a password each time they access email.

To check for any changes to the Exchange policy that could cause this problem:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect changes to the Exchange policy happened.
5. Open the **Configuration** events list.



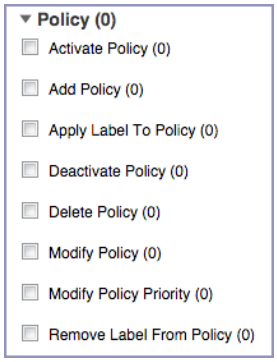
6. Select **Modify Configuration**.
7. Click **Search**.
8. View the results of the search to determine:
   - what changes were made recently to the Exchange policy
   - which admin user made the changes

Users are prompted to create passwords

Suppose your users are prompted to create device passwords when that is not how you set up your MobileIron Core. You can use the audit logs to discover if this requirement is set and when this change occurred.

To check for changes to mandatory passwords:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect changes to the security policy happened.
5. Open the **Policy** events list.



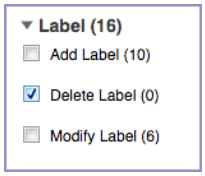
6. Select **Modify Policy**.
7. Click **Search**.
8. View the results of the search to determine:
   - what changes, if any, were made recently to the Security policy
   - which admin user made the changes

Devices have lost their managed apps

If your users report missing managed apps, the cause is usually deleted labels.

To determine whether labels were deleted from your MobileIron Core:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect the labels were deleted.
5. Open the **Label** events list.



6. Select **Delete Label**.
7. Click **Search**.
8. View the results of the search to determine:
   - what labels, if any, were deleted recently
   - which admin user made the changes

MDM Activity

The **Logs > MDM Activity** displays MDM-specific log entries.

NOTE: Many of these entries are also available in **Logs > Audit Logs** in the **MDM** category.

Filter the log entries using the following criteria:

- Platform
- Date range
- States
- Actions
- User
- Device
- Error text
- Detail text
- Date range

Viewing Errors

Errors result in the display of a **View Error** link in the **Error** column. Error details are not available for Android devices.

Certificate Management

The **Logs > Certificate Management** tab displays certificate-related log entries. You can:

- view certificate log entries
- search certificate log entries
- remove selected certificates from the log
- revoke selected certificates from the log
- re-enroll selected certificates from the log

NOTE: Actions on certificates are logged in **Logs > Audit Logs**in the **Certificate** category**.**

How to search for certificate entries

When viewing the **Certificate Management** page, you can search for entries based on:

- expiration date
- user
- setting

Procedure

To search the **Certificate Management** page:

1. In the Admin Portal, go to **Logs > Certificate Management**.
2. Specify one or more of the criteria in the following steps to describe the certificates you want to display.
3. (Optional) To specify a time range within which the certificates expired:
   - In the **Expiration Date Range** field, click the calendar next to the field, and then click on a date. This date is the earliest day the certificates you are searching for expired.
   - In the **To** field click the calendar next to the field, and then click on a date. This date is the latest day the certificates you are searching for expired.

     NOTE: An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:
   - An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:

- select November 13th in the Expired Date Range field (earliest time a certificate expired).
- select October 15th in the To field (latest time a certificate expired).

NOTE: The search can return fewer than all the certificates that expired during the specified time period if you specify other criteria in Step 4.

4. (Optional) In **Search by User/Setting Name**, enter a username or a setting name.

Certificate Enrollment	Displays the name of the Certificate Enrollment setting.
Setting	Displays the configuration using the Certificate Enrollment. The configuration displays only for a non-cached Certificate Enrollment. Configuration names are not available for certificates created in VSP Version 6.0 or earlier. For a cached Certificate Enrollment certificate, you will always see - in the Setting Name, regardless of whether it was created prior to version 7.0 or created in version 7.0. **For Android devices**, the **Setting Name** displays only for APPCONFIG, APPPOLICY, and WEB@WORK settings; otherwise a -displays.

5. Click **Search**.

Search results are displayed in a table with the following columns:

Item	Description
User	The user name of the device user identified by the identity certificate.
Phone Number	The phone number associated with the device user identified by the identity certificate.
Email	The email address associated with the device user identified by the identity certificate.
Certificate Enrollment Name	The name of the certificate enrollment (such as SCEP, Local, Entrust) used to issue the identity certificate.
Setting Name	The name of the setting that uses the certificate enrollment, such as an Exchange or Web@Work setting.
Cert Type	Indicates whether the certificate is a user-provided certificate enrollment. Otherwise, this field is left blank.
Expiration Date	The date by which the identity certificate will no longer be valid.
Content	Click the **View** link to see the contents of the identity certificate itself.

How to remove a certificate

This action removes the certificate from device, but does not remove the SCEP setting.

To remove a certificate:

1. Go to **Logs > Certificate Management**.
2. Select the certificate that you want to remove.
3. Click **Actions > Remove**.

How to revoke a certificate

You can revoke certificates created using a Local Certificate Authority, OpenTrust, Entrust API Version 9, and Symantec Web Service PKI. Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). When a device authenticates with MobileIron Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Go to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

The certificate will be added immediately to the CRL so the next time the device attempts to authenticate, authentication will fail.

How to re-enroll a SCEP certificate

This feature is not supported on Android devices.

Service Diagnostic tests

The Service Diagnostic screen (**Services > Overview)** in the Admin Portal provides a health check for several services. The diagnostic tests determine whether your Core instance can connect to these services. An error indicates that you cannot reach the service.

The services checked are:

TABLE 64. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS

Service	Test
AFW	Checks to see if: • Authentication server https://accounts.google.com/o/oauth2/token is reachable. • API server https://www.googleapis.com/androidenterprise/v1/enterprises is reachable.
APNS	Checks to see if: • MDM-APNS service is reachable. • ENTERPRISE-APNS - No Enterprise APNS certificate configured. • MDM-APNS - feedback service (tccentos122.auto.mobileiron.com:2196) is not reachable.
APPCONFIG_ COMMUNITY_ REPO	Checks to see if the AppConfig Community Repository server is reachable: https://d2e3kgnhdeg083.cloudfront.net/com.example.OneTouchConfiguration/current/appconfig.xml
APP_GATEWAY	Checks to see if App Gateway server is reachable: https://gwtest.mobileiron.com/gateway/gatewayServices/status.html
BYPASS	Checks the connection between your Core instance and the Apple activation lock bypass server
CERTIFICATE ENROLLMENT	Checks to see if: • Certificate Enrollment : System - iOS Enrollment SCEP is reachable. • Certificate Enrollment : System - iOS Enterprise AppStore SCEP is reachable. • Certificate Enrollment : System - Windows Phone Enrollment SCEP is reachable.
CONFIGURATIO NS	Tests the connection to the Certificate Enrollment server from your Core instance.
CONNECTOR	Two tests are run: • One test checks whether Enterprise Connector is enabled (**Services > Connector**) • If Enterprise Connector is enabled, the other test sends an HTTP Post request from your Core instance to each Connector configured, checking whether the Connector can communicate with your Core instance
DEP	Sends a sample GET request to test the connection between your Core instance and the MDM server using Device Enrollment.
FCM	Checks whether Google Firebase Cloud Messaging (FCM) is reachable from your Core instance.
HEALTH_ ATTESTATION_ SERVICE	Checks if the Health Attestation Service serveris reachable. https://has.spserv.microsoft.com/HealthAttestation/ValidateHealthCertificate/v1
LDAP	Two tests are run: • Checks LDAP from Core to verify the communication channel

TABLE 64. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
	• For each Connector configured, checks the communication channel for the path from the LDAP server to Core, then Core to Connector, and finally from Connector to the LDAP server
MAPQUEST	Checks if the MapQuest Service server is reachable: https://api.mqcdn.com/sdk/mapquest-js/v1.0.0/mapquest.js
PROXY	No proxy is configured.
SENTRY	Checks the connection between your Core instance and the Sentry used (either integrated standalone). As part of this test, the connection between ActiveSync server and Sentry is checked also.
SENTRY_WITH_ ACTIVESYNC	No Integrated Sentry server(s) configured. No Standalone Sentry server(s) configured.
SERVICES	Checks whether the IP addresses reserved for FCM are reachable.
VPP	Sends a GET request to verify the connection between Core and the Apple License server.

Running Service Diagnostic tests

To run the Service Diagnostic tests:

1. Go to **Services > Overview**.
2. To test one or all of the services:
   - Click **Verify All** to test the listed services
   - Click **Verify** next to a specific service to test that service

Device log encryption on Android devices

Log files can be emailed by using the **Send Log** option in Mobile@Work for Android. You can choose whether the log files are encrypted when they are provided to the email app. The choice affects the log files of the following:

- Mobile@Work for Android
- Secure Apps Manager
- AppConnect-enabled apps (including what the app logs and what the AppConnect wrapper around the app logs)

The security policy for a device contains the option for choosing whether the emailed log files are encrypted. The default setting is to **not** encrypt the files.

By default, encrypted log files can be decrypted only by MobileIron Technical Support. If you want to encrypt the log files using your own certificate, see Encrypting device logs with your own certificate.

NOTE: Regardless of the device log encryption setting, the log files never include passwords, certificate content, license information, or other sensitive authentication data.

By encrypting the emailed log files, you improve security because the data is readable only by MobileIron Technical Support when using the default encryption, or by your own enterprise when using your certificate for encryption. Since emailing logs for troubleshooting is a common practice, you typically choose to encrypt the logs.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the security policy for the appropriate devices.
3. Click **Edit**.
4. In the **Data Encryption** section. for **Device Log Encryption**, select **On**.
5. Click **Save**.

Encrypting device logs with your own certificate

You can define a log encryption configuration that enables device users to send encrypted logs to an administrator's email address from their devices. The configuration includes a certificate for encrypting logs and an email address to which encrypted logs are to be sent. Devices sync with MobileIron Core and receive the configuration after you assign the configuration to the relevant labels.

This feature requires:

- Mobile@Work 10.0.0.0 for Android through the most recently released version as supported by MobileIron
- Secure Apps Manager 8.3.0.0 through the most recently released version as supported by MobileIron
- On the security policy, device log encryption must be on.

Related topics

Device log encryption on Android devices

Before you begin

Upload a certificate to Core, as described in Certificates settings.

Procedure

1. In the Admin Portal, select **Policies & Configs**> **Configurations**.
2. Click **Add New** and select **LogEncryption**. The New Log Encryption Setting dialog box opens.

3. Fill in the following:

Field	Description
Name	Enter a name for the configuration.
Email Address	Enter an email address to which encrypted logs may be sent. The **To:** field of the email is automatically filled with this address. If you do not enter an email address here, the device user fills in the **To:** field.
Certificate	From the drop-down list, select a certificate you have already uploaded to Core.

4. Click **Save**.
5. On the Configurations page, select the configuration you just defined.
6. Click **Actions** > **Apply to Label**, and select the label to which you want to apply the log encryption configuration.

Pull client logs for client devices

To troubleshoot challenging technical support issues when working with MobileIron Technical Support, you can pull client logs of an Android or iOS client device without requiring any interaction from the end user. From the Admin portal, use the Pull client log command to obtain client logs. The Pull client log action as well as the success or failure of the event is captured in the Audit logs. This feature does not work on Windows and chromeOS devices.

NOTE: The Pull client log command is not available to delegated admin roles; only administrators who have the Manage Devices role can use this feature.

When the Pull client logs command is delivered to the device, it instructs the Mobile@Work client to collect logs running on the device. This may include logs from all the secure apps running on the device. These logs are pulled to the server's file storage.

Potentially, there is one interaction that may cause a message to be displayed to a device user. If the device has an AppConnect configuration and a number of secure apps installed, then the Mobile@Work client may momentarily go to the foreground of the device display and request secure apps logs from the Secure AppManager application. Under these conditions, a message is displayed on the device that states a device administrator is pulling Mobile@Work client logs and logs from the secure applications for analysis. Also, the message states that this is a short interruption.

When you have an AppConnect configuration that is running and SecureApps Manager and the SecureApps Manager does not communicate with Mobile@Work in a timely fashion, then the end user may be prompted to log in again.

NOTE: You can retrieve the client logs from the System Manager. Select **Troubleshooting** > **Logs** in the Export Logs section. Select **Show Tech (All Logs)**. For more information see "Exporting logs" in the *MobileIron Core System Manager Guide*.

Before you pull a client log, you may want to set log encryption and then upload this configuration on the device. When you enable log encryption, the client will encrypt logs when the Pull client log action is taken. By default, log encryption is set to off. To set log encryption, you can use the default log encryption certification or custom certification. See Device log encryption on Android devices for instructions on how to set device log encryption for Android devices.

To access the Pull client log command:

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a device. You may only select one device.
3. Click the **Actions** button.
4. Select **Pull Client Logs**. The Pull Client Logs dialog box displays. The **Devices** field displays the name of the device that you selected. You cannot add additional devices here.
5. (Optional) Add any notes about this action in the **Notes** section.
6. Click the **Pull Client Logs** button to launch this request to the server.

Office 365

This section contains the overview, policies, configurations, user groups, reports and settings as pertains to Office 365:

- Office 365 App Protection overview
- Office 365 App Protection policies
- Office 365 App Protection configurations
- Office 365 App Protection user groups
- Office 365 App Protection reports
- Office 365 App Protection settings

Office 365 App Protection overview

Office 365 App Protection provides important Data Loss Prevention (DLP) for Office 365 apps, such as Microsoft Word, Excel, PowerPoint, and so on. It allows administrators to manage policies and configurations that secure data in Office 365 apps on Android devices.

NOTE: Some Graph APIs can be in beta. Use this feature accordingly.

You can manage Office 365 apps by:

- Enforcing PIN for Office 365 apps
- Disabling contacts to sync from Office 365 apps
- Preventing users from printing from Office 365 apps
- Preventing outbound data sharing from Office 365 apps

Prerequisites for using Office 365 App Protection

Before you can use Office 365 App Protection, you must have:

- A valid MobileIron license.
- A valid Intune subscription or a Microsoft EMS subscription that includes Intune.
- A valid Office Enterprise or Business subscription with access to Office 365 apps on a mobile device.
- One or more Office 365 apps.
- Synced your Active Directory users to your Azure Active Directory.
- One Drive for Business installed on devices to protect data on Word, Excel, and PowerPoint.

- Intune Company Portal app installed on Android devices.
- Device users are not required to sign in, but this app must be installed on the device to protect data on device.

Office 365 App Protection window

NOTE: Before you register MobileIron as an Azure app, only the **Services > Microsoft Graph > Settings** tab is enabled. Once you register MobileIron as an Azure app, all the tabs are enabled.

Access the Office 365 App Protection window by logging into the Admin Portal and going to Services > Microsoft Graph. This window includes the following options:

- **Policies**: Use this tab to add and manage Office 365 DLP policies. You can perform the following actions on each policy:
  - Assign one or more User groups to the policy.
  - Assign apps to the policy.
  - Delete the policy.

  See Adding Office 365 App Protection policies for details on how to add a Office 365 App Protection policy.

- **Configurations**: Use this tab to add and manage Office 365 DLP configurations. You can perform the following actions on each policy:
  - Assign one or more User groups to the configuration.
  - Assign apps to the configuration.
  - Delete the configuration.

  See Office 365 App Protection configurations for details on how to add a Office 365 App Protection configuration.

- **User Groups**: Use this tab to search for and view user groups available to add to a policy or configuration.
- **Reports**: Use this tab to view and download user and app reports and manage wipe requests. These reports are populated with data that comes from Azure Active Directory during real-time syncs.
- **Settings**: Use this tab to register MobileIron as an Office 365 app. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

Office 365 App Protection policies

Once you register MobileIron as an Azure app you can add and manage Office 365 App Protection policies in the Microsoft Azure cloud for Office 365 apps.

This section includes the following topics:

- Adding Office 365 App Protection policies
- Editing Office 365 App Protection policies

- Managing Office 365 App Protection policies
- Add Office 365 App Protection policies window

NOTE: Before using this feature, complete the prerequisites described in the following section: *Prerequisites for using Office 365 App Protection*.

Related topics

- Office 365 App Protection overview
- Office 365 App Protection configurations
- Office 365 App Protection user groups
- Office 365 App Protection reports
- Office 365 App Protection settings

Adding Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Policies > Add**.
3. Complete the **App protection policies** form.
   Refer to Add Office 365 App Protection policies window for details.
4. In the Compliance Actions section, select a Setting, enter the value, and select an Action. Refer to the App protection policies fields table.
5. Click **+Add** to configure additional compliance actions.
6. Click **Save** to add the policy to the list of DLP policies on the **Policies** table.

Editing Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Policies**.
3. Click the name of a policy you want to edit.
4. Complete the **App protection policies** form.
   Refer to Add Office 365 App Protection policies window for details.
5. In the Compliance Actions section, select a Setting, enter the value, and select an Action. Refer to the App protection policies fields table.

6. Click **+Add** to configure additional compliance actions.
7. Click **Save** to save the policy edits.

Managing Office 365 App Protection policies

You can take any of the following actions on each Office 365 App Protection policy:

- Assign User Groups
- Assign Apps
- Delete Policies

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Policies**.
3. Locate a policy you want to manage and go to the **Actions** column.
4. Assign user groups to the App Protection policy.
   a. Click the **Assign User Groups** icon.
   b. Search for user groups.
   c. Select one or more user groups to add to the policy.
   d. Click **Save**.
5. Assign Office 365 apps to the app protection policy.
   a. Click the **Assign Apps** icon.
   b. Search for apps.
   c. Select one or more apps to add to the policy.
   d. Click **Save**.
6. Delete an Office 365 App Protection policy.
   a. Click the **Delete Policy** icon.
   b. Click **Yes** to confirm deletion of the policy.

The Office 365 App Protection policies take affect:

- After assigning the policy to a user group.
- A user from the assigned user group logs into an Office 365 app using AAD credentials.

Add Office 365 App Protection policies window

Access this window by logging into the Admin Portal and selecting **Services > Microsoft Graph > Policy** and clicking **Add** or clicking a policy to edit.

The following table summarizes fields and descriptions in the **Add App Policies** window. Also, refer to the App protection policies fields table.

TABLE 65. APP PROTECTION POLICIES FIELDS

Fields	Description
Name	This required field is the name used to track the Office 365 App Protection policy in Core.
Description	Describes the profile's purpose (optional).
Platform	Select the platform for the Office 365 apps. The options are: **iOS** or **Android**. Some of the other options on this form will change depending on which platform you select. Refer to the relevant platform's Device Management Guide.
Data Relocation	
Prevent Android backups	Choose **Yes** to prevent this app from backing up data to the Android Backup Service Choose **No** to allow this app to back up data. (The default is **Yes**.)
Allow app to transfer data to other apps	Use this option to specify what apps can receive data from this app. The options are listed below. • **Policy managed apps**: Allow transfer only to other policy-managed apps. • **All apps**: Allow transfer to any app (default.) • **None**: Do not allow data transfer to any app, including other policy-managed apps. When any of the above options except *All apps* are selected, the exempted apps are listed to the right of the *Allow app to receive data from other apps* field. Modifying these settings changes how data is transferred to other applications.
Allow app to receive data from other apps	Select an option to specify what apps can transfer data to this app. • **Policy managed apps** - Allow app to receive data from only other policy-managed apps. • **All apps** Allow app to receive data from other apps (default.) • **None** - Do not allow app to receive data from any app, including other policy-managed apps.
Prevent "Save As "	Select to disable the use of the Save As (a new document) option in any app that uses this policy. De-select if you want to allow the use of Save As. (Default is unchecked.) Selecting Prevent Save As activates the **Select which storage services corporate data can be saved to field**. The options are:

TABLE 65. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
	• OneDrive for Business • SharePoint • Local Storage
Restrict cut, copy and paste with other apps	Specifies when cut, copy, and paste actions can be used with this app. The options are listed below. • **Blocked**: Do not allow cut, copy, and paste actions between this app and any other app. • **Policy managed apps**: Allow cut, copy, and paste actions between this app and other policy-managed apps. • **Policy managed with paste in**: Allow cut or copy between this app and other policy-managed apps. Allow data from any app to be pasted into this app. • **Any app**: No restrictions for cut, copy, and paste to and from this app. (This is the default.)
Block screen capture and Android assistant	Check this to block the ability to use screen captures and block Android assistant. Default is allowed.
Encrypt app data	Select to encrypt app data that is associated with an Intune mobile application management policy. Encryption is provided by Microsoft. Data is encrypted synchronously during file I/O operations according to the setting in the mobile application management policy. Managed apps on Android use AES-128 encryption in CBC mode utilizing the platform cryptography libraries. The encryption method is not FIPS 140-2 certified. SHA-256 encryption is supported as an explicit instruction using the SigAlg parameter and will only work on devices 4.2 and above. Content on the device storage is always encrypted.
Disable app encryption when device encryption is enabled	This field activates when the *Encrypt app data* field is selected. Disables app encryption when the device encryption is enabled . Default is de-selected.
Disable contact sync	When this setting is enabled, users cannot sync contacts to the native address book. Default is un-checked.
Disable printing	Select this to block printing protected data from the app. Default is un-checked.
Restrict web content to display in the Managed Browser	Check this to enforce web links in the app to be opened in the Managed Browser app. Uncheck this to open web links in Chrome. Default is de-selected.

TABLE 65. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
Block third party keyboards	When this setting is enabled, a third-party keyboard cannot be used with protected apps.
Access	
Require PIN for access	Select this to require users to enter a PIN to access this app. The user is prompted to set up this PIN the first time the app is run. Default is selected, which activates all the fields in the Access section of this page.
Allow simple PIN	**Allow simple PIN**: Check this to allow users to use simple PIN sequences like 1234 or 1111. Choose No to prevent them from using simple sequences. (The default value is checked.) • **PIN length**: Specify the minimum number of digits in a PIN sequence. (The default value is **4**.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Allow fingerprint of PIN (Android 6.0+)	Select this to allow the user to use Touch ID instead of a PIN for app access. (The default is checked.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Override fingerprint with PIN after timeout (minutes)	If required, depending on the timeout (minutes of inactivity), a PIN prompt will override Touch ID prompts. If this timeout value is not met, the Touch ID prompt will continue to show. This timeout value specified under "Recheck the access requirements after (minutes of Activity)". On iOS, this feature requires the app to have Intune SDK version 8.1.1 or above. **Inactivity timeout**: Specify a time in minutes after which the PIN will override the use of a fingerprint. When the *Require PIN for access* field is de-selected, this field is deactivated.

TABLE 65. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
Disable app PIN when device PIN is managed	Select to disable the app PIN when a device lock is detected on an enrolled device. If you select this option, it overrides the requirements for PIN or Touch ID. (The default is unchecked.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Require corporate credentials for access	Select to require corporate credentials instead of a PIN for app access. Not selecting this option overrides the requirements for PIN or Touch ID. The user will be prompted to provide their corporate credentials. (The default is unchecked.)
Recheck the access requirements after (minutes)	Timeout for access requirements is measured in terms of the time of inactivity between any policy-managed application. • **Timeout**: Enter the number of minutes before the access requirements (defined earlier in the policy) are rechecked. For example, an administrator turns on PIN in the policy, which means a when device user opens a app, a PIN must be entered. When using the Recheck the access requirements setting, the device user would not have to re-enter the PIN on any app for another 30 minutes. (The default is 30.)

Compliance Actions

Use the Compliance Actions Settings to set the security requirements for your access protection policy. Several settings are provided with pre-configured values and actions.

Procedure

1. Select a Setting, enter the value, and select an Action. Refer to the table below.
2. Click **+Add** to configure additional compliance actions.
3. At the top of the Policies tab, click **Save**.

TABLE 66. COMPLIANCE ACTION SETTINGS

Setting	Description
Max PIN attempts (default)	Specify the number of tries the device user has to successfully enter the correct PIN before the configured action is taken. (Default value is 30 minutes.) Actions include: • **Reset PIN** - The user must reset their PIN. • **Wipe data** - The user account that is associated with the application is wiped from the device.
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in minutes) before the access requirements for the app are rechecked. After this period is expired, the app will **Block Access**. The default is 720 minutes (12 hours.)
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in days) before the access requirements for the app are rechecked. After this period is expired, the app will **Wipe data**. The default is 90 days.
Jailbroken/rooted device	• **Block access** - Prevent this app from running on jailbroken or rooted devices. The device user continues to be able to use this app for personal tasks, but will have to use a different device to access data in this app. • **Wipe data** - The device user account that is associated with the application is wiped from the device
Min OS version	Select this to require a minimum operating system to use this app. Enter the value in the following format [major].[minor] and select one of the following actions: • **Block access** - The device user will be blocked from access if the version on the device does not meet the requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the operating system version on the device does not meet the requirement. This notification can be dismissed.
Min App version	Check this option to require a minimum app version to use the app. The user will be blocked from access if the app version on the device does not meet the requirement. • **Block access** - The device user will be blocked from access if the app version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device.

TABLE 66. COMPLIANCE ACTION SETTINGS (CONT.)

Setting	Description
	• **Warn** - The user will see a notification if the app version on the device does not meet the requirement. This notification can be dismissed.
Min Patch version	Select to require devices have a minimum Android security patch released by Google. Click the calendar icon to select the date for the action below to occur: • **Block access** - The device user will be blocked from access if the Android version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the Android version on the device does not meet the requirement. This notification can be dismissed.
Device manufacturer(s)	Specify a device manufacturer that is required to use this app. Actions include: • **Block access** - Only devices that match the specified manufacturer can use the app. All other devices are blocked. • **Wipe data** - The user account that is associated with the application is wiped from the device.

Office 365 App Protection configurations

Once you register MobileIron as an Azure app you can create custom configurations for Office 365 apps. App Configurations can be used to specify custom app configurations for Office 365 apps. Configurations can include setting a local encryption scheme for OneDrive, setting Skype parameters, and so on.

This section includes the following topics:

- Creating Office 365 App Protection configurations
- Editing a Office 365 App Protection configuration
- Managing Office 365 App Protection configurations

NOTE: Before using this feature, complete the prerequisites described in the following section: *Prerequisites for using Office 365 App Protection*.

Related topics

- Office 365 App Protection overview
- Office 365 App Protection policies
- Office 365 App Protection user groups
- Office 365 App Protection reports
- Office 365 App Protection settings

Creating Office 365 App Protection configurations

Configurations use data populated from Azure Active Directory during real-time syncs.

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Configurations > Add**.
3. Add a name (required) and description (optional).
4. Click **Add+** to add one or more key-value pairs.
   The values are strings with no limitations or restrictions.
5. Click **Save** to add the configuration to the list in the configurations table.

Editing a Office 365 App Protection configuration

Configurations use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Configurations**.
3. Click the name of a configuration you want to edit.
   Use the search field to search by name.
4. Make any necessary changes.
5. Click **Save** to update the configuration edits.

Managing Office 365 App Protection configurations

You can take any of the following actions on each Office 365 App Protection configuration:

- Assign User Groups
- Assign Apps
- Delete Policies

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Microsoft Graph > Configurations**.
3. Locate a configuration you want to manage and go to the **Actions** column.
   a. Assign user groups to the app protection configuration.
   b. Click the **Assign User Groups** icon.
   c. Search for user groups.
   d. Select one or more user groups to add to the configuration.
   e. Click **Save**.
4. Assign Office 365 apps to the app protection configuration.
   a. Click the **Assign Apps** icon.
   b. Search for apps.
   c. Select one or more apps to add to the configuration.
   d. Click **Save**.
5. Delete an Office 365 App Protection configuration.
   a. Click the **Delete Configuration** icon.
   b. Click **Yes** to confirm deletion of the configuration.

Changes to the configurations take affect after:

- assigning the configuration to a user group.
- a user from the assigned user group logs into an Office 365 app using AAD credentials.

Office 365 App Protection user groups

Use the **User Groups** tab to search for and view user groups available to add to one or more Office 365 App Protection policies or configurations. Access a list of user groups by logging into the Admin Portal and selecting **Services > Microsoft Graph > User Groups**.

NOTE: Before using this feature, complete the prerequisites described in the following section: *Prerequisites for using Office 365 App Protection*.

Related topics

- Office 365 App Protection overview
- Office 365 App Protection policies
- Office 365 App Protection configurations

Office 365 App Protection reports

Reports for out of compliance data, devices, apps, and users, is populated from Azure Active Directory during real-time syncs. Access the reports by logging into the Admin Portal and selecting **Services > Microsoft Graph > Reports**. Use the **Reports** tab to:

- search, view, or download a .csv report by user
- search, view, or download a .csv report by app
- create and manage wipe requests
- refresh reports

This section includes the following topics:

NOTE: Before using this feature, complete the prerequisites described in the following section: *Prerequisites for using Office 365 App Protection*.

Related topics

- Office 365 App Protection overview
- Office 365 App Protection policies
- Office 365 App Protection configurations
- Office 365 App Protection user groups
- Office 365 App Protection settings

Office 365 App Protection reports window

Manage reports from the Admin Portal by going to **Services > Microsoft Graph** to open the Office 365 App Protection window. This window includes several options, which are listed in the left pane. When you select one, the right pane changes to include details of the selected option.

- **Out of Compliance Users**: This option is selected by default. Use it to manage reports on users who are out of compliance.

- **Selective Wipe**: Use this option to request Azure Active Directory wipe Office 365 app data from selected devices.
- **App Protection Reports**: Use this tab to view and download app protection reports by users and by apps. These reports are populated with data from Azure Active Directory during real-time syncs.
- **App Configuration Reports**: Use this tab to view and download app configuration reports by users and by apps. These reports are populated with data from Azure Active Directory during real-time syncs.

Managing Out of Compliance Users reports

Use this option to manage reports on users who are out of compliance.

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports > Out of Compliance Users**.
3. Click **Download Report** to download a .csv report from Azure Active Directory of users who are out of compliance.
4. Click **Refresh Report** to get the most recent data from Azure Active Directory after the latest sync.
5. Select one or more of the users listed in the report or select all.
6. Click **Wipe Apps Data** to send a wipe request to Azure Active Directory for users.

Managing Selective Wipe reports

Use this option to create and manage requests you send to Azure Active Directory to wipe Office 365 app data from selected devices.

Creating wipe requests

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Expand **Selective Wipe**.
4. Click **Create Wipe Request**.
5. Enter or search for a user name, then select one or more of the user's devices.
6. Click **Create Wipe Request** to request Azure Active Directory wipe Office 365 app data from one or more selected devices.

Managing wipe requests

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Expand **Selective Wipe**.
4. Click **Wipe Request**.
5. Select one or more pending wipe requests and click **Cancel Wipe Request**.
6. Click **Refresh** to update the status of the pending wipe requests.

Downloading App Protection reports

App Protection Reports show applications protected by the policies that are created and assigned to them from the **Policies** tab. Use this option to download app protection .csv reports by users or apps.

Downloading App Protection reports by user

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Expand **App Protection Reports**.
4. Click **User**.
5. Search for, or enter a user name.
   See App Protection User reports table for details.
6. Click **Download Report**.

App Protection User reports table

Select this option to view and download reports and to refresh the report data. This option provides app information for a specified user. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 67. APP PROTECTION USER REPORTS FIELDS

Fields	Description
Bundle ID/Package ID	This column lists the unique identifier for the app.
Device Name	This column lists the name of the device.
Device Type	This column lists the type of device.

TABLE 67. APP PROTECTION USER REPORTS FIELDS (CONT.)

Fields	Description
Policies	This column lists the app protection policies assigned to this app.
Status	This column lists the sync status of the app. The options for this column are: **Synced**, **Synced, but out of date**, and **Not synced**.
Last Check-In	This column lists the time stamp of the last time this app synced with Azure.

Downloading App Protection reports by app

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Click **App**.
4. Complete the form.
   See App Protection App reports table for details.
5. Click **Download Report**.
6. Expand **App Protection Reports**.

App Protection App reports table

This option provides user data for selected apps.These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 68. APP PROTECTION APP REPORTS

Fields	Description
Platform	Select the OS platform for which you want to see apps. The options are Android and iOS.
App	Select the single app for which you want to receive a report. This list changes depending on the platform you select.
Status	Select the user's protection status from the list. The options are **Protected** and **Unprotected.**
User	This column lists the users that match the search criteria.
Email	This column provides the user's email address.

Downloading App Configuration reports

App Configuration Reports show applications with configurations defined and assigned to them under the **Configuration** tab. Use this option to download app configuration .csv reports by users or apps.

Downloading App Configuration reports by user

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Expand **App Configuration Reports**.
4. Click **User**.
5. Search for, or enter a user name.
   See App Configuration User reports table for details.
6. Click **Download Report**.

App Configuration User reports table

Select this option to view and download reports and to refresh the report data. This option provides app information for a specified user. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 69. APP CONFIGURATION USER REPORTS FIELDS

Fields	Description
Bundle ID/Package ID	This column lists the unique identifier for the app.
Device Name	This column lists the name of the device.
Device Type	This column lists the type of device.
Configurations	This column lists the app protection configurations assigned to this app.
Last Check-In	This column lists the time stamp of the last time this app synced with Azure.

Downloading App Configuration reports by app

Procedure

1. Log into the Admin Portal.
2. Select **Services > Microsoft Graph > Reports**.
3. Expand **App Protection Reports**.
4. Click **App**.

5. Complete the form.
   See App Configuration App reports table for details.
6. Click **Download Report**.

App Configuration App reports table

This option provides user data for selected apps.These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 70. APP CONFIGURATION APP REPORTS

Fields	Description
Platform	Select the OS platform for which you want to see apps. The options are Android and iOS.
App	Select the single app for which you want to receive a report. This list changes depending on the platform you select.
User	This column lists the users that match the search criteria.
Email	This column provides the user's email address.

Office 365 App Protection settings

Use the **Settings** tab to set up Office 365 App Protection policies to help protect your company's data.

License Required: This feature requires a separate license. In addition, this feature requires an Intune subscription from Microsoft. Prior to using this feature, ensure your organization has purchased the required licenses.

Related topics

- Office 365 App Protection overview
- Office 365 App Protection policies
- Office 365 App Protection configurations
- Office 365 App Protection user groups
- Office 365 App Protection reports

Zebra Support

MobileIron enables administrators to apply firmware updates to Zebra Devices using Zebra's Cloud OTA (Over the Air) service. Zebra devices are managed without OTA. From Core version 10.6 through the latest release as supported by MobileIron, Zebra OTA firmware update is supported. This allows you to activate the Zebra OTA

service for your Core, thus enabling you to receive firmware updates for OTA-capable Zebra Devices through firmware policies.

Process for Zebra support:

1. Adding a Google account to an Android enterprise managed device
2. Enrolling in the Zebra OTA (Over The Air) service
3. Setting the firmware policy for Zebra devices
4. Checking the Zebra device firmware download status

Enrolling in the Zebra OTA (Over The Air) service

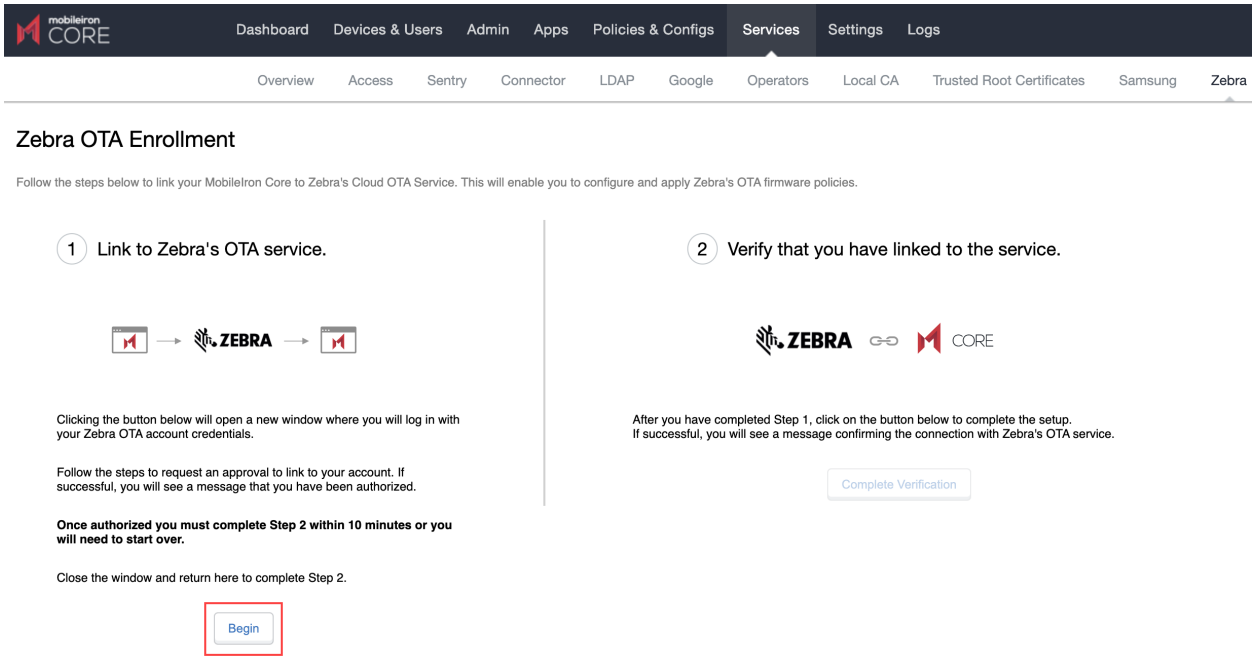
You can activate the Zebra OTA (Over The Air) service for your Core that would enable you to receive firmware updates for OTA capable Zebra devices through firmware policies. Core uses OAuth 2.0 for authentication with Zebra.

Before you begin

- Be sure you have added a Google account to the Android enterprise managed device.
- You will need to write down your Zebra OTA account credentials, when you get them.
- The enrollment process needs to be completed within ten minutes, otherwise the token expires.

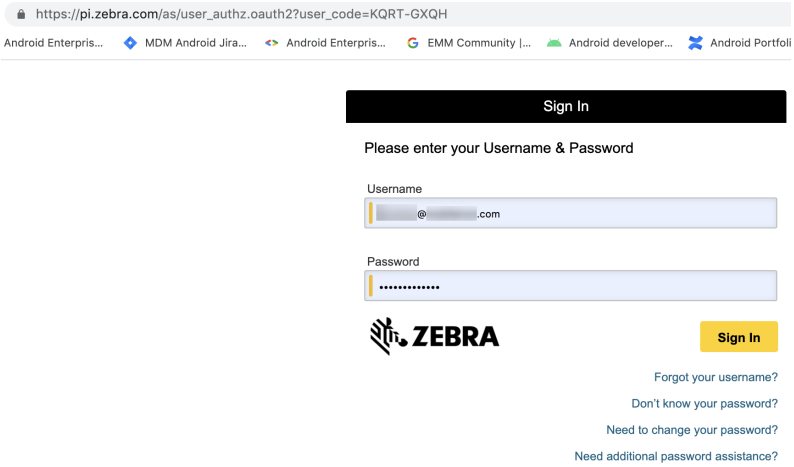
Procedure

1. In the Admin portal, go to **Services > Zebra**.
2. The **Zebra OTA Enrollment** page displays.

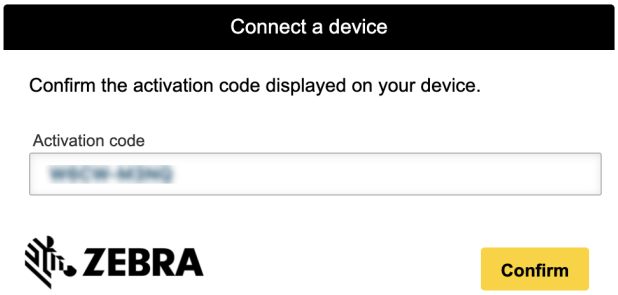


In section one, click the **Begin** button. A new browser window opens the Zebra login page.

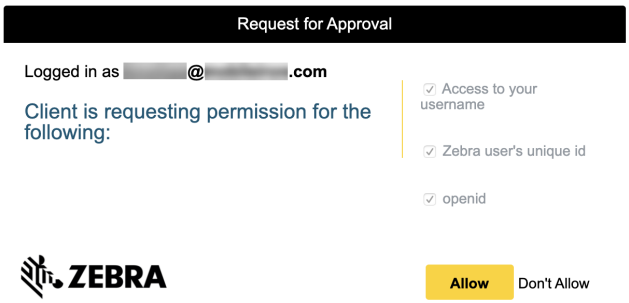
3. Enter your Zebra login credentials and click **Sign In**. If you do not have credentials, contact Zebra.



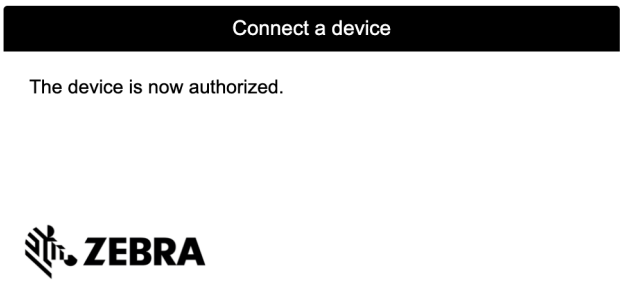
4. The Connect a device page displays with the Activation code already inserted. Click **Confirm**.



5. The Request for Approval page displays. Make sure all the check boxes are selected and then click **Allow**.

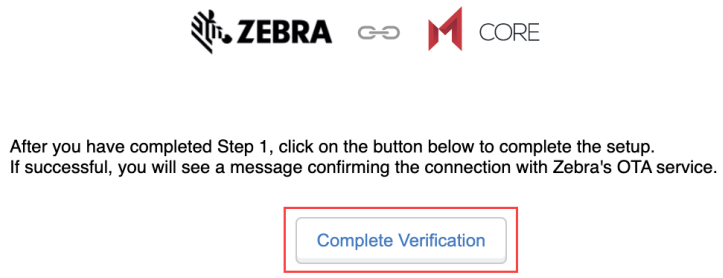


6. The Connect a device page displays. When the device is connected, a confirmation displays.



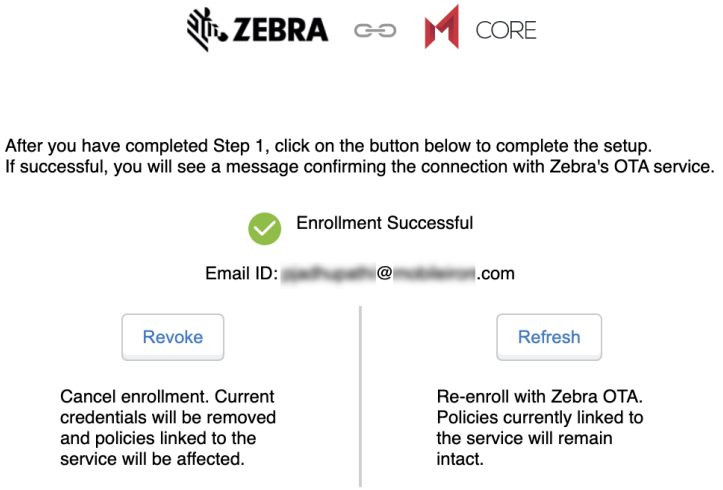
7. Return to the **Core > Services > Zebra** browser page.
8. In section two, click the **Complete Verification** button.

   2 Verify that you have linked to the service.



9. A confirmation displays confirming successful enrollment with Zebra's OTA service, along with your email ID.

   2 Verify that you have linked to the service.



After enrollment, you can enable the Zebra firmware policy (see Setting the firmware policy for Zebra devices) which the Mobile@Work client receives and applies to Zebra devices (running on Android version 8.0 through the latest version as supported by MobileIron) in Work managed device (Device Owner) mode and Managed Device with Work Profile mode. When the policy is applied, the firmware is downloaded and installed on the device as scheduled in the configuration.

Re-enrolling with Zebra OTA

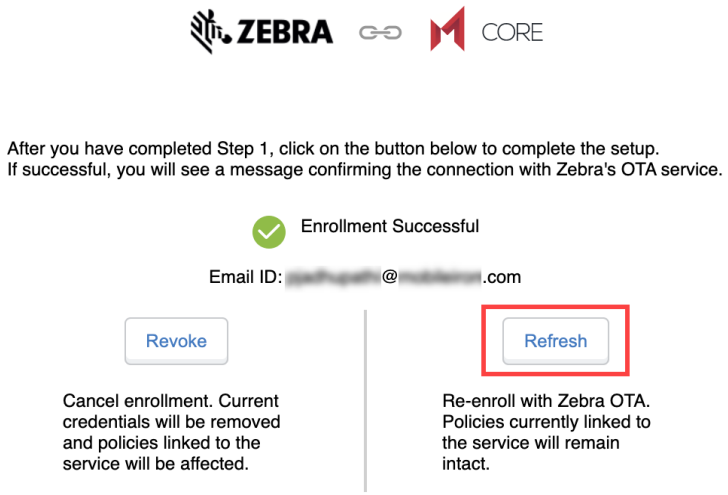
You can do re-enroll with Zebra OTA service and not lose your existing configurations. For example, in the Services > Zebra page, if you see "Enrollment status cannot be verified," then you need to refresh or re-enroll the Zebra OTA

service.

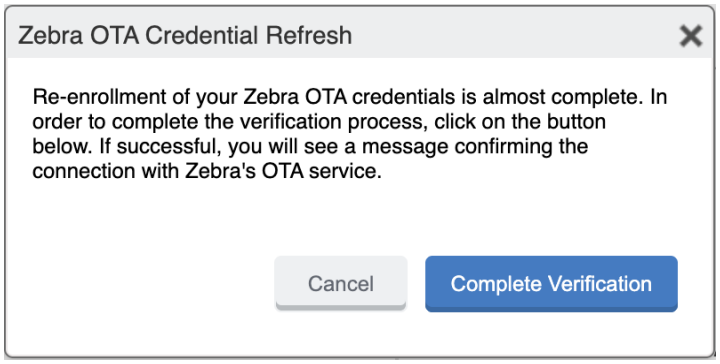
Procedure

1. Go to the **Services** > **Zebra** page.
2. In section two, click the **Refresh** button.

   2 Verify that you have linked to the service.



3. Repeat the enrollment steps in Enrolling in the Zebra OTA (Over The Air) service.
4. The Zebra OTA Credential Refresh dialog box opens. Click **Complete Verification**.



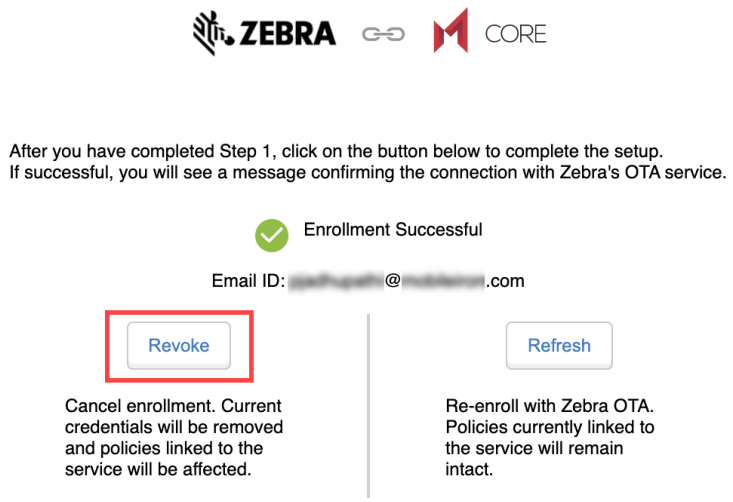
Revoking the Zebra OTA service

If you want to discontinue using Zebra OTA service, you can remove the Zebra OTA service credentials. The Revoke action removes all Zebra OTA configurations from the existing configurations.

Procedure

1. Go to the **Services > Zebra** page.
2. In section two, click the **Revoke** button.

   2 Verify that you have linked to the service.



3. Click **Confirm**.

To enroll again, you will need to start at the beginning of the enrollment process. See Enrolling in the Zebra OTA (Over The Air) service.

Next steps

Setting the firmware policy for Zebra devices

Setting the firmware policy for Zebra devices

Administrators can limit device updates to Zebra OTA (Over The Air) firmware releases using this feature. While creating the firmware policy, the administrator needs to also configure the firmware with respect to the device models. When applying the label to the policy, the policy is pushed to all the devices that meets that label criteria.

The administrator can create and apply multiple policies to a single label. The policy with the highest priority is applied in case of conflicts between multiple policies.

Before you begin

- Activate your Zebra OTA (Over The Air) service. See Enrolling in the Zebra OTA (Over The Air) service.
- Verify that affected devices are running Mobile@Work version 10.6 and above, as supported by MobileIron.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click **Add New > Android > Firmware policy**. The Add Android Firmware Policy dialog box opens.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
   - **Active**: to turn on this policy.
   - **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list. This option is only available if there is more than one policy.
7. Enter a **Description** (optional).
8. Select the **Enable Zebra OTA Firmware Policy** check box. The section expands.
9. See the following table for a description of the fields in the Zebra firmware policy.

Item	Description
Device Model	Lists the model of the Zebra device(s), for example, TC51, TC52.
Current Build ID	Lists the Build ID currently on the selected Zebra device.
Device Count	Lists the number of Zebra devices with the current build ID and device model.
Action	Leaving the selection to **None** indicates no action will be taken. Clicking the **None** link opens a drop-down box to choose: a. **Full Upgrade** - Zebra Android Device firmware upgrade, from selected version to the next major version (for example, from version 1.0 to 2.0.) Includes Build ID, Security Patch Date, OS Version and Description of the firmware. b. **Patch Upgrade** - Zebra Android Device firmware upgrade for patch releases, for example, from version 1.1 to 1.2. Includes Build ID, Security Patch Date, OS Version and Description of the firmware.
Target Build ID	Defines the build selected by the administrator for the firmware upgrade. Core only displays the firmware that is above the Current device build; device firmware downgrade is not supported. Administrator can click on the link of the target build and modify the selected version.
Date	Defines the date when the firmware is released.
OS Version	Operating System version of the Zebra device.
Download over Metered	Disabled by default. Select to require the Zebra Firmware be downloaded

Item	Description
Network	over a metered network.
Require Charging	Enabled by default. Require the Zebra device be plugged in and charging at the time of the firmware download / upgrade.
Require Device Idle	Enabled by default. Require the Zebra device be idle / not being used at the time of the firmware download / upgrade.
Apply Schedule for Download	Selecting the check box activates the section. Select the day(s) of the week, the Start Time and End Time of the download. The time referenced is the local time of the Zebra device.
Apply Schedule for Update	Selecting the check box activates the section. Select the Start Date, End Date, Start Time and End Time of the upgrade. The time referenced is the local time of the Zebra device.

10. Click **Save**.
11. Select the policy then select **Actions > Apply to Label**.
12. Select one or more labels.
13. Click **Apply**.

Related topics

Setting the firmware policy for Samsung devices

Checking the Zebra device firmware download status

You can check the status of the system update for a Zebra Android device by going to the Device details page and viewing the values in the **Zebra Build Fingerprint**, **Zebra Device Build Id**, **Zebra Device System Update**, **Zebra OTA Capable**, and the **Zebra Patch Version** fields.

Procedure

1. In the Admin portal, go to **Devices & Users > Devices**.
2. In the Advance search field, use the **Zebra Device System Update** option as part of your search criteria.
3. The following values can be returned (listed alphabetically):

Setting	Description
Available (Android 8 or Zebra devices)	A system update is currently available for this device.
Downloading (Zebra only)	System update is currently being downloaded to the Zebra device.
Pending (Zebra devices only)	The system update policy has been applied but the update has not been downloaded or applied.
Current	The most current update is installed (applicable for Zebra Android 8.0 through the most recently released version as supported by MobileIron.)
Unknown	Not supported by client or OS version.

4. Alternately, you can expand a device and in the Device Details tab, scroll to the bottom to the **Zebra Device System Update** field.

Samsung Knox Settings

This chapter includes the following topics:

Android Samsung browser settings

Go to **Policies & Configs > Configurations** and click **Add New > Android > Samsung Browser** to configure web browser options for Samsung KNOX devices (API 4.x). This setting also requires the **Samsung KNOX Container** configuration.

The following settings are available:

TABLE 71. SAMSUNG BROWSER OPTIONS

Setting	Description
Name	Enter a name for the Samsung browser setting.
Description	Enter an optional description of the new Samsung broswer setting.
Enable Auto Fill	Select to enable automatic completion of web forms.
Allow Cookies	Select to allow use of cookies.
Enable Javascript	Select to enable Javascript.
Allow Pop-ups	Select to allow pop-ups.
Enable Show Security Warning	Select to display browser security warnings. NOTE: Not supported for Samsung Galaxy S4.
Enable SmartCard Authentication	This feature is not supported.

Android Samsung Knox Container Settings

A Samsung KNOX container configuration creates a secure container on Samsung KNOX devices (API 4.0+). Apps in the KNOX container cannot communicate with apps outside of the container. Data in the secure container cannot be sent outside of the container.

NOTE: Sharing Bluetooth data from within the KNOX Workspace is controlled by a device-level setting by the user. You must enable Bluetooth in the Lockdown policy by going to **Policy & Configs > Policies > Lockdown** and selecting the Bluetooth **Enable** radio button.

To configure the Samsung KNOX Workspace mode:

1. In the Admin Portal, go to **Policies & Configs > Configurations >Add New > Android > Samsung KNOX Container**. The New Samsung KNOX Container Setting dialog box opens.
2. In the **Authentication** section, enter the password rules and behavior you want to enforce.
3. In the **App Settings** section, use the drop-downs to select settings for Browser, Exchange, and VPN in the container.

See Samsung Knox support on page 400 for information about configuring Samsung KNOX.

Use these settings to:

- specify requirements for the container password.
- specify which apps to install in the container.
- specify restrictions.
- select the Android Samsung browser configuration to use in the container.
- select the Exchange configuration to use in the container.
- select the VPN configuration to use in the container.

NOTE: Make sure only one Samsung KNOX container setting applies to each device.

TABLE 72. SAMSUNG KNOX CONTAINER SETTINGS

Item	Description
Name	Enter brief text that identifies this group of Samsung KNOX container settings.
Description	Enter additional text that clarifies the purpose of this group of Samsung KNOX container settings.
Authentication	
Enforce Multi-Factor Authentication	Select **On** to require the device user to enter both a password and a fingerprint to access the Samsung KNOX container. Therefore, the device user must create a fingerprint on the device.

TABLE 72. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
	The default is **Off**. Enforcing multi-factor authentication requires the following on the device: • Mobile@Work 9.1 for Android • Samsung KNOX 2.2 through the most recently released version as supported by MobileIron **Important:** After multi-factor authentication has been enforced on a device, changing this setting to **Off** has no impact on the device. Multi-factor authentication is still enforced, as designed by Samsung.
Password Type	Select the kind of password to require: • Simple: (Supported only on devices with Mobile@Work 8.0 and KNOX version 2.0). • Alphanumeric: Must include at least one alphabetic and one numeric character. • Complex: Must include at least one alphabetic, one numeric, and one special character (i.e., a symbol).
Min Password Length	Specify a minimum length for the password. Valid range is 4-16. The default value is 6.
Min Number of Complex Characters	Specify the minimum number of complex characters for the passcode. Valid range is 0-10. For example, to require at least two complex characters in the passcode, enter 2.
Max Character Occurrences	Specify a limit for the number of times a specific character can occur in the passcode. For example, to prevent a specific character from occurring 3 or more times, enter 2.
Max Character Sequence Length	Specify a limit for the number of characters that can appear in sequence in a passcode. For example, to prevent *abc* from occurring in a passcode, enter 2.
Max Numeric Sequence Length	Specify a limit for the number of numeric characters that can appear in sequence in a passcode. For example, to prevent “123” from occurring in a passcode, enter 2.
Min Character Change Length	Specify a minimum number of characters that must change when the passcode is reset. For example, to ensure that at least 2 characters change, enter 2.
Forbidden Strings	Specify any strings that must not be present in the passcode.

TABLE 72. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
	To add a string: Click + to add an entry. Click the “Name” placeholder in the new entry. Replace “Name” with the string you want to add. For example, to prevent the passcode from including the user’s email address or last name, enter $EMAIL$, $LAST_NAME. Use the tool tip to see a list of substitution variables you can use here.
Max Inactivity Timeout	Specify the idle time duration after which the lock should be enabled. If the password is set, the user is prompted for a password when unlocking the container.
Max Password Age	Specify the number of days after which the password expires.
Stored Password History	Specify the number of previous passwords that are stored and cannot be used when setting a new password.
Max Number of Failed Attempts	Specify the maximum number of failed password attempts to allow. When this number is exceeded, the KNOX container is disabled.
Password Visible Option	Select **Off** to disable the “Make password visible” option.
Apps	
	Select the in-house apps to be installed in the container: Click the + button. Select an app from the **Name** list. The **Version** and **Identifier** fields are filled in automatically.
Restrictions	
Google Play Store	The default setting is **Off**. Select the **On** radio button to enable whitelisting Google accounts.
Whitelist Google Accounts	Enter the domains of accounts that can be added in the KNOX container.
Allow Camera	Select to allow the device user or third-party apps to use the photo camera, video camera, and video telephony features. NOTE: If the camera is allowed in the KNOX container restriction policy, but not allowed via the device lockdown policy, the camera does not function in the KNOX container.
Allow Content Sharing (i.e., Share Via)	Select to allow use of the Share Via List, which is displayed in certain apps that share content with other apps.

TABLE 72. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
Allow Email Account Creation	Select to allow the user to create email accounts. By default, this is unselected and end users cannot create email accounts in the KNOX container.
Allow Non-Secure Keypad	Select to allow keyboards inside the container, regardless of whether they are pre-loaded or third-party keyboards.
Allow Samsung KNOX App Store	Select to allow device users to download apps from the Samsung KNOX app store (www.samsungknox.com).
Allow Screen Capture	Select to allow user to take a screenshot to help with troubleshooting.
Allow Remote Control	Select to allow alternate provisioning of the KNOX container.
Allow NFC	Select to allow enrollment of the device using the NFC bump.
Allow USB	Select to allow so that apps that need USB access function properly.
Install all CA certificates inside KNOX workspace	Select to deploy CA certificates inside and outside of the KNOX container to secure traffic on apps inside the Work Profile mode with a self-signed or well-known certificate. If you deselect this option, CA certificates are only installed on the outside of the container and certificates installed on the inside of the container are removed.
App Settings	

TABLE 72. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
Browser	Specifies the Android Samsung Browser configuration to use in the KNOX container. You need to create the Samsung Browser configuration separately. Otherwise, this list will be empty.
Exchange	Specifies the Exchange configuration to use in the KNOX container. You need to create the Exchange configuration separately. Otherwise, this list will be empty.
VPN	Specifies the VPN configuration to use for Samsung KNOX IPsec in the container. You need to create the configuration separately. Otherwise, this list will be empty. NOTE: The KNOX VPN client must be installed on the device *before* you push the KNOX VPN configuration. 1. Download the KNOX VPN client from the Samsung KNOX portal: https://www.samsungknox.com/en/resources/sdk/download-knox-vpn-client Go to Resources -> Tools (at the bottom) -> Download KNOX VPN Client. To create a user ID in the Samsung KNOX portal, an active KNOX license key (trial or product) is required. 2. Upload the KNOX VPN client to the **App Catalog**. 3. Create a new VPN configuration with Samsung KNOX IPsec specified as the connection type (**Policies & Configs > Configurations > Add New > VPN**). 4. Select the new VPN configuration in the Samsung KNOX container (go to **Policies & Configs > Configurations**, then click **Add New > Android > Samsung KNOX Container**).

Supported variables

You can use the following substitution variables in the Forbidden Strings field in the Samsung KNOX Container Setting:

- $EMAIL$
- $USERID$
- $FIRST_NAME$
- $LAST_NAME$
- $DISPLAY_NAME$
- $USER_CUSTOM1$
- $USER_CUSTOM2$
- $USER_CUSTOM3$

- $USER_CUSTOM4$
- $NULL$

You can also enter strings, such as:

- 12345
- Example password

Samsung KNOX Workspace support for Google Play

You can enable users to use Google Play inside the Samsung KNOX Workspace. Account whitelisting is supported for Google Play Services account types. Other account types, such as accounts defined by an application such as Gmail or Facebook, are not exempted by this whitelist as they are of a different account type. Therefore, it is important to avoid whitelisting applications that can allow undesired accounts into the KNOX Workspace.

NOTE: Users are only permitted to download apps that are whitelisted for the Samsung KNOX Container, but they are still able to browse the entire contents of the Google Play Store.

To enable Samsung KNOX Workspace support for Google Play:

1. In the Admin Portal, go to **Policies & Configs > Configurations >Add New > Android > Samsung KNOX Container** to open the New Samsung KNOX Container Settings dialog box.
2. In the **Restrictions** section, select **Google Play Store: On** radio button to enable the Google Play Store. It is set to **Off** by default.
3. Optionally, in the **Whitelist Google Accounts** field, select the **Account** check box to enter the domain URL or wildcard domain. This specifies which Google accounts or wildcard domains may be used inside the KNOX Container.
4. **Save** your changes.

MobileIron Tunnel support in the Samsung Knox Workspace

You can configure MobileIron tunnel support on Android devices. For detailed information on support and setup for MobileIron Tunnel in the Samsung KNOX container, see the *MobileIron Tunnel for Android Guide for Administrators*.

On-Demand Support for Samsung Knox VPN connections

You can enable On-Demand for Samsung KNOX for VPN apps that support On-Demand connections.

NOTE: On-Demand is not supported for container-wide VPN apps.

To enable On-Demand for Samsung KNOX:

1. In the Admin Portal, go to **Policies & Configs > Configurations >Add New > VPN**. The Add VPN Setting dialog box opens.
2. In the **Connection Type** drop-down menu, select the **Samsung KNOX IPSec** check box. This is a VPN app that supports On-Demand.
3. Enter the information for the Server, Username, and Password.
4. Select the **VPN on Demand** check box.
5. Select the **Per-app VPN Yes** radio button.
6. Click **Save**.

Activating the Samsung firmware E-FOTA license

You can activate the Samsung firmware E-FOTA license for your devices that are capable of receiving system updates over the air when they are made available. To activate the system update policy:

1. Go to **Services > Samsung**
2. The **Samsung Firmware E-FOTA License Management** page is displayed.
3. Enter the Client ID using the following components:
   - MDM ID
   - Customer ID
   - License key
4. Enter the Client Secret.
5. Enter the Corporate ID.
6. Click **Activate**.
   If you choose to click deactivate an existing E-FOTA management service the firmware update policy reverts back to consumer device behavior.

Setting the system update policy for Android devices

This feature applies to managed devices only (with Android enterprise). Administrators can limit device users from managing system updates on Android 6.0 devices (or later releases that are supported by MobileIron). When multiple policies are applied to devices, you can select a priority for applying the policy to avoid conflicts.

Before you begin

- Verify that effected devices are running Android 6.0 (or later releases that are supported by MobileIron).

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.

3. Click **Add New > Android > Firmware policy**.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
   - **Active**: to turn on this policy.
   - **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list.
7. This option is only available if there is more than one priority.
8. Enter a **Description** (optional).
9. Select the **System Update Policy for Android 6.0 or higher** check box and enable the following options:
   - **Automatic**: silently apply the policy whenever new firmware is available.
   - **Update Window**: schedule a time period to silently apply the new firmware.
   - Select a start and end time to schedule the firmware update.
   - **Postpone**: this is hard-coded by the OS and skips any OS updates for up to 30 days after which it becomes automatic.
10. Click **Save**.
11. Select the policy then select **Actions > Apply to Label**.
12. Select one or more labels.
13. Click **Apply**.

Setting the firmware policy for Samsung devices

Administrators can limit device updates to specific firmware releases using this feature. If the device model and carrier code matches what is defined in the policy, the firmware is applied to the device to which the labels are applied. If the device model and the carrier code matches what is defined in the firmware, the label is applied to the device to which the labels is applied. Administrators can create and apply multiple policies to each device. The policy with the highest priority is applied in case of conflicts between multiple policies.

Before you begin

- Activate your Samsung license
- Verify that effected devices are running Samsung Knox version 2.7.1 and above.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click **Add New > Android > Firmware policy**. The Add Android Firmware Policy dialog box opens.

4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
   - **Active**: to turn on this policy.
   - **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list.
   This option is only available if there is more than one priority.
7. Enter a **Description** (optional).
8. Select the **Enable Samsung Firmware Policy** check box.
9. Click **Save**.
10. Select the policy then select **Actions > Apply to Label**.
11. Select one or more labels.
12. Click **Apply**.

Related topics

Setting the firmware policy for Zebra devices

AppConnect for Samsung Knox devices

This feature is not supported on Windows 8.1 Phone devices.

This feature is not supported on iOS devices.

In MobileIron deployments that use AppConnect, AppConnect for Knox is automatically used on Samsung devices that meet the following requirements:

- Device has Samsung Knox 2.1
- Device is running Mobile@Work 7.0 for Android through the most recently released version as supported by MobileIron.
- A Samsung General Policy with a valid Samsung KLM license is applied to a label that is also applied to the device. The Samsung license is required to take advantage of any Knox-related feature.

No changes are required to AppConnect configurations on MobileIron Core.

About AppConnect for Knox

AppConnect is a MobileIron feature that containerizes apps to protect data on the device from unauthorized access. In AppConnect for Knox , Mobile@Work uses Samsung Knox Platform features to provide an added layer of security. Specifically:

- Knox SE for Android (Security Enhancements for Android)

  AppConnect uses an *SE for Android* container for an added layer of security for the container and AppConnect-enabled apps.

  Knox TIMA Keystore
- AppConnect's Secure Apps key is protected using the TIMA keystore.

No user interface changes in Mobile@Work or MobileIron Core are associated with this feature.

The Samsung Knox container, known as the Knox Workspace, is not supported with AppConnect apps. Specifically:

- The Samsung Knox container does not support any AppConnect apps running inside the Knox container.
- MobileIron does not support using both a Knox container and AppConnect container on the same device.

Samsung Knox support

The Samsung Knox Container enables BYOD initiatives by creating a secure container for corporate apps within each device. This container secures access to corporate apps and data.

To configure support for the Samsung Knox Container:

1. Create a **Samsung Browser** configuration.

   If you do not intend to specify browser behavior in the container, you can skip this step.

   See Android Samsung browser settings on page 390.
2. Create an **Exchange** configuration for the container.

   If you do not intend to specify email client behavior in the container, you can skip this step.
3. Create a **Samsung Knox Container** configuration.

   The Samsung Knox Container configuration will specify the **Samsung Browser** configuration and the **Exchange** configuration you created for the container.

   See Android Samsung Knox Container Settings on page 391.
4. Create one or more labels to identify the devices that will receive the Samsung Knox Container configuration.
5. Assign the **Samsung Knox Container** configuration to the appropriate labels.

   Once the configuration is present on the device, then the device begins creating the container as specified.

Disabling the container

To manually disable the Samsung Knox container:

1. Go to **Device & Users > Devices**. Select the devices that have received the **Samsung Knox Container** configuration.

2. Click **Actions > Android Only > Disable Samsung Knox Container**.
3. Choose the container you want to disable from the **Container** list.
4. Click **Disable Samsung Knox Container**.

The container remains disabled until you manually re-enable it.

Re-enabling the container

A Samsung Knox container can be automatically disabled by policy, such as when the device user enters the container password incorrectly too many times. You can manually disable the container using the **Disable Samsung Knox Container** action.

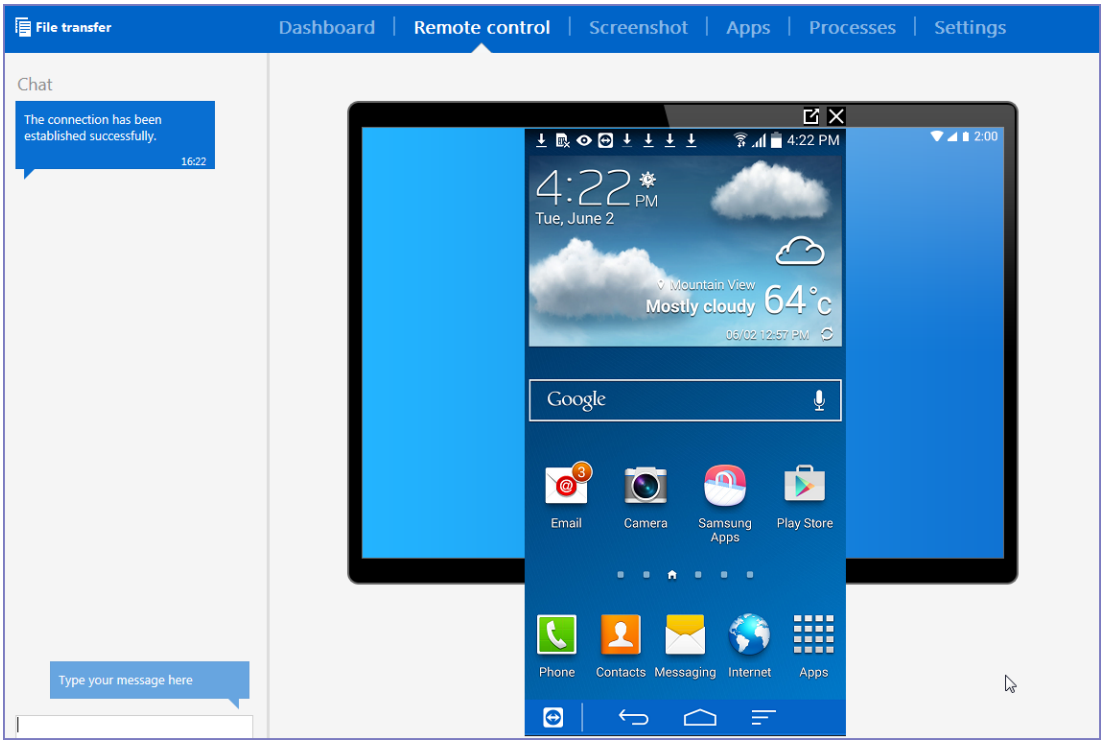
To manually re-enable the Samsung Knox container:

1. Go to **Device & Users > Devices**. Select the devices on which the container has been disabled.
2. Click **Actions > Android Only > Enable Samsung Knox Container.**
3. Choose the container you want to enable from the **Container** list.
4. Click **Enable Samsung Knox Container.**

Help@Work for Android

About Help@Work for Android

Help@Work for Android with TeamViewer is an integration that enables administrators to get remote control access to supported Android devices managed by MobileIron Core. VPN is not required. After initiating a remote control session from the Admin Portal using FCM, administrators can configure Android devices and troubleshoot issues without having the devices in hand. The remote control session displays on the administrator's desktop, enabling point-and-click navigation of the device.



Prerequisites

Help@Work for Android requires:

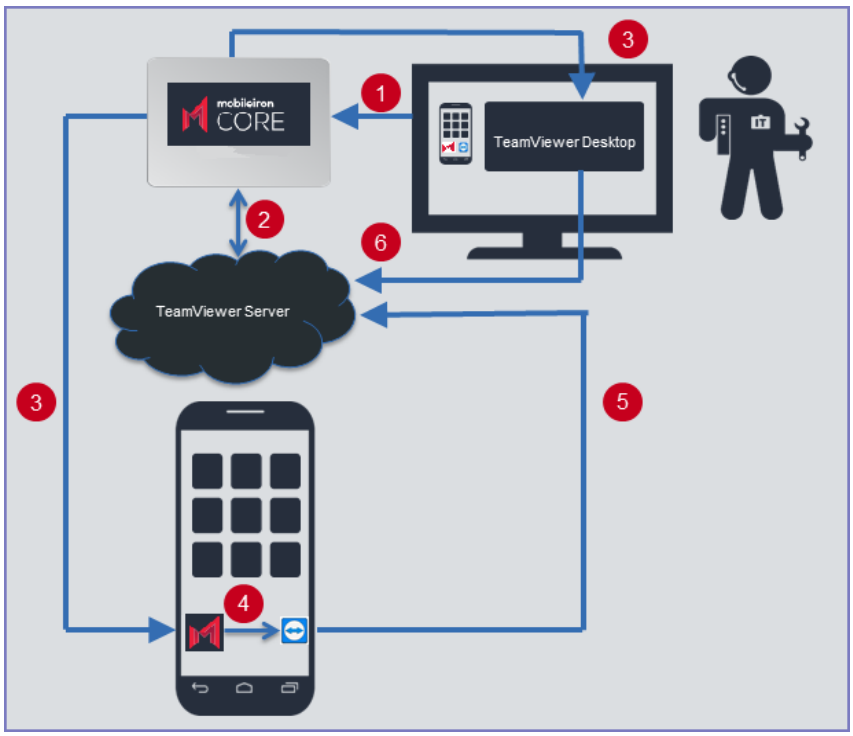
- access to the MobileIron Customer Portal (http://help.mobileiron.com) during initial setup for one-time license activation
- a company email address (belonging to an organization rather than an individual) that can be used for the TeamViewer account
- appropriate firewall rules to support FCM (see the *On-Premise Installation Guide*)
- TeamViewer 10 Desktop edition

Supported devices

For information on supported Android devices, go to https://www.teamviewer.com/En/help/341-How-can-I-control-my-Android-device-with-TeamViewer.aspx.

How Help@Work for Android works

The following diagram illustrates how Help@Work for Android with TeamViewer establishes a remote control session.

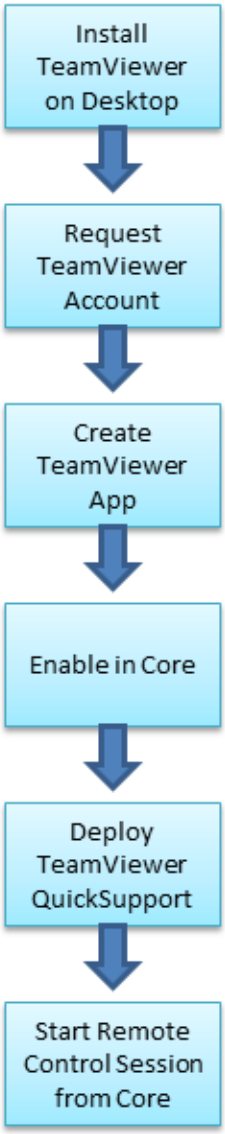


1. Administrator selects a target device in the Admin Portal Devices > Devices.

2. MobileIron Core contacts the TeamViewer Server to create a remote session and retrieve a session ID.
3. Core sends a command to Mobile@Work on the device to start a remote session using the session ID. Core also launches the TeamViewer software on your desktop with the session ID.
4. The Mobile@Work app sends a message (intent message object) containing the session ID to the TeamViewer app to start a remote session.
5. TeamViewer app connects to the TeamViewer Server.
6. Administrator takes remote control of the device.

Help@Work for Android setup overview

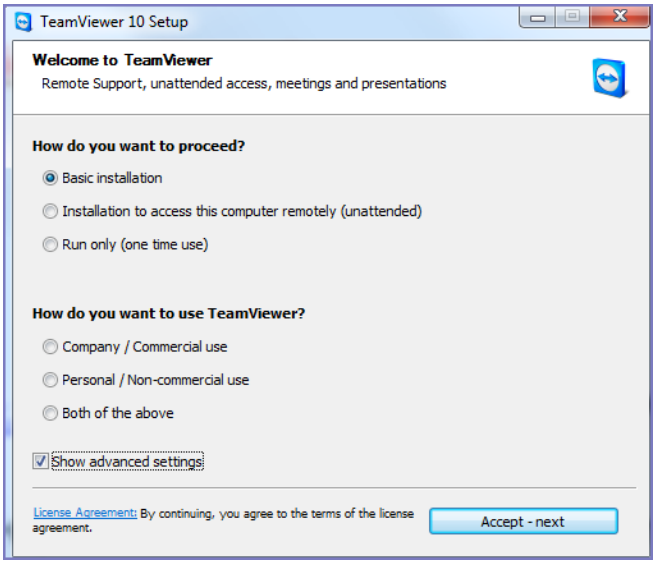
The following diagram illustrates the setup process for Help@Work for Android:



Installing TeamViewer on your desktop

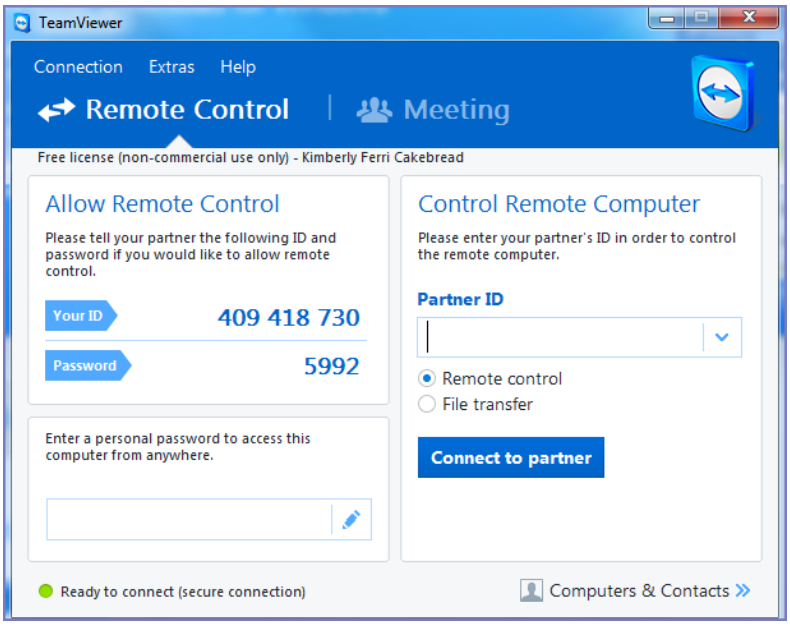
This section explains how to install the TeamViewer full version software on your Windows or macOS computer.

1. Download the installation package for the TeamViewer full version for Windows or macOS from the following location:
   https://www.teamviewer.com/en/download/
2. Launch the TeamViewer installation program.



3. Select **Basic Installation.**
4. Select **Company / Commercial use.**
5. Click **Accept - next.**

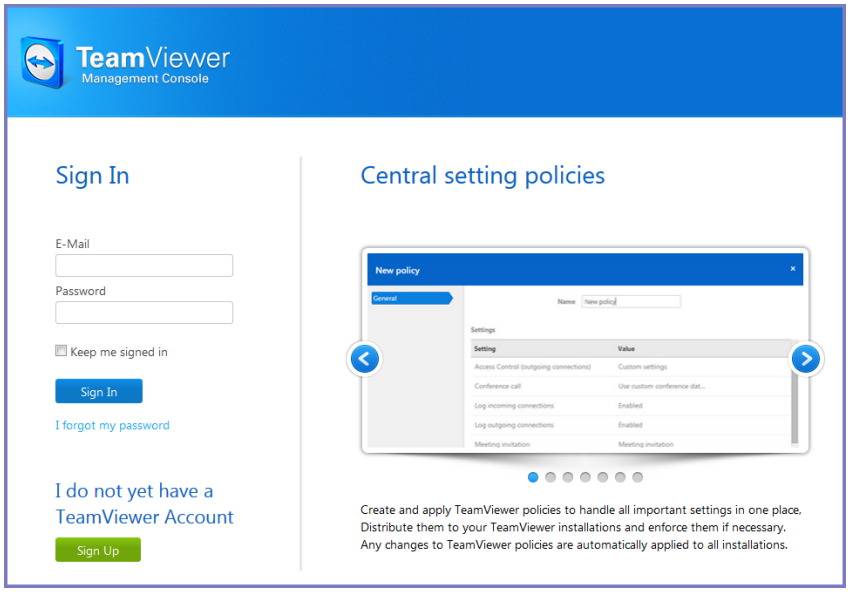
   When the installation is complete, the following screen displays.



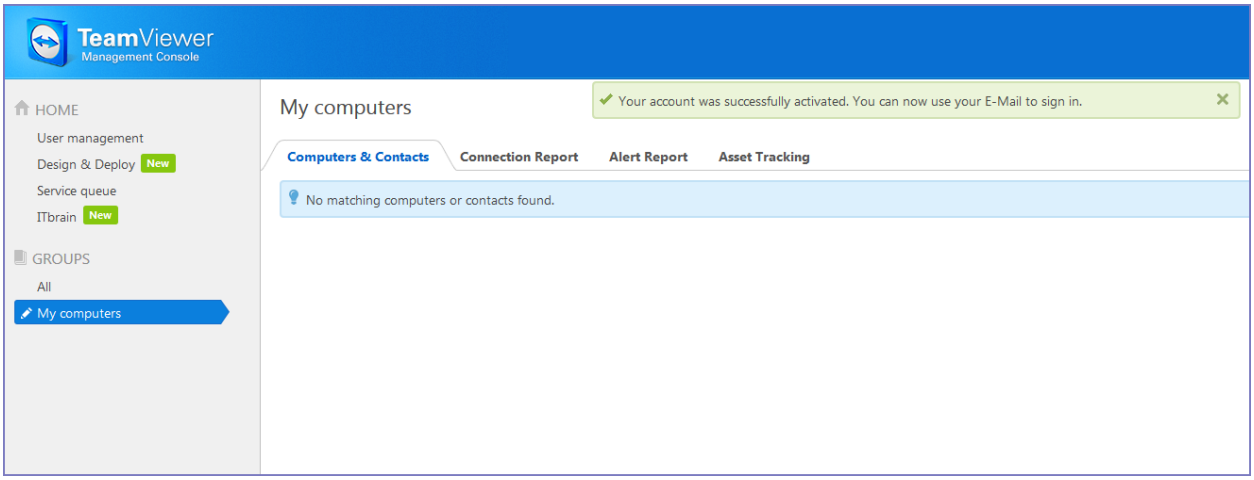
Requesting a TeamViewer account

This section explains how to get a TeamViewer account.

1. Go to https://login.teamviewer.com/LogOn#register.



2. Click **Sign Up.**
3. Set a TeamViewer email address and password.
4. Check the email account for a TeamViewer activation email.
   It might take several minutes for this email to arrive.
5. Complete the instructions in the email to activate your account.
   When the account has been activated, the following page displays:

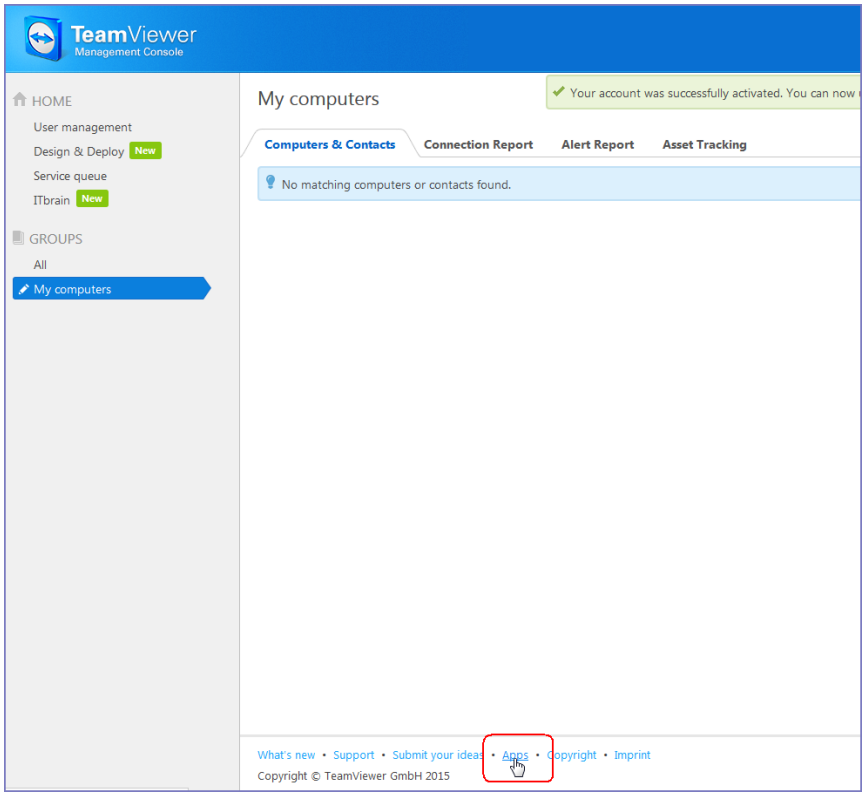


6. Bookmark this page for future reference.

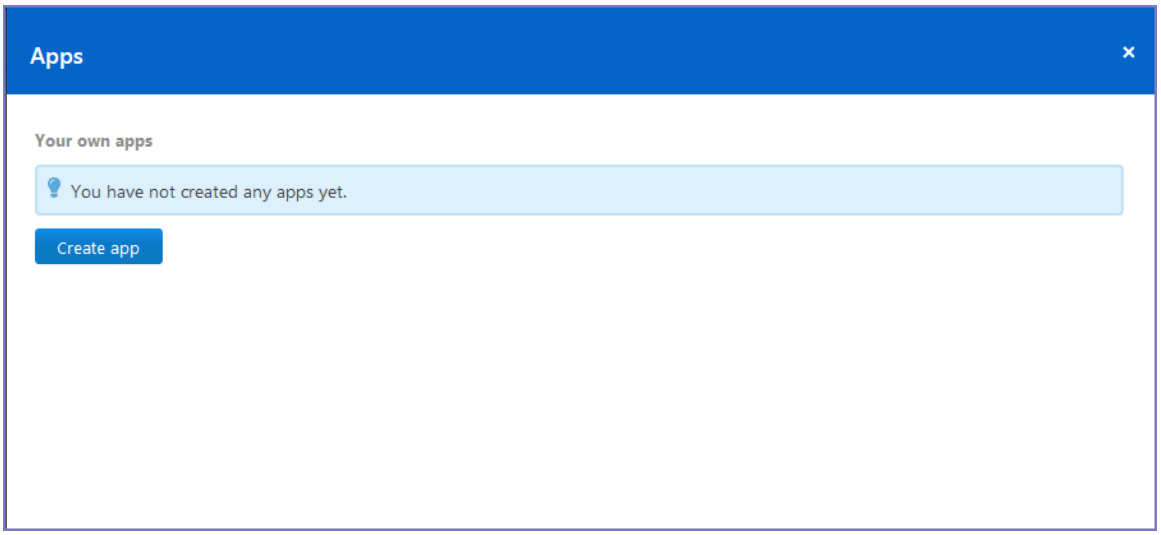
Creating a TeamViewer app

This section explains how to create a TeamViewer app for use with your MobileIron Core.

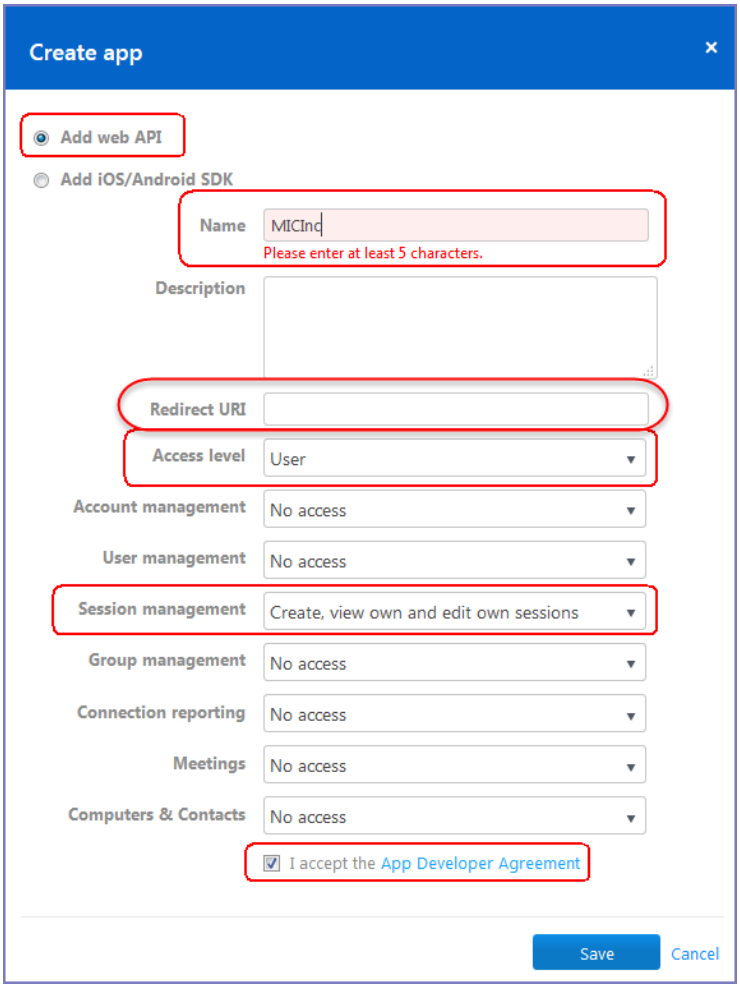
1. If you are not already logged in after TeamViewer account activation, to the TeamViewer Home page you bookmarked in Requesting a TeamViewer account on page 406.



2. Click the **Apps** link at the bottom of the TeamViewer Home page (displayed after account activation).

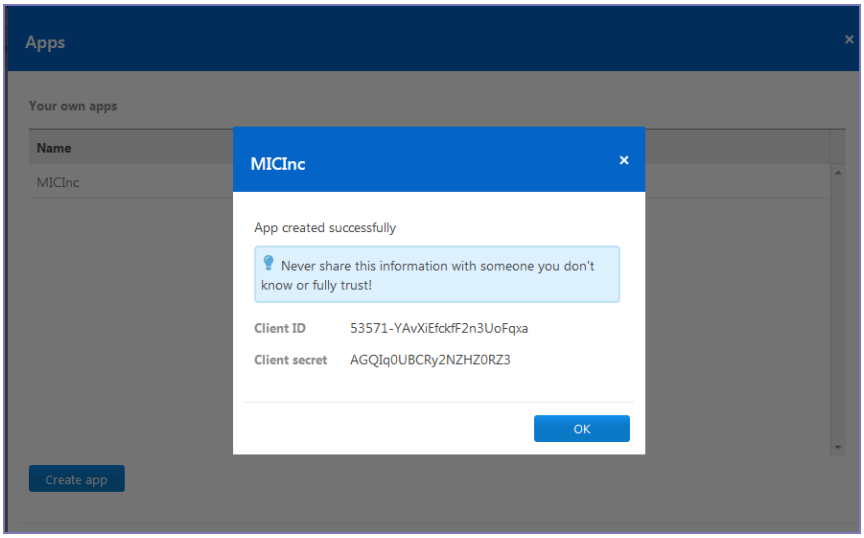


3. Click **Create app**.



4. Select **Add web API.**
5. Enter at least 5 characters to use as the app name.
   Enter at least 5 characters to use as the app name.
6. For **Redirect URI**:
   Enter it in the form of `https://<mobileironcore>/mifs/teamViewerRedirect`, where `<mobileironcore>` is the URL of your MobileIron Core installation.

   Note: Using a redirect URI is required.
7. For **Access level**,select **User**.
8. For **Session management**, select **Create, view own and edit own sessions**.
9. Select **I accept the App Developer Agreement.**
10. Click **Save**.



11. Copy the displayed Client ID and Client secret.
    You will need this information for Enabling Help@Work in MobileIron Core.
12. Click **OK**.

Enabling Help@Work in MobileIron Core

This section explains how to enable Help@Work for Android and iOS in the MobileIron Core Admin Portal.

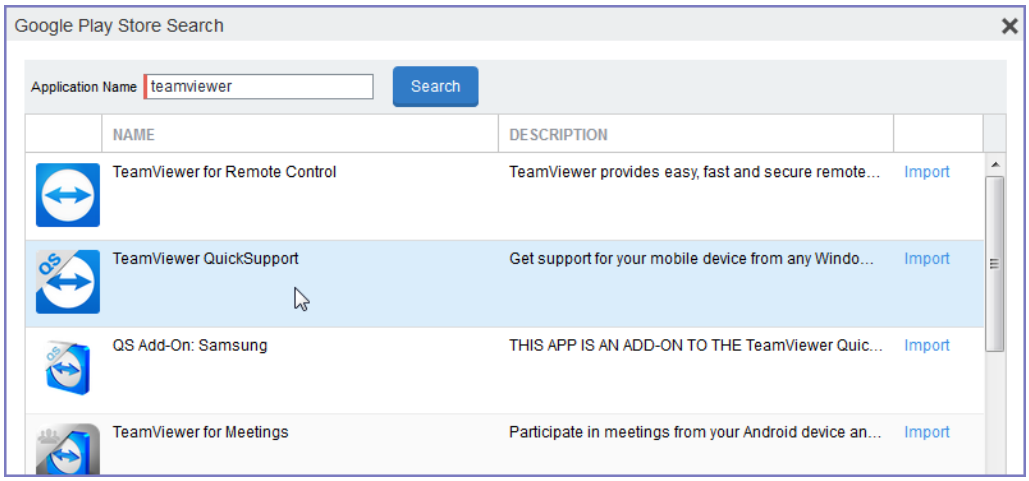
1. Log into the Admin Portal.
2. Select **Settings** > **System Settings**.
3. Select **Additional Products** > **Licensed Products.**
4. Select **Help@Work for Android and iOS 10 and higher** .
5. Accept the displayed TeamViewer license agreement and to open the Help@Work wizard.
6. Paste the **Client ID** and **Client secret** values you copied in Creating a TeamViewer app.
7. Click **Validate**.
8. In the displayed TeamViewer page, enter your TeamViewer email and password.
9. Click **Allow** to provide MobileIron Core with session management permission for your TeamViewer app.
10. Click **Sign In**.
11. Click **Activate** in the wizard to open the Customer Support login screen:
12. Enter your MobileIron Customer Support credentials.
13. Click **Login**.
14. Enter the email address you used for your TeamViewer account.
15. Click **Submit**.

NOTE: Though your license is now activated, your TeamViewer software will still display a notice about trial software. Your licensing applies to the session established using the integration, so the trial notice remains in the console.

Deploying the TeamViewer QuickSupport app

This section explains how to deploy the TeamViewer QuickSupport app to Android devices managed by MobileIron Core.

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **Quick Import**.
3. Select **Google Play**.
4. In the **Application Name** field, enter teamviewer.
5. Click **Search**.

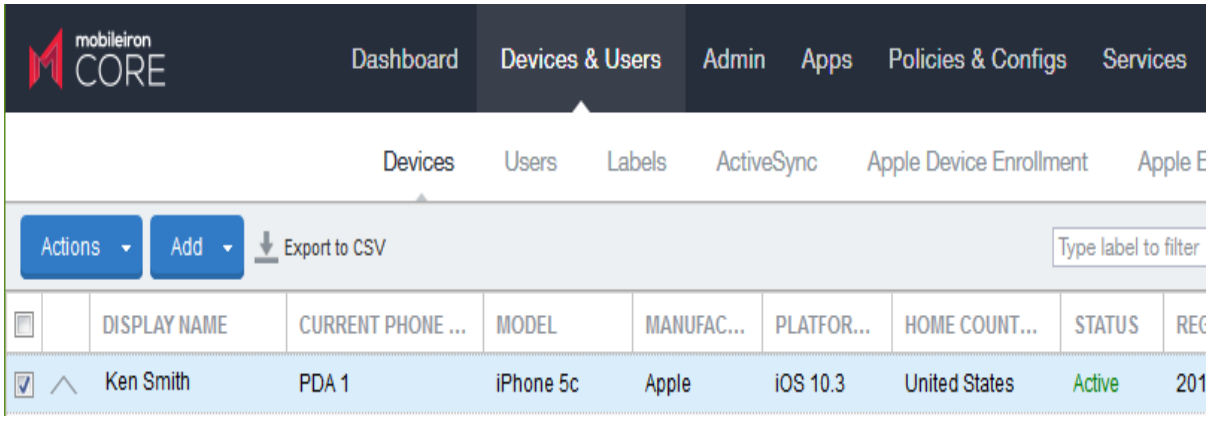


6. Find the app in the search results.
7. Click **Import**.
8. Dismiss the displayed message and the Google Play Store Search dialog.
9. Under **Apps > App Catalog**, select the app you just imported.
10. Select **Actions > Apply To Labels.**
11. Select labels that represent the devices that should have the app added to the app catalog.
12. Click **Apply**.
13. Instruct Android device users to install the app.
14. Instruct Android device users to launch the app.
    If an add-on is available for the device, the device user will be prompted to install it.
15. Instruct device users to install the add-on if prompted to do so.

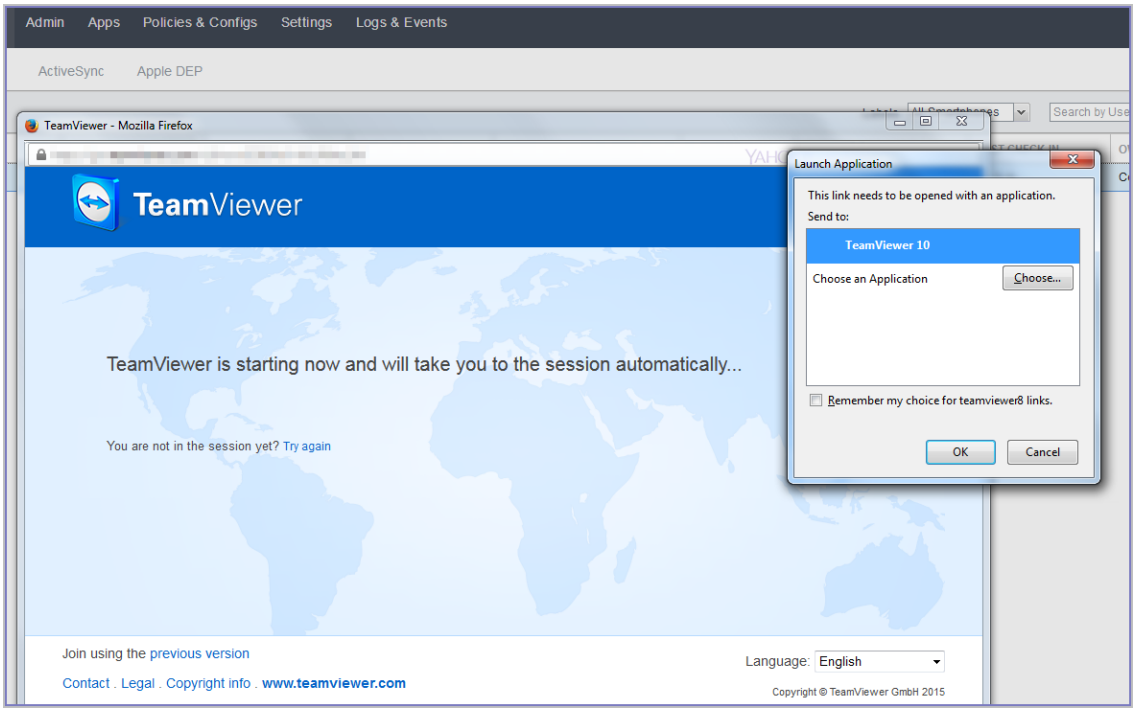
Starting a remote control session

This section explains how to start a Help@Work for Android remote control session.

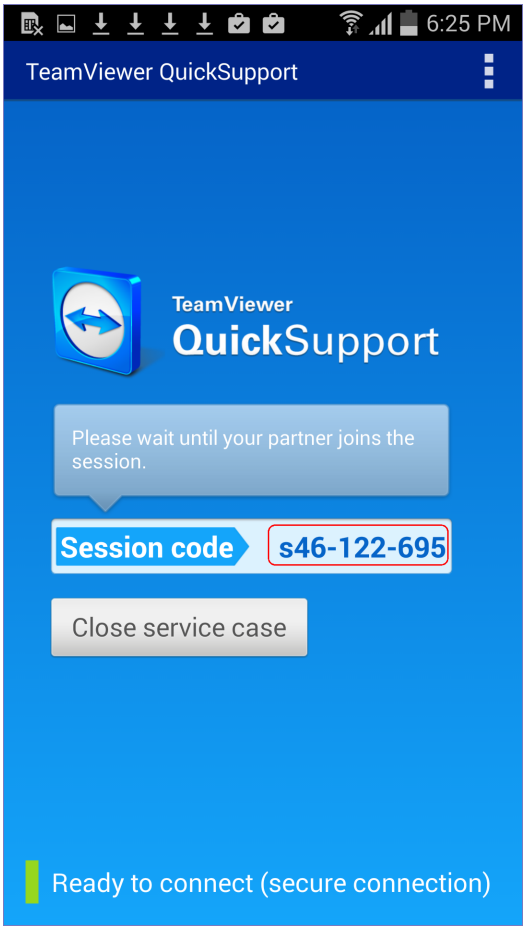
1. Ask the device user to install the TeamViewer QuickSupport app.
   It should be displayed in the MobileIron app catalog on the device.
2. In the Admin Portal, go to **Devices & Users > Devices**.
3. Select the entry for the device.



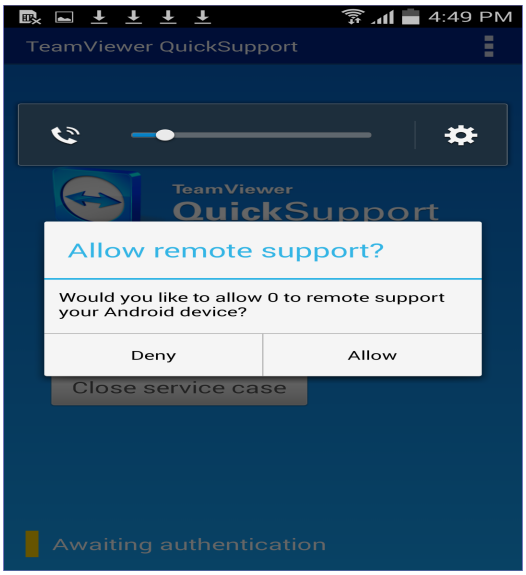
4. Confirm that the device is supported by Help@Work for Android.
   See Help@Work for Android on page 402.
5. Select **Actions > Android Only > Remote Control**.
6. If a page requesting a session ID displays, ignore it.



7. Launch the TeamViewer 10 application when prompted.
8. If your browser has pop-up blocking enabled, then allow pop-ups for your MobileIron Core URL.
9. If the TeamViewer QuickSupport app does not launch on the device, ask the device user to tap the Mobile@Work icon.
   The required session ID is automatically displayed on the device.

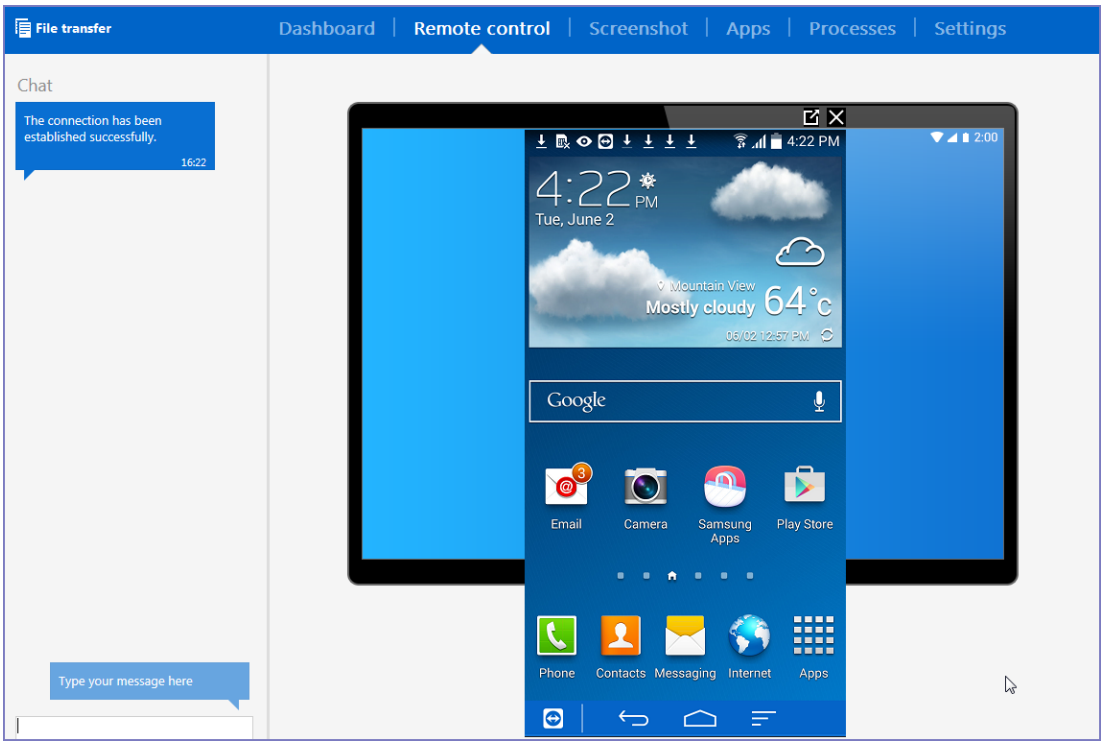


The device user should then see a prompt similar to the one below.



10. Ask the device user to tap **Allow**.

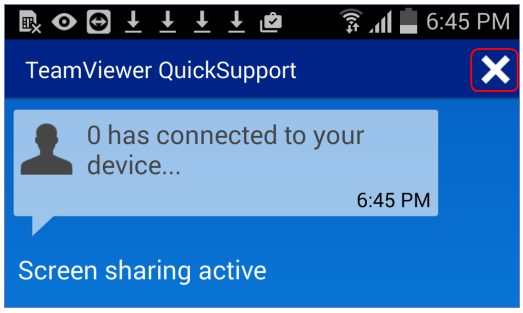
You should now see the remote control session displayed on your screen.



To close a remote control session from the device

To close a remote control session from the desktop:

1. Tap the TeamViewer QuickSupport app icon.

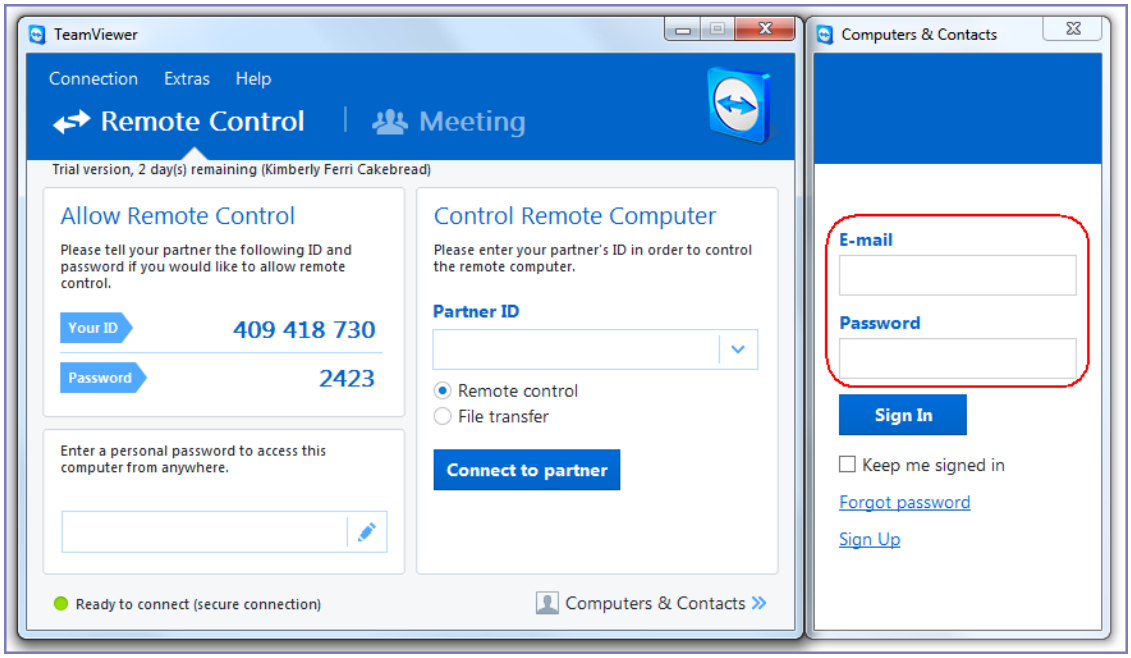


2. Tap the X in the upper right corner of the TeamViewer QuickSupport app.

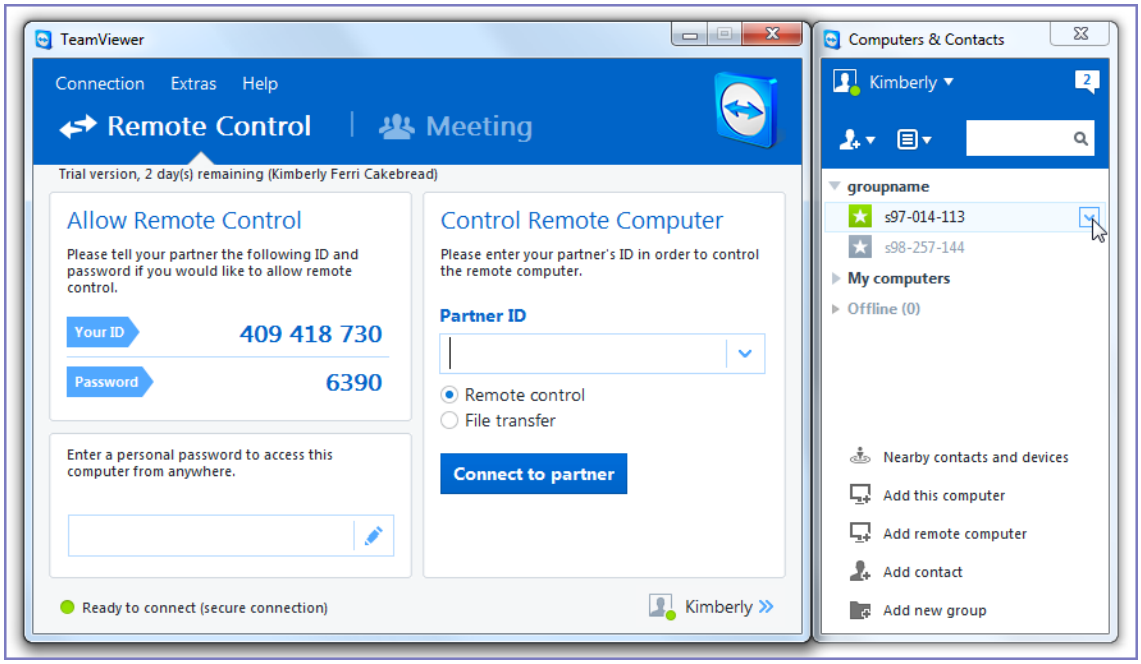
To close a remote control session from the desktop

To close a remote control session from the desktop:

1. Launch the TeamViewer desktop.



2. Sign in using your TeamViewer credentials.



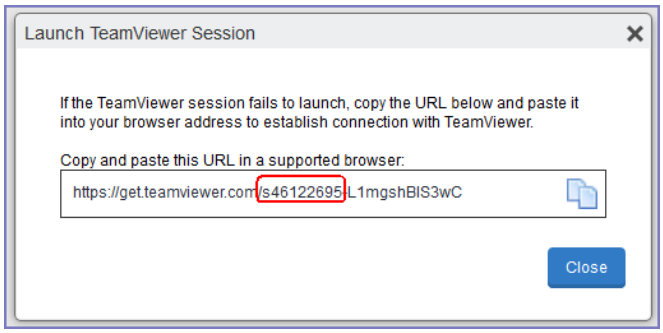
3. Select the session.
4. Click **Close**.

For more information on using remote control

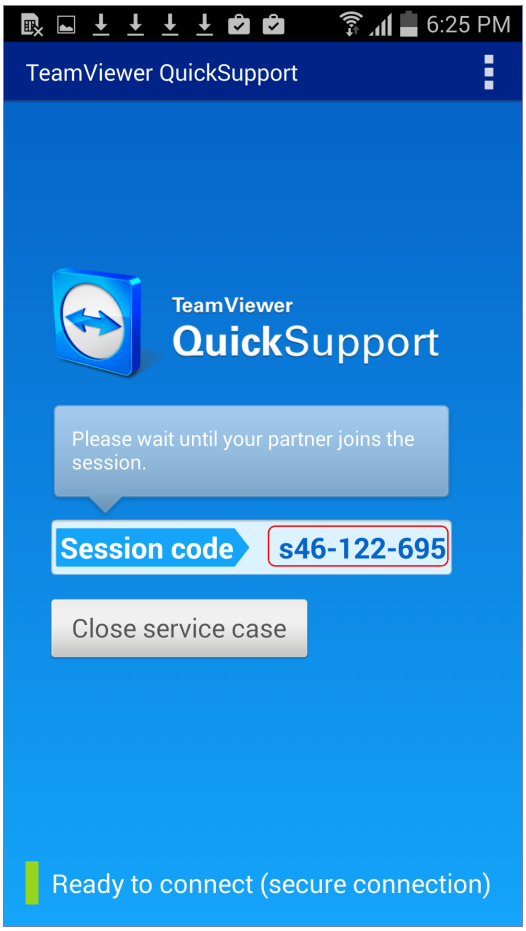
For information on how to use TeamViewer remote control, see
http://downloadus1.teamviewer.com/docs/en/v10/TeamViewer10-Manual-Remote-Control-en.pdf

If you accidentally close the session

If you close the session window on your desktop, you can re-establish the session using the URL displayed in the Launch TeamViewer Session dialog.



This dialog displays at the beginning of each session, but might be hidden behind other windows. Copy and paste the displayed URL in a browser window to regain access to the session. Make sure the session ID displayed in the dialog matches the one displayed in the TeamViewer app on the device.


6:25 PM
TeamViewer QuickSupport
TeamViewer
QuickSupport
Please wait until your partner joins the session.
Session code
s46-122-695
Close service case
Ready to connect (secure connection)

Language Support

This section addresses the language settings for MobileIron client apps (Mobile@Work.)

Translated versions of MobileIron client apps

MobileIron client apps (Mobile@Work) are localized to a number of languages. A device's locale setting (or selected language) determines the language that the MobileIron client app appears in on the device. If the device's locale is not supported, the app appears in English (United States) by default.

Once the device communicates a language change to MobileIron Core, MobileIron Core sends messages to the device in the selected language, assuming the language is supported and selected in Core's **Settings > System Settings > General > Language**.

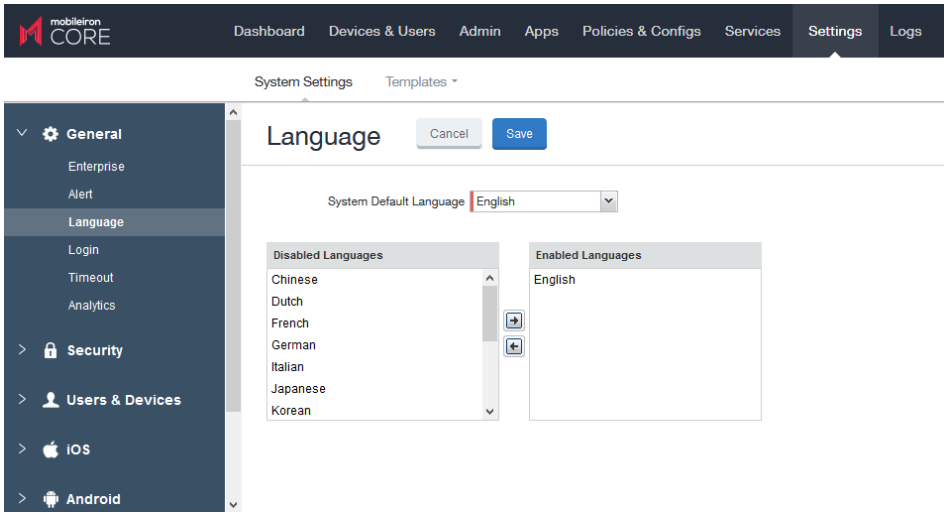
Please refer to the Core release notes for each release to see which languages and locales are supported.

Selecting languages for MobileIron Core messages

You can enable or disable languages for the messages sent from MobileIron Core to devices. For example, if you have only Japanese-speaking users, you might want to remove the other message templates from the Admin Portal.

To enable or disable languages:

1. Log into the System Manager.
2. Go to **Settings > System Settings > General > Language**.

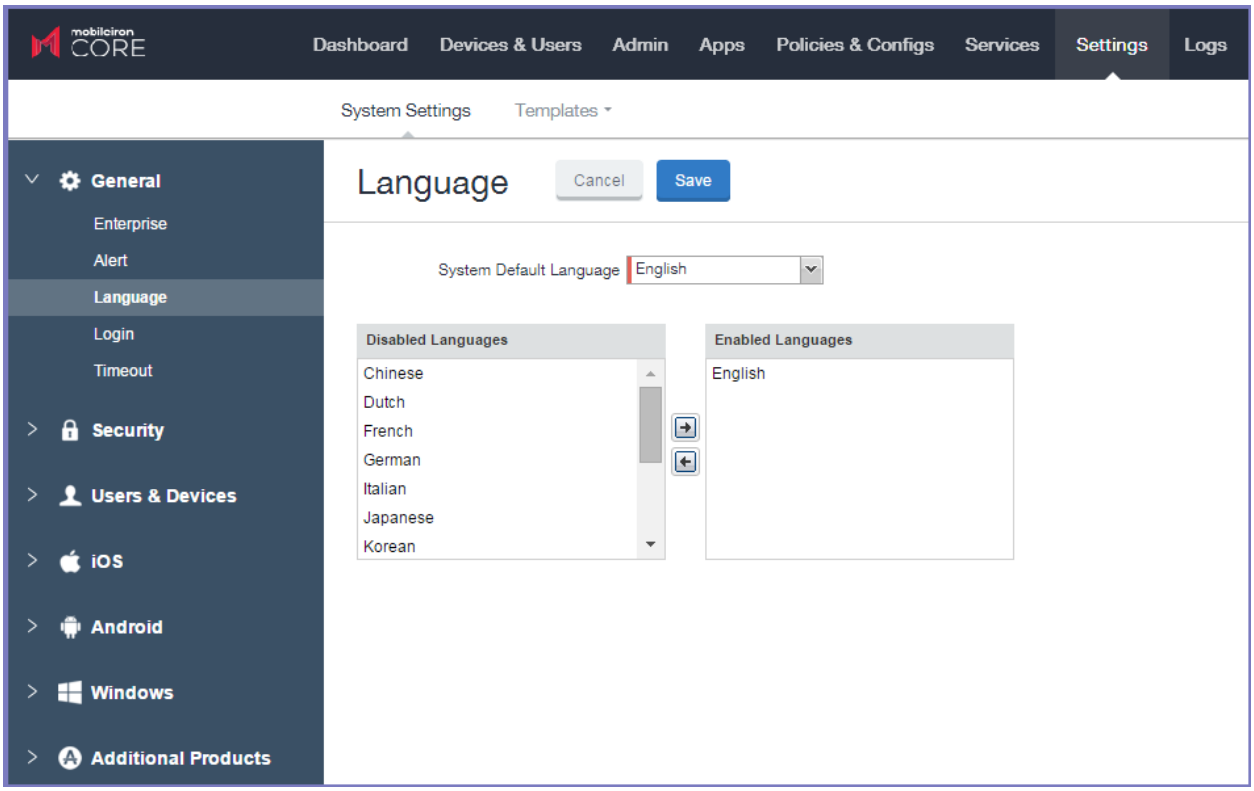


3. Move the languages you want to support from **Disabled Languages** to **Enabled Languages**.
4. Click **Save**.

Setting the system default language

The **System Default Language** setting under **Settings > System Settings > General > Language** determines the language to be used if the locale of the device cannot be determined or the corresponding language is not supported. The languages available for this setting are determined by the languages in the **Enabled Languages** list.

This language setting applies to the messages sent from MobileIron Core.



Changing language selection from the Admin Portal

Administrators can manually change the language selection for devices that do not report their locale. In this case, language selection applies only to the messages sent from MobileIron Core (e.g., Event Center alerts). If the device later reports a different locale, then MobileIron Core honors the reported locale.

To change the language selection for a specific device:

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Select the check box next to the device.
3. Click **Actions > Change Language**.
   The **Change Language** dialog appears.
4. From the **Set Language** drop-down, select the preferred language.
5. Click **Change Language**.

Samsung Android Kiosk Support

About Samsung Android kiosk

The Samsung Android kiosk feature enables you to configure supported Samsung Android devices to use only specified apps. Samsung Android kiosk mode is intended for devices that serve very specific functions for an organization.

Examples include:

- A retail store might want to use tablets to provide one or two custom apps for customers to use while shopping.
- A school might want to distribute tablets that present only appropriate apps for the user who signs in.

NOTE: Though the Samsung Android kiosk feature allows multiple users to log in on a given device, it does not represent full multi-user support. It is intended as a view filter for apps. The profiles on the device do not change when different users log in. Instead, a custom list of apps displays based on the current user.

The kiosk feature has two modes of operation:

- single-app mode, where only one app is allowed to run on the device
- multiple-app mode, where multiple designated apps are allowed to run on the device

NOTE: AppConnect apps are supported only in multiple-app mode. They are not supported in single-app mode. Multiple-app mode support with AppConnect apps is not available prior to Mobile@Work 9.1 for Android.

Requirements

- Samsung Android kiosk mode is available on Samsung KNOX devices.

Setting up Samsung Android kiosk mode

To set up a Samsung Android kiosk device for single-app mode:

- Create an Android kiosk policy.

To set up a Samsung Android kiosk device in multiple-app mode:

1. Create an Android kiosk policy.
2. Create one Android kiosk configuration for each combination of LDAP group and accessible apps.

Device users must belong to the designated LDAP groups.

The policy specifies the kiosk type. The configuration specifies which apps to display to which users in multiple-app mode.

The following instructions assume that the apps are already installed on the devices. If an app specified in the kiosk setup is not installed on the device, that app is represented by a blank icon.

Finding the package name for an Android app

For public apps available on the Google Play store:

1. Use a web browser to locate the app in Google Play.
2. Select the app.
3. Examine the URL displayed in the browser.

FIGURE 14. FINDING THE PACKAGE NAME FOR AN ANDROID APP

The package name is included in the URL, as shown in Finding the package name for an Android app.

For in-house apps:

1. Open the .apk as a zip file.
2. Use a text editor to open AndroidManifest.xml.
3. Locate the “package manifest” entry.
   This entry is set to the package name.

Samsung Android kiosk policy

The Samsung Android kiosk policy defines the behavior of a kiosk device, determining if the kiosk mode is for a single app or for multiple apps.

NOTE: Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.

Setting up a single-app kiosk policy

A single-app kiosk policy specifies one app for use on the designated devices. For example, if the device is intended to run an in-house app for staff in a hospital recovery room, you can define a single-app kiosk policy to prevent users from accessing other apps and device resources on that device.

Procedure

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Samsung Kiosk**. The New Android Kiosk Policy dialog box opens. **Single App** is selected by default.
3. Use Samsung Android kiosk policy to complete remaining options.
4. Click **Save**.
5. Assign the policy to the appropriate label to push it to the target devices.

Single-app kiosk policy

See the following table for a description of the fields in a single-app kiosk policy.

TABLE 73. SAMSUNG KIOSK SINGLE APP POLICY

Item	Description
Single App package name	Enter the package name for the app. The typical package name has the following format: com.company.app Important: Do not add the Mobile@Work package name here. The device must already have Mobile@Work installed and be registered with MobileIron Core when it receives the kiosk policy.
Enable Android functions	
System bar	System bars are screen areas dedicated to navigation and the display of notifications and status. Clear this option if you want to hide the system bar when the device is acting as a single-app kiosk.

TABLE 73. SAMSUNG KIOSK SINGLE APP POLICY (CONT.)

Item	Description
Task manager	The task manager enables device users to open an app that is currently running on the device. Select this option if you want device users to be able to access the built-in task manager on the device.
Notification bar expansion	The notification bar typically displays at the top of the device. Swiping down expands the bar to the full size of the screen so that the device user can see notification details. Select this option if you want device users to be able to expand the notification bar.
Navigation bar	For Android 4.0, the navigation bar is present only on devices that don't have the traditional hardware keys. It contains the Back, Home, and Recents controls. Select this option to allow device users to access the navigation bar. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Status bar	The status bar displays pending notifications, and status such as time, battery level, or signal strength. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Share via	When “Share via” is enabled, the user can share data from apps that offer data sharing. Select this option to allow data sharing.

Setting up a multiple-apps kiosk policy

A multiple-app kiosk policy specifies behavior for a device that will run multiple apps. You must also define at least one Android kiosk configuration to specify the permitted apps.

The multiple-app Kiosk Policy provides these additional options:

- multiple user login support
- inactivity logout interval
- administrative access to exit kiosk mode
- branding options for the kiosk launcher/desktop

To specify a multiple-app kiosk policy:

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Samsung Kiosk.** The New Android Kiosk Policy dialog box opens.
3. In the Android (Samsung Safe) section select the **Multiple Apps** radio button.
4. Use Samsung Android kiosk policy to complete the remaining options.

5. Click **Save**.
6. Assign the policy to the appropriate label to push it to the target devices.
7. Create an Android kiosk configuration to specify the apps to be used.

Multiple-apps kiosk policy

See the following table for a description of the fields in a multi-app kiosk policy.

TABLE 74. MULTIPLE-APPS KIOSK POLICY

Item	Description
Kiosk multi-user login	Enable this option to allow different users to log in. Device users enter their MobileIron credentials to access the kiosk. The credentials entered determine who is recorded as the current user, the apps to display, and whether that user has permission to exit kiosk mode from the device. Note: The credentials entered do not affect the profiles installed on the device.
Inactivity logout	Select the duration of inactivity after which the user will be signed out. This option applies to multiple-user kiosks only.
Administrative access to exit Kiosk mode	If you want to specify users who have permission to disable kiosk mode from the device, specify the corresponding LDAP groups for those users. You can choose from the LDAP groups that you specified in **Services > LDAP** for each LDAP server.
Branding	
Background Color	Enter the hexadecimal triplet for the color you want to apply to the kiosk display background.
Banner Color	Enter the hexadecimal triplet for the color you want to apply to the banner at the top of the kiosk display.
Banner Text Color	Enter the hexadecimal triplet for the color you want to apply to the text in the banner at the top of the kiosk display.
Banner Text	Enter the text you want to display in the banner at the top of the kiosk display.
Banner Logo	Click **Browse** to select a logo. The logo must be a JPEG or PNG graphic. Image pixel size: Image sizes vary for different devices. For most smaller screened devices, 120x120 pixels is appropriate. For most tablets or larger screens, 180x180 pixels is appropriate . Image file size: must be smaller than 100 KB.

TABLE 74. MULTIPLE-APPS KIOSK POLICY (CONT.)

Item	Description
Enable Android functions	
System bar	System bars are screen areas dedicated to navigation and the display of notifications and status. Clear this option to hide the system bar.
Task manager	The task manager enables device users to open an app that is currently running on the device. Select this option if you want device users to be able to access the built-in task manager on the device.
Notification bar expansion	The notification bar typically displays at the top of the device. Swiping down expands the bar to the full size of the screen so that the device user can see notification details. Select this option if you want device users to be able to expand the notification bar.
Multi Window	Multi window is a Samsung feature that enables users to multitask by viewing two apps at the same time. Select this option to allow the multi window feature.
Navigation bar	For Android 4.0, the navigation bar is present only on devices that don't have the traditional hardware keys. It contains the Back, Home, and Recents controls. Select this option to allow device users to access the navigation bar. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Status bar	The status bar displays pending notifications, and status such as time, battery level, or signal strength. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Share via	When “Share via” is enabled, the user can share data from apps that offer data sharing. Select this option to allow data sharing.

Creating a Samsung Android kiosk configuration for multiple-app mode

The Samsung Android kiosk configuration has the following functions:

- specifies the apps to be displayed for multiple-app devices
- specifies which LDAP groups, (and, therefore, which users) have access to those apps

You can apply more than one kiosk configuration to a single device. The union of the configurations determines which apps to display.

NOTE: The LDAP group access specified in the configuration would effectively disable the specified apps on a single-app mode device.

WARNING: Do not add the Mobile@Work app to an Android Kiosk Configuration. This usage is not supported and can cause errors.

Procedure

1. Go to **Policies & Configs > Configurations.**
2. Click **Add New > Android > Samsung Kiosk**.
   The **New Android Kiosk App Setting** dialog box opens.
3. If you intend to use LDAP groups to restrict access to apps on kiosk devices, then select the LDAP groups you want to allow. You can choose from the LDAP groups that you specified in **Services > LDAP** for each LDAP server.
   These users will have access to the specified apps on kiosk devices, that is, those devices that have a kiosk policy applied.
   To enable all kiosk users to have access to all specified apps, do not select any LDAP groups.
   The available LDAP groups are based on the last sync between Core and the LDAP server. If you made a recent change to LDAP data, it will not be reflected until the next sync (scheduled or manual).
4. Select the apps you want to make accessible for kiosk devices that receive this configuration.
   Note that the name displayed is the common name for the app. The package name is the unique identifier determined by the app developer.
   Do not add the Mobile@Work app to an Android Kiosk Configuration. This usage is not supported and can cause errors.
5. Click **Save**.
6. Assign the configuration to the appropriate label to push it to the target devices. One or more kiosk configurations may be applied to a single device.

Enabling and Disabling Samsung Android kiosk mode

The first time the necessary policy and configuration are pushed to the device, a kiosk item displays in the Apps@Work screen on the device. Tap **Kiosk Mode** to initiate kiosk mode.

Afterwards, you can enable and disable Android kiosk mode from the Admin Portal. Users with assigned privileges can also disable kiosk mode on a kiosk device.

Enabling Samsung Android kiosk mode from the Admin Portal

NOTE: Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.

1. Select the device in the **Device & Users > Devices** page.
2. Click **Actions > Android Only > Enable Kiosk**.

Disabling Samsung Android kiosk mode from the Admin Portal

1. Select the device in the **Device & Users > Devices** page.
2. Click **Actions > Android Only > Disable Kiosk**.

Enabling Samsung Android kiosk mode from the device

1. Start the Mobile@Work app.
2. Tap **Kiosk Mode**.

NOTE: Kiosk Mode displays only if the kiosk policy has been configured and sent to the device.

Disabling Samsung Android kiosk mode from the device

Only users configured for administrative access in the kiosk policy can disable kiosk mode from the device. The kiosk must be configured to support multiple apps and multiple users.

Procedure

1. Log in as a kiosk administrator.
2. Tap the **Exit Kiosk** icon at the top of the screen.

An example of Samsung Android kiosk mode

NOTE: Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.

Consider a school that wants to install the followings apps on several tablets. Although all the apps are installed on each tablet, the apps that are displayed depend on which user has logged in.

An example of Samsung Android kiosk mode shows the apps and the LDAP groups that should have access to them.

TABLE 75. ANDROID KIOSK MODE EXAMPLE: LDAP GROUPS AND APPS

LDAP Groups	Apps			
	View	Update	Send 2 Parents	Send 2 Teachers
Teachers	yes	yes	yes	yes
Tutors	yes	yes		yes
Students	yes			

The following table shows one way to implement this scenario.

TABLE 76. ANDROID KIOSK MODE EXAMPLE: ANDROID CONFIGURATIONS WITH LDAP GROUPS AND APPS

Android Kiosk configurations	LDAP Groups	Apps			
		View	Update	Send 2 Parents	Send 2 Teachers
KioskTeachers	Teachers	yes	yes	yes	yes
KioskTutors	Tutors	yes	yes		yes
KioskStudents	Students	yes			

Information about Samsung Android kiosk mode in device details

The **Device Details** pane in the Admin Portal displays the following information about kiosk mode:

- whether kiosk mode has been enabled
- the device user currently logged in on the device.

To view device details:

1. Go to **Device & Users > Devices**
2. Expand device details by clicking the caret next to the check box for the device of interest.
3. Look for the kiosk attributes in the Device Details tab.

Samsung Android kiosk mode deployment notes

- Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See Setting kiosk policy for Android Managed devices.
- Samsung Android kiosk mode is a viewing filter only
  - Kiosk mode is not an app blocking feature. It only restricts the viewing of apps which can be launched.
  - Apps must be installed on the device for them to launch from the kiosk.
- Distribute apps with the silent install option enabled to ease the deployment process.
- Configuring which apps to run
  - Single app mode uses the **Android Samsung Kiosk policy** on the **Policies** page.
  - Multiple app mode uses the **Android Samsung Kiosk policy** on the **Policies** page, and one or more **Android Samsung Kiosk configurations** on the **Configurations** page.
  - Apps defined in kiosk configurations with no LDAP groups selected apply to ALL kiosk users.
  - For multiple app mode, the union of all kiosk configurations applicable for a kiosk user (based on their LDAP group membership) determines the list of apps to display, and whether or not they are allowed to bypass kiosk mode.
- If the device loses its connection to MobileIron Core, then kiosk mode cannot be disabled. You must do a factory reset.
- After a Samsung kiosk policy and Samsung kiosk configuration (for multi-app kiosk mode) have been pushed to a device, press the Home button on the device or restart the device. These actions avoid Android OS issues which leave the Android home screen available. Similarly, press the Home button or restart the device when kiosk mode is re-entered after having been exited due to administrator action or device maintenance.

Setting kiosk policy for Android Managed devices

As a Space or Global admin you can set up a policy to customize the look of the Android Kiosk as well as the apps which it contains. In addition, you can select to switch to the Kiosk mode automatically. This feature is supported on devices in Device Owner mode with Android enterprise.

1. Go to **Policies & Configs > Policies**
2. Select **Add New > Android > Android Kiosk Mode** to display the New Android Kiosk App Setting Policy dialog box.
   If a Kiosk App policy exists, the Edit Android Kiosk App Setting Policy page opens.
3. Enter a **Name** for the new policy.
4. Ensure the Status field is set to **Active**.
5. In the Kiosk Branding section, customize the kiosk with a banner, background color or background image.
6. In the Kiosk Settings section, select the appropriate check boxes for your implementation:
   - **Enable Lock Task Mode**: Enables the Lock Task Mode on the Android enterprise devices connected to Android Kiosk to increase the level of security on the user devices in kiosk mode by limiting access

to white listed kiosk and system apps. When a device user swipes away from an app, they will only have access to the white listed and system apps. This feature is supported on devices in Device Owner mode with Android enterprise. By default, this field is enabled.

- **Disable Quick Settings**: Select so that the device will not display the system notification drop-down menu at the top of the screen.
  If the following settings are enabled, the settings will be display as kiosk Settings menu items. The user can customize each of the settings for use in the kiosk.
- **Allow User to Access Wi-FI Settings**: Select to permit the device user to access Wi-Fi settings.
- **Allow User to Access Bluetooth Settings**: Select to permit the device user to access Bluetooth settings.
- **Allow User to Access Location Settings**: Select to permit the device user to access Location settings.
- **Enter Kiosk Mode Immediately**: Allows you to switch to Kiosk mode automatically after you save your settings (by clicking the **Save** button).
- **Kiosk Exit Pin**: Enter a 4 - 6 digit PIN into the field.
  If the Kiosk Exit Pin field is left blank it disables the ability to exit Kiosk mode. The user will not be able to exit Kiosk mode without a Kiosk exit pin.

7. In the **Choose Apps** section, optionally choose to
   - allow any third -party phone or camera app by manually adding the package name (ID).

     The built-in apps must be enabled in Device Owner mode. This may not be the case with all manufacturers.
   - Set the apps allowed in Kiosk Mode Allowed Apps
   - Add apps from the App Catalog Apps
   - Add apps manually by entering a Package ID in the **Manually Add Apps with Package ID** field and click **+Add**.
     After an app has been installed and is listed in the **Kiosk Mode Allowed Apps** section of the **Edit Android Kiosk App Setting Policy** page, it can be dragged up or down to change the order of appearance in the kiosk.
8. Optionally, hide an app. Select an app in the **Kiosk Mode Allowed Apps** section and click the eye icon to hide the app.

Note The Following:

- When an app is hidden it can be used by other apps, but not available to launch in the kiosk. For example, a browser can be added to the kiosk but hidden so that it can be used to open URLs from an email app.
- The Kiosk itself does not install any app. You need to install any app that you include in the kiosk using Apps@Work or other method.

The SMS Archive Feature

About the SMS & Call Log Archive feature

The optional SMS & Call Log Archive feature enables organizations to:

- address regulatory requirements for archiving inbound and outbound SMS messages and calls.
- encrypt SMS and call logs

Supported devices

- The SMS archive feature is supported for Samsung Knox devices.
- The call log archive feature is supported for all Android devices.

Setting Up the SMS & Call Log Archive feature

Complete the following steps to set up the SMS & Call Log Archive feature.

Procedure

1. In the Admin Portal, go to **Settings > System Settings.**
2. Go to **Android > SMS & Call Log Archive**.
3. Select the type of archive:
   - Email
   - Splunk
   - Store and Forward to Internal Server
   - Do not archive to turn off the feature
4. If you select **Email**, use the following guidelines to complete the settings in **Email Configuration**:

Setting	Description
Default From Address	Enter the email address to include in the From field of the emails generated for archiving the SMS and call log messages.
Destination Email Addresses	Enter the email addresses for the archival systems to which the generated emails are being sent. Separate the email addresses with commas (,).
Host/IP Addresses	Enter the host name or IP address of each SMTP server to use for relaying the email to the SMS archival destinations. You may specify the same SMTP server that you specified when you configured MobileIron Core. If you specify multiple addresses, then MobileIron attempts to connect to each in the order specified until a successful connection is established.
TLS Enabled	Select Yes if you want to enable TLS for communication with the SMTP relay server.
STARTTLS Required	If you selected Yes for the TLS Enabled option, indicate whether the STARTTLS protocol is required for the specified SMTP servers.
Check SMTP Connection	Click this option to confirm SMTP access.

- Because most archival systems are designed for archiving email (and, therefore, parsing SMTP content), the MobileIron SMS & Call Log Archive feature can forward SMS content and other data via email. MMS data is not captured as part of this feature.

5. If you select **Splunk Forwarder**, make sure that Splunk Forwarder is configured in System Manager (see MobileIron Core System Manager Guide for details).
6. If you select **Store and Forward to Internal Server**, use the following guidelines to complete the settings in **Server Configuration**:

Setting	Description
Forward using	Select either SFTP or SCP as the protocol
Host/IP	Host name or IP address of the server (required)
Port Number	22 (default port number on the server)
Username	Username of user associated with the server
Password	Password for user specified in Username
Confirm Password	Enter the password again to confirm
Server Path	Path to the server
Check Server Connection	Click to test the connection to the specified server

7. If you requested encryption of the logs, click **Upload Encryption Certificate** to upload the certificate.
8. In **Archive Settings**, enter the number of hours that MobileIron Core should wait before forwarding collected messages to their archival destinations. The default value is 4.
9. (Optional) Click **Send Now** to immediately archive all currently collected messages.
10. Click **Save**.

Setting up encrypted SMS and call log archive encryption

MobileIron privacy policies specify whether SMS and call log content is encrypted. These policies impact whether SMS and call log content is archived as well.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Locate and select the privacy policy intended for supporting SMS and call log archive devices.
3. Click **Edit**. The Modify Privacy Policy dialog box opens.
4. Set the **SMS Log** option to:
   - **Sync Content- Clear Text** to specify the logs are not to be encrypted
   - **Sync Content - Encrypted** to specify the logs are to be encrypted
   - None to stop archiving SMS messages.
5. Set the **Call Log** option to:
   - **Sync Content - Clear Text** to specify the logs are not to be encrypted
   - **Sync Content - Encrypted** to specify the logs are to be encrypted
   - None to stop archiving SMS messages.
6. Click **Save**.
7. If the policy has not already been applied to the SMS or call log archive devices, apply the policy to the proper labels (click **Actions > Apply To Label**).

Monitoring the SMS & Call Log archive

You can monitor:

- the number of messages queued for delivery
- the health of the SMS & Call Log Archive feature using Events

Overriding the SMS and call log delivery interval

When you set up the SMS & Call Log Archive feature, you specify the **SMS Delivery Interval,** which determines how often MobileIron Core forwards the collected messages to the archival destinations.

Procedure

1. Go to **Settings > System Settings > Android > SMS & Call Log Archive**.
2. Click **Send Now**.

   NOTE: Note that **Send Now** is enabled only if there are queued SMS or call log messages.

Checking the number of delivered SMS and call log messages

MobileIron keeps a perpetual count of the SMS and call log messages delivered to archival destinations.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select and open the privacy policy that supports the SMS & Call Log Archive feature.
   The details for the policy are displayed to the right of the policy list.
3. Note the number of messages listed in **Call Logs** and **SMS Logs** at the bottom of the section.

Event Center options

The following Event Center options are available to help manage the health of the SMS Archive feature:

- SMTP Relay server is unreachable
- SMTP Relay server error
- SMS Message archive queue is full

See System event settings on page 316 for information on these events.

Self-service User Portal

This section addresses device registration and its related components.

- Device management with the user portal
- Assigning user portal device management roles
- Requiring user portal password change
- Configuring help desk contact information
- User portal information for your users

User portal overview

This section addresses the settings an administrator can make to allow device users to manage their own devices

- Benefits of the user portal
- Impacts of using the user portal
- User portal authentication options
- About registering devices in the user portal
- About changing device ownership in the user portal
- About uploading certificates in the user portal
- About generating a one-time PIN for resetting a secure apps passcode
- About getting Entrust derived credentials

The user portal allows your users to:

- access MobileIron device management actions such as wipe and lock
- view details of their registered devices
- register devices, which includes requesting device registration PINs and requesting derived credentials
- reset the user PIN
- change device ownership from company-owned to user-owned or the reverse
- upload, as well as view, replace, and delete user-provided certificates
  These certificates are used, for example, for S/MIME or for authenticating to internal servers.
- generate a one-time PIN for resetting a forgotten secure apps passcode

One of your decisions when you distribute MobileIron Core management is whether or not to enable your users to manage one or more device actions such as locking or unlocking a device. Your users access the actions you assign them through the user portal.

To enable users to manage their devices, you assign them roles to perform any or all of the following actions:

- wipe their device
- lock their device
- unlock their device
- locate their device
- retire their device
- register their device
- change device ownership
- reset their secure apps passcode

NOTE: The **Device Registration** role replaces the **MyPhone@Work Registration** role. The **MyPhone@Work Registration** role is removed. The old user portal, MyPhone@Work, was available only through Core 8.0.1.

Benefits of the user portal

Giving users the ability to perform device management tasks:

- distributes mobile device management
- gives your users more control of their devices
- adds efficiency to device registration by saving administrators' time as well as wait time that device users might experience

Impacts of using the user portal

When you enable users to manage their own devices, you need to:

- define which users have access to which device management actions
- provide your users with the information they need to use the user portal
- consider how changing device ownership from company-owned to employee-owned or vice-versa may impact:
  - the policies and configurations that are applied to the device.
  - the apps that are available through Apps@Work.
  - iBooks that are available on the device.

    Devices are impacted when they check-in with MobileIron depending on the labels to which company-owned or employee-owned devices are applied.

User portal authentication options

You can allow device users to authenticate to the user portal with:

- a user name and password
  These are the credentials a device user uses to register a device with MobileIron Core.
- an identity certificate from a smart card
  This authentication method is supported only on desktop computers. It is not supported with:
- mobile devices
- Firefox

You can allow one or both of these authentication mechanisms. You make your selection in the MobileIron Core System Manager.

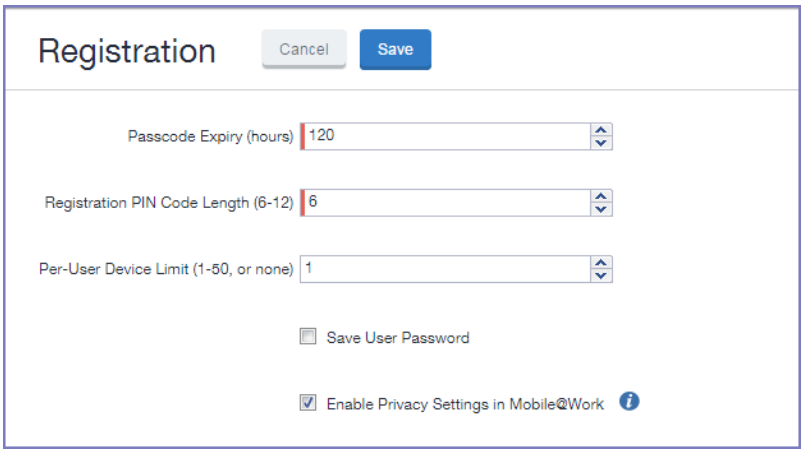
For information about how to configure the user portal authentication options, see “Advanced: Portal authentication” in the *MobileIron Core System Manager Guide.*

About registering devices in the user portal

To allow device users to register devices in the user portal, you must assign those users the **Device Registration** role in the Admin Portal in **Devices & Users > Users**.

Device limit

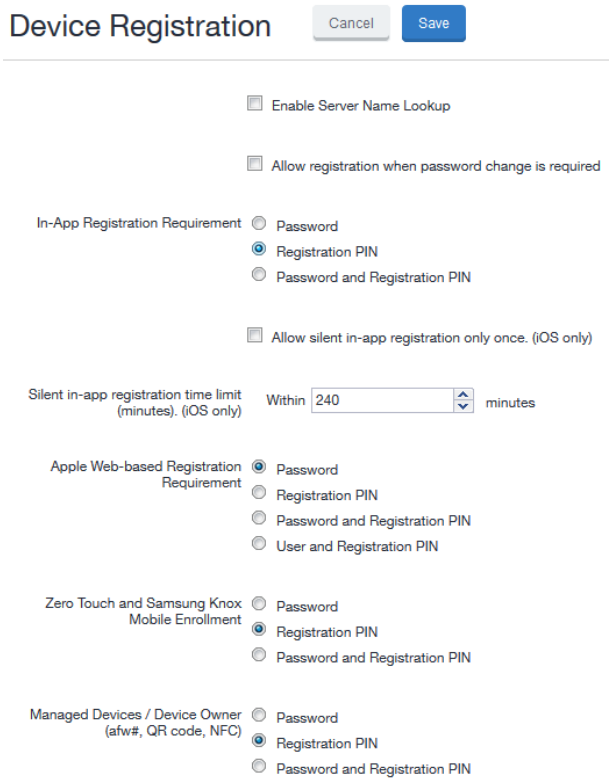
Users will be limited to register only the number of devices specified in **Settings > System Settings > Users & Devices > Registration > Per-User Device Limit.**



Registration PIN

Users who can register devices can also request and receive device registration PINs. To allow users to request a registration PIN, PIN-based registration must be selected in **Settings > System Settings > Users & Devices >**

Device Registration. Any option that includes Registration PIN will enable device users to obtain a PIN in the user portal.



Note the following about registration PIN:

- Even though a PIN is generated, device users will not be prompted to enter a PIN if the device platform does not require PIN for registration.

Password and Registration PIN

Users who can register devices can also request and receive device passwords and registration PINs. To allow managed Android device users to request a password and registration PIN, the **Password and Registration PIN** radio buttons for Zero Touch and Samsung Knox Mobile Enrollment OR Managed Devices / Device Owner (afw#, QR code, NFC) fields must be selected in **Settings > System Settings > Users & Devices > Device Registration**.

About changing device ownership in the user portal

To allow device users to change device ownership through the user portal, you must assign those users the **Change Device Ownership** role in the Admin Portal in **Devices & Users > Users**.

Users cannot assign ownership of a device during device registration in the user portal. Device ownership is automatically set to company-owned. Once users have registered their devices through the user portal, they can change the ownership of the device from company-owned to user-owned or the reverse.

About uploading certificates in the user portal

On a desktop computer, device users can upload their own certificates in the user portal. They can use these certificates for different purposes, such as:

- S/MIME signing
- S/MIME encryption
- Authenticating to servers, such as internal servers that support apps.

The device users can upload multiple PKCS 12 files, each of which contains a certificate and one private key. MobileIron Core does not support PKCS 12 files which contain more than one private key.

NOTE: This capability is available in the user portal on desktop computers, but not on mobile devices.

Associating a certificate with a user-provided certificate enrollment setting

When the user uploads a certificate, the user chooses a configuration to associate with the certificate. The configuration refers to a user-provided certificate enrollment setting that you configured. When you configure a user-provided certificate enrollment setting, you specify a display name. The user portal presents the display name in its list of configurations for the user to choose.

For example, you might create a user-provided certificate enrollment setting for S/MIME signing, another for S/MIME encryption, and another for server authentication. Each setting has a display name:

- S/MIME signing
- S/MIME encryption
- Authentication

When the user uploads a certificate, they see these display names as configurations, and they choose the one for the certificate. The user can upload the same certificate or different certificates for each configuration.

If you have not created at least one user-provided certificate enrollment setting, the user portal disables the option for the user to upload a certificate.

See also:

- Certificate Enrollment settings on page 271.

About generating a one-time PIN for resetting a secure apps passcode

On the AppConnect global policy, you can configure MobileIron Core to allow Android device users to reset their secure apps (AppConnect) passcode when they forget it. When you have configured this option, device users who registered with Core using a user name and *password* can enter those credentials in the Secure Apps Manager to authenticate themselves and then reset their secure apps passcode. However, device users who registered with Core using a *registration PIN* need a different mechanism for authenticating themselves.

This mechanism involves these steps:

1. The user generates a one-time PIN on the user portal. The one-time PIN is valid for 24 hours.
2. In the Secure Apps Manager on a device, the user follows the instructions for resetting a forgotten secure apps passcode.
3. When prompted for his user credentials, the user enters his user name and the one-time PIN.
4. The user resets his secure apps passcode.

Configuration requirements to allow the user portal to generate a one-time PIN

The user portal displays the option to generate a one-time PIN only if you have configured all of the following in the Admin Portal:

- The user portal role that allows the user to reset their secure apps passcode
- A license for AppConnect third-party and in-house apps, Docs@Work, or Web@Work
- An AppConnect global policy for the device that allows users to recover their AppConnect passcodes.

Configuring the user portal to generate a one-time PIN

Configure the following in the Admin Portal to allow the user portal to generate a one-time PIN:

1. In **Devices & Users > Users**, select the user.
2. Select **Actions > Assign Roles.**
3. In the Assign Role(s) dialog box, select **Reset Secure Apps Passcode**.
4. Click **Save**.
5. In **Settings > System Settings > Additional Products > Licensed Products**, select at least one of the following:
   - **AppConnect for Third-party and In-house Apps**
   - **Docs@Work**
   - **Web@Work**
6. In **Policies & Configurations > Policies**, select the AppConnect global policy for the device.
7. In the Policy Details panel, click Edit. The Modify AppConnect Global Policy dialog box opens
8. In the **AppConnect passcode** section, select **Passcode is required for Android devices**.

9. Select **Allow Android users to recover their passcode**.
10. Click **Save**.

About getting Entrust derived credentials

When using certificate authentication to the user portal, you can set up MobileIron Core so that Android users can get their Entrust derived credentials when they get their Core registration PIN. Specifically, in the System Manager, you provide Core with the Entrust IdentityGuard Self-Service Module (SSM) URL. This URL is a deep link that points directly to the page on the Entrust self-service portal where a user can get a derived credential.

When the user requests a derived credential on the user portal, the user portal redirects the user to the URL you provided. The user interacts with the Entrust self-service portal to get a derived credential, after which the Entrust self-service portal redirects the user back to the MobileIron Core user portal. The user uses the PIV-D Entrust app on a device to activate the derived credential.

For information about how to enable the user to get a derived credential on the user portal, see “Advanced: Portal authentication” in the *MobileIron Core System Manager Guide.*

Device management with the user portal

This section addresses the settings your users need to use the user portal.

- Logging in to the user portal with user name and password
- Logging in to the user portal on a desktop computer with a certificate
- What users see after they login
- Uploading certificates in the user portal on a desktop computer
- Viewing, replacing, and deleting certificates in the user portal
- When a user-provided certificate is deleted

Assigning user portal device management roles

The MobileIron Core user portal provides several device management options for your users. You give them access to these management tasks by assigning them roles in the Admin Portal.

Procedure

1. In Admin Portal, go to **Devices & Users**.
2. Select the users receiving device management privileges.
3. From **Actions**, select **Assign Roles**.
4. Check **User Portal**.

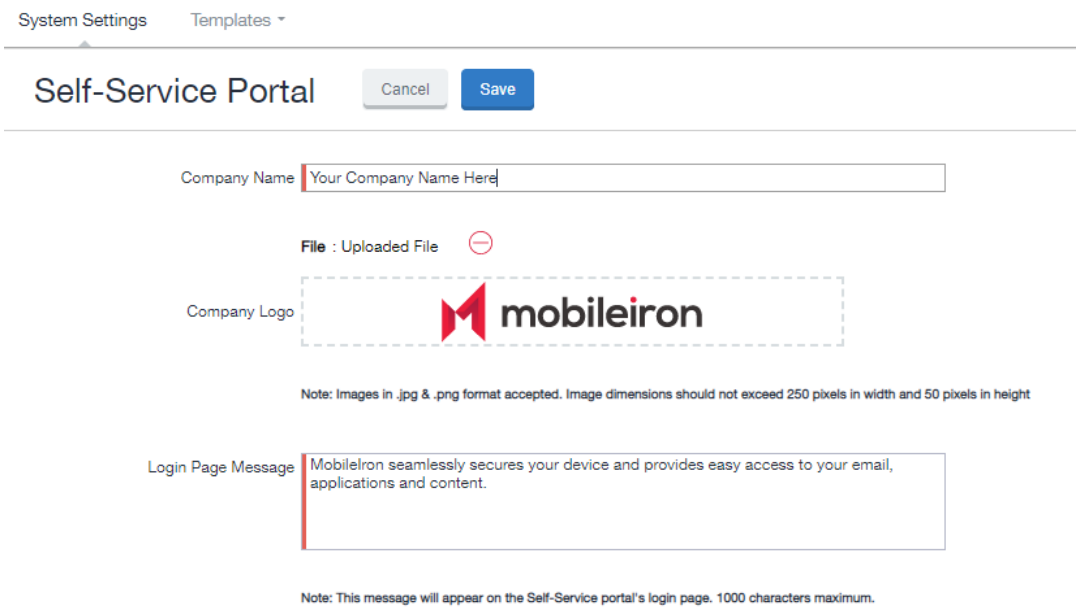
5. Check one or more roles to assign the corresponding management actions to the selected users.
6. User roles include:
   - Wipe Device
   - Lock Device
   - Unlock Device
   - Locate Device
   - Retire Device
   - Register Device
   - Change Device Ownership
   - Reset PIN
   - Reset Secure Apps Passcode
   - Use Google Device Account (For Android enterprise device only)
7. Click **Save**.

Customizing the Mobile@Work self-service user portal

Beginning with MobileIron Core release 10.6.0.0, you can customize the logo, text, and company name for your Mobile@Work self-service user portal.

Procedure

1. From the Admin portal, navigate to **Settings > System Settings > General > Self-Service Portal**. The Self-Service Portal page displays.



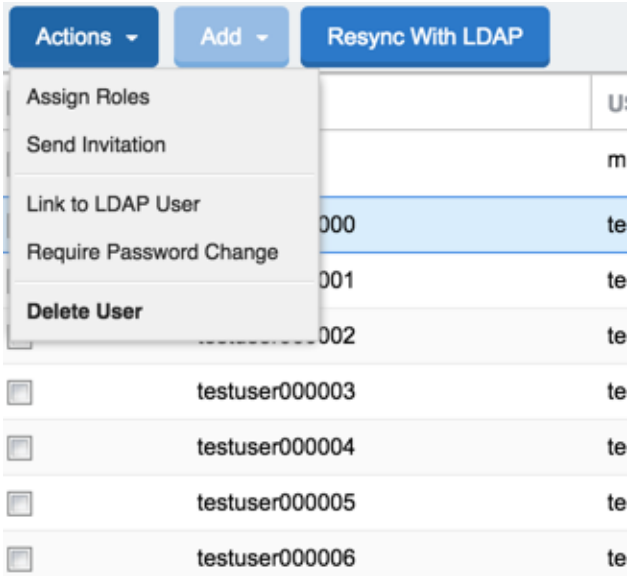
2. **Company Name**: Enter a customized company name.
3. **Company Logo**: Upload a customized company logo. Images can be JPG or PNG format, and must not exceed 250 by 50 pixels.
4. **Login Page Message**: Modify or replace the existing message that displays on the Self-Service Portal's log in page, up to 1,000 characters.
5. Click **Save**. A confirmation message displays.
   Modify the following URL to see the new custom portal page on Core:
6. Verify the new custom portal page on Core by substituting your Core hostname and SSP user name:
   https://<*hostname*>/mifs/<*user*>

Requiring user portal password change

You can require local users to change their user portal password the next time the device checks in with MobileIron Core. This feature is not available for LDAP users.

To require a local user to change their user portal password:

1. In Admin Portal, go to **Devices & Users**.
2. Click **Users**.
3. Select one or more local users you want to change their user portal passwords the next time they check in with Core.
4. Click **Actions**.



5. Select **Require Password Change**.
   Core prompts you to confirm the requirement.
6. Click **Yes** to require the selected users to create a new password at the next check in.

Limiting devices per user by LDAP group membership

You can limit the number of allowed devices per user, using LDAP group membership as the conditional limiter. You can:

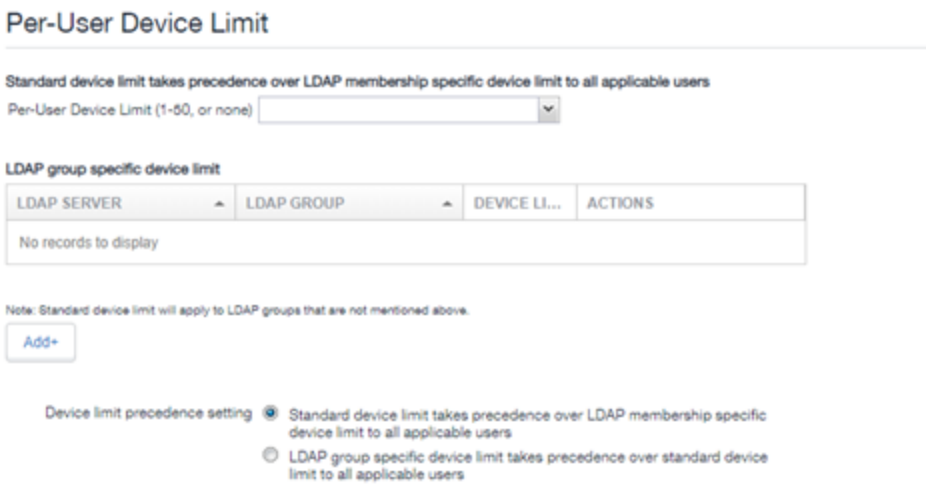
- Select a global device limit of 0-50 devices per user
- Add LDAP user groups to the LDAP group-specific device limit table
- Edit LDAP user groups
- Delete LDAP user groups from the device limit table
- Set the device limit precedence setting: you can choose whether the standard device limit takes precedence over LDAP membership-specific device limits, or LDAP group-specific device limits take precedence over the standard device limit (for all applicable users)
  For example, you could set a global device limit of four devices, but restrict members of specific LDAP groups to one or two devices.

Before you begin

You must have previously configured an LDAP server to support LDAP groups before you can set per-user device limits.

Procedure

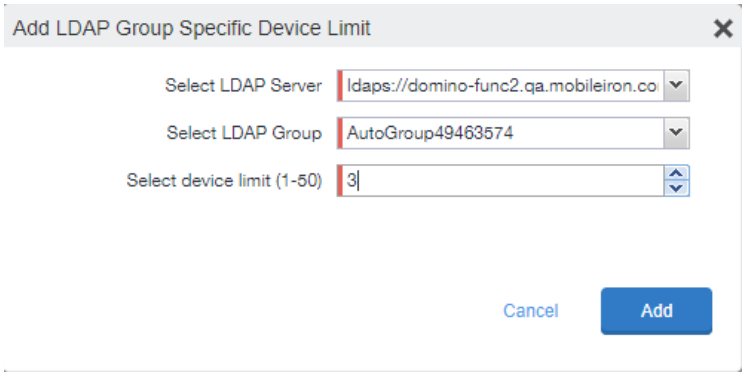
1. From the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration** page
2. In the **Per-User Device Limit** section, enter the following information:



3. **Per-User Device Limit (1-50, or none)**: Set the default number of devices each user can register with Core. This is the "standard" device limit, that by default takes precedence over LDAP membership-specific device limits.You can change this priority by selecting a device limit precedence setting (step 5).

4. **LDAP group specific device limit**: This setting allows you to create LDAP group-specific device limits that vary from the default device limit you set as the per-user device limit.

   a. From below the LDAP group table, click **Add+**. The Add LDAP Group Specific Device Limit dialog opens.



   b. Select a configurable LDAP server from the **Select LDAP Server** drop-down.

   c. Select a group from the **LDAP Group** drop-down.

d. Select the device limit (1-50) from the **Select device limit** field.

e. Click **Add**.

5. Select a device limit precedence setting:

   a. Standard device limit takes precedence over LDAP membership-specific device limit for all applicable users.

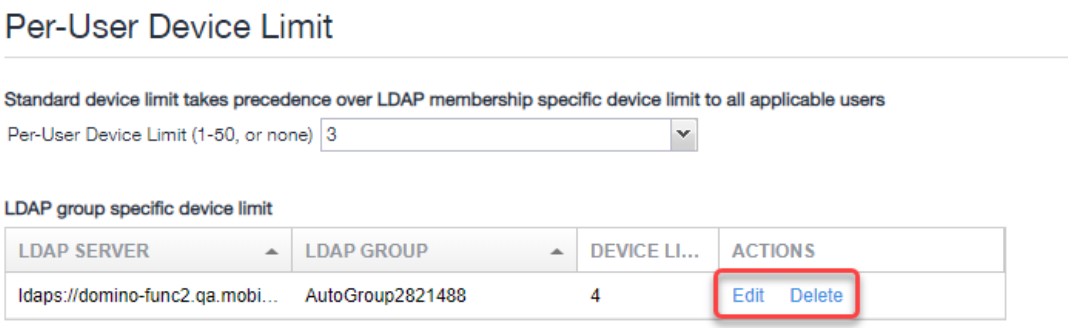
   b. LDAP group-specific device limit takes precedence over standard device limit for all applicable users.

Editing or Deleting an LDAP group-specific device limit

You can modify or delete your LDAP group-specific device limits from the LDAP group-specific device limit table.

Procedure

1. Locate the LDAP group that you want to edit or delete in the LDAP group-specific device limit table.



2. Click **Edit** to re-open the Add LDAP Group Specific Device Limit dialog.
3. Click **Delete** to delete the LDAP group-specific device limit.

Configuring help desk contact information

MobileIron Core administrators with **Manage settings and services** permission can configure the help desk contact information to display in the self-service user portal.

Procedure

1. In the MobileIron Core Admin Portal, go to **Settings > General > Helpdesk**.
2. Enter the following information:

Item	Description
Name	Enter a name for the configuration.
Description	Enter a brief description for the configuration. Maximum characters allowed is 100.
Contact(s)	Enter one or more phone numbers. If you are entering multiple phone numbers, enter a comma-separated list.
Email(s)	Enter one or more email addresses. If you are entering multiple email addresses, enter a comma-separated list.

NOTE: Either a phone number or an email address is required.

Related topics

Viewing the help desk contact information.

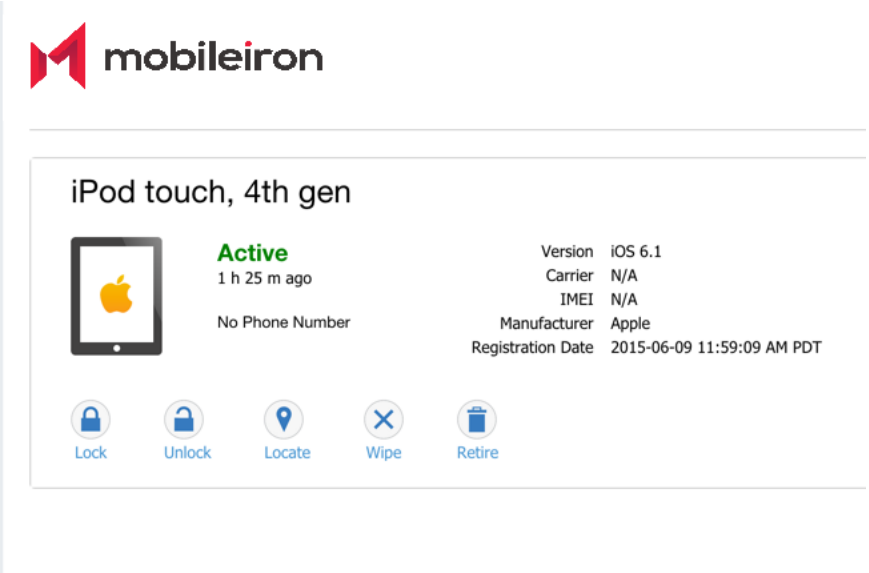
User portal information for your users

This section presents the information that your users need to use the user portal.

The user portal displays:

- Icons for each device management action the user is allowed to perform.
- User and device information, including:
  - device type (iPod touch, 4th gen in the example)
  - status (Active, for example)
  - last check-in (example, 2 hours ago)
  - phone number
  - OS and version (to 3 digits, iOS 7.1.1, for example)
  - carrier (for example, AT&T)
  - IMEI value, if applicable
  - manufacturer
  - date the device was registered with MobileIron
- Accounts settings and certificates uploaded by the device user.
- Helpdesk contact information configured by the MobileIron Core administrator.

FIGURE 15. USER PORTAL SHOWING USER'S DEVICE INFORMATION



Logging in to the user portal with user name and password

Device users can log in to the user portal to register and manage their devices.

Procedure

1. Go to https://<*MobileIron server*>, where <*MobileIron server*> is the address of your MobileIron server. Contact your administrator if you do not have this address.
2. If you are not logged in, provide your user name and password, when prompted, and then select **Sign In with Password**.
   The user portal displays on your device. You can:
   - click the icon for one of the available device management actions available to you.
   - view your device information.

Logging in to the user portal on a desktop computer with a certificate

If set up by the MobileIron Core administrator, device users can log in to the user portal on a desktop computer using an identity certificate on a smart card.

Procedure

1. Attach your smart card reader with your smart card to a USB port on the desktop computer.
   If your computer has a built-in smart card reader, insert your smart card.
2. Go to https://<*MobileIron server*>, where <*MobileIron server*> is the address of your MobileIron server. Contact your administrator if you do not have this address.

3. If you are not logged in, select **Sign In with Certificate**.
   A prompt appears to select your certificate
4. Select the certificate from the smart card.
5. If prompted, enter the password of the private key of the identity certificate on your smart card.
   The user portal displays. You can:
   - select the icon for one of the available device management actions available to you.
   - view your device information.

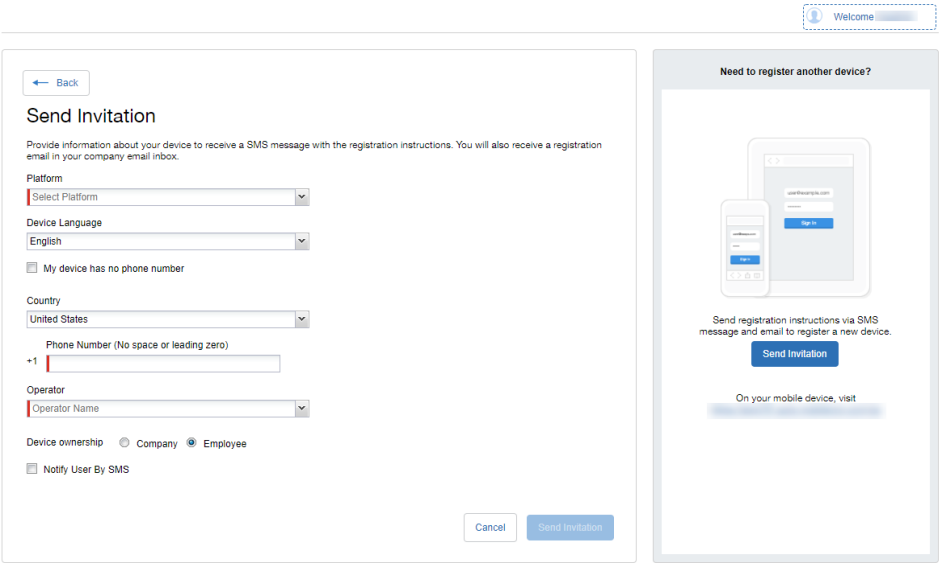
What users see after they login

Depending on the user portal role enabled, device users may have a different view of the user portal.

If Register Device role is enabled

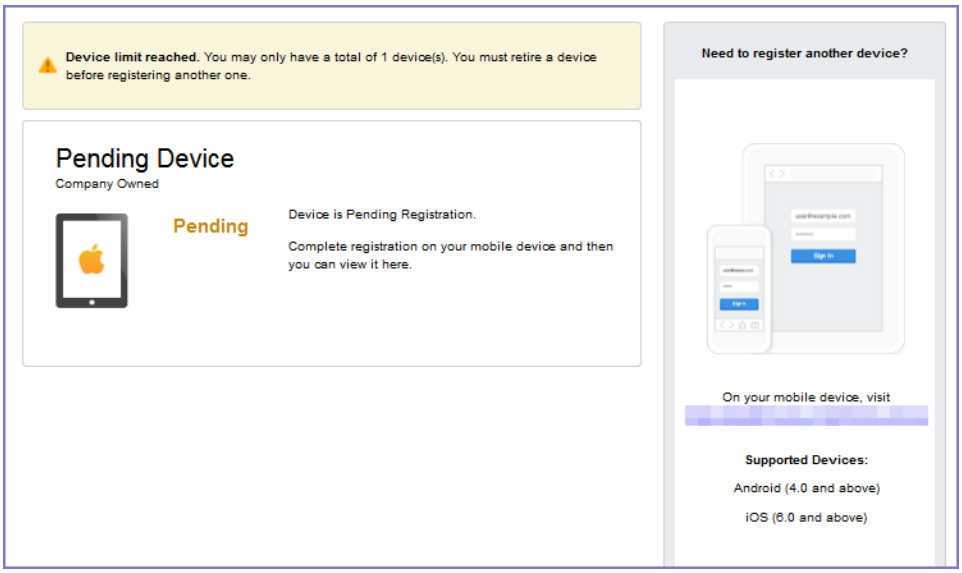
If the **Register Device** role is enabled, device users will be able to send an invitation from the user portal to register their device.

FIGURE 16. SEND INVITATION TO REGISTER



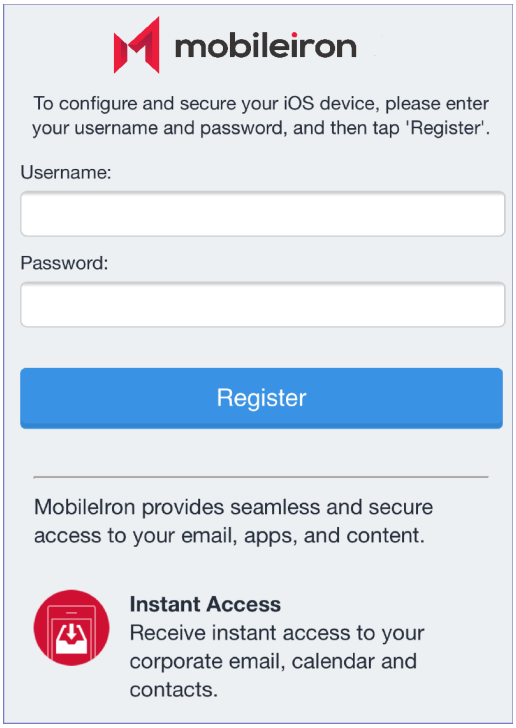
After the invitation is sent, the device status is seen as **Pending**.

FIGURE 17. REGISTRATION PENDING FOR DEVICE



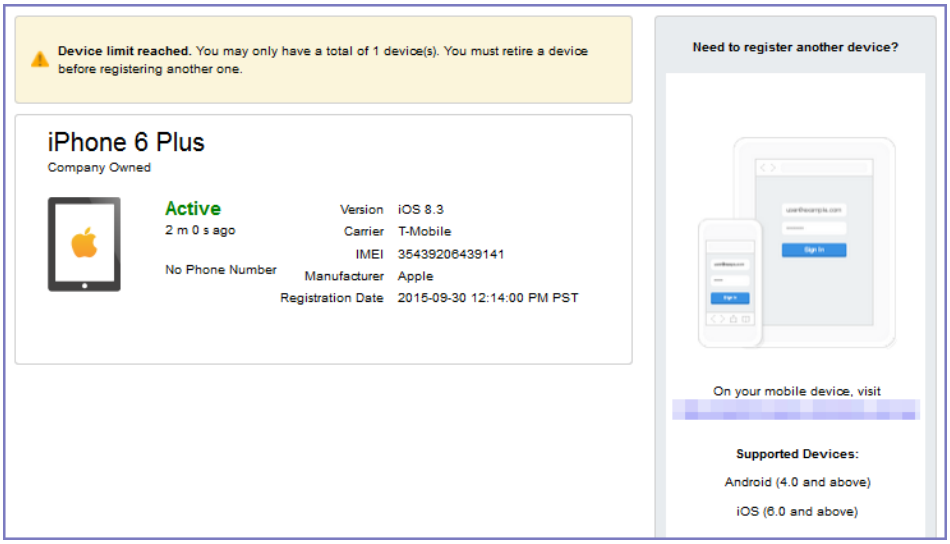
Device users can complete the registration on their mobile device at https://<*Core_Server_FQDN*>/go.

FIGURE 18. COMPLETE DEVICE REGISTRATION



After registration is completed on the mobile device, the status for the device is changed to **Active**.

FIGURE 19. ACTIVE DEVICE STATUS



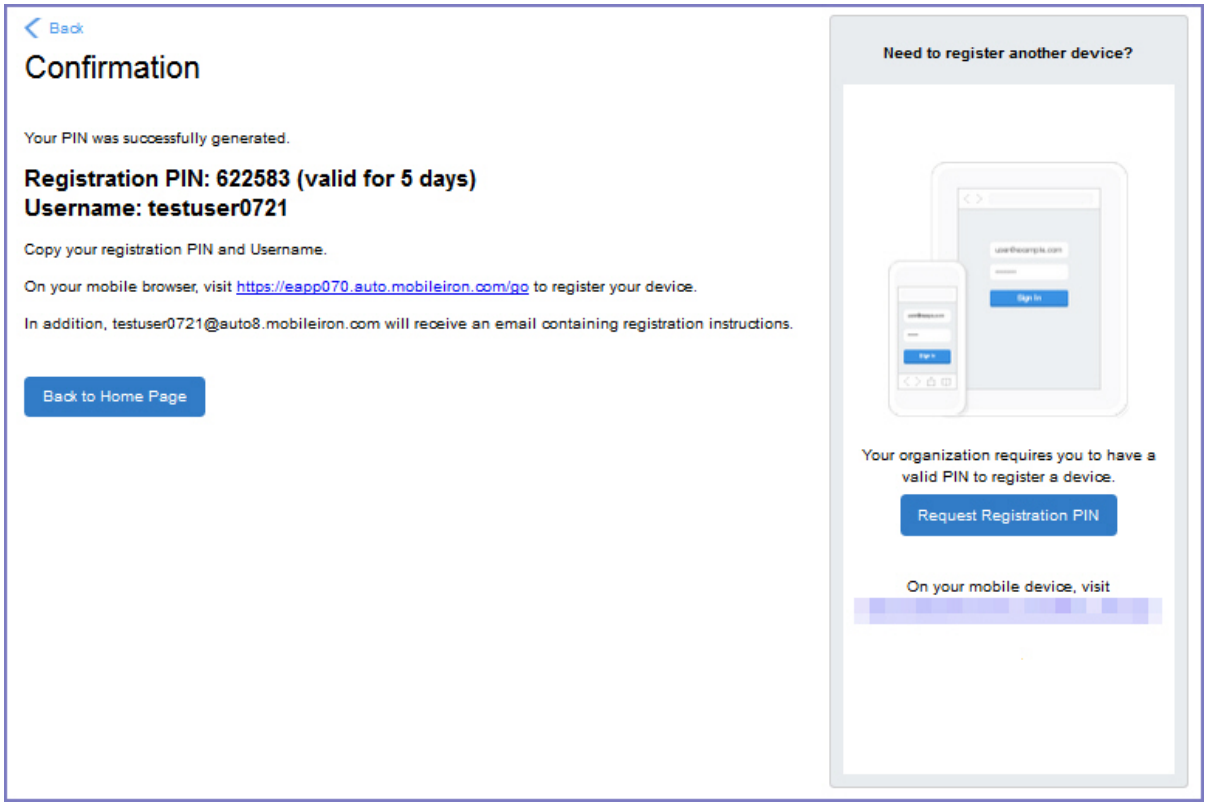
Registration instructions

On Android devices, users can follow the prompts to download Mobile@Work and complete the registration.

If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see **Request Registration PIN**. Clicking on **Request Registration PIN** allows device users to send an invitation for registration as well as generate a PIN.

FIGURE 20. REGISTRATION WITH PIN

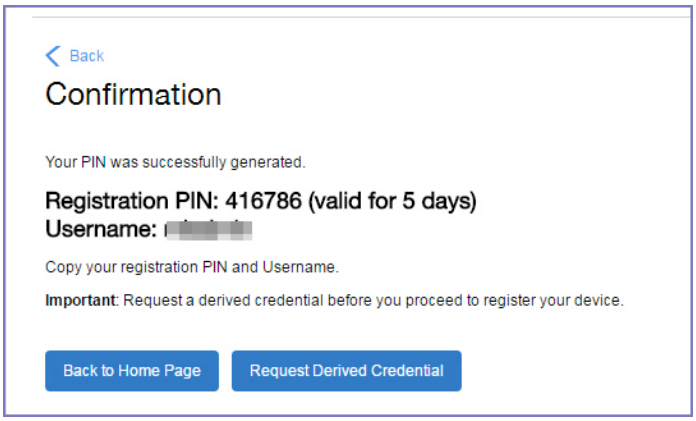


Device users can complete the registration on their mobile device at https://<*Core_Server_FQDN*>/go. They will have to enter the PIN if prompted.

If getting an Entrust derived credential is enabled

If you enabled getting an Entrust derived credential in the System Manager, device users will see **Request Derived Credential** when they receive their registration PIN for a device. Before using the registration PIN to register Mobile@Work to MobileIron Core, the device user should request a derived credential.

FIGURE 21. REQUEST DERIVED CREDENTIALS



To get a derived credential:

1. Click **Request Derived Credential.**
   The user is directed to the Entrust IdentityGuard self-service module URL that you specified in the System Manager.
2. The user interacts with the Entrust self-service portal to get a derived credential, including naming the derived credential.
   The Entrust self-service portal provides a Derived Mobile Smart Credential Activation Password.
   Important: The user must record this password for later use in activating the derived credential.
3. After recording the password, the user follows directions to indicate he is done.
   The user is directed back to the user portal. A brief message indicates whether getting the derived credential was successful. If it was successful, **Request Derived Credential** is disabled.

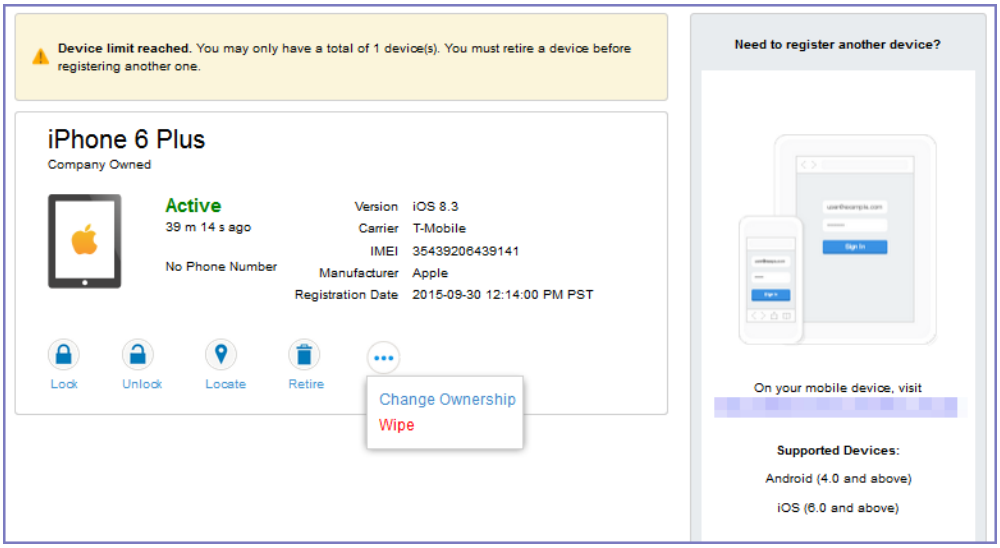
The user then does the following:

1. Use Mobile@Work to register the device to MobileIron Core.
2. Use the PIV-D Entrust app on the device to activate the derived credential.

If Change Device Ownership role is enabled

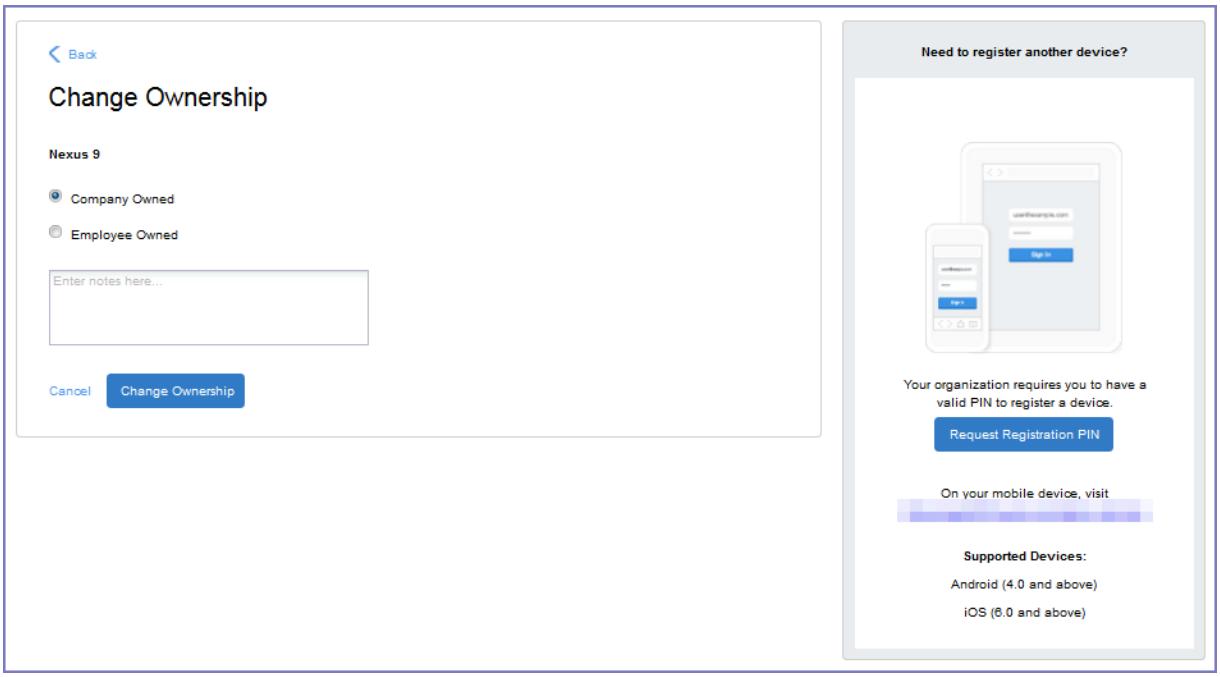
If the **Change Device Ownership** role is enabled, device users will see the option to change the device ownership.

FIGURE 22. CHANGE DEVICE OWNERSHIP OPTION



Clicking on **Change Ownership** allows the user to change the device ownership.

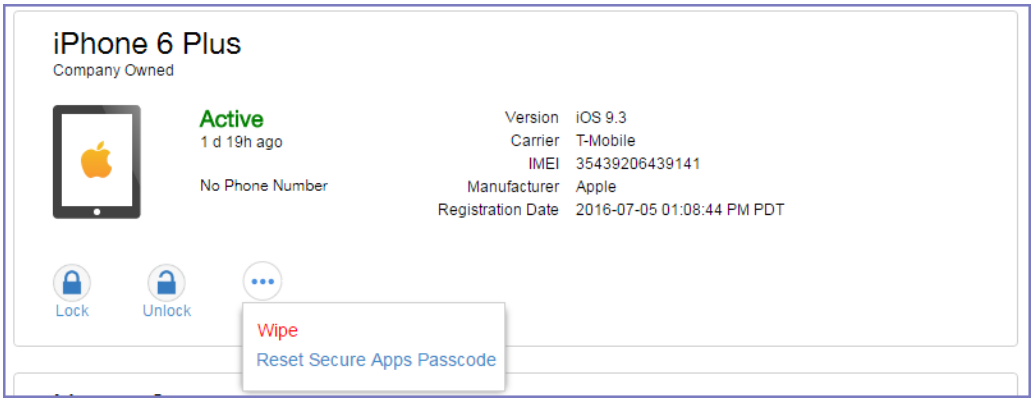
FIGURE 23. CHANGE DEVICE OWNERSHIP SETTINGS



If generating a one-time PIN for resetting the secure apps passcode is enabled

If you have configured MobileIron Core as described in About generating a one-time PIN for resetting a secure apps passcode on page 442, the device user sees the option **Reset Secure Apps Passcode**. This option is among the device management actions presented to the user for iOS and Android devices.

FIGURE 24. RESET SECURE APPS PASSCODE



Procedure

1. Click **Reset Secure Apps Passcode**.
2. On the next screen, click the button **Reset Secure Apps Passcode.**

3. A dialog box displays containing the one-time PIN.
4. In Mobile@Work on an iOS device, or in the Secure Apps Manager on an Android device, follow the instructions for resetting a forgotten secure apps passcode.
5. When prompted for user credentials, enter the user name and the one-time PIN.
6. Follow the instructions to create a new secure apps passcode.

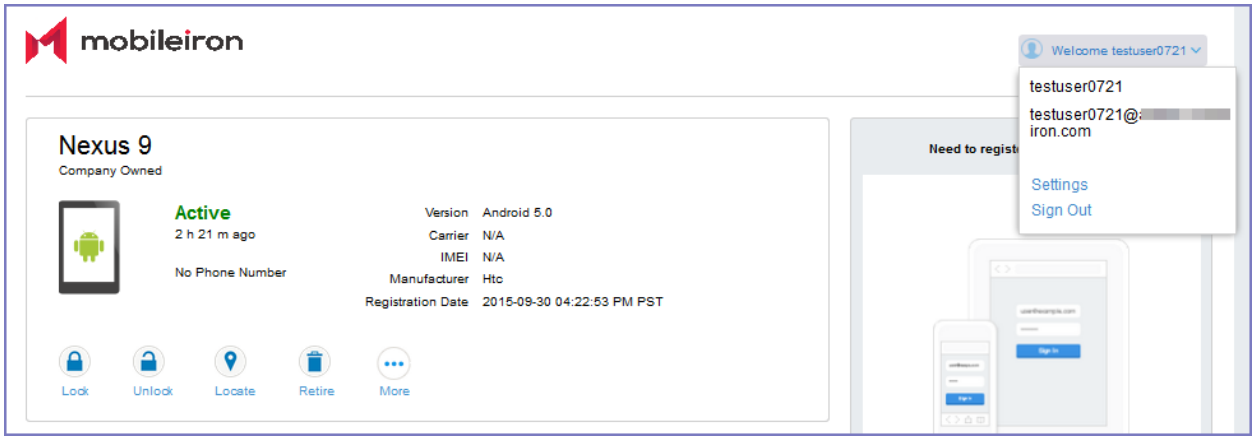
Uploading certificates in the user portal on a desktop computer

Device users can upload a certificate in the user portal on a desktop computer (available only if at least one user-provided certificate enrollment setting has been created).

Procedure

1. Go to https://<*Core_Server_FQDN*>/user.
2. Click on the device user's name in the top right corner.
3. Click on **Settings** in the drop down menu.

FIGURE 25. USER PROVIDED CERTIFICATE MANAGEMENT



4. Click **Upload New Certificate**.
5. In the **Configuration** field, select a value from the drop-down list that corresponds with how you want to use the certificate.

   NOTE: If you select a configuration for which you have already uploaded a certificate, the previously uploaded certificate will be replaced.
6. Click **Browse** next to the **User-Provided Certificate File** field.
7. Select a PKCS 12 file to upload.
8. If a **Password** field displays, enter the password of the certificate's private key.

Viewing, replacing, and deleting certificates in the user portal

Device users can view, replace, or delete certificates in the user portal.

Procedure

1. Go to https://<*Core_Server_FQDN*>/user.
2. Click on the device user's name in the top right corner.
3. Click on **Settings** in the drop down menu.
   The **User-Provided Certificate Management** page appears.
4. To view information about an uploaded certificate, click the "i" next to the certificate.
5. To replace a certificate, click the edit icon next to the certificate.
6. To delete a certificate, click the delete icon next to the certificate.

When a user-provided certificate is deleted

The user can delete the private key from the PKCS 12 file, and password if provided, from the Core file system using the user portal. A web services API is also available to delete them. Whether you want the private key and password deleted from Core depends on your security requirements.

WARNING: This action means that the certificate and private key in the PKCS 12 file (and password if provided) *are still available and usable on existing devices that already had received them from Core*. Because the private key was deleted from the Core file system, the certificate is **not** available to newly registered devices or to re-provisioned devices.

Because the certificate without the private key is still available on Core, you can view information about the certificate, such as its expiration date. This information can help you manage devices still using the certificate.

Viewing the help desk contact information

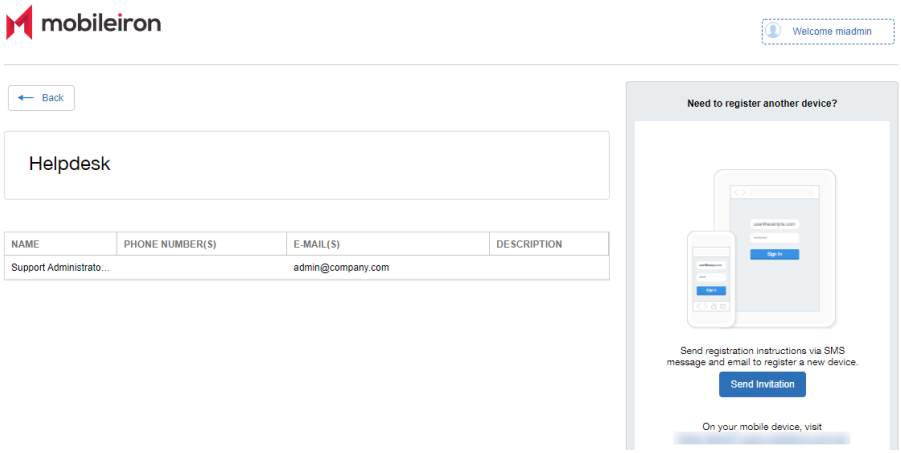
If the help desk contact information is configured in the MobileIron Admin Portal, device users can view the contact information in the self-service user portal.

For information about configuring the help desk contact information see, Configuring help desk contact information

Procedure

1. Go to https://<*Core_Server_FQDN*>/user.
2. Click on the device user's name in the top right corner.
3. Click **Helpdesk** in the drop down menu.
   The **Helpdesk** page appears.

FIGURE 26. HEPDESK CONTACT INFORMATION



Setting up Android enterprise with the alternative method

The alternative method enables you to use Android enterprise and requires sharing your user information with Google and binding your domain with Google. Each of your end users must have a Google account. However, MobileIron recommends setting up your Android enterprise account *without* binding your domain with Google as described in Enabling Android enterprise.

- Using the alternative method to set up Android enterprise
- Managing users for Android enterprise

Using the alternative method to set up Android enterprise

The alternative setup method consists of the following steps:

- Step 1: Sign up for Android enterprise with Google and get the EMM Token: in the Google Admin Console.
- Step 2: Create a Google service account and get a JSON file: in the Google Admin Console
- Step 3: Generate the JSON enrollment file: from the MobileIron Support site
- Step 4: Bind Core with Android enterprise: in MobileIron Core
- Step 5: Authorize MobileIron to view and manage your Google users: in MobileIron Core
- Step 6: Create the Android enterprise setting: in MobileIron Core

After completing these steps, continue to Managing users for Android enterprise.

Step 1: Sign up for Android enterprise with Google and get the EMM Token

Follow Google's set up instructions to sign up for Android enterprise, and then receive the EMM Token.

Prerequisite:

- Your company has a corporate Google Account or will create one following Google's instructions

You will need:

- access to your company's Google Admin account

NOTE: This step is performed on Google's website and is subject to change by Google.

In a web browser:

1. Go to Google's Android enterprise sign up page:
   "Sign up for Android enterprise"
   https://www.google.com/a/signup/u/0/?enterprise_product=ANDROID_WORK
2. Follow Google's instructions
   - Your setup may involve several steps, depending on whether or not your domain is already a Google Apps customer.
   - You may need to verify ownership of your domain with Google.
   - You may be directed to create a service account. The instructions for the service account are in Step 2.

   You will need to set up a service account, because it authenticates interactions between MobileIron Core in your domain and the Google EMM Play API. Follow Google's instructions to do so here:
   "Setup with a third-party EMM provider"
   https://support.google.com/work/android/answer/6174046

Next, generate an EMM Token.

1. Sign in to the Google Admin Console (admin.google.com) with your super administrator credentials.
2. Navigate to **Security> Android enterprise Settings.** The page shows a token if one was generated in the last 30 days, or a button to generate a new token.
3. Copy this token (as text) to use in Step 3.

Step 2: Create a Google service account and get a JSON file

In this step, you create a Google project and a service account with the EMM API enabled. You then receive a JSON file that holds a public/private key pair used to authorize interactions between apps on your domain and Google APIs.

NOTE: This step is performed on Google's website and is subject to change by Google. These instructions are based on: "Setup with a third-party EMM provider" https://support.google.com/work/android/answer/6174046

NOTE: You will need access to your company's Google Admin account

In a web browser:

1. Go to Google's Developers Console: https://console.developers.google.com
2. Log in with your Google Admin account credentials.
3. Create a new project.
4. With the dashboard showing the new project, click "Enable and manage APIs".
5. Search for "Google Play EMM API". Click the search result to select the API.
6. Click "Enable" to enable Google Play EMM API for your project.
7. Click "Credentials" in the left navigation pane.
8. Click "Create credentials" and choose "Service account key".

9. For “Service account”, select “New service account” and type in a name.
10. Select “Furnish a new private key”
11. For “Key type”, select JSON.
12. Click “Create”.

The JSON file will be downloaded to your computer. Check that the download file is given the name as indicated in the confirmation dialog with a “.json” extension, as some browsers may use a generic filename. Important: Store this file securely.

Step 3: Generate the JSON enrollment file

In this step, you will use the EMM Token and JSON file you obtained from Google to receive the **ActivateAfWForCore.json** enrollment file from the MobileIron Support portal. You can use the same enrollment file to enroll or re-enroll any number of Core instances that run on your domain.

You will need:

- your company’s login account for the MobileIron Support site at https://help.mobileiron.com.
- To get a login account, go to https://info.mobileiron.com/LoginRequest.html.
- administrator access to MobileIron Core
- the EMM Token from Step 1
- the Google JSON file from Step 2

In MobileIron Core:

1. Log in to the support portal at https://help.mobileiron.com.
2. Select **Android enterprise Enrollments.**
3. Click **Create New Android enterprise Enrollment.**
4. Click **Use Alternate Setup** to fill out the dialog with your EMM Token and domain URL.
5. Click **Choose file** to upload the Google JSON file from Step 2: Create a Google service account and get a JSON file.
6. Click **Submit**.
   The enrollment file will be generated.
7. Click **Download Google JSON Enrollment file.**
8. The **ActivateAfWForCore.json** enrollment file is downloaded to your computer.
   Some browsers may save the enrollment file with another name. Rename the file to *ActivateAfwForCore.json* before continuing.

IMPORTANT: Store the *ActivateAfWForCore.json* file securely.

You can use the same *ActivateAfwForCore.json* file to enable Android enterprise on multiple Core instances that belong to the same domain. You can also reuse the same file if you remove Android enterprise from Core, and then want to re-enroll it following the next steps again.

When this step completes successfully, MobileIron will be your Unified Endpoint Management (UEM) provider for Android enterprise, and will appear in the Security > Android enterprise settings on admin.google.com,

Step 4: Bind Core with Android enterprise

In this step, you upload the enrollment file from Step 3 to MobileIron Core, in order to bind Core with your domain's Android enterprise account.

You will need:

- administrator access to MobileIron Core
- the ActivateAfWForCore.json file from Step 3

In MobileIron Core:

1. Go to **Services > Google**.
2. Click **Browse** in the **Android enterprise** section, in the box labeled "2".
3. Select the **ActivateAfwForCore.json** file you collected in Step 3.
4. Click **Connect**.
5. When the Google Account is connected successfully, box 2 will show a confirmation including **Status: Connected**.

Step 5: Authorize MobileIron to view and manage your Google users

In this step, you give MobileIron permission to read Android enterprise user IDs from existing Google user accounts. Users with Google user accounts are eligible to use Android enterprise.

By default, Core uses the substitution value $EMAIL$ as the Google user account name. You can change this value to match your environment. You make this change by modifying the **User Sync Variable** field in this step. You can use any Core substitution variables along with hard-coded strings, as long as the format of the string after variable substitution has the format of a Google email address.

The following table gives some examples:

TABLE 77. EXAMPLES OF CORE SUBSTITUTION VARIABLES FOR THE GOOGLE USER ACCOUNT NAME

User Sync Variable value	Use this value when...
$USER_CUSTOM1$	You have set $USER_CUSTOM1$ in your LDAP setting in the Admin Portal (at **Services > LDAP**) to be the Google email address of an LDAP user. For example, after substitution: jdoe@someComany.com
$USERID$@someCompany.com	$USERID$ of an LDAP user is the same as the user name part of the user's Google email address. For example, after substitution: jdoe@someCompany.com
$USERID$@$USER_CUSTOM2$ $USERID$@someSubDomain.$USER_CUSTOM2$	• The Google account domain has a subdomain. • $USERID$ of an LDAP user is the same as the user name part of the user's Google email address. • You have set $USER_CUSTOM2$ in your LDAP setting in the Admin Portal (at **Services > LDAP**) to the LDAP user domain. For example, after substitution: jdoe@someSubDomain.someCompany.com

You will need:

- Steps 1 -4 completed

In MobileIron Core:

1. Go to **Services > Google**.
2. Change $EMAIL$ in the **User Sync Variable** field if $EMAIL$ is not the Google user account name that you have set up for your users.

   NOTE: Changing the User Sync Variable later requires you to remove the Android enterprise account as described in Removing the Android enterprise account in Core.
3. Click **Authorize** in the **Android enterprise** section, in the box labeled "3".

When authorization completes successfully, the Android enterprise section replaces the three steps with your account settings.

Step 6: Create the Android enterprise setting

In this step, you create the **Android enterprise setting** in MobileIron Core. This setting must be applied to each Android enterprise-capable device in order for the device to have Android enterprise functionality.

In the MobileIron Core Admin Portal:

1. Go to **Policies & Configs > Configurations**
2. Click **Add New > Android > Android enterprise**. The New Android enterprise (all modes) Setting dialog box opens.
3. Type a name for this setting (for example, “Android enterprise enabled”)
4. Click **Save**.
5. Apply it to a label that is also applied to Android enterprise-capable devices.
   Important Recommendation: Apply this setting to the built-in **Android** label, or a custom label that is defined using the filter “android.afw_capable = true”. For more details, refer to the Getting Started with MobileIron Core.

Impact of Android enterprise setting to devices that are not Android enterprise-capable

There is no impact to devices that are not Android enterprise-capable to have the Android enterprise setting applied. Some devices might become Android enterprise-capable in the future, if the carrier upgrades the device’s firmware.

To view the status of the Android enterprise setting for a device:

- Go to **Devices & Users > Devices**.
- Open the device details for the device.
- Click the **Configurations** tab.
- Look for the Android enterprise setting. The **Status** column will show:
  - **Pending**: The device has not yet confirmed that it has received the setting.
  - **Applied**: the setting is applied.
  - **Sent**: the device is not Android enterprise-capable; the setting is ignored by Mobile@Work.

Managing users for Android enterprise

User accounts in MobileIron Core that are meant for Android enterprise use are added, edited, and deleted in the same way as any Core user accounts. However, when you bind your user domain with Google, a user can register an Android enterprise device only if the user is added as a user in your corporate Google Account.

MobileIron Core automatically syncs with your corporate Google Account to enable Android enterprise for eligible users.

Syncing Google user accounts with Core

When you enabled Android enterprise on Core, you provided Core with access to view your corporate Google Account including the list of users. Core has read-only access to the Google user accounts, which means Core cannot add or modify your users’ Google accounts.

Therefore, Core keeps a list of which of its users have Google user accounts, thereby linking each Core user account with its corresponding Google user account.

MobileIron Core automatically syncs the users in Core with the users in your corporate Google Account. However, the sync behavior depends on whether you use $EMAIL$ for the Google user accounts, as specified in the user sync variable.

NOTE: Removing a Google account for Core causes any Android enterprise devices to retire when they check in.

TABLE 78. CORE BEHAVIOR AND THE USER SYNC VARIABLE

Sync time	User sync variable is $EMAIL$	User sync variable is NOT $EMAIL
Upon authorizing MobileIron to view the Google Account, when first enabling Android enterprise	Core **adds** users to its list of Google user accounts if the user is in Google's list.	No action.
On periodic intervals (approximately every 15 hours; subject to change)	Core **adds** users to and **deletes** users from its list of Google user accounts based on Google's list.	Core **deletes** users from its list of Google user accounts based on Google's list.
On demand when a new user is added in Core	No action.	No action.
On demand when a user registers a device to Core	Core **adds** the user to its list of Google user accounts if the user is in Google's list.	Core **adds** the user to its list of Google user accounts if the user is in Google's list.

Note: Core ignores Google user accounts that have no corresponding user account in Core.

Adding a new user in Core

For the MobileIron administrator, there are no differences to the process for adding new users when working with Android enterprise. Users can be added as local users, or automatically through LDAP, as usual.

Using Android enterprise on a device

To be eligible to use Android enterprise on a device, the user must have a Google account. This feature is applicable to Work Profile mode, Work managed device mode, and Managed device with work profile mode.

When the Google Play authentication token expires or changes were made (password, permissions, etc) requiring re-authorization, Mobile@Work will inform Core to reissue a new authorization token. This triggers Core to send a new authorization token to Mobile@Work in order to reauthorize Google Play. Mobile@Work can make up to 10 reauthorization requests within a 24-hour period. Upon the 11th request, an error message displays on the device, the device will be considered non-compliant and retired. In the Dashboard, a non-compliant icon displays next to the device to indicate to the administrator that there is a problem. The administrator should retire the device instance. It is recommended that all devices associated to that Google user ID to resync with Core. The device

user will need to re-register with Google Play. Below is a log showing the client reauthorization requests and eventual revocation of token.

	Client requested Googl…	Success	miadmin	2019-05-09 03:56:50…	2019-05-09 03:56:50…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google re-authorization token			2019-05-09 03:55:50…	2019-05-09 03:55:50…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:55:44…	2019-05-09 03:55:44…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:54:36…	2019-05-09 03:54:36…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:53:48…	2019-05-09 03:53:48…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:53:37…	2019-05-09 03:53:37…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:53:33…	2019-05-09 03:53:33…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Googl…	Success	miadmin	2019-05-09 03:52:53…	2019-05-09 03:52:53…	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Revoking Google User …	Success	miadmin	2019-05-09 03:36:44…	2019-05-09 03:36:44…	miadmin (Android 7.1 - PDA 12)	Revoking Google user token

Additional information on Android enterprise apps and related settings can be found in the *MobileIron Apps@Work Guide*.

Google account method for Android enterprise profile provisioning

On the Google Admin Console, you can enforce EMM policies on Android devices. If enforced, when a device user adds a managed Google account to a device, such as from Settings, Mobile@Work is automatically downloaded and launched. Once the user has registered Mobile@Work with MobileIron Core and the work profile is created, the account is automatically added to the work profile.

On work managed devices, after factory reset, when the device user logs in with the managed Google account, Mobile@Work is automatically downloaded and launched. Once the user has as registered Mobile@Work with MobileIron Core, the device is enrolled with Core as a work managed device.