MobileIron

MobileIron® Core
Device Management Guide
For Android for Work

MobileIron Core version 9.0.0.0
Mobile@Work 9.0.0.0 for Android

Revised: March 23, 2016

Proprietary and Confidential
Do Not Distribute

Revision History

Date	Revision
March 23, 2016	Updated to include features that work with Mobile@Work 9.0.0.0 for Android, and instructions updated to match Google site changes.

Contents

Chapter 1

Getting Started with Android for Work

Introduction

Android for Work is Google's program for supporting Android devices for enterprise. Android for Work 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 is an EMM provider that supports Android for Work. By following the instructions in this document, you will enable MobileIron Core to manage Android for Work devices.

MobileIron Core also supports other "containerized" solutions in addition to Android for Work, including MobileIron AppConnect and Samsung KNOX. A single device can use only one of these solutions at a time. However, Core can have each of the solutions configured for different devices.

MobileIron Core manages Android devices with or without Android for Work. Follow the instructions in this document if you are enabling Android for Work.

About this document

This is a complete guide for MobileIron Core administrators for installing, setting up, and managing Android for Work with MobileIron Core. A general understanding of Core administration is assumed.

Related documents include:

Title	**Purpose**
Mobile@Work for Android New Features and *Mobile@Work for Android Release Notes*	Describes the features of the client app, Mobile@Work for Android
How to Provision Android for Work 'Work Managed Devices'	To provision corporate-owned devices as work managed devices, you need MobileIron's Provisioner app. Refer to this document for complete instructions on downloading and using the provisioning app

Note: MobileIron Core does not require enabling Android for Work to manage Android devices. See also: *MobileIron Core Device Management Guide for Android.*

Requirements

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

- a Google Account for your enterprise
- corporate domain ownership (must match the domain for user email addresses)
- Google accounts for all Android for Work users
- MobileIron Core
  - version 8.5.0.0 or 9.0.0.0 (supports both “work profile” and “work managed device” modes), or
  - version 8.0 - 8.0.0.2c (supports only “work profile” mode)
- access to Google Play on Android devices and Core

To enable an Android for Work “work profile” on a given device, the following is required:

- an Android for Work-capable device, with Mobile@Work for Android app installed
- the registering user’s email address must match their Google account email
- Android for Work Configuration applied by label to the device

To enable Android for Work in “work managed device” mode, all the above is required, and also:

- a separate Android device with NFC, running the MobileIron Provisioner app. For complete details on downloading and using Provisioner, refer to: *How to Provision Android for Work ‘Work Managed Devices’.*

Limitations

MobileIron Core 8.0 - 9.0 supports native Android for Work devices, and can enable a “work profile” (also known as “profile owner”), allowing the user’s private profile and the corporate work profile to exist on the same device. A work profile is typically used in BYOD deployments.

MobileIron Core versions 8.5 and 9.0 support both the “work profile” mode and the “work managed device” mode (also known as “device owner”). A work managed device is typically corporate owned, and contains no private data.

To use Android for Work, a device must be natively “Android for Work-capable”. Devices that do not support Android for Work natively, or that require Google’s “Android for Work App” in order to have a work profile are not supported in Core 8.0 - 9.0.

The Mobile@Work app on Android devices shows “Android for Work-capable” in the About dialog for devices that are Android for Work capable.

Terminology

This document uses the terms “work profile” and “work managed device” to refer to the two ways in which Android for Work devices may be registered.

- A device with a **work profile** is an Android for Work device that 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.
- A **work managed device** is an Android for Work device that is typically corporate-owned. The device has a single profile with corporate data and apps. MobileIron Core has administrative control over the device, with more lockdown features available than for device using a work profile.

In Android developer documentation, “work profile” is referred to as “profile owner” and “work managed device” is referred to as “device owner”.

Enabling Android for Work for your enterprise

To enable MobileIron Core to provide Android for Work features, you must perform setup steps with Google, MobileIron Support, and MobileIron Core. The setup consists of the following steps:

Step #	Where	Description	Result
1	Google Admin Console	Step 1: Sign up for Android for Work with Google and get the EMM Token	EMM Token
2	Google Developer's Console	Step 2: Create a Google service account and get a JSON file	JSON file
3	MobileIron Support site	Step 3: Generate the JSON enrollment file	"ActivateAfwForCore.json" enrollment file for Core
4	MobileIron Core	Step 4: Bind Core with Android for Work	Android for Work is enabled on this Core
5	MobileIron Core	Step 5: Authorize MobileIron to view and manage your Google users	Your Google users can be linked to users on Core
6	MobileIron Core	Step 6: Create the Android for Work Configuration	Devices with this configuration and a Google user account can get an Android for Work profile

Step 1: Sign up for Android for Work with Google and get the EMM Token

Follow Google's set up instructions to sign up for Android for Work, 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:

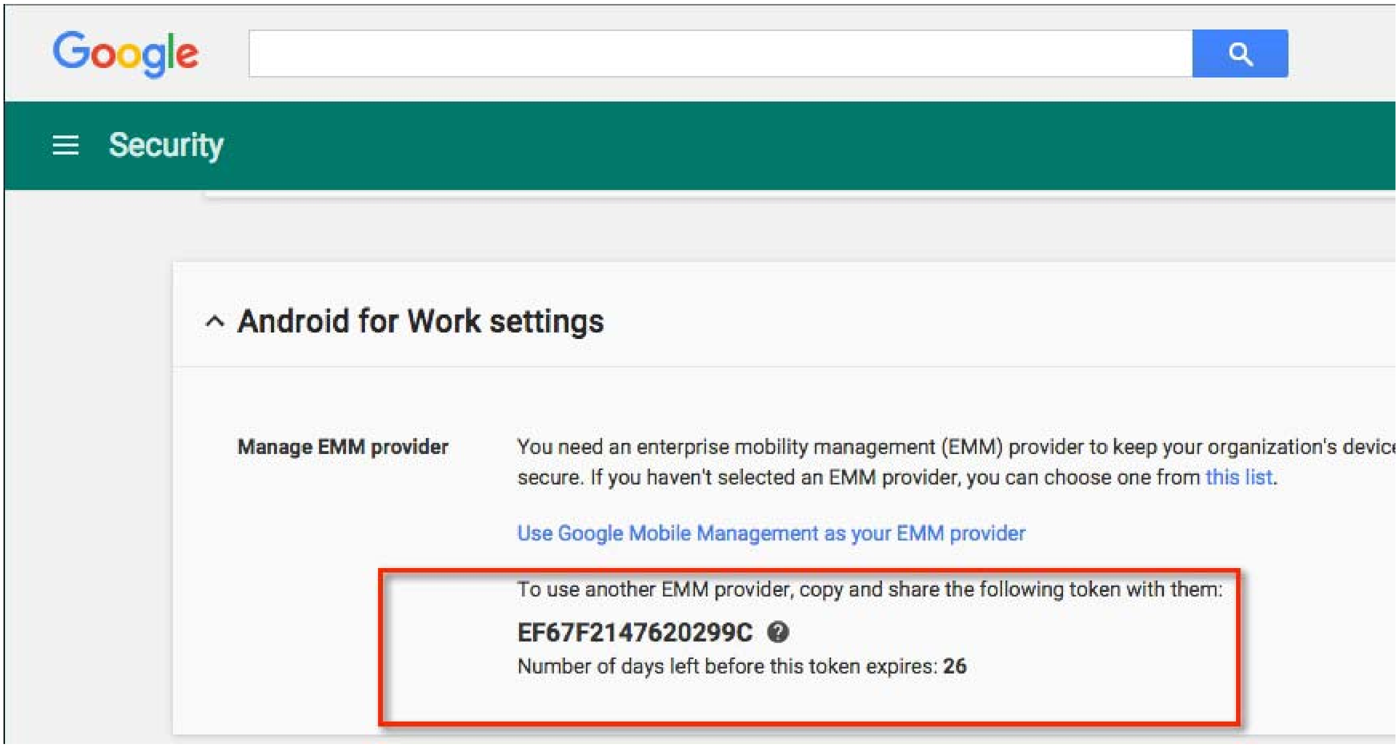
1. Go to Google's Android for Work sign up page:
   "Sign up for Android for Work"
   https://www.google.com/a/signup/u/0/?enterprise_product=ANDROID_WORK
2. Follow Google's instructions
   - Your setup may involve several steps, depending on whether or not your domain is already a Google Apps customer.
   - 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

3. Sign in to the Google Admin Console (admin.google.com) with your super administrator credentials.
4. Navigate to **Security**> **Android for Work Settings.** The page shows a token if one was generated in the last 30 days, or a button to generate a new token.



Security

Android for Work settings

Manage EMM provider

You need an enterprise mobility management (EMM) provider to keep your organization's devic secure. If you haven't selected an EMM provider, you can choose one from this list.

Use Google Mobile Management as your EMM provider

To use another EMM provider, copy and share the following token with them:

EF67F2147620299C

Number of days left before this token expires: 26

5. 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

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

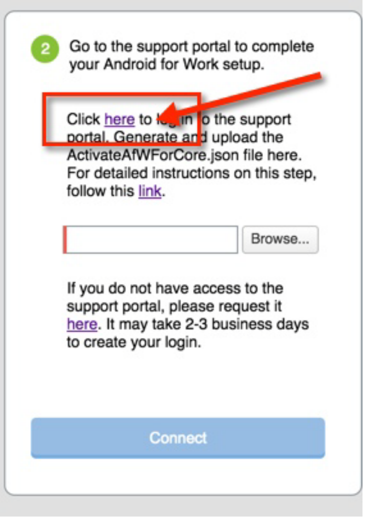
In this step, you will use the EMM Token and JSON file you obtained from Google to receive the **ActivateAfWForCore.json** enrollment file from the MobileIron Support portal. You can use the same enrollment file to enroll or re-enroll any number of Core instances that run on your domain.

You will need:

- your company’s login account for the MobileIron Support site
- administrator access to MobileIron Core
- the EMM Token from Step 1
- the Google JSON file from Step 2

In MobileIron Core:

1. Go to **Services** > **Google**.
2. In the box labeled “2” under **Android for Work**, click the first link to access the support portal.

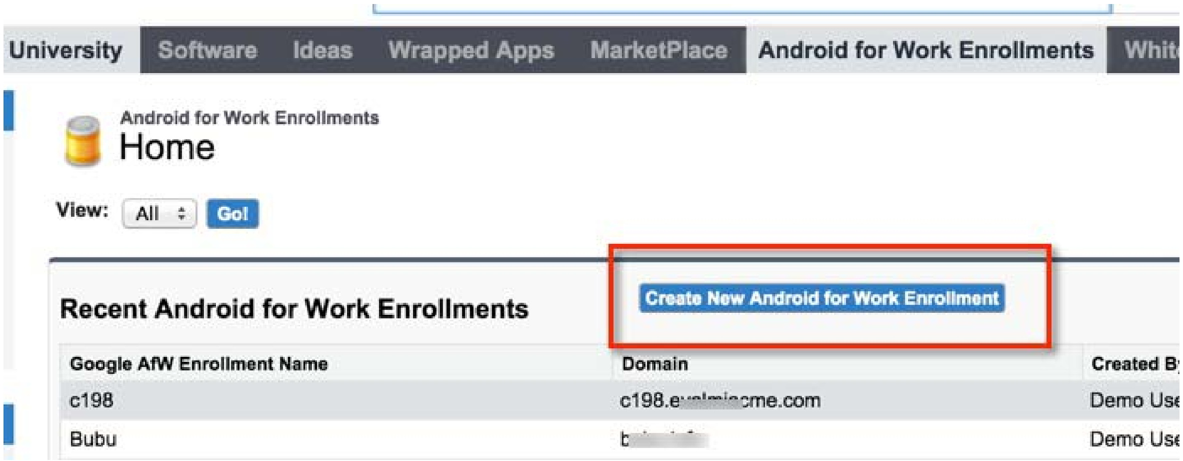


Go to the support portal to complete your Android for Work setup.

Click here to log in to the support portal. Generate and upload the ActivateAfWForCore.json file here. For detailed instructions on this step, follow this link.

If you do not have access to the support portal, please request it here. It may take 2-3 business days to create your login.

3. Log in to the support portal, and click **Create New Android for Work Enrollment**


University
Software
Ideas
Wrapped Apps
MarketPlace
Android for Work Enrollments
Whit
View: All
Go!
Create New Android for Work Enrollment

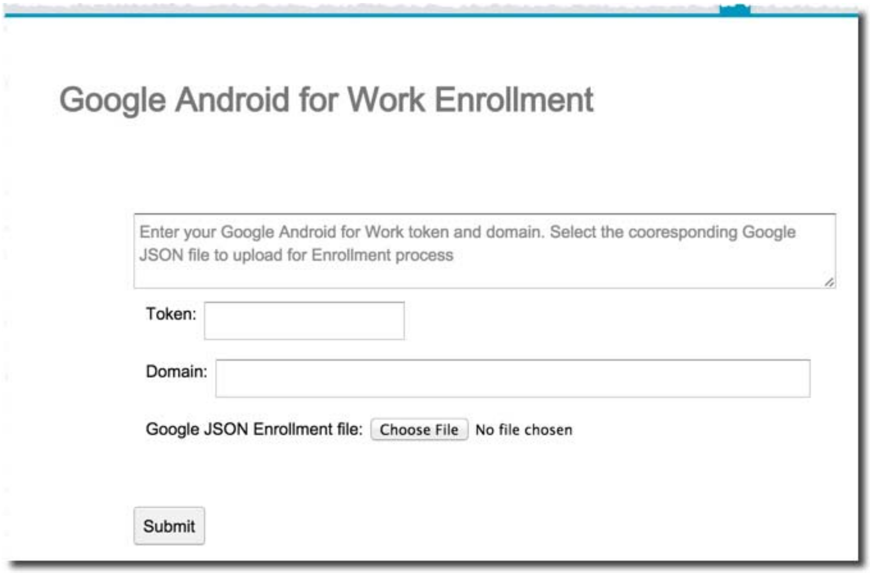
Android for Work Enrollments

Home

Recent Android for Work Enrollments

Google AfW Enrollment Name	Domain	Created B
c198	c198.e[redacted]cme.com	Demo Use
Bubu	b[redacted]	Demo Use

4. Fill out the dialog with your EMM Token and domain URL.



Google Android for Work Enrollment

Enter your Google Android for Work token and domain. Select the cooresponding Google JSON file to upload for Enrollment process

Token:

Domain:

Google JSON Enrollment file:

5. Click **Choose file** to upload the Google JSON file from step 2.
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.
   Note: 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 for Work on multiple Core instances that belong to the same domain. You can also reuse the same file if you remove Android for Work from Core, and then want to re-enroll it following the next steps again.

When this step completes successfully, MobileIron will be your EMM provider for Android for Work, and will appear in the Security > Android for Work settings on admin.google.com,

Step 4: Bind Core with Android for Work

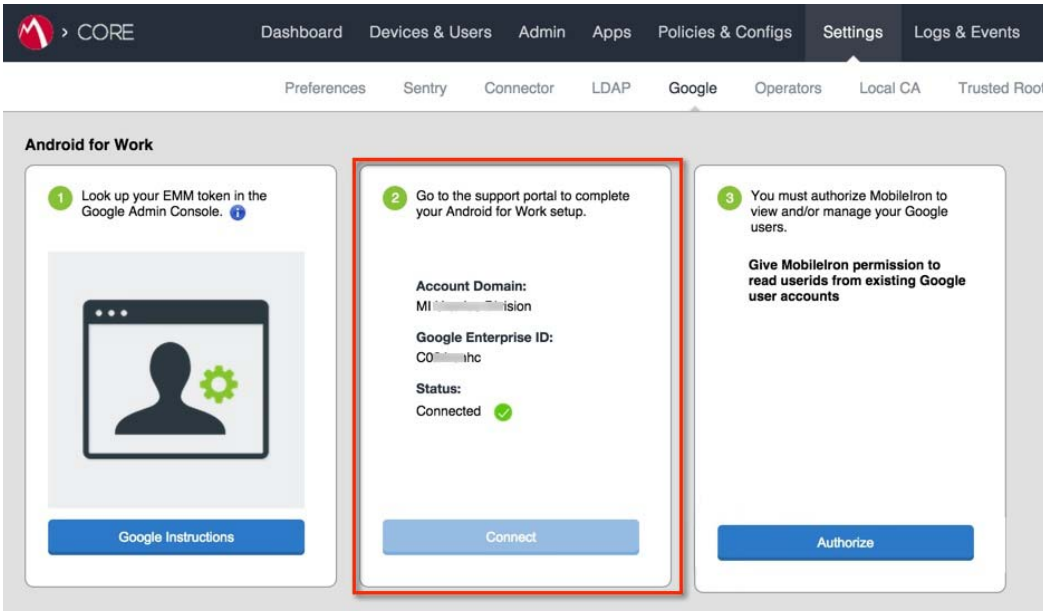
In this step, you upload the enrollment file from Step 3 to MobileIron Core, in order to bind Core with your domain's Android for Work account.

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 for Work** section, in the box labeled "2".
3. Select the **ActivateAfwForCore.json** file you collected in Step 3.
4. Click **Connect**.



Android for Work

1 Look up your EMM token in the Google Admin Console.

2 Go to the support portal to complete your Android for Work setup.

Account Domain:
MI[redacted]ision

Google Enterprise ID:
CO[redacted]hc

Status:
Connected ✓

3 You must authorize MobileIron to view and/or manage your Google users.

Give MobileIron permission to read userids from existing Google user accounts

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

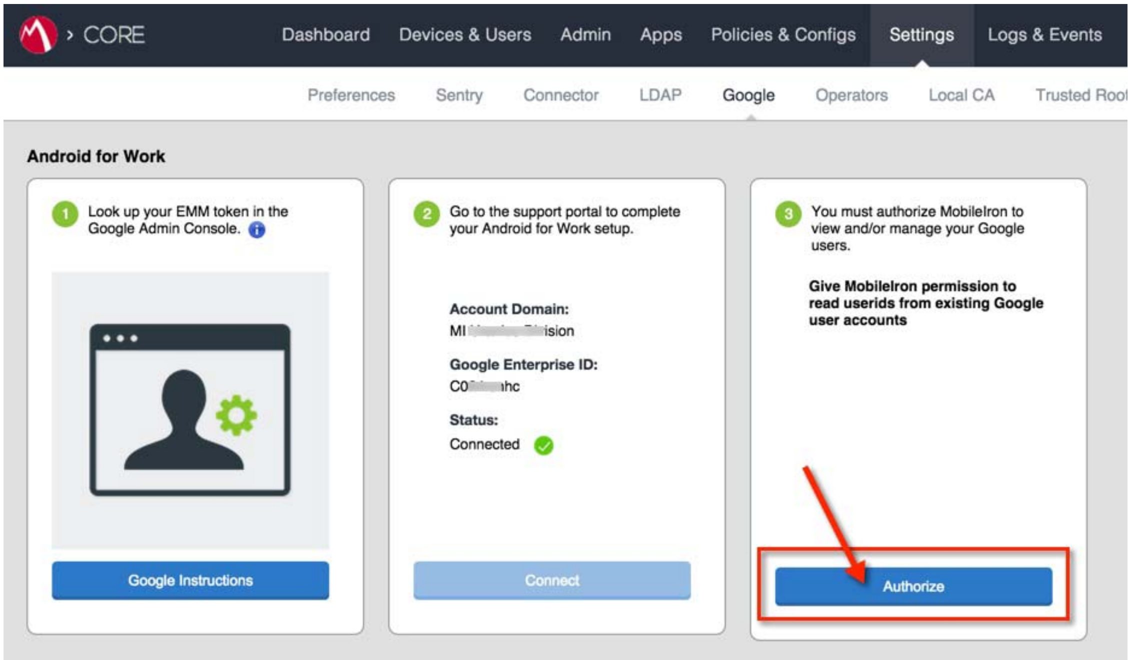
In this step, you give MobileIron permission to read user IDs from existing Google user accounts. Users with Google user accounts are eligible to use Android for Work.

You will need:

- Steps 1 -4 completed

In MobileIron Core:

1. Go to **Services** > **Google**.
2. Click **Authorize** in the **Android for Work** section, in the box labeled "3".



Android for Work

1 Look up your EMM token in the Google Admin Console.

2 Go to the support portal to complete your Android for Work setup.

Account Domain:
MI[redacted]ision

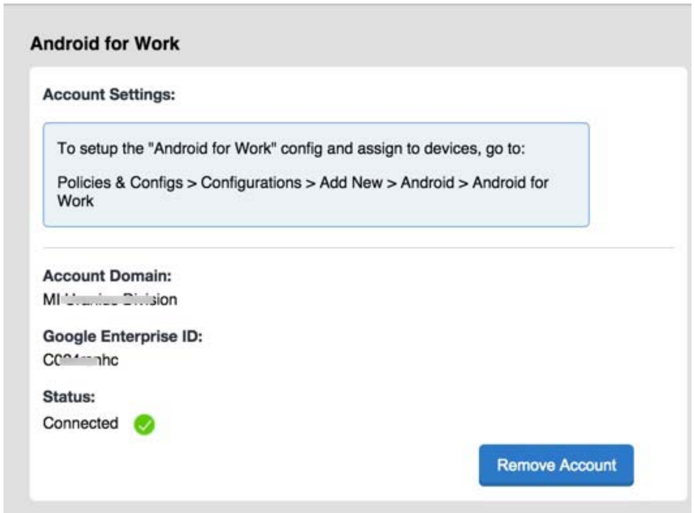
Google Enterprise ID:
C0[redacted]hc

Status:
Connected ✓

3 You must authorize MobileIron to view and/or manage your Google users.

Give MobileIron permission to read userids from existing Google user accounts

When authorization completes successfully, the Android for Work section will display your account settings instead of the three steps:



Android for Work

Account Settings:

To setup the "Android for Work" config and assign to devices, go to:

Policies & Configs > Configurations > Add New > Android > Android for Work

Account Domain:
MI[redacted]sion

Google Enterprise ID:
C0[redacted]hc

Status:
Connected ✓

Step 6: Create the Android for Work Configuration

In this step, you create the **Android for Work Configuration** in MobileIron Core. This configuration must be applied to each Android for Work-capable device in order for the device to have Android for Work functionality.

In the MobileIron Core Admin Portal:

1. Go to **Policies & Configs** > **Configurations**
2. Click **Add New** > **Android** > **Android for Work**
3. Type a name for this configuration (for example, "Android for Work enabled")

4. Click **Save**.
5. Apply it to a label that is also applied to Android for Work-capable devices.
   Important Recommendation: Apply this configuration to the built-in **Android** label, or a custom label that is defined using the filter “android.afw_capable = true”. For more details, see: “Choosing a label for the Android for Work Configuration” on page 20

Impact

There is no impact to devices that are not Android for Work-capable to have the Android for Work Configuration applied. Keep in mind that some devices may become Android for Work-capable in the future, if the carrier upgrades the device’s firmware.

To view the status of the Android for Work Configuration for a device:

- Go to **Devices & Users** > **Devices**.
- Open the device details for the device, and click the **Configurations** tab.
- Look for the Android for Work Configuration. The **Status** column will show:
  - **Pending**: the device does not meet the requirements to receive the configuration.
  - **Applied**: the configuration is applied.
  - **Sent**: the device is not Android for Work-capable; configuration is ignored by client.

Note: Devices that are not Android for Work-capable will show the configuration state as “SENT”. This is normal.

Next steps

By successfully completing Steps 1 - 6, your MobileIron Core is ready to register devices for Android for Work.

You may wish to set up further policies, configurations, and apps for Android for Work devices.

To register Android for Work devices:

- Users register a “work profile” device as usual, by installing Mobile@Work client and following the regular registration process. (See *MobileIron Core Device Management Guide for Android*, for more information.)
- Administrators must provision “work managed” devices using a master device that is running the Provisioner app. See *How to Provision Android for Work ‘Work Managed’ Devices* for complete instructions.

Removing and unbinding Android for Work

Removing the Android for Work account from MobileIron Core severs Core's connection with the Google Account. Removing Android for Work account as detailed below affects the single Core server and does not unbind your domain. The reasons to remove your account may include:

- to change the Google service account for the specific Core
- as an optional first step to unbind your domain from using MobileIron as an EMM provider
- to stop supporting Android for Work devices on the specific Core

Impact of removing the Android for Work account

Removing the Android for Work account *does not* retire devices.

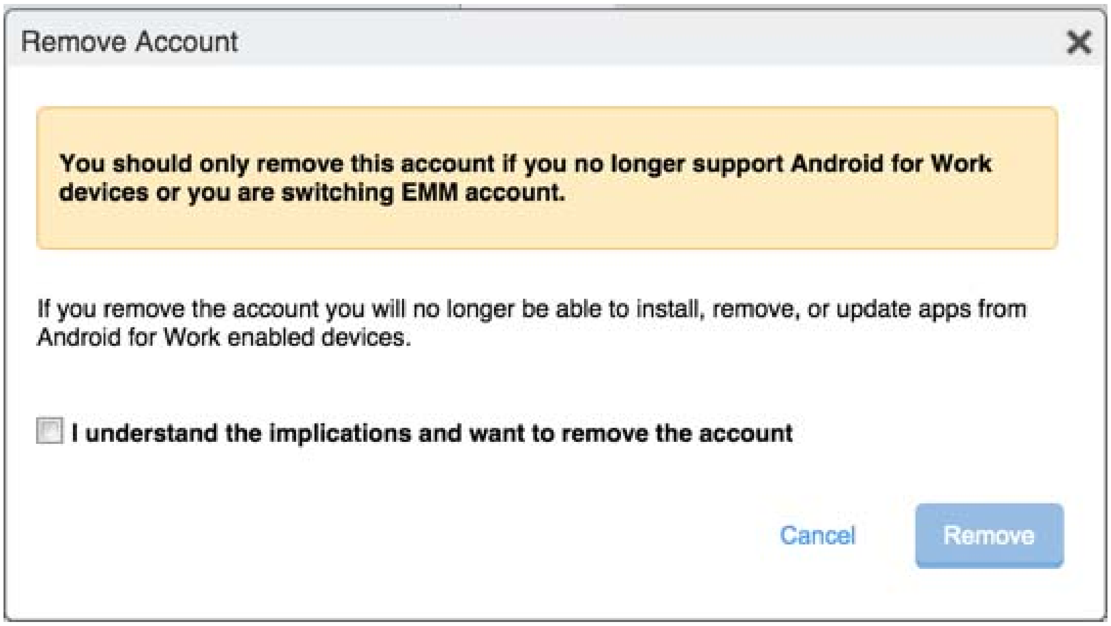
By removing the Google Account from Core, the following affects the Core instance:

- MobileIron Core can no longer install, remove, or update apps from Android for Work-enabled devices
- users continue to have access to the apps, however, the apps cannot be updated through Apps@Work
- Android for Work devices will continue to be managed by MobileIron Core with the policies and configurations that are applied to them
- no new users can register devices with Android for Work.

Removing the Android for Work account in Core

In Core Admin Portal:

1. Go to **Services** > **Google**
2. Under **Android for Work** click **Remove** . The **Remove Account** dialog appears.



Remove Account

You should only remove this account if you no longer support Android for Work devices or you are switching EMM account.

If you remove the account you will no longer be able to install, remove, or update apps from Android for Work enabled devices.

□ **I understand the implications and want to remove the account**

3. If you wish to remove the Android for Work binding with Core, click the checkbox for "I understand" and then click **Remove**.

Unbinding your domain from MobileIron

Google allows a domain to be bound to a single EMM provider for Android for Work. You may want to unbind your domain from MobileIron if you want to use an EMM solution from another vendor, or if you have an issue with your domain.

Impact of unbinding your domain

Unbinding your domain removes MobileIron as the Android for Work EMM provider for your domain and affects *all* instances of MobileIron Core on your domain.

Unbinding your domain *does not* retire devices.

Unbinding your domain has the following effects:

- any MobileIron Core on your domain can no longer install, remove, or update apps from Android for Work-enabled devices
- users continue to have access to the apps, however, the apps cannot be updated through Apps@Work
- Android for Work devices continue to be managed by MobileIron Core with the policies and configurations that are applied to them
- no new users can register devices with Android for Work
- the JSON enrollment file, ActivateAfwForCore.json, becomes invalid. You can no longer use it to bind your domain with MobileIron.

Unbinding your domain

You will need:

- login account for the MobileIron Support site

See instructions for unbinding your domain on the Mobile Support site Knowledge Base article:

https://help.mobileiron.com/customer/articles/MI_Article/Android-for-Work

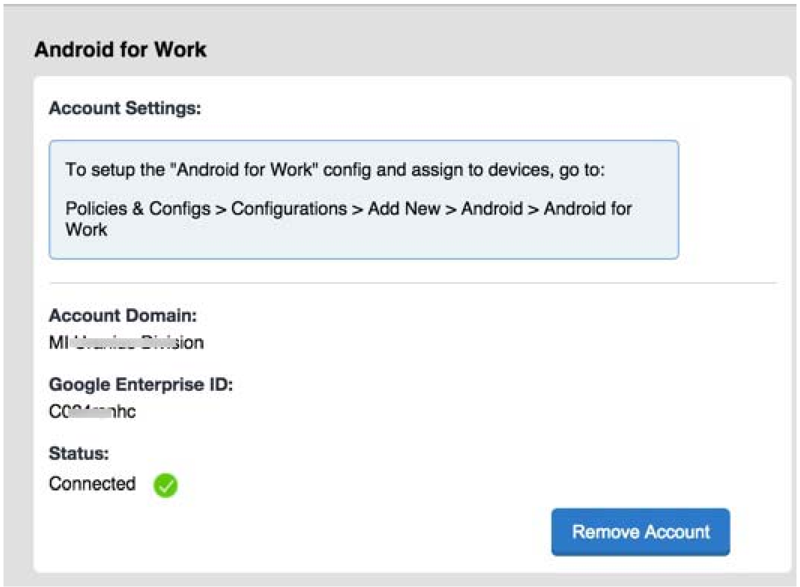
Determining if Android for Work is available on Core and devices

Use these checklists to determine if MobileIron Core is successfully set up for Android for Work, and if a given device is eligible for Android for Work.

Determining if Core is set up for Android for Work

To verify if MobileIron Core is successfully enabled for Android for Work:

- Go to **Services** > **Google**. In the **Android for Work** section, ensure that the page shows a single "**Account Settings**" box with "**Status: Connected**" as shown below.
- If you see boxes with steps 1, 2, 3, Android for Work is not enabled for Core.



Android for Work

Account Settings:

To setup the "Android for Work" config and assign to devices, go to:

Policies & Configs > Configurations > Add New > Android > Android for Work

Account Domain:
MI[redacted]sion

Google Enterprise ID:
CO[redacted]nhc

Status:
Connected ✓

Determining if a device is eligible for Android for Work

Prerequisite: ensure that Core is successfully enabled for Android for Work.

Next, a device is eligible to get the Android for Work profile as soon as all the following conditions are met:

- The user has a Google account, and the account email matches the user's email in Core.
- The device is Android for Work-capable. See: "Verifying if a device is Android for Work-capable" on page 18
- The device is assigned a label with the Android for Work Configuration

A device will automatically migrate to Android for Work if it is already registered, and the above conditions are met after registration.

If the conditions are met before the device registers, the device will register directly into the Android for Work "work profile" mode.

Verifying if a device is Android for Work-capable

You can check if a device is Android for Work capable in these ways:

- On the device, open Mobile@Work. Tap the menu, and tap **Settings** > **About**. Look for "Android for Work capable" in the About box text.
- 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 for Work Capable" row. The value is true if the device is capable.

Chapter 2

Policies and Configurations

- Basic label
- Creating a dynamic label for Android for Work devices
- Choosing a label for the Android for Work Configuration
- When the Android for Work Configuration is removed
- Lockdown policy
- Security policy

Basic label

You may find it useful to have a label that identifies all Android for Work-capable devices, to use when assigning policies and configurations.

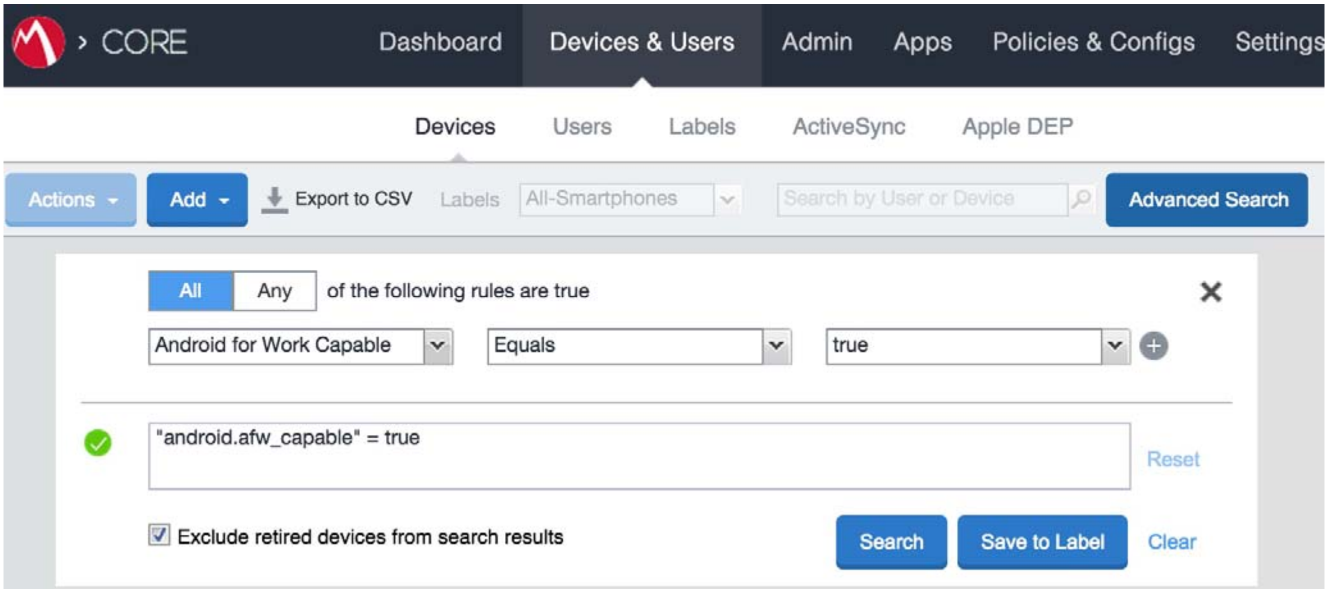
Note: to apply the required **Android for Work Configuration** to devices, use only the built-in **Android** label or a custom label that is defined using the filter "android.afw_capable = true".

Creating a dynamic label for Android for Work devices

You can create a label that dynamically applies itself to all Android for Work-capable devices. Use this label to assign configurations, policies, and apps that you want to apply to all Android for Work devices.

To create the label, in Core Admin Portal:

1. Go to **Devices & Users** > **Devices**
2. Click **Advanced Search**
3. Fill out the expression with these values:
   Field = **Android for Work Capable**
   Operator = **Equals**
   Value = **true**



All | Any of the following rules are true

Android for Work Capable | Equals | true

"android.afw_capable" = true

☑ Exclude retired devices from search results

4. Click **Save to Label**
5. Type a name for the label (for example: "Android for Work Capable")
6. Click **Save**.

Choosing a label for the Android for Work Configuration

Every device is required to have the **Android for Work Configuration** applied to it in order to have Android for Work functionality.

It is strongly recommended to use the built-in **Android** label, or alternatively **All_Smartphones,** or a dynamic label that is defined using the filter "android.afw_capable = true" for applying the **Android for Work Configuration.**

Important note for work managed devices: Failing to use a recommended label will prevent the provisioned device from successfully completing registration. The device will perform a factory reset and will need to be re-provisioned.

Note for work profile only: by applying the Android for Work Configuration to a built-in label or a custom label defined by "android.afw_capable = true", the Android for Work-capable devices can register directly with a work profile. However, if you use a dynamic label (excluding one defined by "android.afw_capable = true"), the device will first register as a regular Android device, and then migrate itself to have the Android for Work profile. See also: "Migrating devices to Android for Work" on page 30

When the Android for Work Configuration is removed

Removing the Android for Work Configuration from a device causes the device to become "unregistered."

The Android for Work Configuration can be inadvertently removed from a device if:

- the configuration is applied to a dynamic label instead of a built-in label (not recommended), and
- the device is dynamically dis-included from the label for any reason, or
- the Android from Work Configuration is manually removed from a label shared with a device.

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

Android for Work status	**If Android for Work Configuration 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.
work managed device	• The device becomes unregistered and performs a factory reset. • Device must be returned to the administrator to be re-provisioned.

Recommendation: Use the built-in system label "Android" to assign the Android for Work Configuration to devices.

Additional policies and configurations

The following are policies and configurations you may want to create for and apply to Android for Work devices.

Lockdown policy

The Lockdown policy has a special section for Android for Work. No other options in Lockdown policy apply to Android for Work devices. If you do not apply a custom Lockdown policy to a device, the default Lockdown policy is in effect. By default, the lockdown policy sets all Android for Work features to be allowed.

The policies listed under "**Android for Work** "apply to all Android for Work devices.

The policies listed under "**Work Profile**" apply to devices with a work profile.

The policies listed under "**Work Managed Device Profile**" apply to devices that are provisioned to be work managed devices.

To create a new Lockdown policy:

1. Go to **Policies & Configs** > **Policies**
2. Click **Add New** > **Lockdown**
3. Type a name for this policy
4. Scroll down to the **Android for Work** section.
5. Ensure the checkbox is selected to allow a feature, or deselected it to disallow the feature.

Lockdown Feature	**Description**	**Applies to Android for Work modes:**
Allow screen capture	Allows screen capture of apps or data inside the Android for Work profile	All
Allow the user to turn on location sharing	Allows device GPS location to be shared with Work apps. Supported on Android 5.1 only.	All
Allow modification of applications in Settings or launchers	Allows user to change application settings such as clearing cache, deleting data, uninstalling, or force stopping apps in App settings screen. Note: use "Block uninstall" option in App Catalog app details to prevent user from uninstalling the app.	All
Allow the user to configure user credentials	Allows user to change credentials in the Work profile, in Android Settings > Security > Trusted Credentials > Work.	All

Lockdown Feature	Description	Applies to Android for Work modes:
Allow the user to create and modify accounts	Allows user to create or modify accounts in the Work profile, in Android Settings > Account. *Caution*: To install the Divide Productivity app, this setting must be allowed until the app configuration is completed.	All
Allow the user to transfer app data over NFC	Allows use of NFC to transfer app data. Supported on Android 5.1 only.	All
WORK PROFILE		
Allow copy and paste	Allows copy and paste from apps inside the Android for Work profile to apps outside the profile.	work profile
Allow caller ID across profiles	Allows caller ID to be visible to apps in all profiles.	work profile
WORK MANAGED DEVICE PROFILE		
Allow camera	Allows camera to function.	work managed device
Allow master volume un-mute	Allows user to un-mute master volume. Note: volume is not muted by default.	work managed device
Allow microphone un-mute	Allows user to un-mute microphone	work managed device
Allow automatic date & time	If checked, user can change date and time. If unchecked, user can make changes but system will reset the date and time automatically.	work managed device
Allow automatic timezone	Allows timezone to be set automatically. Note: the user can re-enable the ability to update time and timezone if this setting is disallowed.	work managed device
Allow safe boot of the device	Allows user to reboot the device into safe mode.	work managed device
Allow factory reset	Allows user to initiate a factory reset of the device.	work managed device
PHONE AND NETWORK RESTRICTIONS		
Allow SMS	Allow user to send and receive SMS messages.	work managed device
Allow outgoing calls	Allow user to place outgoing calls.	work managed device
Allow data roaming	Allow use of data while user is traveling outside of data plan area. Note: the user can re-enable this feature from settings.	work managed device

Lockdown Feature	Description	Applies to Android for Work modes:
Allow Wi-Fi	If Allow Wi-FI is: • enabled (default), the device user can turn Wi-Fi on or off • not enabled, the device user cannot turn Wi-Fi on **Caution**: Turning off Wi-Fi on a Wi-Fi only device will make the device unable to communicate with MobileIron Core or any network. A factory reset will be needed to restore Wi-Fi capability on the device.	work managed device
Allow Wi-Fi to be configured	Allows user to configure Wi-Fi.	work managed device
Allow Wi-Fi sleep policy to be configured	Allows user to configure Wi-Fi sleep policy. Note: the user can re-enable this feature from settings.	work managed device
Allow Bluetooth	If **Allow Bluetooth** is: • enabled (default), the device user can turn Bluetooth on or off • not enabled, the device user cannot turn Bluetooth on	work managed device
Allow Bluetooth to be configured	Allows user to configure Bluetooth.	work managed device
Allow Emergency Broadcasts to be configured	Allows user to configure Emergency Broadcasts.	work managed device
Allow mobile network to be configured	Allows user to configure the mobile network.	work managed device
Allow tethering and mobile hotspots to be configure	Allows the user to configure tethering and hotspots.	work managed device
Allow VPN to be configured	Allows user to configure VPN.	work managed device

6. Click **Save**.
7. Apply the policy to a label for Android for Work-capable devices.

Security policy

You can use the same security policy settings as you would for any Android device.

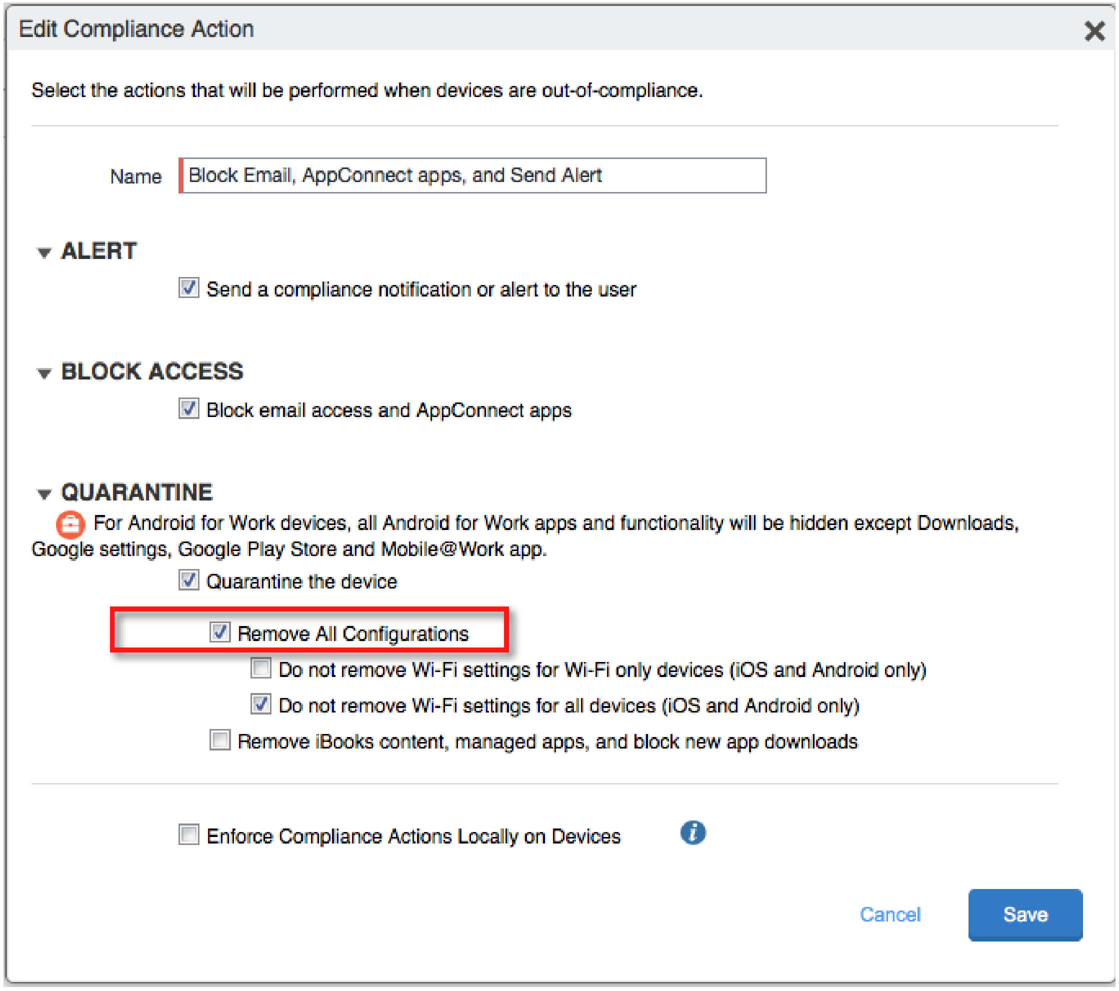
To apply the security policy to Android for Work devices, apply the policy to an Android for Work-related label that is also applied to Android for Work-capable devices.

The specific behavior of “quarantine” for an Android for Work profile is described next.

Quarantine compliance action

To create a quarantine compliance action that you can use for Android for Work configurations, do the following.

1. Go to **Policies & Configs** > **Compliance Actions**
2. Click **Add+**
3. Enter a **Name**
4. To configure the quarantine, you must select checkboxes, as shown below:
   - **Quarantine the device,** and
   - **Remove All Configurations**
   - and either "**Do not remove Wi-Fi settings for Wi-Fi only devices**" or "**Do not remove Wi-Fi settings for all devices**"
5. Click **Save**
6. You can now select this compliance action in the Security policy.



Edit Compliance Action

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

Name: Block Email, AppConnect apps, and Send Alert

ALERT

☑ Send a compliance notification or alert to the user

BLOCK ACCESS

☑ Block email access and AppConnect apps

QUARANTINE

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

☑ Quarantine the device

☑ Remove All Configurations

□ Do not remove Wi-Fi settings for Wi-Fi only devices (iOS and Android only)

☑ Do not remove Wi-Fi settings for all devices (iOS and Android only)

□ Remove iBooks content, managed apps, and block new app downloads

□ Enforce Compliance Actions Locally on Devices

How quarantine behaves on Android for Work devices

Quarantine behaves as described below:

Android for Work status	Quarantine behavior
work profile and work managed device	Android for Work apps and functionality is hidden, except: • Downloads • Google settings • Google Play store • Mobile@Work

Chapter 3

Managing Users and Devices

- Managing users for Android for Work
- Managing the Android for Work device lifecycle

Managing users for Android for Work

User accounts in MobileIron Core that are meant for Android for Work use are added, edited, and deleted in the same way as any Core user accounts. However, a user can register an Android for Work 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 for Work for eligible users.

Syncing Google user accounts with Core

When you enabled Android for Work 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.

MobileIron Core automatically syncs the users in Core with the users in your corporate Google Account by comparing email address. A sync occurs:

- on periodic intervals (approximately every 15 hours; subject to change)
- on demand when a new user is added in Core, or
- upon authorizing MobileIron to view the Google Account, when first enabling Android for Work.

If a new Core user has a Google account, the two accounts are linked in Core. Core determines if a new user has a Google account by comparing email addresses. Google user accounts without a corresponding user account in Core are ignored.

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 for Work. Users can be added as local users, or automatically through LDAP, as usual.

However, to be eligible to use Android for Work on a device:

- the user must have a Google account
- user's Core email address must match their Google account email address.

Core automatically determines if a new user has a Google account by comparing email addresses. Core does not add Google Accounts for Core users that have no Google account.

Managing the Android for Work device lifecycle

Provisioning a device

Provisioning is necessary only for work managed devices. You can provision factory reset Android devices using the Provisioner app, which uses the NFC bump method. Once provisioned, a work managed device can register with MobileIron Core as usual.

For details about provisioning, see *How to Provision Android for Work 'Work Managed Devices'.*

Registering a device

To register an Android for Work-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 for Work capable, and performs the correct registration steps automatically.

Prerequisites

To register an Android for Work-capable device to have an Android for 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 for Work as described in "Enabling Android for Work for your enterprise" on page 8. To confirm the setup, go to **Settings > Google**. In the **Android for Work** section you should see **Account Settings:** information with **Status: Connected**.
- The **Android for Work Configuration** is applied to an appropriate label.
- The user account on Core must match to a Google user account. If there is no match, the user will not see Android for Work on their device, even if the device is Android for Work-capable.

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

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

- on a device with a work profile, check that the Mobile@Work app appears with the Android for Work 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.

Migrating devices to Android for Work

"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 already Android for Work enabled. It applies only to device that are not in Android for Work mode, yet.

Migration triggers

A registered device may migrate to an Android for Work profile (assuming Core has Android for Work enabled, users have Google accounts, and the device has the Android for Work configuration applied to it) when the following occurs:

- user upgrades from pre-8.0 Mobile@Work to Mobile@Work 8.0 or newer, on an Android for Work-capable device
- the device becomes Android for Work-capable after it receives a firmware update from the carrier
- Core 8.0-9.0 is newly enabled for Android for Work, and the Android for Work-capable device is already running Mobile@Work 8.0 or newer
- the user with a registered Android for Work-capable device is assigned a Google account for the first time, and the account is synced with Core.

Note: see also "Determining if Core is set up for Android for Work" on page 17 and "Determining if a device is eligible for Android for Work" on page 17.

Impact

In the scenarios listed in Migration triggers, the Android devices begin their migration to use Android for Work profile automatically.

Migration scenarios do not apply to work managed devices, because such devices are provisioned with Android for Work from the start.

Preventing automatic migration

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

Note: If you applied the **Android** label to the **Android for Work Configuration**, then all Android devices potentially have the configuration, and all Android for Work-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 Android for 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 for Work work profile is created.
4. The Mobile@Work app icon appears with the Android for Work badge.
5. Configuration steps appear as needed.

Quarantine on Android for Work devices

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

Android for Work status	**Quarantine behavior**
work profile	- All the apps in the Work profile are hidden, except: - Google Play - Mobile@Work - Contacts are hidden. - The Wi-Fi configurations are kept or removed based on the quarantine settings.
work managed device	same behavior as for work profile

Retiring an Android for Work device

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

Android for Work status	**Retire behavior**
work profile	- The work profile is removed. - All apps, data, and contacts in the work profile are removed. - The Mobile@Work app is disabled and therefore hidden from the user after **Retire**. User can re-enable Mobile@Work by accessing it on Google Play. - A user can re-register a retired device.
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.

Wiping an Android for Work device

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

Android for Work 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. • The Mobile@Work app is disabled and therefore hidden from the user after **Wipe**. User can re-enable Mobile@Work by accessing it on Google Play. • A user can re-register a wiped device.
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 for Work device

The **Lock** command locks the screen of an Android for Work device. To Lock the device:

- Go to **Devices & Users** > **Devices**.
- Select the device.
- Click **Actions** > **Lock.**
- Click **Lock**.

  The device will lock as soon as it receives the command. The user can unlock the device using their regular screen unlock passcode.

The **Unlock** command is not supported for Android for Work devices.

Note: Google's Android Device Manager enables the user to manage their personal device through their Google account. Please refer to Google for more information about the Android Device Manager.

Unlocking an Android for Work device

The **Unlock** command is not supported for Android for Work devices.

Chapter 4

Managing Apps for Android for Work

- About Apps for Android for Work
- Deploying public, private, and private channel apps
- How to deploy Divide Productivity with Android for Work

About Apps for Android for Work

You can make public and private (in-house) apps available for download to Android for Work devices in the App Catalog on Core by selecting the “**Install this app for Android for Work**” setting in the app details. However, not all apps are available for Android for Work. For example, apps that require configuration (also called “restrictions”) must be developed specifically for Android for Work.

The special features of apps for Android for Work are:

- **Silent Install**: Any public or private app can be silently installed for Android for Work.
- **Block Uninstall**: Prevents the user from uninstalling the apps.
- **Accepting Permissions:** You must accept app permissions on behalf of the users in order to add the app to the App Catalog.
- **Configurations**: Android for Work apps can have configurations (also called “restrictions”) that are key-value pairs defined by the app developer. You set the restrictions when you add the app to the App Catalog.
- **New Permissions**: If an app version has new permissions that you have not yet accepted on behalf of users, an icon appears in the **New Permissions** column on the App Catalog page. Note: until you accept new app permissions on behalf of users, new silent app installs for newly registered devices and silent app updates for currently registered devices will not proceed.
- An app designated as available to Android for Work devices can also be available to all Android devices. The app will install appropriately on Work profiles or non-Android for Work devices.

Otherwise, working with the Android for Work apps in the App Catalog is the same as for any other platform:

- you can mark an app as Featured
- you can assign an app to one or more Categories
- you must apply an app to a label to make it available to users.

You can choose or change the “**Install this app for Android for Work**” setting for each app in the app’s details, on the App Catalog page, at any time.

About app configurations

App configurations (also referred to as app restrictions) are key-value pair settings that are provided by the app developer. When you select the “**Install this app for Android for Work**” setting when adding an app, the **Configurations** section appears in the app wizard.

Refer to the app’s documentation and help hints for information on the configuration settings.

Substitution variables for configuring apps

Substitution variables can be used for configuring values from LDAP or the MobileIron Core devices database, such as $EMAIL$ for the email address.

You may use the following variables when configuring any Android for Work app:

```
$USERID$
$EMAIL$
$PASSWORD$
$FIRST_NAME$
```

```
$LAST_NAME$
$DISPLAY_NAME$
$USER_DN$
$USER_UPN$
$USER_LOCALE$
$DEVICE_UUID$
$DEVICE_UUID_NO_DASHES$
$DEVICE_IMSI$
$DEVICE_IMEI$
$DEVICE_SN$
$DEVICE_ID$
$DEVICE_MAC$
$DEVICE_CLIENT_ID$
$USER_CUSTOM1$
$USER_CUSTOM2$
$USER_CUSTOM3$
$USER_CUSTOM4$
$MI_APPSTORE_URL$
$REALM$
$TIMESTAMP_MS$
$NULL$
```

Substitution variable for certificate aliases

Some apps including Divide Productivity and Pulse Secure use SCEP certificates and accept certificate aliases in the app configuration. The substitution variable to provide a SCEP certificate alias is:

`$CERT_ALIAS:<certificate config name>$` where

`<certificate config name>` is the name you gave to the SCEP configuration.

To use a certificate with apps, in the Core Admin Portal:

1. Go to **Policies & Configs > Configurations**
2. Locate your SCEP certificate. Note its name. You will need the name for the alias variable.
3. Ensure the SCEP certificate is assigned to a label that is also used for distributing the apps that require the certificate.
4. Go to **Apps > App Catalog**.
5. Edit the app by clicking the app name, then clicking **Edit**.
6. Ensure that the Android for Work setting "**Install this app for Android for Work**" is selected.
7. In the **Configurations** section, type in the SCEP certificate alias in the field that requires it:

   ```
   $CERT_ALIAS:<name of certificate config>$
   ```
8. Click **Finish** to save your changes.

Deploying public, private, and private channel apps

Public apps are apps that are available to the general public in the Google Play Store.

Private apps are apps developed for your organization in-house or by 3rd party developers that you distribute privately through Google Play. Only members of your domain have visibility into your private apps.

Private channel apps (not supported) are in-house apps that are hosted on a private server rather than in the Google Play Store. MobileIron Core does not support using a private channel for Android for Work apps.

To add in-house (or “private”) apps, you must use the method described in “Deploying private apps” on page 38. The “In-house” option in the app wizard does not support apps for Android for Work profiles.

Deploying public apps

A public app is available in the public Google Play store. You can add public apps to the App Catalog using either of two methods:

- the app wizard, which steps you through all options and configurations, or
- Store Import, a fast way to add multiple apps using default settings. (Options and configurations can be edited later as needed.)

To add an app using the app wizard, in the Core Admin Portal:

1. Go to **Apps** > **App Catalog.**
2. Click **Add+.**
3. Click **Google Play**
4. Enter a name or bundle ID in the Application Name field.
5. Click **Search**.
6. The search results from Google Play Store appear below.
7. Click the row to select the desired app.
8. Click **Next**.
9. Fill out the rest of the fields in the app wizard. To make the app available to Android for Work profiles, select “**Install this app for Android for Work**”.
10. **App Configurations** may appear. Configurations are determined by the app developer and are key-value pairs unique to each app. Fill out the configurations sections as needed. Refer to the app’s documentation.
11. Click **Finish**.
12. Select the app in the App Catalog.
13. Click **Actions** > **Apply to Label**. Select the appropriate labels to make the app available to device users.

To add an app using Quick Import:

1. Go to **Apps** > **App Catalog.**
2. Click **Quick Import** > **Google Play.**
3. Enter any part of an application name or bundle id.

4. Click **Search**. Search results from the Google Play Store appear.
5. Click **Import**, at the end of the line, to add the app to the App Catalog.
6. The store import dialog remains open so you can quickly search and add more apps.
7. Click **X** to close the dialog.
8. Next, edit the app details for the imported app and select **Install this app for Android for Work**. See also : "Editing app details" on page 40.
9. Fill out the Android for Work-related restrictions as necessary.
10. Click **Save**.

All apps that are available to be installed for Android for Work (for which you have selected **Install this app for Android for Work**) have the "suitcase" badge on their icon. These apps can also be installed on non-Android for Work devices.

Deploying private apps

A private app is an app developed for your organization in-house or by 3rd party developers that you distribute privately through Google Play. Your private Google Play store-hosted apps are available to users of your domain only.

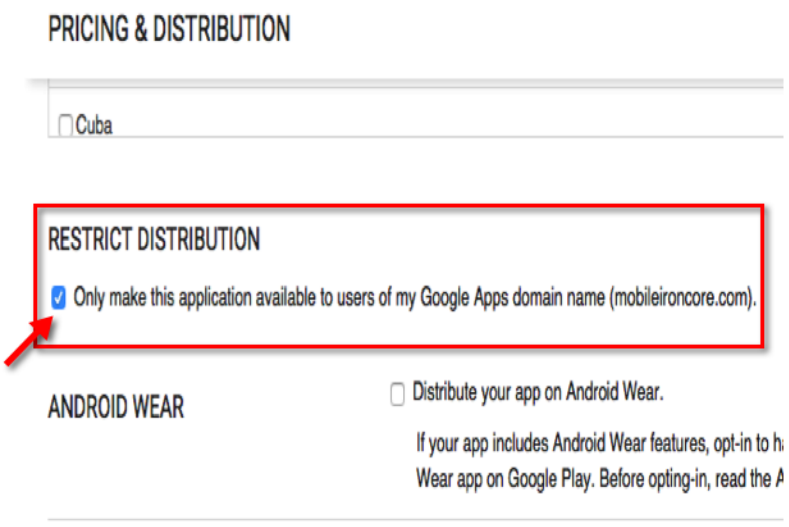
The high-level steps to deploy a private app are:

1. Publish your app on Google Play to domain users only
2. Manually add the app to Core's App Catalog using the package name

Publishing your private app on Google Play

These steps are performed on Google's websites.

1. You must be registered as a Google developer.
2. Follow Google's instructions to publish the app on Google Play.
3. To make it available privately to your domain users, for "Pricing & Distribution" choices, under "Restrict Distribution" check the choice "**Only make this application available to users of my Google Apps domain name** (<your domain name appears>)" on the Google site.



PRICING & DISTRIBUTION

□ Cuba

RESTRICT DISTRIBUTION

☑ Only make this application available to users of my Google Apps domain name (mobileironcore.com).

ANDROID WEAR

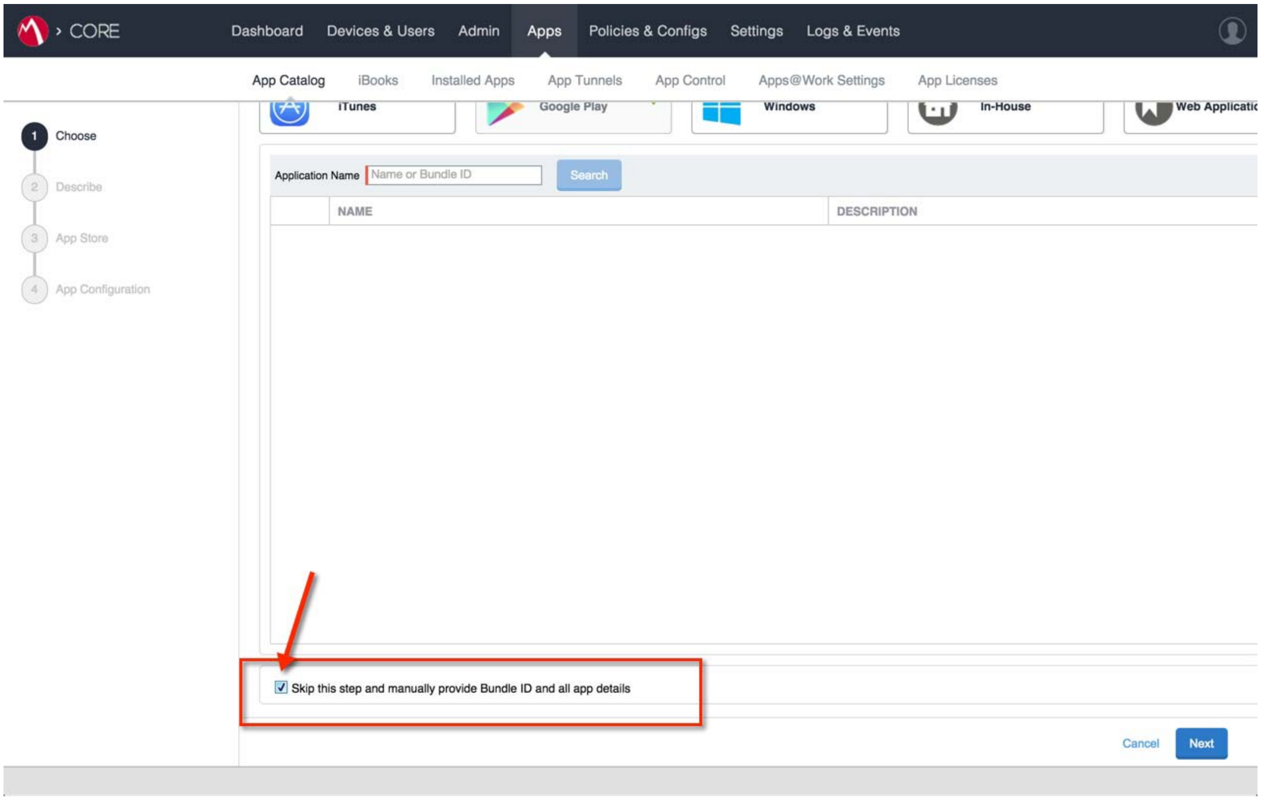
□ Distribute your app on Android Wear.

If your app includes Android Wear features, opt-in to h
Wear app on Google Play. Before opting-in, read the A

Adding your private app to Core's App Catalog

In Core Admin Portal:

1. Go to **Apps** > **App Catalog.**
2. Click **Add+**.
3. Click **Google Play**.
4. Scroll down to the bottom of the page and select the checkbox for **Skip this step and manually provide Bundle ID and all app details.**



☑ Skip this step and manually provide Bundle ID and all app details

5. Click **Next**.
6. Fill out the New App information. Note: You must provide the app's package name.
7. Complete the remaining steps of the app wizard and click **Finish**.
8. Select the app in the App Catalog.
9. Click **Actions** > **Apply to Label,** and select the appropriate labels to make this app available to device users.

Private Channel apps are not supported

Private channel apps are in-house apps that are hosted on a private server rather than on the Google Play store. MobileIron Core does not support using a private channel for Android for Work apps.

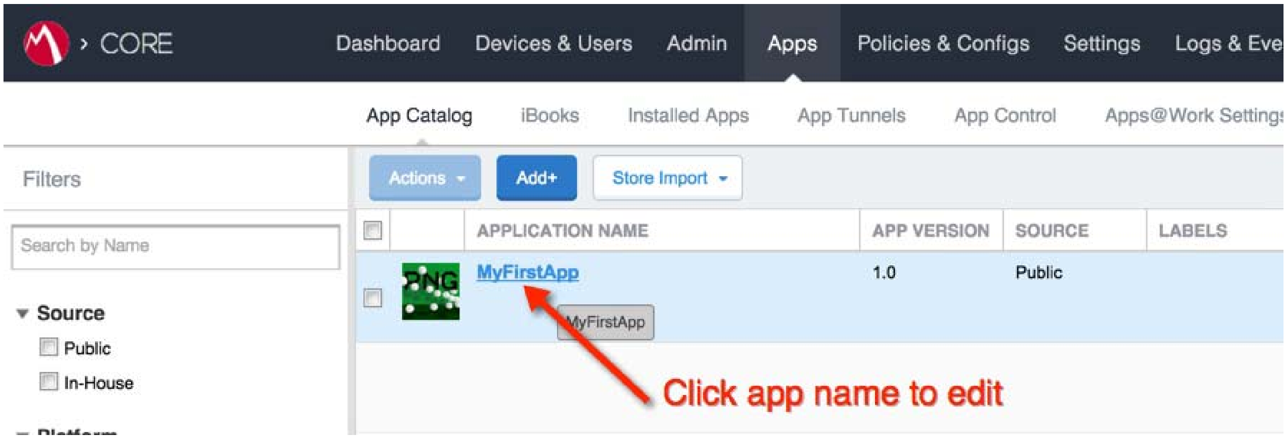
To add in-house apps, you must use the method described in "Deploying private apps" on page 38. The "In-house" option in the app wizard does not support apps for Android for Work profiles.

Editing app details

You can edit app details anytime after you have added an app to the App Catalog.

To edit the app details:

- click the app name (which is a link),
- then click **Edit**.



□		APPLICATION NAME	APP VERSION	SOURCE	LABELS
□		MyFirstApp	1.0	Public	

Click app name to edit

How to deploy Divide Productivity with Android for Work

Divide Productivity is a PIM app you can deploy to Android for Work devices. It provides a set of business apps that includes email, calendar, contacts, tasks, and downloads.

To deploy Divide Productivity:

1. Go to **Apps** > **App Catalog**.
2. Click **Add+.**
3. Click **Google Play.**
4. In the **Application Name** field, type “Divide Productivity” and click **Search.**
5. Look for Divide Productivity app in the list of results. Click the row to select it.
6. Click **Next.**
7. For **Min. OS Version**, select “5.0”.
8. Optionally, add this app to a **Category.**
9. Click **Next**
10. In the **Android for Work** section, select **Install this app for Android for Work.**
    Additional fields appear. Select the options using the following guidelines:

Setting	**Description**
Silently Install	Select this to install the app on the user’s device without requiring any action from the user.
Block Uninstall	Prevents user from uninstalling the app. (Selected by default if **Silently Install** is selected.)
By distributing this app you will accept the following permissions on behalf of users	Select this option to accept app permissions on behalf of users. (Required)

11. In the Configurations section, use the following guidelines to enable options. Note that Configurations are determined by the app developer.

Setting	**Description**
Email Address	Use substitution variables to define the email address (for example $EMAIL$)
Password	Use substitution variables to define the password (for example $PASSWORD$)
Host	Enter the host name of the mail server to use. Enter the fully qualified domain name of the ActiveSync server. If you are using a Standalone Sentry, enter its fully qualified domain name (FQDN) instead. Example: mySentry.mycompany.com Port 443 is assumed, if not included.
Server Type	Select the type of mail server.

Setting	Description
Username	Use variables to define the username for the email account.
Is Ssl Required	Select if you want secure communication using https: to the server that you specified in the Host field.
Trust All Certificates	Select only if you want the app to automatically accept untrusted certificates. Typically, you select this option only when working in a test environment.
Default Email Signature	Enter the default email signature for all emails. The end user can change this at any time. Once the device user changes it, later changes to this field have no effect.
Email Max Attachment Size	Enter the maximum size allowed for attached files.
Enable Tasks	Select to synchronize tasks.
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: `$CERT_ALIAS:<certificate config name>`
Smime Signing Certificate Alias	The value should be a string alias representing an SMIME signing certificate stored in the work profile keystore.For example: `$CERT_ALIAS:<certificate config name>`
Smime Encryption Certificate Alias	The value should be a string alias representing an SMIME encryption certificate stored in the work profile keystore. For example: `$CERT_ALIAS:<certificate config name>`

12. Click **Finish**.
13. Select the checkbox next to Divide Productivity in the table.
14. Click **Actions > Apply to Labels.** Select labels that are applied to Android for Work devices.