

MobileIron Core UEM 10.5 & Knox Platform for Enterprise

July 2020
Samsung R&D Centre UK
(SRUK)

1. Pre-requisites for Knox Platform for Enterprise
2. Configure Android Enterprise
3. Android Enterprise Deployment Modes
 - BYOD
 - Company-owned Device
 - Fully Managed Device with a Work Profile
 - Dedicated Device
4. Managed Google Play [MGP] Configuration
5. AppConfig in MobileIron Core UEM
6. Configure Knox Platform for Enterprise : Standard Edition
7. Configure Knox Platform for Enterprise : Premium Edition
8. Configure Knox Service Plugin [KSP]

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

<https://help.mobileiron.com/>

1. Obtain access to MobileIron Core UEM console
2. A Gmail account to map to MobileIron Core for Managed Google Play
3. MobileIron Customer Portal Access
4. Consider what enrollment method to use:
 - Knox Mobile Enrollment (KME)
 - QR Code enrollment
 - Email enrollment
 - Server details enrollment

Configure Android Enterprise

- Log into the MobileIron Customer Support Portal. Navigate to: Homepage -> Bottom of page -> (Quick Links) Android Enterprise -> Create New Android Enterprise Enrollment -> Begin

Announcements

→ Community Blog

Trending Articles

MobileIron Eval

Mar 7, 2019

Nic Lechner

261

MobileIron Cloud: Ports, Hosts, and IP Addresses

May 16, 2019

Russell Mohr

228

Resizing Disk Partition of a Core Virtual Machine

Aug 12, 2015

Mike Veinott

214

Quick Links

Ideas

Android Enterprise Enrollment

Whitelist Core Server Hostname

Wrapped Apps

Community Help

Feedback

Android enterprise Enrollments

All

Create New Android Enterprise Enrollment

Search this list...

Android Enterprise Enrollment...	Domain	Created By	Created Date
1	SAMSUNG TEST	Nikhil Kamdar	3/27/2019 2:52 PM

Android enterprise Enrollment

Android enterprise Setup - Step 1

Recommended Setup Method (This recommended method is not supported prior to Core 9.2)

Use this method if you do not have a Google Managed Domain. Device users will be provisioned with Google automatically to gain access to Android enterprise. This method does not require the device user to enter a password to authenticate with Google to use Android enterprise. If you do have a Google Managed Domain, please use the alternate method. This recommended method is not supported prior to Core 9.2.

Begin

Alternate Setup Method

Use this method if you have a Google Managed Domain. A managed domain requires you to provision device users manually to gain access to Android enterprise or to sync users between your LDAP directory and Google with Google App Directory Sync (GADS). Choose this option if you are a current Google for Work subscriber and you have already set up the required infrastructure.

Use Alternate Setup

Configure Android Enterprise

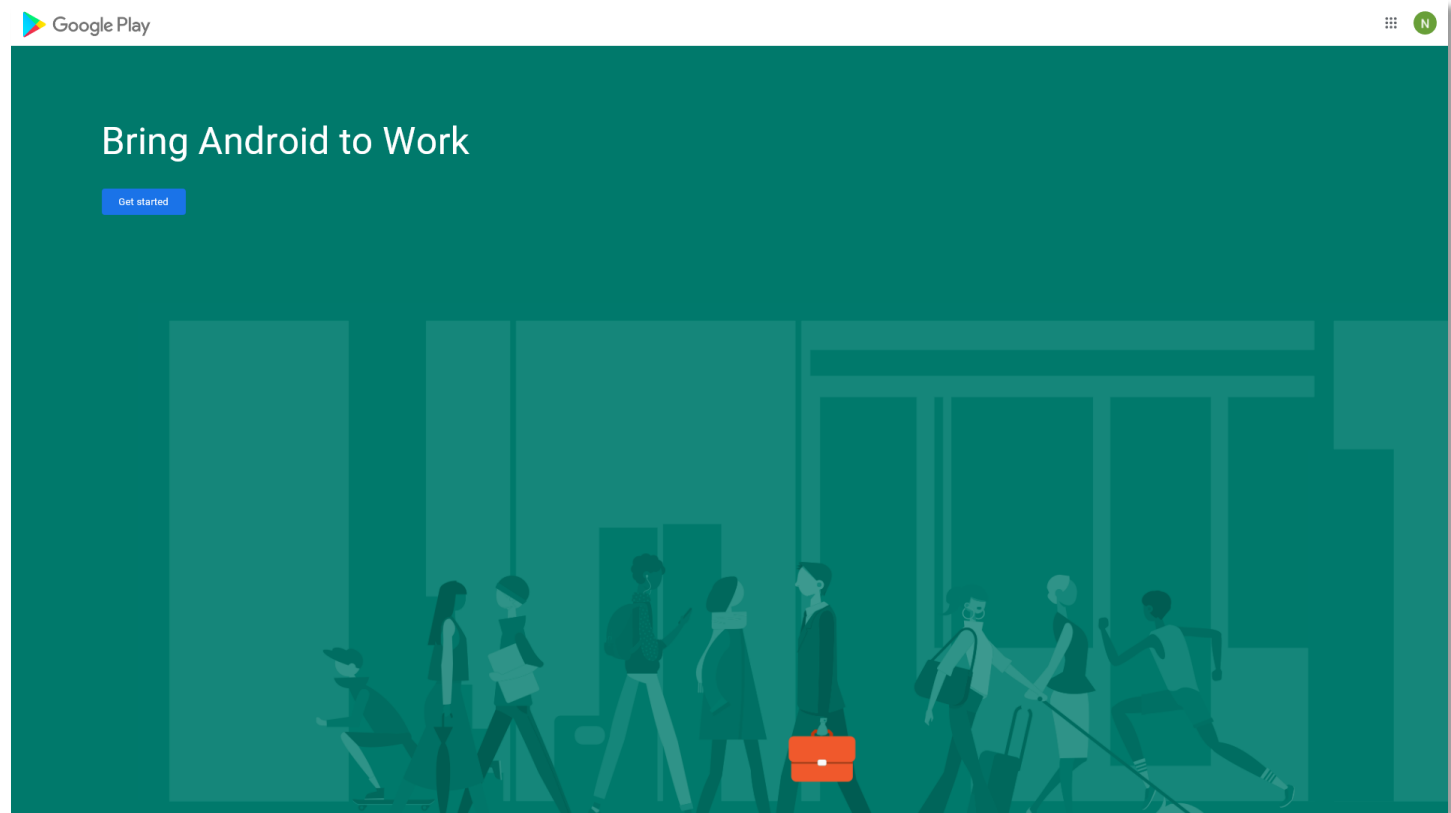
- Click on submit and make sure that you have signed into the Google Account that you would wish to bind.
- MobileIron Customer Support Portal will forward you to the Google Android Enterprise binding page. Click 'Get started'

Android enterprise Enrollment

Android enterprise Setup - Step 2

Choose which brand you are associating your Google account to. When you click Submit, you will be redirected to a Google site to authenticate to your Google account with your Google credentials and to agree to EMM association. After you accept Google's agreement, you will be returned to Salesforce to download your JSON file to register to Core. NOTE: DO NOT lose this file. It contains your private key. Google and Salesforce do not keep a copy of the file.

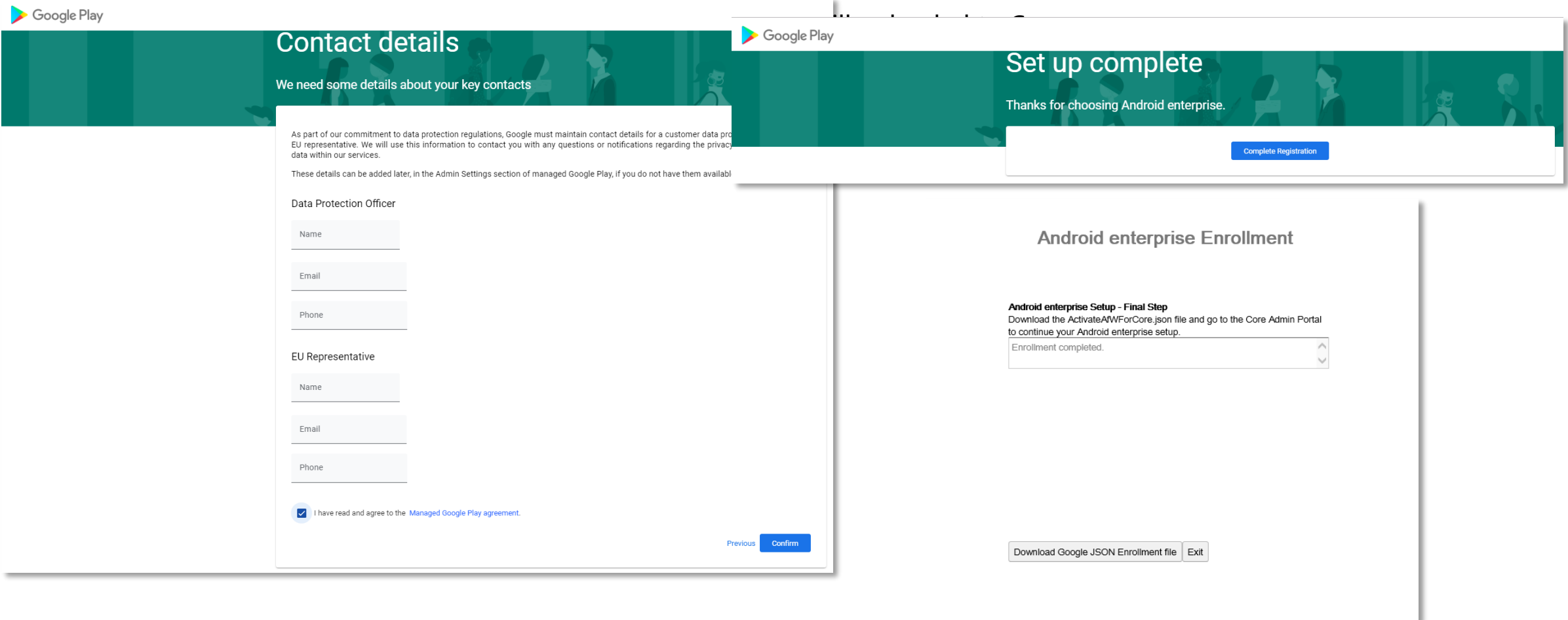
CancelSubmit



Configure Android Enterprise

Configure Android Enterprise

- Fill out the Contact details page, tick the Managed Google Play agreement page and then select Confirm. These text fields are not mandatory, so you can alternatively leave them blank and just tick the Managed Google Play agreement and then select Confirm.
- Click Complete Registration to complete the Android Enterprise configuration and return to MobileIron Customer Support Portal.



The image displays two screenshots of the Google Play Android Enterprise configuration interface. The left screenshot shows the 'Contact details' page, which includes a header with the Google Play logo and the title 'Contact details'. Below the header, there is a sub-header 'We need some details about your key contacts' and a paragraph explaining that Google must maintain contact details for a customer data protection EU representative. A note states that these details can be added later in the Admin Settings section. The form contains two sections: 'Data Protection Officer' and 'EU Representative', each with input fields for Name, Email, and Phone. At the bottom, there is a checkbox labeled 'I have read and agree to the Managed Google Play agreement.' and a 'Confirm' button. The right screenshot shows the 'Set up complete' page, which has a header with the Google Play logo and the title 'Set up complete'. Below the header, there is a sub-header 'Thanks for choosing Android enterprise.' and a 'Complete Registration' button. Below this, there is a section titled 'Android enterprise Enrollment' with a sub-header 'Android enterprise Setup - Final Step'. The text in this section instructs the user to download the ActivateAWForCore.json file and go to the Core Admin Portal to continue the setup. A status box shows 'Enrollment completed.' with up and down arrows. At the bottom, there are two buttons: 'Download Google JSON Enrollment file' and 'Exit'.

Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection EU representative. We will use this information to contact you with any questions or notifications regarding the privacy of data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available.

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

☒ I have read and agree to the [Managed Google Play agreement](#).

[Previous](#) [Confirm](#)

Set up complete

Thanks for choosing Android enterprise.

[Complete Registration](#)

Android enterprise Enrollment

Android enterprise Setup - Final Step

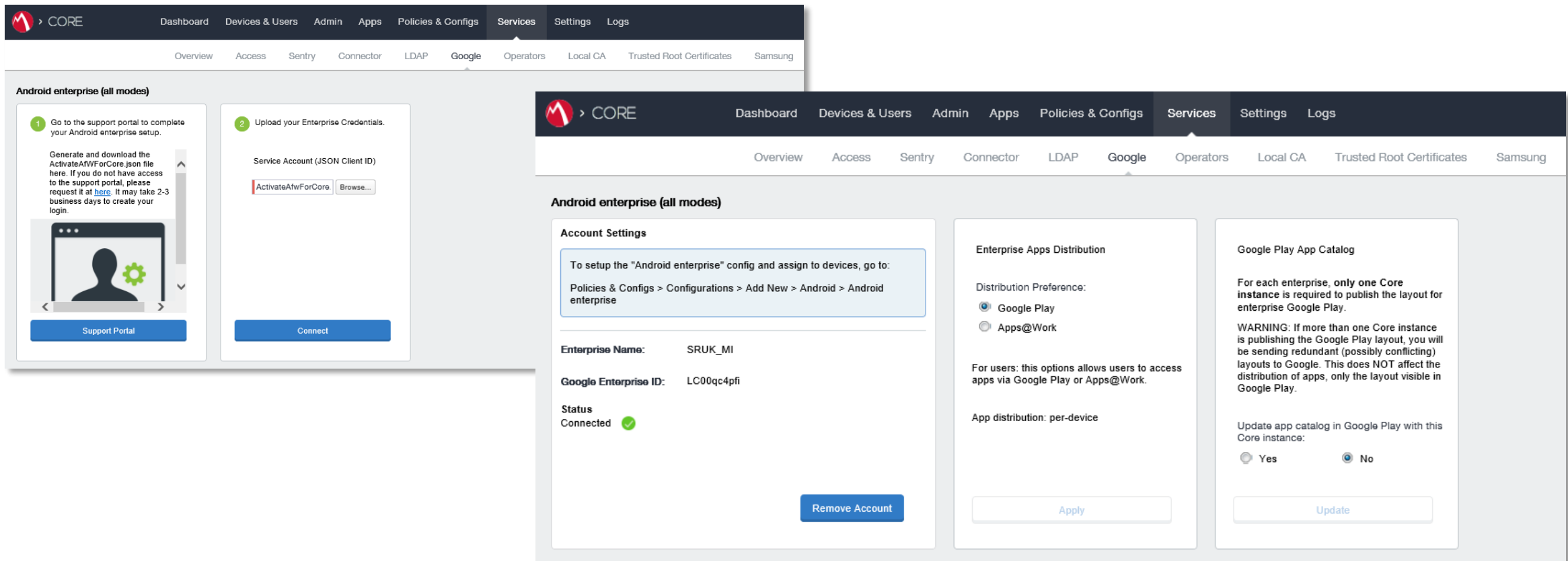
Download the ActivateAWForCore.json file and go to the Core Admin Portal to continue your Android enterprise setup.

Enrollment completed.

[Download Google JSON Enrollment file](#) [Exit](#)

Configure Android Enterprise

- Log into the MobileIron UEM console and navigate to Services -> Google
- Here you can bind MobileIron to Android Enterprise using the JSON file created in the last step.
- Once the JSON file has been selected under 'Upload your Enterprise Credentials' and then 'Connect' Android Enterprise is bound.



The image displays two screenshots of the MobileIron UEM console interface, specifically the 'Services' section under 'Google'.

Left Screenshot: Shows the initial setup steps for Android Enterprise.

- Step 1:** "Go to the support portal to complete your Android enterprise setup." It includes instructions to generate and download the 'ActivateAfwForCore.json' file from the support portal. A "Support Portal" button is visible.
- Step 2:** "Upload your Enterprise Credentials." It shows a field for "Service Account (JSON Client ID)" with a "Browse..." button and a "Connect" button.

Right Screenshot: Shows the configuration page after the account is connected.

- Account Settings:** Displays the "Enterprise Name" (SRUK_MI), "Google Enterprise ID" (LC00qc4pfi), and "Status" (Connected with a green checkmark). A "Remove Account" button is at the bottom.
- Enterprise Apps Distribution:** Shows "Distribution Preference" with radio buttons for "Google Play" (selected) and "Apps@Work". It includes a note: "For users: this options allows users to access apps via Google Play or Apps@Work." and "App distribution: per-device". An "Apply" button is at the bottom.
- Google Play App Catalog:** Includes a warning: "For each enterprise, only one Core instance is required to publish the layout for enterprise Google Play." and a "WARNING: 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." Below this, there is a section "Update app catalog in Google Play with this Core instance:" with radio buttons for "Yes" and "No" (selected). An "Update" button is at the bottom.

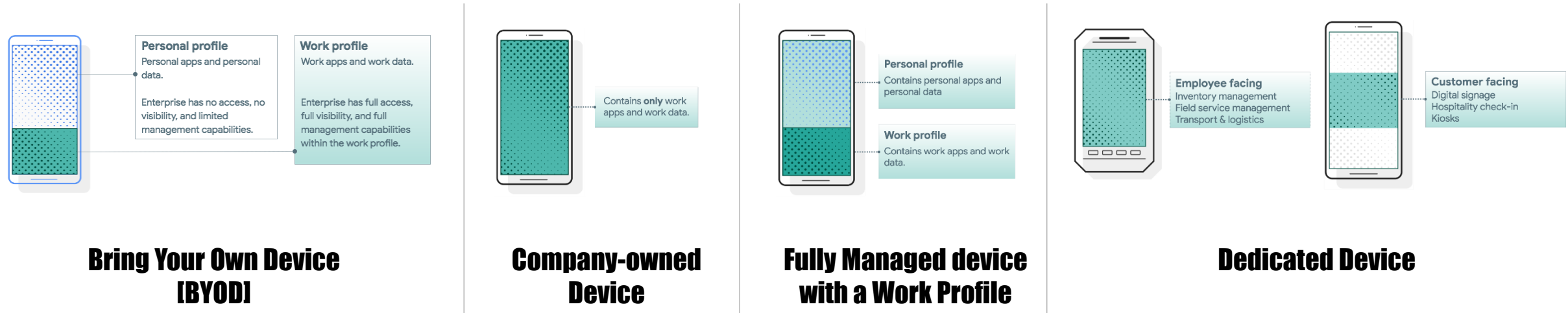
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 4 deployment modes

1. **BYOD** [*formerly known as Profile Owner*]
2. **Company-owned Device** [*formerly known as Device Owner*]
3. **Fully Managed device with a work profile** [*formerly known as COMP*]
4. **Dedicated device** [*formerly known as COSU*]

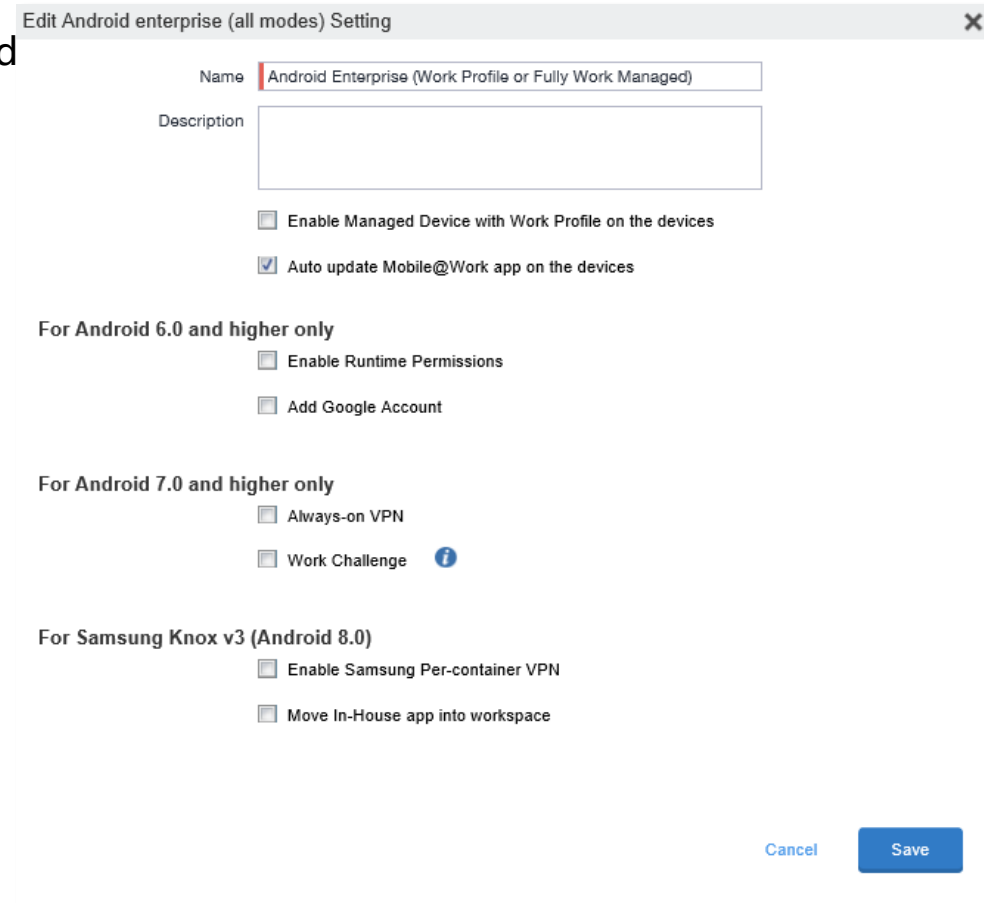
MobileIron UEM can support **all** 4 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in MobileIron UEM for your device fleet.



Android Enterprise BYOD Deployment

To enroll a device in the Android Enterprise BYOD deployment type, you simply need to create a 'Android Enterprise Setting' configuration.

- Go to *Policies & Configs* -> *Configurations* -> *Add New* -> *Android* -> *Android Enterprise*
- Give the configuration a name and save it.
- By having this config, it enabled BYOD and Company-owned
- Apply this config to a label.



Edit Android enterprise (all modes) Setting

Name

Description

☐ Enable Managed Device with Work Profile on the devices

☒ Auto update Mobile@Work app on the devices


For Android 6.0 and higher only

☐ Enable Runtime Permissions

☐ Add Google Account

For Android 7.0 and higher only

☐ Always-on VPN

☐ Work Challenge 

For Samsung Knox v3 (Android 8.0)

☐ Enable Samsung Per-container VPN

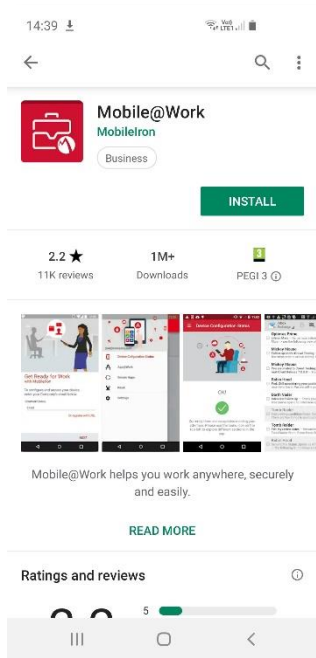
☐ Move In-House app into workspace

Cancel Save

Android Enterprise BYOD Deployment

Now all you simply need to do is enroll your device by completing the following:

- On your device, go to the Google Play Store, download the Mobile@Work client, and enroll your device into MobileIron.



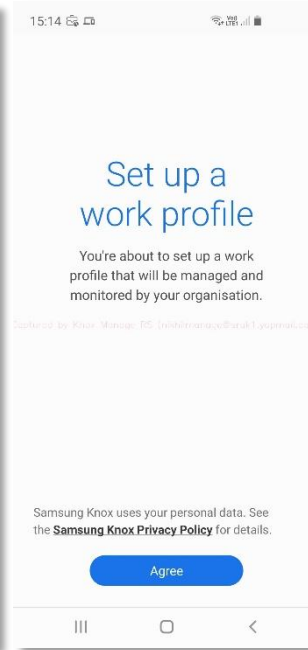
Install Mobile@Work client



Enter server URL
& hit NEXT



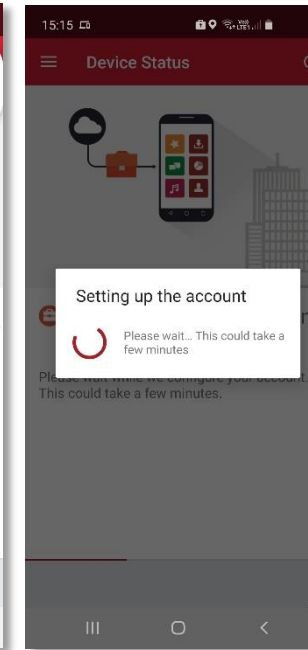
Enter credentials
& hit SIGN IN



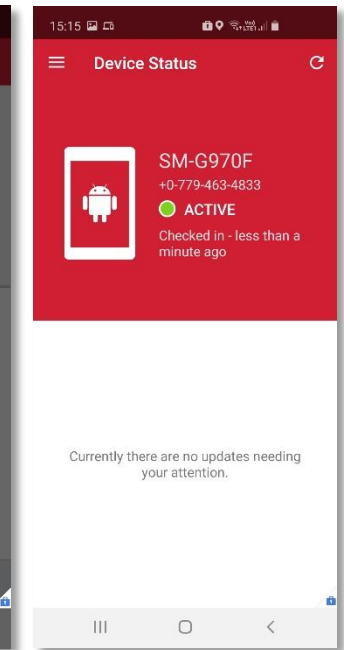
Create
Work Profile by clicking
Agree



Creating
Work Profile



Setting up Managed
Google Play Account



Device Enrollment
Successful!

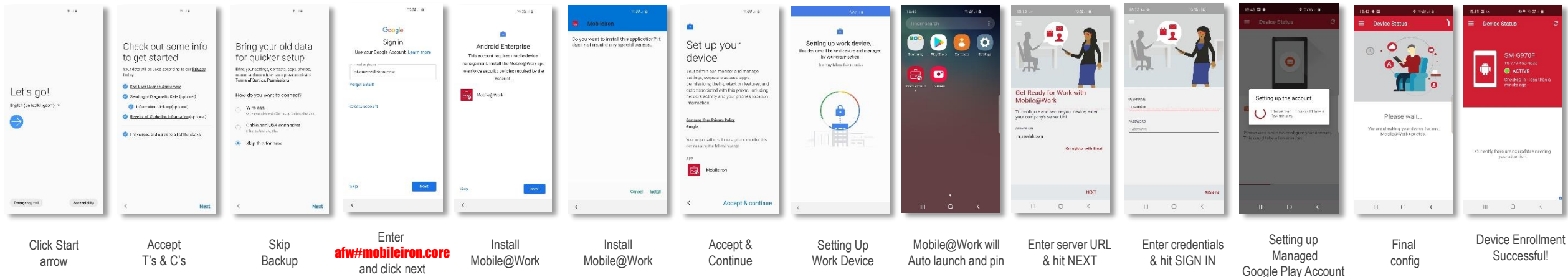
Android Enterprise: Company-owned Device

Android Enterprise Company-owned Device Deployment

To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into MobileIron Core UEM as an Android Enterprise Company-owned device. Use the same 'Android Enterprise Setting' configuration but start from a factory reset device.

1. DPC Identifier [Also known as the hashtag method] **afw#mobileiron.core**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

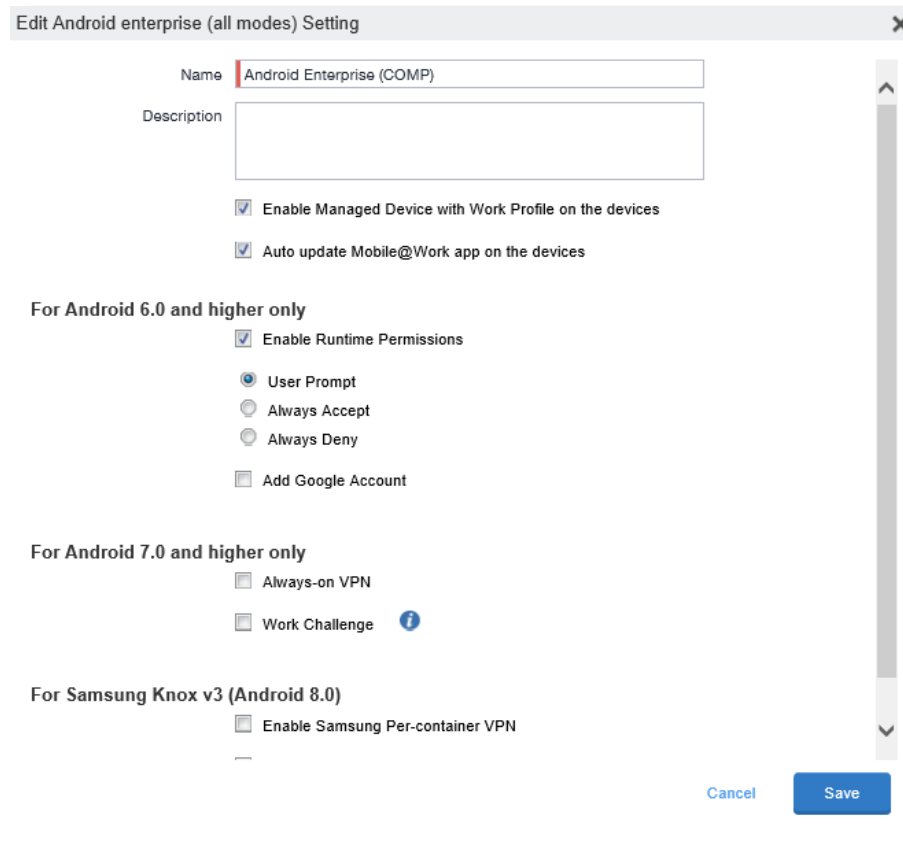
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Android Enterprise Fully Managed Device with a Work Profile Deployment

To enroll a device in the Android Enterprise Fully Managed Device with a Work Profile Deployment type, the final pre requisites is to modify the 'Android Enterprise Setting' configuration to look like the below...

- You must click on the checkbox 'Enable Managed Device with Work Profile on the devices'
- This needs to be in a separate 'Android Enterprise Setting' configuration if you need more than one set of devices enrolling as 'Company-owned Devices' & 'Fully Managed Device with a Work Profile'.



Edit Android enterprise (all modes) Setting

Name

Description

☒ Enable Managed Device with Work Profile on the devices

☒ Auto update Mobile@Work app on the devices

For Android 6.0 and higher only

☒ Enable Runtime Permissions

☒ User Prompt


☐ Always Accept

☐ Always Deny

☐ Add Google Account

For Android 7.0 and higher only

☐ Always-on VPN

☐ Work Challenge 

For Samsung Knox v3 (Android 8.0)

☐ Enable Samsung Per-container VPN

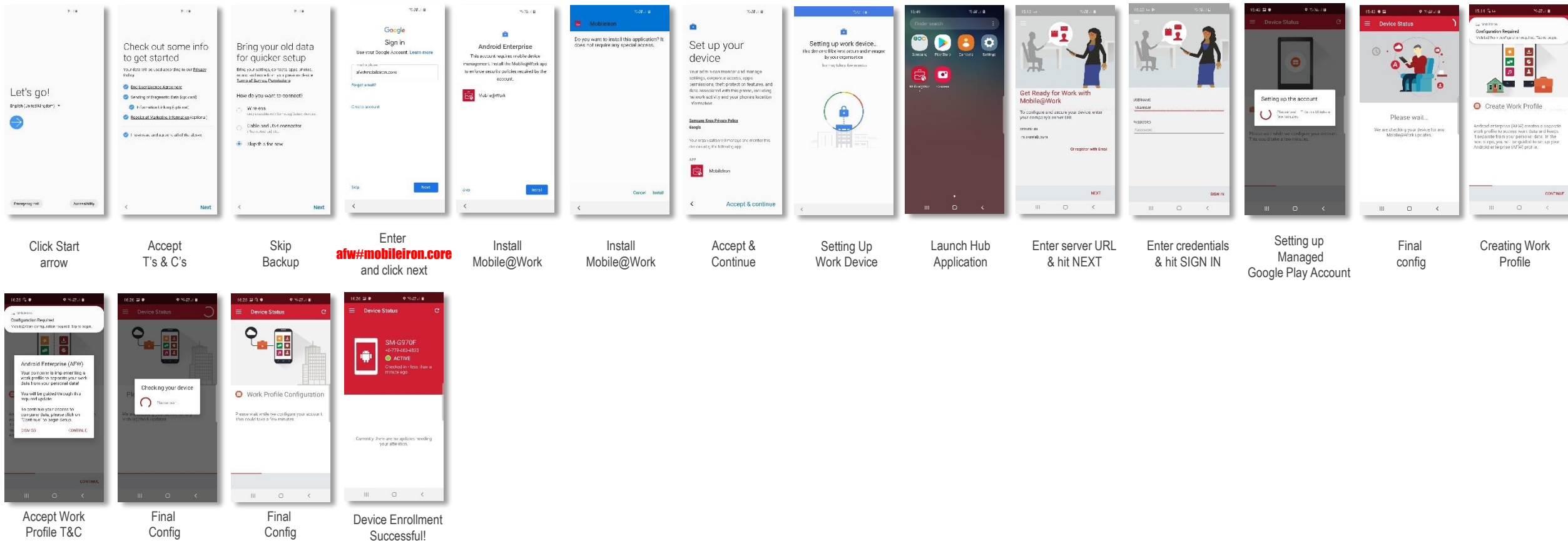
Cancel Save

Android Enterprise: Fully Managed Device with a Work Profile

Android Enterprise Fully Managed Device with a Work Profile Deployment

To enroll your device as an Android Enterprise Fully Managed Device with a Work Profile, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into MobileIron Core UEM as an Android Enterprise Company-owned device.

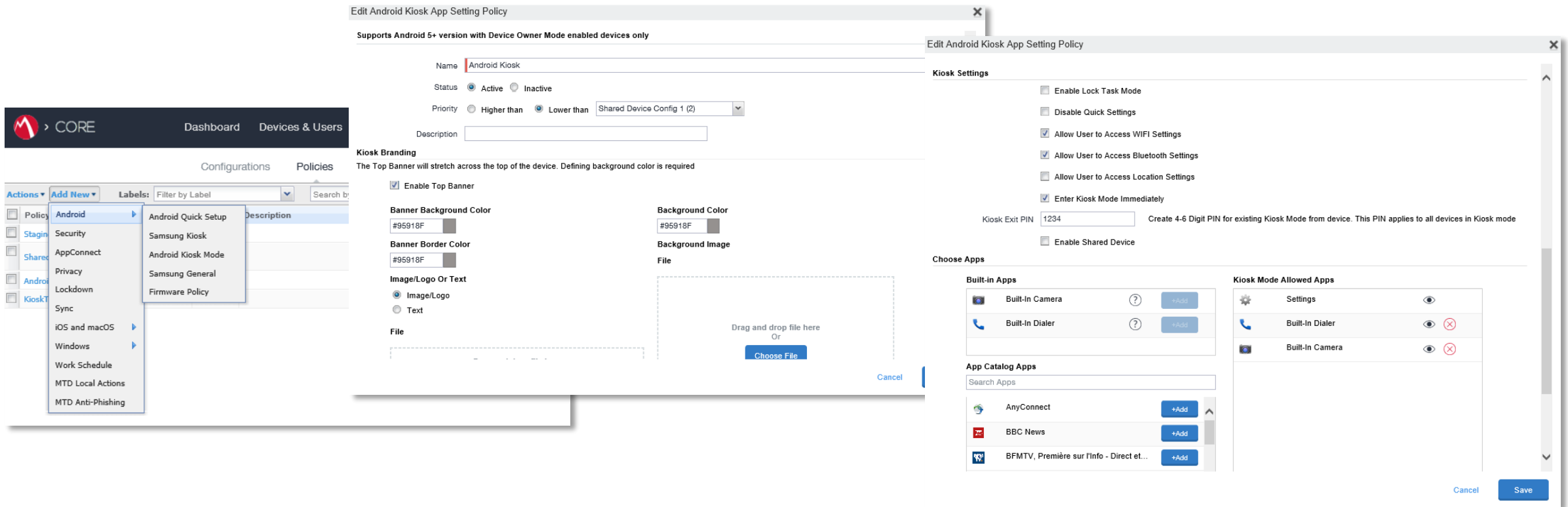
1. DPC Identifier [Also known as the hashtag method] **afw#mobileiron.core**
 2. QR Code Enrollment / NFC Enrollment
 3. Knox Mobile Enrollment
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Android Enterprise Dedicated Device Deployment

To enroll a device in the Android Enterprise Dedicated Device deployment type, you must have the 'Android Enterprise Setting' configuration applied to your label. Also you need to apply the 'Android Kiosk Mode' to your label.

- Go to Policies & configs -> *Policies* -> *Add New* -> *Android* -> *Android Kiosk Mode*
- Here you can configure branding, restrictions and apps that you would like to be in your Android Enterprise Kiosk



The screenshot displays the 'Edit Android Kiosk App Setting Policy' interface, which is used to configure kiosk mode for Android devices. The interface is divided into several sections:

- Header:** 'Edit Android Kiosk App Setting Policy' with a close button.
- Supports:** 'Supports Android 5+ version with Device Owner Mode enabled devices only'.
- Policy Details:**
 - Name:** 'Android Kiosk'
 - Status:** 'Active' (selected) or 'Inactive'.
 - Priority:** 'Higher than' or 'Lower than' (selected) 'Shared Device Config 1 (2)'.
 - Description:** A text input field.
- Kiosk Branding:**
 - Enable Top Banner:** A checkbox that is checked.
 - Banner Background Color:** A color picker set to '#95918F'.
 - Banner Border Color:** A color picker set to '#95918F'.
 - Image/Logo Or Text:** Radio buttons for 'Image/Logo' (selected) and 'Text'.
 - File:** A dashed box for uploading a file, with a 'Choose File' button and a 'Cancel' button.
- Kiosk Settings:**
 - Enable Lock Task Mode:** A checkbox.
 - Disable Quick Settings:** A checkbox.
 - Allow User to Access WIFI Settings:** A checked checkbox.
 - Allow User to Access Bluetooth Settings:** A checked checkbox.
 - Allow User to Access Location Settings:** A checkbox.
 - Enter Kiosk Mode Immediately:** A checked checkbox.
 - Kiosk Exit PIN:** A text input field set to '1234'.
 - Create 4-6 Digit PIN for existing Kiosk Mode from device. This PIN applies to all devices in Kiosk mode:** A text input field.
 - Enable Shared Device:** A checkbox.
- Choose Apps:**
 - Built-in Apps:** A list of built-in apps (Built-In Camera, Built-In Dialer) with '+Add' buttons.
 - App Catalog Apps:** A search bar and a list of apps from the catalog (AnyConnect, BBC News, BFMTV, Première sur l'Info - Direct et...) with '+Add' buttons.
 - Kiosk Mode Allowed Apps:** A list of apps allowed in kiosk mode (Settings, Built-In Dialer, Built-In Camera) with toggle switches.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

Android Enterprise: Dedicated Device

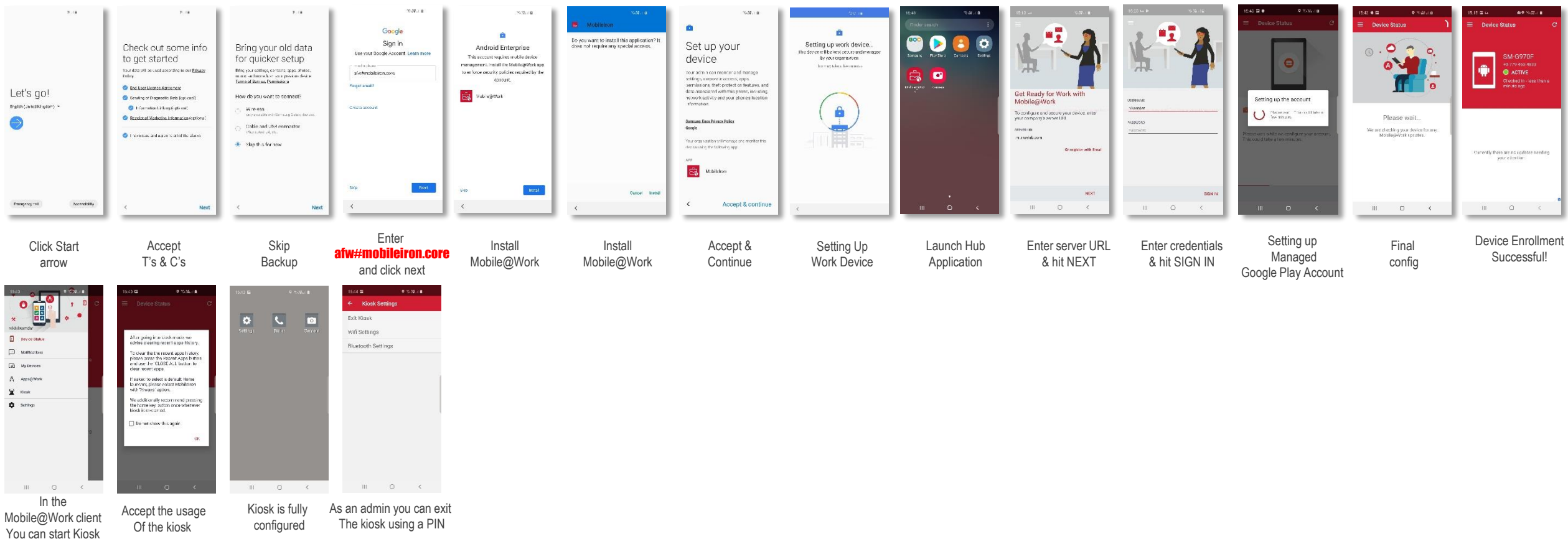
Android Enterprise Dedicated Device Deployment

The Android Enterprise Dedicated Device deployment is part of the Company-owned Device Deployment where the Kiosk is a bolt on feature on top.

Once you have done this you then enroll your device. To enroll your device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into MobileIron UEM as an Android Enterprise Dedicated device.

1. DPC Identifier [Also known as the hashtag method] **afw#mobileiron.core**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Click Start arrow

Accept T's & C's

Skip Backup

Enter **afw#mobileiron.core** and click next

Install Mobile@Work

Install Mobile@Work

Accept & Continue

Setting Up Work Device

Launch Hub Application

Enter server URL & hit NEXT

Enter credentials & hit SIGN IN

Setting up Managed Google Play Account

Final config

Device Enrollment Successful!

In the Mobile@Work client You can start Kiosk

Accept the usage Of the kiosk

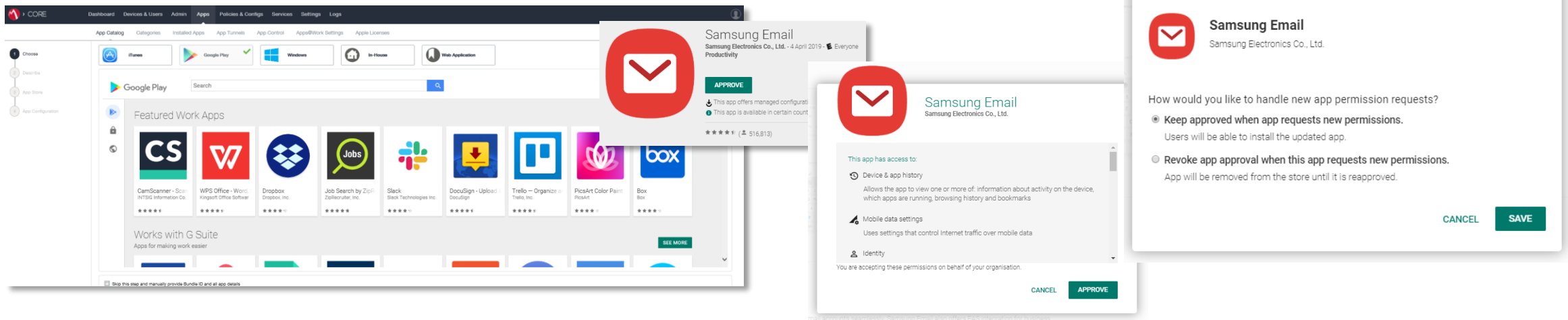
Kiosk is fully configured

As an admin you can exit The kiosk using a PIN

Managed Google Play Configuration

In the Configuring of Android Enterprise section of this document, we completed the majority of the work needed to configure applications to be used for Managed Google Play. MobileIron Core UEM supports the Google iFrame directly within the console. So there is no need to navigate to <https://play.google.com/work> for managing Google play applications.

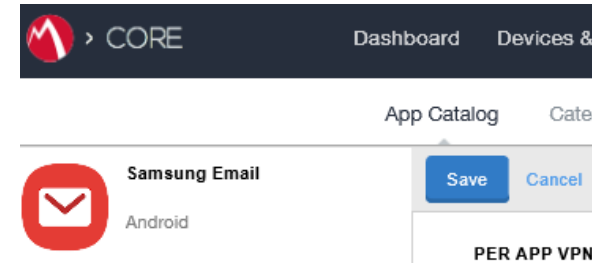
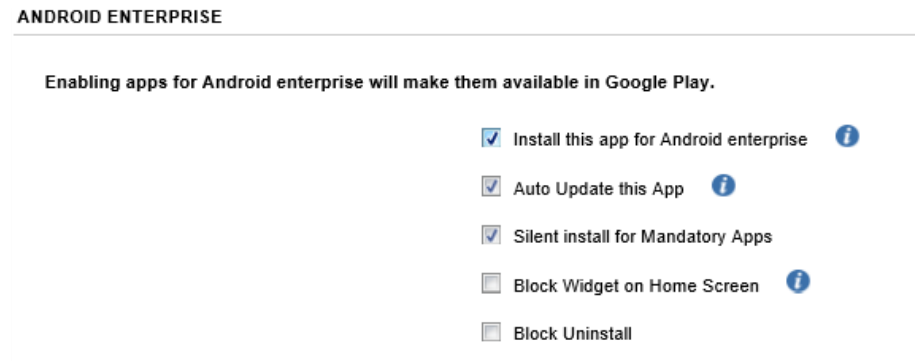
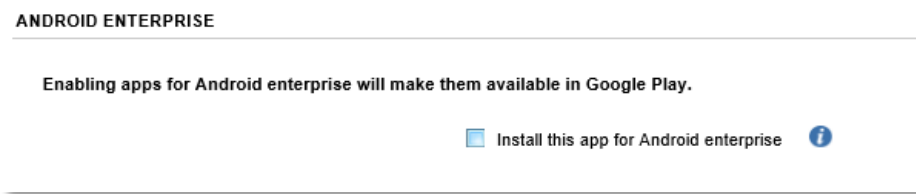
- Navigate to Apps -> Add+ -> Google Play
- Search for the App you want to distribute. For example; Samsung Email
- Click the APPROVE button.
- APPROVE the App Permission request
- Choose how you would like to handle new app permission requests and then click SAVE
- You will now see your app lists in your MobileIron App Catalog
- You must do one more step to make it deployable to an Android Enterprise enabled device.



Managed Google Play Configuration

You must navigate to the target app via Apps -> App Catalog -> Click on app -> Edit -> Scroll to the 'Android Enterprise' section -> select 'Install this app for Android enterprise'

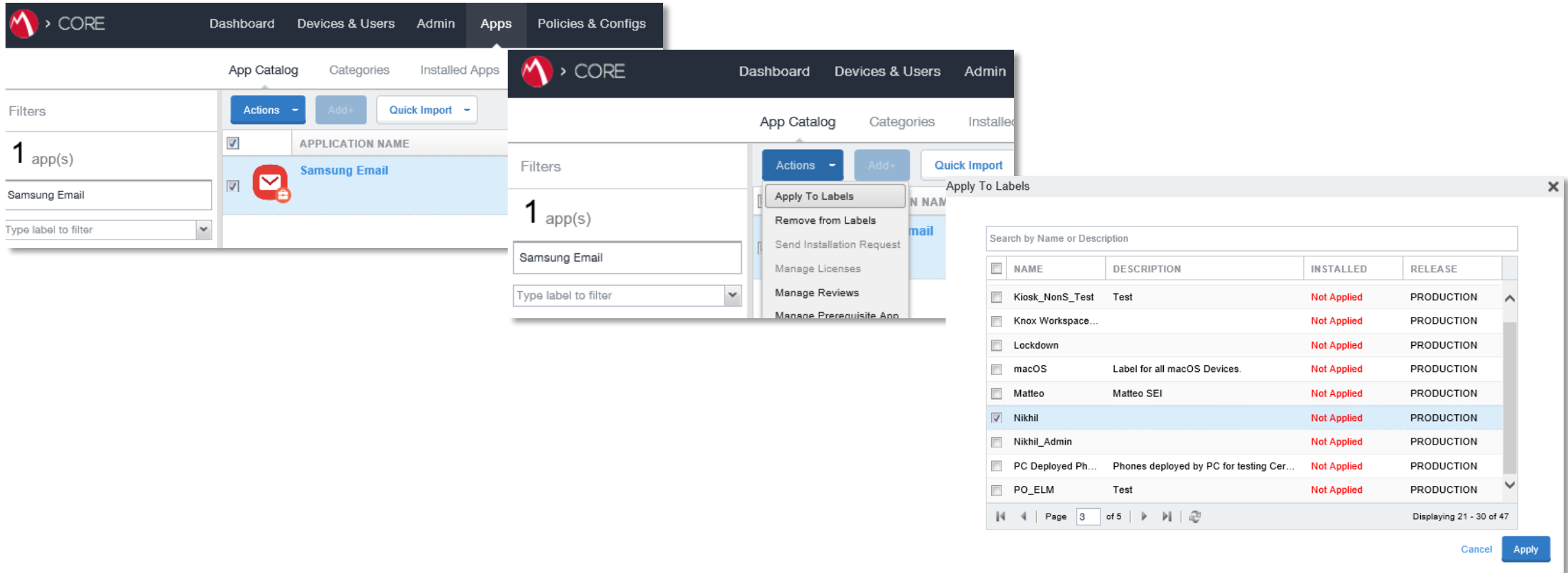
- There are a few configuration you can set for the Android Enterprise app, select what is needed.
- Once the below has been completed, save the config.



Managed Google Play Configuration

Now we have approved an application we would like to distribute in MobileIron Core.

- Simply select the checkbox next to the app then click on Actions -> Apply to Labels -> select your target label -> Apply
- Depending on the app config attributes the app will now automatically start to download and install on the device.



The screenshot illustrates the process of applying an application to a label in the MobileIron Core interface. It shows three overlapping windows:

- App Catalog Window:** Displays a list of applications. The 'Samsung Email' app is selected, and the 'Actions' menu is open.
- Apply To Labels Dialog:** A modal dialog showing a list of labels. The 'Nikhil' label is selected.
- App Details Window:** Shows the details of the 'Samsung Email' app, including its name and a 'Type label to filter' dropdown.

The 'Apply To Labels' dialog contains a table with the following data:

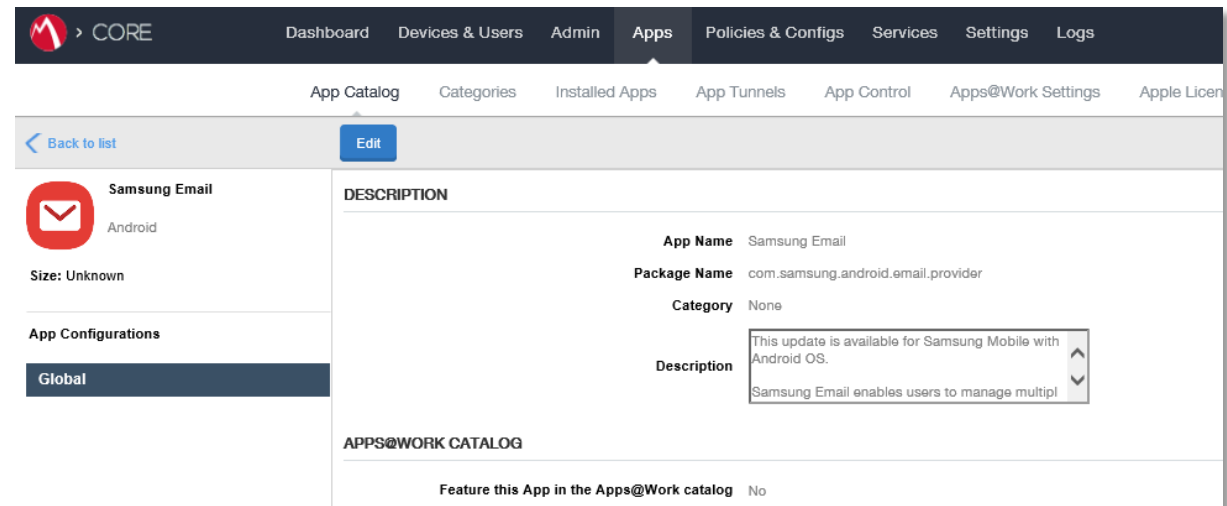
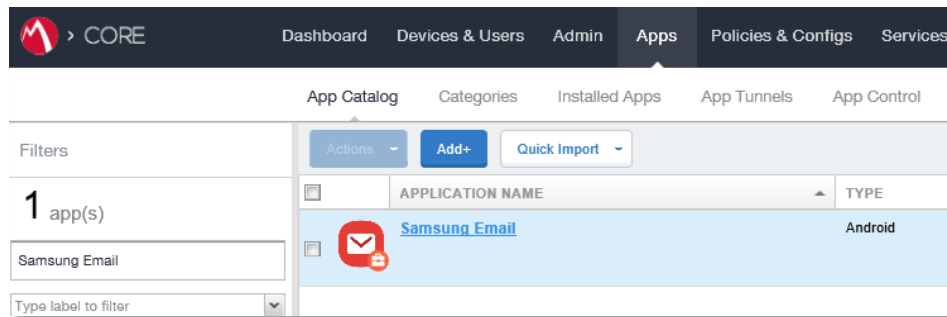
NAME	DESCRIPTION	INSTALLED	RELEASE
Kiosk_NonS_Test	Test	Not Applied	PRODUCTION
Knox Workspace...		Not Applied	PRODUCTION
Lockdown		Not Applied	PRODUCTION
macOS	Label for all macOS Devices.	Not Applied	PRODUCTION
Matteo	Matteo SEI	Not Applied	PRODUCTION
<input checked="" type="checkbox"/> Nikhil		Not Applied	PRODUCTION
Nikhil_Admin		Not Applied	PRODUCTION
PC Deployed Ph...	Phones deployed by PC for testing Cer...	Not Applied	PRODUCTION
PO_ELM	Test	Not Applied	PRODUCTION

The dialog also includes a search bar, pagination controls (Page 3 of 5), and 'Cancel' and 'Apply' buttons.

AppConfig

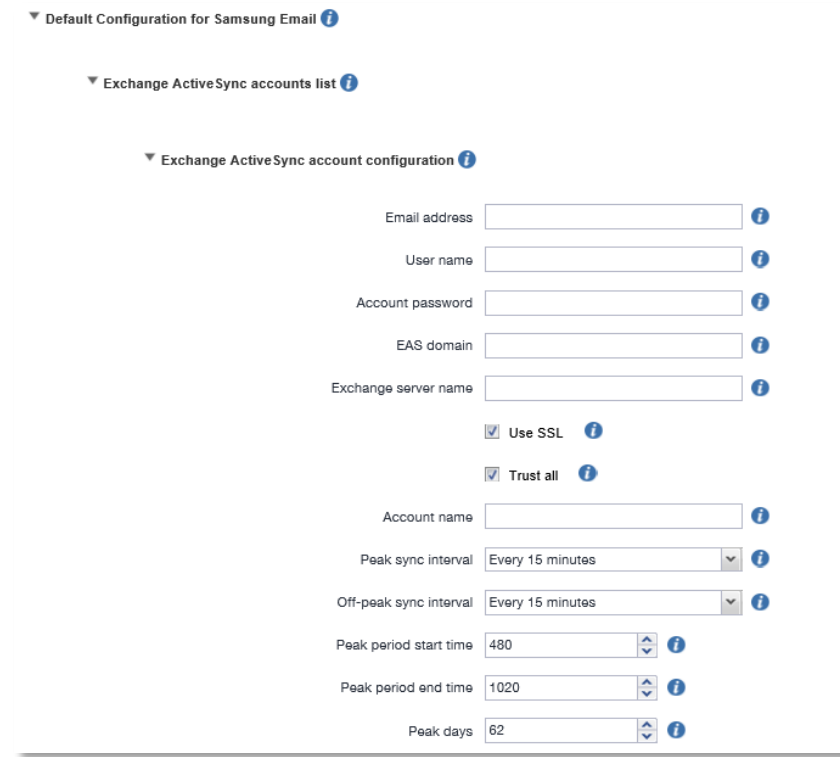
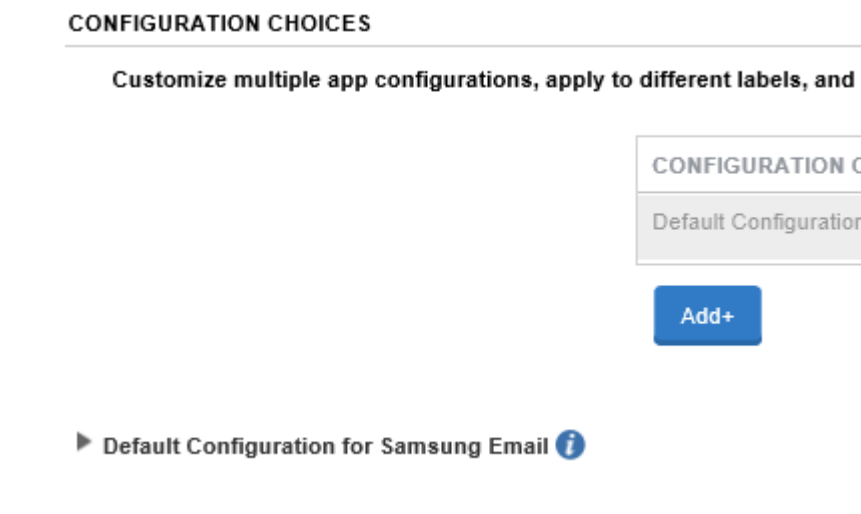
AppConfig enables you to send down application configuration profiles along with your managed apps when you distribute them through your Managed Google Play Store. This saves on having to have the UEM implement the required APIs for the app you are using so you can remotely configure it. To use AppConfig on MobileIron Core UEM, follow the below instructions.

- Navigate to **Apps -> App Catalog -> Click on the app you would like to configure -> Edit**



AppConfig

- Scroll down to the 'Configuration Choices' section
- Expand 'Default Configuration for xxx' & configure the various options you wish and then when you are finished, click the Save button.
- Confirm the assignment by clicking Save. You have now used AppConfig to distribute a Managed Play app with a config profile.



Knox Platform for Enterprise : Standard Edition

The Knox Platform for Enterprise solution provides a robust set of features on top of the core Android Enterprise platform, to fill security and management gaps and meet the strict requirements of highly regulated industries.

The Knox Platform for Enterprise solution comes in a two tiered offering:

- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [\$]

Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise on Oreo or above.

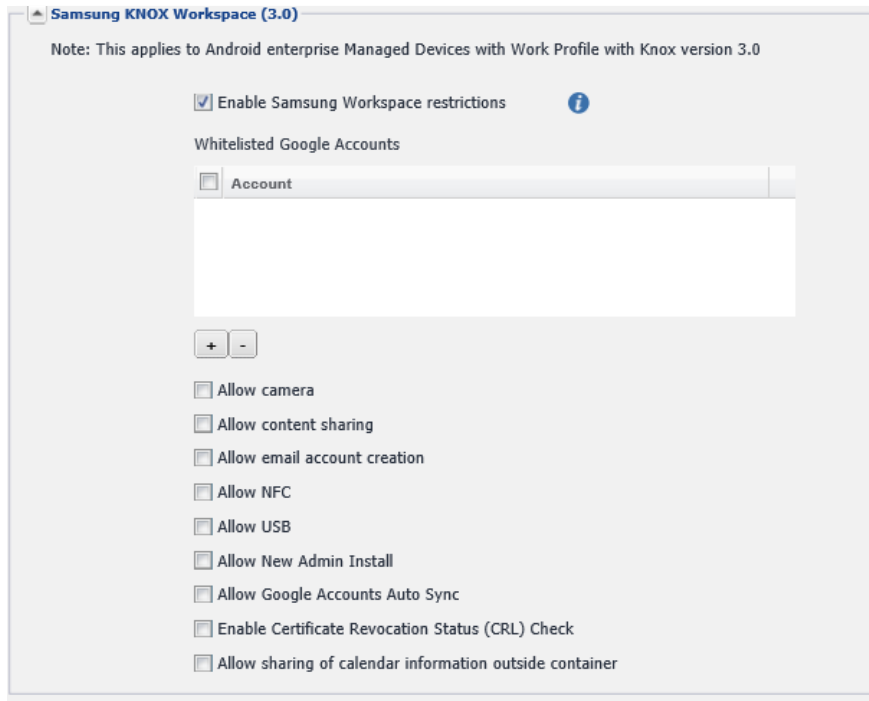


Configure Knox Platform for Enterprise : Standard Edition

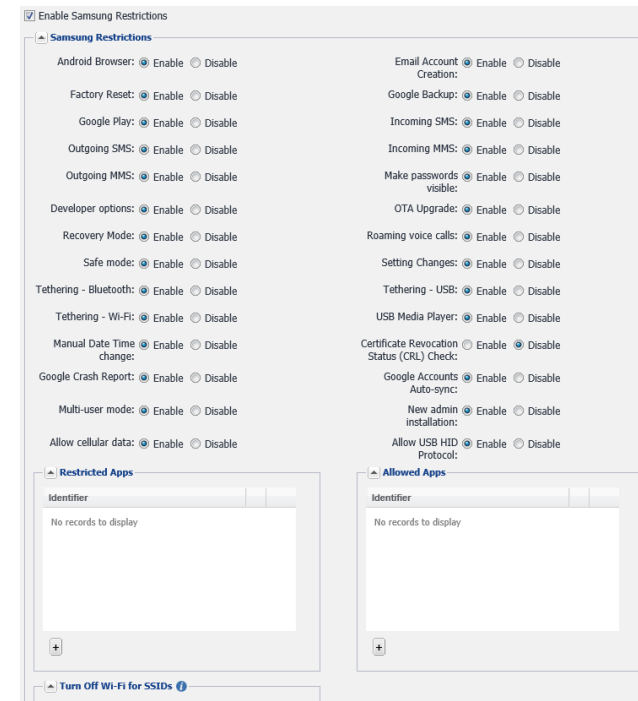
Configure KPE : Standard Edition on MobileIron Core UEM

To take advantage of the free additional APIs available in KPE Standard Edition, simply complete the below instructions.

- Navigate to **Policies & Configs -> Policies > Add New -> Lockdown Policy**
- You have now enabled all the additional KPE Standard APIs available to you in your configuration. You are now free to select those features and take advantage of the free additional APIs found in KPE Standard Edition!



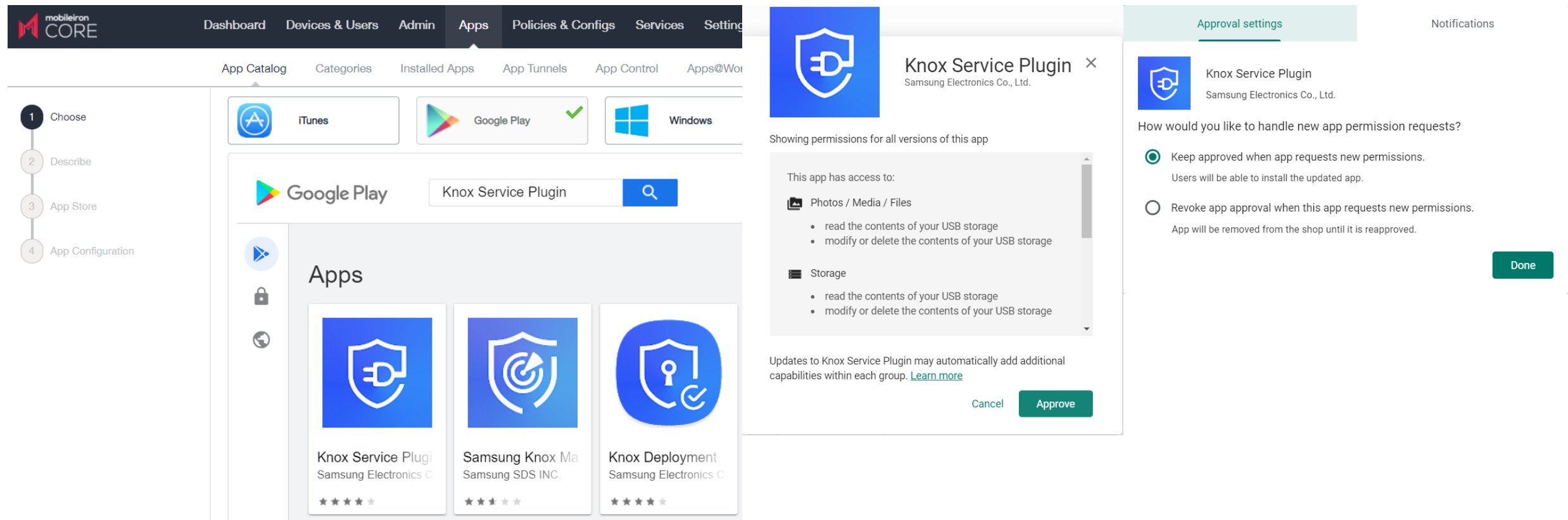
Work Profile Samsung KPE Standard Features



Managed Device Samsung KPE Standard Features

Knox Service Plugin [KSP]

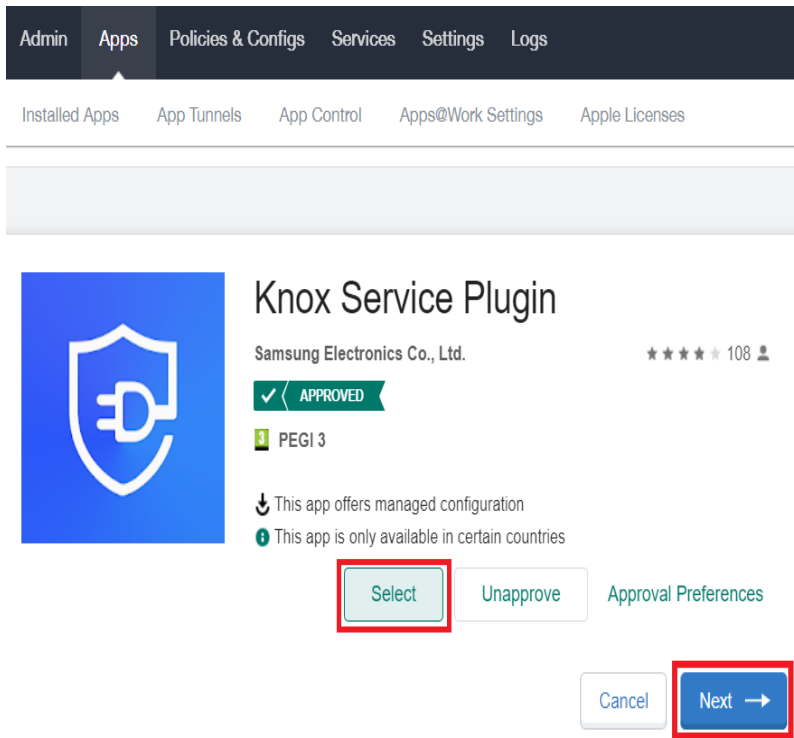
- In the MobileIron console, navigate to: Apps > App Catalog > Add > Google Play
- Search for and approve the Knox Service Plugin Application.
- Choose how you would like to handle new app permission requests and then click Done.



The screenshot displays the MobileIron CORE console interface. The top navigation bar includes links for Dashboard, Devices & Users, Admin, Apps, Policies & Configs, Services, and Settings. The 'Apps' section is active, showing a sidebar with steps: 1 Choose, 2 Describe, 3 App Store, and 4 App Configuration. The main content area shows the 'App Catalog' with options for iTunes, Google Play (selected with a green checkmark), and Windows. A search bar for 'Knox Service Plugin' is visible. Below the search bar, three app cards are shown: 'Knox Service Plugin' by Samsung Electronics Co., 'Samsung Knox Ma' by Samsung SDS INC., and 'Knox Deployment' by Samsung Electronics Co. A modal window is open for the 'Knox Service Plugin' app, showing its icon, name, and developer. It lists permissions: 'Photos / Media / Files' (read and modify/delete contents of USB storage) and 'Storage' (read and modify/delete contents of USB storage). A note mentions that updates may add additional capabilities. At the bottom of the modal are 'Cancel' and 'Approve' buttons. To the right of the modal, the 'Approval settings' section is visible, asking 'How would you like to handle new app permission requests?'. Two options are provided: 'Keep approved when app requests new permissions.' (selected with a radio button) and 'Revoke app approval when this app requests new permissions.' (unselected). A 'Done' button is at the bottom right of the approval settings.

Knox Service Plugin [KSP]

- Select the Knox Service Plugin and then click Next.
- Category is optional, select Next.
- Select Install this app for Android Enterprise and make sure Silent install for work managed devices, Auto Update this App and Block Uninstall are ticked.



Admin Apps Policies & Configs Services Settings Logs

Installed Apps App Tunnels App Control Apps@Work Settings Apple Licenses

Knox Service Plugin

Samsung Electronics Co., Ltd. ★★★★★ 108

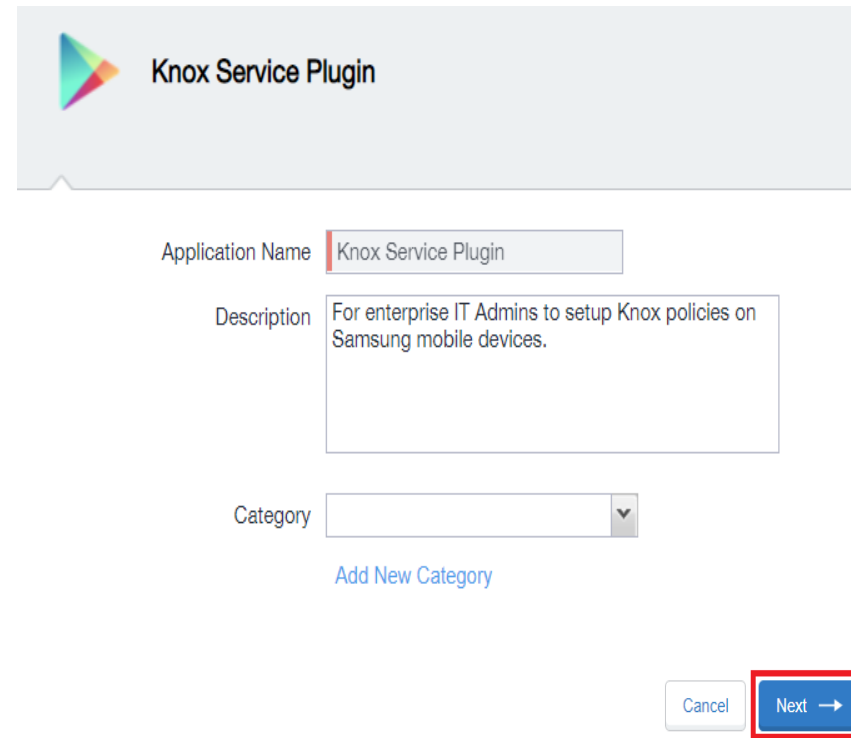
✓ APPROVED

1 PEGI 3

⬇ This app offers managed configuration
ⓘ This app is only available in certain countries

Select Unapprove Approval Preferences

Cancel Next →



Knox Service Plugin

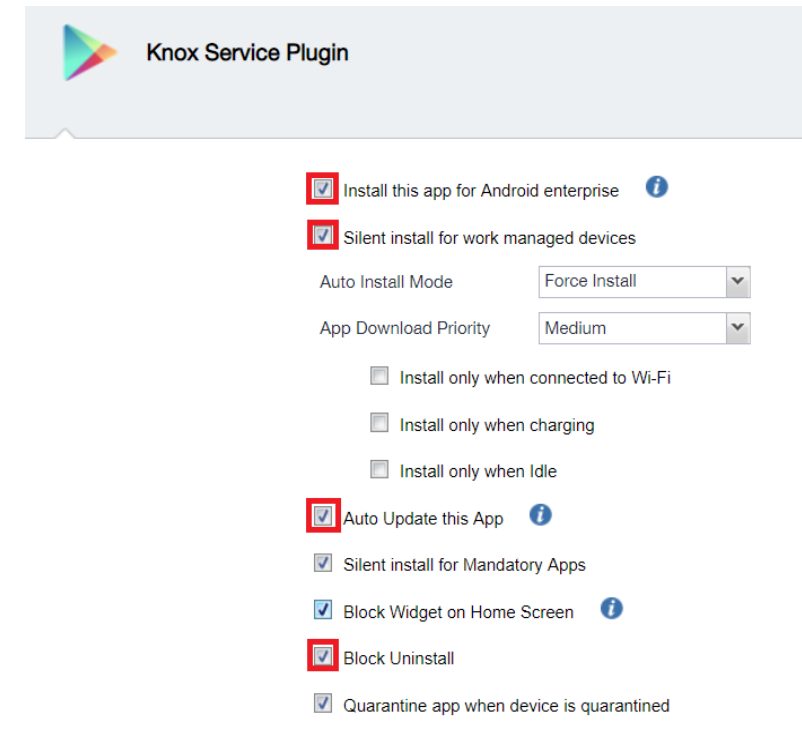
Application Name: Knox Service Plugin

Description: For enterprise IT Admins to setup Knox policies on Samsung mobile devices.

Category: ▼

[Add New Category](#)

Cancel Next →



Knox Service Plugin

☒ Install this app for Android enterprise ⓘ

☒ Silent install for work managed devices

Auto Install Mode: Force Install ▼

App Download Priority: Medium ▼

☐ Install only when connected to Wi-Fi

☐ Install only when charging

☐ Install only when Idle

☒ Auto Update this App ⓘ

☒ Silent install for Mandatory Apps

☒ Block Widget on Home Screen ⓘ

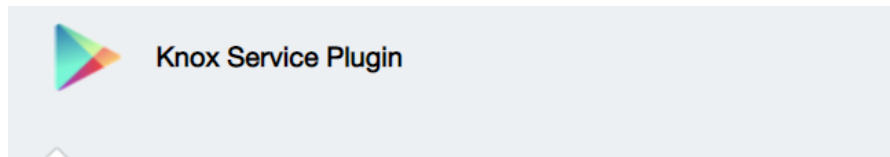
☒ Block Uninstall

☒ Quarantine app when device is quarantined

Cancel Next →

Knox Platform for Enterprise : Premium Edition

- Scroll down to Default Configuration for Knox Service Plugin.
- Enter a Profile name of your choice.
- Copy and Paste your KPE Premium License Key from your Samsung Knox Portal.
- To configure the KPE premium settings, scroll down and select configure against the desired configuration option.
- Select Finish.



▼ Default Configuration for Knox Service Plugin ⓘ

Profile name ⓘ

KPE Premium License key ⓘ

☐ Debug Mode ⓘ

▶ Device-wide policies (Device Owner) ⓘ

▶ Work profile policies (Profile Owner) ⓘ

▶ DeX customization profile (Premium) ⓘ

▼ Device and Settings customization profile (Premium) ⓘ

Knox Service Plugin

▼ VPN policy (Premium) ⓘ

☒ Enable VPN controls ⓘ

VPN type ⓘ

▶ Manage list of apps that use VPN ⓘ

☒ Enable on-demand VPN ⓘ

▶ Manage list of apps that can bypass VPN ⓘ

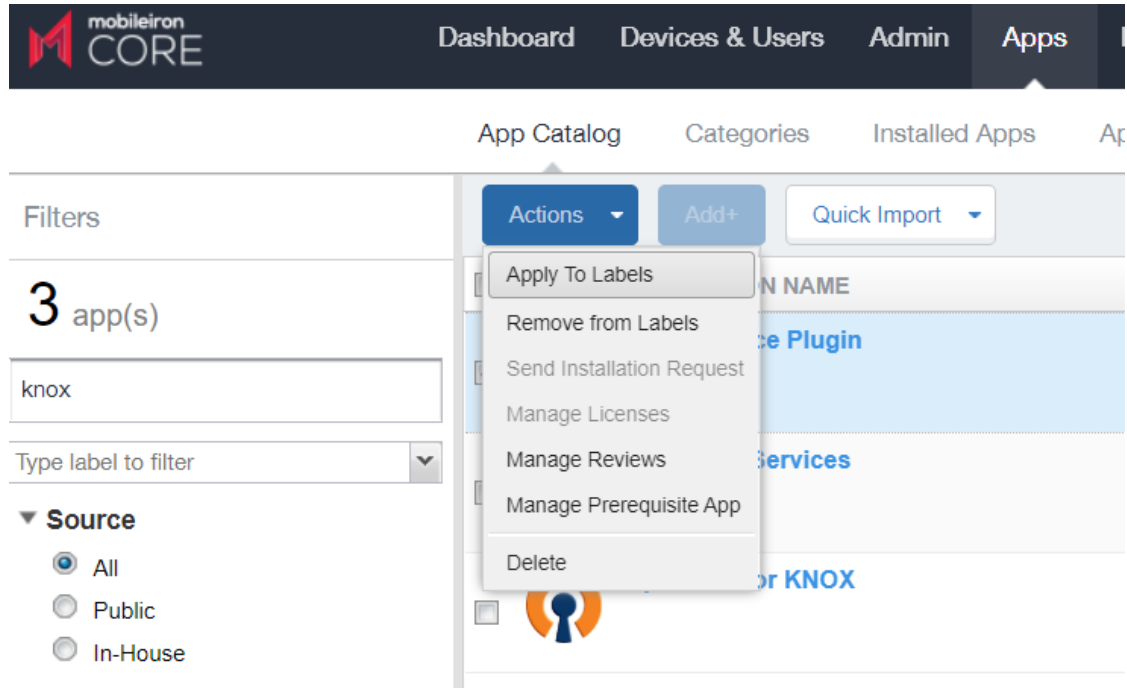
Name of VPN profile to use ⓘ

☐ Enable VPN chaining ⓘ

Name of secondary VPN profile to use ⓘ

Knox Platform for Enterprise : Premium Edition

- Knox Service Plugin will now appear in your App Catalog list.
- To assign, tick the Knox Service Plugin, select Actions and then Apply To Labels.
- Select your label and then click Apply.



mobileiron CORE

Dashboard Devices & Users Admin Apps

App Catalog Categories Installed Apps

Filters

3 app(s)

knox

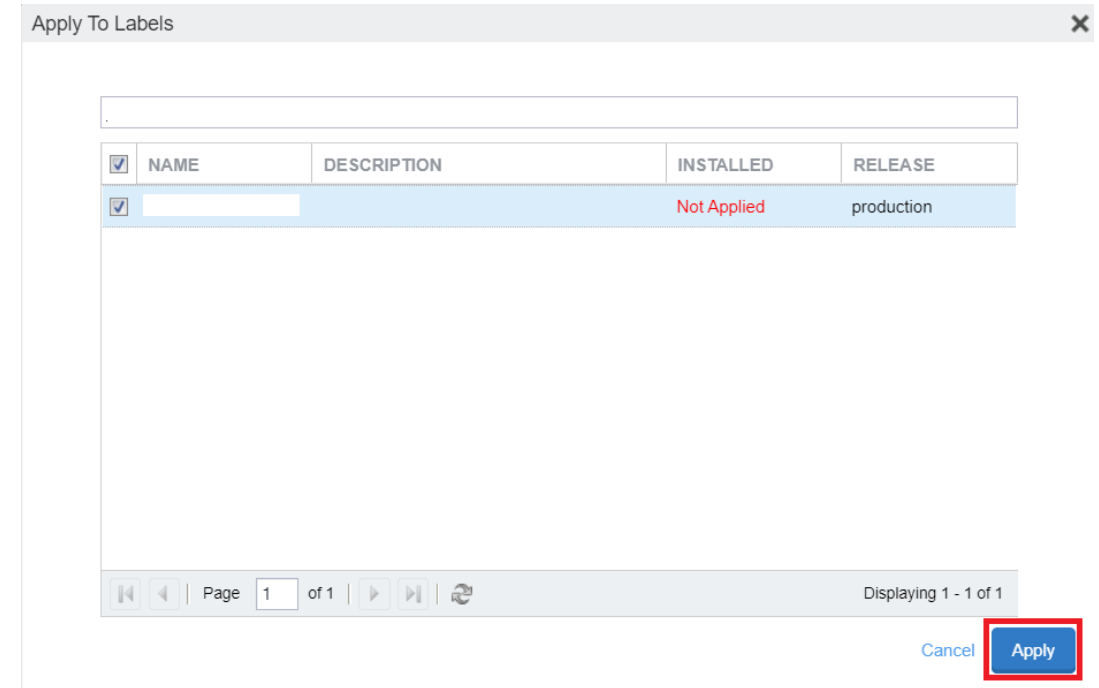
Type label to filter

Source

- All
- Public
- In-House

Actions

- Apply To Labels
- Remove from Labels
- Send Installation Request
- Manage Licenses
- Manage Reviews
- Manage Prerequisite App
- Delete



Apply To Labels

<input checked="" type="checkbox"/>	NAME	DESCRIPTION	INSTALLED	RELEASE
<input checked="" type="checkbox"/>			Not Applied	production

Page 1 of 1

Displaying 1 - 1 of 1

Cancel Apply

Document Information

This is version 2.1 of this document.

Thank you!

