MobileIron Core UEM 10.5

&

Knox Platform for Enterprise

August 2020
Samsung R&D Centre UK
(SRUK)

Agenda

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
     - Work Profile on Company Owned Device
   - 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]

MobileIron Collateral & Contacts

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

https://forums.ivanti.com/s/welcome-mobileiron?language=en_US

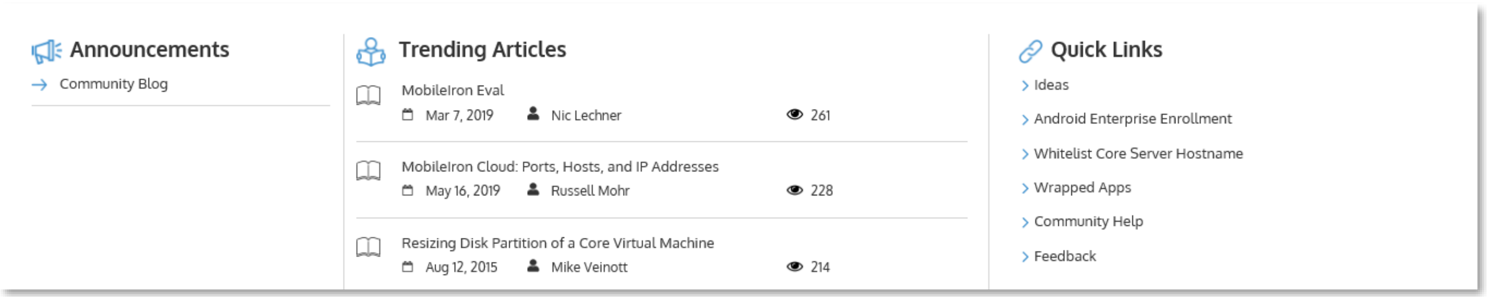
Pre-Requisites for Knox Platform for Enterprise

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

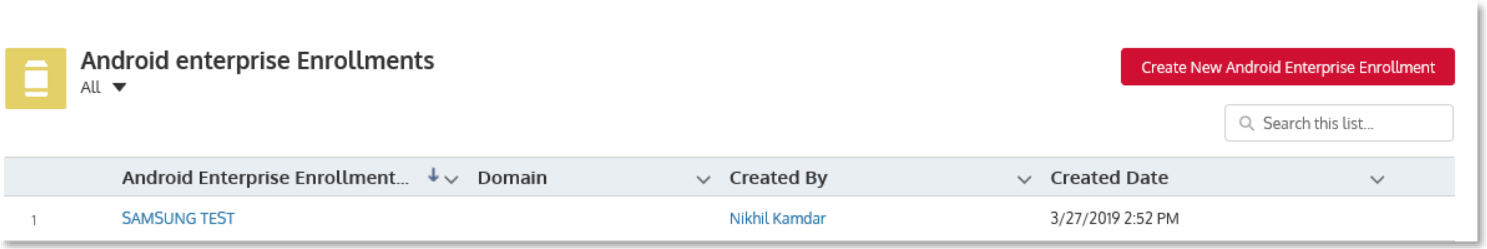
Configure Android Enterprise

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

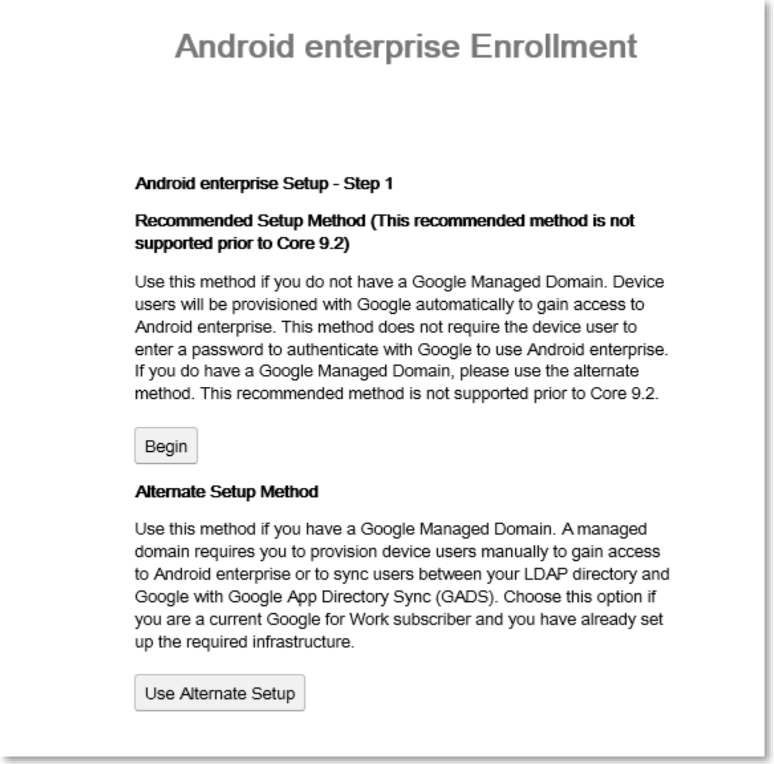


Article	Date	Author	Views
MobileIron Eval	Mar 7, 2019	Nic Lechner	261
MobileIron Cloud: Ports, Hosts, and IP Addresses	May 16, 2019	Russell Mohr	228
Resizing Disk Partition of a Core Virtual Machine	Aug 12, 2015	Mike Veinott	214



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.

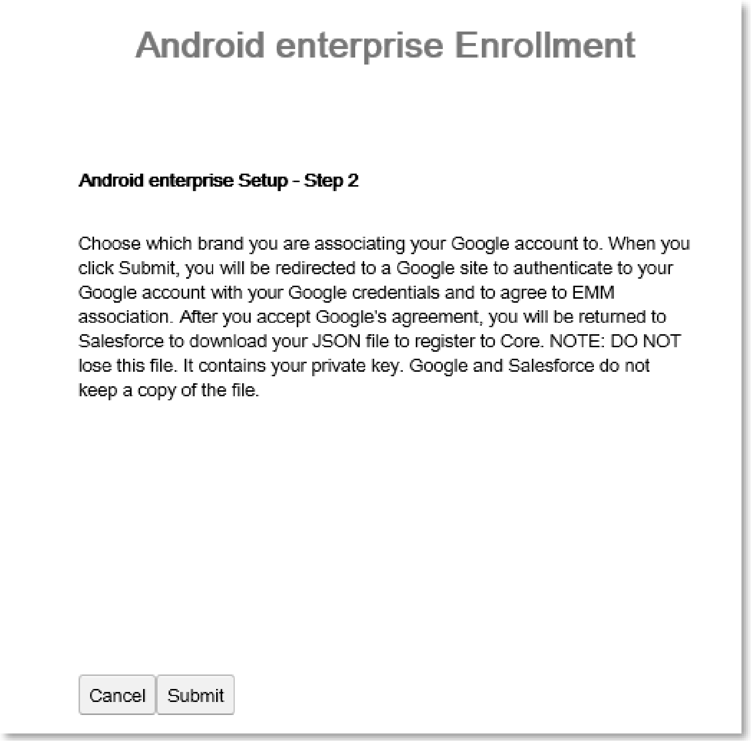
Alternate Setup Method

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.

Configure Android Enterprise

Configure Android Enterprise

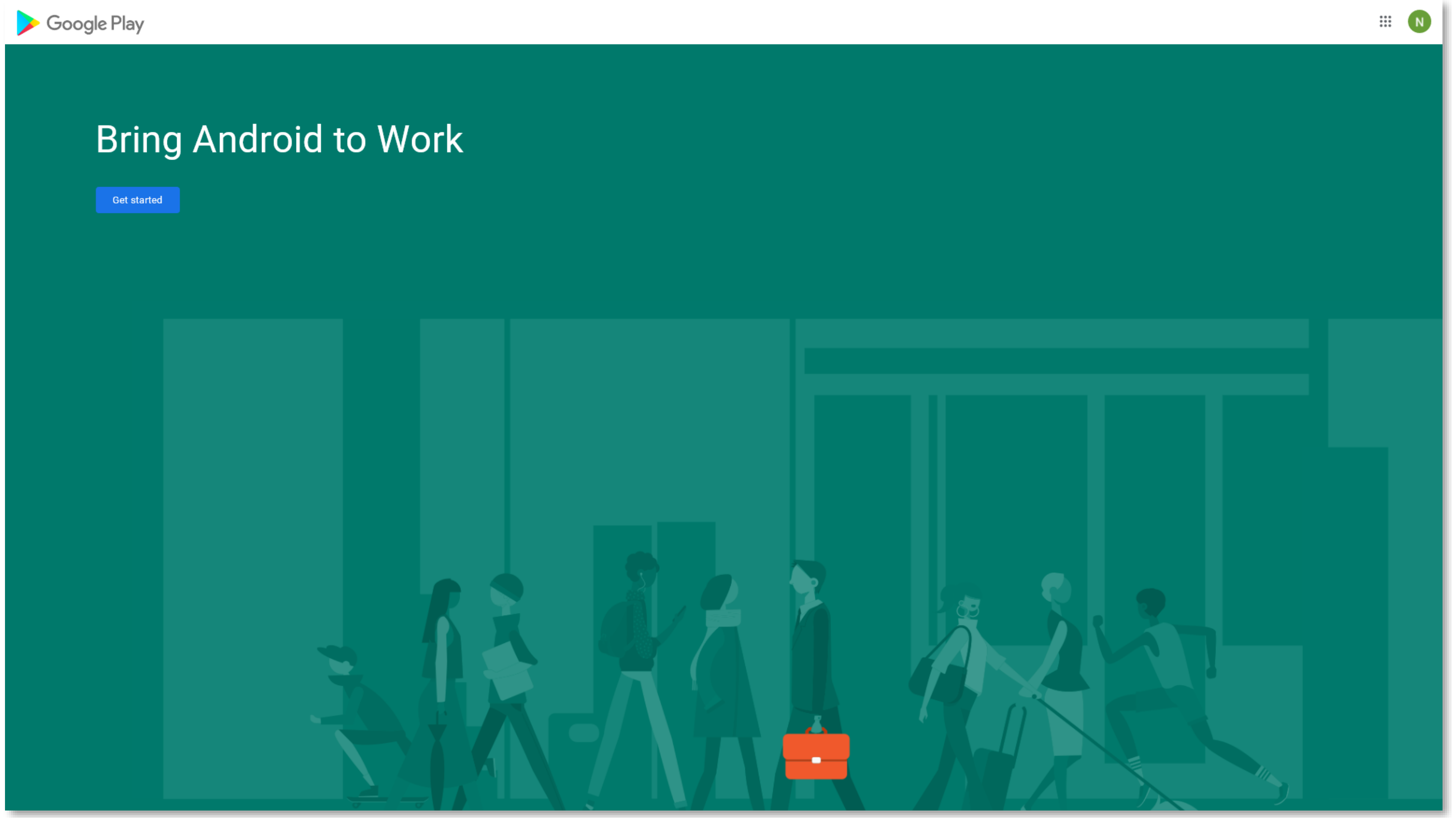
- Click on Submit and make sure that you have signed into the Google Account that you would wish to bind.
- MobileIron Customer Support Portal will forward you to the Google Android Enterprise binding page. Click 'Get started'



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.

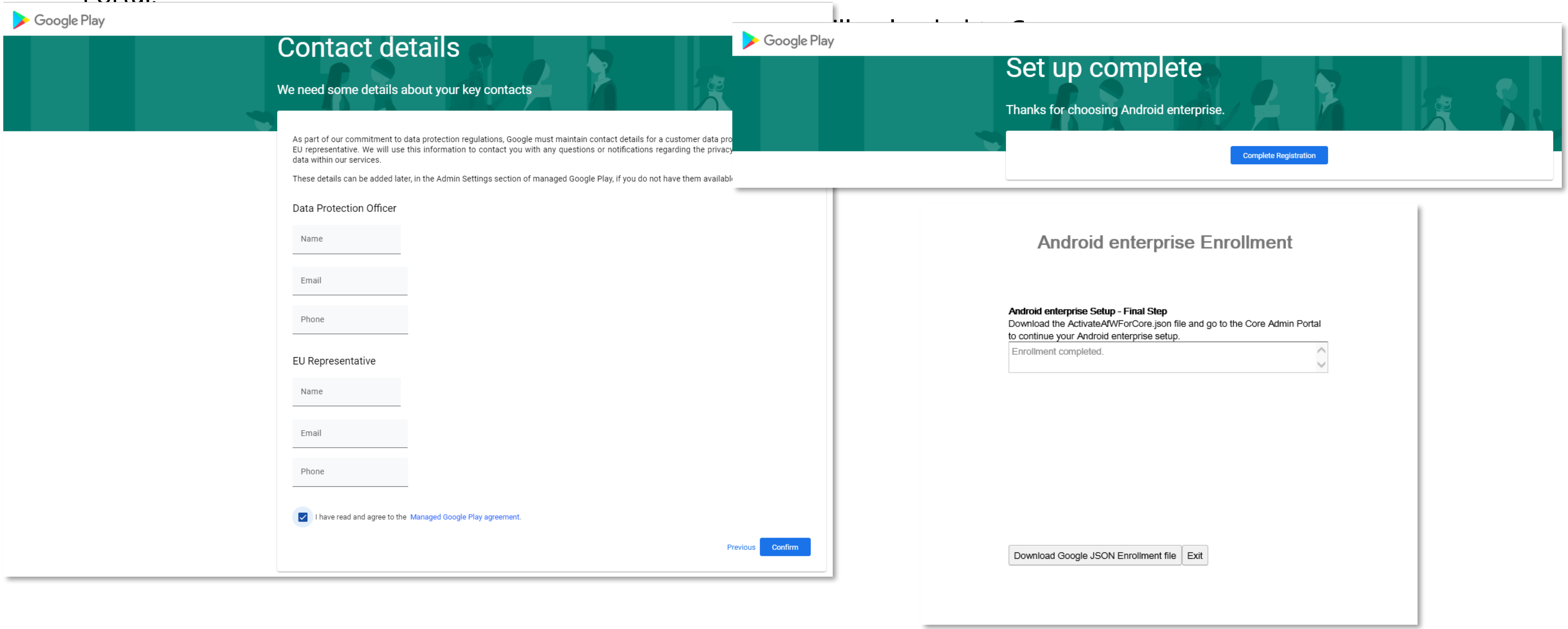


Bring Android to Work

Configure Android Enterprise

Configure Android Enterprise

- Fill out the Contact details page, tick the Managed Google Play agreement 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.



Google Play

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 pro EU representative. We will use this information to contact you with any questions or notifications regarding the privacy 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 availabl

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

☑ I have read and agree to the Managed Google Play agreement.

Google Play

Set up complete

Thanks for choosing Android enterprise.

Android enterprise Enrollment

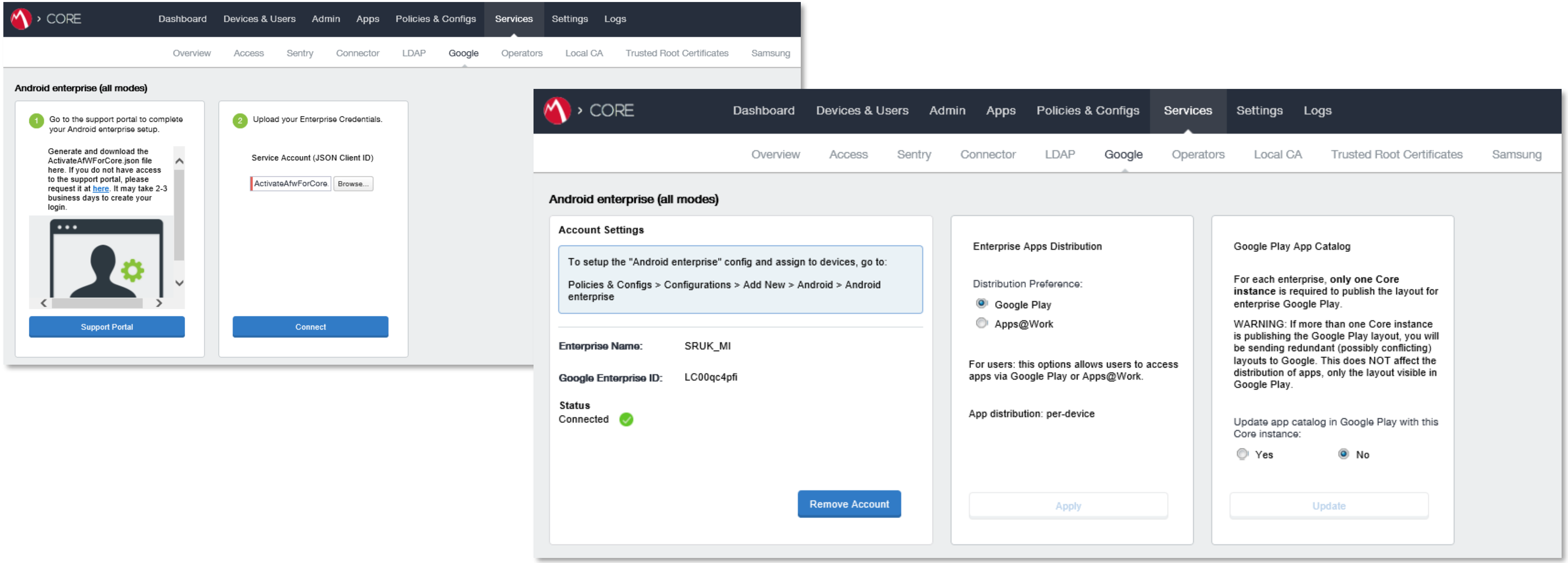
Android enterprise Setup - Final Step
Download the ActivateAfWForCore.json file and go to the Core Admin Portal to continue your Android enterprise setup.

Enrollment completed.

Configure Android Enterprise

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 click 'Connect', Android Enterprise is bound.



Android enterprise (all modes)

1 Go to the support portal to complete your Android enterprise setup.

Generate and download the ActivateAfWForCore.json file here. If you do not have access to the support portal, please request it at here. It may take 2-3 business days to create your login.

2 Upload your Enterprise Credentials.

Service Account (JSON Client ID): ActivateAfwForCore.

Android enterprise (all modes)

Account Settings

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

Policies & Configs > Configurations > Add New > Android > Android enterprise

Enterprise Name: SRUK_MI

Google Enterprise ID: LC00qc4pfi

Status
Connected ✓

Enterprise Apps Distribution

Distribution Preference:

● Google Play
○ Apps@Work

For users: this options allows users to access apps via Google Play or Apps@Work.

App distribution: per-device

Google Play App Catalog

For each enterprise, **only one Core instance** is required to publish the layout for enterprise Google Play.

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.

Update app catalog in Google Play with this Core instance:

○ Yes ● No

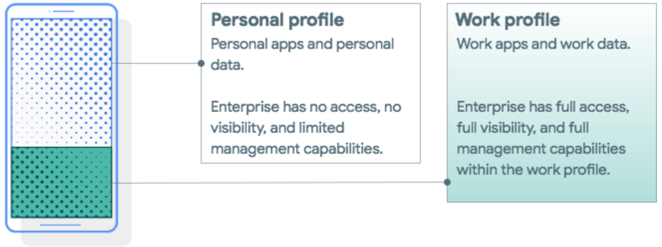
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 5 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. **Work Profile on a Company Owned Device [Android 11+]**
5. **Dedicated device** [*formerly known as COSU*]

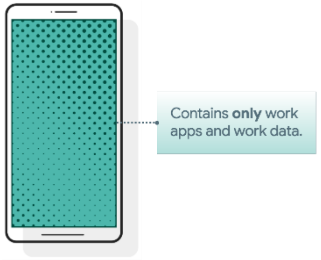
MobileIron UEM can support **all** 5 of these deployment modes. In this next section we will show you how to configure each of these 5 deployment modes in MobileIron UEM for your device fleet.



Personal profile
Personal apps and personal data.
Enterprise has no access, no visibility, and limited management capabilities.

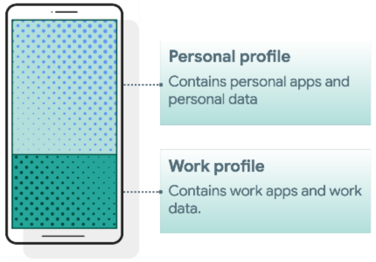
Work profile
Work apps and work data.
Enterprise has full access, full visibility, and full management capabilities within the work profile.

Bring Your Own Device [BYOD]



Contains **only** work apps and work data.

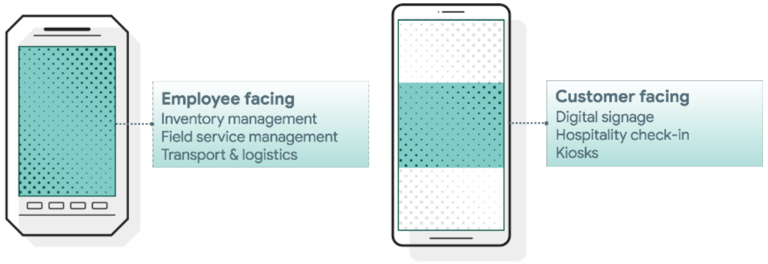
Company-owned Device



Personal profile
Contains personal apps and personal data

Work profile
Contains work apps and work data.

Fully Managed device with a Work Profile or Work Profile on a Company Owned Device



Employee facing
Inventory management
Field service management
Transport & logistics

Customer facing
Digital signage
Hospitality check-in
Kiosks

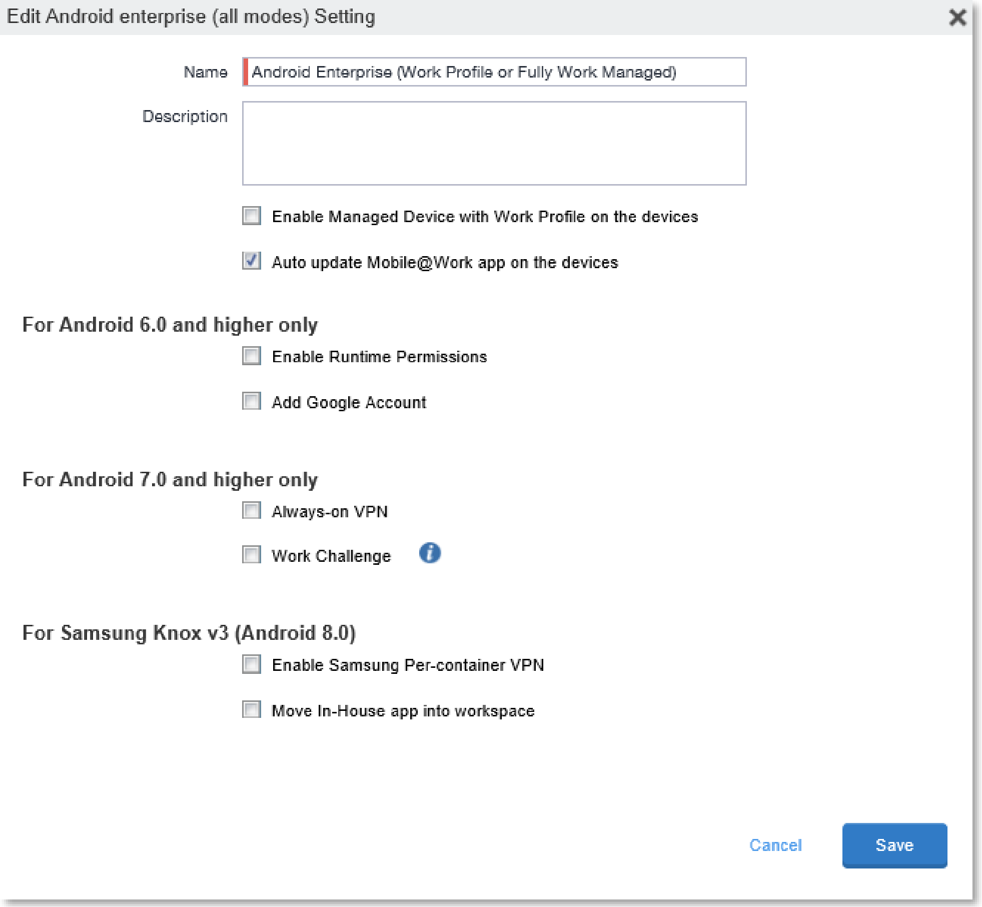
Dedicated Device

Android Enterprise: BYOD (Work Profile)

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 device.
- Apply this config to a label.



Edit Android enterprise (all modes) Setting

Name: Android Enterprise (Work Profile or Fully Work Managed)

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

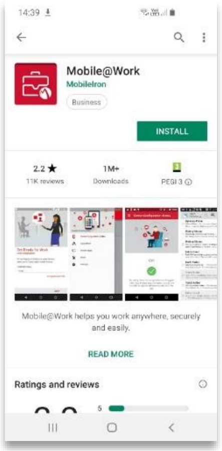
☐ Move In-House app into workspace

Android Enterprise: BYOD

Android Enterprise BYOD Deployment

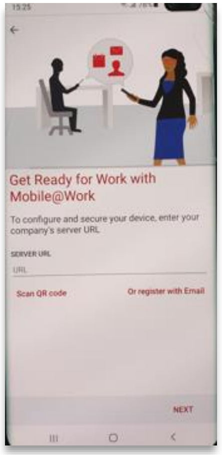
Now all you simply need to do is enroll your device by completing the following:

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



Mobile@Work helps you work anywhere, securely and easily.

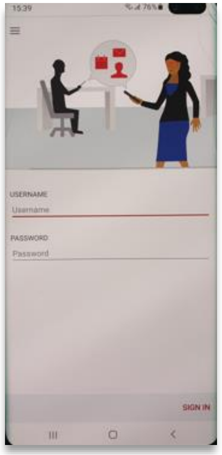
Install Mobile@Work client



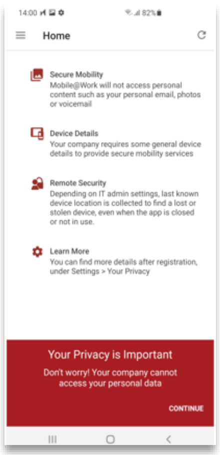
Get Ready for Work with Mobile@Work

To configure and secure your device, enter your company's server URL

Enter server URL & hit NEXT



Enter credentials & hit SIGN IN



Secure Mobility
Mobile@Work will not access personal content such as your personal email, photos or voicemail

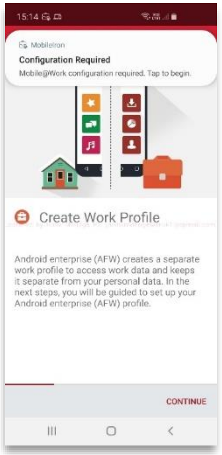
Device Details
Your company requires some general device details to provide secure mobility services

Remote Security
Depending on IT admin settings, last known device location is collected to find a lost or stolen device, even when the app is closed or not in use.

Learn More
You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important
Don't worry! Your company cannot access your personal data

CONTINUE

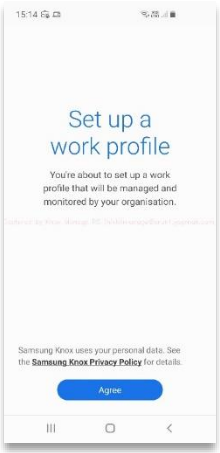


Configuration Required
Mobile@Work configuration required. Tap to begin.

Create Work Profile

Android enterprise (AFW) creates a separate work profile to access work data and keeps it separate from your personal data. In the next steps, you will be guided to set up your Android enterprise (AFW) profile.

CONTINUE

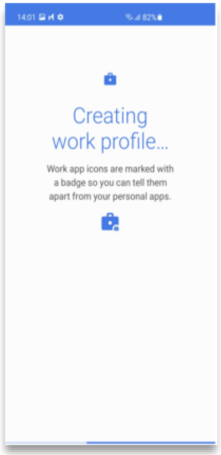


Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the Samsung Knox Privacy Policy for details.

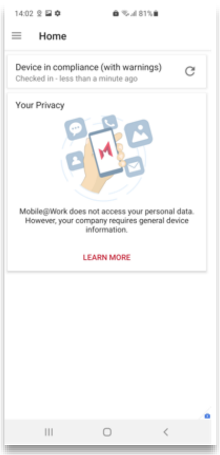
Set up a work profile tap Agree



Creating work profile...

Work app icons are marked with a badge so you can tell them apart from your personal apps.

Creating Work Profile

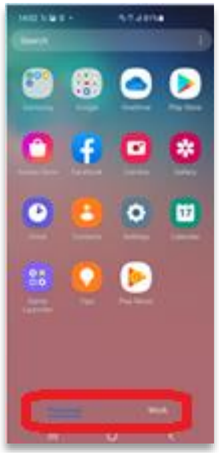


Device in compliance (with warnings)
Checked in - less than a minute ago

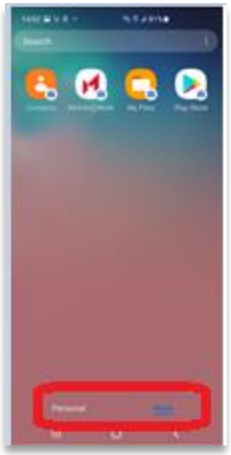
Your Privacy

Mobile@Work does not access your personal data. However, your company requires general device information.

Device Enrollment Successful!



The Personal profile is created



The Work profile is created

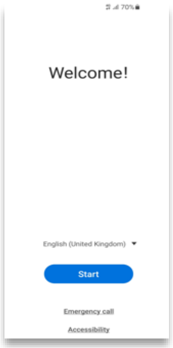
Android Enterprise: Company-owned Device

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.


Welcome!

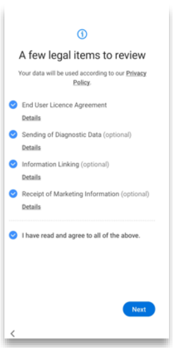
English (United Kingdom)

Start

Emergency call

Accessibility

Click Start arrow

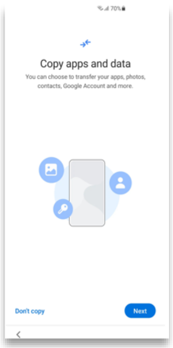

A few legal items to review

Your data will be used according to our Privacy Policy.

- End User Licence Agreement — Details
- Sending of Diagnostic Data (optional) — Details
- Information Linking (optional) — Details
- Receipt of Marketing Information (optional) — Details
- I have read and agree to all of the above.

Next

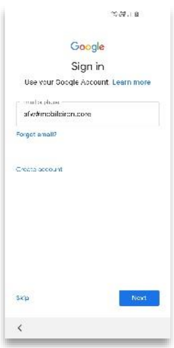
Accept T's & C's


Copy apps and data

You can choose to transfer your apps, photos, contacts, Google Account and more.

Don't copy — Next

Don't Copy


Google

Sign in

Use your Google Account. Learn more

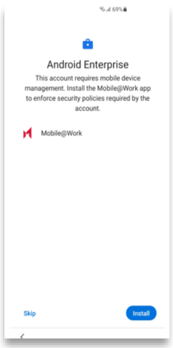
Email or phone: afw#mobileiron.core

Forgot email?

Create account

Skip — Next

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

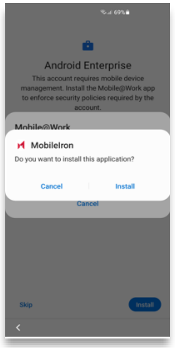

Android Enterprise

This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.

Mobile@Work

Skip — Install

Install Mobile@Work


Android Enterprise

This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.

Mobile@Work

MobileIron

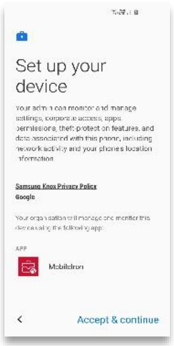
Do you want to install this application?

Cancel — Install

Cancel

Skip — Install

Install Mobile@Work


Set up your device

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information.

Samsung Knox Privacy Policy

Google

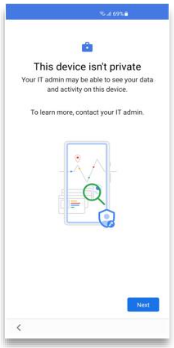
Your organisation will manage and monitor this device using the following app:

APP

MobileIron

Accept & continue

Accept & continue

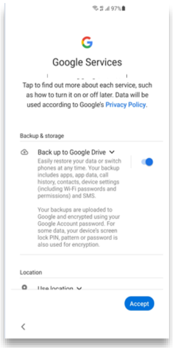

This device isn't private

Your IT admin may be able to see your data and activity on this device.

To learn more, contact your IT admin.

Next

Next


Google Services

Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

Backup & storage

Back up to Google Drive

Easily restore your data or switch phones at any time. Your backup includes apps, app data, call history, contacts, device settings (including Wi-Fi passwords and permissions) and SMS.

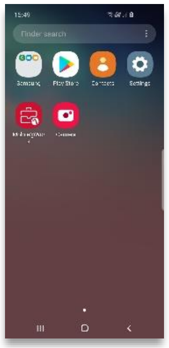
Your backups are uploaded to Google and encrypted using your Google Account password. For some data, your device's screen lock PIN, pattern or password is also used for encryption.

Location

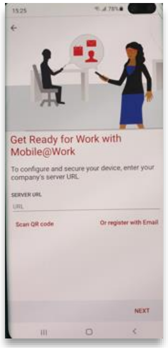
Use location

Accept

Setting up Managed Google Play Account



Mobile@Work will Auto launch and pin


Get Ready for Work with Mobile@Work

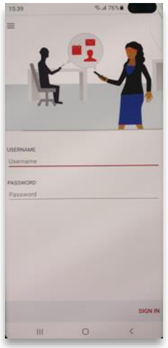
To configure and secure your device, enter your company's server URL

SERVER URL: URL

Scan QR code — Or register with Email

NEXT

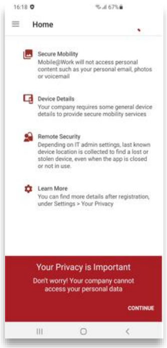
Enter server URL & hit NEXT


USERNAME: Username

PASSWORD: Password

SIGN IN

Enter credentials & hit SIGN IN


Home

Secure Mobility — Mobile@Work will not access personal content such as your personal email, photos or voicemail

Device Details — Your company requires some general device details to provide secure mobility services

Remote Security — Depending on IT admin settings, last known device location is collected to find a lost or stolen device, even when the app is closed or not in use.

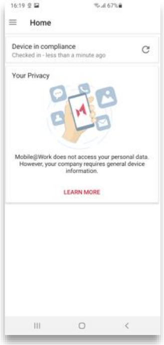
Learn More — You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important

Don't worry! Your company cannot access your personal data

CONTINUE

CONTINUE


Home

Device in compliance

Checked in - less than a minute ago

Your Privacy

Mobile@Work does not access your personal data. However, your company requires general device information.

LEARN MORE

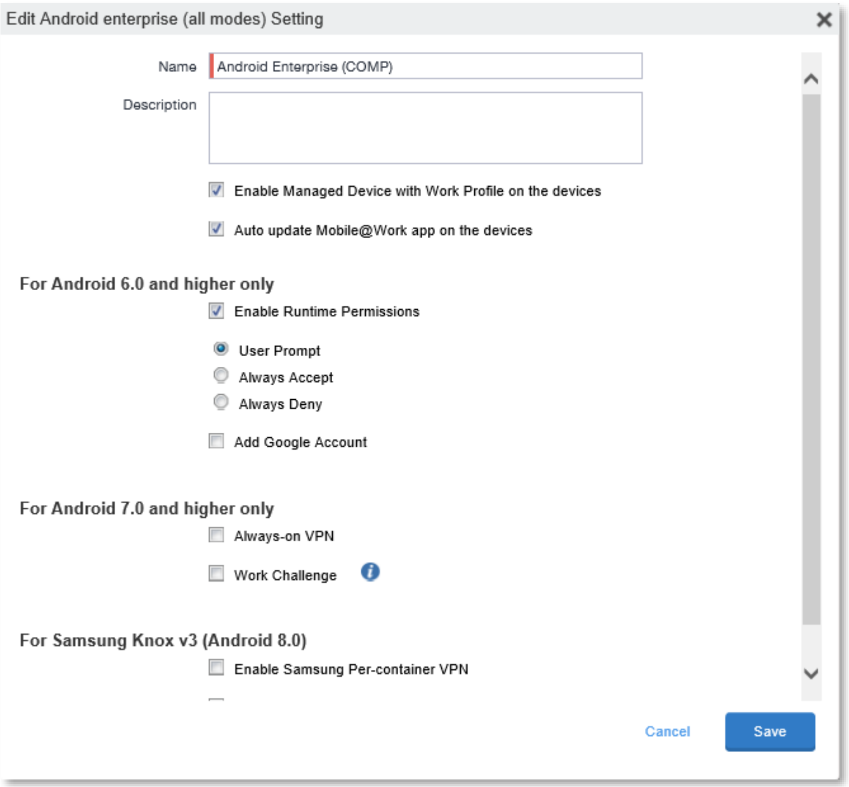
Device Enrollment Successful!

Android Enterprise: Fully Managed Device with a Work Profile
Work Profile on a Company Owned Device (Android 11+)

Android Enterprise Fully Managed Device with a Work Profile Deployment or Work Profile on a Company Owned Device (Android 11+)

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 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: Android Enterprise (COMP)

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

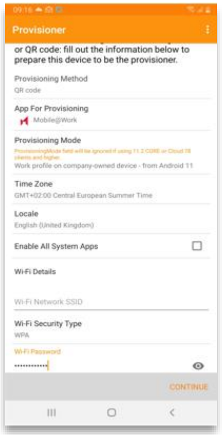
Android Enterprise: Fully Managed Device with a Work Profile Work Profile on a Company Owned Device (Android 11+)

Android Enterprise Fully Managed Device with a Work Profile or Work Profile on a Company Owned Device (Android 11+) Deployment

To enroll your device using this type of configuration will require a QR code using the MobileIron Provisioner app: https://play.google.com/store/apps/details?id=com.mobileiron.client.android.nfcprovisioner. NFC is not available on Android 10 or above

- App for Provisioner: Mobile@Work
- Provisioning Mode: Work profile on company-owned device – Android 11
- Enter you Wi-Fi Network SSID and password

Below is a screen-by-screen play to enroll your device using the QR Code method.



Provisioner

or QR code: fill out the information below to prepare this device to be the provisioner.

Provisioning Method: QR code

App For Provisioning: Mobile@Work

Provisioning Mode: Work profile on company-owned device - from Android 11

Time Zone: GMT+02:00 Central European Summer Time

Locale: English (United Kingdom)

Enable All System Apps □

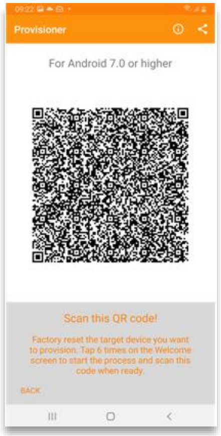
Wi-Fi Details

Wi-Fi Network SSID

Wi-Fi Security Type: WPA

Wi-Fi Password: ••••••••••••

App Provisioner Settings on provisioning device



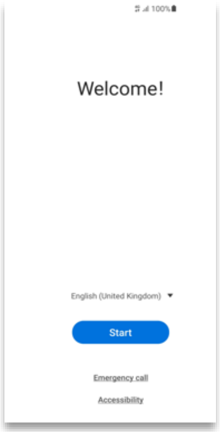
Provisioner

For Android 7.0 or higher

Scan this QR code!

Factory reset the target device you want to provision. Tap 6 times on the Welcome screen to start the process and scan this code when ready.

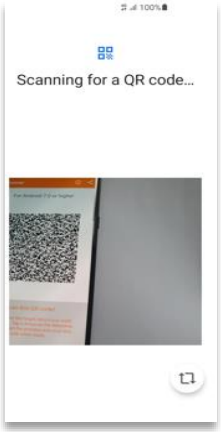
Tap continue For QR code From provisioning device



Welcome!

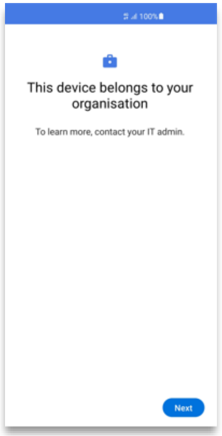
English (United Kingdom)

Tap 6 times



Scanning for a QR code...

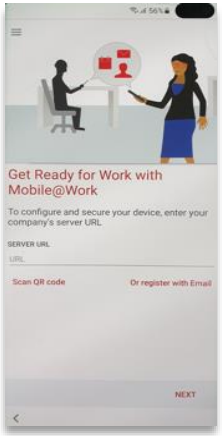
Scan QR Code



This device belongs to your organisation

To learn more, contact your IT admin.

Click Next

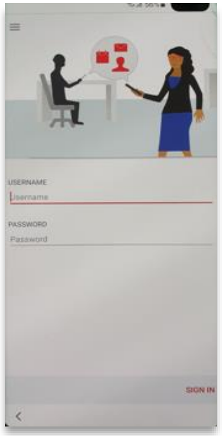


Get Ready for Work with Mobile@Work

To configure and secure your device, enter your company's server URL

SERVER URL: URL

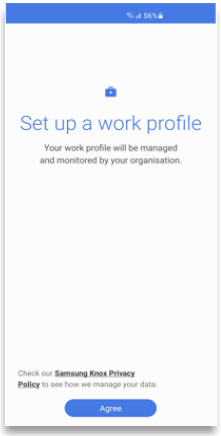
Enter Server URL



USERNAME: Username

PASSWORD: Password

Enter User credentials

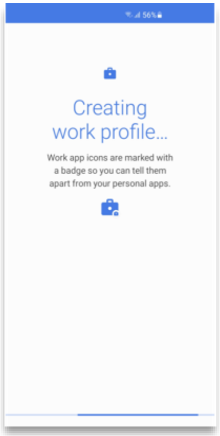


Set up a work profile

Your work profile will be managed and monitored by your organisation.

Check our Samsung Knox Privacy Policy to see how we manage your data.

Set up work profile, click Agree

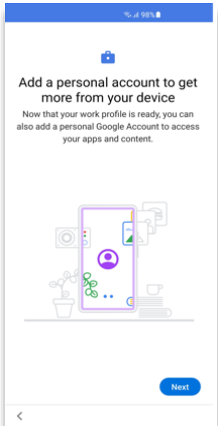


Creating work profile...

Work app icons are marked with a badge so you can tell them apart from your personal apps.

Work profile gets created

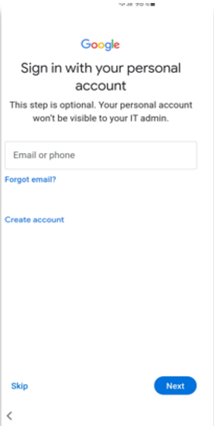
Android Enterprise: Fully Managed Device with a Work Profile
Work Profile on a Company Owned Device (Android 11+)



Add a personal account to get more from your device

Now that your work profile is ready, you can also add a personal Google Account to access your apps and content.

Add a personal account

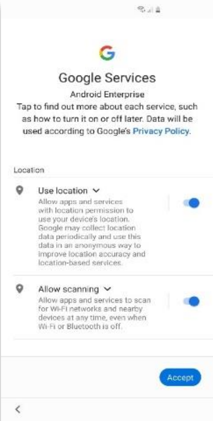


Sign in with your personal account

This step is optional. Your personal account won't be visible to your IT admin.

Email or phone

Enter the Credentials & click Next


Google Services

Android Enterprise

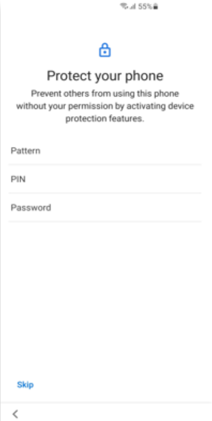
Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

Location

Use location: Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Allow scanning: Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

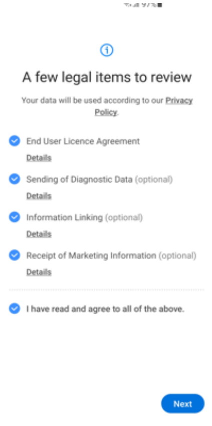
Scroll down, and Accept



Protect your phone

Prevent others from using this phone without your permission by activating device protection features.

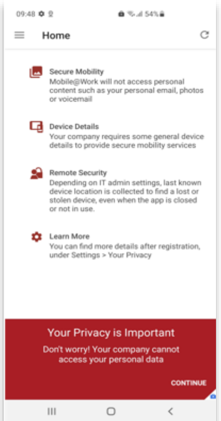
Protect your phone


A few legal items to review

Your data will be used according to our Privacy Policy.

- ✓ End User Licence Agreement — Details
- ✓ Sending of Diagnostic Data (optional) — Details
- ✓ Information Linking (optional) — Details
- ✓ Receipt of Marketing Information (optional) — Details
- ✓ I have read and agree to all of the above.

Accept the legal terms & click Next



Secure Mobility Mobile@Work will not access personal content such as your personal email, photos or voicemail

Device Details Your company requires some general device details to provide secure mobility services

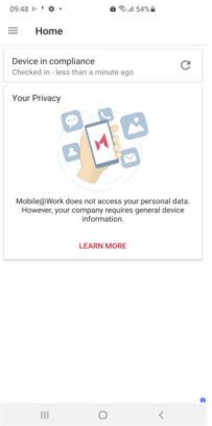
Remote Security Depending on IT admin settings, last known device location is collected to find a lost or stolen device, even when the app is closed or not in use.

Learn More You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important

Don't worry! Your company cannot access your personal data

Launch Mobile@Work click CONTINUE



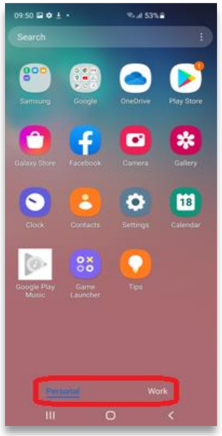
Device in compliance

Checked in - less than a minute ago

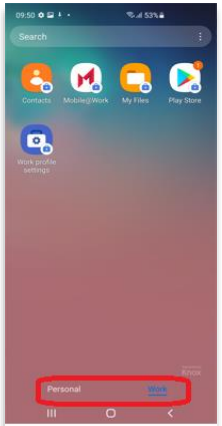
Your Privacy

Mobile@Work does not access your personal data. However, your company requires general device information.

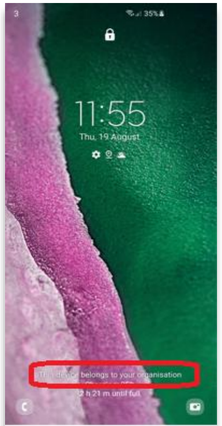
Device is enrolled



A personal profile is created



A Work profile is created



This device belongs to your organisation

2 h 21 m until full

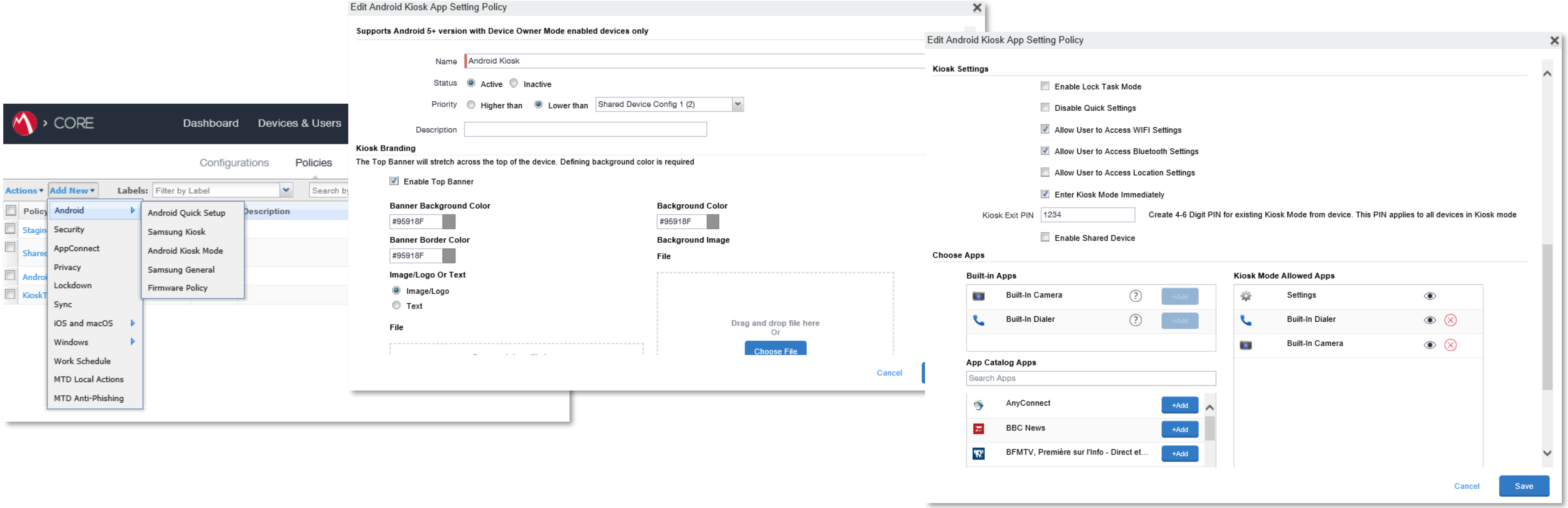
We see the device belongs to the organization

Android Enterprise: Dedicated Device

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



Edit Android Kiosk App Setting Policy

Supports Android 5+ version with Device Owner Mode enabled devices only

Name: Android Kiosk

Status: ● Active ○ Inactive

Priority: ○ Higher than ● Lower than Shared Device Config 1 (2)

Description:

Kiosk Branding

The Top Banner will stretch across the top of the device. Defining background color is required

☑ Enable Top Banner

Banner Background Color: #95918F

Banner Border Color: #95918F

Image/Logo Or Text: ● Image/Logo ○ Text

File

Background Color: #95918F

Background Image

File

Drag and drop file here
Or
Choose File

Cancel

Edit Android Kiosk App Setting Policy

Kiosk Settings

□ Enable Lock Task Mode
□ Disable Quick Settings
☑ Allow User to Access WIFI Settings
☑ Allow User to Access Bluetooth Settings
□ Allow User to Access Location Settings
☑ Enter Kiosk Mode Immediately

Kiosk Exit PIN: 1234 Create 4-6 Digit PIN for existing Kiosk Mode from device. This PIN applies to all devices in Kiosk mode

□ Enable Shared Device

Choose Apps

Built-in Apps
- Built-In Camera +Add
- Built-In Dialer +Add

App Catalog Apps

Search Apps
- AnyConnect +Add
- BBC News +Add
- BFMTV, Première sur l'Info - Direct et... +Add

Kiosk Mode Allowed Apps
- Settings
- Built-In Dialer
- Built-In Camera

Cancel Save

Android Enterprise: Dedicated Device

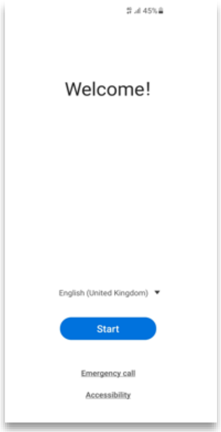
Android Enterprise Dedicated Device Deployment

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 than 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.



Welcome!

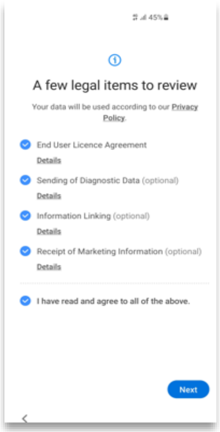
English (United Kingdom) ▾

Start

Emergency call

Accessibility

Click Start



A few legal items to review

Your data will be used according to our Privacy Policy.

● End User Licence Agreement
Details

● Sending of Diagnostic Data (optional)
Details

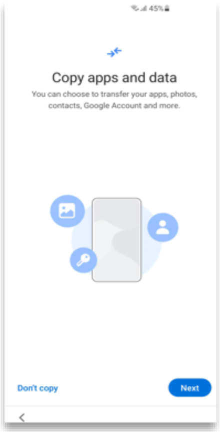
● Information Linking (optional)
Details

● Receipt of Marketing Information (optional)
Details

● I have read and agree to all of the above.

Next

Accept T’s & C’s



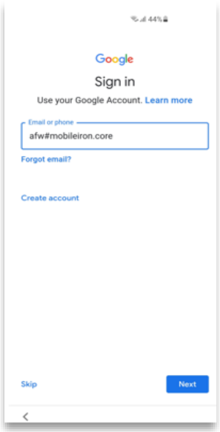
Copy apps and data

You can choose to transfer your apps, photos, contacts, Google Account and more.

Don't copy

Next

Choose Don’t Copy



Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#mobileiron.core

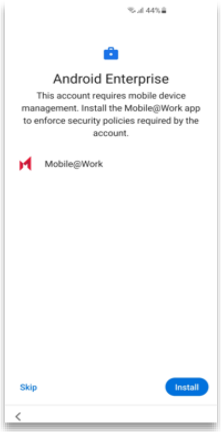
Forgot email?

Create account

Skip

Next

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



Android Enterprise

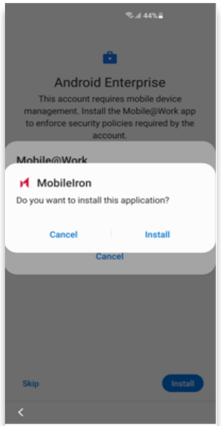
This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.

Mobile@Work

Skip

Install

Install Mobile@Work



Android Enterprise

This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.

Mobile@Work

MobileIron

Do you want to install this application?

Cancel

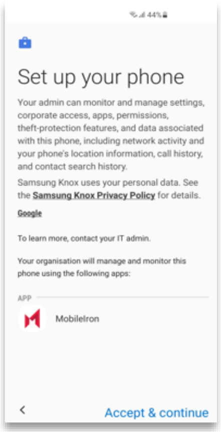
Install

Cancel

Skip

Install

Install Mobile@Work



Set up your phone

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information, call history, and contact search history.

Samsung Knox uses your personal data. See the Samsung Knox Privacy Policy for details.

Google

To learn more, contact your IT admin.

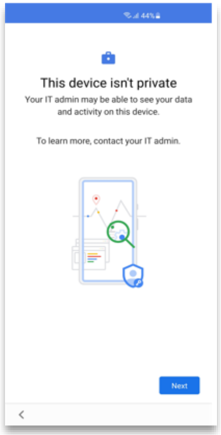
Your organisation will manage and monitor this phone using the following apps:

APP

MobileIron

Accept & continue

Accept & continue



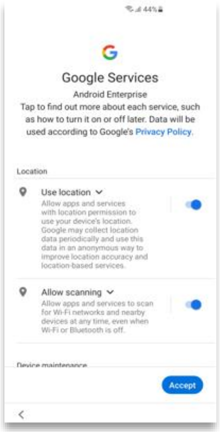
This device isn't private

Your IT admin may be able to see your data and activity on this device.

To learn more, contact your IT admin.

Next

Click Next



Google Services

Android Enterprise

Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

Location

Use location
Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

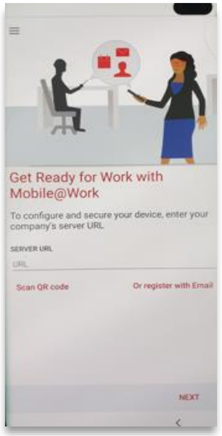
Allow scanning
Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

Device maintenance

Accept

Accept the Google terms

Android Enterprise: Dedicated Device



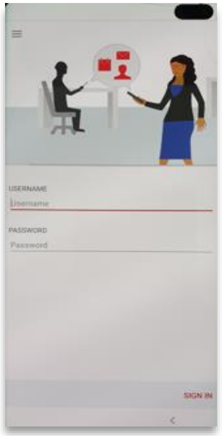
Get Ready for Work with Mobile@Work

To configure and secure your device, enter your company's server URL

SERVER URL

URL

Enter server URL
& hit NEXT



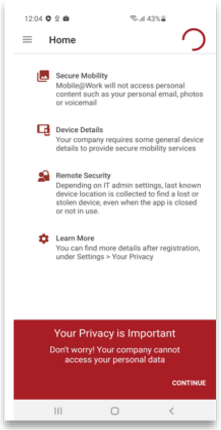
USERNAME

Username

PASSWORD

Password

Enter credentials
& hit SIGN IN



12:04 43%

Home

Secure Mobility
Mobile@Work will not access personal content such as your personal email, photos or voicemail

Device Details
Your company requires some general device details to provide secure mobility services

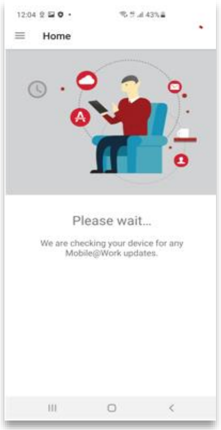
Remote Security
Depending on IT admin settings, last known device location is collected to find a lost or stolen device, even when the app is closed or not in use.

Learn More
You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important

Don't worry! Your company cannot access your personal data

Tap CONTINUE



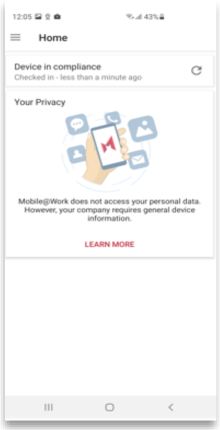
12:04 43%

Home

Please wait...

We are checking your device for any Mobile@Work updates.

Please wait
For a short while



12:05 43%

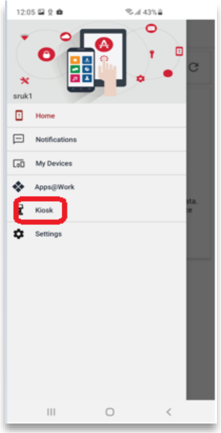
Home

Device in compliance
Checked in - less than a minute ago

Your Privacy

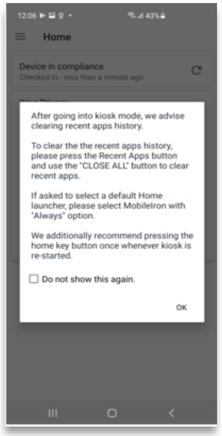
Mobile@Work does not access your personal data. However, your company requires general device information.

Device Enrollment
Successful!



12:05 43%

In the
Mobile@Work client
you can start Kiosk



12:06 43%

Home

Device in compliance
Checked in - less than a minute ago

After going into kiosk mode, we advise clearing recent apps history.

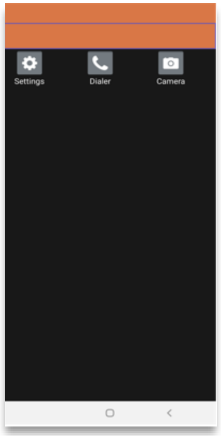
To clear the the recent apps history, please press the Recent Apps button and use the "CLOSE ALL" button to clear recent apps.

If asked to select a default Home launcher, please select MobileIron with "Always" option.

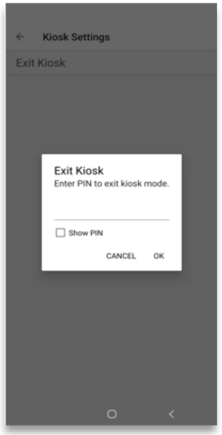
We additionally recommend pressing the home key button once whenever kiosk is re-started.

□ Do not show this again.

Accept the usage
of the kiosk



Kiosk is fully
configured



Kiosk Settings

Exit Kiosk

Exit Kiosk
Enter PIN to exit kiosk mode.

□ Show PIN

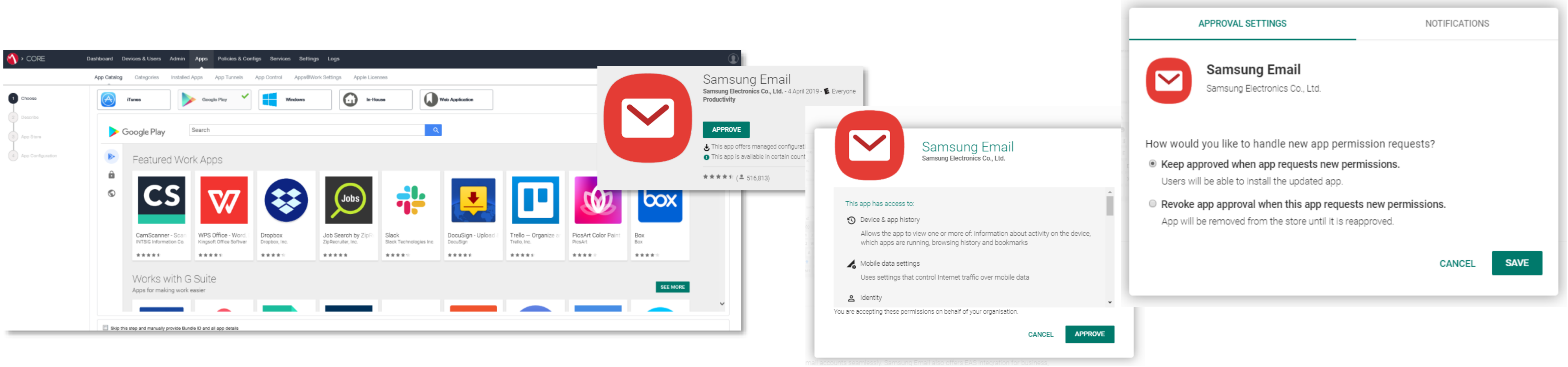
As an admin you can exit
the kiosk using a PIN

Managed Google Play Configuration

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.



Samsung Email
Samsung Electronics Co., Ltd. - 4 April 2019 - Everyone
Productivity

APPROVE

This app offers managed configurati
This app is available in certain count

★★★★½ (516,813)

Samsung Email
Samsung Electronics Co., Ltd.

This app has access to:

Device & app history
Allows the app to view one or more of: information about activity on the device, which apps are running, browsing history and bookmarks

Mobile data settings
Uses settings that control Internet traffic over mobile data

Identity

You are accepting these permissions on behalf of your organisation.

CANCEL APPROVE

APPROVAL SETTINGS NOTIFICATIONS

Samsung Email
Samsung Electronics Co., Ltd.

How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

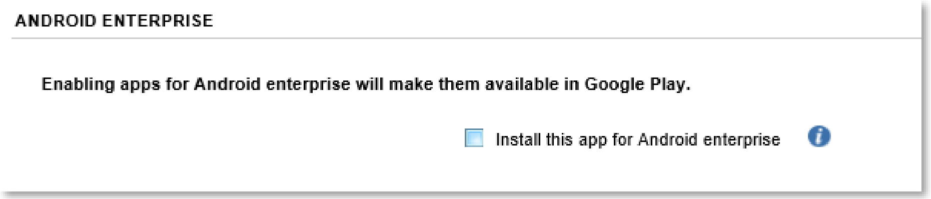
CANCEL SAVE

Managed Google Play Configuration

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’

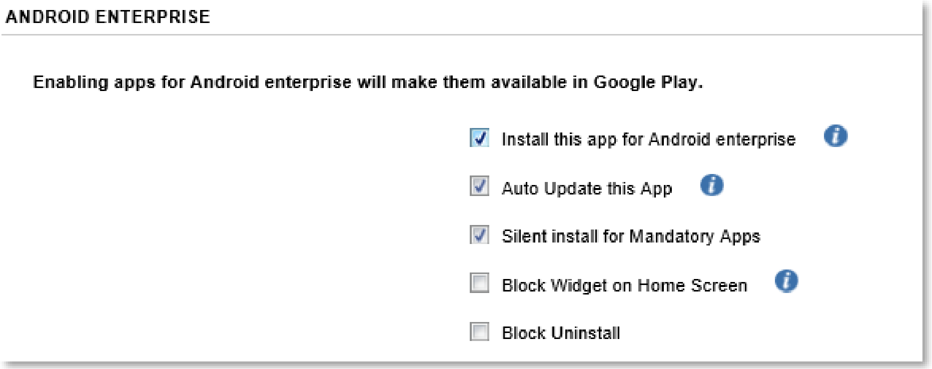
- There are a few configurations you can set for the Android Enterprise app, select what is needed.
- Once this has been completed, save the config by clicking Save.



ANDROID ENTERPRISE

Enabling apps for Android enterprise will make them available in Google Play.

□ Install this app for Android enterprise



ANDROID ENTERPRISE

Enabling apps for Android enterprise will make them available in Google Play.

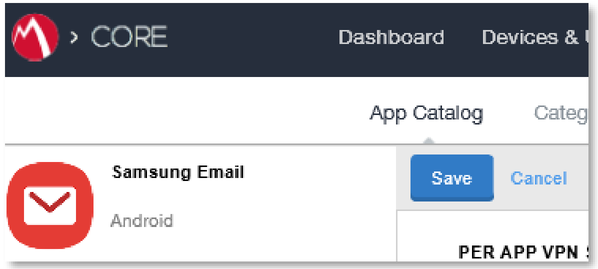
☑ Install this app for Android enterprise

☑ Auto Update this App

☑ Silent install for Mandatory Apps

□ Block Widget on Home Screen

□ Block Uninstall



Samsung Email

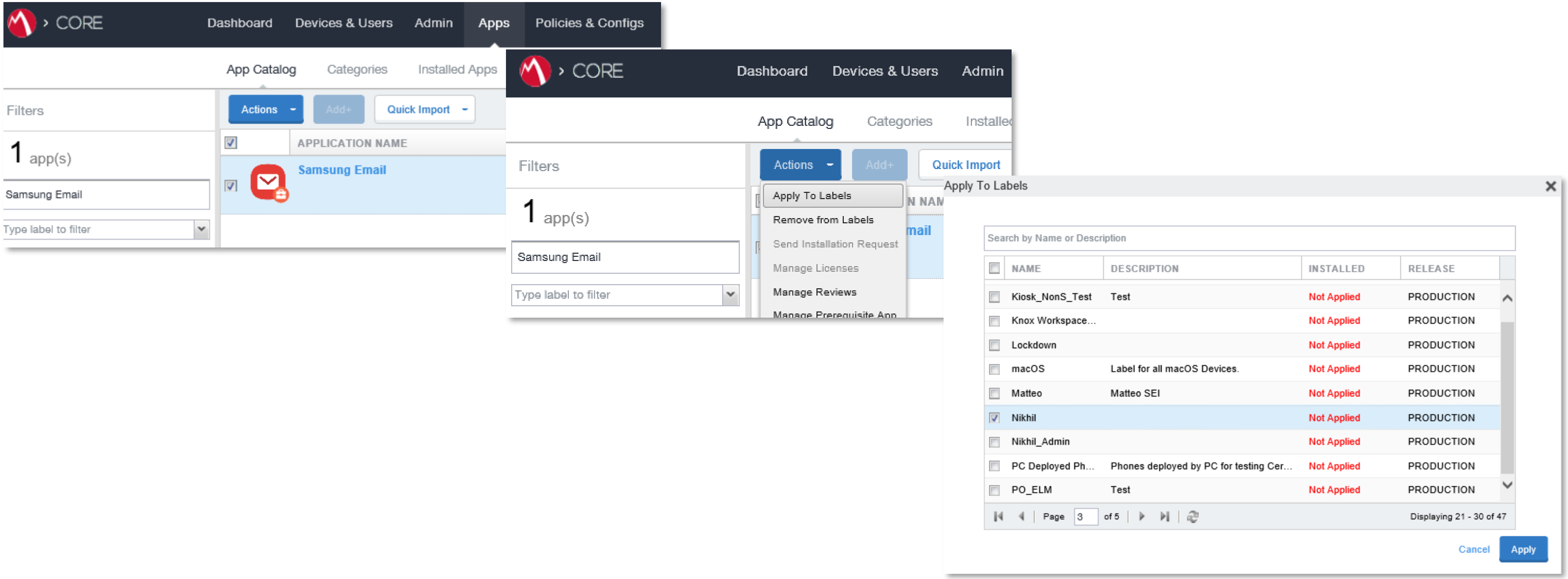
Android

Managed Google Play Configuration

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.



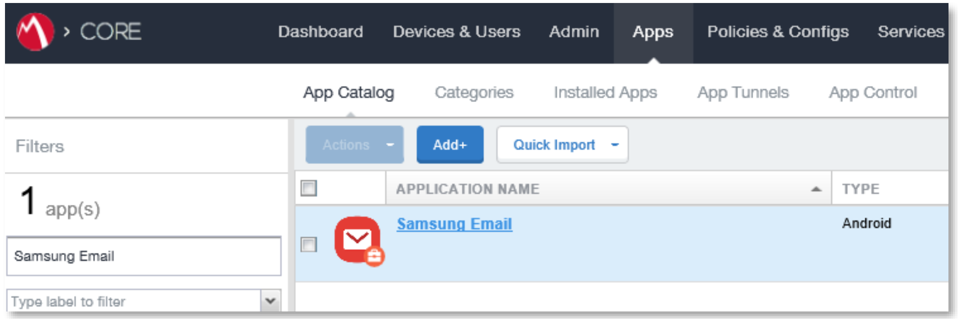
□	NAME	DESCRIPTION	INSTALLED	RELEASE
□	Kiosk_NonS_Test	Test	Not Applied	PRODUCTION
□	Knox Workspace…		Not Applied	PRODUCTION
□	Lockdown		Not Applied	PRODUCTION
□	macOS	Label for all macOS Devices.	Not Applied	PRODUCTION
□	Matteo	Matteo SEI	Not Applied	PRODUCTION
☑	Nikhil		Not Applied	PRODUCTION
□	Nikhil_Admin		Not Applied	PRODUCTION
□	PC Deployed Ph…	Phones deployed by PC for testing Cer…	Not Applied	PRODUCTION
□	PO_ELM	Test	Not Applied	PRODUCTION

AppConfig on MobileIron Core UEM

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 instructions below.

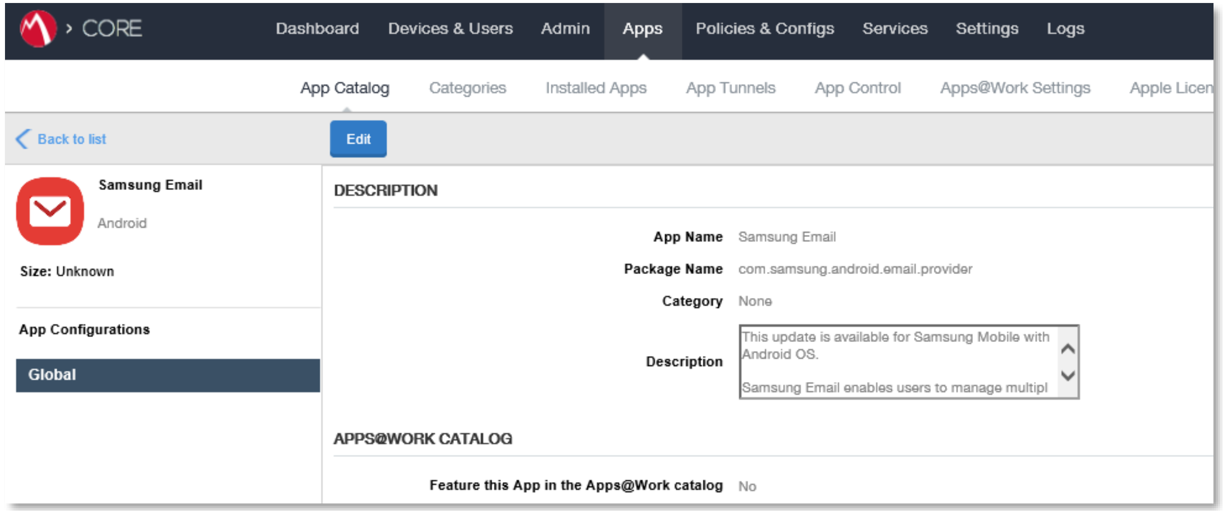
- Navigate to **Apps -> App Catalog -> Click on the app you would like to configure -> Edit**



1 app(s)

Samsung Email

APPLICATION NAME	TYPE
Samsung Email	Android



Samsung Email

Android

Size: Unknown

DESCRIPTION

App Name: Samsung Email

Package Name: com.samsung.android.email.provider

Category: None

Description: This update is available for Samsung Mobile with Android OS.

Samsung Email enables users to manage multipl

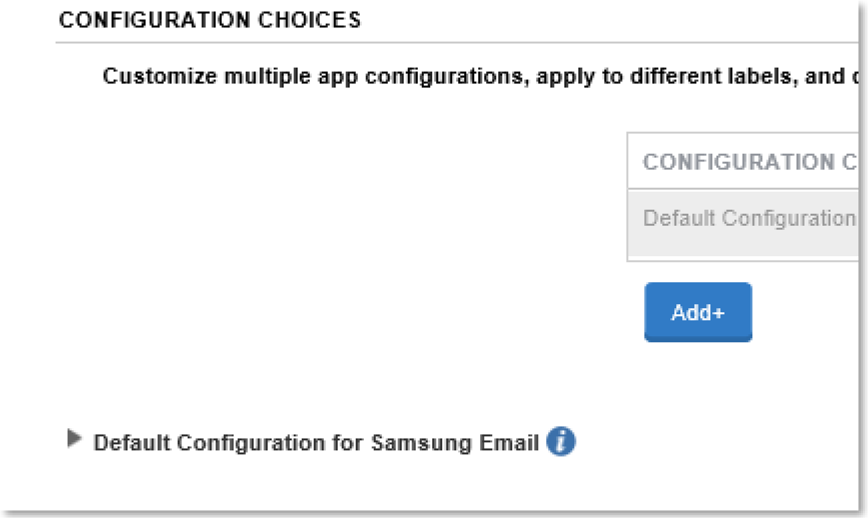
APPS@WORK CATALOG

Feature this App in the Apps@Work catalog: No

AppConfig on MobileIron Core UEM

AppConfig

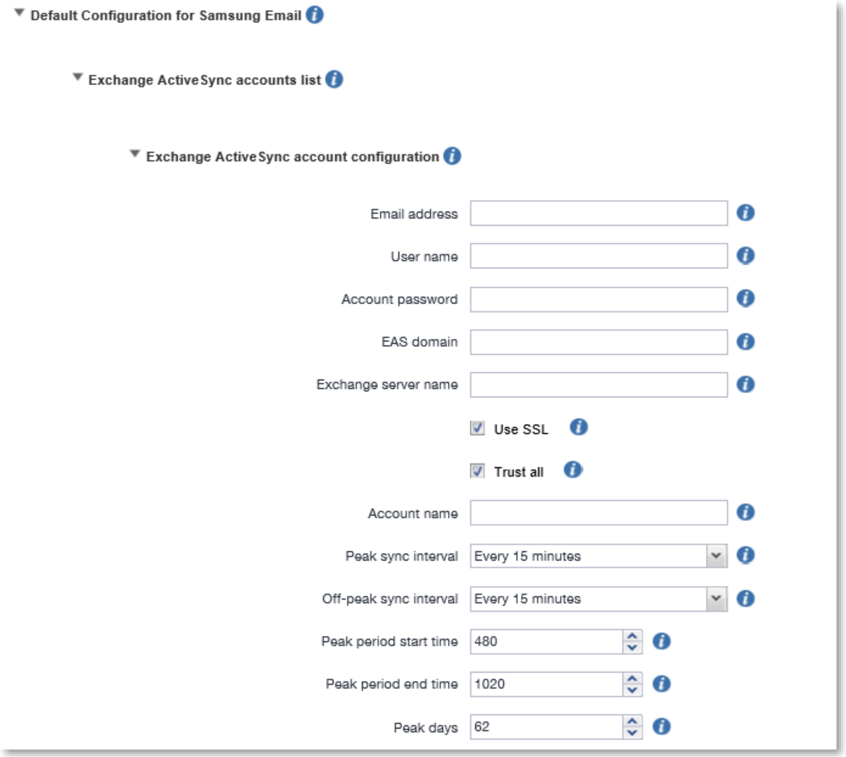
- Scroll down to the ‘Configuration Choices’ section
- Expand ‘Default Configuration for xxx’ & configure the various options you wish and then when you are finished, click the Save button.
- Confirm the assignment by clicking Save. You have now used AppConfig to distribute a Managed Play app with a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



CONFIGURATION CHOICES

Customize multiple app configurations, apply to different labels, and c

▶ Default Configuration for Samsung Email



▼ Default Configuration for Samsung Email

▼ Exchange ActiveSync accounts list

▼ Exchange ActiveSync account configuration

Email address
User name
Account password
EAS domain
Exchange server name
☑ Use SSL
☑ Trust all
Account name
Peak sync interval: Every 15 minutes
Off-peak sync interval: Every 15 minutes
Peak period start time: 480
Peak period end time: 1020
Peak days: 62

Configure Knox Platform for Enterprise : Standard Edition

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 [FREE or $ for some special options such as Dual DAR]

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 8.0 or above.

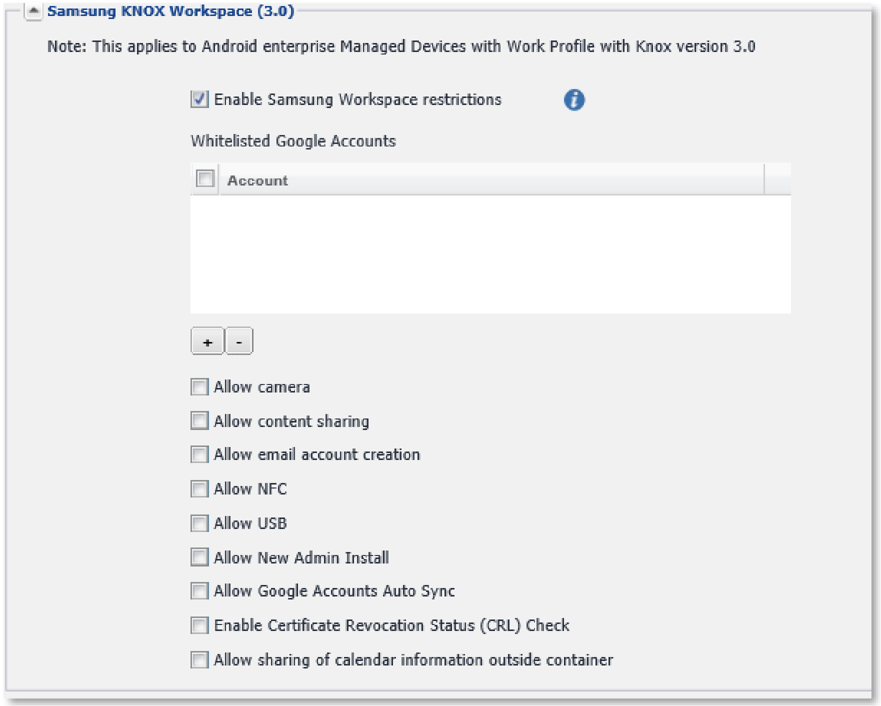
SAMSUNG
Knox Platform for Enterprise
Android Enterprise

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 instructions below.

- 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!



Samsung KNOX Workspace (3.0)

Note: This applies to Android enterprise Managed Devices with Work Profile with Knox version 3.0

☑ Enable Samsung Workspace restrictions

Whitelisted Google Accounts

□ Account

□ Allow camera

□ Allow content sharing

□ Allow email account creation

□ Allow NFC

□ Allow USB

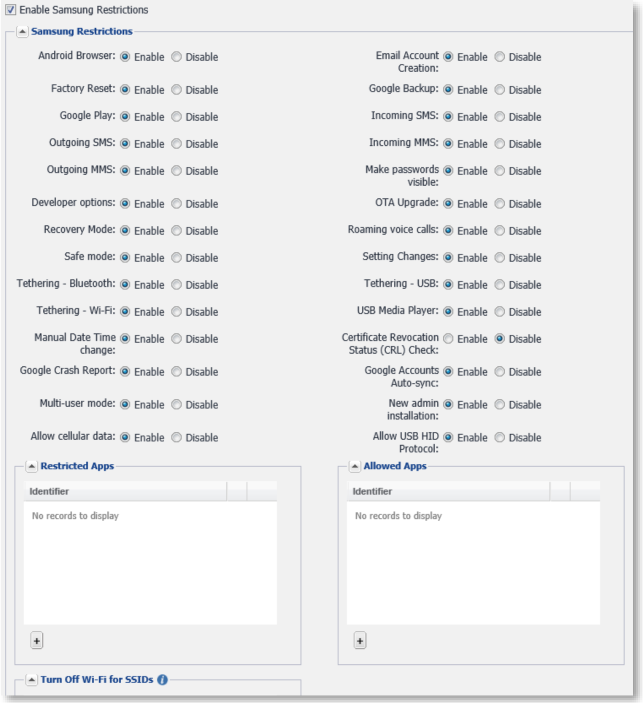
□ Allow New Admin Install

□ Allow Google Accounts Auto Sync

□ Enable Certificate Revocation Status (CRL) Check

□ Allow sharing of calendar information outside container

Work Profile Samsung KPE Standard Features



☑ Enable Samsung Restrictions

Samsung Restrictions

Android Browser: ● Enable ○ Disable

Factory Reset: ● Enable ○ Disable

Google Play: ● Enable ○ Disable

Outgoing SMS: ● Enable ○ Disable

Outgoing MMS: ● Enable ○ Disable

Developer options: ● Enable ○ Disable

Recovery Mode: ● Enable ○ Disable

Safe mode: ● Enable ○ Disable

Tethering - Bluetooth: ● Enable ○ Disable

Tethering - Wi-Fi: ● Enable ○ Disable

Manual Date Time change: ● Enable ○ Disable

Google Crash Report: ● Enable ○ Disable

Multi-user mode: ● Enable ○ Disable

Allow cellular data: ● Enable ○ Disable

Email Account Creation: ● Enable ○ Disable

Google Backup: ● Enable ○ Disable

Incoming SMS: ● Enable ○ Disable

Incoming MMS: ● Enable ○ Disable

Make passwords visible: ● Enable ○ Disable

OTA Upgrade: ● Enable ○ Disable

Roaming voice calls: ● Enable ○ Disable

Setting Changes: ● Enable ○ Disable

Tethering - USB: ● Enable ○ Disable

USB Media Player: ● Enable ○ Disable

Certificate Revocation Status (CRL) Check: ○ Enable ● Disable

Google Accounts Auto-sync: ● Enable ○ Disable

New admin installation: ● Enable ○ Disable

Allow USB HID Protocol: ● Enable ○ Disable

Restricted Apps

Identifier

No records to display

Allowed Apps

Identifier

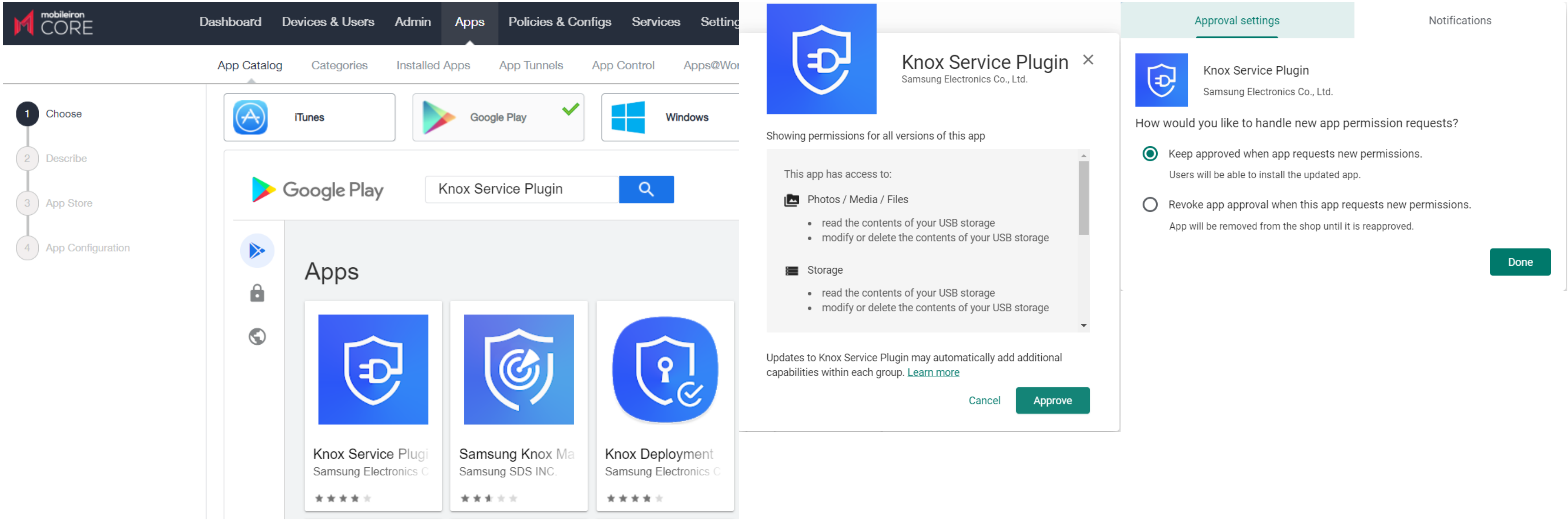
No records to display

Turn Off Wi-Fi for SSIDs

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.**



Knox Service Plugin

Knox Service Plugin
Samsung Electronics Co., Ltd.

Showing permissions for all versions of this app

This app has access to:

Photos / Media / Files
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Storage
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Updates to Knox Service Plugin may automatically add additional capabilities within each group. Learn more

Knox Service Plugin
Samsung Electronics Co., Ltd.

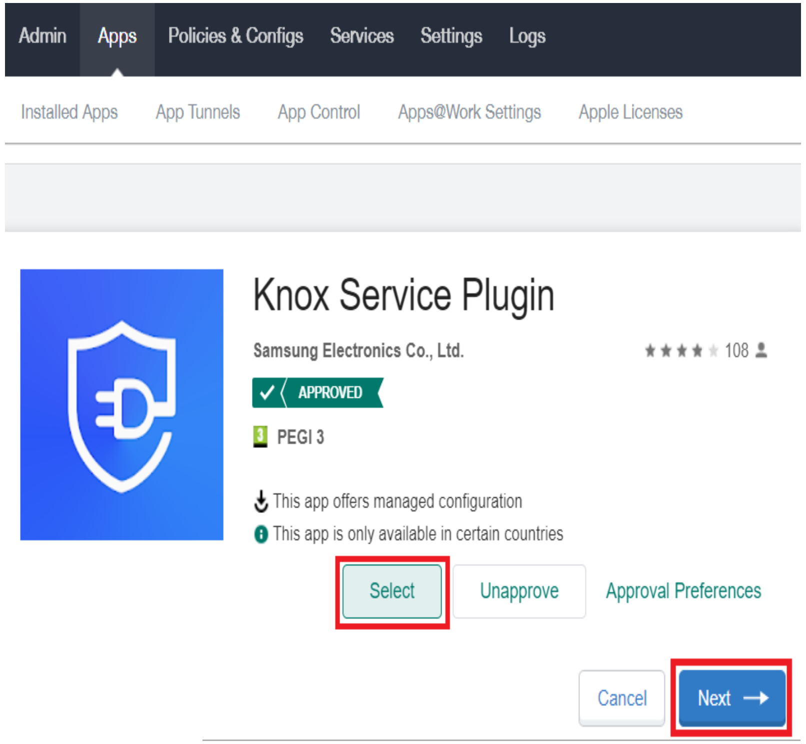
How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the shop until it is reapproved.

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.**



Knox Service Plugin

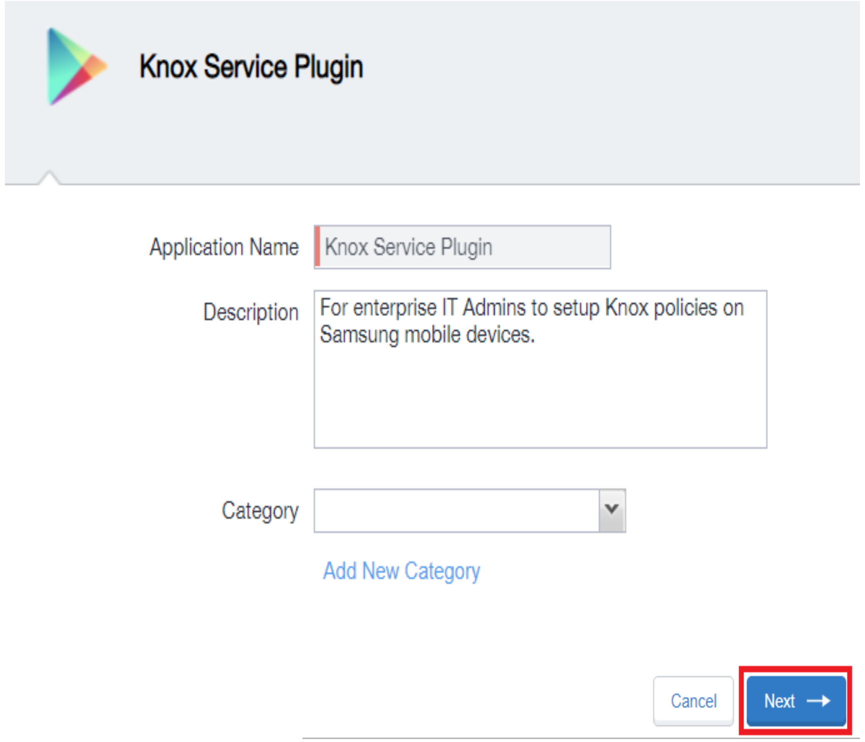
Samsung Electronics Co., Ltd. ★★★★ 108

APPROVED

PEGI 3

This app offers managed configuration

This app is only available in certain countries

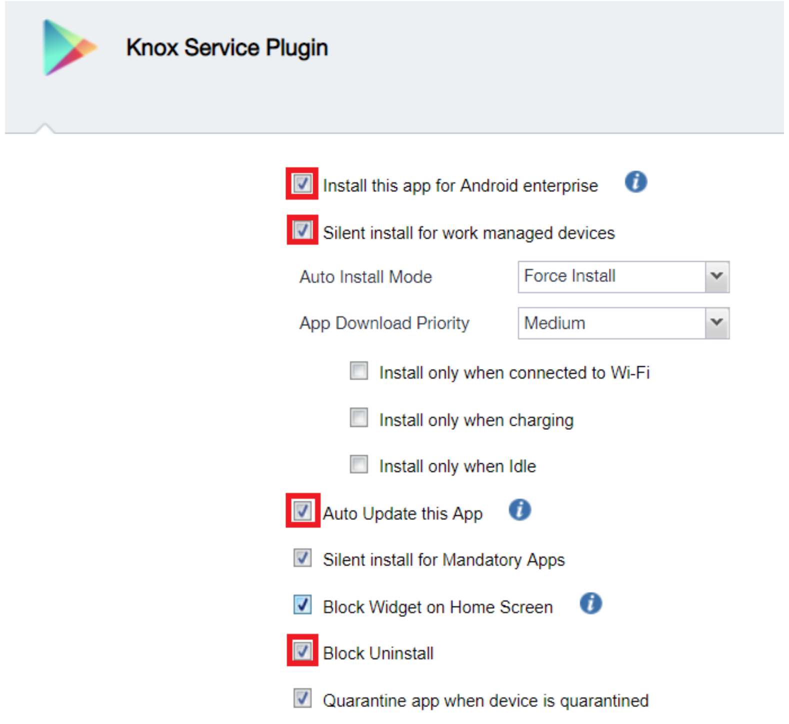


Knox Service Plugin

Application Name: Knox Service Plugin

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

Category:

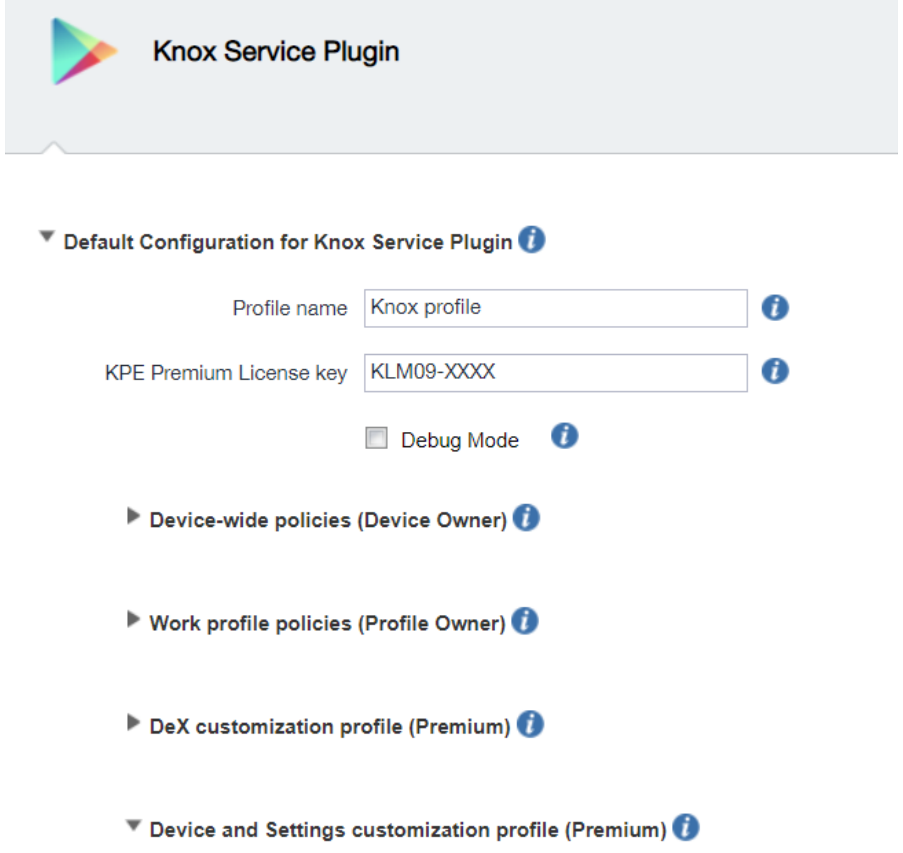


Knox Service Plugin

- ☑ 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

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.**



Knox Service Plugin

▼ Default Configuration for Knox Service Plugin

Profile name: Knox profile

KPE Premium License key: KLM09-XXXX

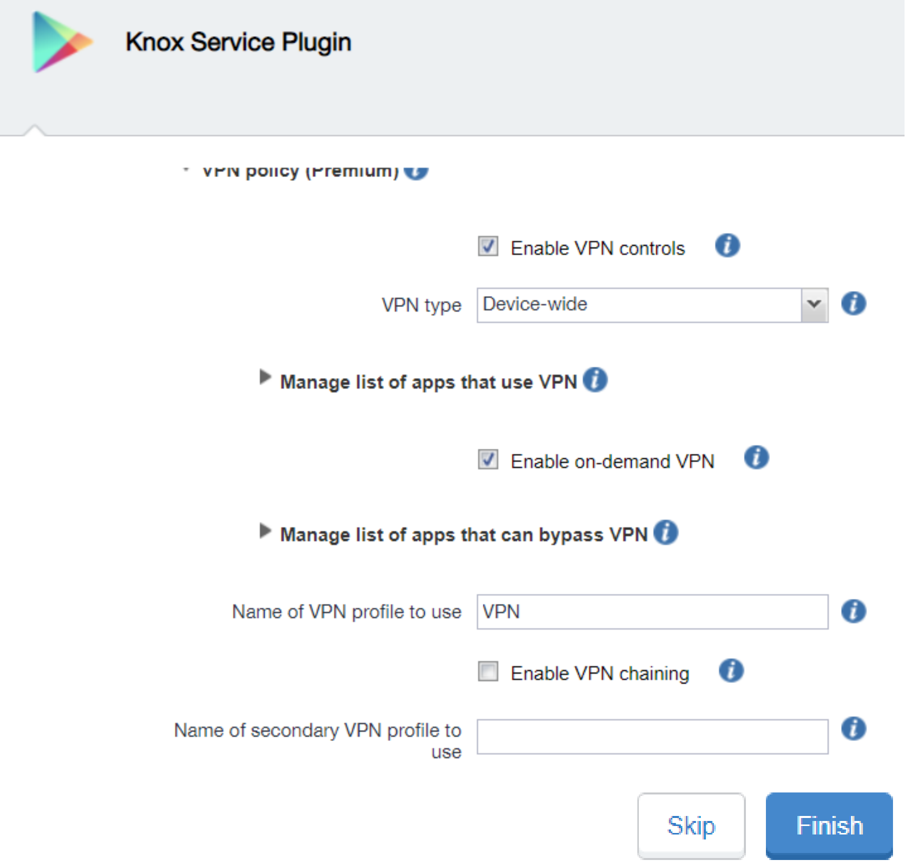
□ Debug Mode

▶ 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: Device-wide

▶ Manage list of apps that use VPN

☑ Enable on-demand VPN

▶ Manage list of apps that can bypass VPN

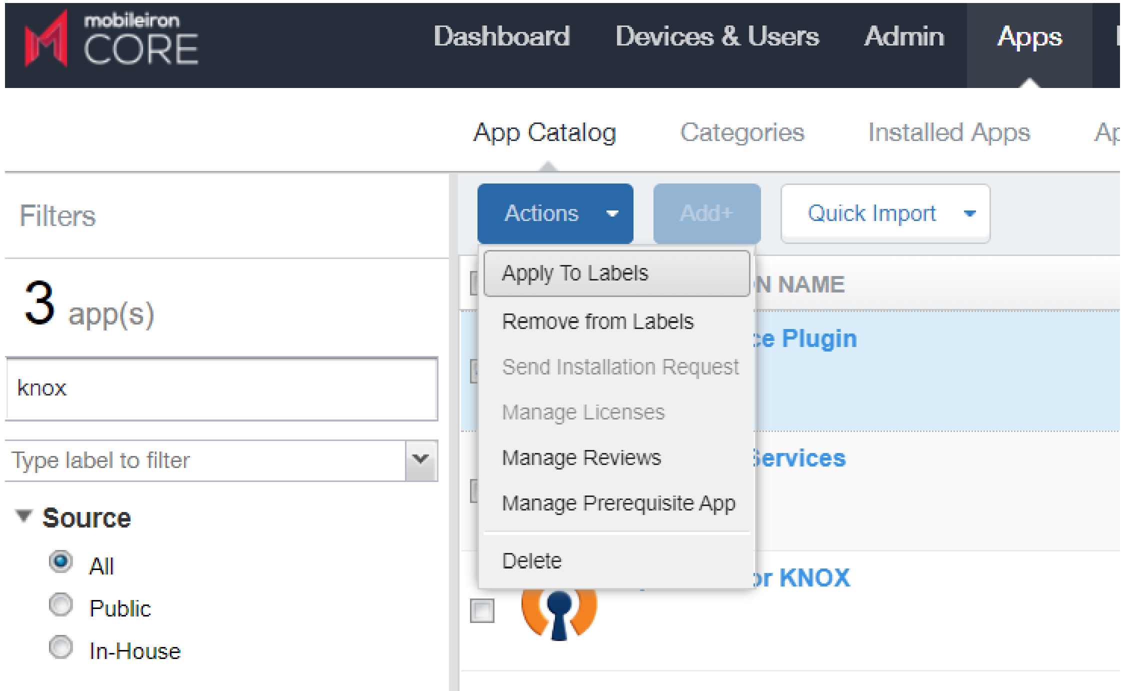
Name of VPN profile to use: VPN

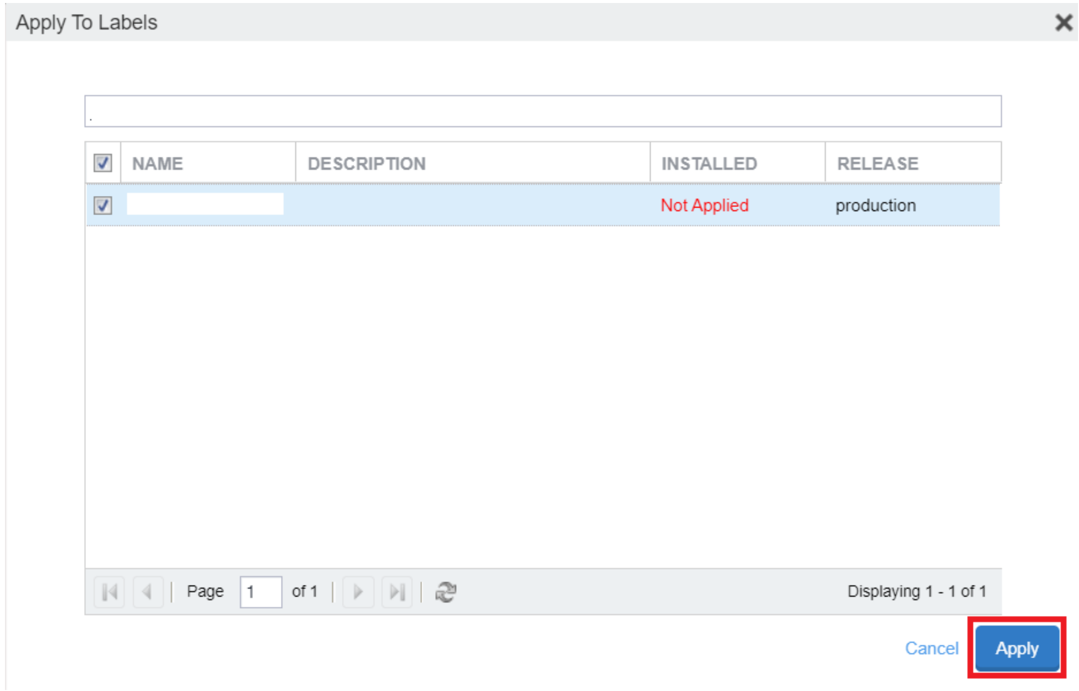
□ Enable VPN chaining

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.**




Apply To Labels

☑	NAME	DESCRIPTION	INSTALLED	RELEASE
☑			Not Applied	production

Page 1 of 1 — Displaying 1 - 1 of 1

Document Information

This is version 2.2 of this document.

Thank you!

Knox