MobileIron Cloud UEM 78

Knox Platform for Enterprise

August 2021
Samsung R&D Centre UK
(SRUK)

Agenda

1. Pre-requisites for Knox Platform for Enterprise
2. Configure Android Enterprise
3. Android Enterprise Deployment Modes
   - Work Profile
   - Fully Managed 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 Cloud
6. Configure Knox Platform for Enterprise : Standard Edition
7. Configure Knox Service Plugin [KSP]
8. Configure Knox Platform for Enterprise : Premium Edition

MobileIron Collateral & Contacts

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

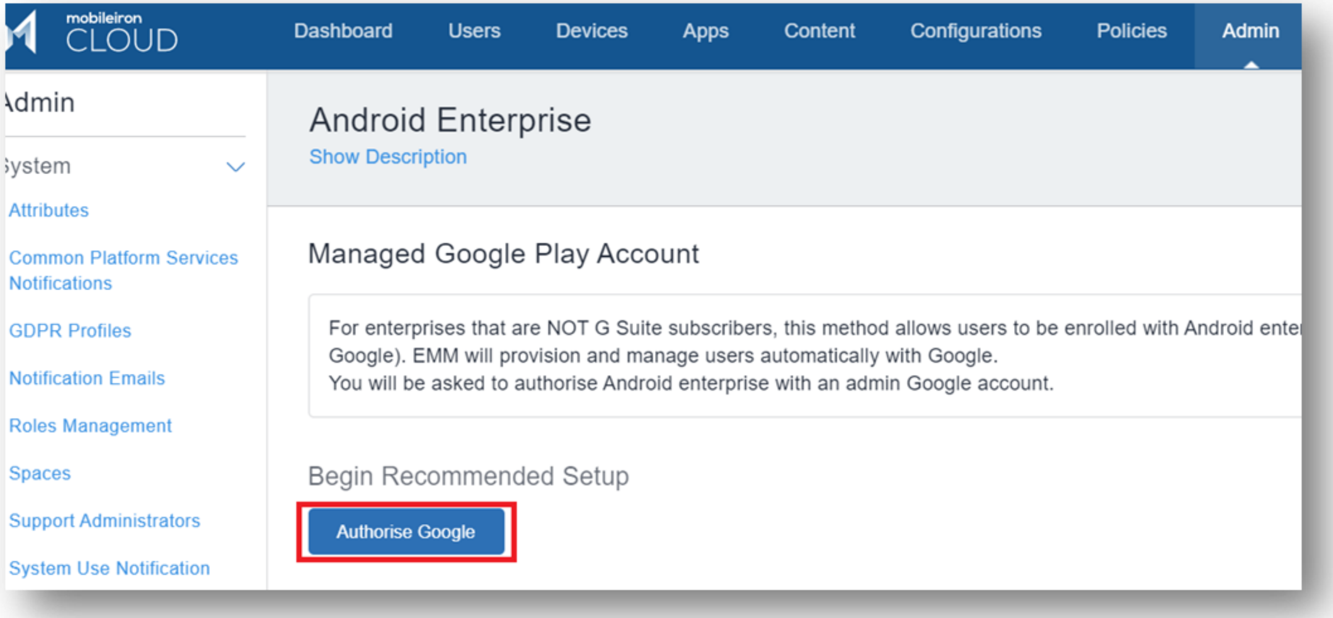
https://forums.ivanti.com/s/welcome-mobileiron?language=en_US

Pre-Requisites for Knox Platform for Enterprise

1. Obtain access to MobileIron Cloud console
2. A Gmail account to map to MobileIron Cloud 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

- Within the MobileIron Cloud console, navigate to: Admin > Google > Android Enterprise
- Under Begin Recommended Setup, select Authorise Google
- Sign into your Google account and select Get started

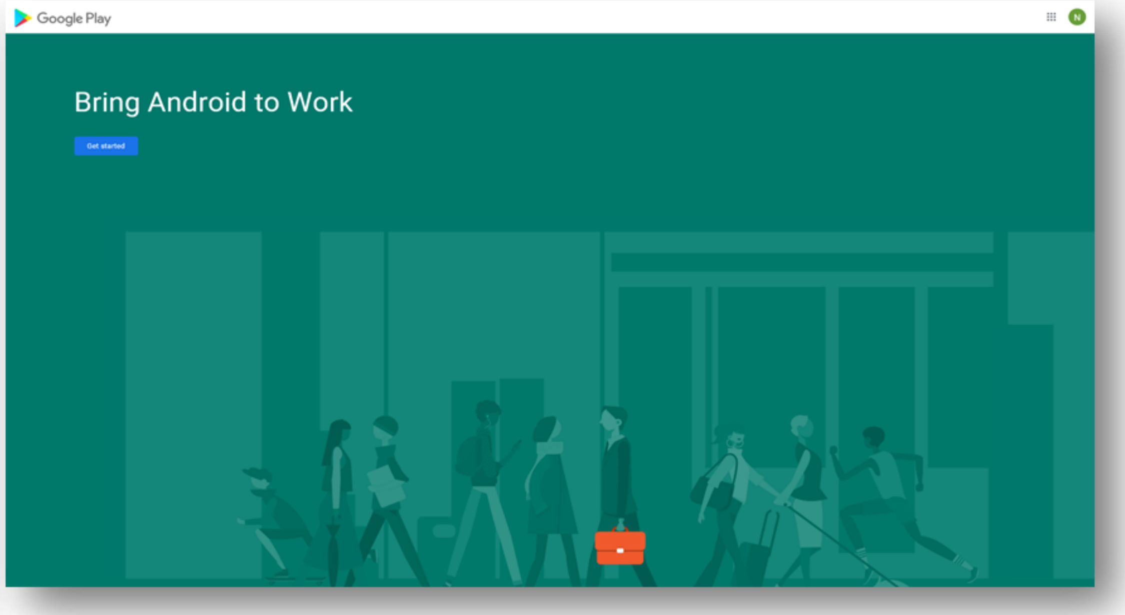


Android Enterprise

Managed Google Play Account

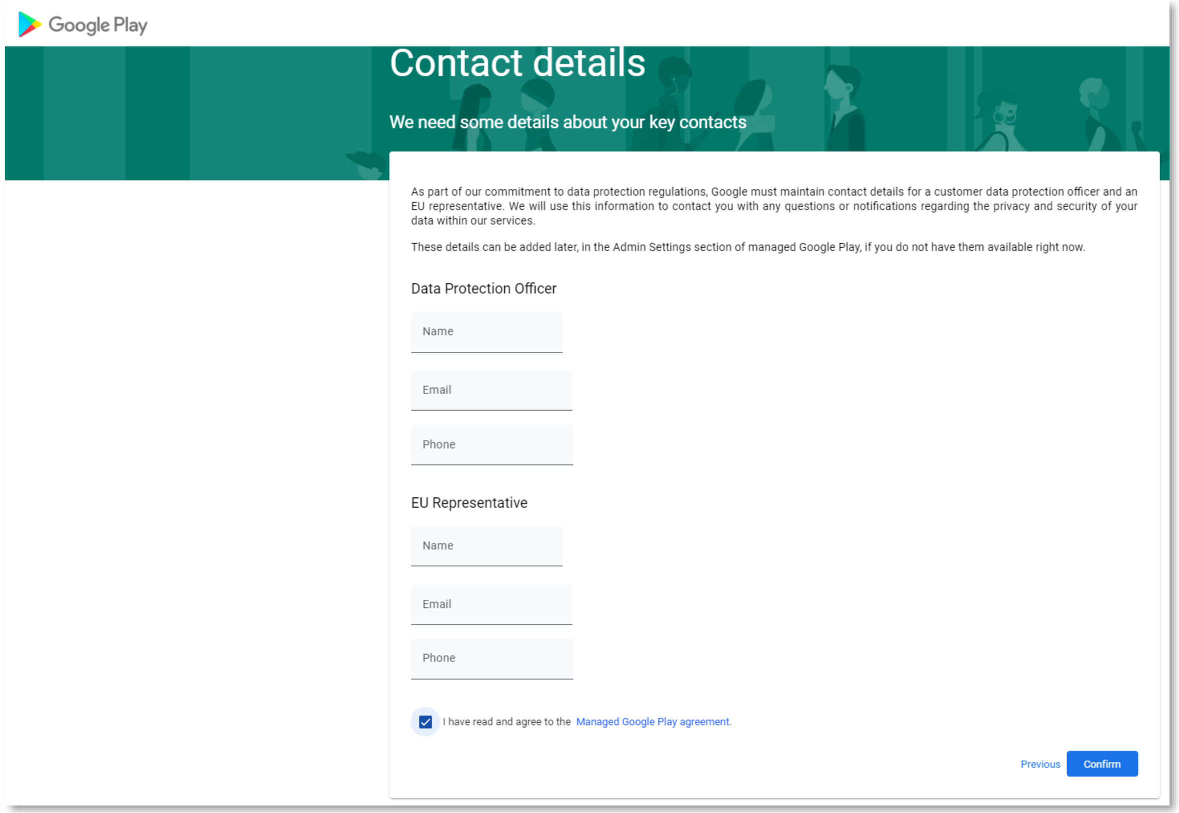
For enterprises that are NOT G Suite subscribers, this method allows users to be enrolled with Android ente
Google). EMM will provision and manage users automatically with Google.
You will be asked to authorise Android enterprise with an admin Google account.

Begin Recommended Setup



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 the MobileIron Cloud console.



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 protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your 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 right now.

Data Protection Officer

Name

Email

Phone

EU Representative

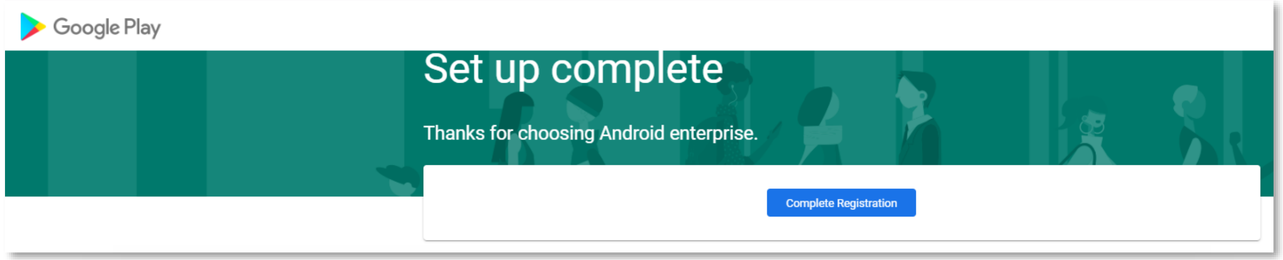
Name

Email

Phone

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

Previous Confirm

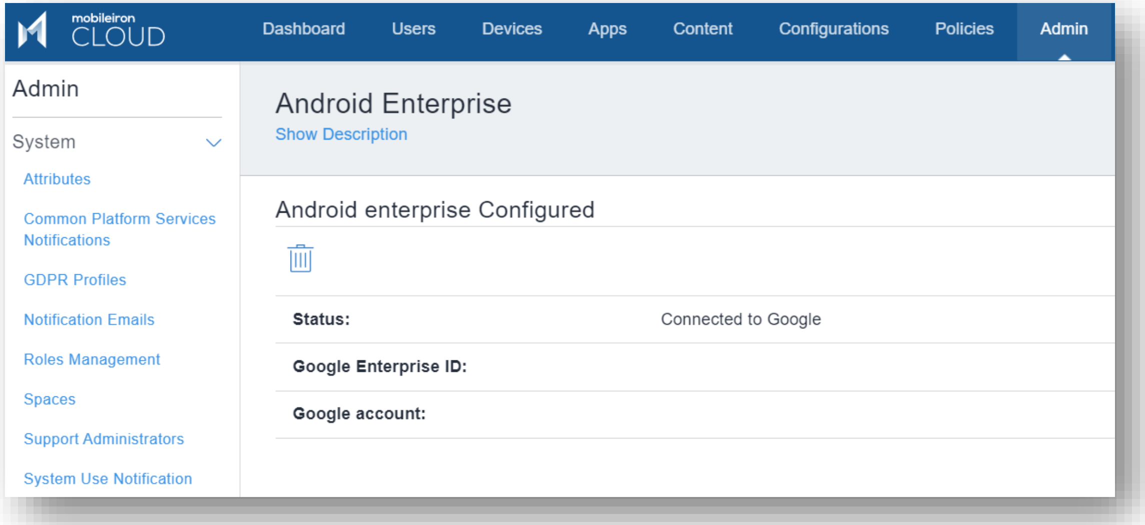


Google Play

Set up complete

Thanks for choosing Android enterprise.

Complete Registration



Admin

System

- Attributes
- Common Platform Services Notifications
- GDPR Profiles
- Notification Emails
- Roles Management
- Spaces
- Support Administrators
- System Use Notification

Android Enterprise

Show Description

Android enterprise Configured

Status:	Connected to Google
Google Enterprise ID:	
Google account:	

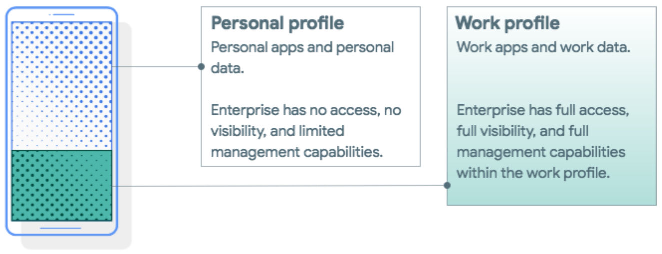
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 5 deployment modes

1. Work Profile [*formerly known as Profile Owner*]
2. Fully Managed Device [*formerly known as Device Owner*]
3. Fully Managed Device with a Work Profile [*formerly known as COMP*]
4. Work Profile on Company Owned Device [Android 11+]
5. Dedicated device [*formerly known as COSU*]

MobileIron Cloud 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.



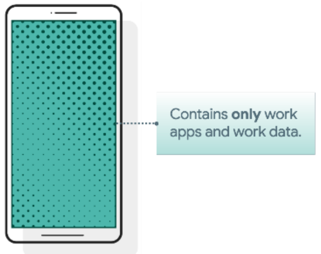
Personal apps and personal data.

Enterprise has no access, no visibility, and limited management capabilities.

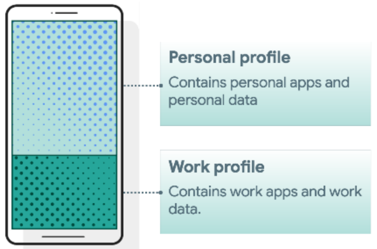
Work apps and work data.

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

Work Profile


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

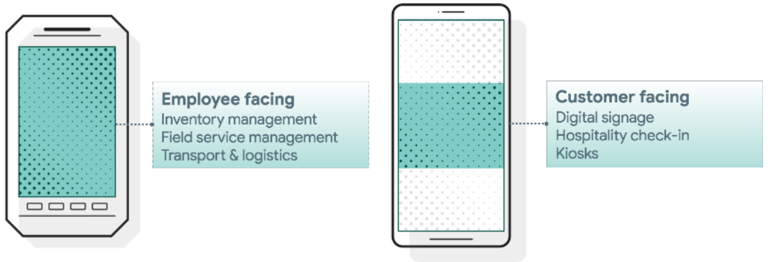
Fully Managed Device



Contains personal apps and personal data

Contains work apps and work data.

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

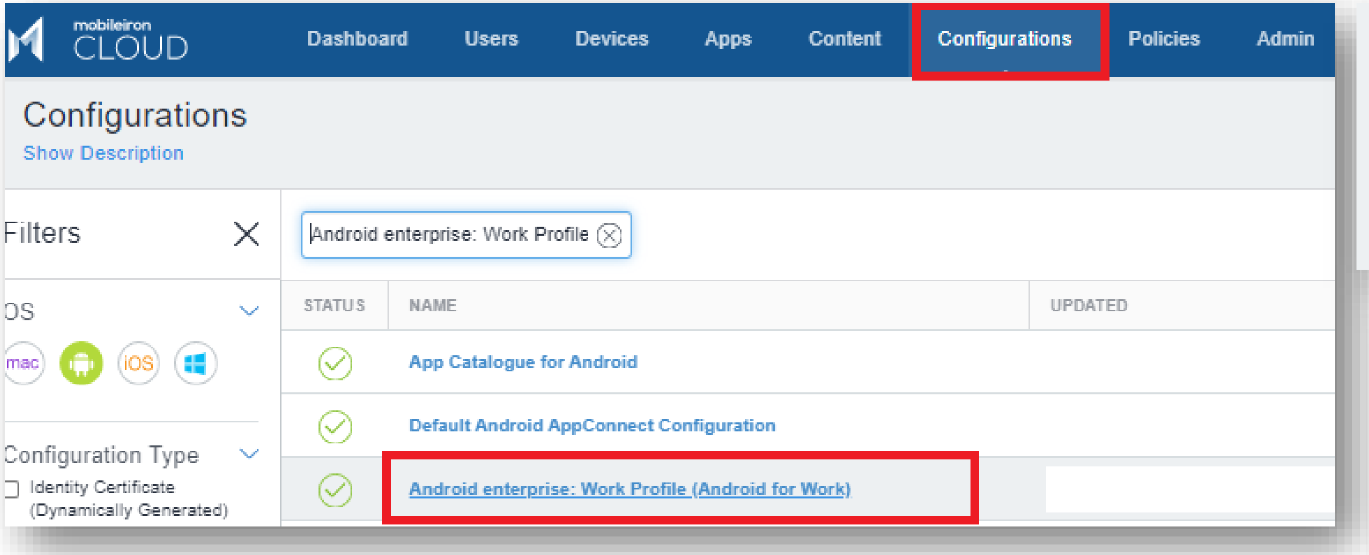


Dedicated Device

Android Enterprise: Work Profile

First, you will need to assign your Device Group to the Work Profile configuration.

- Within the MobileIron console, navigate to: Configurations and search for "Android enterprise: Work Profile"
- Select 'Android enterprise: Work Profile (Android for Work)'
- Select Edit
- Select Next

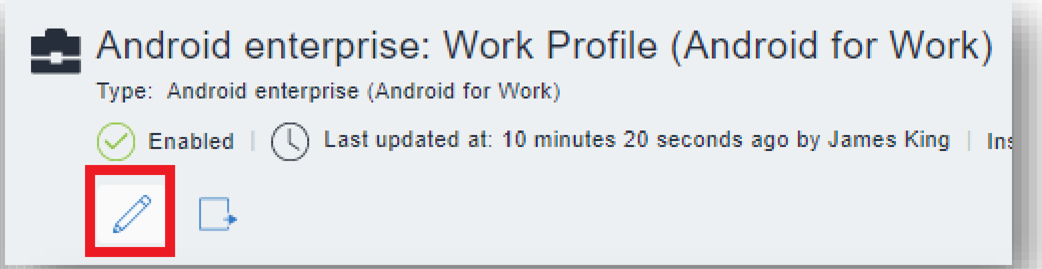


Configurations

Android enterprise: Work Profile

☐ Identity Certificate (Dynamically Generated)

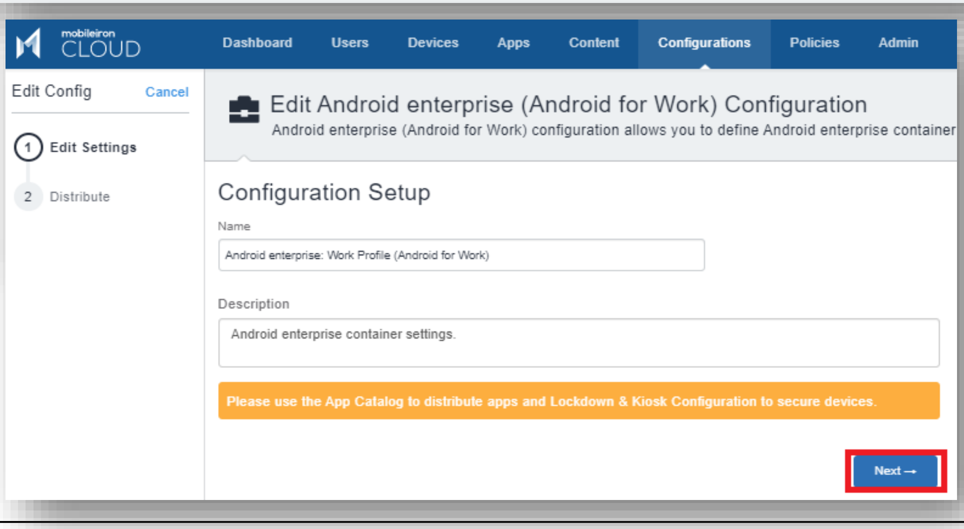
STATUS	NAME	UPDATED
✓	App Catalogue for Android	
✓	Default Android AppConnect Configuration	
✓	Android enterprise: Work Profile (Android for Work)	



Android enterprise: Work Profile (Android for Work)

Type: Android enterprise (Android for Work)

✓ Enabled | Last updated at: 10 minutes 20 seconds ago by James King | Ins



Edit Android enterprise (Android for Work) Configuration

Android enterprise (Android for Work) configuration allows you to define Android enterprise container

Configuration Setup

Name: Android enterprise: Work Profile (Android for Work)

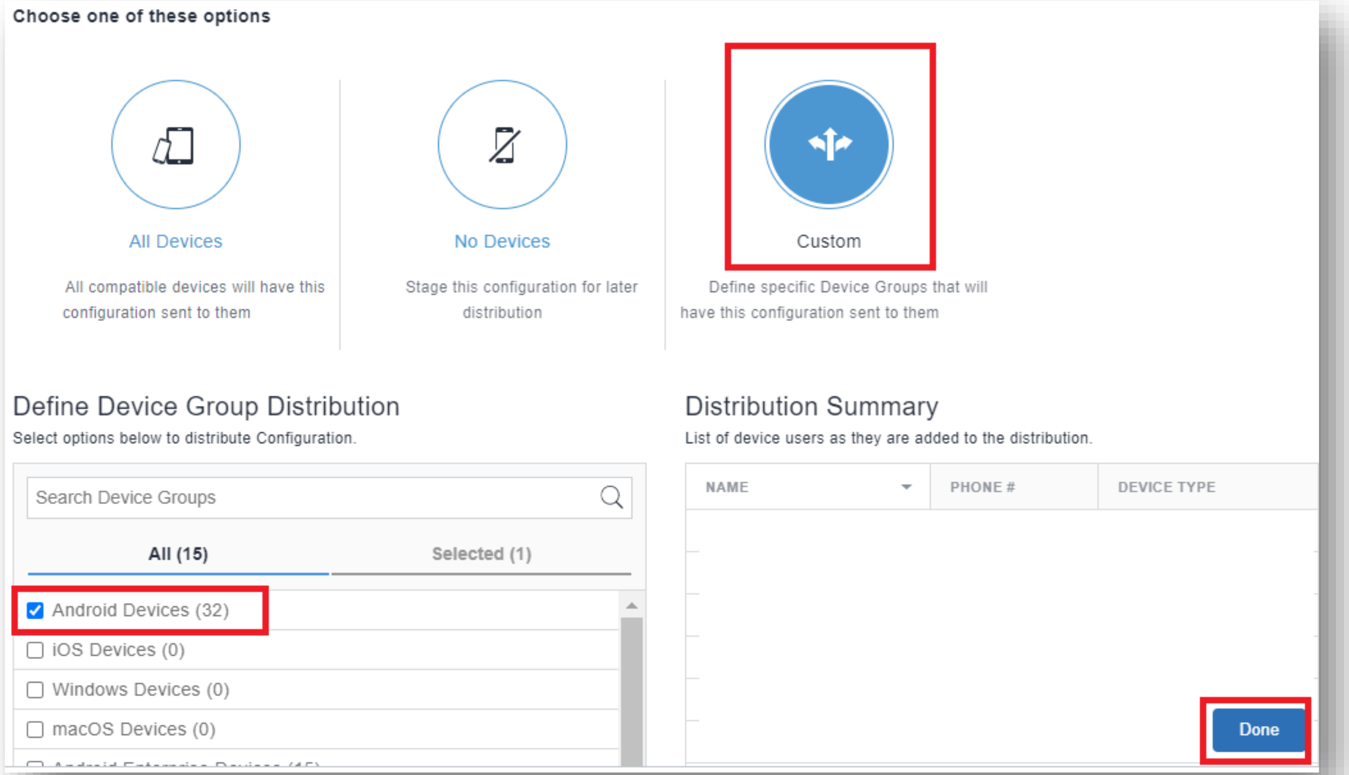
Description: Android enterprise container settings.

Please use the App Catalog to distribute apps and Lockdown & Kiosk Configuration to secure devices.

Android Enterprise: Work Profile

You will then need to assign this configuration to a device group.

- Select Custom
- In the Device Group Distribution box, choose your desired Device Group
- Review the Distribution Summary
- Select Done



Choose one of these options

All Devices

All compatible devices will have this configuration sent to them

No Devices

Stage this configuration for later distribution

Custom

Define specific Device Groups that will have this configuration sent to them

Define Device Group Distribution

Select options below to distribute Configuration.

Search Device Groups

All (15) | Selected (1)

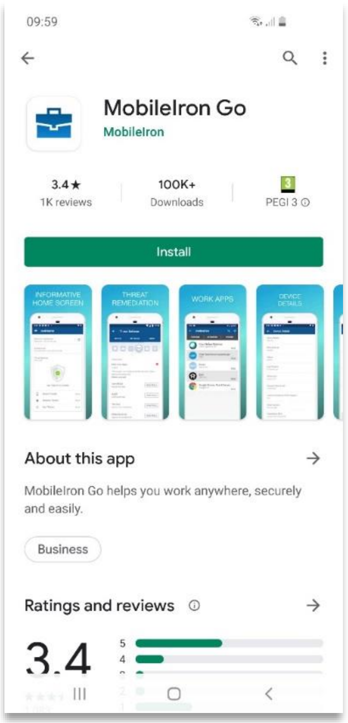
- ☑ Android Devices (32)
- ☐ iOS Devices (0)
- ☐ Windows Devices (0)
- ☐ macOS Devices (0)
- ☐ Android Enterprise Devices (15)

Distribution Summary

List of device users as they are added to the distribution.

NAME	PHONE #	DEVICE TYPE

Android Enterprise: Work Profile Enrollment



MobileIron Go
MobileIron

3.4★ 1K reviews | 100K+ Downloads | PEGI 3

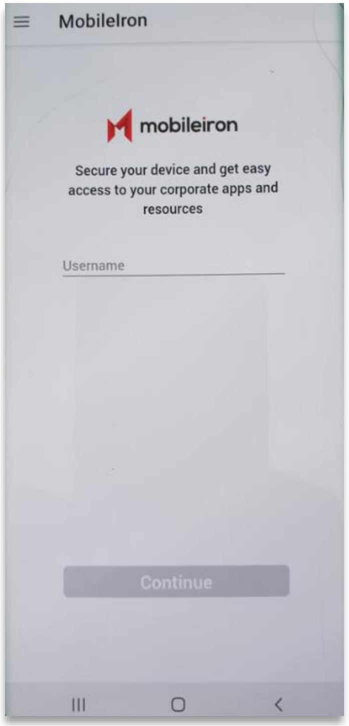
About this app

MobileIron Go helps you work anywhere, securely and easily.

Ratings and reviews

3.4

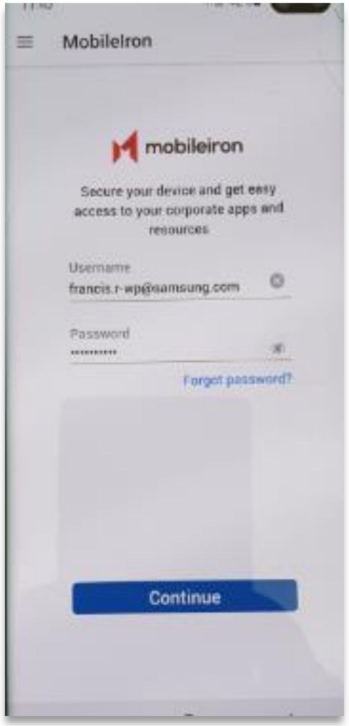
Install MobileIron Go from the Google Play Store



Secure your device and get easy access to your corporate apps and resources

Username

Open MobileIron Go, Enter Your Username and select Continue

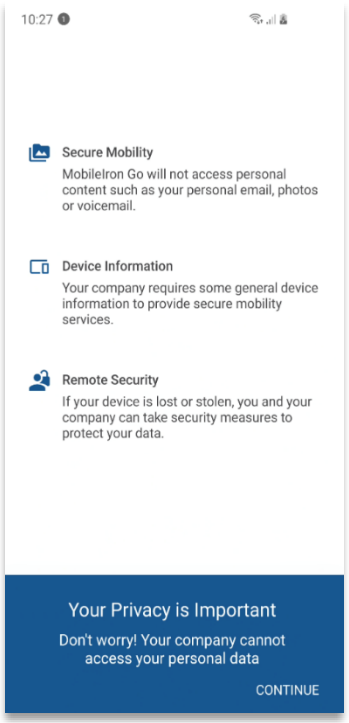


Secure your device and get easy access to your corporate apps and resources

Username: francis.r-wp@samsung.com

Password: **********

Enter your Password and select Continue



Secure Mobility
MobileIron Go will not access personal content such as your personal email, photos or voicemail.

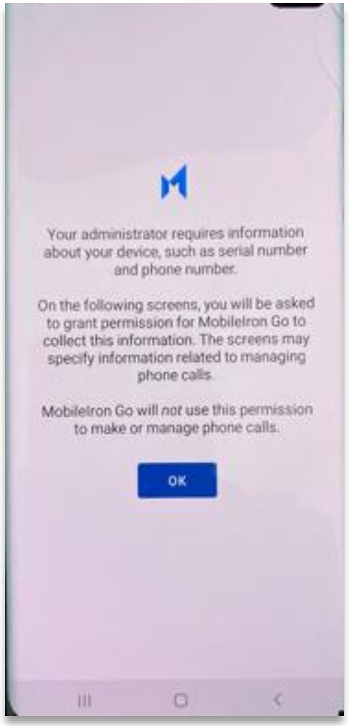
Device Information
Your company requires some general device information to provide secure mobility services.

Remote Security
If your device is lost or stolen, you and your company can take security measures to protect your data.

Your Privacy is Important

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

Select CONTINUE

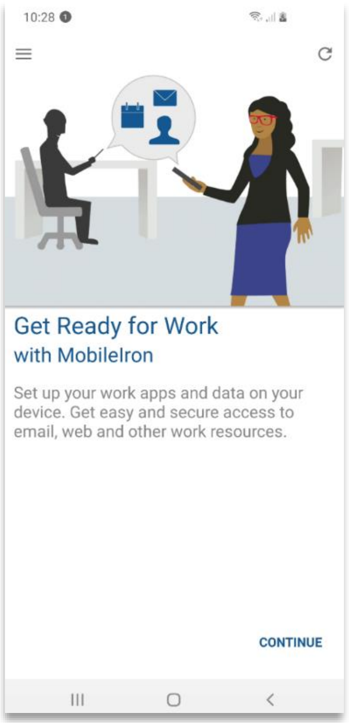


Your administrator requires information about your device, such as serial number and phone number.

On the following screens, you will be asked to grant permission for MobileIron Go to collect this information. The screens may specify information related to managing phone calls.

MobileIron Go will *not* use this permission to make or manage phone calls.

Select OK

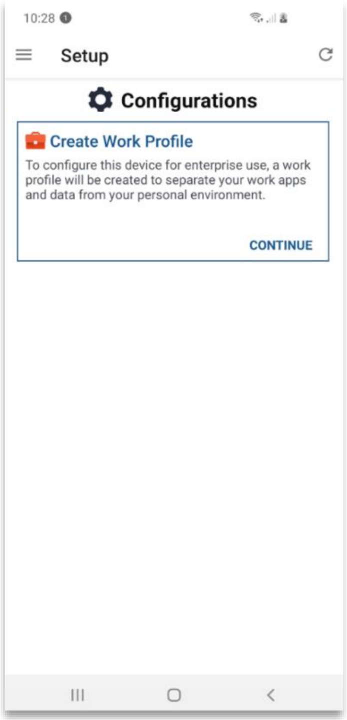


Get Ready for Work with MobileIron

Set up your work apps and data on your device. Get easy and secure access to email, web and other work resources.

Select CONTINUE

Android Enterprise: Work Profile Enrollment


10:28

Setup

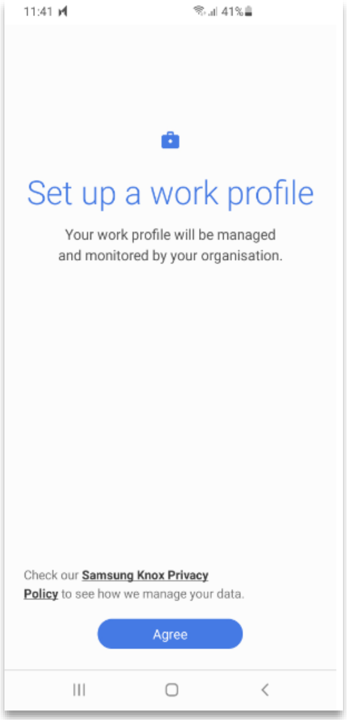
Configurations

Create Work Profile

To configure this device for enterprise use, a work profile will be created to separate your work apps and data from your personal environment.

CONTINUE

Select CONTINUE


11:41 41%

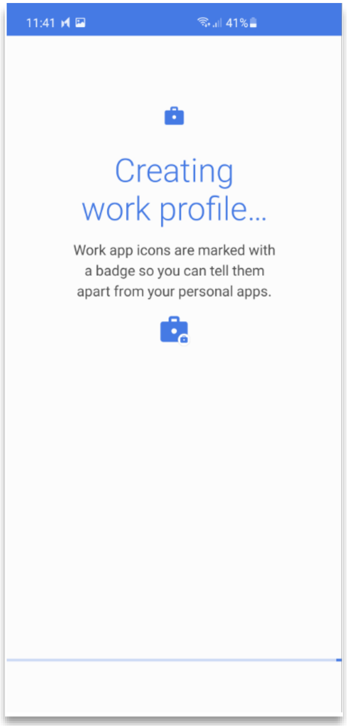
Set up a work profile

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

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

Agree

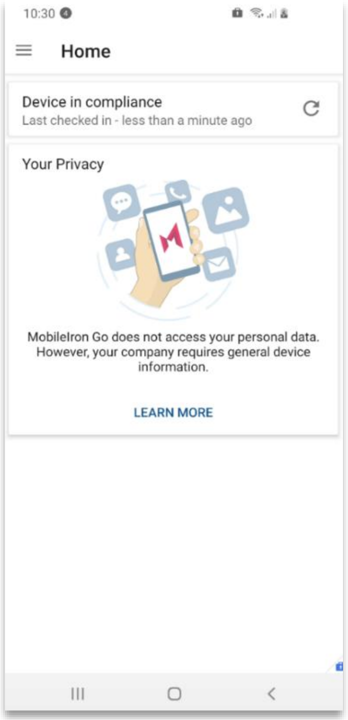
Select Agree


11:41 41%

Creating work profile...

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

The work profile will be created


10:30

Home

Device in compliance

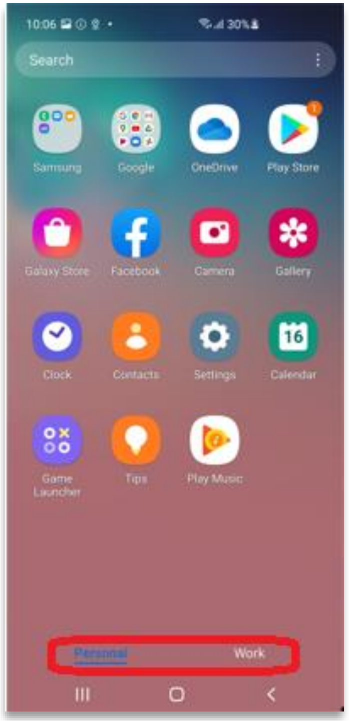
Last checked in - less than a minute ago

Your Privacy

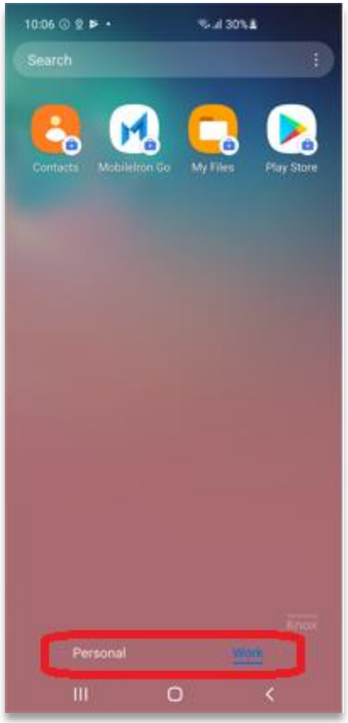
MobileIron Go does not access your personal data. However, your company requires general device information.

LEARN MORE

Your device is now enrolled



The Personal profile is created

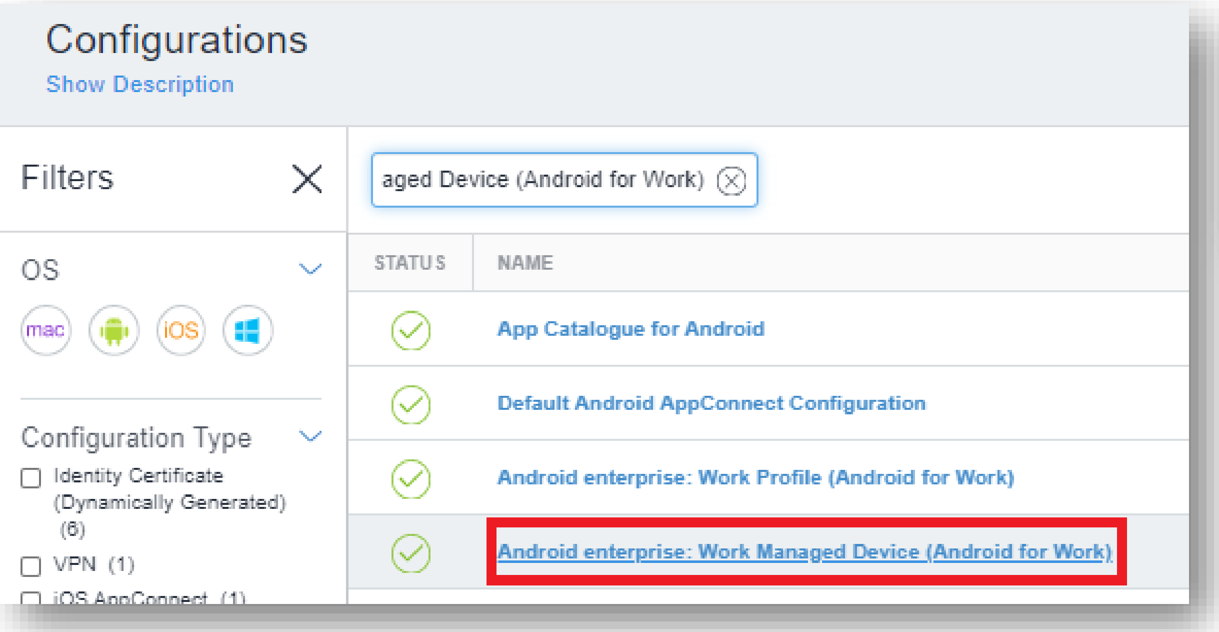


The Work profile is created

Android Enterprise: Fully Managed

First, you will need to assign your Device Group to the Work Managed Device configuration.

- Navigate to: Configurations and search for "Android enterprise: Work Managed Device (Android for Work)"
- Select 'Android enterprise: Work Managed Device (Android for Work)'
- Select Edit
- Select Next



Configurations

Show Description

Filters ✕

aged Device (Android for Work) ⊗

OS

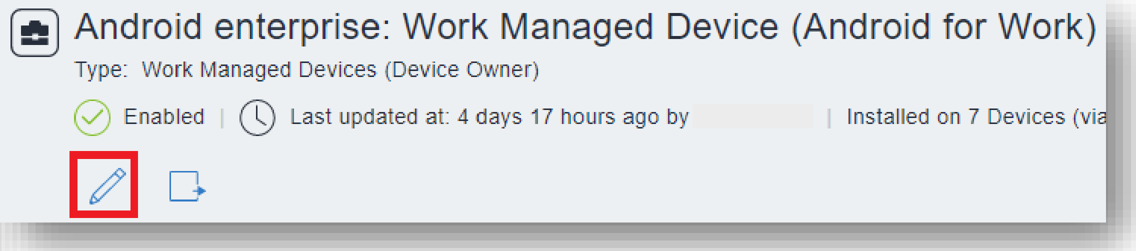
Configuration Type

☐ Identity Certificate (Dynamically Generated) (6)

☐ VPN (1)

☐ iOS AppConnect (1)

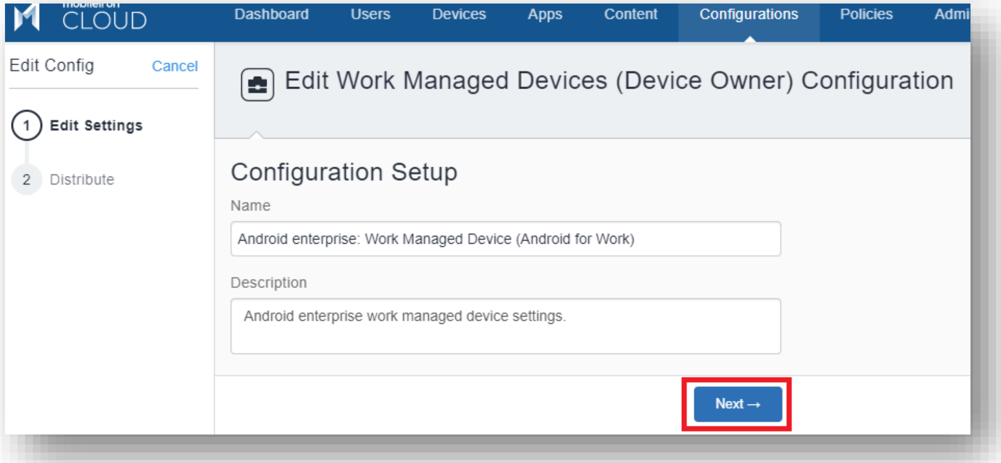
STATUS	NAME
✓	App Catalogue for Android
✓	Default Android AppConnect Configuration
✓	Android enterprise: Work Profile (Android for Work)
✓	Android enterprise: Work Managed Device (Android for Work)



Android enterprise: Work Managed Device (Android for Work)

Type: Work Managed Devices (Device Owner)

✓ Enabled | Last updated at: 4 days 17 hours ago by [redacted] | Installed on 7 Devices (via



Edit Config Cancel

1 Edit Settings

2 Distribute

Edit Work Managed Devices (Device Owner) Configuration

Configuration Setup

Name: Android enterprise: Work Managed Device (Android for Work)

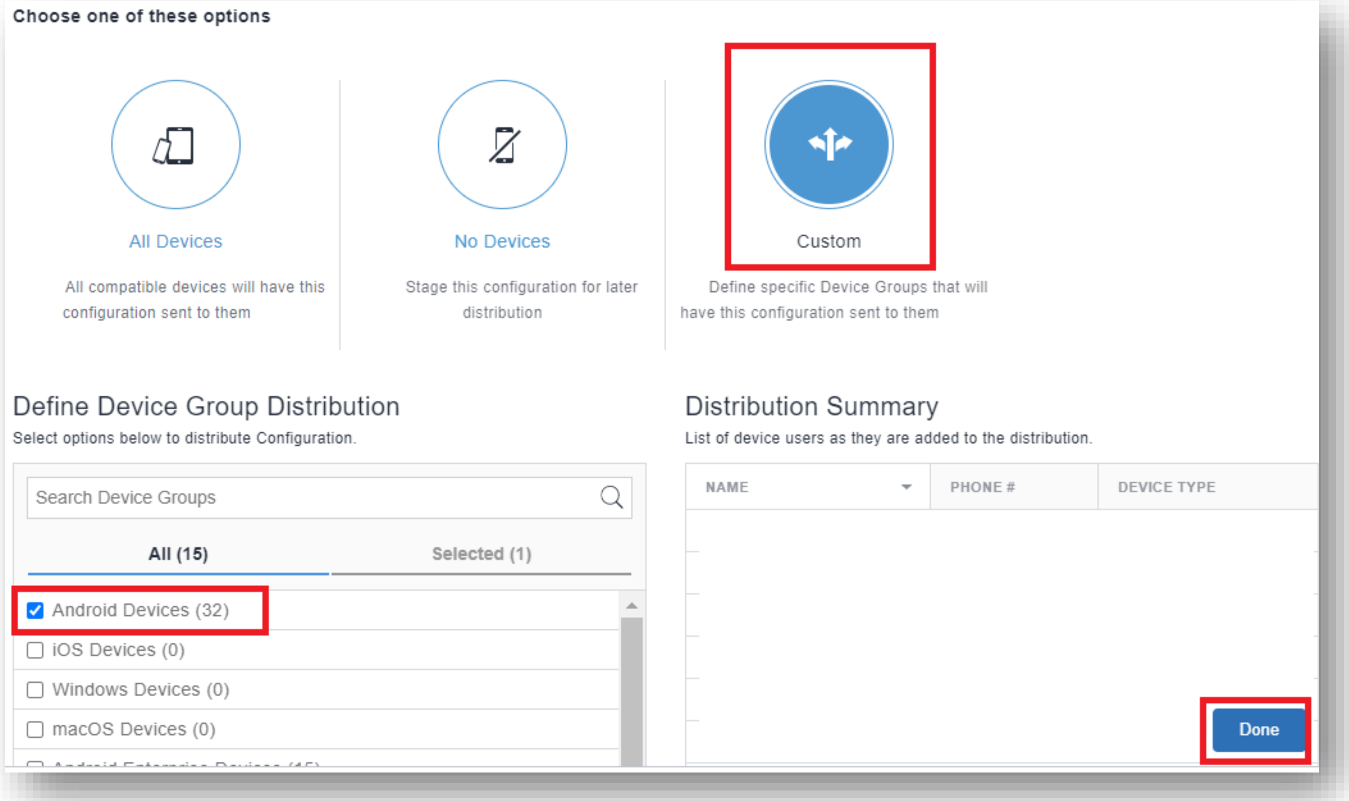
Description: Android enterprise work managed device settings.

Next →

Android Enterprise: Fully Managed

You will then need to assign this configuration to your device group.

- Select Custom
- In the Device Group Distribution box, choose your desired Device Group
- Review the Distribution Summary
- Select Done



Choose one of these options

All Devices

All compatible devices will have this configuration sent to them

No Devices

Stage this configuration for later distribution

Custom

Define specific Device Groups that will have this configuration sent to them

Define Device Group Distribution

Select options below to distribute Configuration.

☑ Android Devices (32)

□ iOS Devices (0)

□ Windows Devices (0)

□ macOS Devices (0)

□ Android Enterprise Devices (15)

Distribution Summary

List of device users as they are added to the distribution.

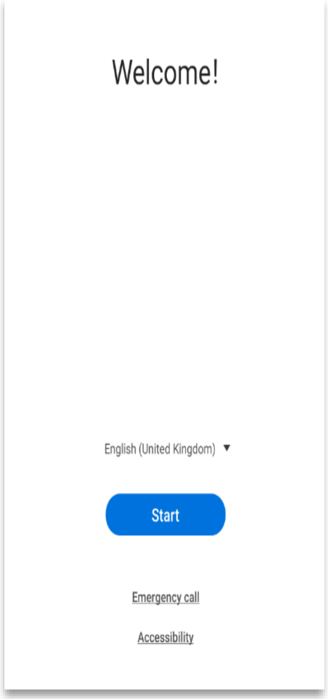
NAME	PHONE #	DEVICE TYPE

Android Enterprise: Fully Managed Enrollment

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 Cloud 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.cloud
2. QR Code Enrollment / NFC Enrollment [Not available for Android 10+ via App Provisioner]
3. Knox Mobile Enrollment

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



Welcome!

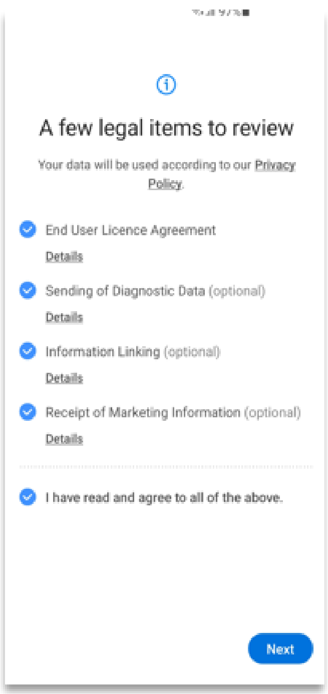
English (United Kingdom) ▼

Start

Emergency call

Accessibility

Tap the 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

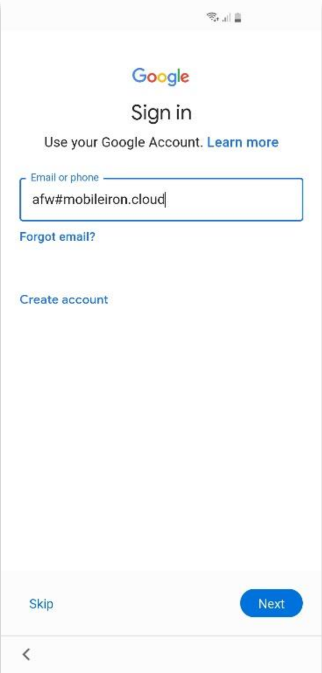
☑ Information Linking (optional)
Details

☑ Receipt of Marketing Information (optional)
Details

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

Next

Accept the
License Agreement and tap Next



Google

Sign in

Use your Google Account. Learn more

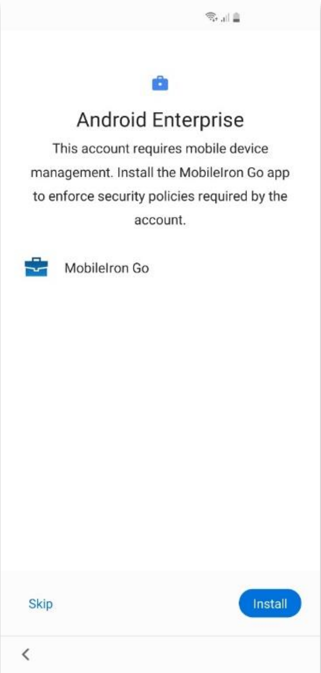
Email or phone: afw#mobileiron.cloud

Forgot email?

Create account

Skip | Next

Type: afw#mobileiron.cloud
Select Next



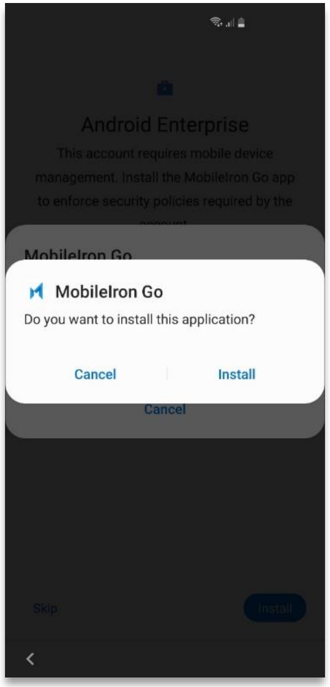
Android Enterprise

This account requires mobile device management. Install the MobileIron Go app to enforce security policies required by the account.

MobileIron Go

Skip | Install

Install

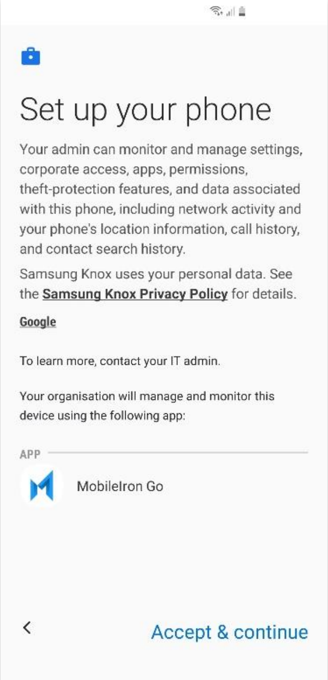


MobileIron Go

Do you want to install this application?

Cancel | Install

Install



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 device using the following app:

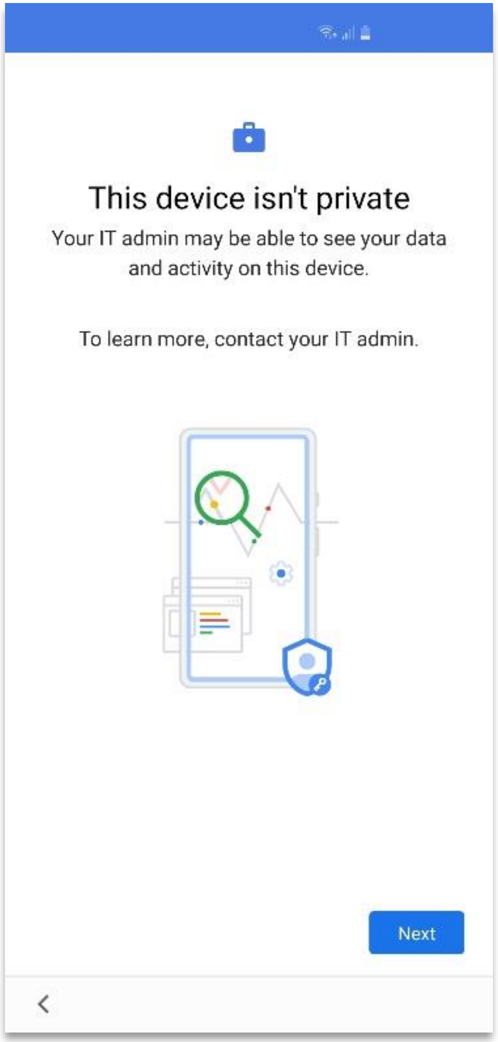
APP

MobileIron Go

Accept & continue

Accept & continue

Android Enterprise: Fully Managed Enrollment

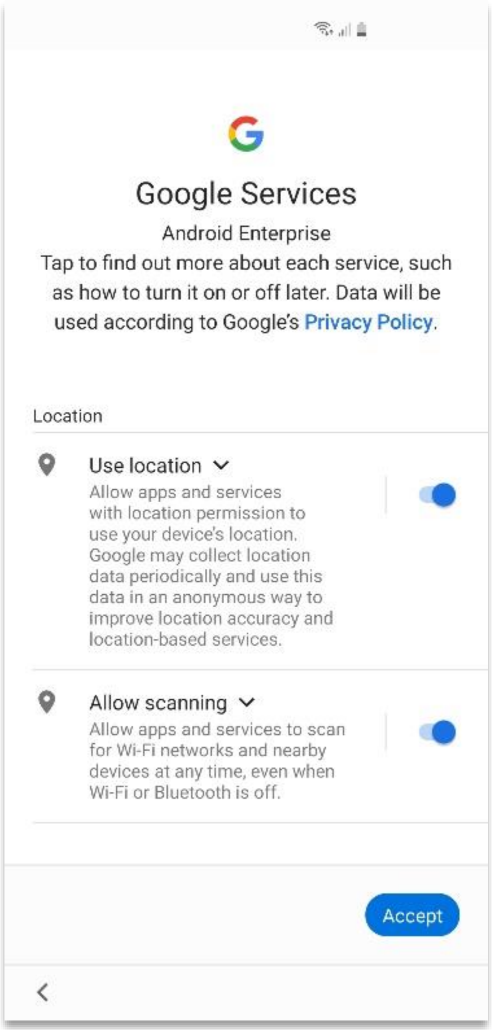


This device isn't private

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

To learn more, contact your IT admin.

Next



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

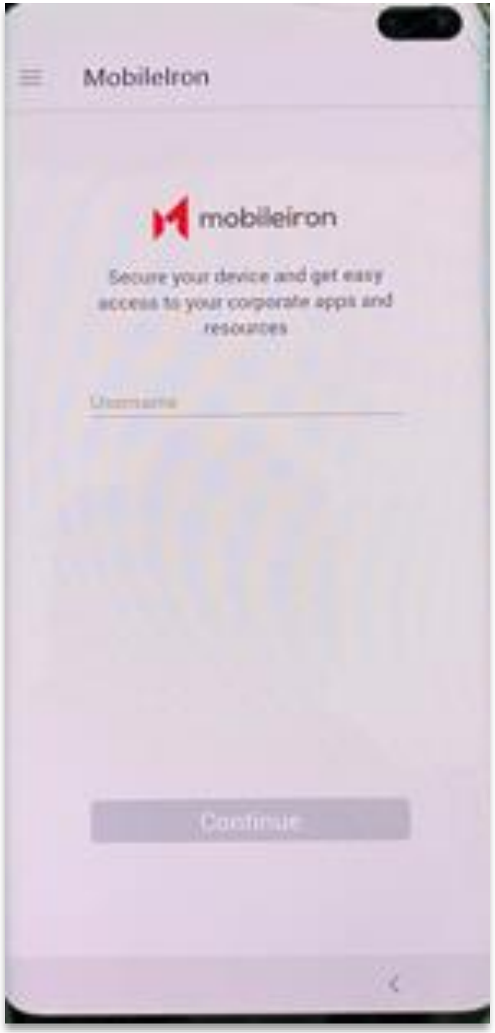
Use location

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, Accept



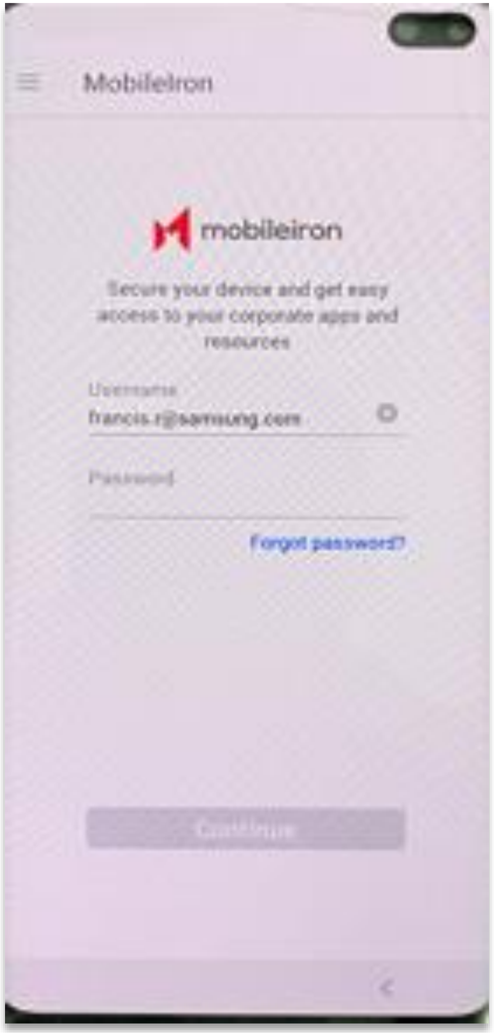
MobileIron

mobileiron

Secure your device and get easy access to your corporate apps and resources

Username

Enter your Username and select Continue



MobileIron

mobileiron

Secure your device and get easy access to your corporate apps and resources

Username

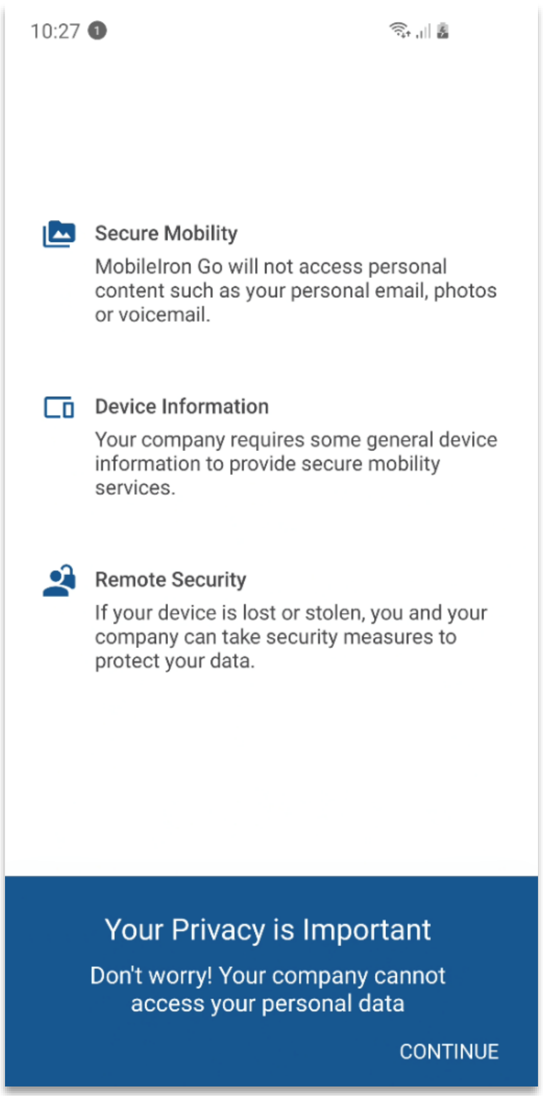
francis.r@samsung.com

Password

Forgot password?

Enter your Password and select Continue

Android Enterprise: Fully Managed Enrollment



10:27

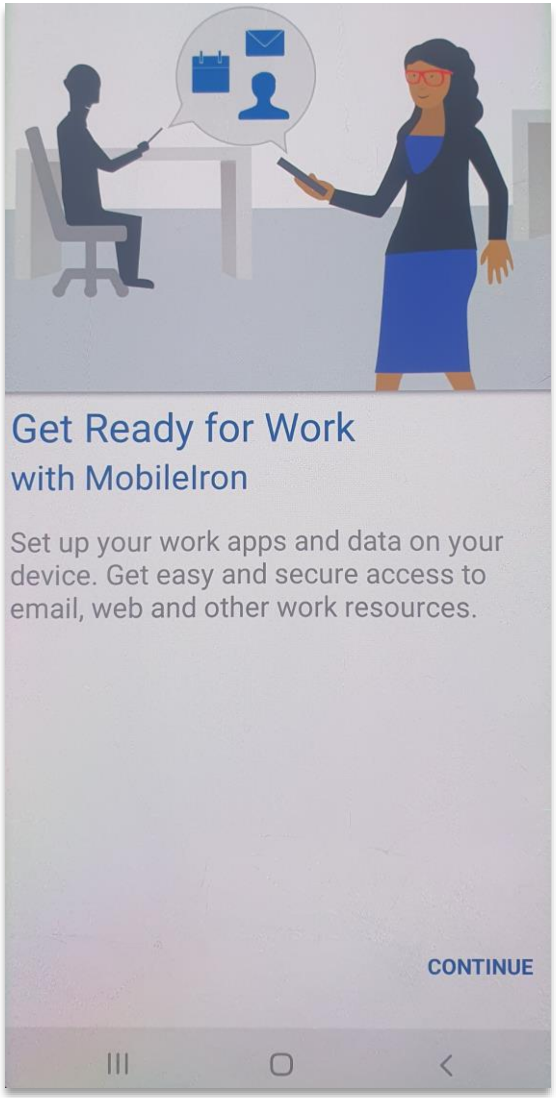
Secure Mobility
MobileIron Go will not access personal content such as your personal email, photos or voicemail.

Device Information
Your company requires some general device information to provide secure mobility services.

Remote Security
If your device is lost or stolen, you and your company can take security measures to protect your data.

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

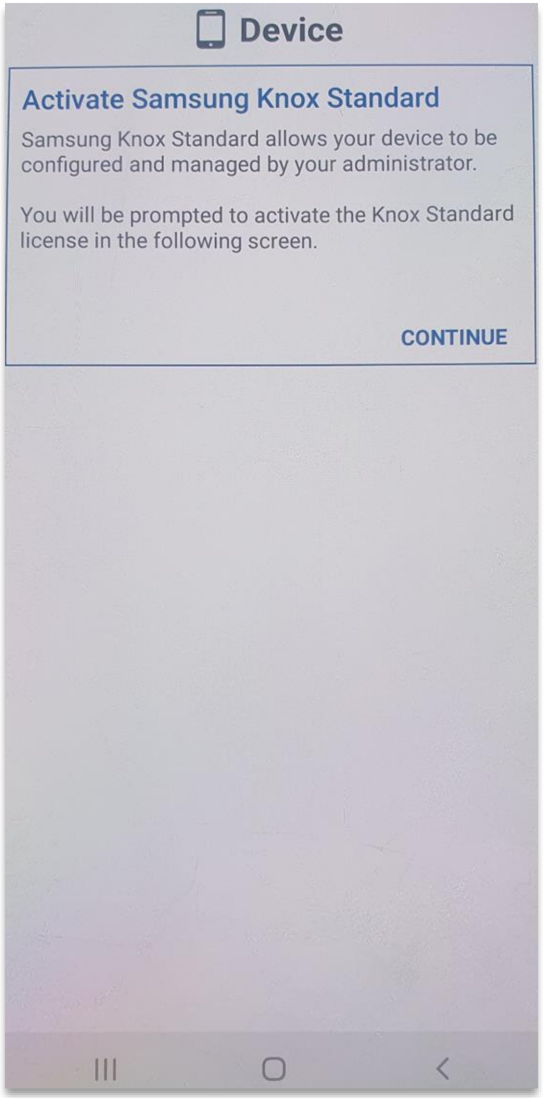
CONTINUE



Get Ready for Work with MobileIron

Set up your work apps and data on your device. Get easy and secure access to email, web and other work resources.

CONTINUE



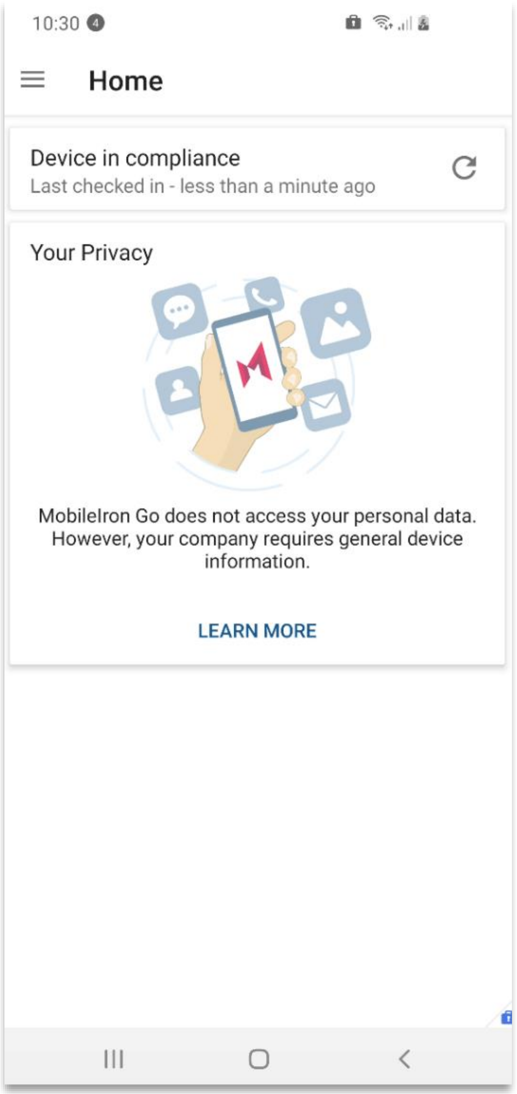
Device

Activate Samsung Knox Standard

Samsung Knox Standard allows your device to be configured and managed by your administrator.

You will be prompted to activate the Knox Standard license in the following screen.

CONTINUE



10:30

Home

Device in compliance
Last checked in - less than a minute ago

Your Privacy

MobileIron Go does not access your personal data. However, your company requires general device information.

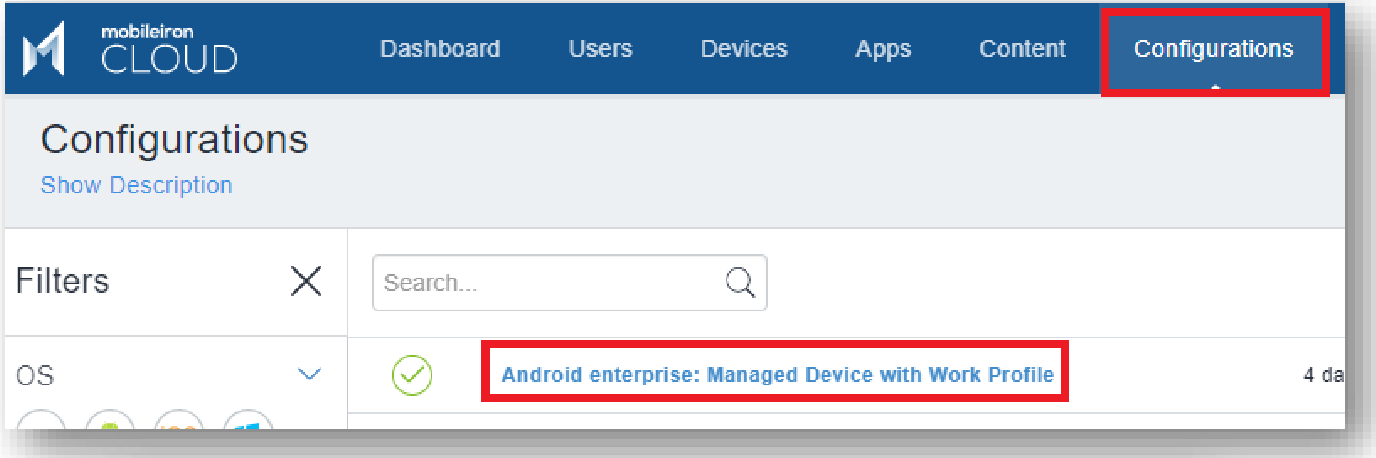
Device is now enrolled

Android Enterprise: Fully Managed Device with a Work Profile

Work Profile on a Company Owned Device [Android 11+]

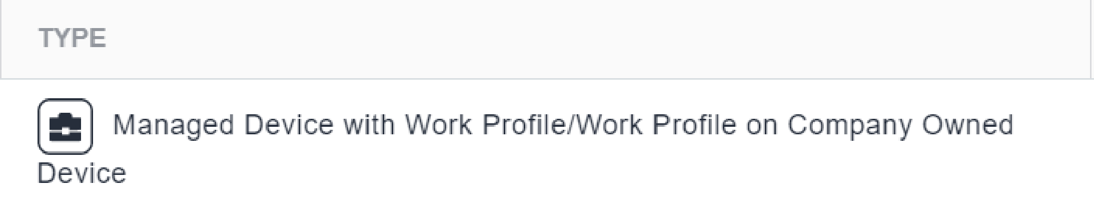
First, you will need to assign your Device Group to the Managed Device with a Work Profile configuration, “Type – Managed Device with Work Profile/Work Profile on Company Owned Device”

- Navigate to: Configurations and search for “Android enterprise: Managed Device with Work Profile”
- Select ‘Android enterprise: Managed Device with Work Profile’
- Select Edit
- Select Next

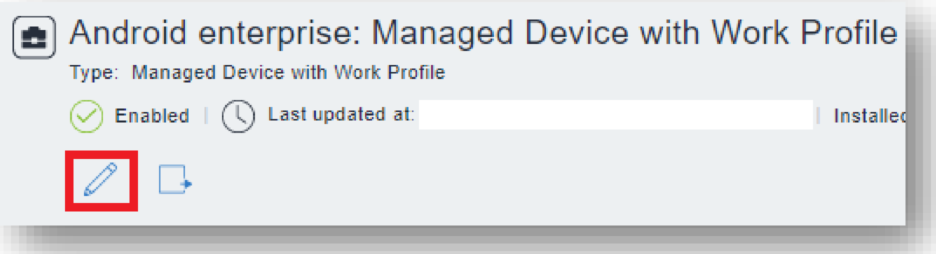


Configurations

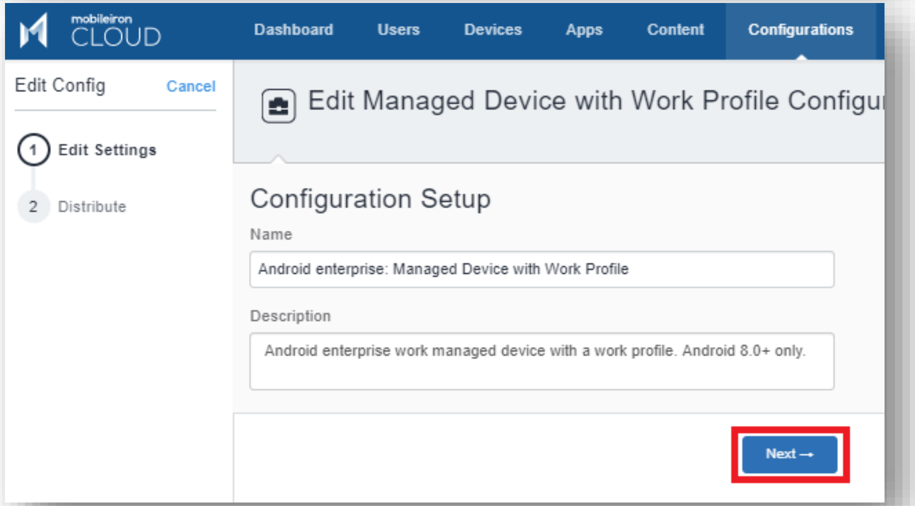
Android enterprise: Managed Device with Work Profile


TYPE

Managed Device with Work Profile/Work Profile on Company Owned Device


Android enterprise: Managed Device with Work Profile

Type: Managed Device with Work Profile



Edit Managed Device with Work Profile Configu

Configuration Setup

Name: Android enterprise: Managed Device with Work Profile

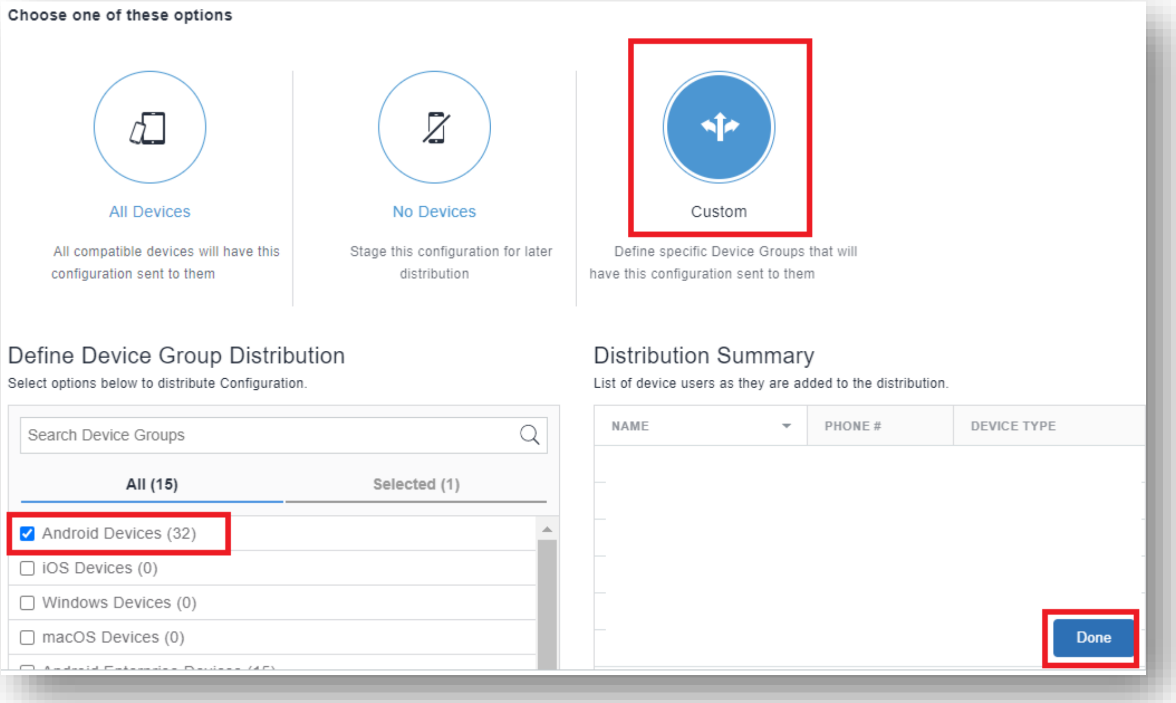
Description: Android enterprise work managed device with a work profile. Android 8.0+ only.

Android Enterprise: Fully Managed Device with a Work Profile

Work Profile on a Company Owned Device [Android 11+]

You will then need to assign this configuration to your device group.

- Select Custom
- In the Device Group Distribution box, choose your desired Device Group
- Review the Distribution Summary
- Select Done



Choose one of these options

All Devices

All compatible devices will have this configuration sent to them

No Devices

Stage this configuration for later distribution

Custom

Define specific Device Groups that will have this configuration sent to them

Define Device Group Distribution

Select options below to distribute Configuration.

Search Device Groups

All (15) | Selected (1)

☑ Android Devices (32)

□ iOS Devices (0)

□ Windows Devices (0)

□ macOS Devices (0)

□ Android Enterprise Devices (15)

Distribution Summary

List of device users as they are added to the distribution.

NAME	PHONE #	DEVICE TYPE

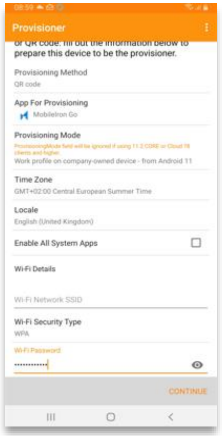
Done

Android Enterprise: Fully Managed Device with a Work Profile

Work Profile on a Company Owned Device[Android 11+]

To enroll the device using this type of configuration will require a QR code using the MobileIron Provisioner: 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: MobileIron Go
- Provisioning Mode: Work profile on company-owned device – from Android 11
- Enter your Wi-Fi Network SSID and password



Provisioner

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

Provisioning Method
QR code

App For Provisioning
MobileIron Go

Provisioning Mode
ProvisioningMode field will be ignored if using 11.2 CORE or Cloud 78 clients and higher
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

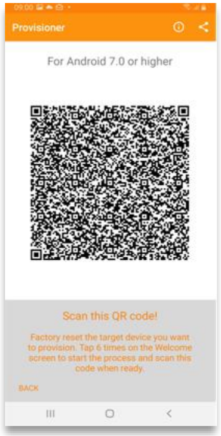
Wi-Fi Network SSID

Wi-Fi Security Type
WPA

Wi-Fi Password
••••••••••••

CONTINUE

App Provisioner settings on provisioning device



Provisioner

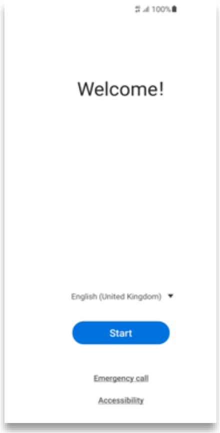
For Android 7.0 or higher

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.

BACK

Tap continue For QR code from provisioning device



Welcome!

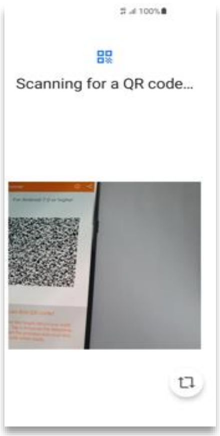
English (United Kingdom)

Start

Emergency call

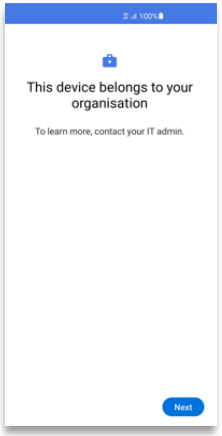
Accessibility

Tap 6 times



Scanning for a QR code...

Scan QR Code

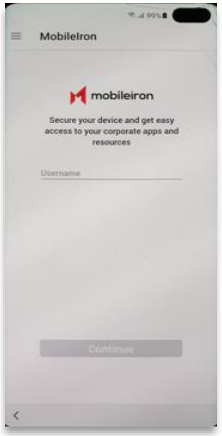


This device belongs to your organisation

To learn more, contact your IT admin.

Next

Click Next



MobileIron

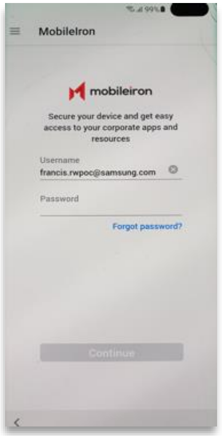
mobileiron

Secure your device and get easy access to your corporate apps and resources

Username

Continue

Enter the Username



MobileIron

mobileiron

Secure your device and get easy access to your corporate apps and resources

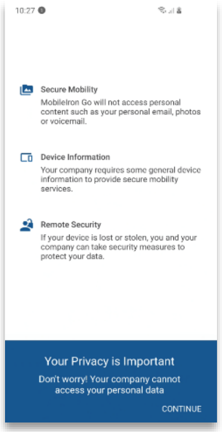
Username
francis.rwpoc@samsung.com

Password

Forgot password?

Continue

Enter the Password



Secure Mobility
MobileIron Go will not access personal content such as your personal email, photos or voicemail.

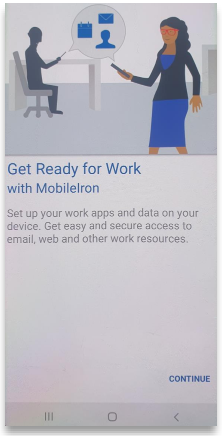
Device Information
Your company requires some general device information to provide secure mobility services.

Remote Security
If your device is lost or stolen, you and your company can take security measures to protect your data.

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

CONTINUE

CONTINUE



Get Ready for Work with MobileIron

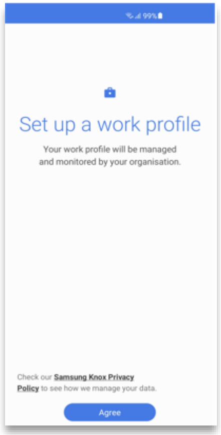
Set up your work apps and data on your device. Get easy and secure access to email, web and other work resources.

CONTINUE

CONTINUE

Android Enterprise: Fully Managed Device with a Work Profile Enrollment

Work Profile on a Company Owned Device [Android 11+]

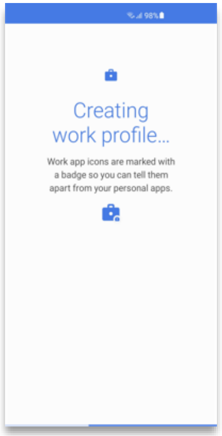


Set up a work profile

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

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

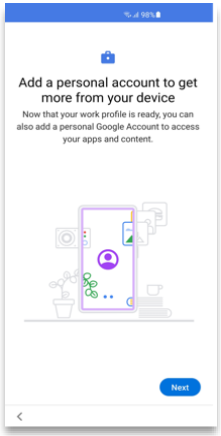
Agree



Creating work profile...

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

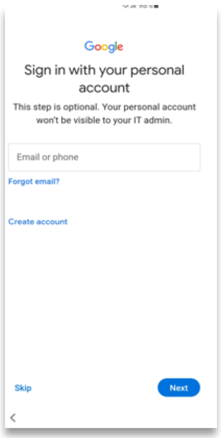
Work profile gets created



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.

Next



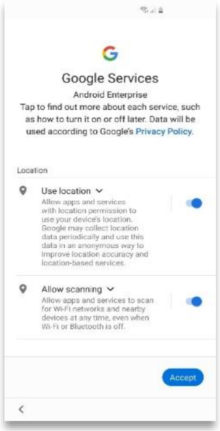
Google

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 your 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

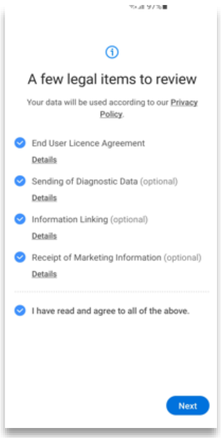
Use location ●

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, Accept



A few legal items to review

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement
Details

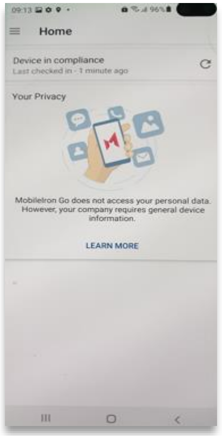
☑ Sending of Diagnostic Data (optional)
Details

☑ 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



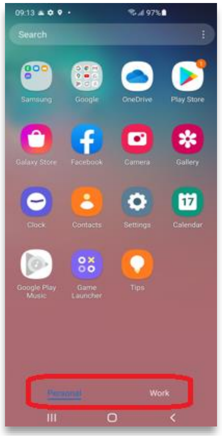
Home

Device in compliance
Last checked in - 1 minute ago

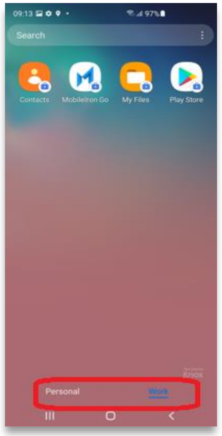
Your Privacy

MobileIron Go does not access your personal data. However, your company requires general device information.

Device is enrolled



A Personal profile is created

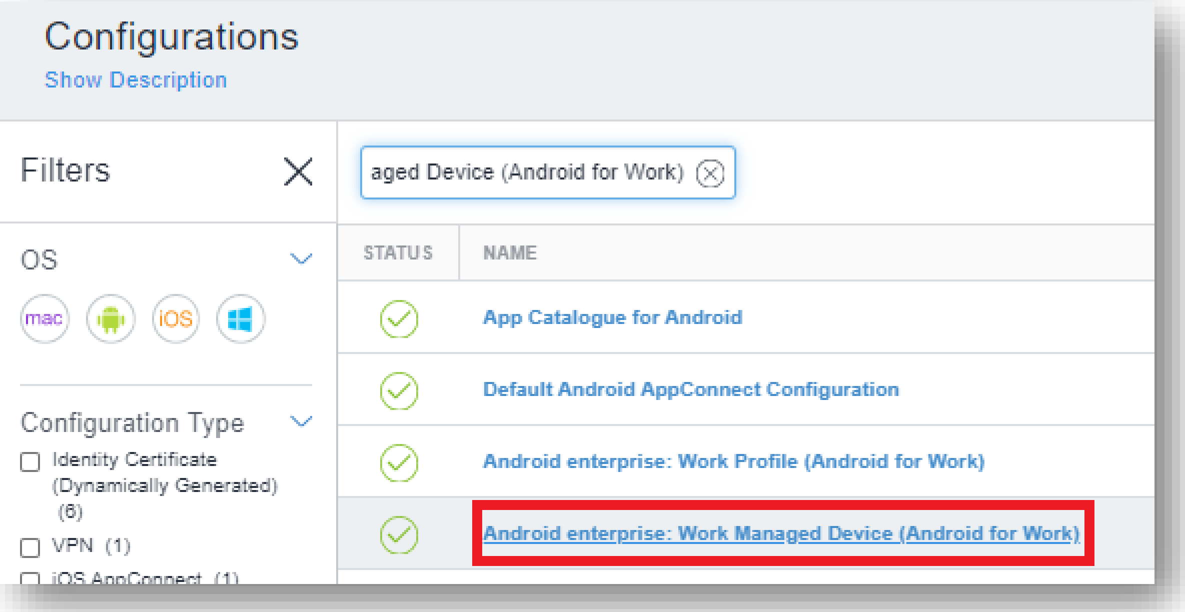


A Work profile is created

Android Enterprise: Dedicated Device

First, you will need to assign your Device Group to the Work Managed Device configuration.

- Navigate to: Configurations and search for “Android enterprise: Work Managed Device (Android for Work)”
- Select ‘Android enterprise: Work Managed Device (Android for Work)’
- Select Edit
- Select Next



Configurations

Show Description

Filters

OS

Configuration Type

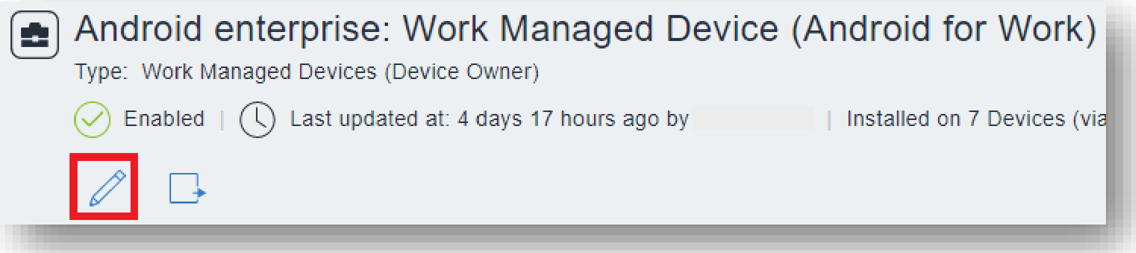
□ Identity Certificate (Dynamically Generated) (6)

□ VPN (1)

□ iOS AppConnect (1)

aged Device (Android for Work)

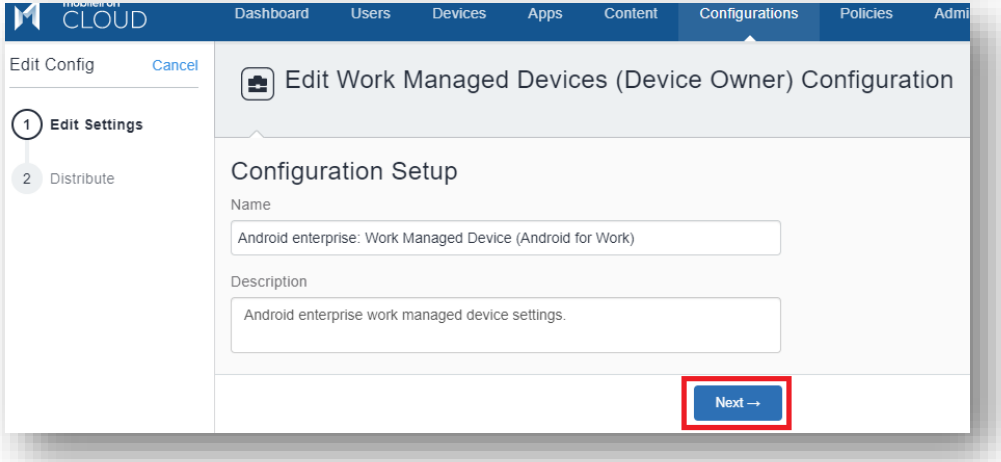
STATUS	NAME
✓	App Catalogue for Android
✓	Default Android AppConnect Configuration
✓	Android enterprise: Work Profile (Android for Work)
✓	Android enterprise: Work Managed Device (Android for Work)



Android enterprise: Work Managed Device (Android for Work)

Type: Work Managed Devices (Device Owner)

Enabled | Last updated at: 4 days 17 hours ago by [redacted] | Installed on 7 Devices (via



Edit Config Cancel

1 Edit Settings

2 Distribute

Edit Work Managed Devices (Device Owner) Configuration

Configuration Setup

Name

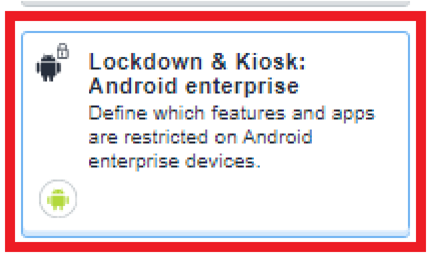
Android enterprise: Work Managed Device (Android for Work)

Description

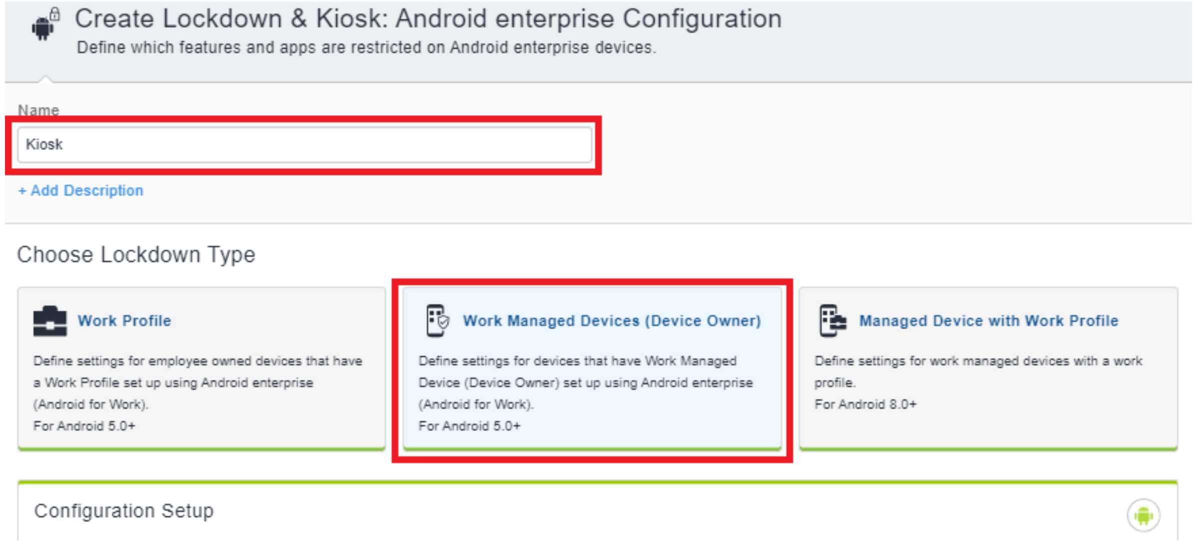
Android enterprise work managed device settings.

Android Enterprise: Dedicated Device

- Navigate to: Configurations and select Add
- Select ‘Lockdown & Kiosk: Android enterprise’
- Enter a name and select Work Managed Devices (Device Owner)
- Enable Kiosk Mode and set the desired configuration
- Select Next



Lockdown & Kiosk: Android enterprise
Define which features and apps are restricted on Android enterprise devices.



Create Lockdown & Kiosk: Android enterprise Configuration
Define which features and apps are restricted on Android enterprise devices.

Name: Kiosk

+ Add Description

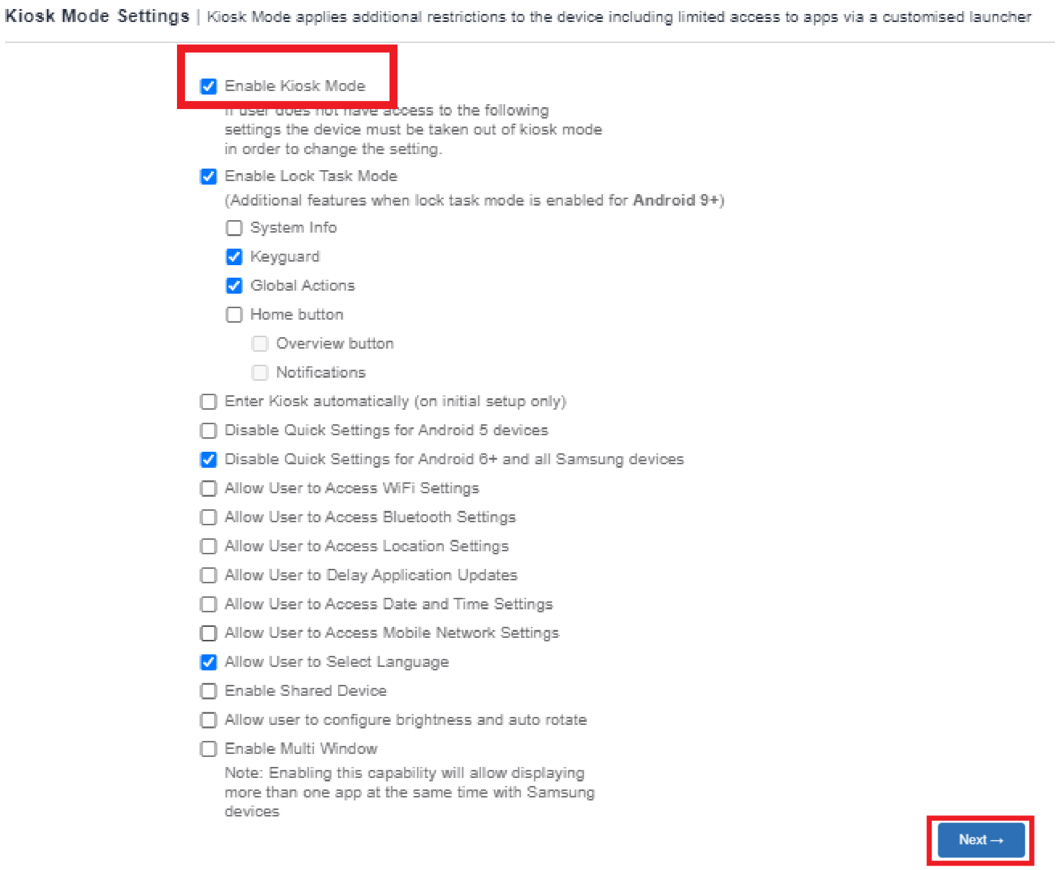
Choose Lockdown Type

Work Profile
Define settings for employee owned devices that have a Work Profile set up using Android enterprise (Android for Work).
For Android 5.0+

Work Managed Devices (Device Owner)
Define settings for devices that have Work Managed Device (Device Owner) set up using Android enterprise (Android for Work).
For Android 5.0+

Managed Device with Work Profile
Define settings for work managed devices with a work profile.
For Android 8.0+

Configuration Setup



Kiosk Mode Settings | Kiosk Mode applies additional restrictions to the device including limited access to apps via a customised launcher

☑ Enable Kiosk Mode
If user does not have access to the following settings the device must be taken out of kiosk mode in order to change the setting.

☑ Enable Lock Task Mode
(Additional features when lock task mode is enabled for **Android 9+**)

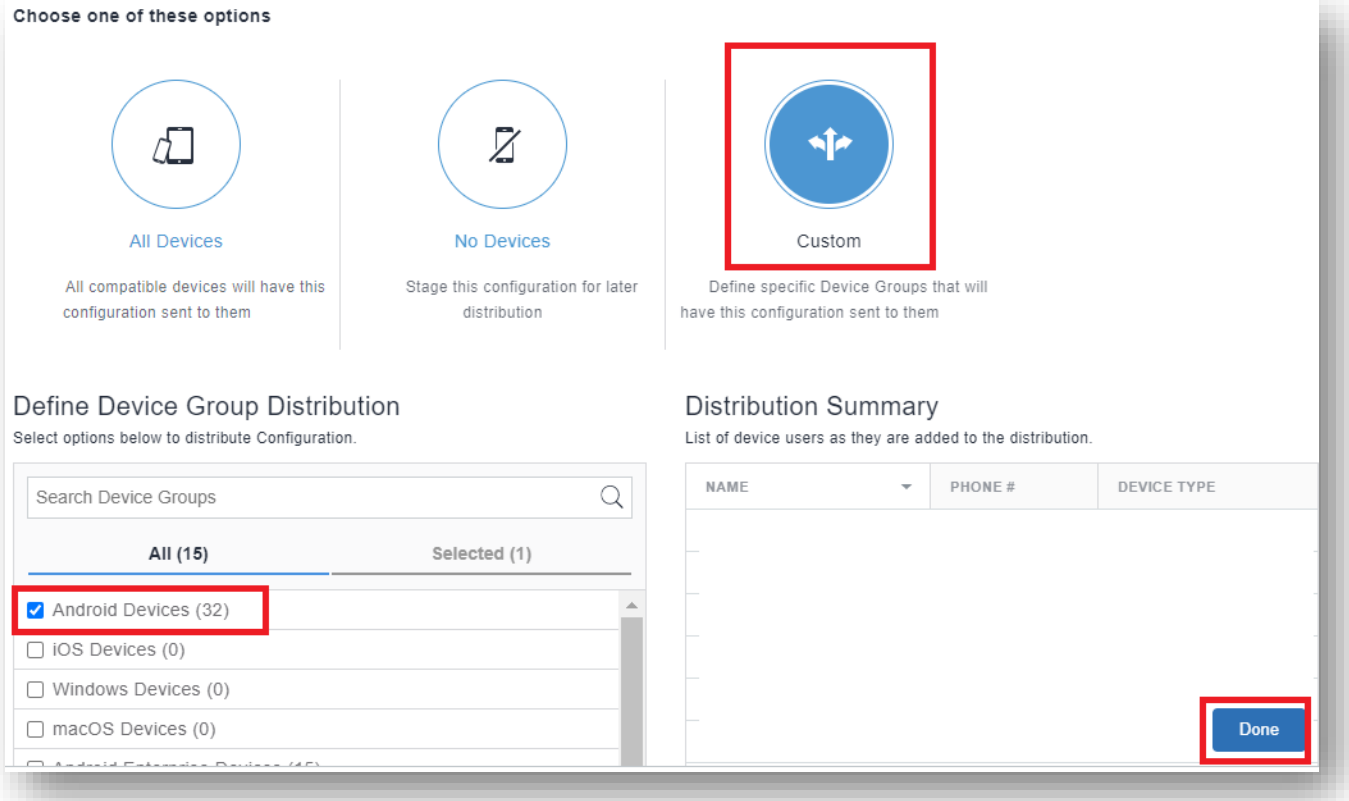
- □ System Info
- ☑ Keyguard
- ☑ Global Actions
- □ Home button
  - □ Overview button
  - □ Notifications

□ Enter Kiosk automatically (on initial setup only)
□ Disable Quick Settings for Android 5 devices
☑ Disable Quick Settings for Android 6+ and all Samsung devices
□ Allow User to Access WiFi Settings
□ Allow User to Access Bluetooth Settings
□ Allow User to Access Location Settings
□ Allow User to Delay Application Updates
□ Allow User to Access Date and Time Settings
□ Allow User to Access Mobile Network Settings
☑ Allow User to Select Language
□ Enable Shared Device
□ Allow user to configure brightness and auto rotate
□ Enable Multi Window
Note: Enabling this capability will allow displaying more than one app at the same time with Samsung devices

Android Enterprise: Dedicated Device

You will then need to assign this configuration to your device group.

- Select Custom
- In the Device Group Distribution box, choose your desired Device Group
- Review the Distribution Summary
- Select Done



Choose one of these options

All Devices
All compatible devices will have this configuration sent to them

No Devices
Stage this configuration for later distribution

Custom
Define specific Device Groups that will have this configuration sent to them

Define Device Group Distribution
Select options below to distribute Configuration.

Search Device Groups

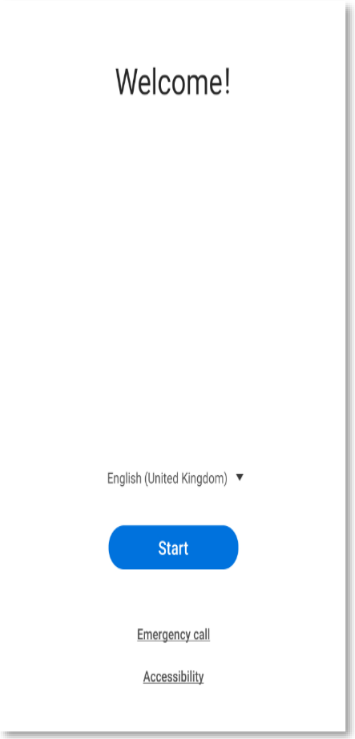
All (15) | Selected (1)

- ☑ Android Devices (32)
- □ iOS Devices (0)
- □ Windows Devices (0)
- □ macOS Devices (0)
- □ Android Enterprise Devices (15)

Distribution Summary
List of device users as they are added to the distribution.

NAME	PHONE #	DEVICE TYPE

Android Enterprise: Dedicated Device Enrollment



Welcome!

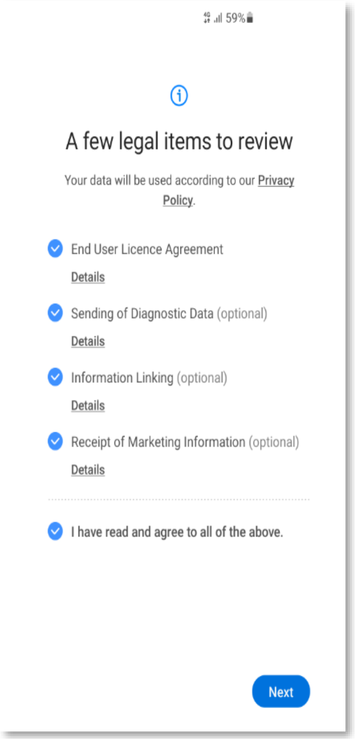
English (United Kingdom) ▾

Start

Emergency call

Accessibility

Tap the Start



59%

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

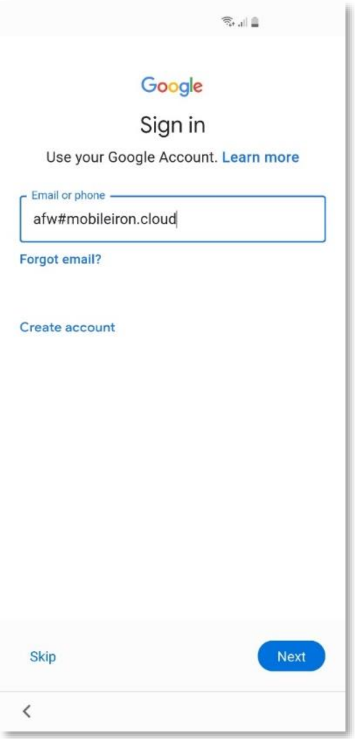
☑ Information Linking (optional)
Details

☑ Receipt of Marketing Information (optional)
Details

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

Next

Accept the
License Agreement
and tap Next



Google

Sign in

Use your Google Account. Learn more

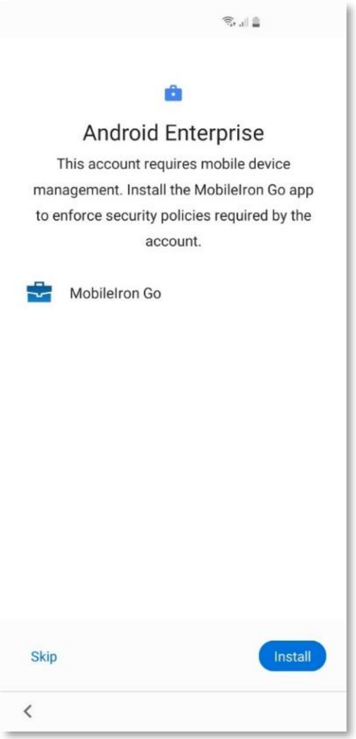
Email or phone: afw#mobileiron.cloud

Forgot email?

Create account

Skip Next

Type: afw#mobileiron.cloud
Select Next



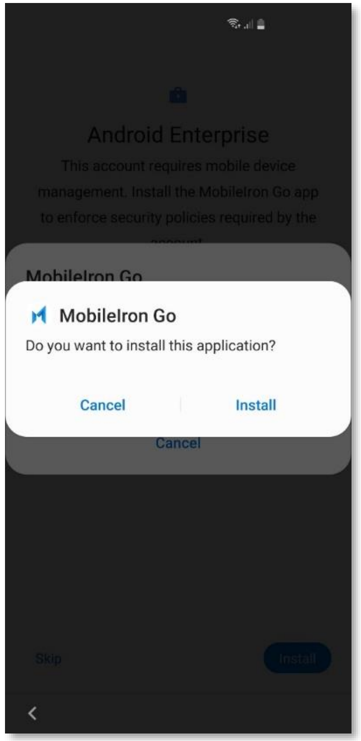
Android Enterprise

This account requires mobile device management. Install the MobileIron Go app to enforce security policies required by the account.

MobileIron Go

Skip Install

Install



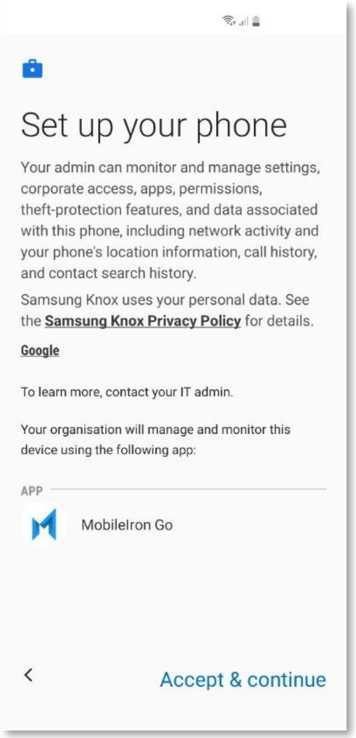
MobileIron Go

Do you want to install this application?

Cancel Install

Install

Android Enterprise: Dedicated Device Enrollment



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

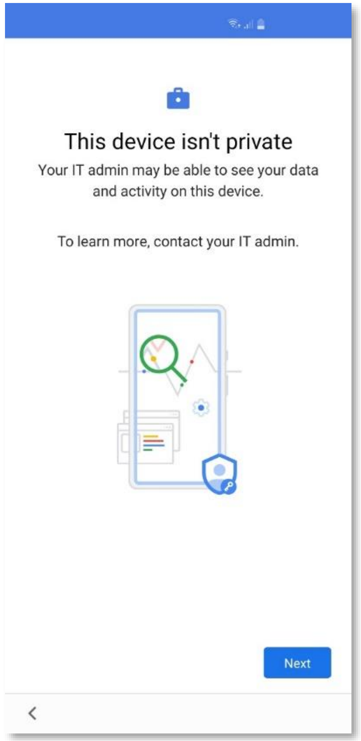
To learn more, contact your IT admin.

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

APP

MobileIron Go

Accept & continue

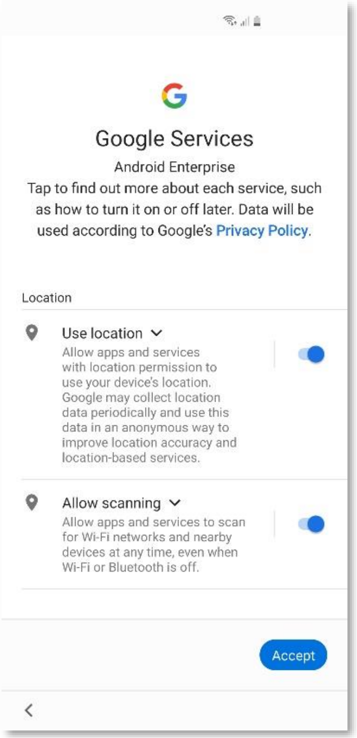


This device isn't private

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

To learn more, contact your IT admin.

Next



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

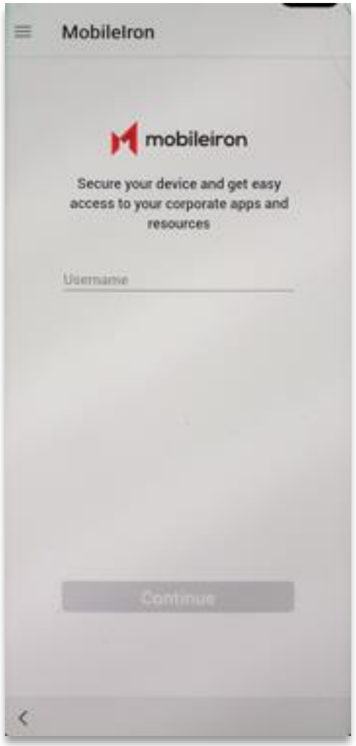
Use location ●

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, Accept



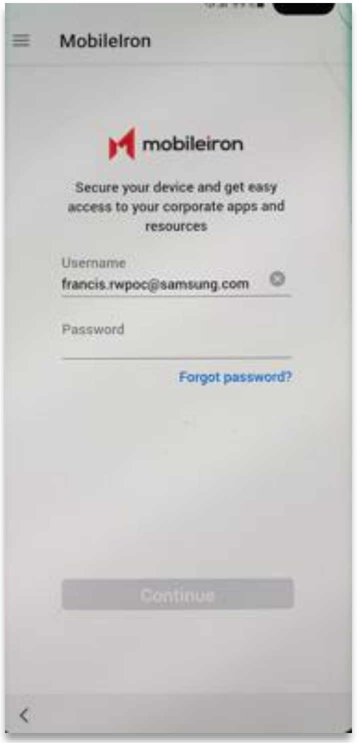
MobileIron

mobileiron

Secure your device and get easy access to your corporate apps and resources

Username

Enter your Username and select Continue



MobileIron

mobileiron

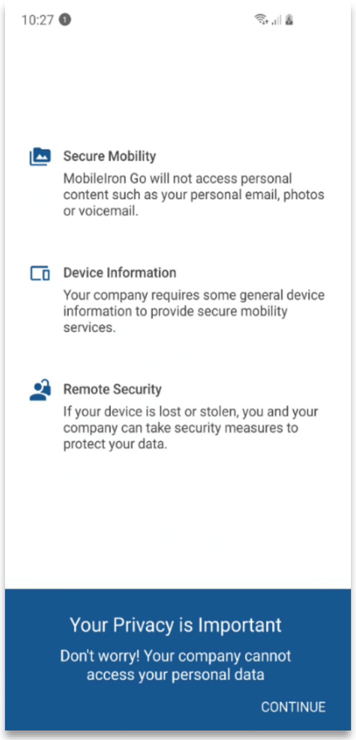
Secure your device and get easy access to your corporate apps and resources

Username: francis.rwpoc@samsung.com

Password

Enter your Password and select Continue

Android Enterprise: Dedicated Device Enrollment



10:27

Secure Mobility
MobileIron Go will not access personal content such as your personal email, photos or voicemail.

Device Information
Your company requires some general device information to provide secure mobility services.

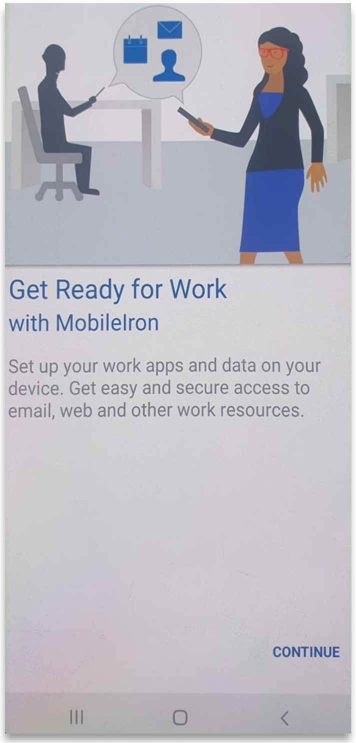
Remote Security
If your device is lost or stolen, you and your company can take security measures to protect your data.

Your Privacy is Important

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

CONTINUE

CONTINUE

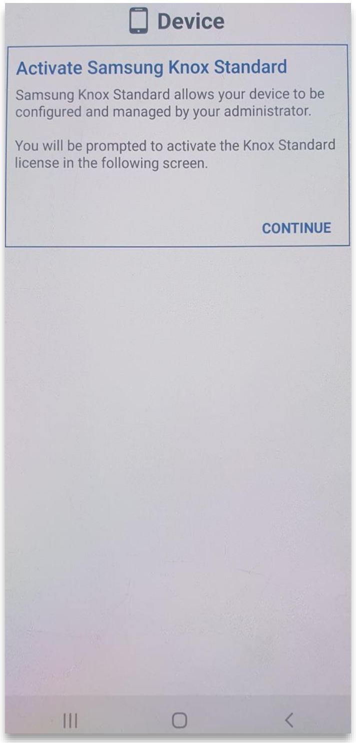


Get Ready for Work with MobileIron

Set up your work apps and data on your device. Get easy and secure access to email, web and other work resources.

CONTINUE

CONTINUE



Device

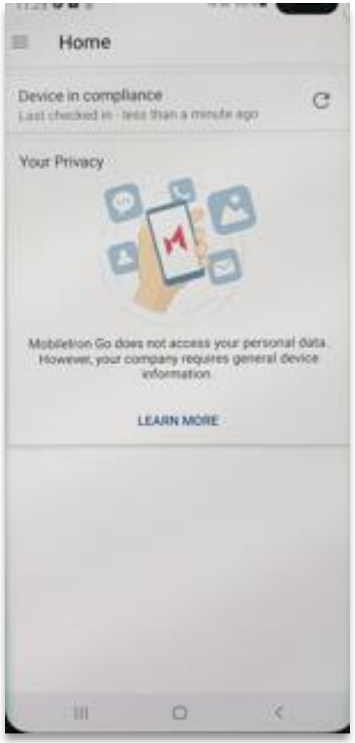
Activate Samsung Knox Standard

Samsung Knox Standard allows your device to be configured and managed by your administrator.

You will be prompted to activate the Knox Standard license in the following screen.

CONTINUE

CONTINUE



Home

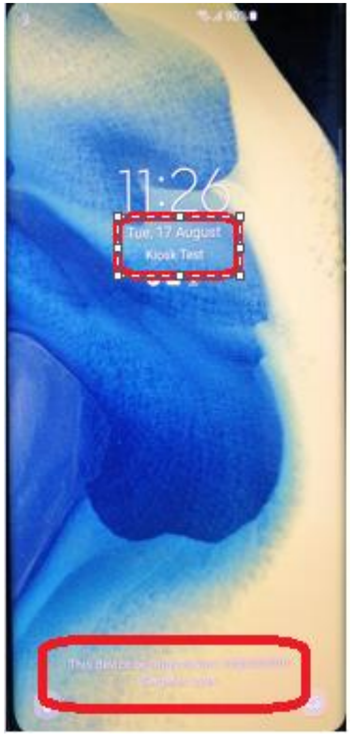
Device in compliance
Last checked in - less than a minute ago

Your Privacy

MobileIron Go does not access your personal data. However, your company requires general device information.

LEARN MORE

The device
is now enrolled



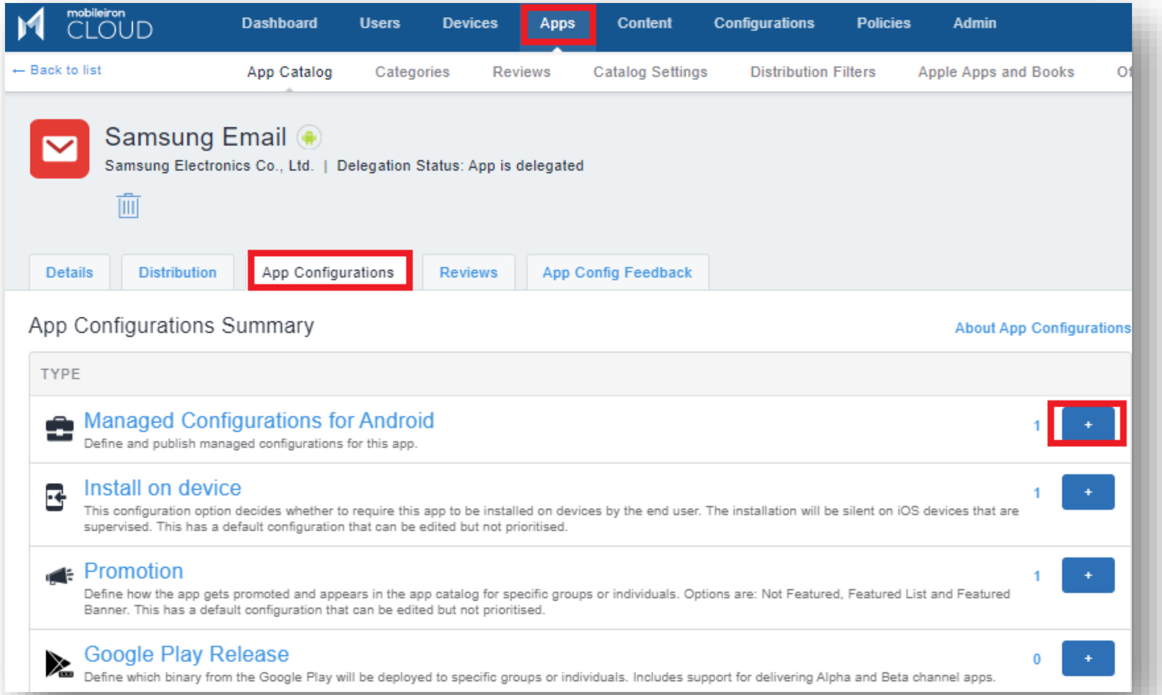
This device [illegible]

Locked Device
with message

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 Cloud, follow the instructions below.

- Navigate to Apps -> App Catalog -> Click on the app you would like to configure -> App Configurations
- Click on the + icon next to Managed Configurations for android
- Under Managed Configurations the selected app will populate input fields for you to prepopulate with values if it is supported
- Select Next and assign to the desired device group

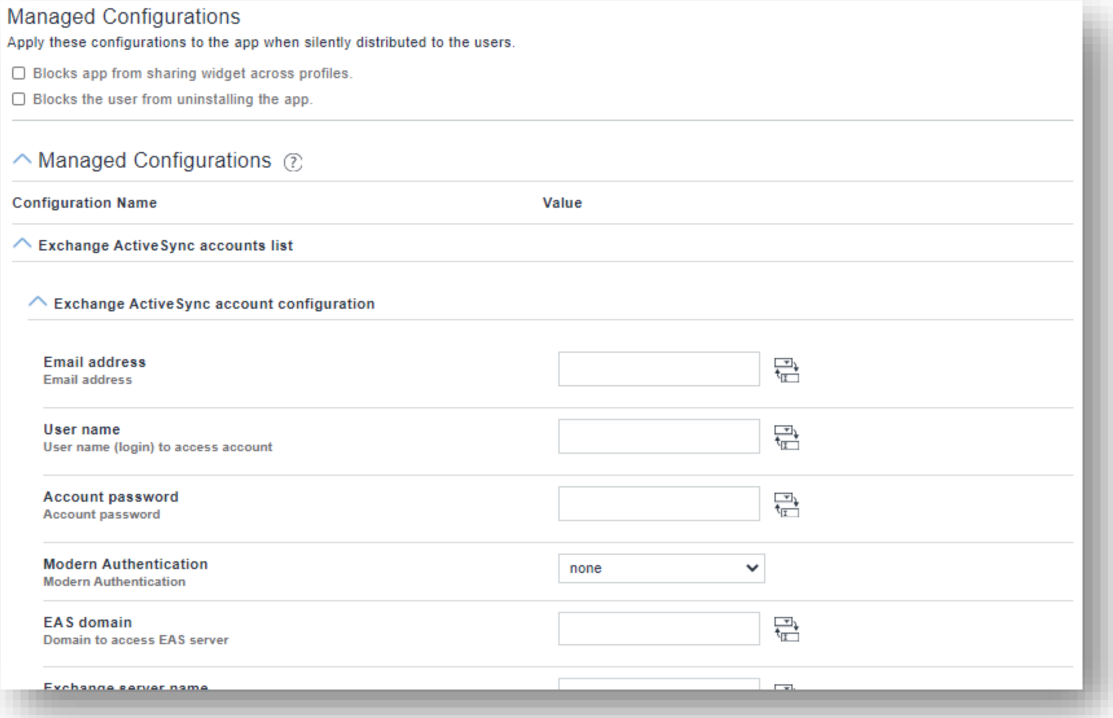


Samsung Email

Samsung Electronics Co., Ltd. | Delegation Status: App is delegated

App Configurations Summary

TYPE		
Managed Configurations for Android Define and publish managed configurations for this app.	1	+
Install on device This configuration option decides whether to require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritised.	1	+
Promotion Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritised.	1	+
Google Play Release Define which binary from the Google Play will be deployed to specific groups or individuals. Includes support for delivering Alpha and Beta channel apps.	0	+



Managed Configurations

Apply these configurations to the app when silently distributed to the users.

☐ Blocks app from sharing widget across profiles.

☐ Blocks the user from uninstalling the app.

Managed Configurations ?

Configuration Name	Value
Exchange ActiveSync accounts list	
Exchange ActiveSync account configuration	
Email address Email address	
User name User name (login) to access account	
Account password Account password	
Modern Authentication Modern Authentication	none
EAS domain Domain to access EAS server	
Exchange server name	

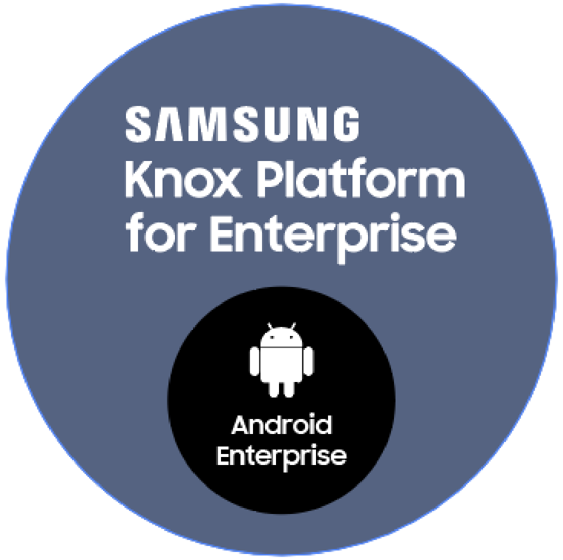
Knox Platform for Enterprise

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:

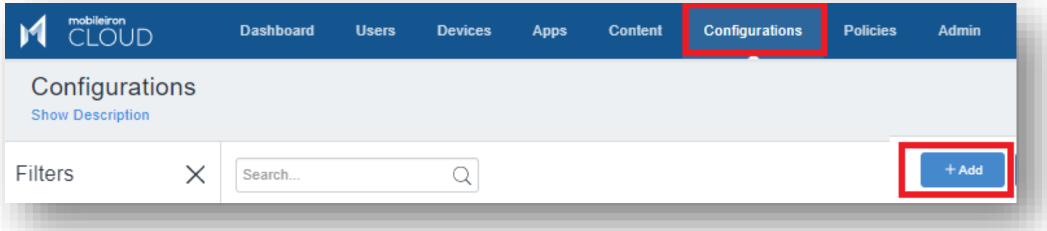
- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [FREE or $ for some special options such as Dual DAR]

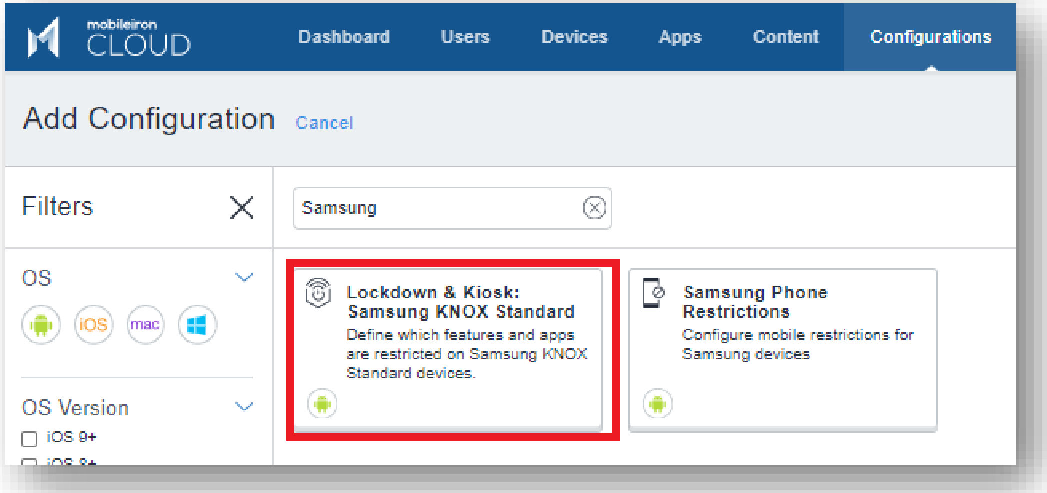
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise 8 or above.



Configure Knox Platform for Enterprise : Standard Edition

- Navigate to: Configurations and select Add
- Search for Samsung and select Lockdown & Kiosk: Samsung KNOX Standard
- Enter a Name
- Configuration Setup will list the available lockdown settings; choose the desired config
- Select Next and assign to your chosen group

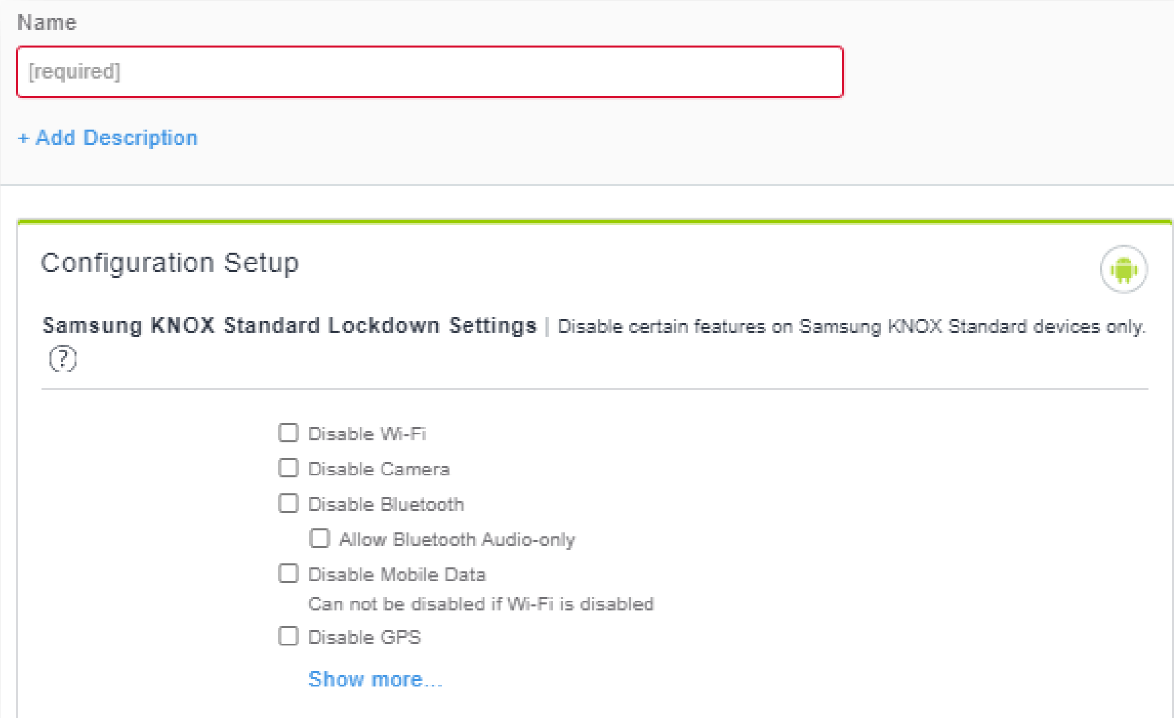




Samsung

Lockdown & Kiosk: Samsung KNOX Standard
Define which features and apps are restricted on Samsung KNOX Standard devices.

Samsung Phone Restrictions
Configure mobile restrictions for Samsung devices



Name
[required]

Configuration Setup

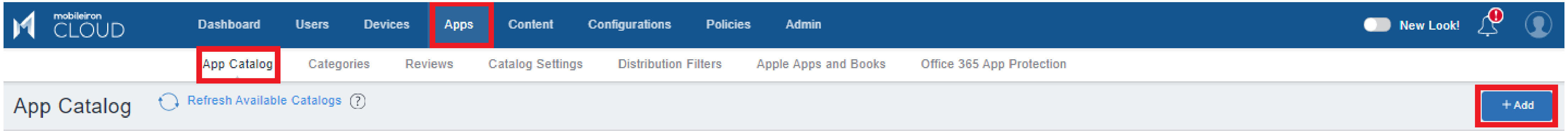
Samsung KNOX Standard Lockdown Settings | Disable certain features on Samsung KNOX Standard devices only.

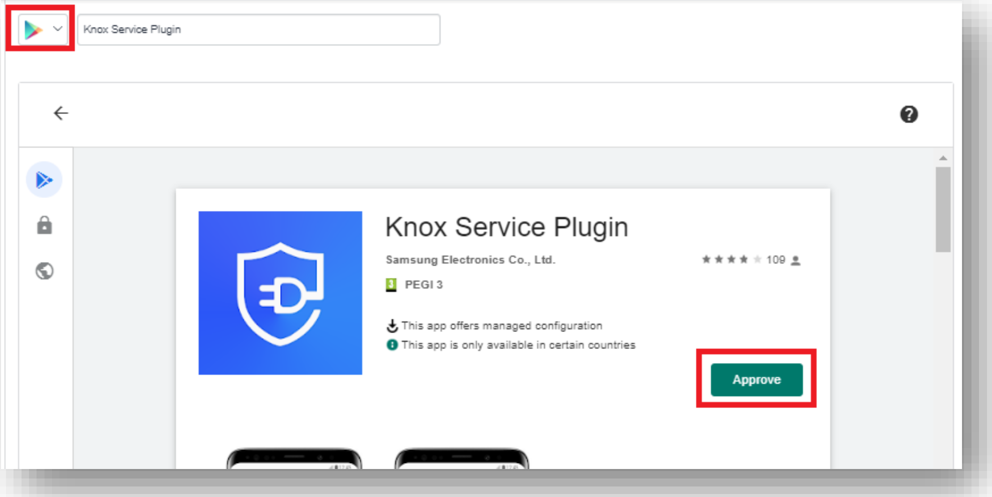
- ☐ Disable Wi-Fi
- ☐ Disable Camera
- ☐ Disable Bluetooth
  - ☐ Allow Bluetooth Audio-only
- ☐ Disable Mobile Data
  Can not be disabled if Wi-Fi is disabled
- ☐ Disable GPS

Configure Knox Platform for Enterprise : Premium Edition

In order to configure the Knox Platform for Enterprise premium features within MobileIron Cloud, you need to add the Knox Service Plugin App via the Manage Google Play Store and add an app config. The steps below illustrate how this is achieved.

- Navigate to Apps > App Catalog > Add
- Select Google Play in the drop down menu and search for Knox Service Plugin
- Select Approve twice





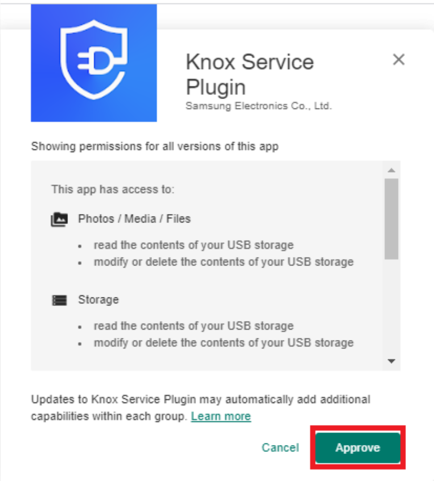
Knox Service Plugin

Samsung Electronics Co., Ltd.

PEGI 3

This app offers managed configuration

This app is only available in certain countries



Knox Service Plugin

Samsung Electronics Co., Ltd.

Showing permissions for all versions of this app

This app has access to:

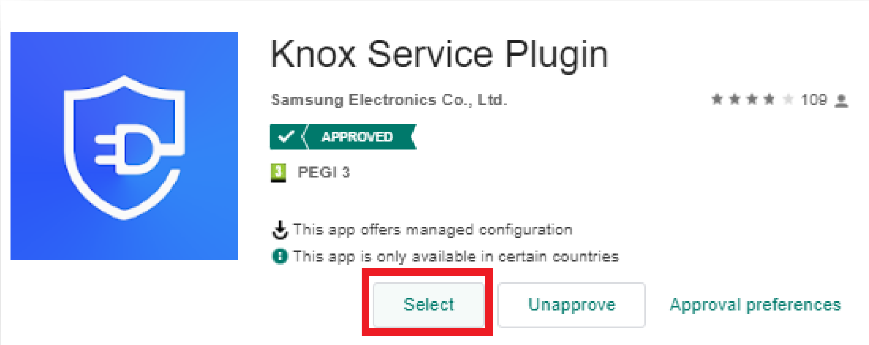
Photos / Media / Files
- read the contents of your USB storage
- modify or delete the contents of your USB storage

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

Configure Knox Platform for Enterprise : Premium Edition

- Click Select then Next
- Choose the desired assignment and select Next
- Click on the + next to Managed Configurations for Android



Knox Service Plugin

Samsung Electronics Co., Ltd.

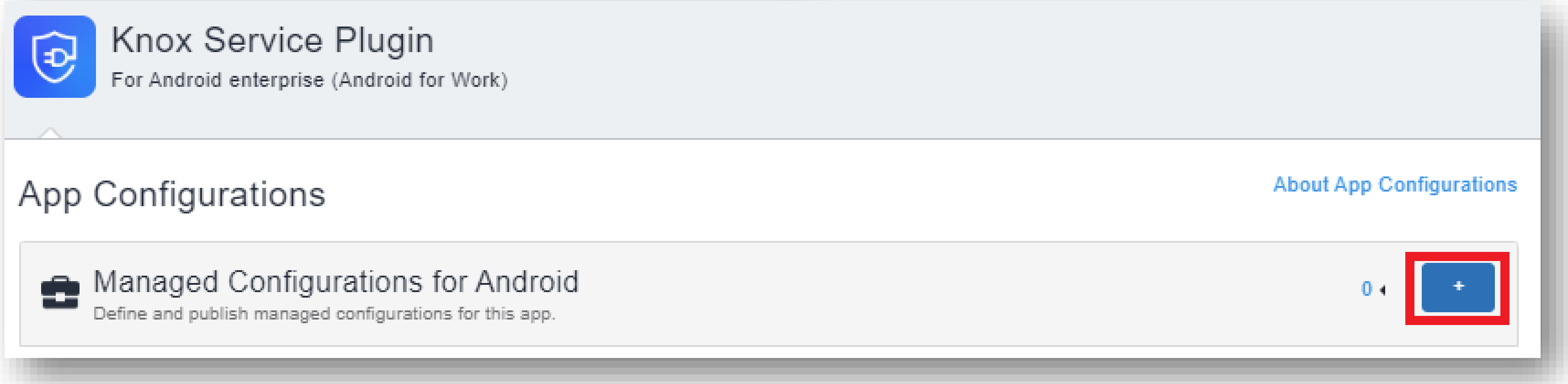
★★★★★ 109

APPROVED

PEGI 3

This app offers managed configuration

This app is only available in certain countries



Knox Service Plugin

For Android enterprise (Android for Work)

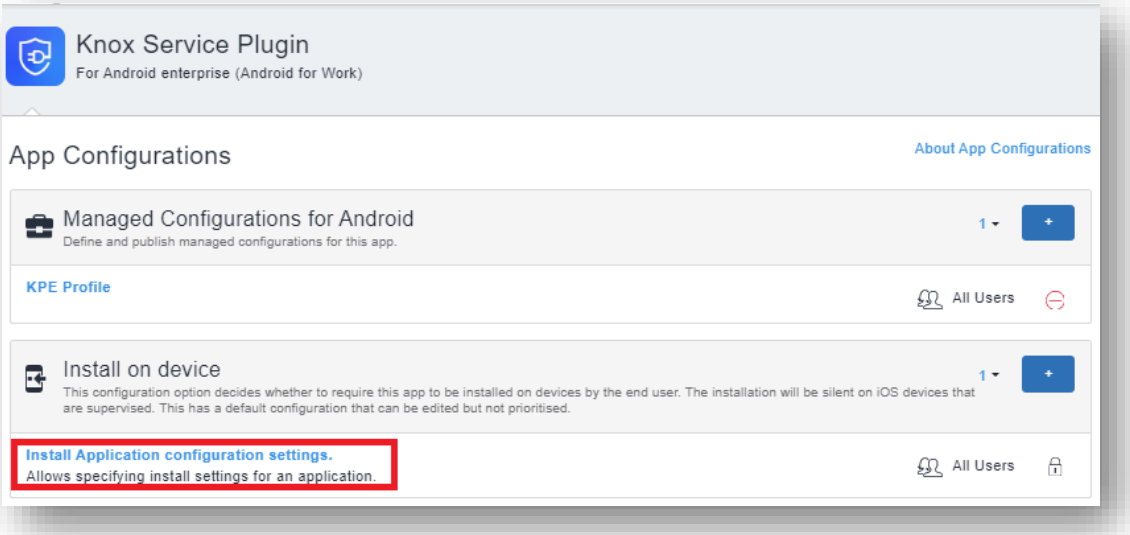
App Configurations

Managed Configurations for Android

Define and publish managed configurations for this app.

Configure Knox Platform for Enterprise : Premium Edition

- Select Install Application configuration settings
- Turn Install on Device ON
- Tick Silently install on Samsung KNOX
- Select Next
- Select Done



Knox Service Plugin
For Android enterprise (Android for Work)

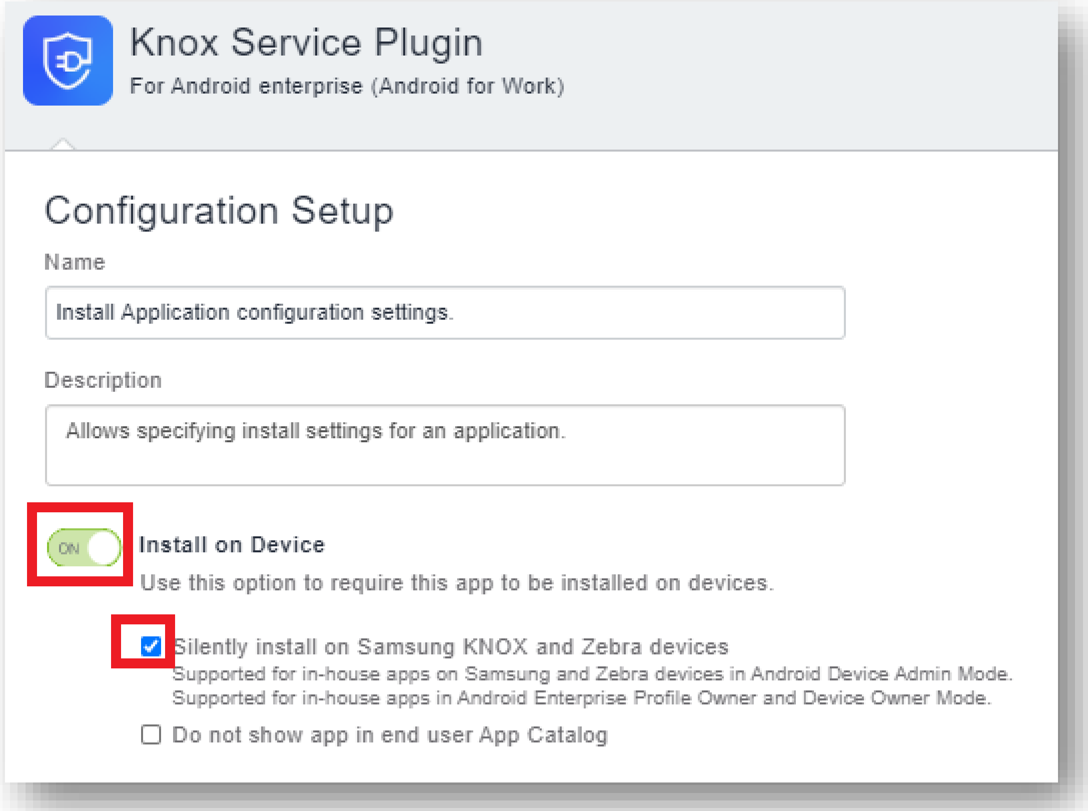
App Configurations

Managed Configurations for Android 1
Define and publish managed configurations for this app.

KPE Profile — All Users

Install on device 1
This configuration option decides whether to require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritised.

Install Application configuration settings.
Allows specifying install settings for an application. — All Users



Knox Service Plugin
For Android enterprise (Android for Work)

Configuration Setup

Name: Install Application configuration settings.

Description: Allows specifying install settings for an application.

ON Install on Device
Use this option to require this app to be installed on devices.

☑ Silently install on Samsung KNOX and Zebra devices
Supported for in-house apps on Samsung and Zebra devices in Android Device Admin Mode.
Supported for in-house apps in Android Enterprise Profile Owner and Device Owner Mode.

☐ Do not show app in end user App Catalog

Document Information

This is version 2.1 of this document.

Thank you!

Knox