Knox

FAMOC v 5.13.1

Knox Platform for Enterprise

December 2020
Samsung R&D Centre UK
(SRUK)

Agenda

1. Pre-requisites for Knox Platform for Enterprise
2. Managed Google Play [MGP] Configuration
3. Android Enterprise Deployment Modes
   - Work Profile
   - Fully Managed Device
   - Fully Managed Device with a Work Profile
   - Dedicated Device
4. Android Enterprise configuration
5. Work Profile enrollment
6. Fully Managed Device enrollment
7. Fully Managed Device with a Work Profile enrollment
8. Dedicated Device configuration
9. Configure Knox Service Plugin [KSP] Standard and Premium

FAMOC Collateral & Contacts

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

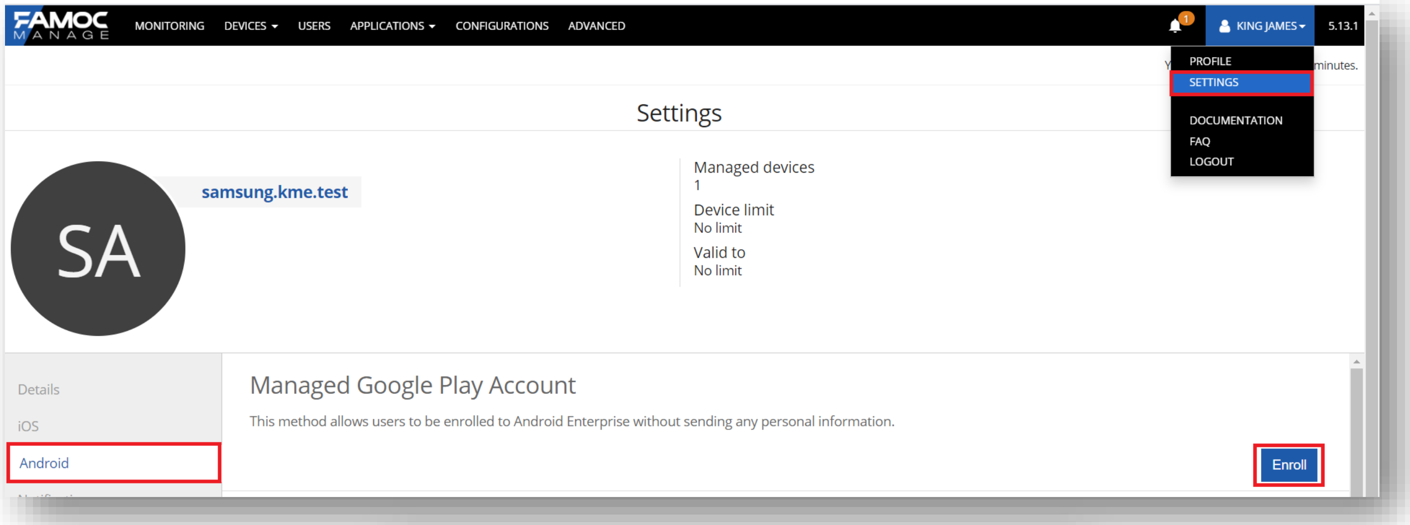
https://support.famoc.com

Pre-Requisites for Knox Platform for Enterprise

1. Obtain access to the FAMOC console
2. A Gmail account to map to FAMOC for Managed Google Play
3. Consider what enrollment method to use:
   - Knox Mobile Enrollment (KME)
   - QR Code enrollment
   - Email enrollment
   - Server details enrollment

Configure Android Enterprise

- Within the console, select your account name in the top right corner and then select SETTINGS
- Select Android and then Enroll
- Select Authorize Google



Settings

samsung.kme.test

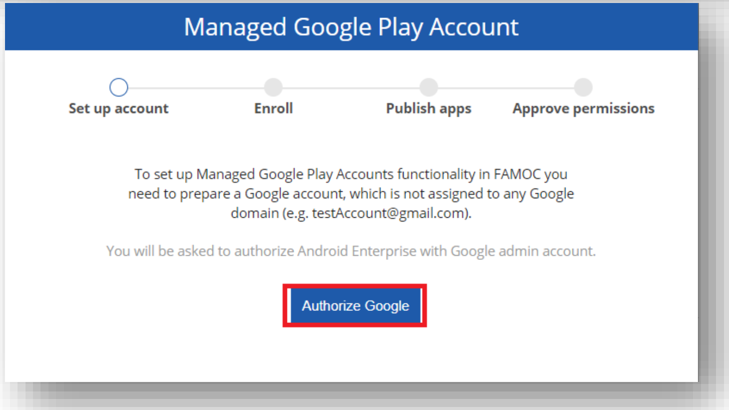
Managed devices
1

Device limit
No limit

Valid to
No limit

Managed Google Play Account

This method allows users to be enrolled to Android Enterprise without sending any personal information.



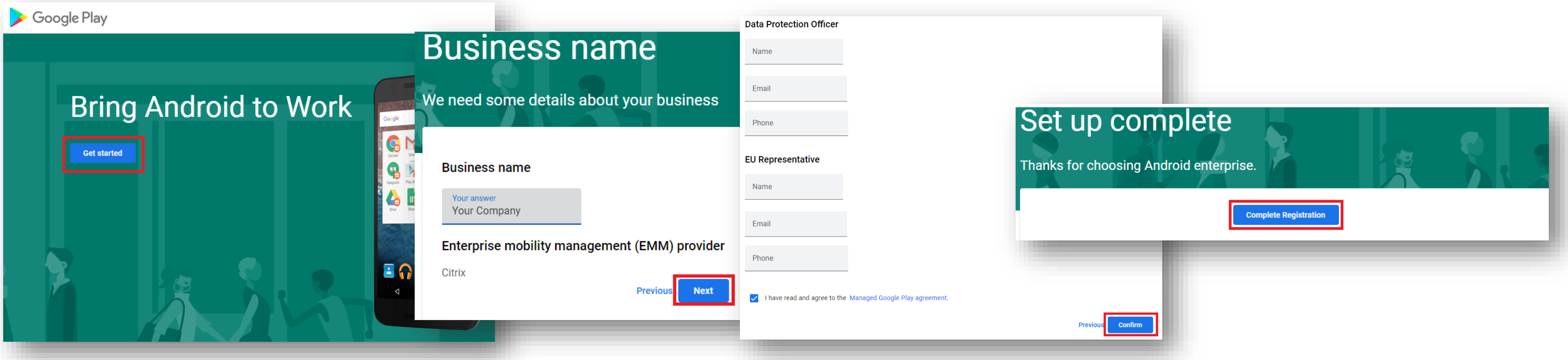
Managed Google Play Account

To set up Managed Google Play Accounts functionality in FAMOC you need to prepare a Google account, which is not assigned to any Google domain (e.g. testAccount@gmail.com).

You will be asked to authorize Android Enterprise with Google admin account.

Configure Android Enterprise

- Sign in with your Google Account and select Get Started
- Enter a Business name, select Next
- Data Protection Officer and EU Representative are optional, select Confirm
- Select Complete Registration



Google Play

Bring Android to Work

Get started

Business name

We need some details about your business

Business name

Your answer: Your Company

Enterprise mobility management (EMM) provider

Citrix

Previous Next

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

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

Previous Confirm

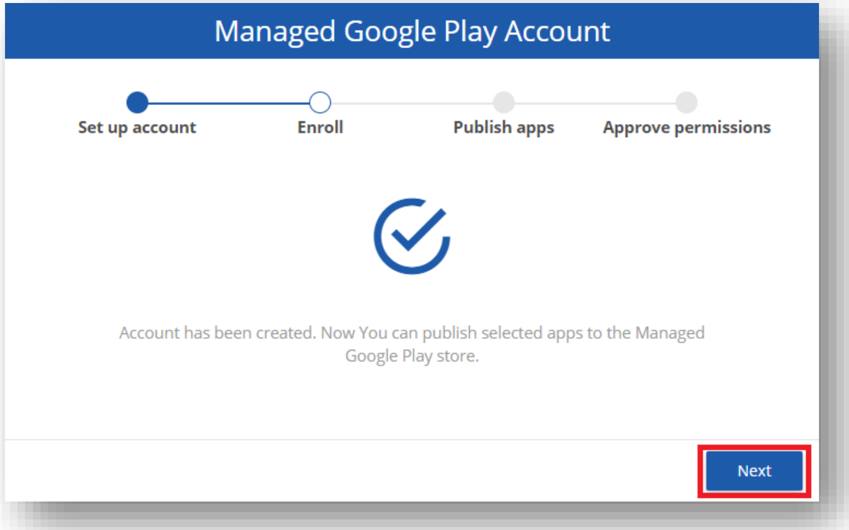
Set up complete

Thanks for choosing Android enterprise.

Complete Registration

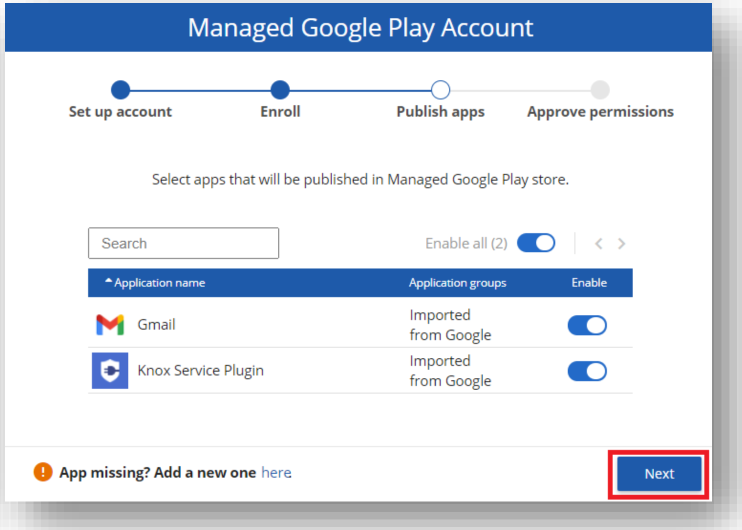
Configure Android Enterprise

- **Select Next**
- **Choose whether to import any pre-approved applications, then select Next**
- Select Close



Managed Google Play Account

Account has been created. Now You can publish selected apps to the Managed Google Play store.

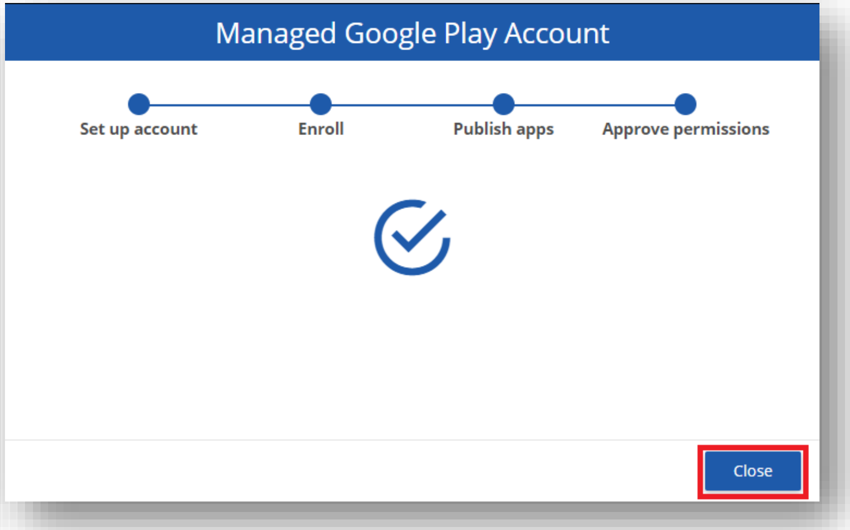


Managed Google Play Account

Select apps that will be published in Managed Google Play store.

Application name	Application groups	Enable
Gmail	Imported from Google	●
Knox Service Plugin	Imported from Google	●

App missing? Add a new one here



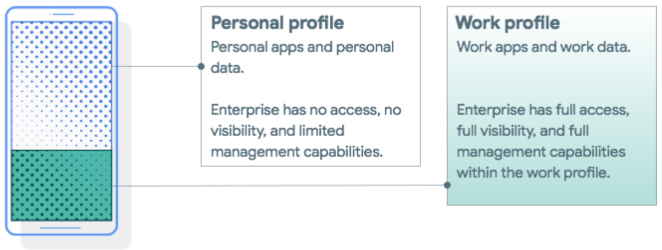
Managed Google Play Account

Android Enterprise Deployment Modes

Android Enterprise can be deployed in the following 4 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. Dedicated Device [*formerly known as COSU*]

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



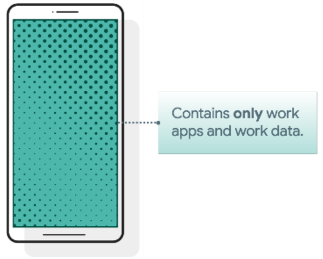
Personal profile
Personal apps and personal data.

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

Work profile
Work apps and work data.

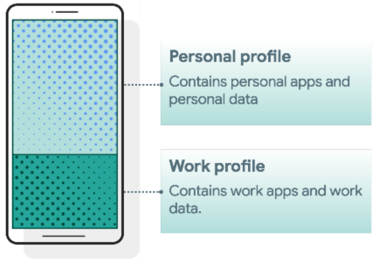
Enterprise has full access, full visibility, and full management capabilities within the work profile.

Work Profile



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

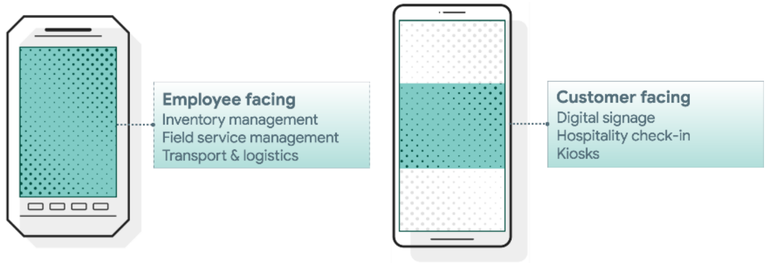
Fully Managed Device



Personal profile
Contains personal apps and personal data

Work profile
Contains work apps and work data.

Fully Managed Device with a Work Profile



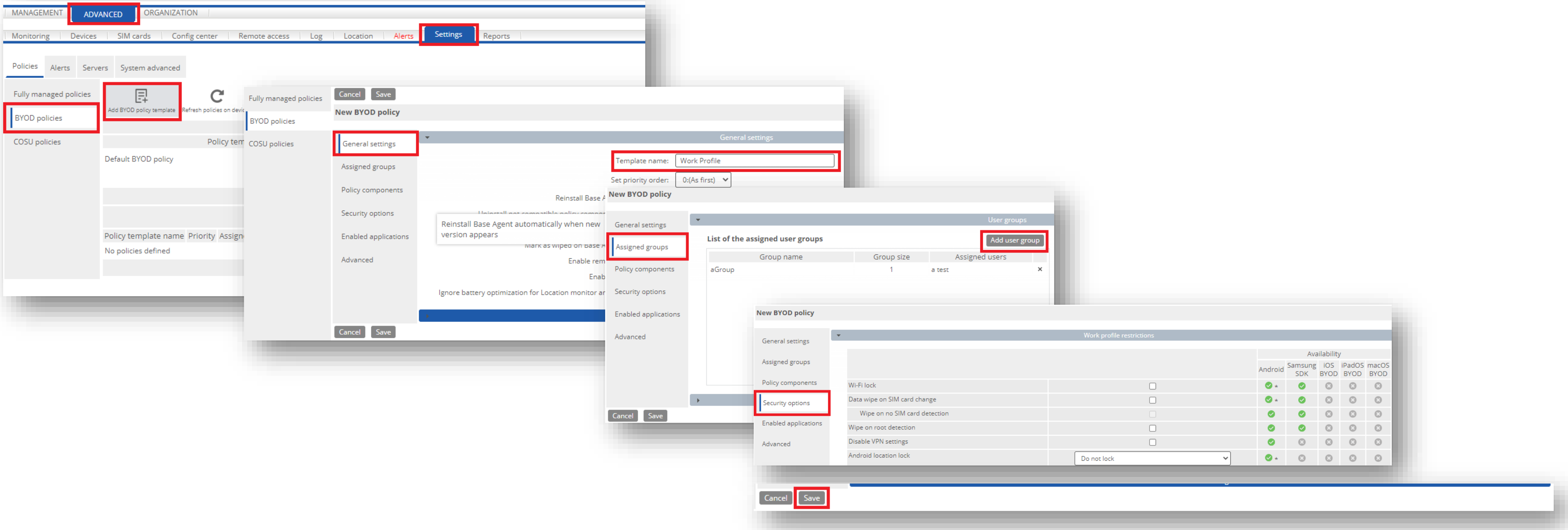
Employee facing
Inventory management
Field service management
Transport & logistics

Customer facing
Digital signage
Hospitality check-in
Kiosks

Dedicated Device

Work Profile Configuration

- Navigate to: ADVANCED > Settings > BYOD policies
- Select Add BYOD policy template
- In the General settings tab, enter a Template name
- In the Assigned groups tab, select Add user group. Select your target group.
- In the Security options tab, select your desired restrictions and then select Save



Default BYOD policy

Policy template name	Priority	Assign
No policies defined		

New BYOD policy

General settings

Template name: Work Profile

Set priority order: 0:(As first)

Reinstall Base Agent automatically when new version appears

New BYOD policy

List of the assigned user groups

Add user group

Group name	Group size	Assigned users	
aGroup	1	a test	×

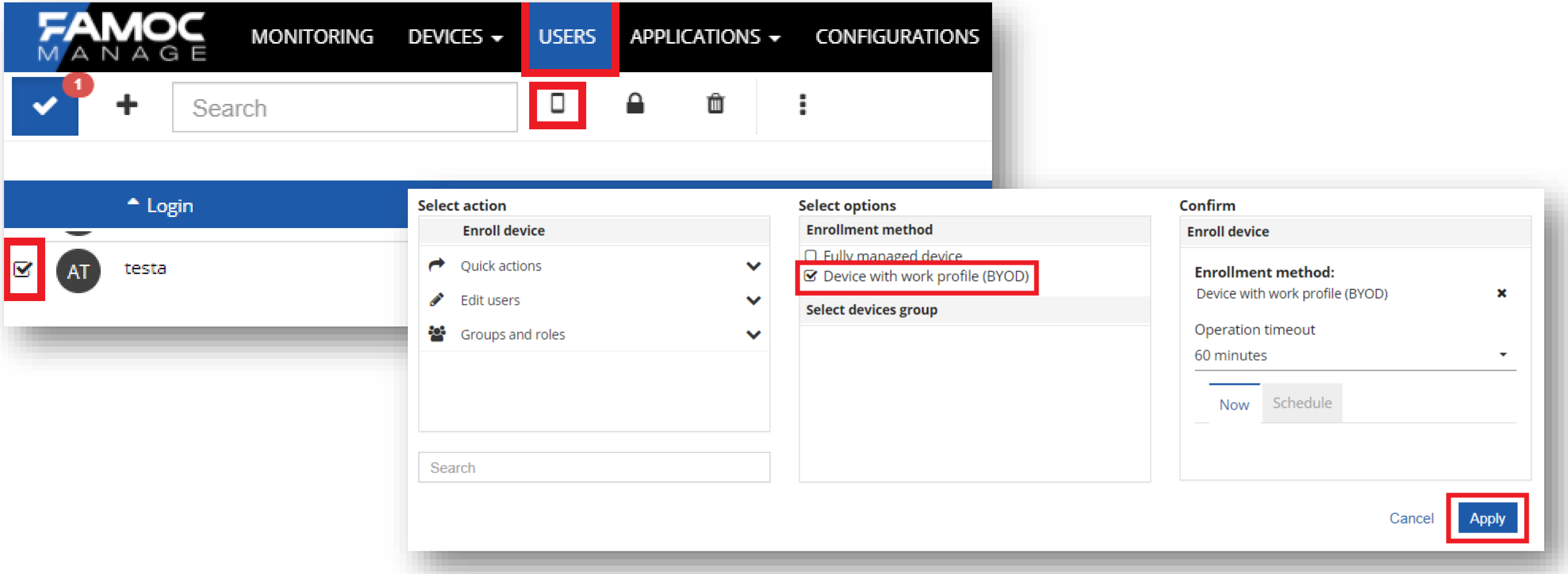
New BYOD policy

Work profile restrictions

		Availability				
		Android	Samsung SDK	iOS BYOD	iPadOS BYOD	macOS BYOD
Wi-Fi lock	☐	✓ *	✓	⊗	⊗	⊗
Data wipe on SIM card change	☐	✓ *	✓	⊗	⊗	⊗
Wipe on no SIM card detection	☐	✓	✓	⊗	⊗	⊗
Wipe on root detection	☐	✓	✓	⊗	⊗	⊗
Disable VPN settings	☐	✓	⊗	⊗	⊗	⊗
Android location lock	Do not lock	✓ *	⊗	⊗	⊗	⊗

Work Profile Configuration

- Navigate to: USERS
- Select the user you wish to enroll
- Select the Enroll Device button (mobile phone icon)
- For Enrollment method, select Device with work profile (BYOD)
- Select Apply, this will now email the end user a QR code which will be used for the device enrollment



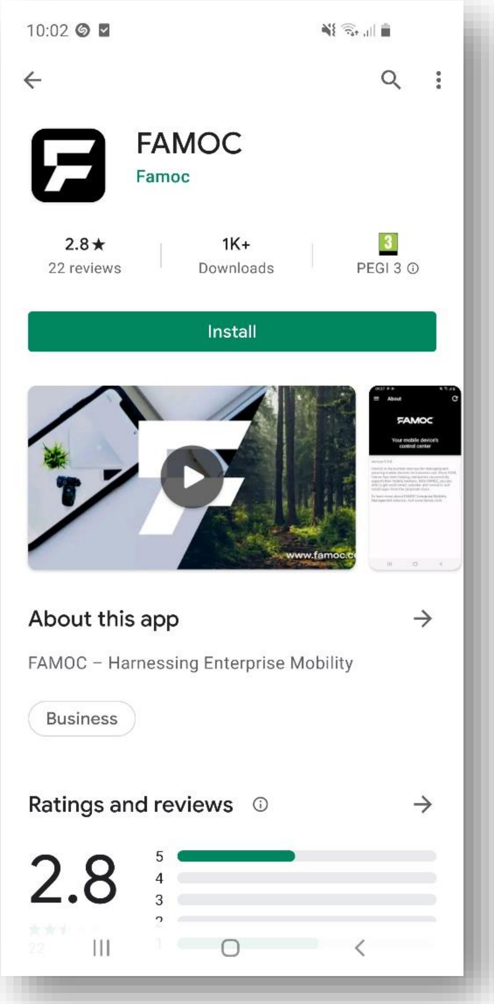
Enrollment method
□ Fully managed device
☑ Device with work profile (BYOD)
Select devices group

Enroll device

Enrollment method:
Device with work profile (BYOD)

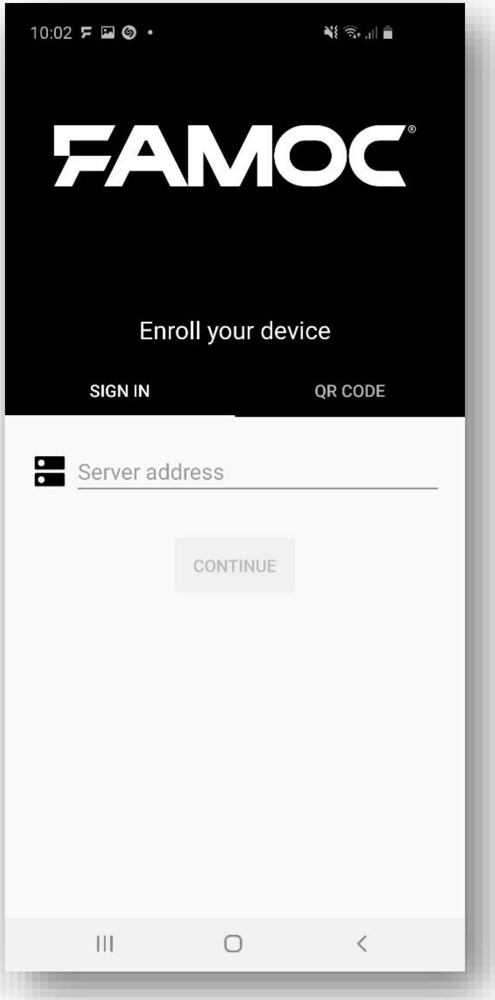
Operation timeout
60 minutes

Android Enterprise: Work Profile Enrollment

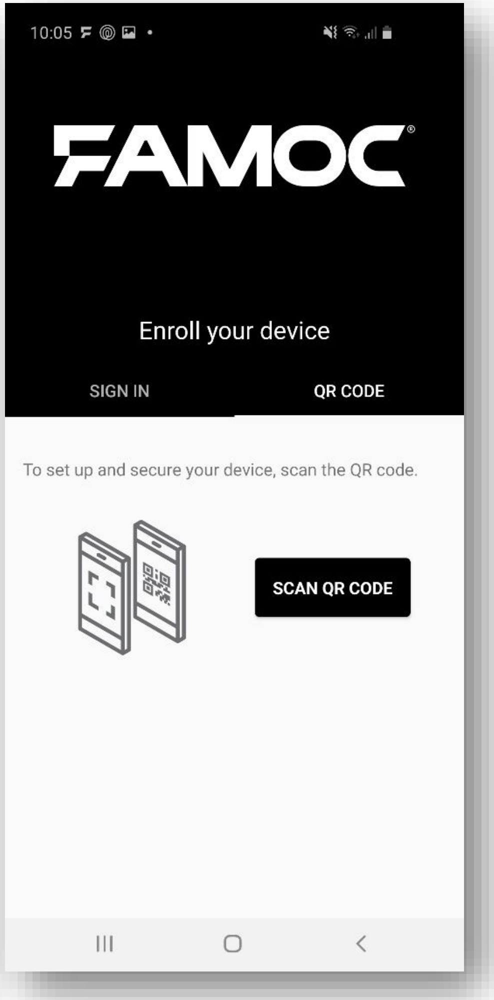


FAMOC – Harnessing Enterprise Mobility

Install FAMOC
From the Google Play Store

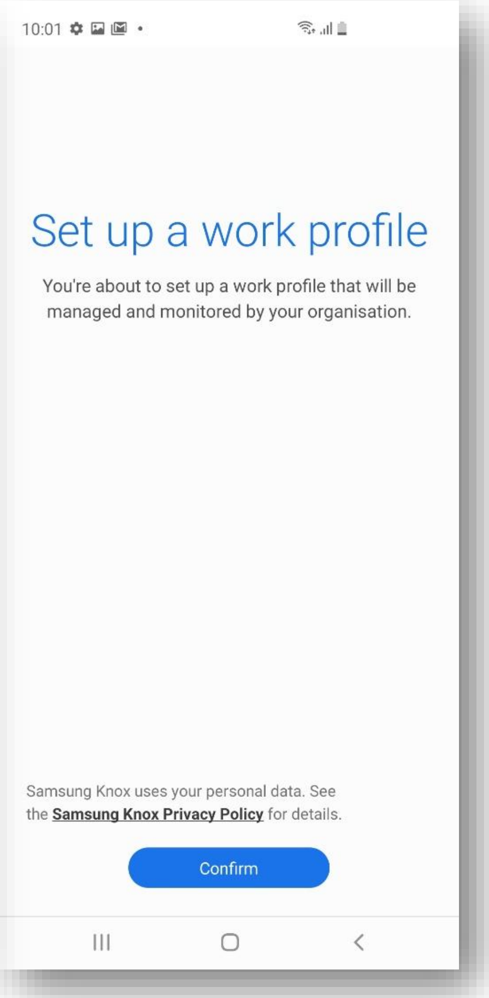


Select QR CODE



To set up and secure your device, scan the QR code.

Select SCAN QR CODE, then
Scan the code sent to you by email

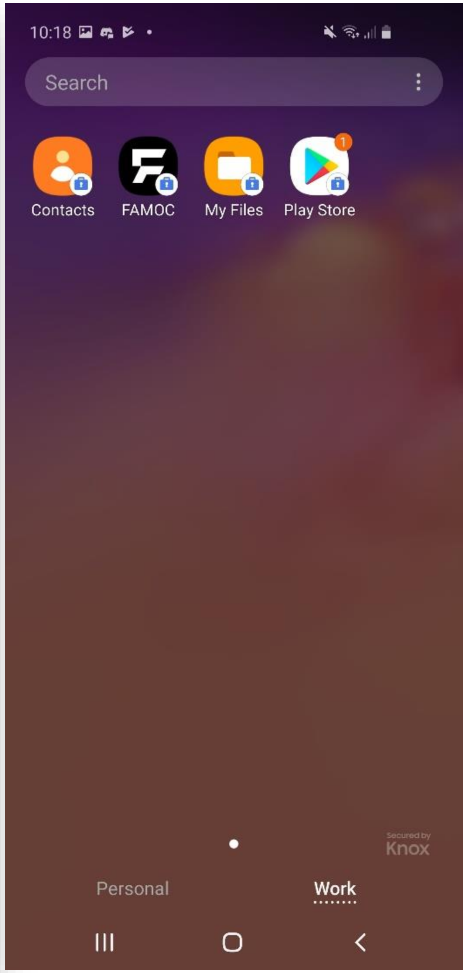


Set up a work profile

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.

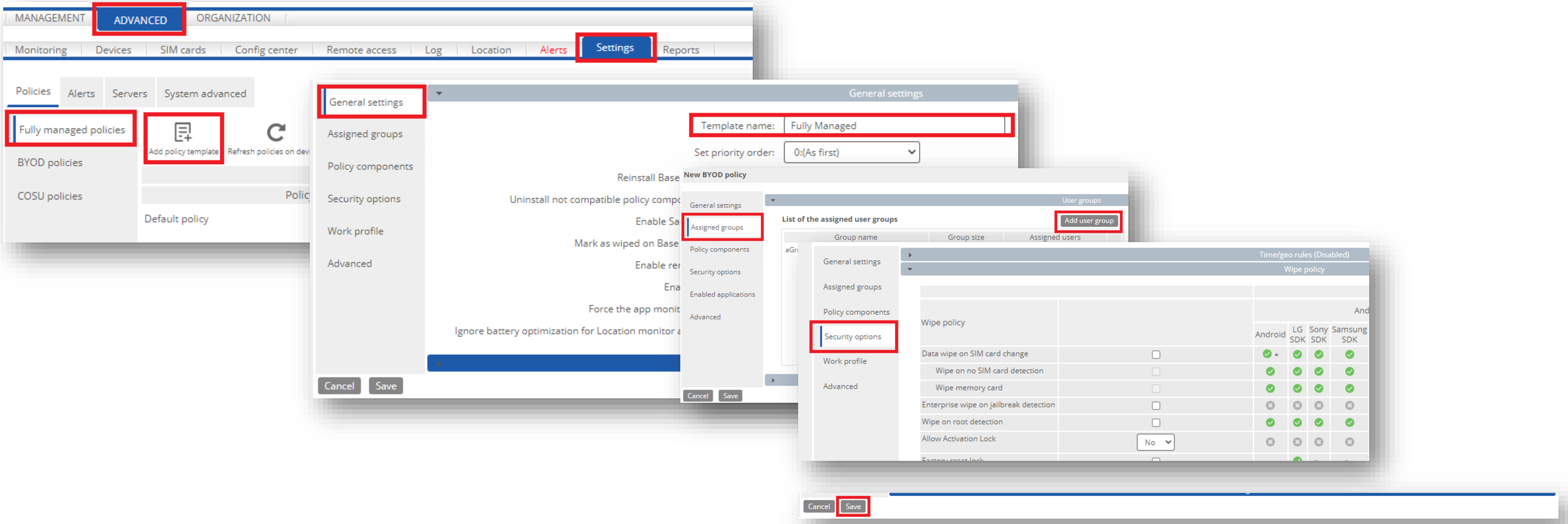
Confirm



Device is now enrolled

Fully Managed Device Configuration

- Navigate to: ADVANCED > Settings > Fully managed policies
- Select Add policy template
- In the General settings tab, enter a Template name
- In the Assigned groups tab, select Add user group. Select your target group.
- In the Security options tab, select your desired restrictions and then select Save



Template name: Fully Managed

Set priority order: 0:(As first)

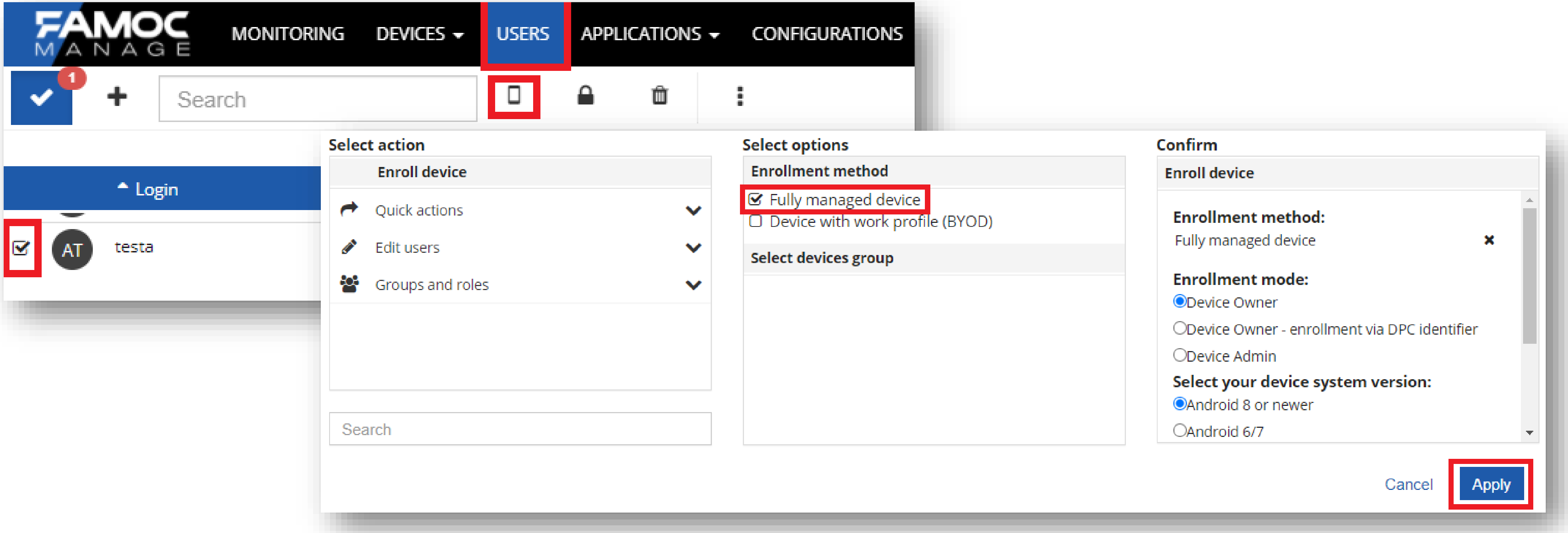
List of the assigned user groups

Group name	Group size	Assigned users

Wipe policy		Android	LG SDK	Sony SDK	Samsung SDK
Data wipe on SIM card change	☐	✓ *	✓	✓	✓
Wipe on no SIM card detection	☐	✓	✓	✓	✓
Wipe memory card	☐	✓	✓	✓	✓
Enterprise wipe on jailbreak detection	☐	☒	☒	☒	☒
Wipe on root detection	☐	✓	✓	✓	✓
Allow Activation Lock	No	☒	☒	☒	☒
Factory reset lock	☐		✓		

Fully Managed Configuration

- Navigate to: USERS
- Select the user you wish to enroll
- Select the Enroll Device button (mobile phone icon)
- For Enrollment method, select Fully managed device
- Select Apply, this will now email the end user a QR code which will be used for the device enrollment



Enrollment method

☑ Fully managed device

□ Device with work profile (BYOD)

Select devices group

Confirm

Enroll device

Enrollment method:
Fully managed device

Enrollment mode:
● Device Owner
○ Device Owner - enrollment via DPC identifier
○ Device Admin

Select your device system version:
● Android 8 or newer
○ Android 6/7

Android Enterprise: Fully Managed Device Enrollment

Android Enterprise Fully Managed Device Deployment

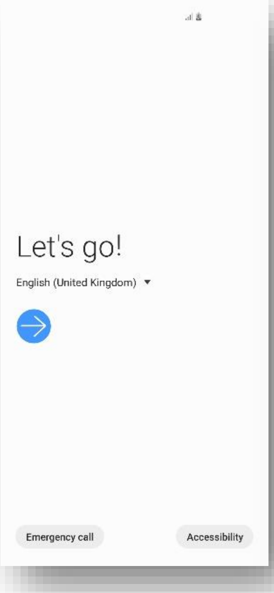
To enroll your device as an Android Enterprise Fully Managed Device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into FAMOC as an Android Enterprise Fully Managed Device.

1. DPC Identifier [Also known as the hashtag method] afw#famoc

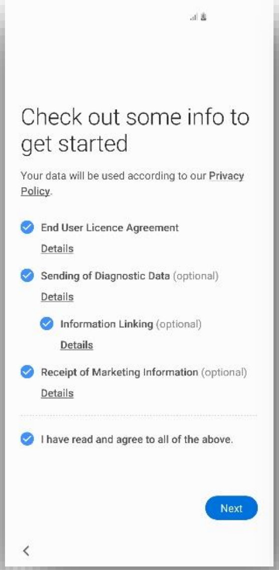
2. QR Code Enrollment / NFC Enrollment

3. Knox Mobile Enrollment

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



Select the arrow


Check out some info to get started

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement Details

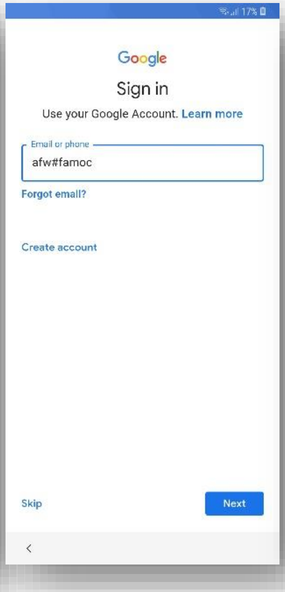
☑ Sending of Diagnostic Data (optional) Details

☑ Information Linking (optional) Details

☑ Receipt of Marketing Information (optional) Details

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

Accept the EULA, Next

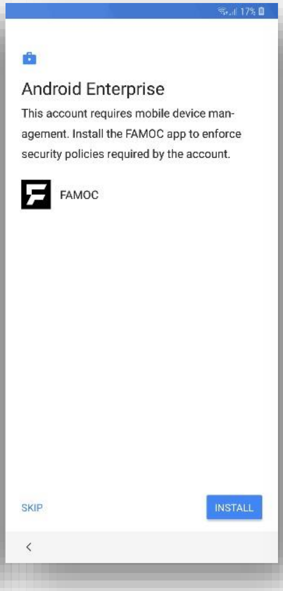

Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#famoc

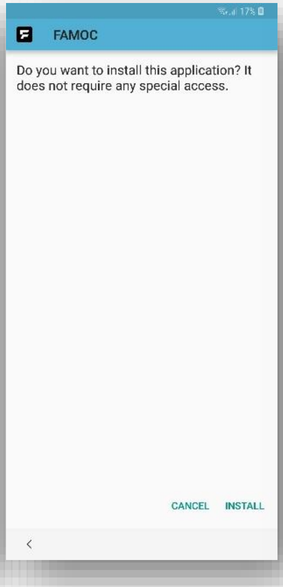
Enter afw#famoc then select Next


Android Enterprise

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

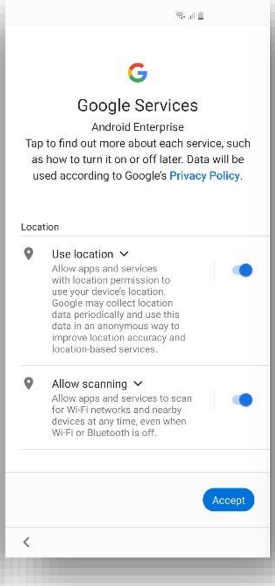
FAMOC

INSTALL


FAMOC

Do you want to install this application? It does not require any special access.

INSTALL


Google Services

Android Enterprise

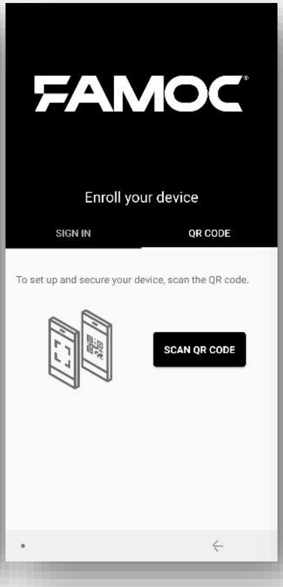
Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

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.

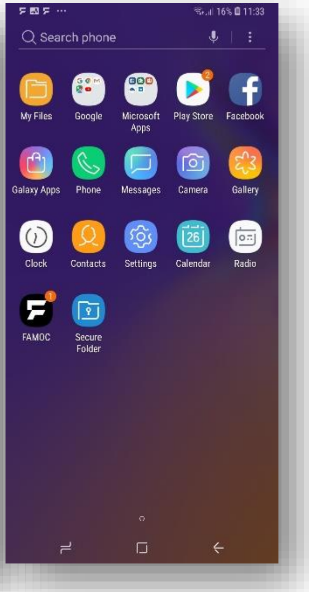
Accept


FAMOC

Enroll your device

To set up and secure your device, scan the QR code.

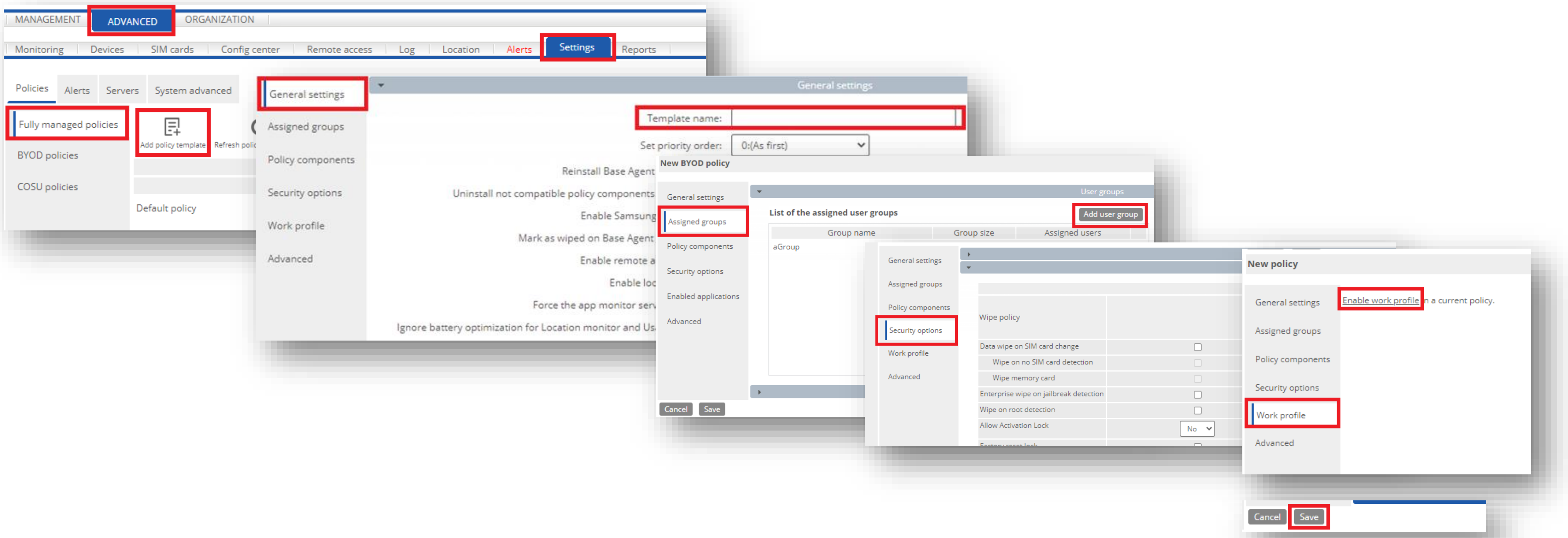
Scan the QR code sent to you by email



Device is now enrolled

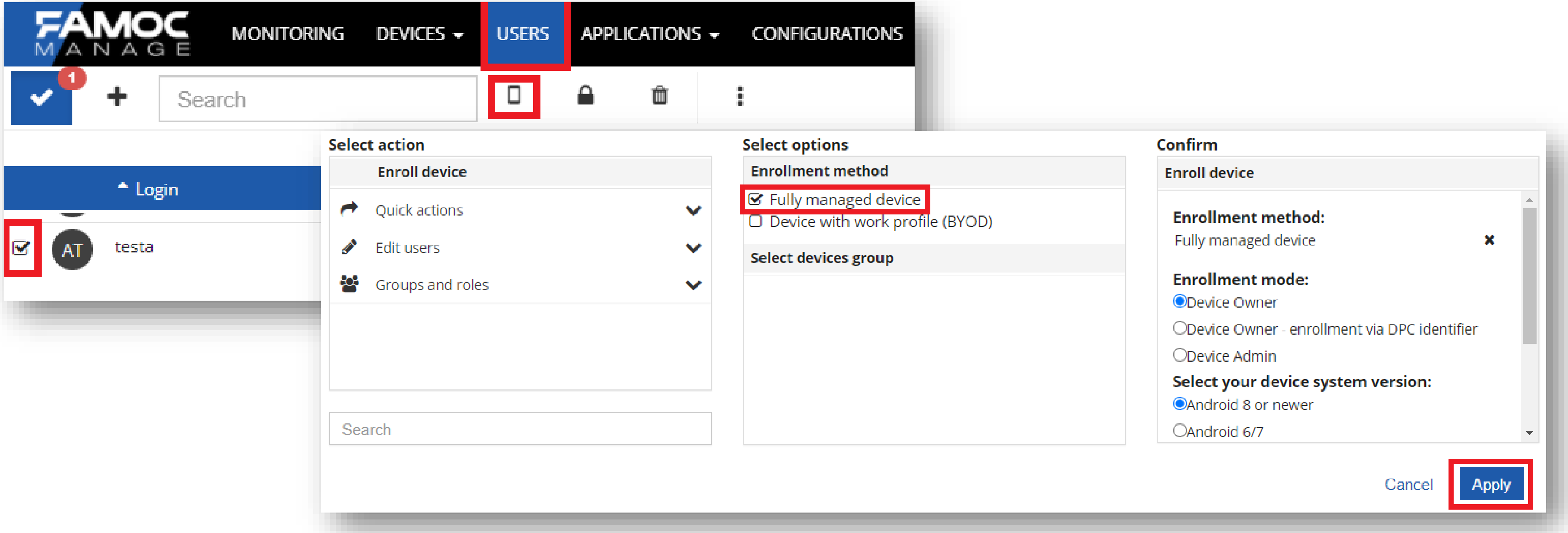
Fully Managed Device with a Work Profile Configuration

- Navigate to: ADVANCED > Settings > Fully managed policies
- Select Add policy template
- In the General settings tab, enter a Template name
- In the Assigned groups tab, select Add user group. Select your target group.
- In the Security options tab, select your desired restrictions
- In the Work Profile tab, select Enable work profile
- Once you have configured your policy, select Save
- Save



Fully Managed Device with a Work Profile Configuration

- Navigate to: USERS
- Select the user you wish to enroll
- Select the Enroll Device button (mobile phone icon)
- For Enrollment method, select Fully managed device
- Select Apply, this will now email the end user a QR code which will be used for the device enrollment



Select action

Enroll device

Select options

Enrollment method

☑ Fully managed device

☐ Device with work profile (BYOD)

Select devices group

Confirm

Enroll device

Enrollment method:
Fully managed device

Enrollment mode:

● Device Owner

○ Device Owner - enrollment via DPC identifier

○ Device Admin

Select your device system version:

● Android 8 or newer

○ Android 6/7

Android Enterprise: Fully Managed Device with a Work Profile Enrollment

Android Enterprise Fully Managed Device with a Work Profile Deployment

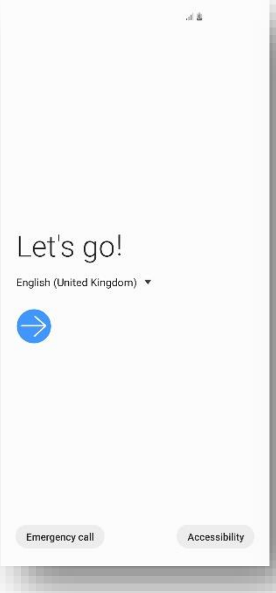
To enroll your device as an Android Enterprise Fully Managed Device with a Work Profile, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into FAMOC as an Android Enterprise Fully Managed Device with a Work Profile.

1. DPC Identifier [Also known as the hashtag method] afw#famoc

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.**



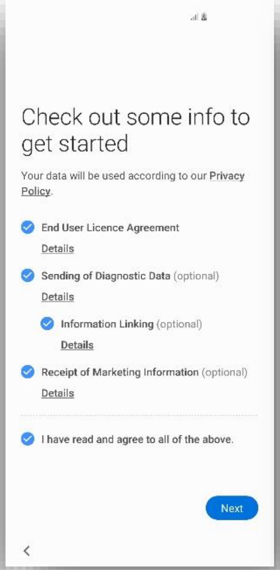
Let's go!

English (United Kingdom) ▾

Emergency call

Accessibility

Select the arrow



Check out some info to get started

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement
Details

☑ Sending of Diagnostic Data (optional)
Details

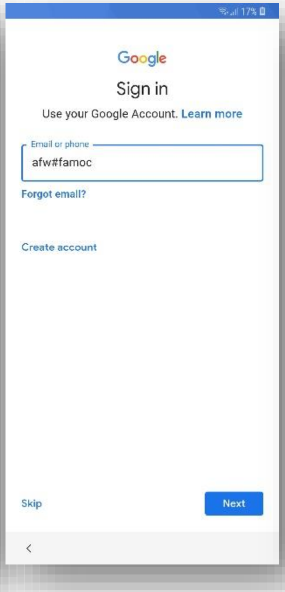
☑ Information Linking (optional)
Details

☑ Receipt of Marketing Information (optional)
Details

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

Next

Accept the EULA, Next



Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#famoc

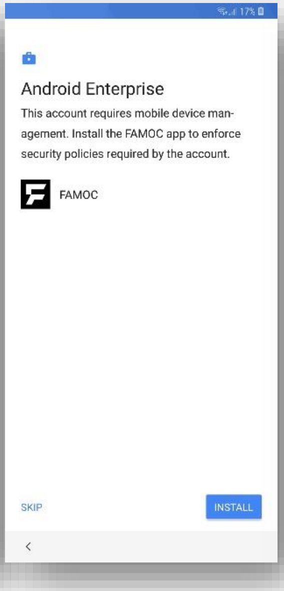
Forgot email?

Create account

Skip

Next

Enter afw#famoc then select Next



Android Enterprise

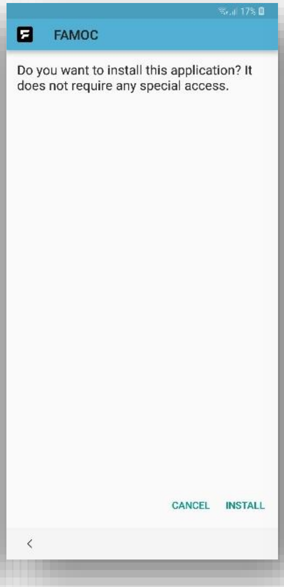
This account requires mobile device management. Install the FAMOC app to enforce security policies required by the account.

FAMOC

SKIP

INSTALL

INSTALL



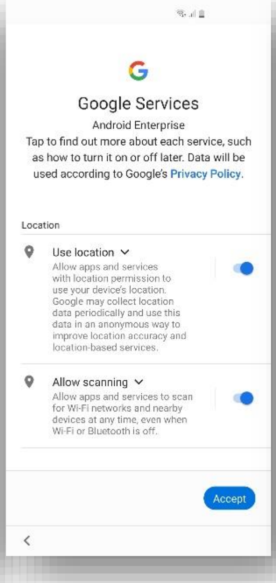
FAMOC

Do you want to install this application? It does not require any special access.

CANCEL

INSTALL

INSTALL



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.

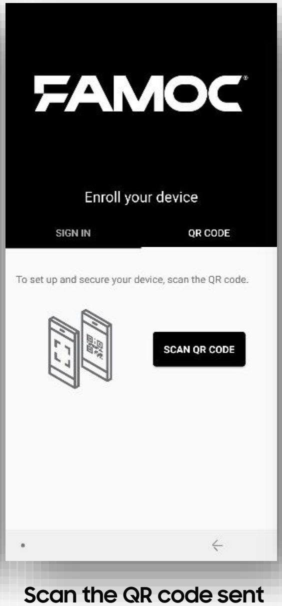
Location

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.

Accept

Accept



FAMOC

Enroll your device

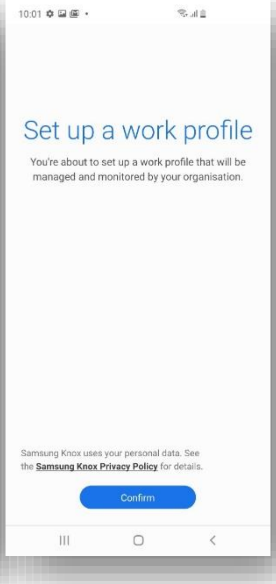
SIGN IN

QR CODE

To set up and secure your device, scan the QR code.

SCAN QR CODE

Scan the QR code sent to you by email



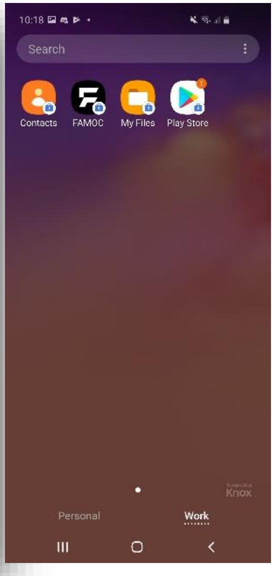
Set up a work profile

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.

Confirm

Confirm

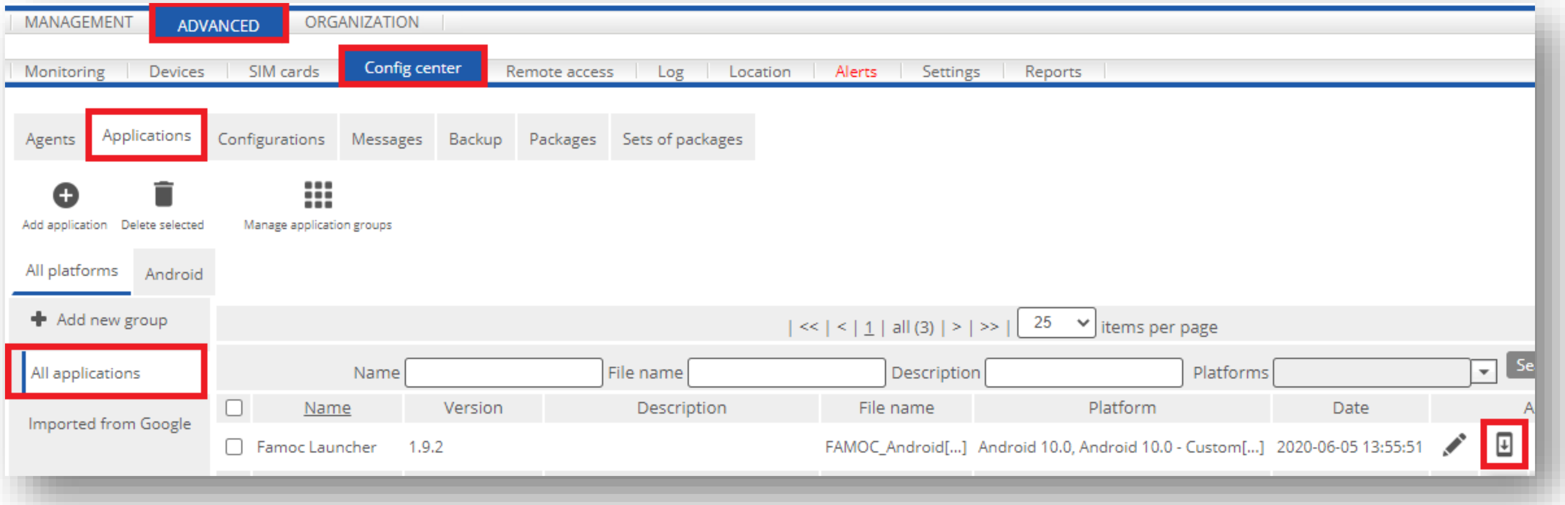


Device is now enrolled

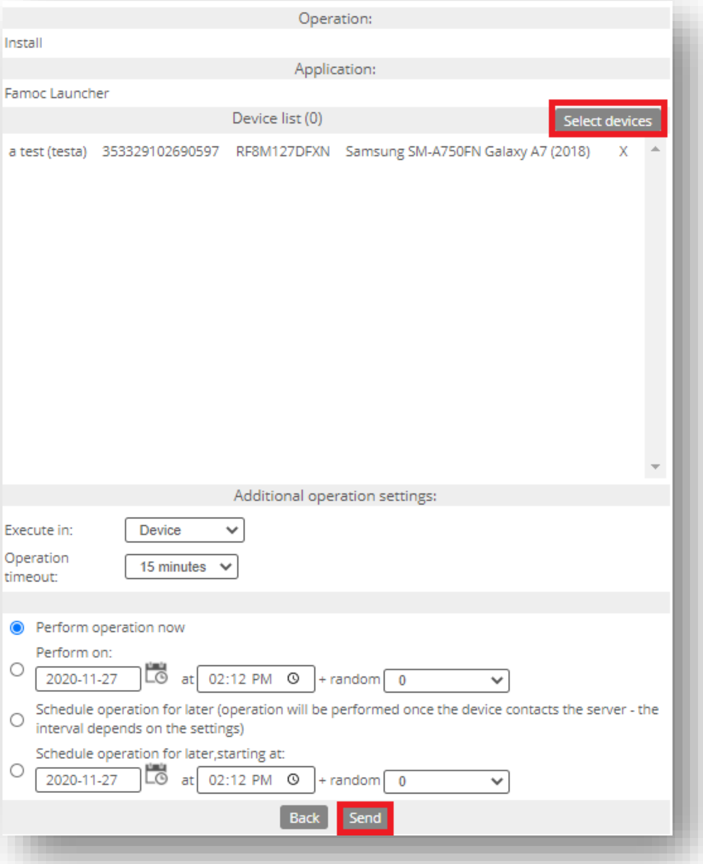
Dedicated Device Configuration

To setup a Dedicated device in FAMOC, you must first enroll your device using the Fully Managed Enrollmen

- Navigate to: ADVANCED > Config center > Applications > All applications
- Next to the Famoc Launcher, select the Install application button
- Click on Select devices and choose the devices you want to target
- Select Send



□	Name	Version	Description	File name	Platform	Date	A
□	Famoc Launcher	1.9.2		FAMOC_Android[...]	Android 10.0, Android 10.0 - Custom[...]	2020-06-05 13:55:51	


Operation:

Install

Application:

Famoc Launcher

Device list (0)

a test (testa) 353329102690597 RF8M127DFXN Samsung SM-A750FN Galaxy A7 (2018) X

Additional operation settings:

Execute in: Device

Operation timeout: 15 minutes

● Perform operation now

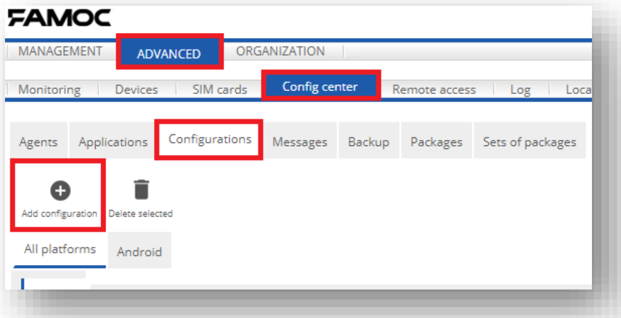
○ Perform on: 2020-11-27 at 02:12 PM + random 0

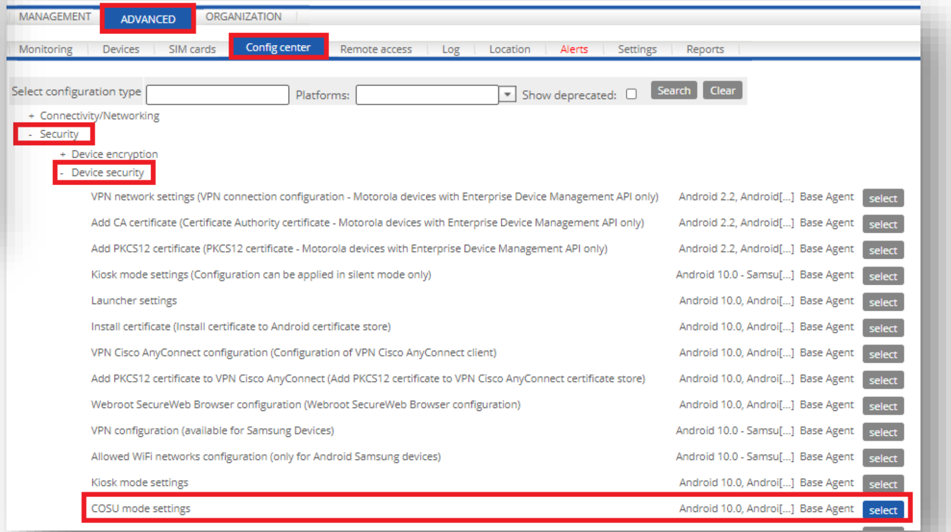
○ Schedule operation for later (operation will be performed once the device contacts the server - the interval depends on the settings)

○ Schedule operation for later,starting at: 2020-11-27 at 02:12 PM + random 0

Dedicated Device Configuration

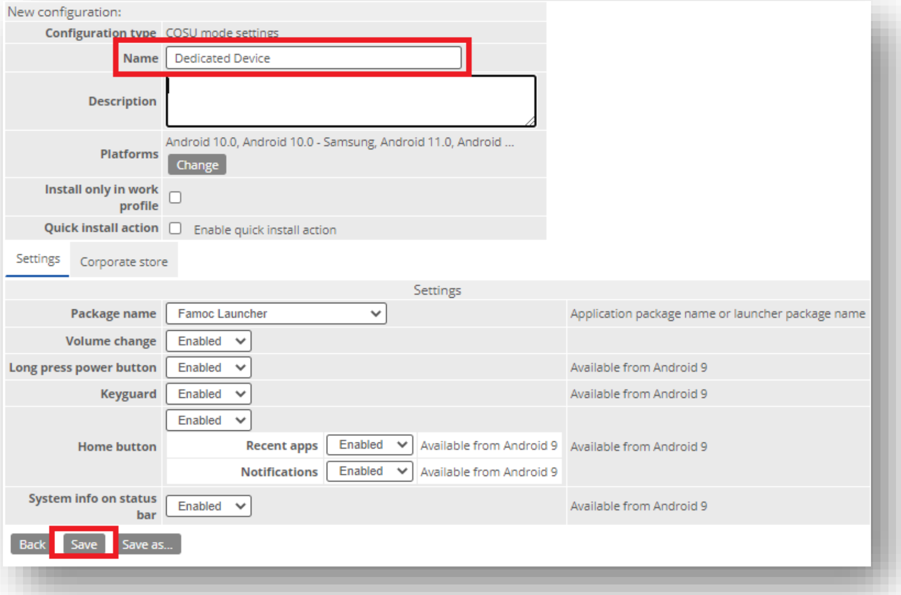
- Navigate to: ADVANCED > Config center > Configurations
- Select Add Configuration
- Navigate to Security > Device security
- Select COSU mode settings
- Enter a Name
- Once you have configured your profile, select Save





+ Connectivity/Networking
- Security
  + Device encryption
  - Device security

VPN network settings (VPN connection configuration - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Add CA certificate (Certificate Authority certificate - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Add PKCS12 certificate (PKCS12 certificate - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Kiosk mode settings (Configuration can be applied in silent mode only)	Android 10.0 - Samsu[...]	Base Agent	select
Launcher settings	Android 10.0, Androi[...]	Base Agent	select
Install certificate (Install certificate to Android certificate store)	Android 10.0, Androi[...]	Base Agent	select
VPN Cisco AnyConnect configuration (Configuration of VPN Cisco AnyConnect client)	Android 10.0, Androi[...]	Base Agent	select
Add PKCS12 certificate to VPN Cisco AnyConnect (Add PKCS12 certificate to VPN Cisco AnyConnect certificate store)	Android 10.0, Androi[...]	Base Agent	select
Webroot SecureWeb Browser configuration (Webroot SecureWeb Browser configuration)	Android 10.0, Androi[...]	Base Agent	select
VPN configuration (available for Samsung Devices)	Android 10.0 - Samsu[...]	Base Agent	select
Allowed WiFi networks configuration (only for Android Samsung devices)	Android 10.0 - Samsu[...]	Base Agent	select
Kiosk mode settings	Android 10.0, Androi[...]	Base Agent	select
COSU mode settings	Android 10.0, Androi[...]	Base Agent	select



New configuration:

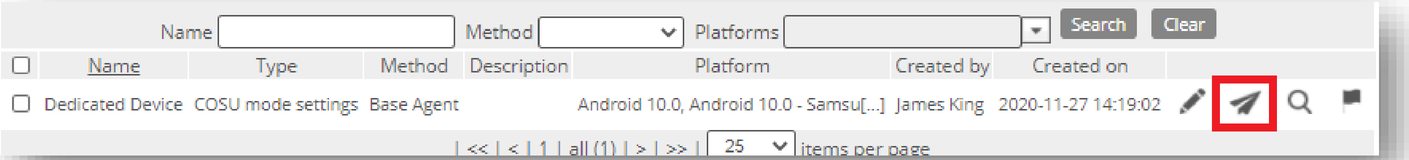
Configuration type	COSU mode settings
Name	Dedicated Device
Description	
Platforms	Android 10.0, Android 10.0 - Samsung, Android 11.0, Android ...
Install only in work profile	□
Quick install action	□ Enable quick install action

Settings

Package name	Famoc Launcher	Application package name or launcher package name
Volume change	Enabled	
Long press power button	Enabled	Available from Android 9
Keyguard	Enabled	Available from Android 9
Home button	Enabled Recent apps: Enabled — Available from Android 9 Notifications: Enabled — Available from Android 9	Available from Android 9
System info on status bar	Enabled	Available from Android 9

Dedicated Device Configuration

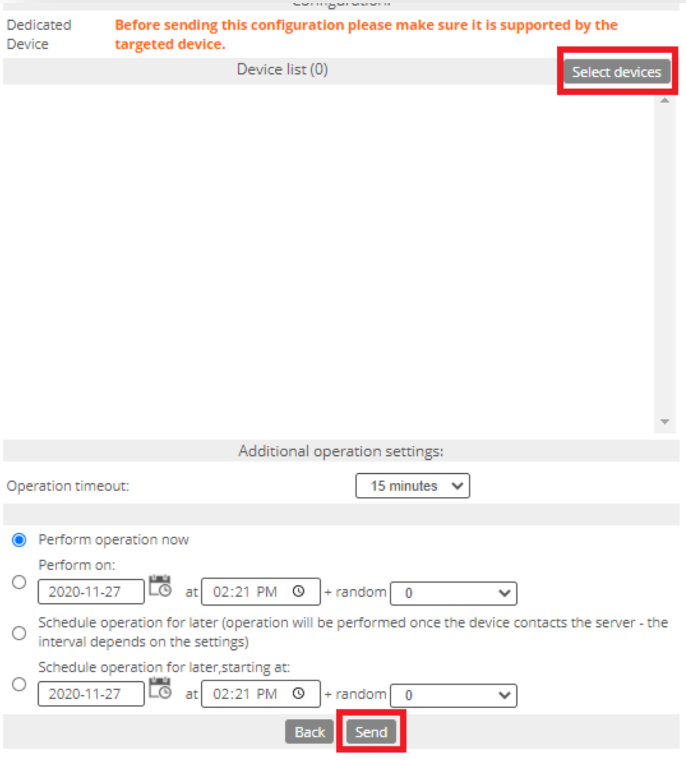
- Select the Send configuration button
- Click on Select devices and choose the devices you want to target
- Select Send



Name Method Platforms

□	Name	Type	Method	Description	Platform	Created by	Created on
□	Dedicated Device	COSU mode settings	Base Agent		Android 10.0, Android 10.0 - Samsu[...]	James King	2020-11-27 14:19:02

| << | < | 1 | all (1) | > | >> | 25 items per page



Dedicated Device

Before sending this configuration please make sure it is supported by the targeted device.

Device list (0)

Additional operation settings:

Operation timeout: 15 minutes

● Perform operation now

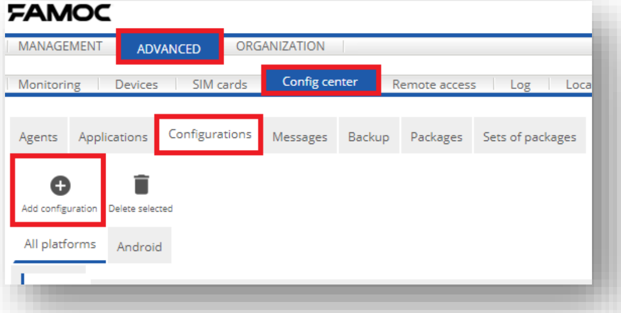
○ Perform on: 2020-11-27 at 02:21 PM + random 0

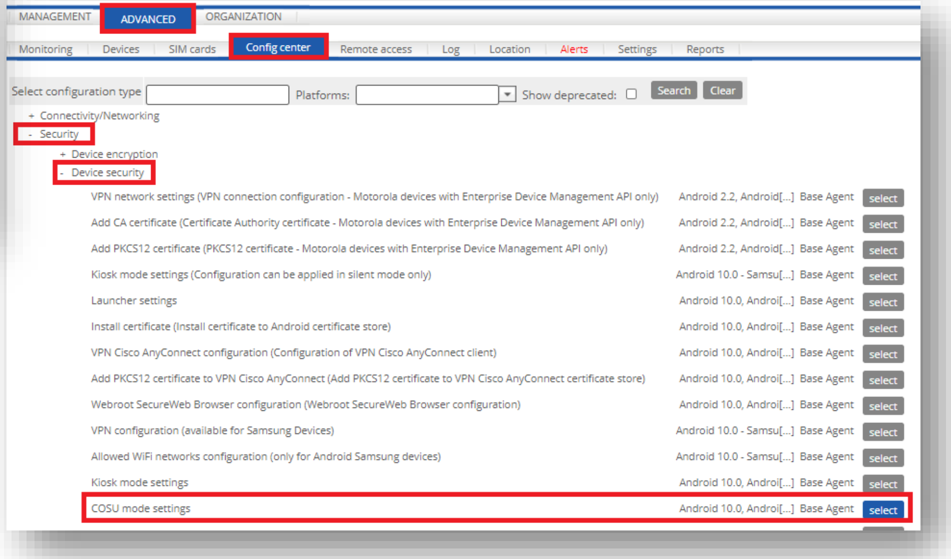
○ Schedule operation for later (operation will be performed once the device contacts the server - the interval depends on the settings)

○ Schedule operation for later,starting at: 2020-11-27 at 02:21 PM + random 0

Dedicated Device Configuration

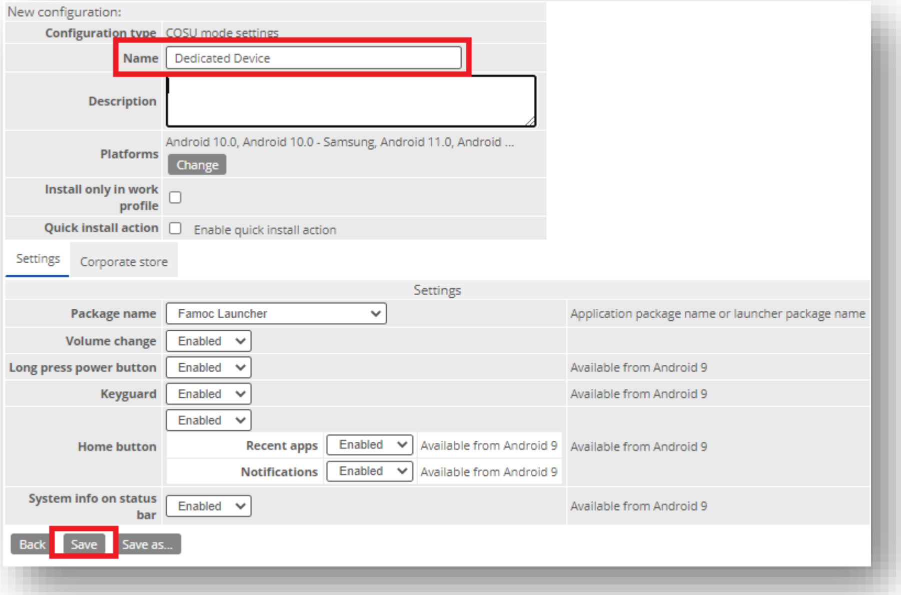
- Navigate to: ADVANCED > Config center > Configurations
- Select Add Configuration
- Navigate to Security > Device security
- Select COSU mode settings
- Enter a Name
- Once you have configured your profile, select Save





- + Connectivity/Networking
- - Security
  - + Device encryption
  - - Device security

VPN network settings (VPN connection configuration - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Add CA certificate (Certificate Authority certificate - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Add PKCS12 certificate (PKCS12 certificate - Motorola devices with Enterprise Device Management API only)	Android 2.2, Android[...]	Base Agent	select
Kiosk mode settings (Configuration can be applied in silent mode only)	Android 10.0 - Samsu[...]	Base Agent	select
Launcher settings	Android 10.0, Androi[...]	Base Agent	select
Install certificate (Install certificate to Android certificate store)	Android 10.0, Androi[...]	Base Agent	select
VPN Cisco AnyConnect configuration (Configuration of VPN Cisco AnyConnect client)	Android 10.0, Androi[...]	Base Agent	select
Add PKCS12 certificate to VPN Cisco AnyConnect (Add PKCS12 certificate to VPN Cisco AnyConnect certificate store)	Android 10.0, Androi[...]	Base Agent	select
Webroot SecureWeb Browser configuration (Webroot SecureWeb Browser configuration)	Android 10.0, Androi[...]	Base Agent	select
VPN configuration (available for Samsung Devices)	Android 10.0 - Samsu[...]	Base Agent	select
Allowed WiFi networks configuration (only for Android Samsung devices)	Android 10.0 - Samsu[...]	Base Agent	select
Kiosk mode settings	Android 10.0, Androi[...]	Base Agent	select
COSU mode settings	Android 10.0, Androi[...]	Base Agent	select



New configuration:

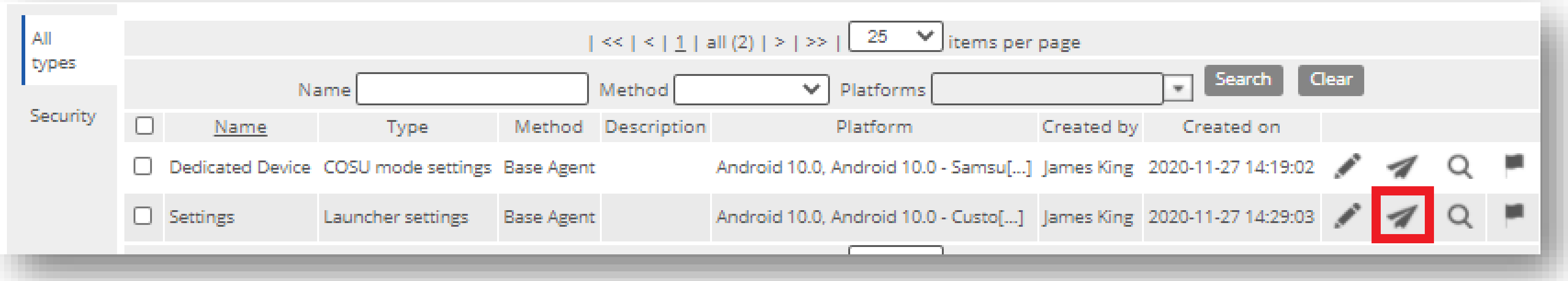
Configuration type	COSU mode settings
Name	Dedicated Device
Description	
Platforms	Android 10.0, Android 10.0 - Samsung, Android 11.0, Android ...
Install only in work profile	□
Quick install action	□ Enable quick install action

Settings

Package name	Famoc Launcher	Application package name or launcher package name
Volume change	Enabled	
Long press power button	Enabled	Available from Android 9
Keyguard	Enabled	Available from Android 9
Home button	Enabled Recent apps: Enabled — Available from Android 9 Notifications: Enabled — Available from Android 9	Available from Android 9
System info on status bar	Enabled	Available from Android 9

Dedicated Device Configuration

- Select the Send configuration button against the Launcher settings you just created
- Your device will now be configured



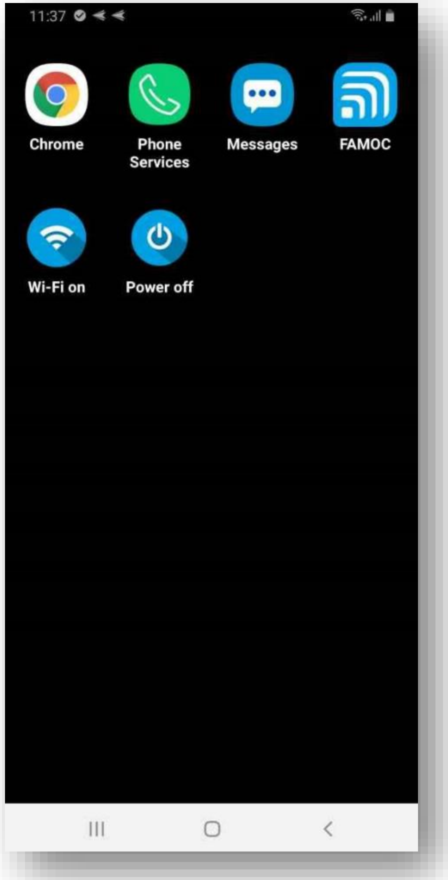
All types

Security

| << | < | 1 | all (2) | > | >> | 25 items per page

Name [ ] Method [ ] Platforms [ ] Search Clear

□	Name	Type	Method	Description	Platform	Created by	Created on				
□	Dedicated Device	COSU mode settings	Base Agent		Android 10.0, Android 10.0 - Samsu[...]	James King	2020-11-27 14:19:02	✎	➤	🔍	⚑
□	Settings	Launcher settings	Base Agent		Android 10.0, Android 10.0 - Custo[...]	James King	2020-11-27 14:29:03	✎	➤	🔍	⚑



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 [$]

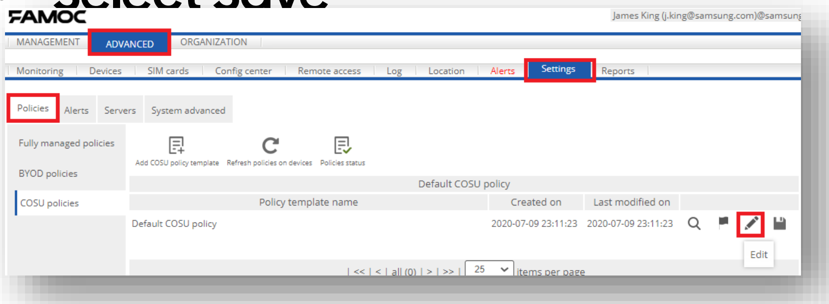
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android 8 or above.

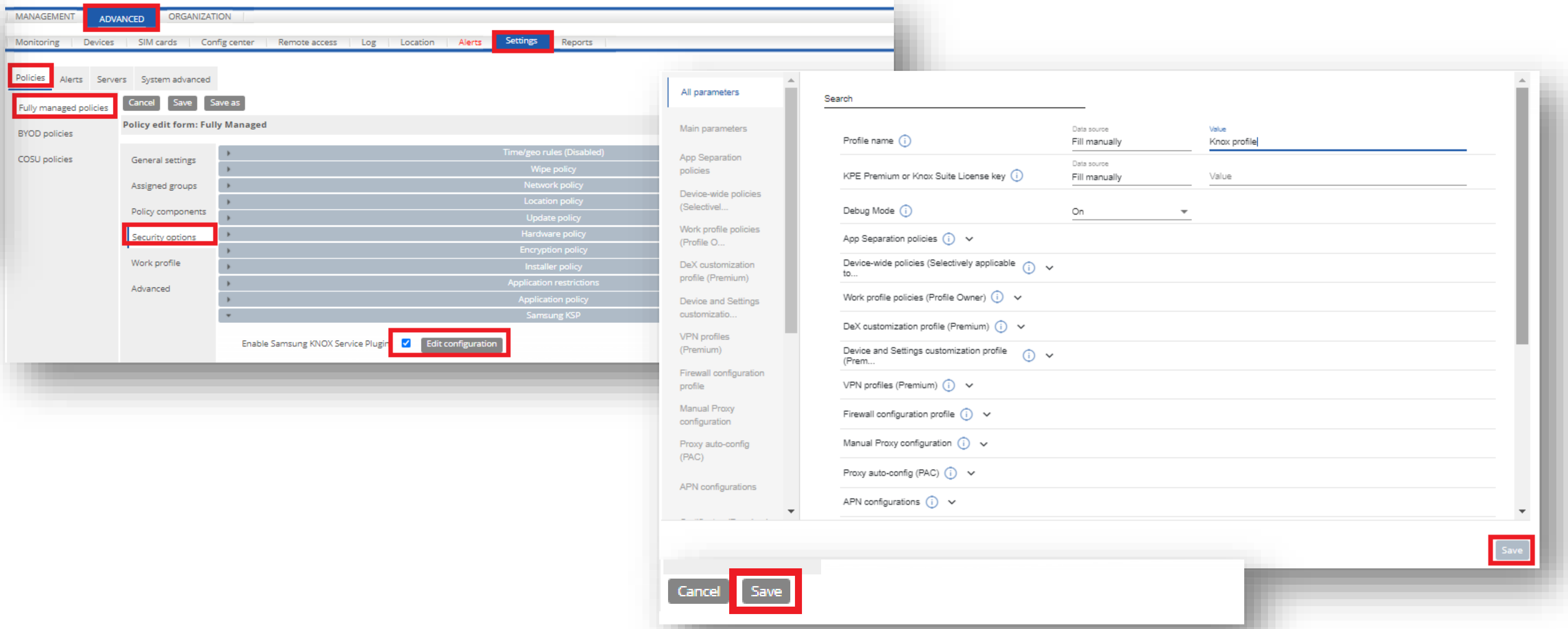
SAMSUNG
Knox Platform for Enterprise
Android Enterprise

Configure Knox Platform for Enterprise using Knox Service Plugin

When you bind your work Managed Google Play account to the FAMOC console, this will automatically pre-approve the Knox Service Plugin app.

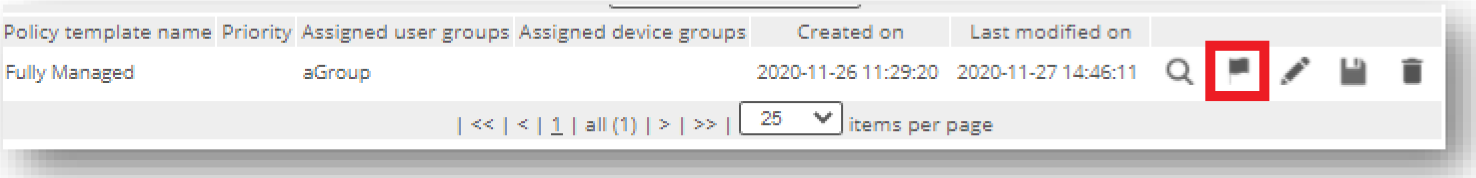
- Navigate to: Advanced > Settings > Policies
- Select the edit button on your desired policy
- In the Security options tab, select Samsung KSP and then tick Enable Samsung Knox Service Plugin
- Select Edit configuration
- You can now make use of the KSP configuration features, once finished, select Save
- Select Save



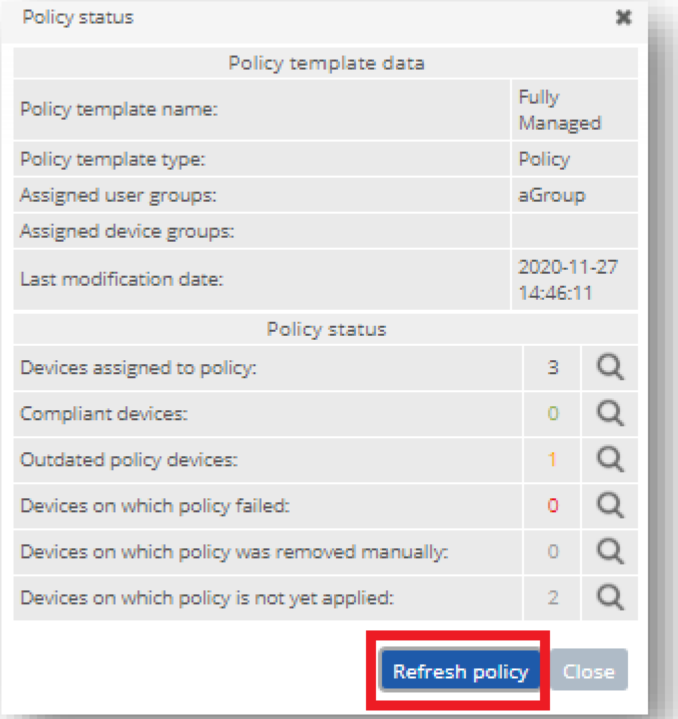


Configure Knox Platform for Enterprise using Knox Service Plugin

- Select the Flag icon next to your policy
- Select Refresh policy



Policy template name	Priority	Assigned user groups	Assigned device groups	Created on	Last modified on
Fully Managed		aGroup		2020-11-26 11:29:20	2020-11-27 14:46:11



Policy status

Policy template data	
Policy template name:	Fully Managed
Policy template type:	Policy
Assigned user groups:	aGroup
Assigned device groups:	
Last modification date:	2020-11-27 14:46:11

Policy status	
Devices assigned to policy:	3
Compliant devices:	0
Outdated policy devices:	1
Devices on which policy failed:	0
Devices on which policy was removed manually:	0
Devices on which policy is not yet applied:	2

Document Information

This is version 2.0 of this document.

Thank you!

Knox