

FAMOC v 5.19.0

# Knox Platform for Enterprise

July 2021

Samsung R&D Centre UK  
(SRUK)

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)**
  - **Work Profile on a Company Owned Device**
  - **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**

## Contacts:

[sruk.rtam@samsung.com](mailto:sruk.rtam@samsung.com)

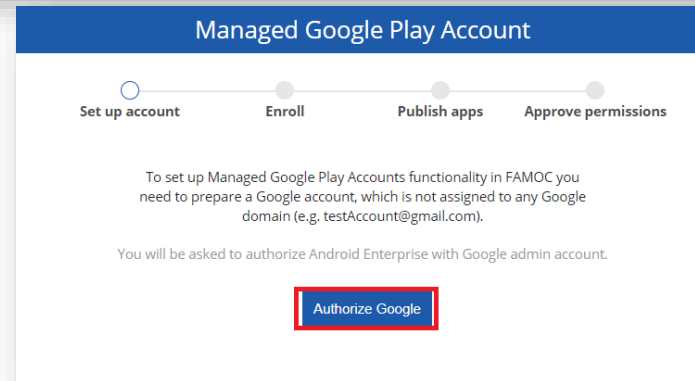
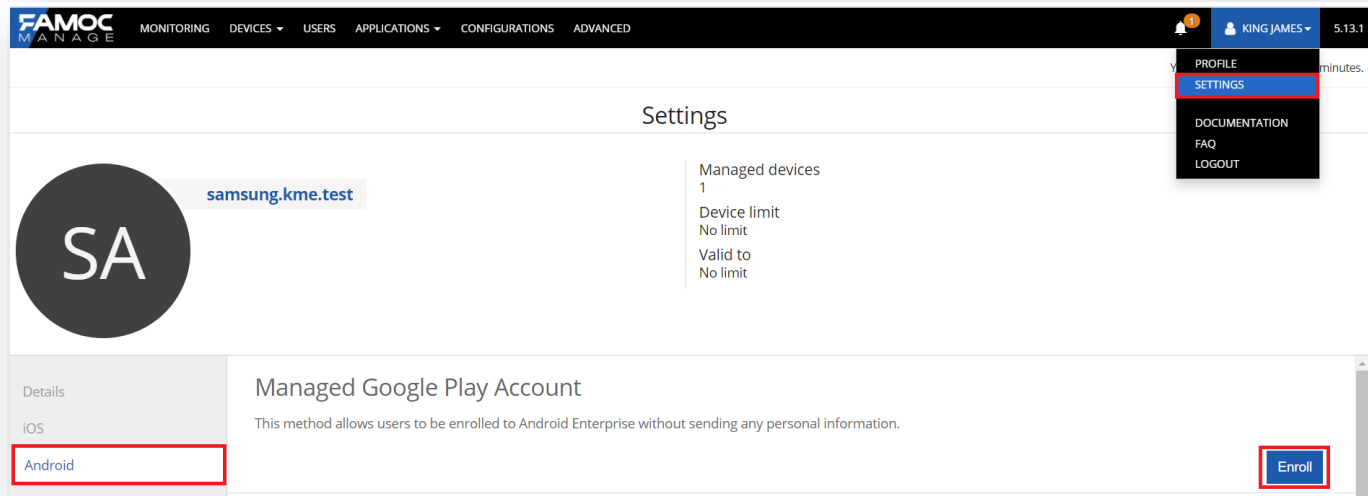
## Knowledge Base:

<https://support.famoc.com>

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**



# 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**

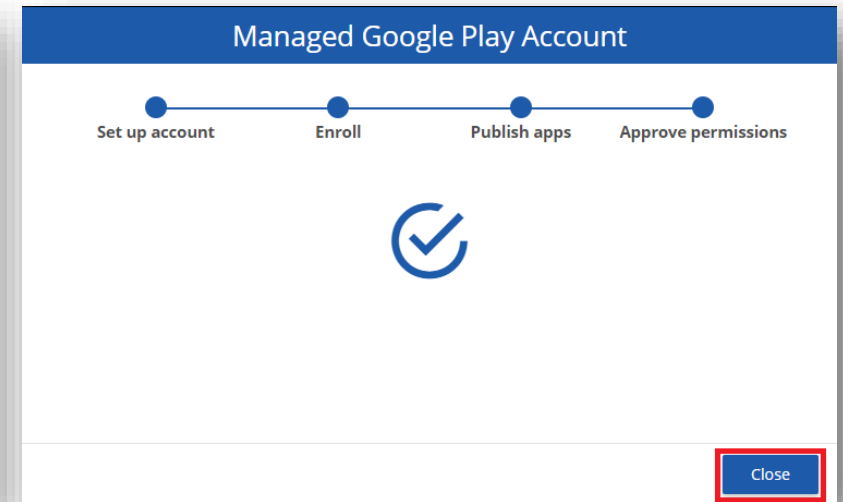
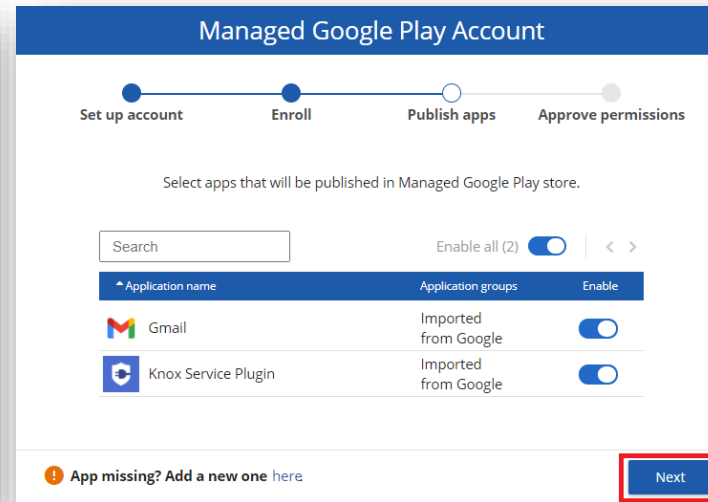
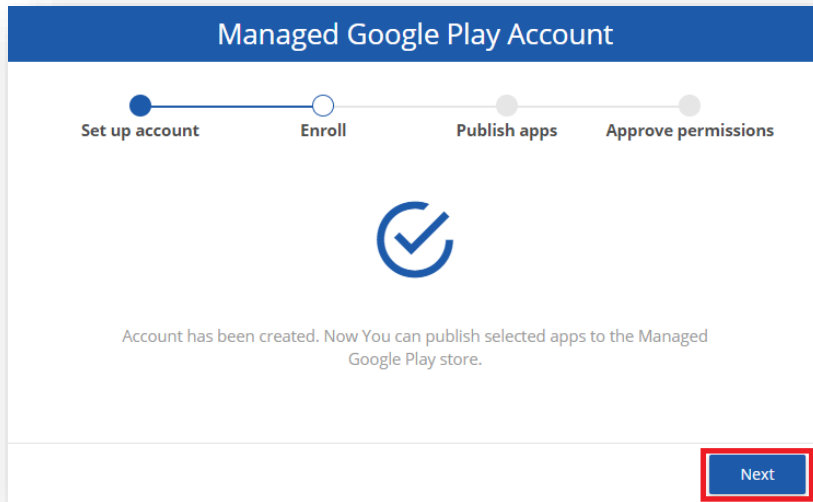
## Set up complete

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**

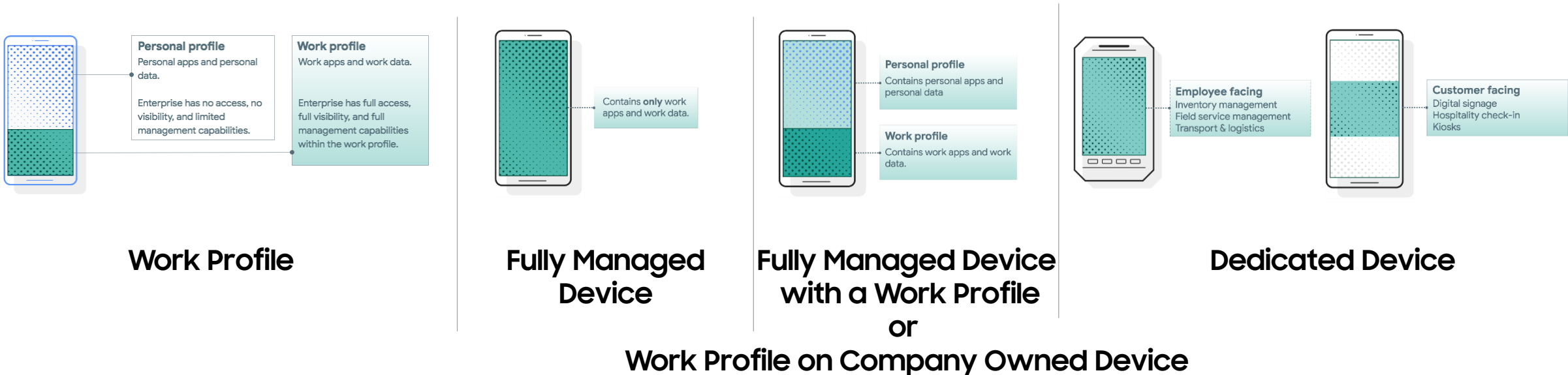


# Android Enterprise Deployment Modes

Android Enterprise can be deployed in the following 4 deployment modes

1. Work Profile [*formerly known as Profile Owner or PO*]
2. Fully Managed Device [*formerly known as Device Owner or DO*]
3. Fully Managed Device with a Work Profile [*formerly known as COMP, up to Android 10*]
4. Work Profile on Company Owned Device [WPC, Android 11 or after]
5. Dedicated Device [*formerly known as COSU*]

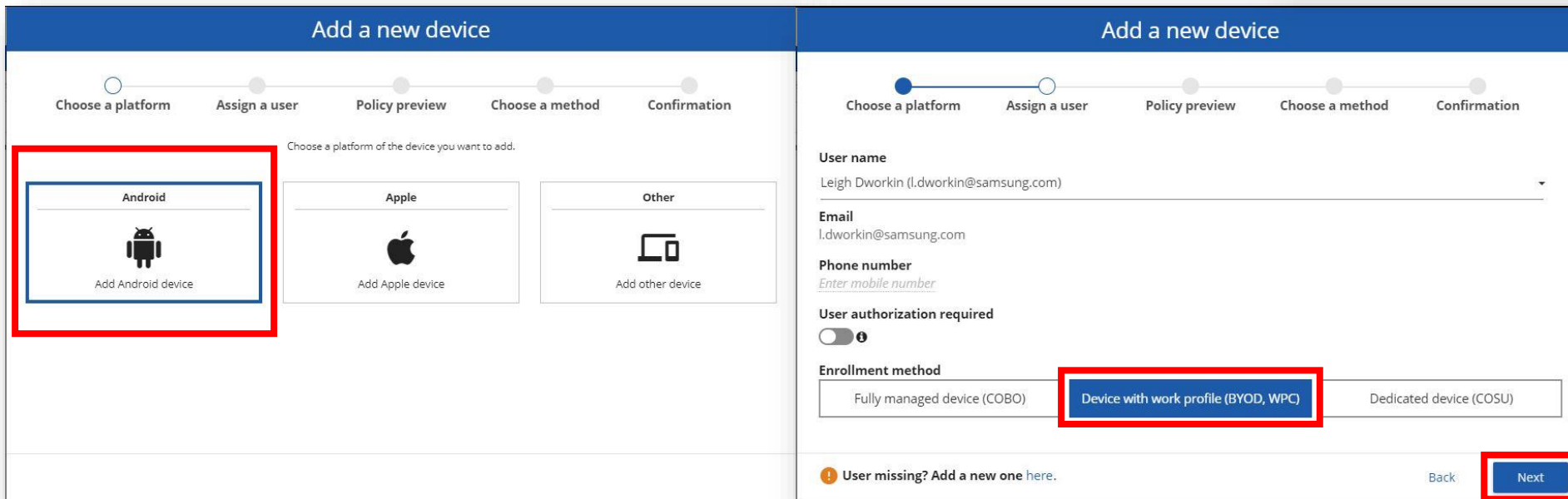
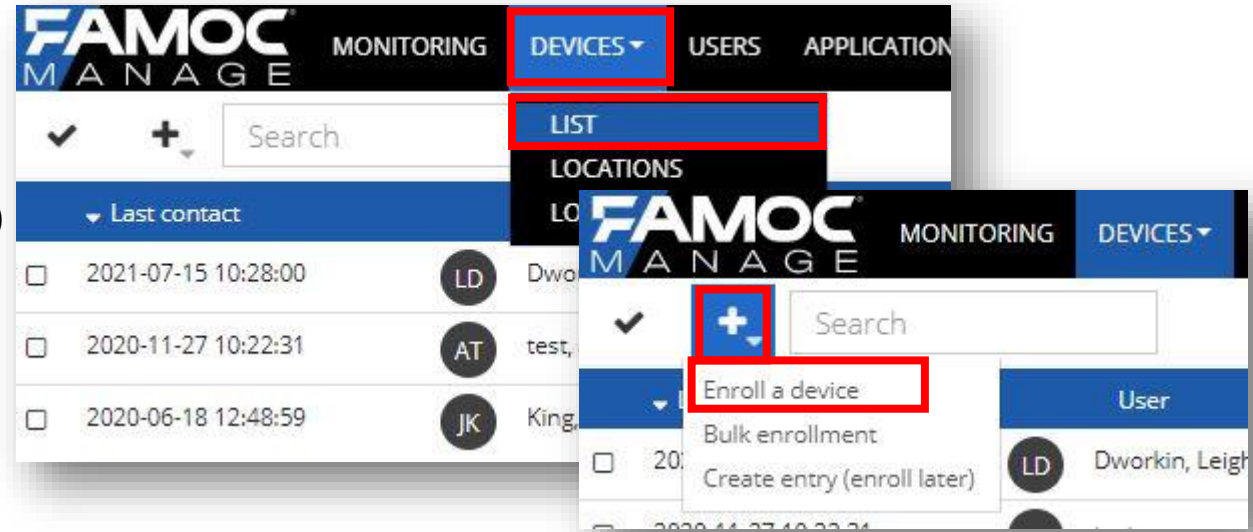
FAMOC can support 4/5 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in FAMOC for your device fleet.





# Work Profile Configuration

- Navigate to: DEVICES > LIST
- Select the + and then Enroll a device
- Select Add Android device
- Select Device with work profile (BYOD, WPC)
- Select Next



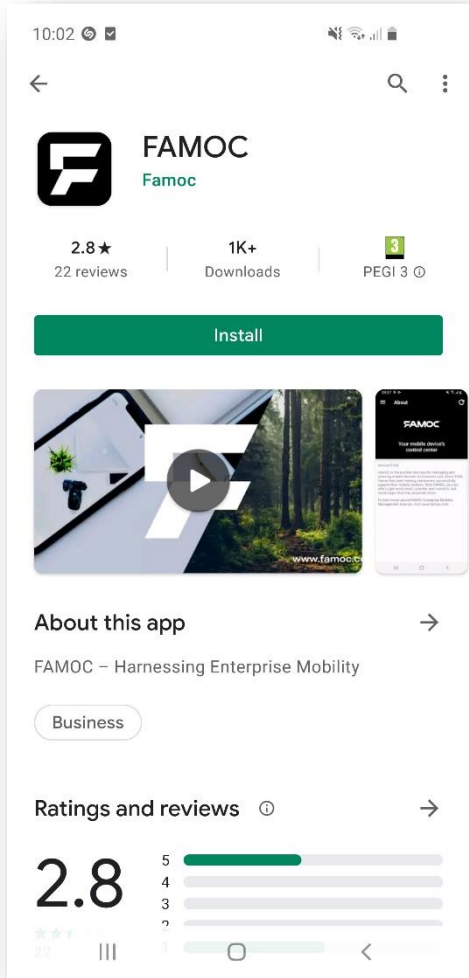
# Work Profile Configuration

- View the BYOD/WPC policy if desired
- Select Next
- Select Private device with work profile (BYOD)
- Optionally send an enrollment link to your email address
- A QR code is presented which will be used in the device enrollment

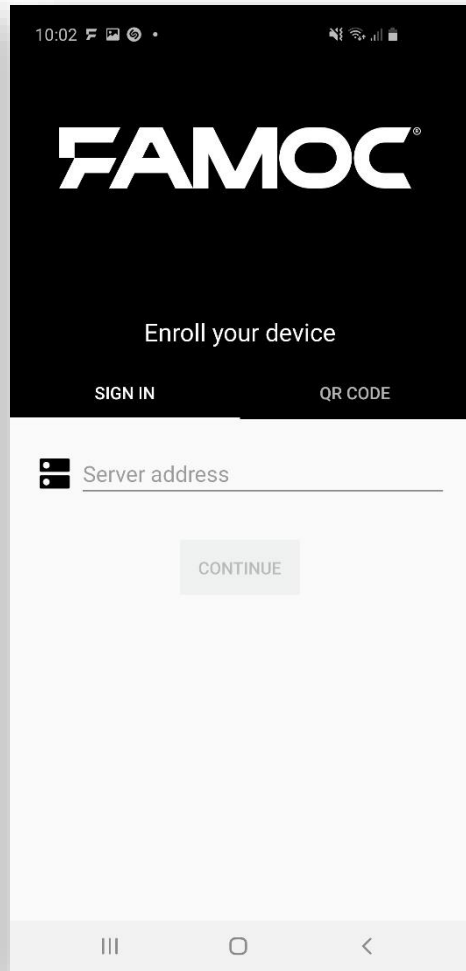
The image displays three sequential screenshots of the 'Add a new device' configuration process:

- First Screenshot:** Shows the 'Policy preview' step. A red dashed box highlights the text: 'View the BYOD/WPC policy assigned to your device'. Below this, it shows 'Policy: Default BYOD/WPC policy' and a list of security settings.
- Second Screenshot:** Shows the 'Choose a method' step. Two options are presented: 'Corporate-owned device with work profile (WPC)' and 'Private device with work profile (BYOD)'. The 'Private device with work profile (BYOD)' option is highlighted with a red box. Below it, requirements for BYOD mode are listed: 'Running Android 10.0+', 'New/factory reset', and 'Connected to the charger'.
- Third Screenshot:** Shows the 'Choose a method' step with two sub-options: 'BYOD mode - send enrollment link' and 'BYOD mode - scan QR code'. The 'send enrollment link' option is highlighted with a red dashed box, showing an email address 'l.dworkin@samsung.com' and a 'Send' button. The 'scan QR code' option shows a QR code with a red box around it and 'Copy link' and 'Refresh' options.

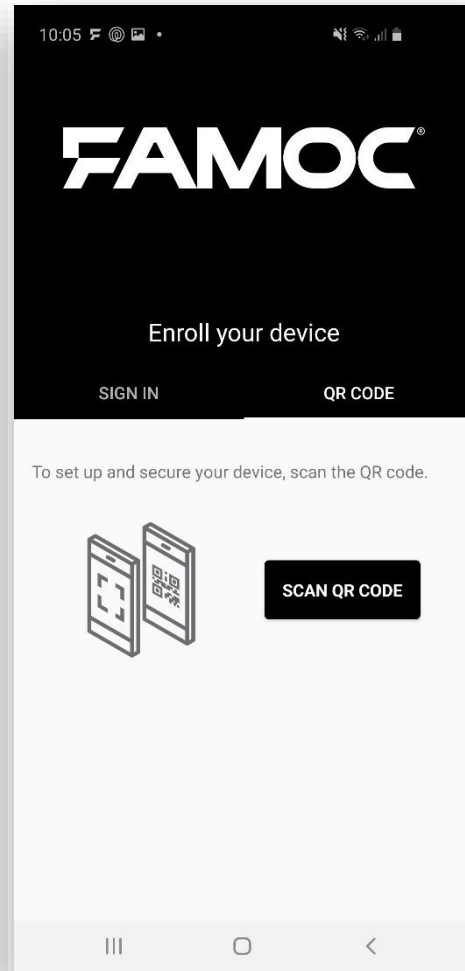
# Android Enterprise: Work Profile Enrollment



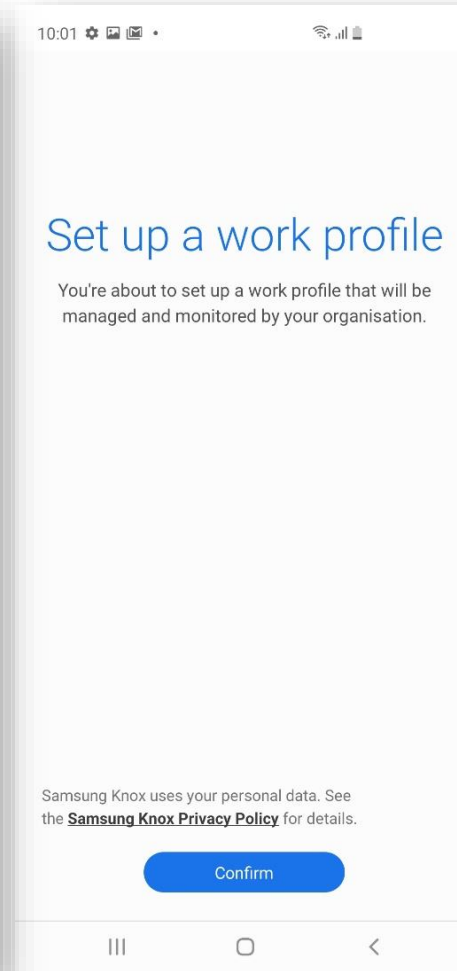
**Install FAMOC**  
From the Google Play Store



**Select QR CODE**



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



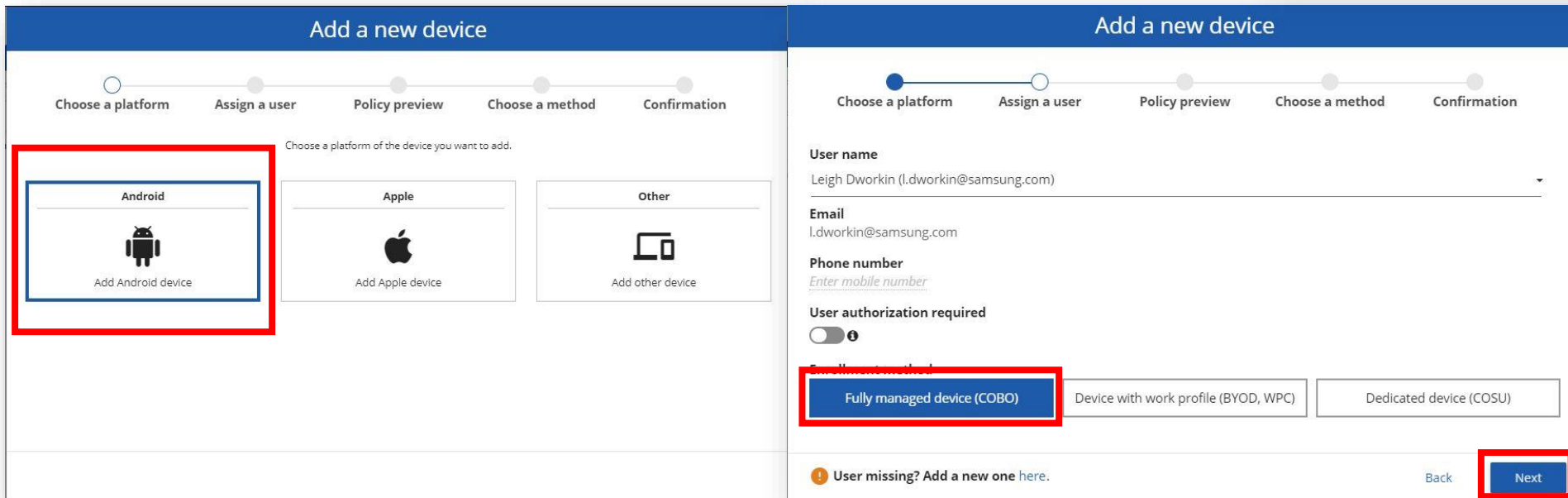
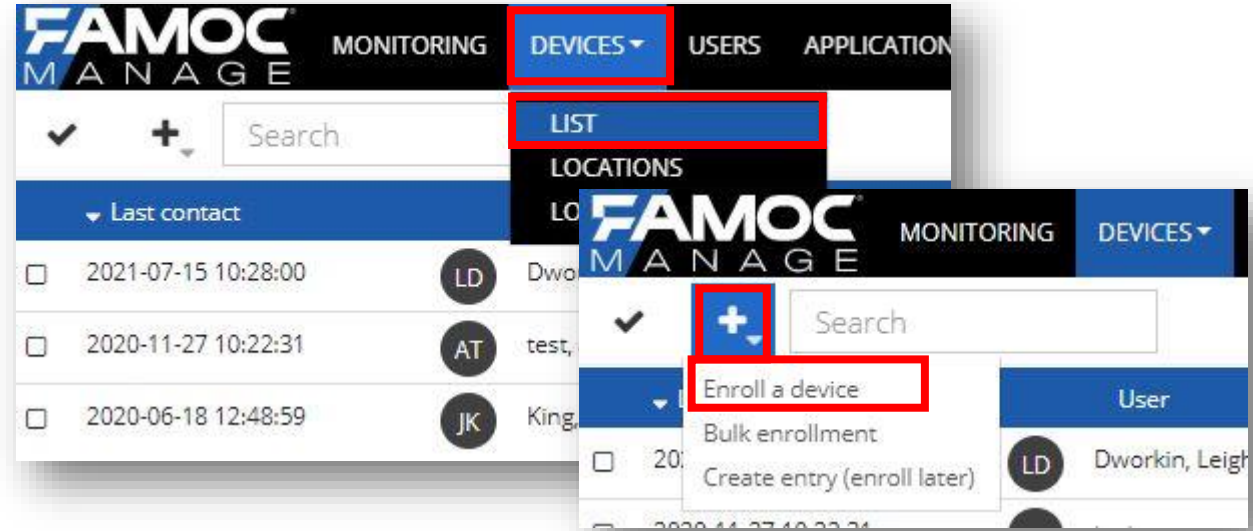
**Confirm**



**Device is now enrolled**

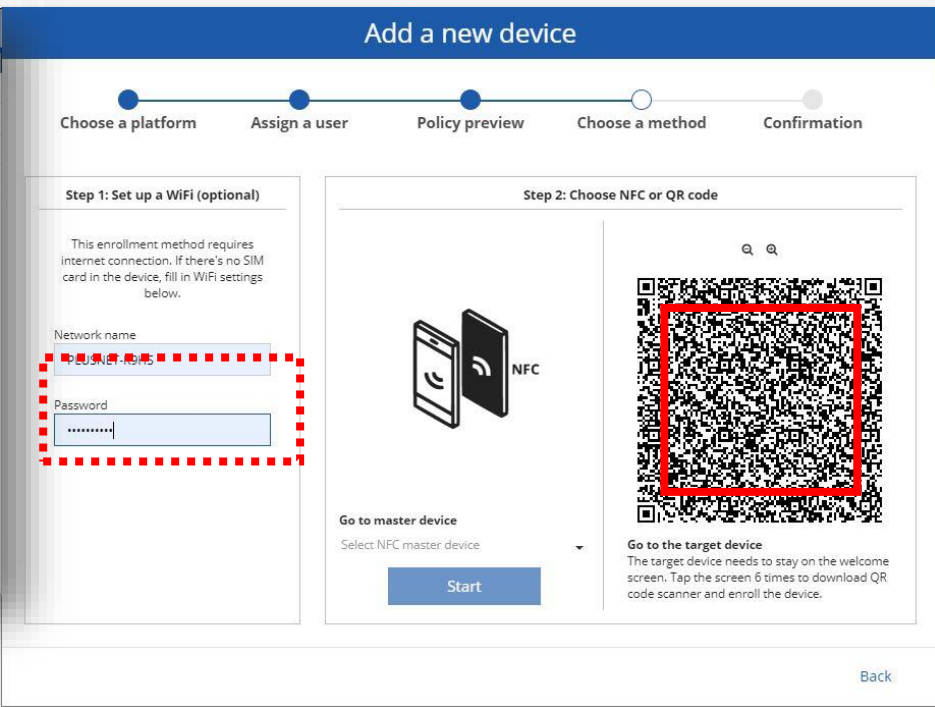
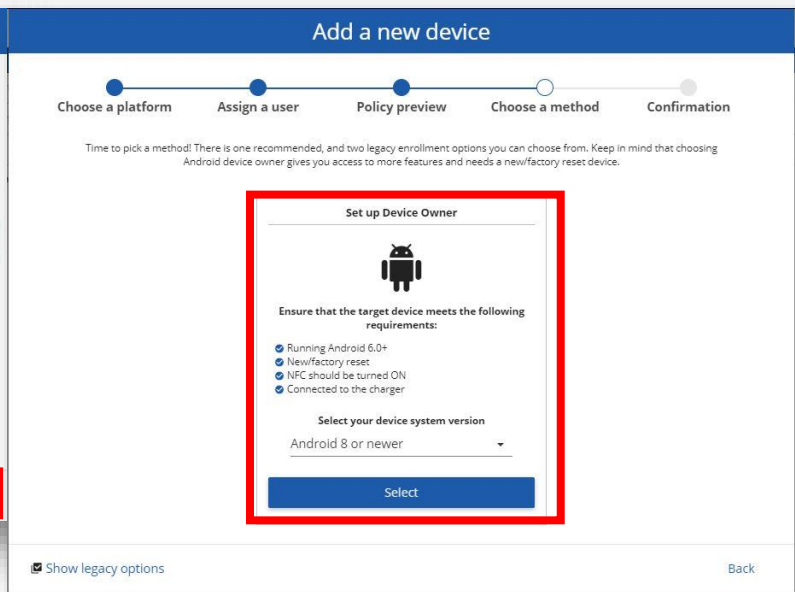
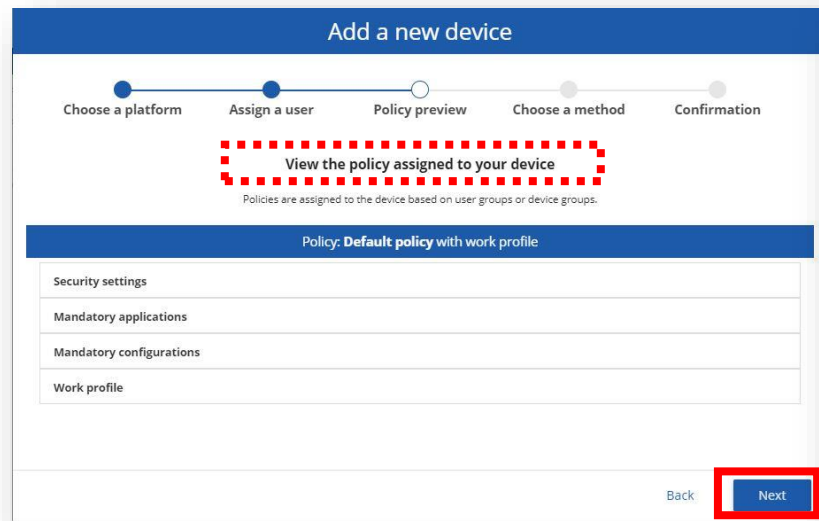
# Fully Managed Device Configuration

- Navigate to: DEVICES > LIST
- Select the + and then Enroll a device
- Select Add Android device
- Select Fully managed device (COBO)
- Select Next



# Fully Managed Device Configuration

- View the policy assigned if desired
- Select Next
- Select your device system version and click Select
- Optionally enter WiFi credentials
- A QR code is presented which will be used in the device enrollment



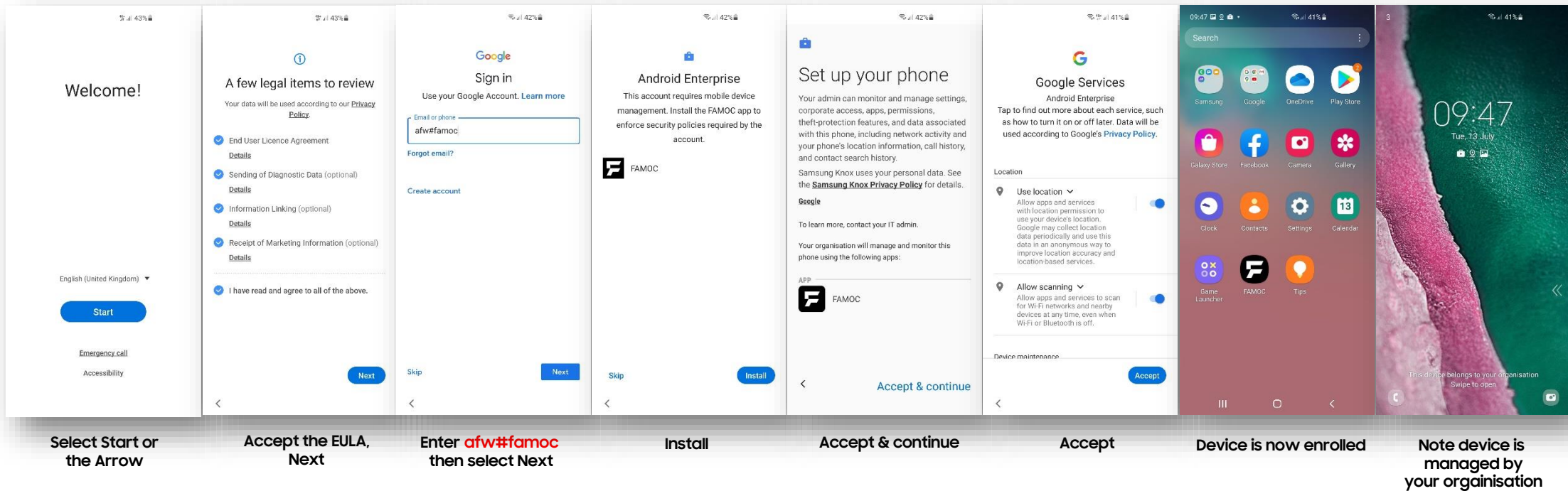
# Android Enterprise: Fully Managed Device Enrollment (hashtag)

## 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 Start or the Arrow

Accept the EULA, Next

Enter **afw#famoc** then select Next

Install

Accept & continue

Accept

Device is now enrolled

Note device is managed by your organisation

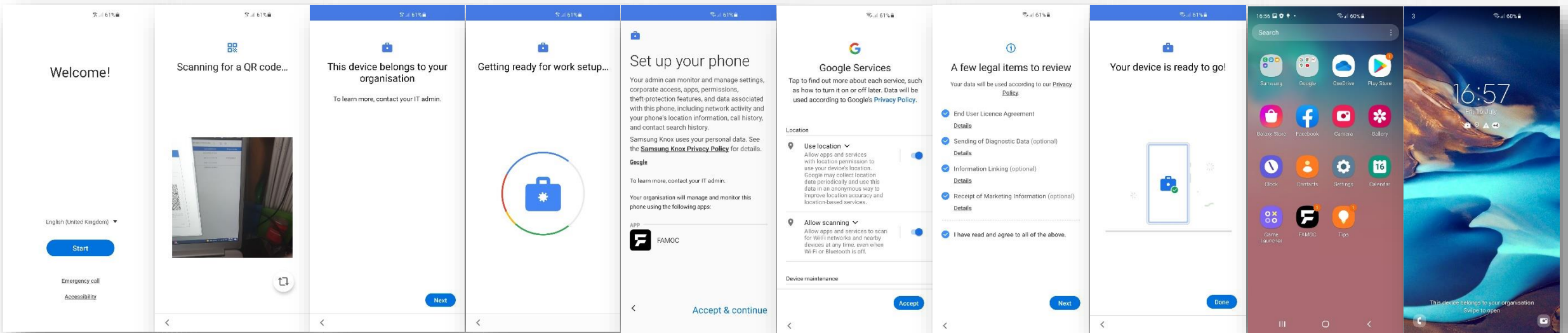
# Android Enterprise: Fully Managed Device Enrollment (QR code)

## 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 QR Code method.



Tap first screen 6 times    Scan the QR code Generated in console    Next    Accept and continue    Accept    Accept T&Cs then Next    Done    Device is now enrolled    Note device is managed by your organisation

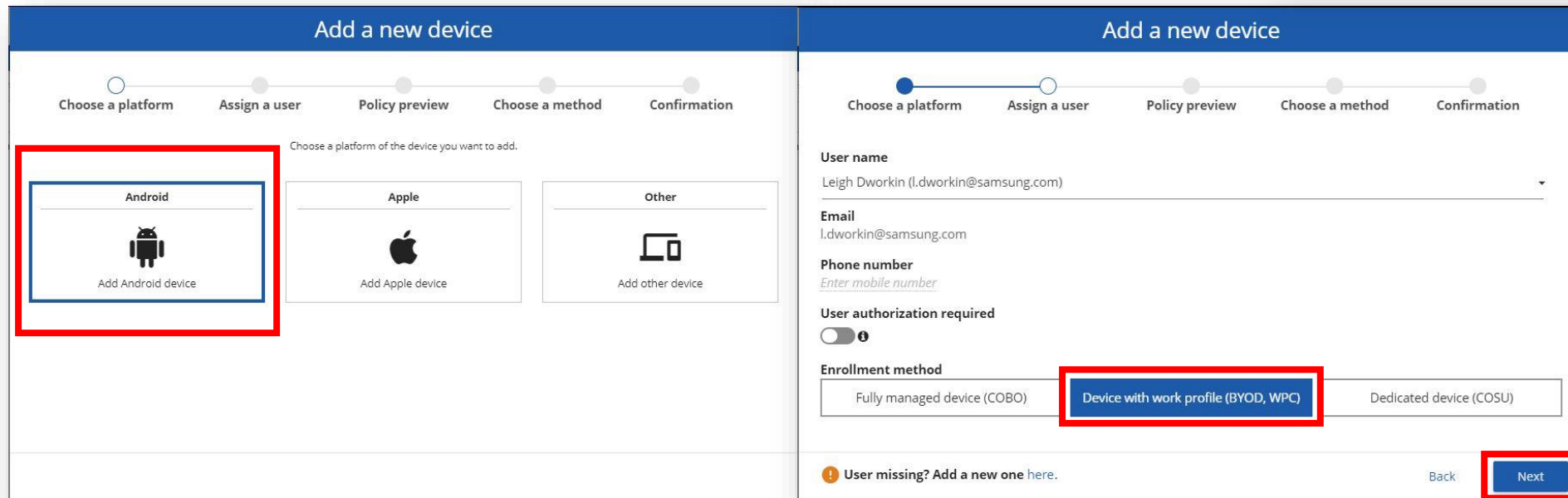
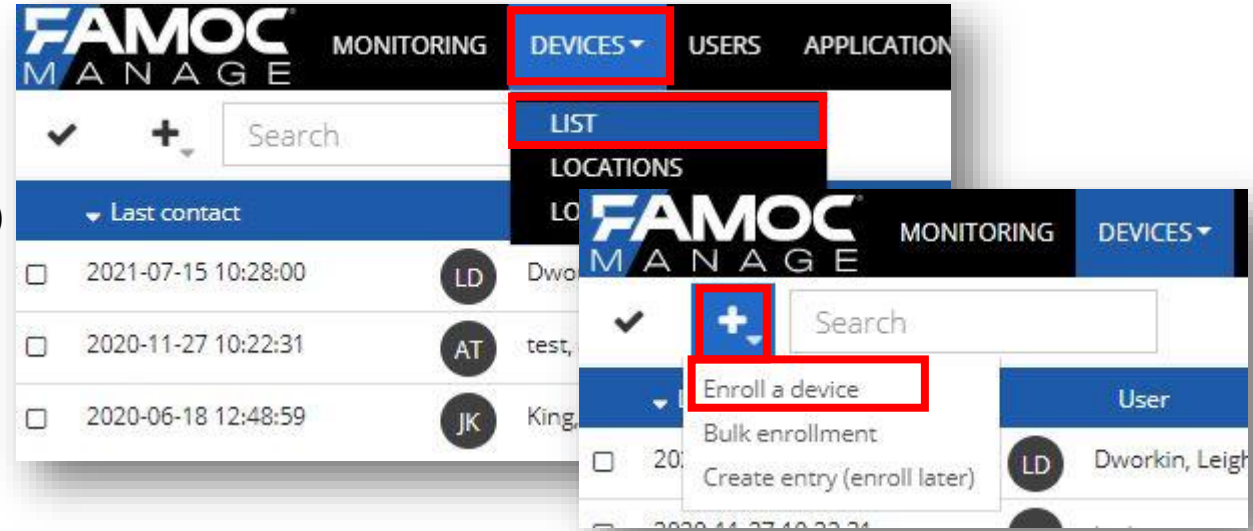
# Fully Managed Device with a Work Profile Configuration

- **This was supported on FAMOC 5.13.1**
- **It is not supported on FAMOC 5.19.0 even on Android devices before 11.0**



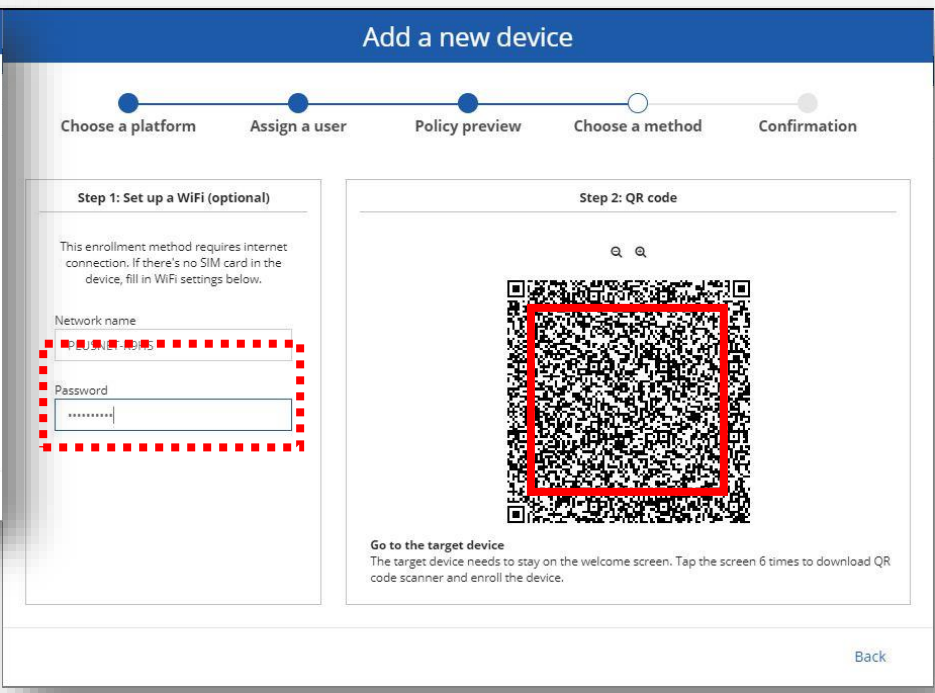
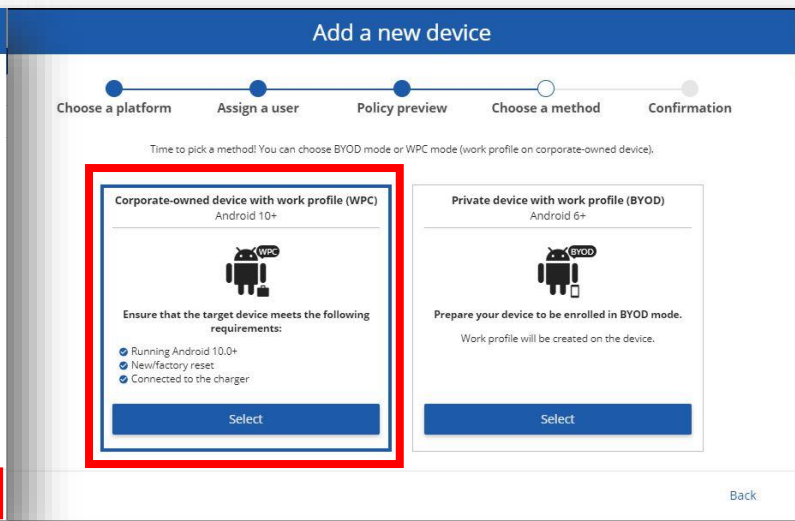
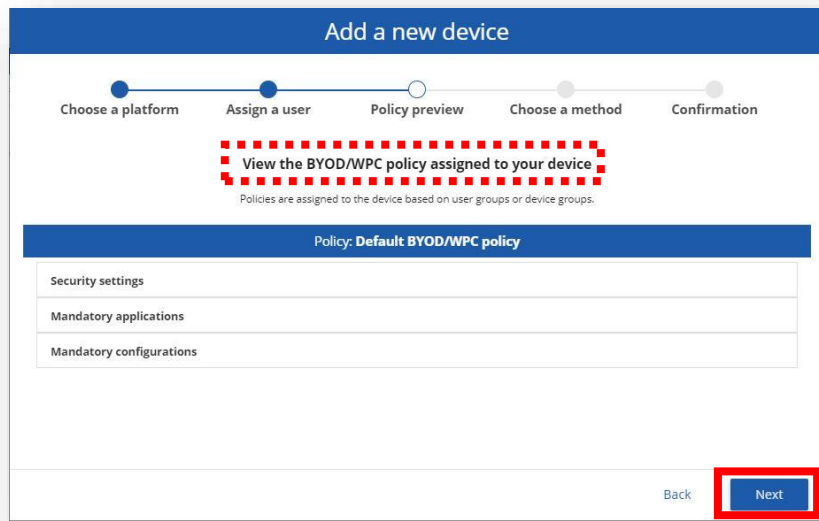
# Work Profile on Company Owned Device (WPC) Configuration

- Navigate to: DEVICES > LIST
- Select the + and then Enroll a device
- Select Add Android device
- Select Device with work profile (BYOD, WPC)
- Select Next



# Work Profile on Company Owned Device (WPC) Configuration

- View the BYOD/WPC policy if desired
- Select Next
- Select Corporate-owned device with work profile (WPC)
- Optionally enter WiFi credentials
- A QR code is presented which will be used in the device enrollment



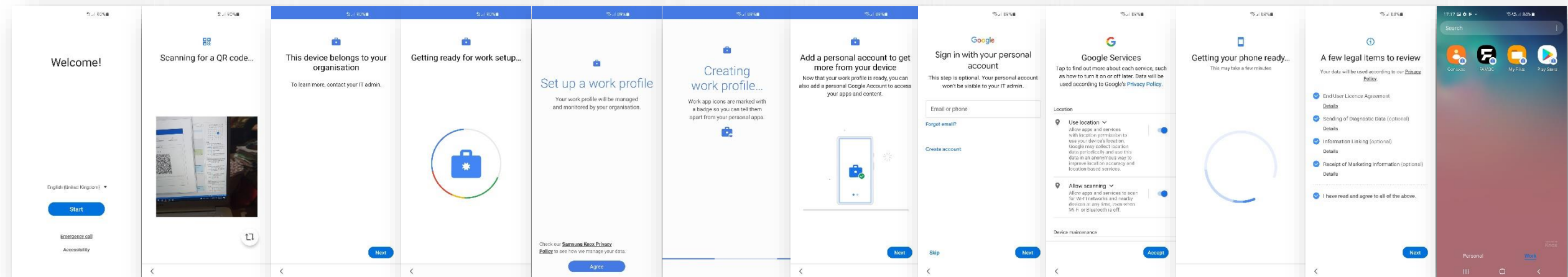
# Android Enterprise: Work Profile on Company Owned Device Enrollment

## Android Enterprise Work Profile on Company Owned Device Deployment

To enroll your device as an Android Enterprise Work Profile on Company Owned Device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 2 ways you can enroll your device into FAMOC as an Android Enterprise Work Profile on Company Owned Device.

1. QR Code Enrollment / NFC Enrollment
2. Knox Mobile Enrollment

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



Tap 6 times on the Welcome screen

Scan the QR code

Note device ownership then select Next

Agree to Set up work profile

Select Next

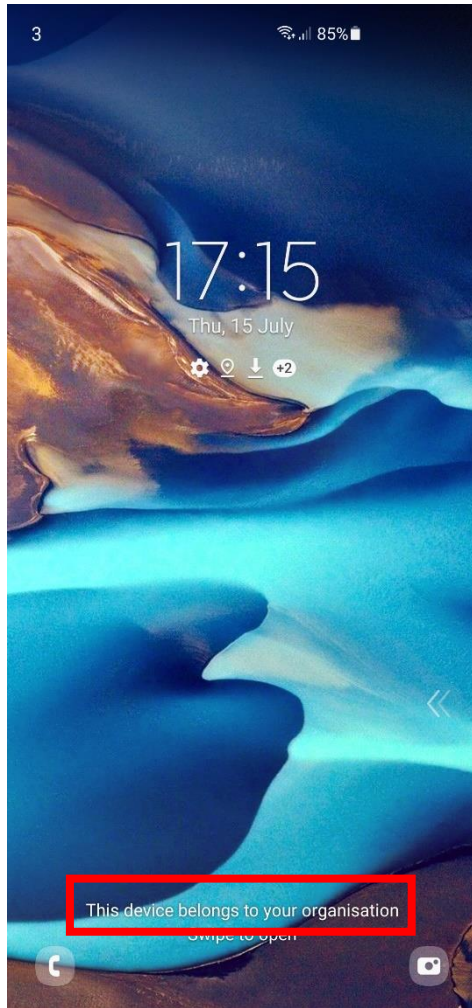
Optionally select a personal Google account then select Next

Choose Google Services then Accept

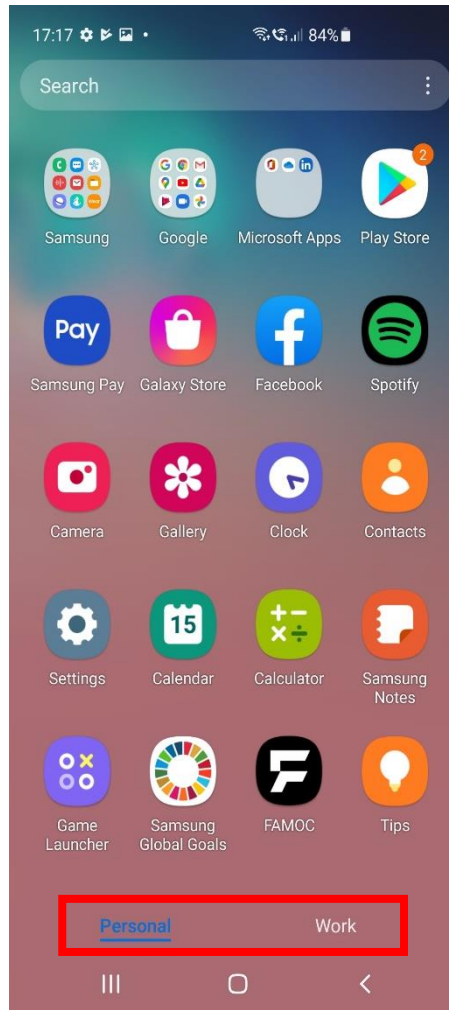
Accept the legal terms, then select Next

Device is now enrolled

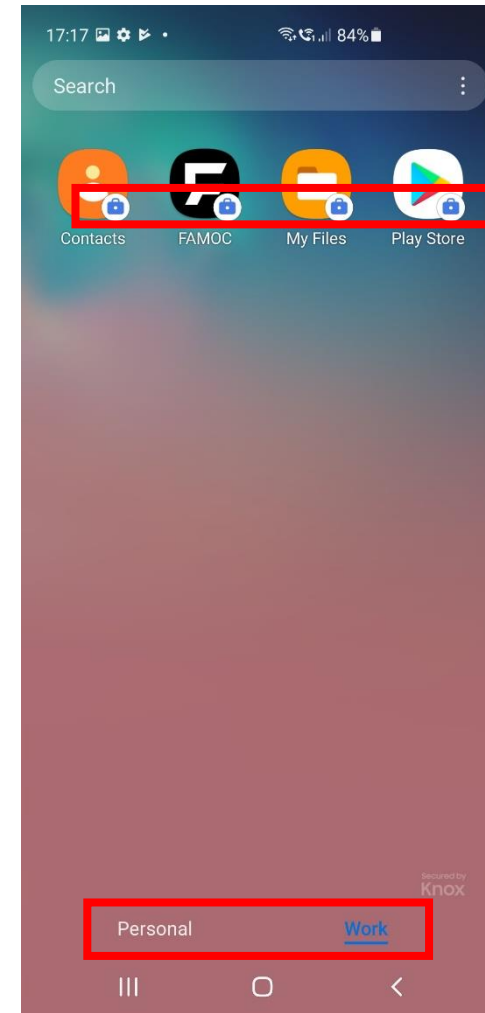
# Android Enterprise: Work Profile on Company Owned Device Proof



This device belongs to your organization on Lock Screen



Personal Tab

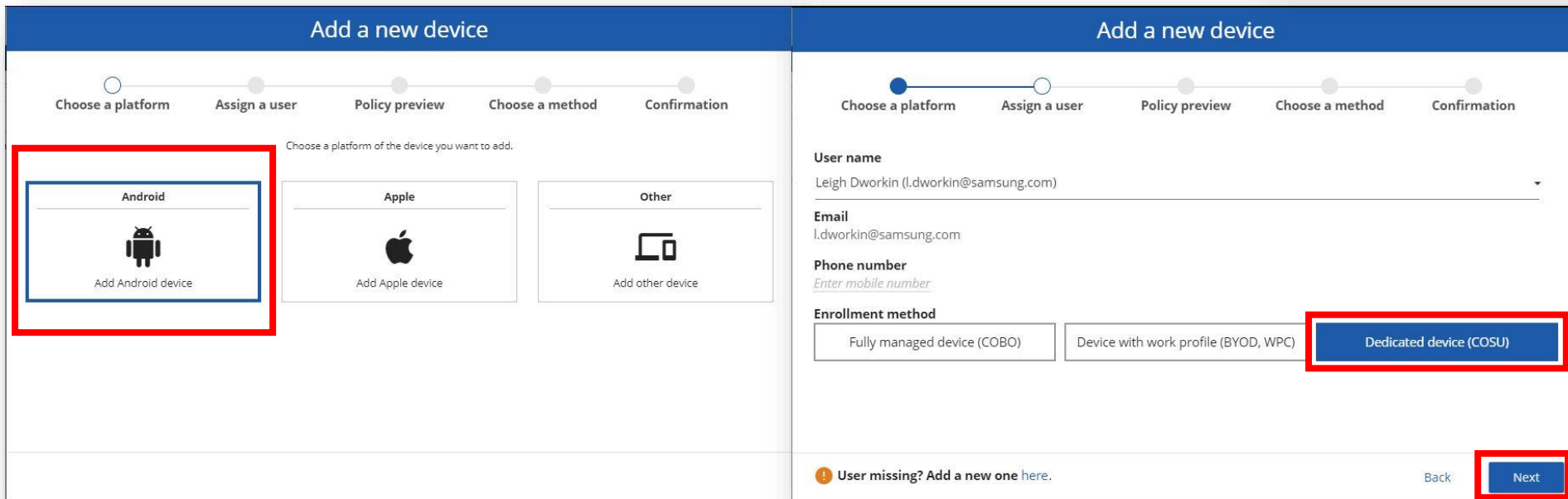
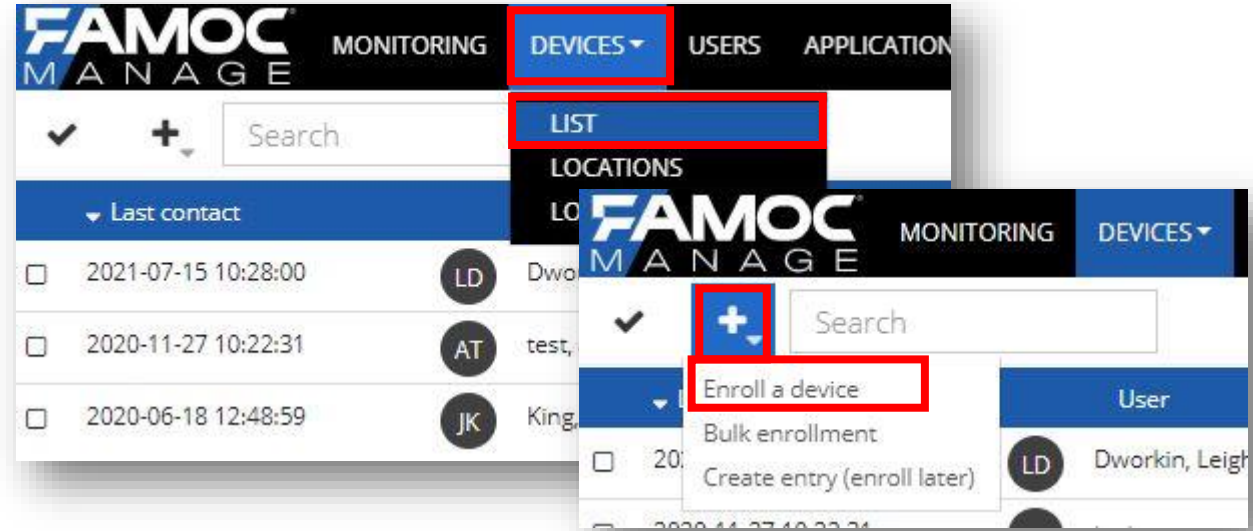


Work Tab

Badged icons in Work Profile

# Dedicated Device (COSU) Configuration

- Navigate to: DEVICES > LIST
- Select the + and then Enroll a device
- Select Add Android device
- Select Dedicated Device (COSU)
- Select Next



# Dedicated Device (COSU) Configuration

- View the COSU policy if desired
- Select Next
- Select Set up Device Owner
- Optionally enter WiFi credentials
- A QR code is presented which will be used in the device enrollment

The image displays three sequential screenshots of the 'Add a new device' configuration process:

- First Screenshot:** Shows the 'Policy preview' step. A red dashed box highlights the text 'View the COSU policy assigned to your device'. Below this, a table lists settings: Security settings, Mandatory applications, Mandatory configurations, and COSU mode settings. The 'Next' button at the bottom right is highlighted with a red box.
- Second Screenshot:** Shows the 'Set up Device Owner' step. A red box highlights the entire 'Set up Device Owner' section, which includes an Android icon, a list of requirements (Running Android 8.0+, New/factory reset, NFC should be turned ON, Connected to the charger), and a 'Select' button.
- Third Screenshot:** Shows the 'Choose a method' step. It is divided into two sections: 'Step 1: Set up a WiFi (optional)' with fields for Network name and Password (both highlighted with red dashed boxes), and 'Step 2: Choose NFC or QR code'. The QR code is highlighted with a red box. A 'Start' button is visible at the bottom.

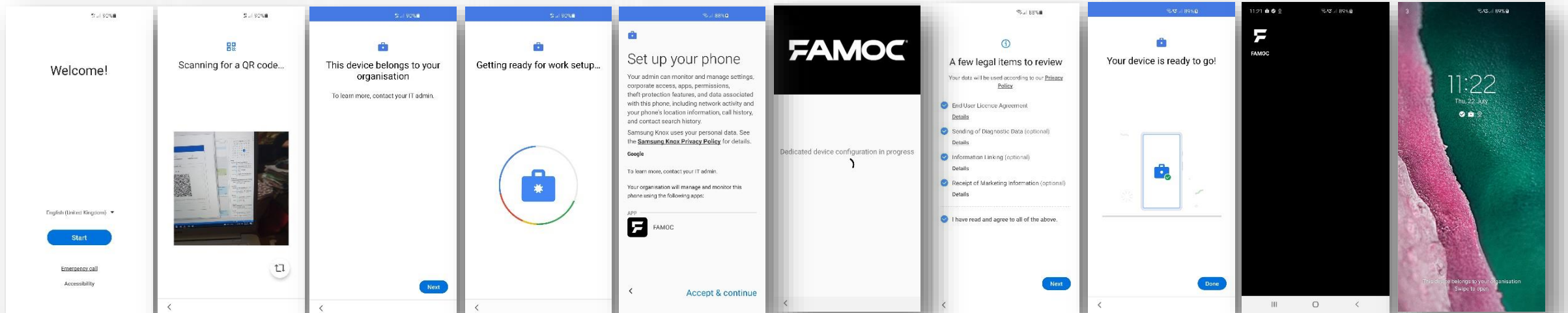
# Dedicated Device (COSU) Enrollment

## Android Enterprise Dedicated Device Deployment

To enroll your device as an Android Enterprise Dedicated Device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 2 ways you can enroll your device into FAMOC as an Android Enterprise Dedicated Device.

1. QR Code Enrollment / NFC Enrollment
2. Knox Mobile Enrollment

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



Tap 6 times on the Welcome screen

Scan the QR code

Note device ownership then select Next

Accept & continue

Dedicated Device configuration in progress

Accept the legal terms, then select Next

Ready to go! Select Done

Device is now enrolled & kiosk

Device belongs to Your organisation

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.





# 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

The image displays three sequential screenshots from the FAMOC console interface, illustrating the steps to configure the Samsung Knox Service Plugin. Red boxes highlight key UI elements.

- First Screenshot:** Shows the 'ADVANCED' settings page. The 'Policies' tab is selected, and the 'Settings' menu item is highlighted. A table lists 'Fully managed policies' and 'COSU policies', with an 'Edit' button highlighted for the 'Default COSU policy'.
- Second Screenshot:** Shows the 'Policy edit form: Fully Managed' page. The 'Security options' section is expanded, and the 'Samsung KSP' option is selected. The 'Enable Samsung KNOX Service Plugin' checkbox is checked, and the 'Edit configuration' button is highlighted.
- Third Screenshot:** Shows the configuration details for the Samsung KSP. The 'Profile name' is set to 'Knox profile'. The 'Debug Mode' is set to 'On'. A 'Save' button is highlighted at the bottom right.

# 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	   







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

### 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	

[Refresh policy](#) [Close](#)

**This is version 2.1 of this document.**

**Thank you!**

