

FAMOC v 5.13.1

Knox Platform for Enterprise

December 2020
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
 - 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

Knowledge Base:

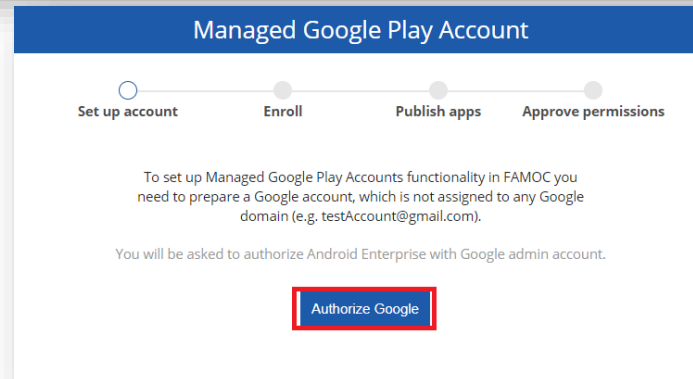
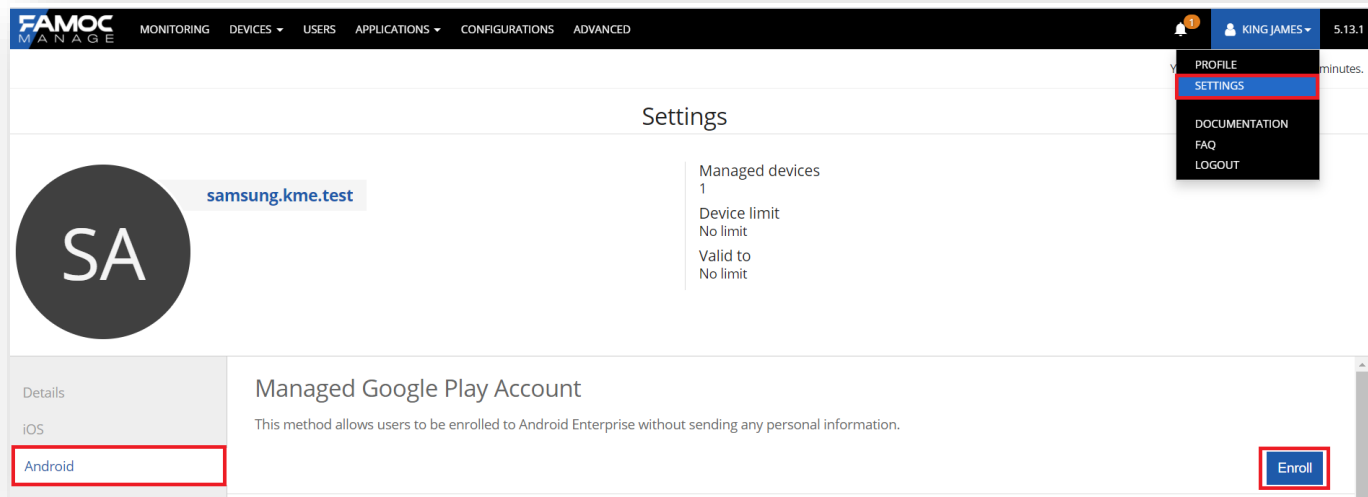
<https://support.famoc.com>

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



Configure Android Enterprise

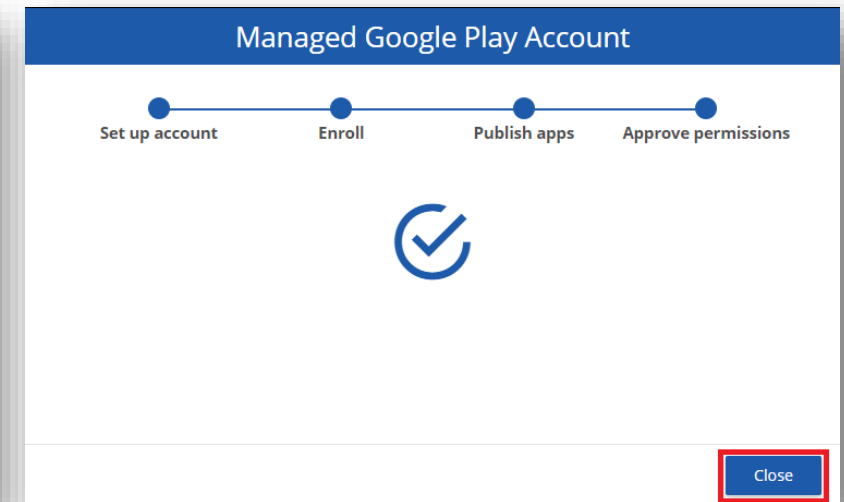
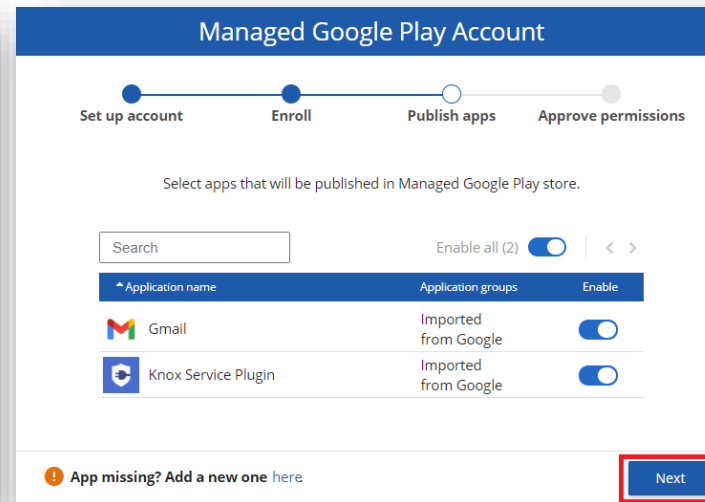
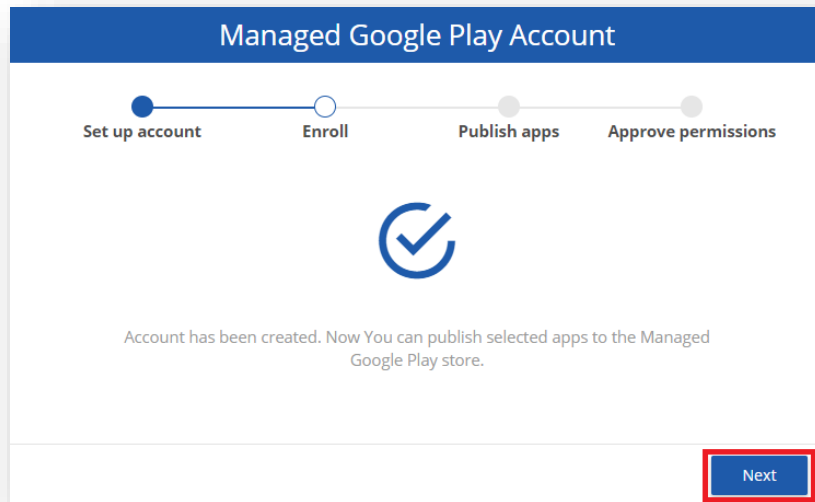
- Sign in with your Google Account and select Get Started
- Enter a Business name, select Next
- Data Protection Officer and EU Representative are optional, select Confirm
- Select Complete Registration

The image displays a sequence of four screenshots from the Android Enterprise setup process, with key buttons highlighted by red boxes:

- Screen 1: Bring Android to Work**
The 'Get started' button is highlighted.
- Screen 2: Business name**
The 'Next' button is highlighted.
- Screen 3: Data Protection Officer and EU Representative**
The 'Confirm' button is highlighted.
- Screen 4: Set up complete**
The 'Complete Registration' button is highlighted.

Configure Android Enterprise

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

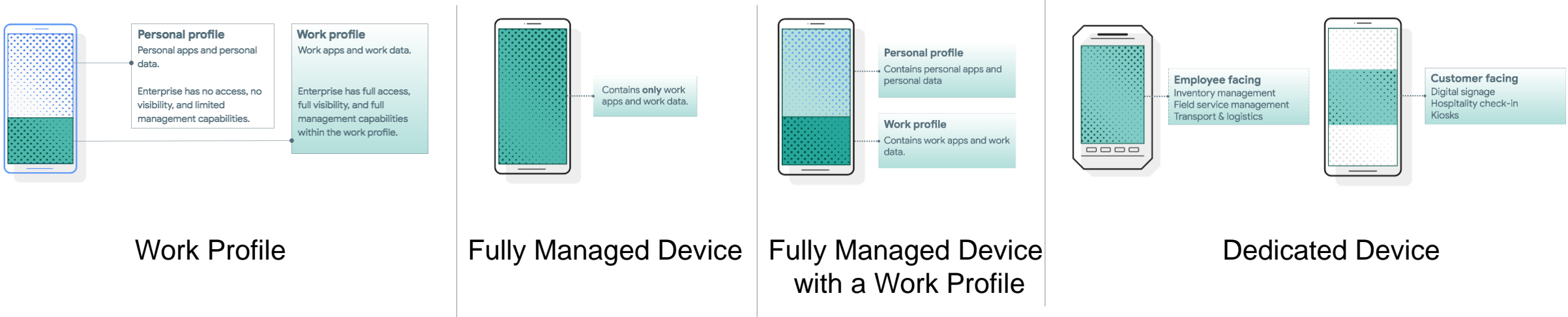


Android Enterprise Deployment Modes

Android Enterprise can be deployed in the following 4 deployment modes

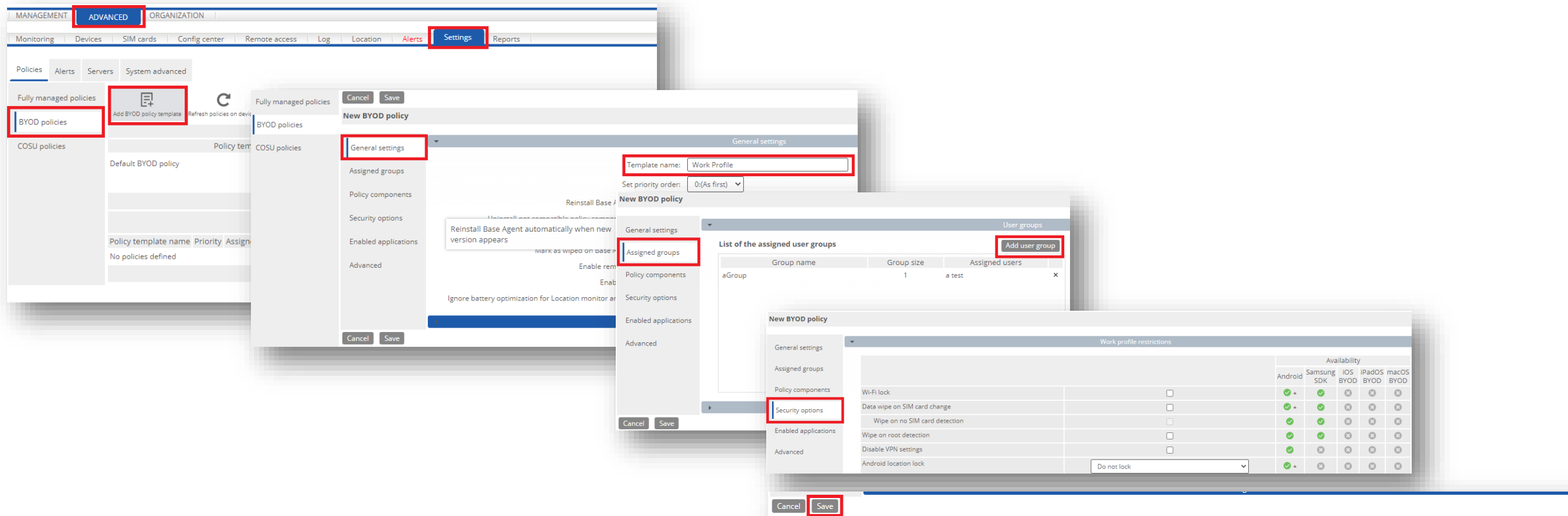
1. Work Profile [*formerly known as Profile Owner*]
2. Fully Managed Device [*formerly known as Device Owner*]
3. Fully Managed Device with a Work Profile [*formerly known as COMP*]
4. Dedicated Device [*formerly known as COSU*]

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.



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

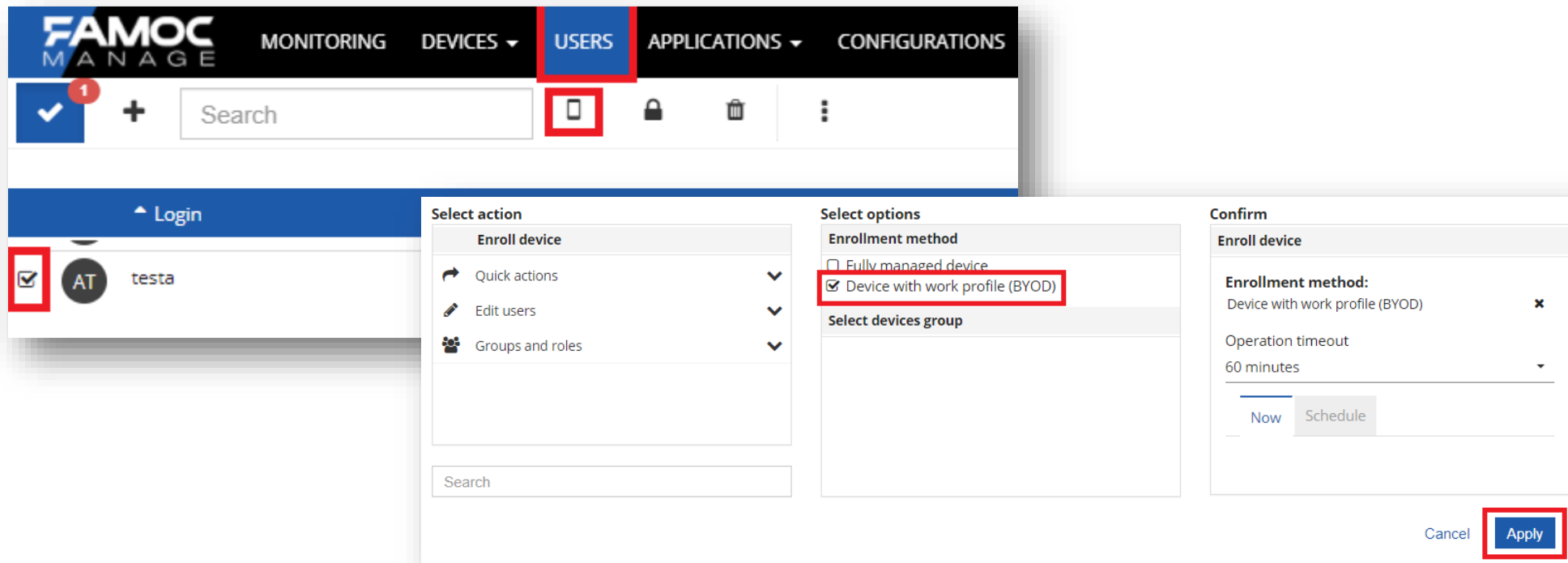


The screenshots illustrate the following steps:

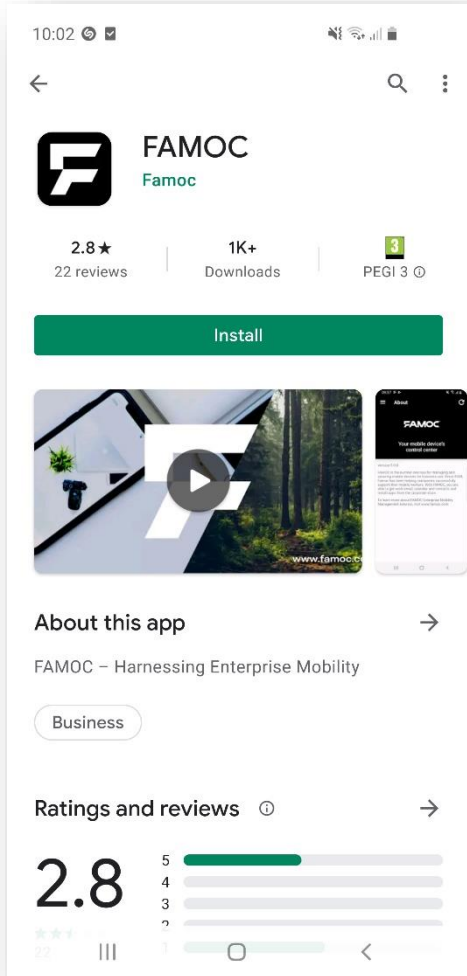
- Navigate to **ADVANCED > Settings**.
- Select **BYOD policies** under the Policies section.
- Click **Add BYOD policy template**.
- In the **General settings** tab, enter the **Template name: Work Profile**.
- In the **Assigned groups** tab, click **Add user group**.
- In the **Security options** tab, select the desired restrictions (e.g., 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).
- Click **Save**.

Work Profile Configuration

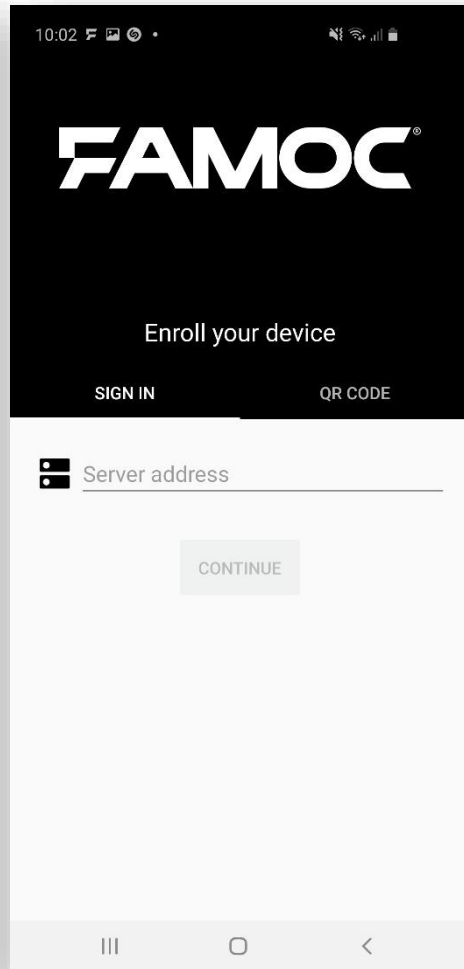
- Navigate to: USERS
- Select the user you wish to enroll
- Select the Enroll Device button (mobile phone icon)
- For Enrollment method, select Device with work profile (BYOD)
- Select Apply, this will now email the end user a QR code which will be used for the device enrollment



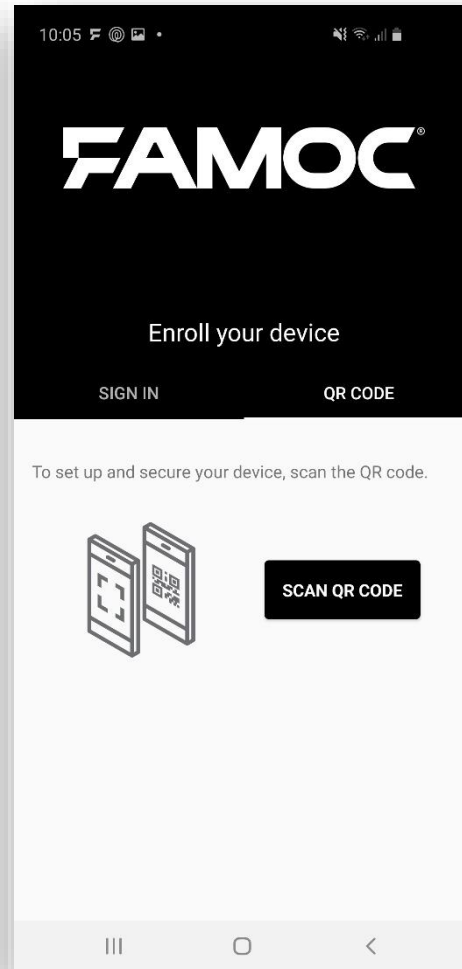
Android Enterprise: Work Profile Enrollment



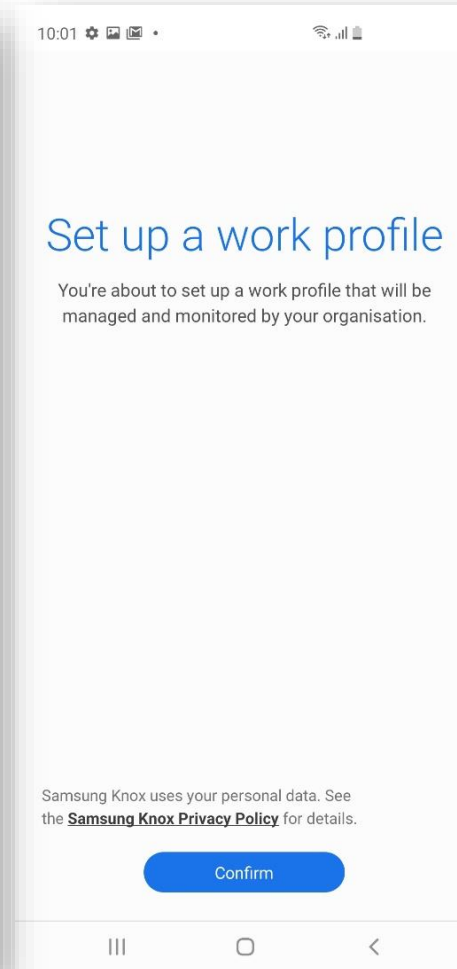
Install FAMOC
From the Google Play Store



Select QR CODE



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



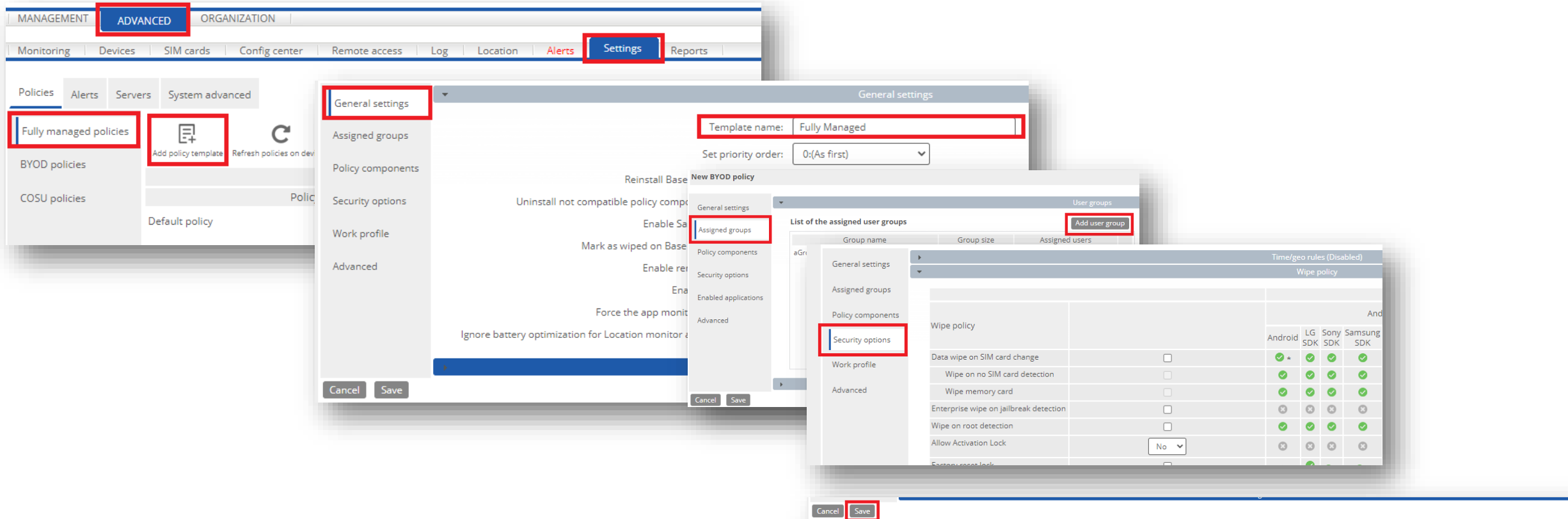
Confirm



Device is now enrolled

Fully Managed Device Configuration

- Navigate to: 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

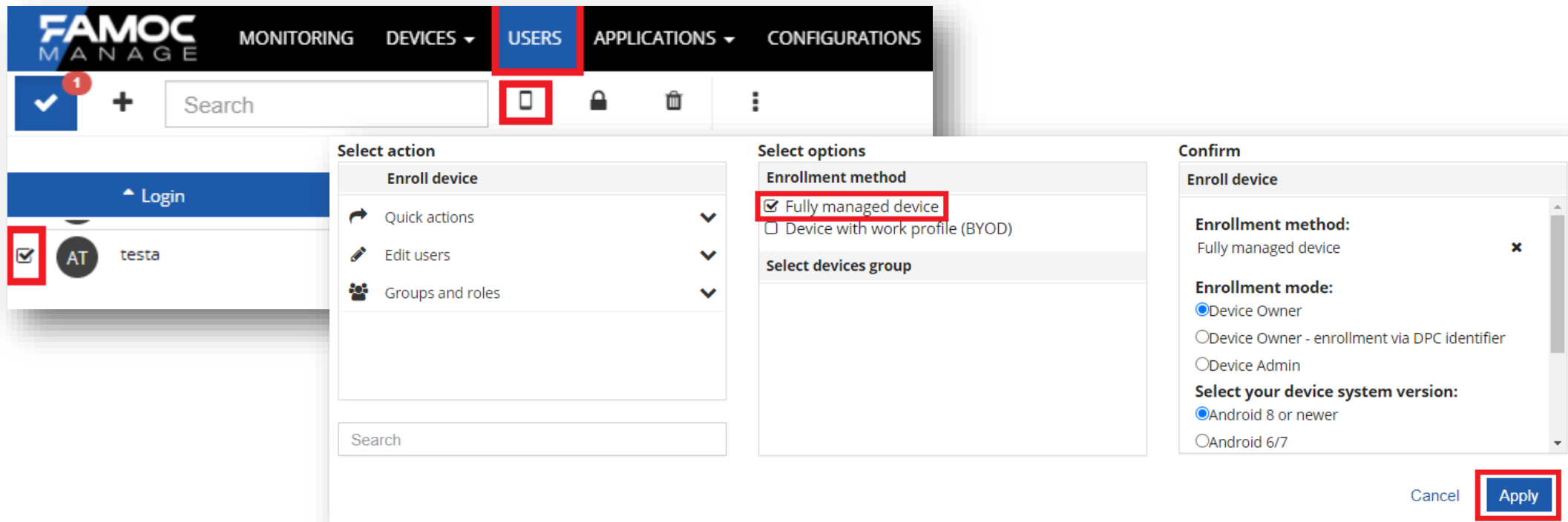


The screenshot illustrates the configuration process for a Fully Managed policy in the Knox interface. The main navigation bar shows 'MANAGEMENT', 'ADVANCED', and 'ORGANIZATION'. The 'ADVANCED' tab is selected, and the 'Settings' sub-tab is active. The left sidebar lists 'Fully managed policies' under the 'Policies' section. The 'Add policy template' button is highlighted. The 'General settings' dialog is open, showing 'Template name: Fully Managed' and 'Set priority order: 0:(As first)'. The 'Assigned groups' dialog is also open, showing 'Add user group' button. The 'Security options' dialog is open, showing a table of security options for different Android versions.

		Android	LG SDK	Sony SDK	Samsung SDK
Wipe policy					
Data wipe on SIM card change	<input type="checkbox"/>	✓ +	✓	✓	✓
Wipe on no SIM card detection	<input type="checkbox"/>	✓	✓	✓	✓
Wipe memory card	<input type="checkbox"/>	✓	✓	✓	✓
Enterprise wipe on jailbreak detection	<input type="checkbox"/>	✗	✗	✗	✗
Wipe on root detection	<input type="checkbox"/>	✓	✓	✓	✓
Allow Activation Lock	No	✗	✗	✗	✗

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



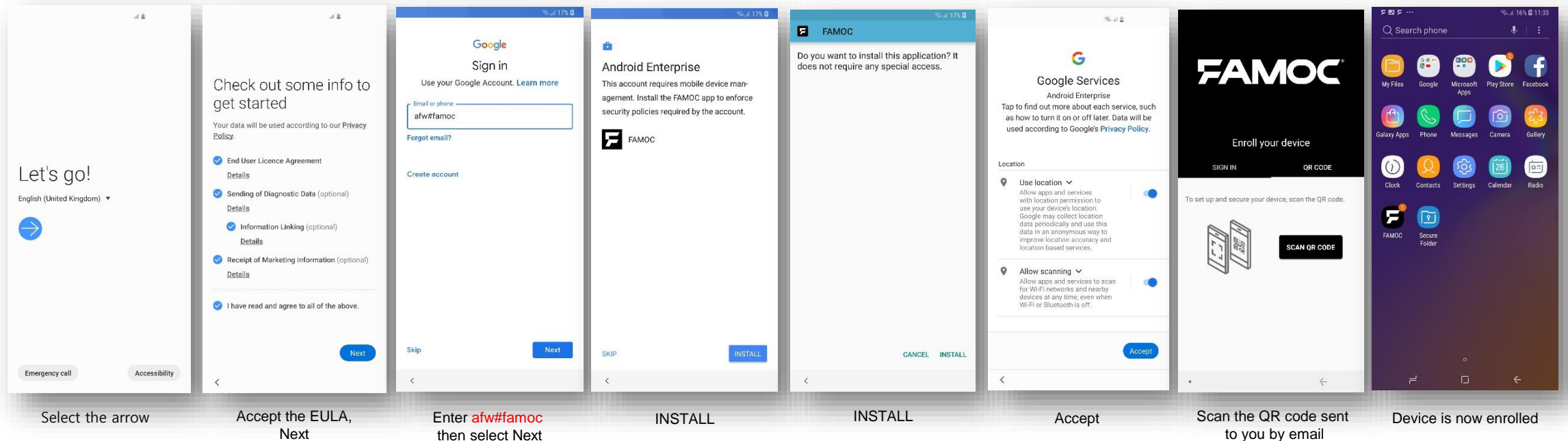
Android Enterprise: Fully Managed Device Enrollment

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.

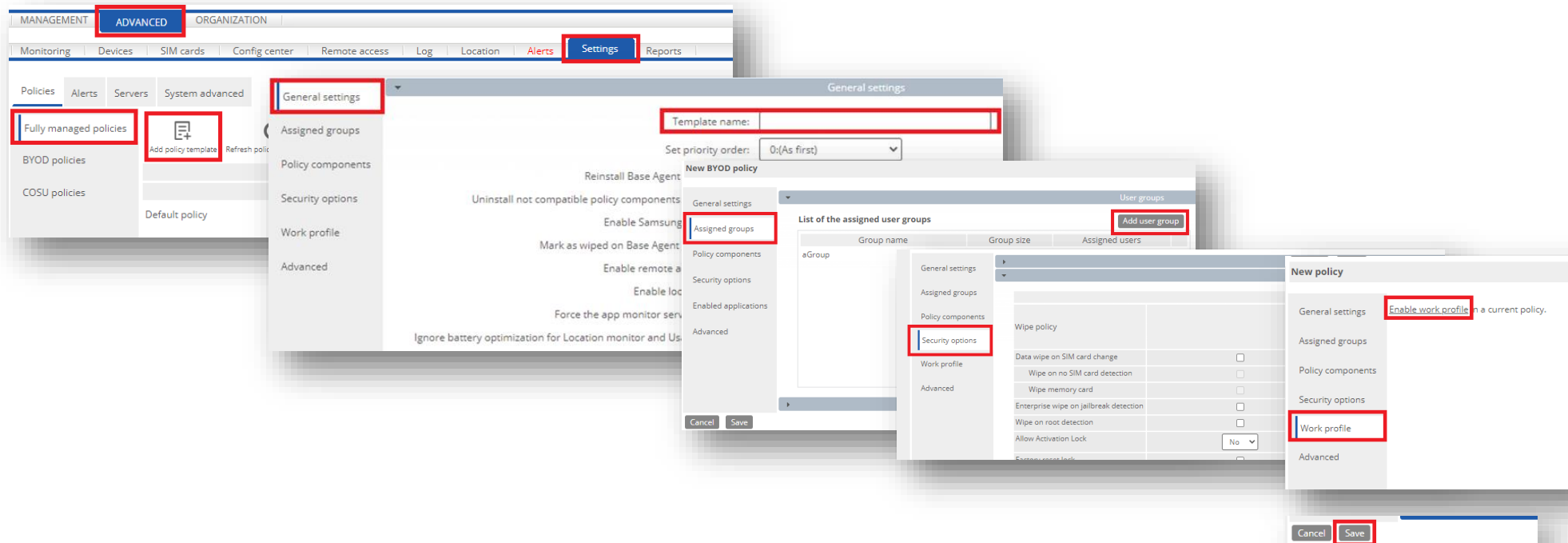
1. DPC Identifier [Also known as the hashtag method] **afw#famoc**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

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



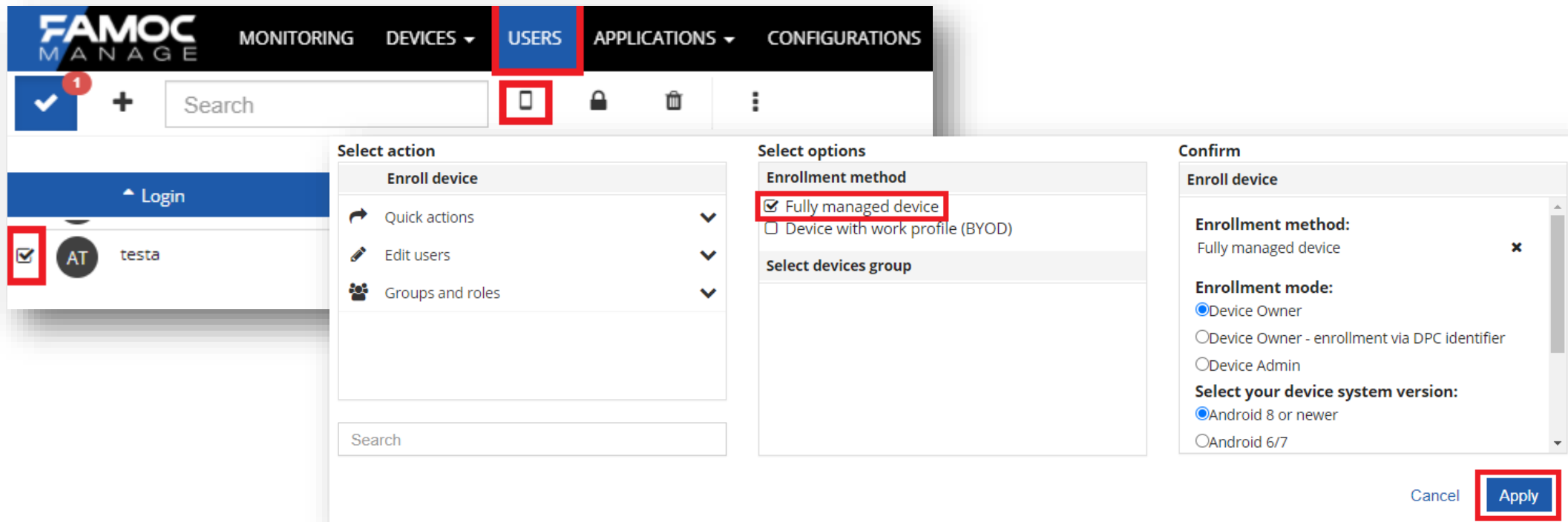
Fully Managed Device with a Work Profile Configuration

- 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



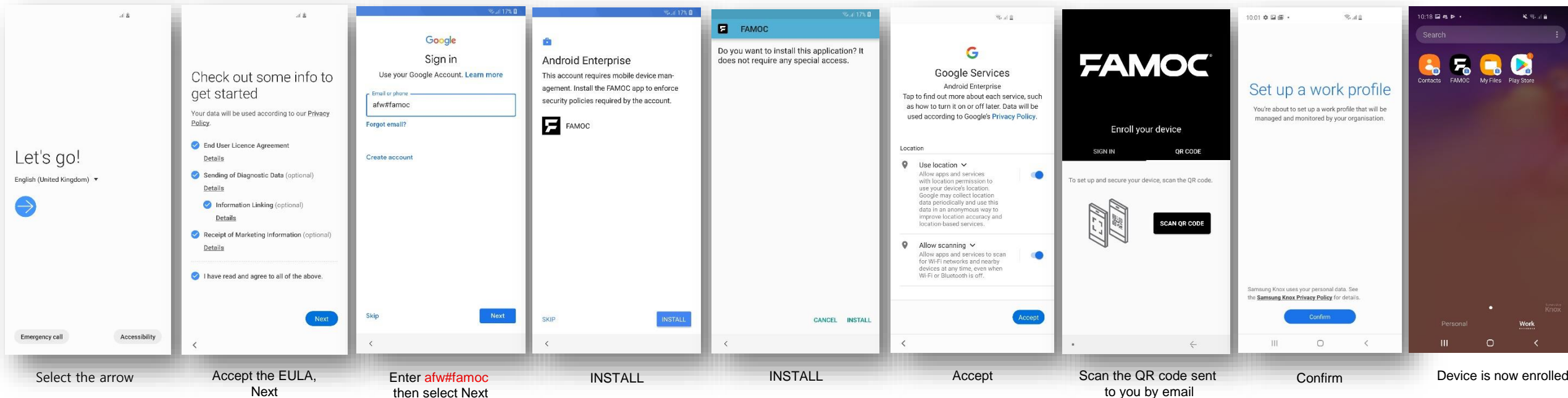
Android Enterprise: Fully Managed Device with a Work Profile Enrollment

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

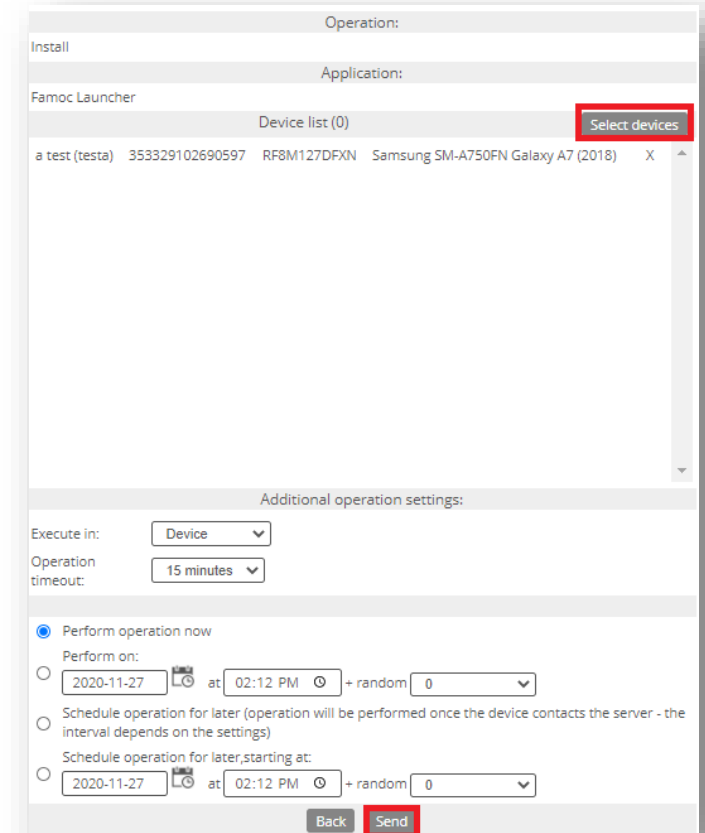
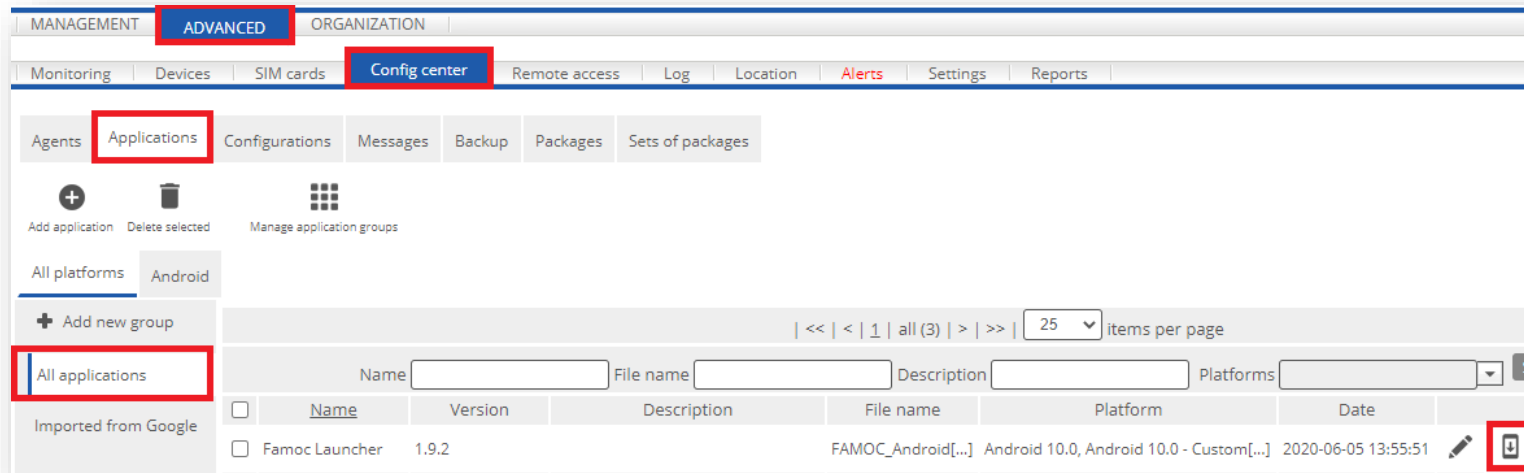
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Dedicated Device Configuration

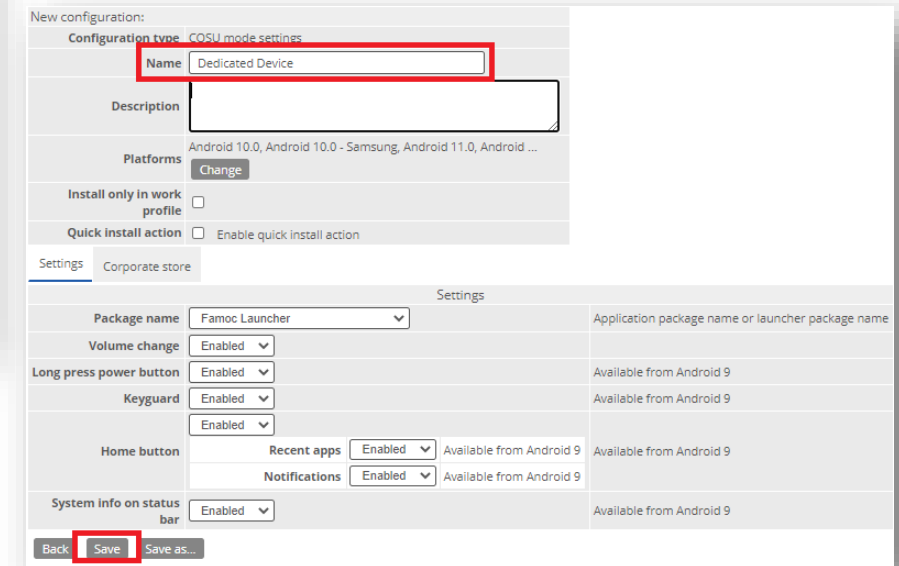
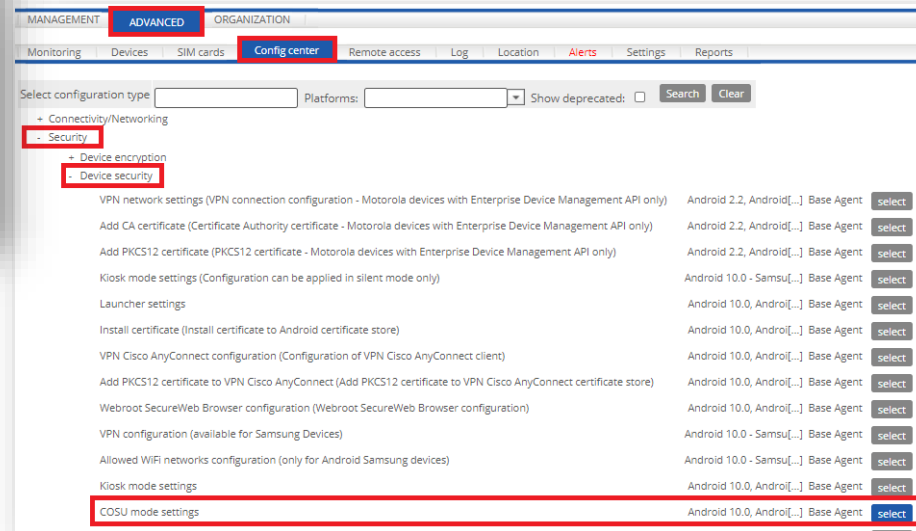
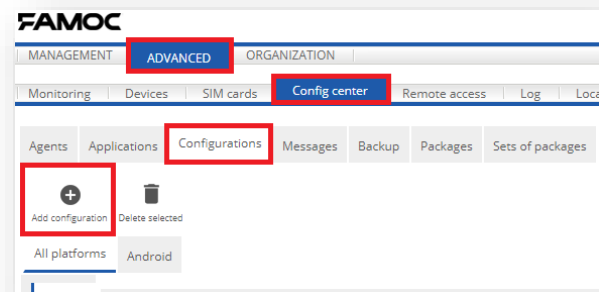
To setup a Dedicated device in FAMOC, you must first enroll your device using the Fully Managed Enrollment method.

- 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



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



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 Search Clear

<input type="checkbox"/>	Name	Type	Method	Description	Platform	Created by	Created on	
<input type="checkbox"/>	Dedicated Device	COSU mode settings	Base Agent		Android 10.0, Android 10.0 - Samsu[...]	James King	2020-11-27 14:19:02	

25 items per page

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

Device list (0) Select devices

Additional operation settings:

Operation timeout: 15 minutes

☒ Perform operation now

☐ Perform on:

at + random

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

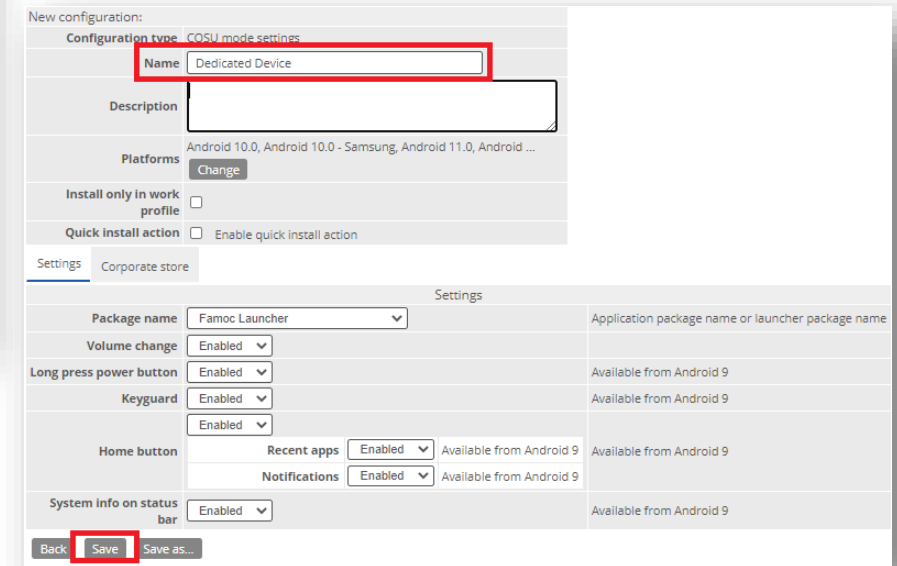
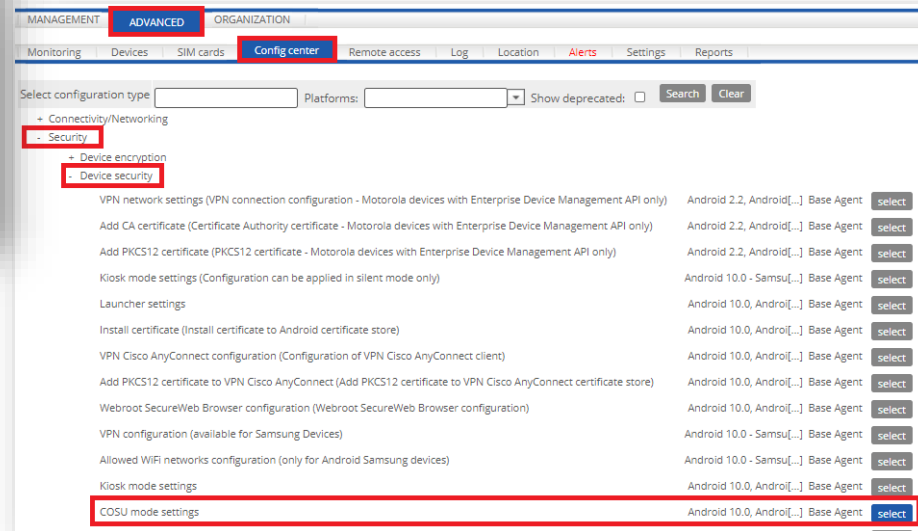
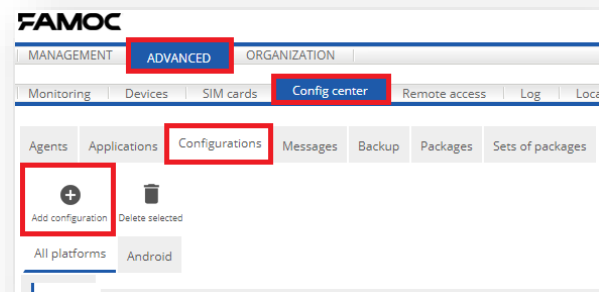
☐ Schedule operation for later, starting at:

at + random

Back Send

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



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

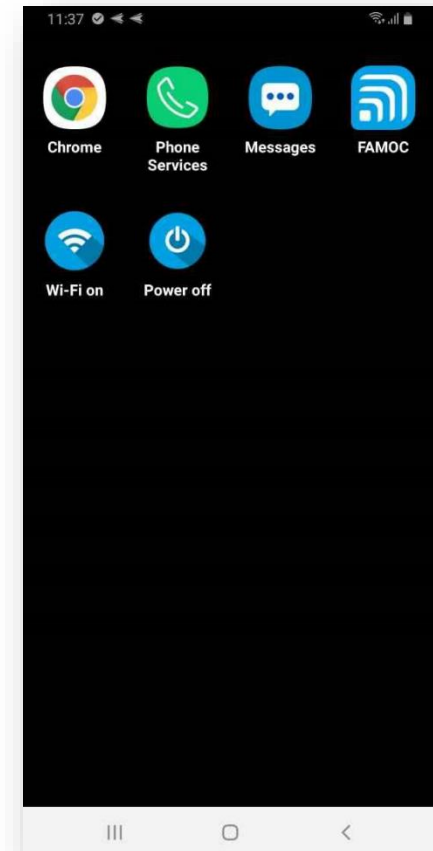
Method

Platforms

Search

Clear

<input type="checkbox"/>	Name	Type	Method	Description	Platform	Created by	Created on	
<input type="checkbox"/>	Dedicated Device	COSU mode settings	Base Agent		Android 10.0, Android 10.0 - Samsu[...]	James King	2020-11-27 14:19:02	
<input type="checkbox"/>	Settings	Launcher settings	Base Agent		Android 10.0, Android 10.0 - Custod[...]	James King	2020-11-27 14:29:03	



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 [\$]

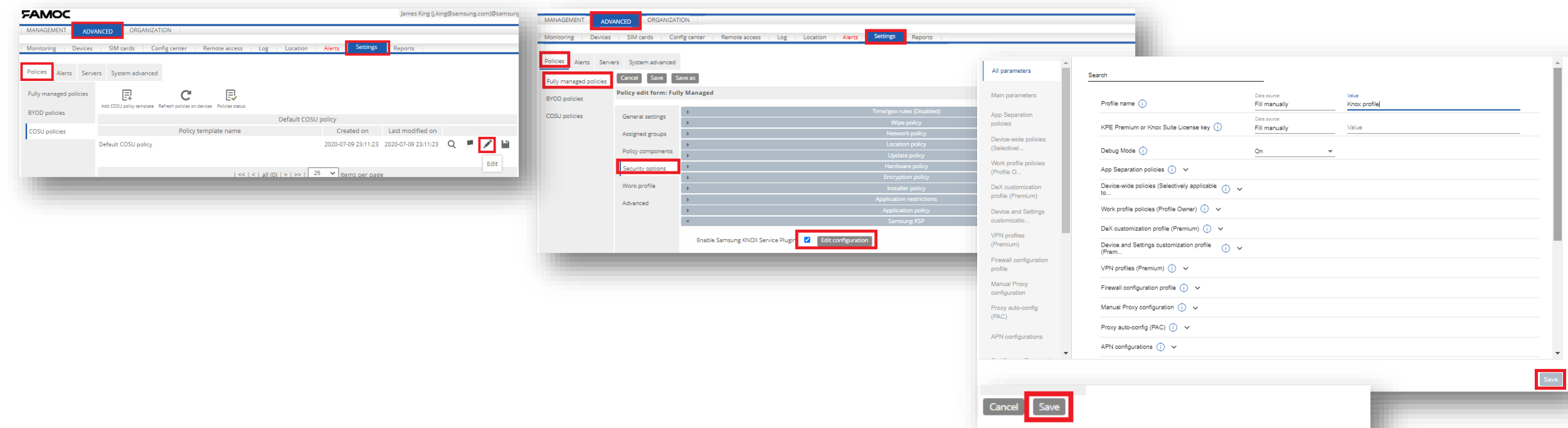
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android 8 or above.



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 (Firmware and Asset Management Over-the-Cloud) console, illustrating the process to configure the Samsung Knox Service Plugin.





First Screenshot: The 'MANAGEMENT' tab is active, and the 'ADVANCED' sub-tab is selected. The 'Policies' link in the left sidebar is highlighted with a red box. The main area shows a table of 'Fully managed policies' with columns for 'Policy template name', 'Created on', and 'Last modified on'. An 'Edit' button is visible at the bottom right of the table.

Second Screenshot: The 'Policies' page is shown with the 'Fully managed policies' tab selected. 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 with a red box.

Third Screenshot: The 'Edit configuration' dialog for the Samsung KSP is shown. The 'All parameters' tab is active. The 'Profile name' is set to 'Knox profile'. The 'KPE Premium or Knox Suite License key' is set to 'Fill manually'. The 'Debug Mode' is set to 'On'. The 'Save' button at the bottom right is highlighted with a red box.

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 2.0 of this document.

Thank you!

