



SOTI MobiControl v15.1.2.1035 & Knox Platform for Enterprise

August 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
 - Dedicated Device
4. Android Enterprise configuration
5. Work Profile enrollment flow
6. Fully Managed enrollment flow
7. Dedicated Device configuration
8. Configure Knox Service Plugin [KSP] Standard and Premium

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

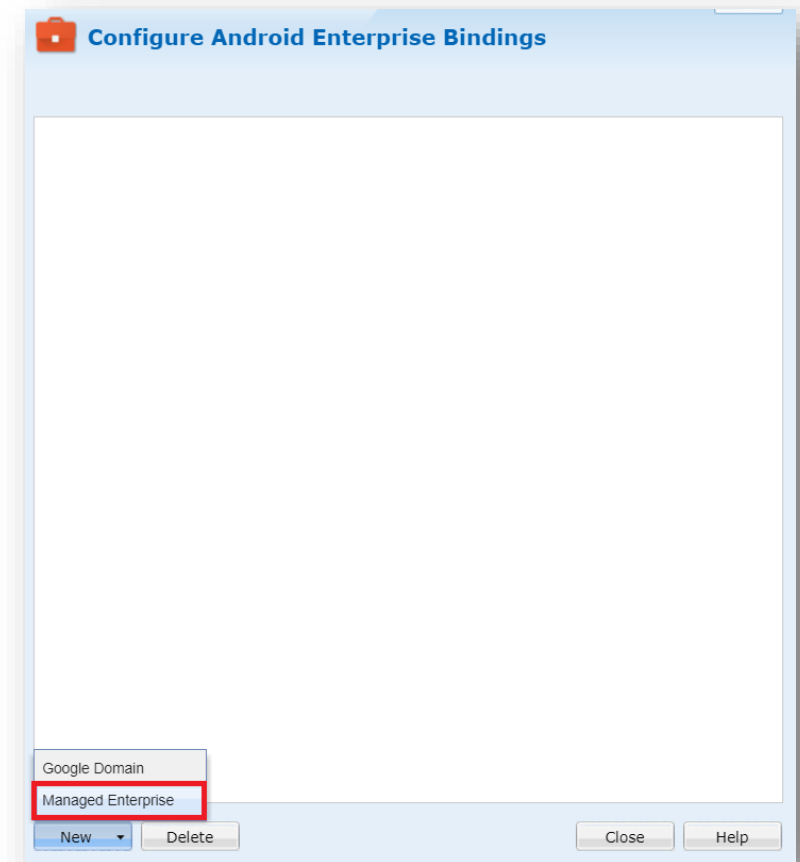
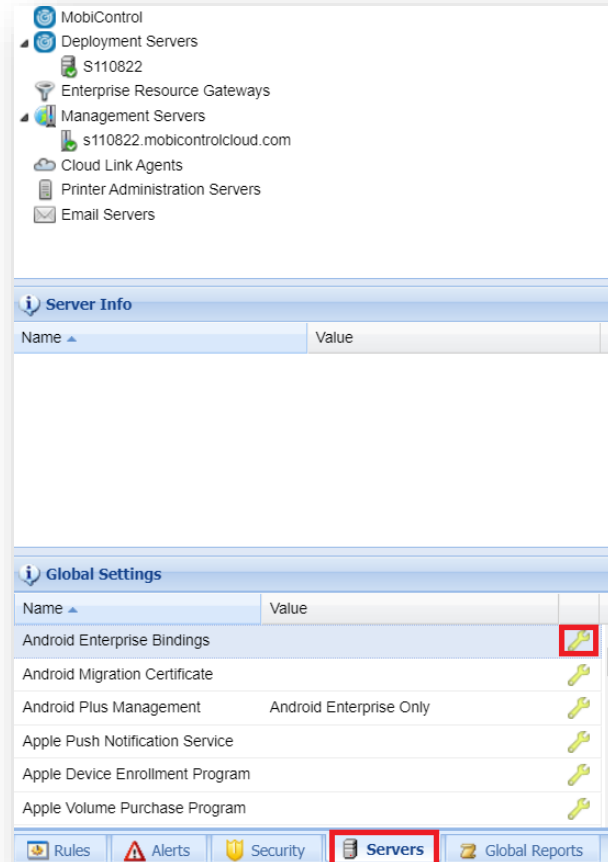
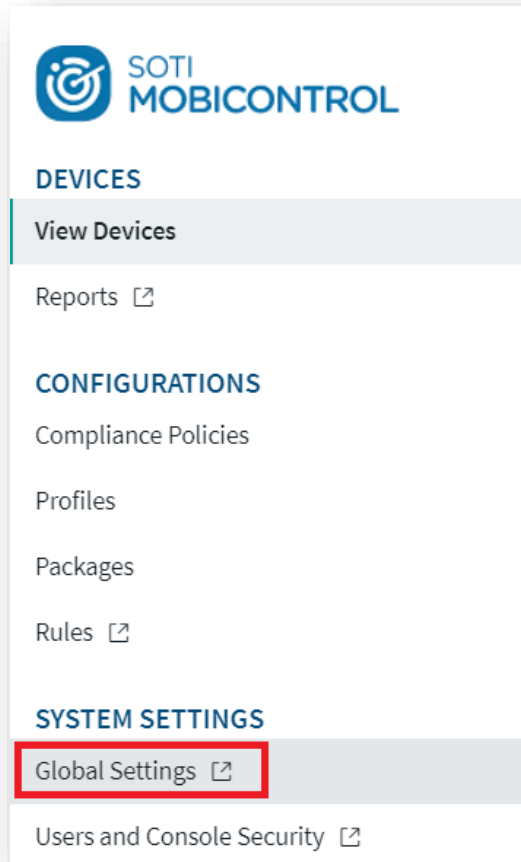
<https://www.soti.net/mc/help/v15.1/en/start.html>

Pre-Requisites for Knox Platform for Enterprise

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

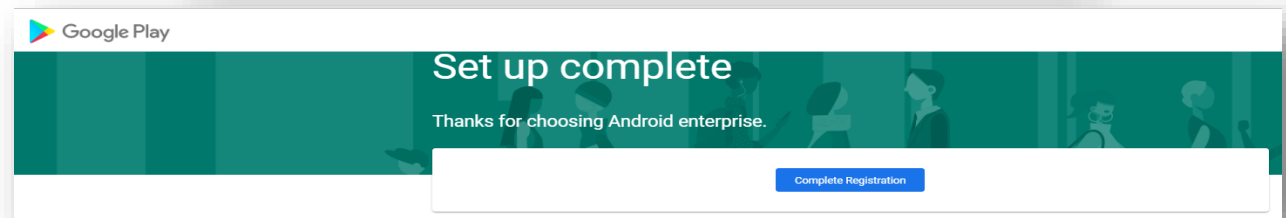
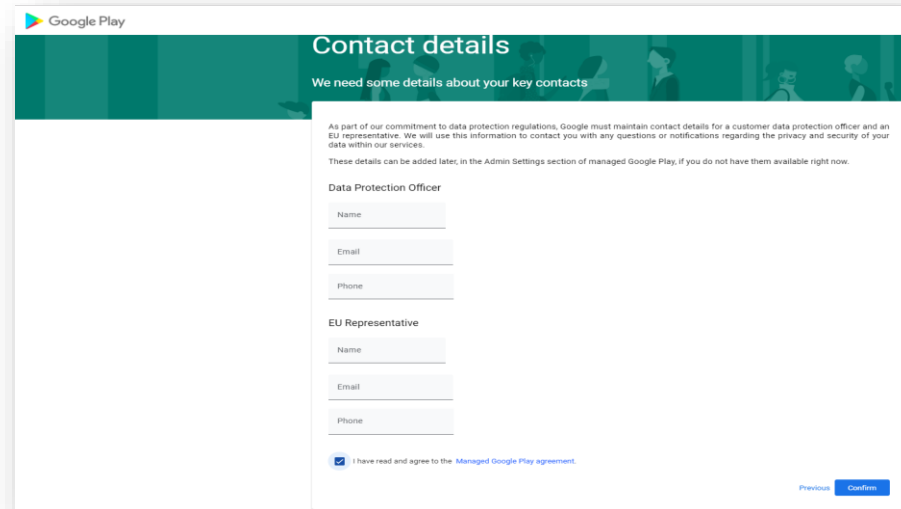
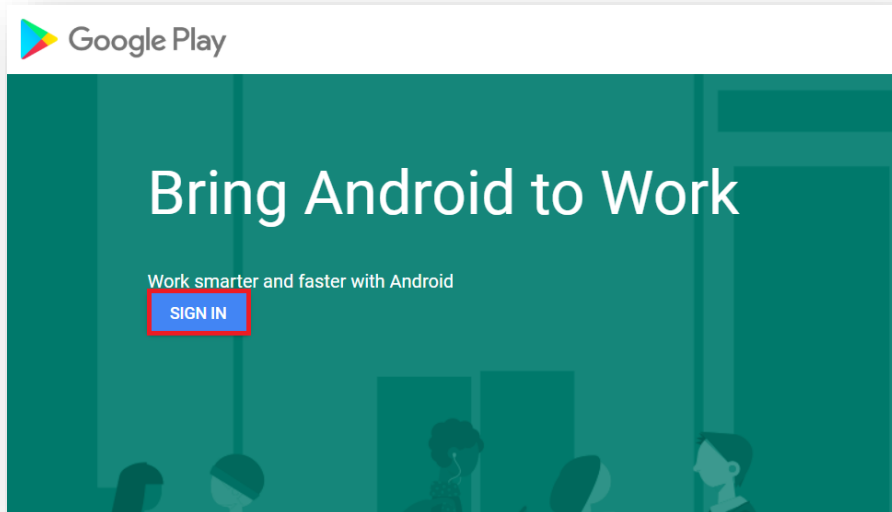
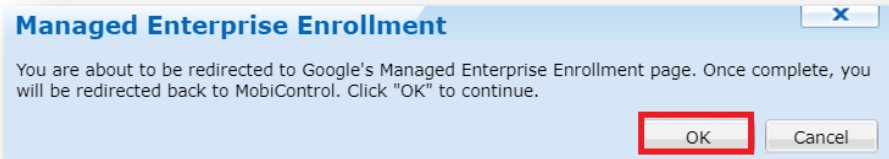
Configure Android Enterprise

- Within the SOTI MobiControl console, select Global Settings on the left
- Select Servers at the bottom and then select the spanner icon next to Android Enterprise Bindings
- Select New then Managed Enterprise



Configure Android Enterprise

- Select OK and sign in with your Google Account
- Fill out the Contact details page, tick the Managed Google Play agreement and then select Confirm. These text fields are not mandatory, so you can alternatively leave them blank and just tick the Managed Google Play agreement and then select Confirm.
- Click Complete Registration to complete the Android Enterprise configuration and return to the SOTI MobiControl console.



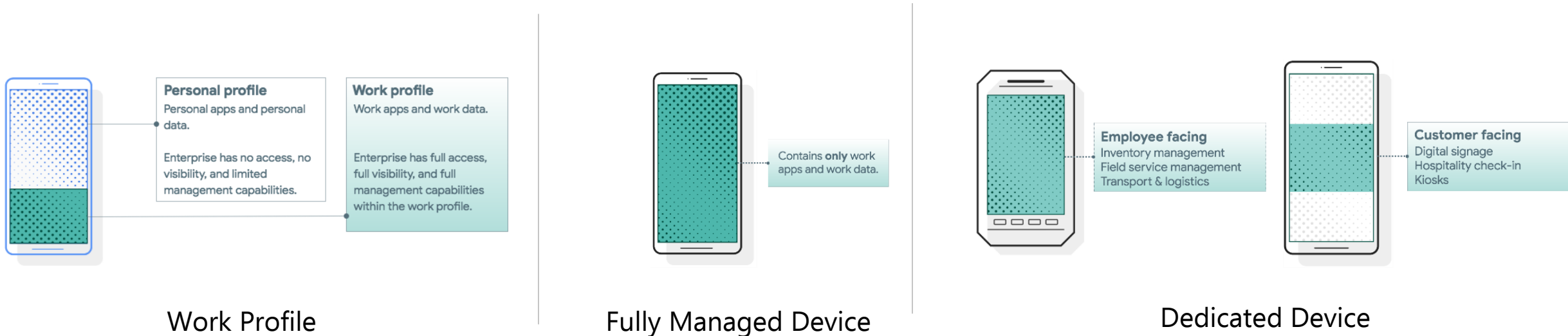
Android Enterprise Deployment Modes

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 (Not Supported) [*formerly known as COMP*]
4. Dedicated device [*formerly known as COSU*]

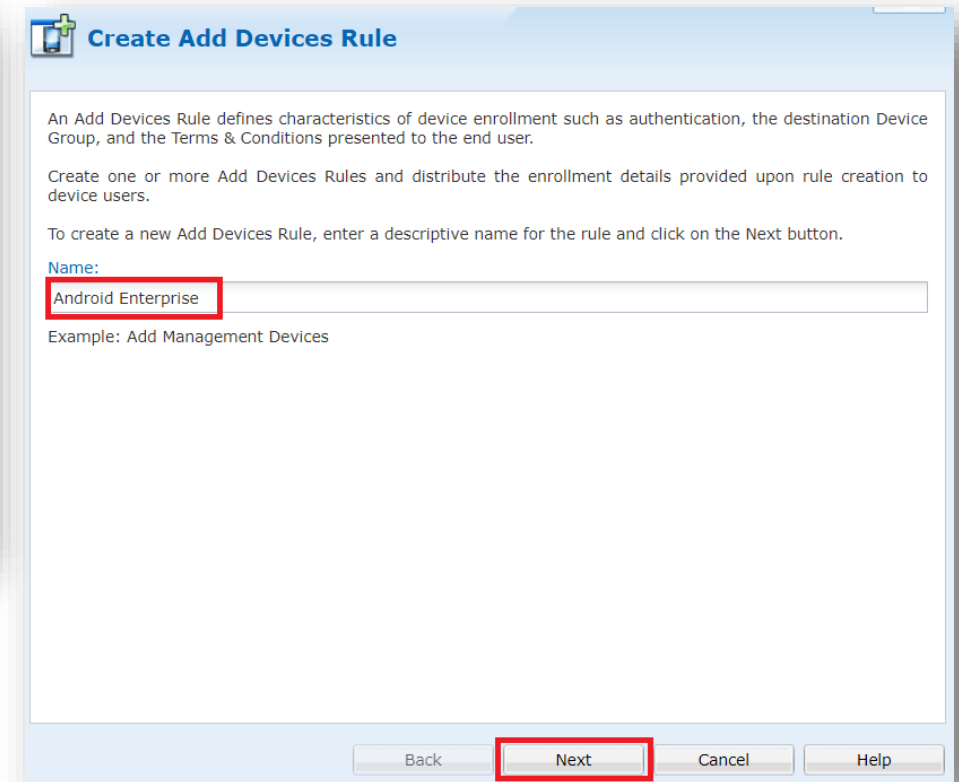
SOTI MobiControl can support 3 of these deployment modes. In this next section we will show you how to configure each of these 3 deployment modes in SOTI MobiControl for your device fleet.



Create Android Enterprise Device Rule

Creating an Android Enterprise Device Rule will enable the enrollment methods Work Profile and Fully Managed. The steps below illustrate how this is done.

- Within the SOTI MobiControl Global Settings, Select Android Plus at the top
- Right click on Add Devices and click Create Add Devices Rule
- Type a name of your choice and select Next



Create Android Enterprise Device Rule

- Choose which devices to target, select Next
- Select a device group, select Next
- Select how you would like users to authenticate, select Next

Create Add Devices Rule

Choose which method to use when selecting the destination Device Group for devices enrolling using this Add Device Rule.

☒ **Manual**
Choose the Device Group that devices will be enrolled to.

☐ **Based on User Group Membership**
Map user groups to device groups. Devices whose user is a member of a specified user group will be placed in the corresponding device group.

Back Next Cancel Help

Create Add Devices Rule

Select the device group that the rule should target.

- My Company
 - DeX KSP demo
 - ☒ Management Devices
 - Sales Devices
 - Warehouse Devices

Child Selected Parent Selected Selected 0 Total Device(s) Targeted

Back Next Cancel Help

Create Add Devices Rule

User Authentication Options

☐ Utilize user groups to authenticate users during device enrollment. Required for resolution of username macros on Exchange, VPN or WiFi payloads.

☒ **Directory Service** ☐ Identity Provider

Search entity from directory service... Add

All authenticated users can enroll with this rule

☐ Consider LDAP user as an enrollment user and assign all the user profiles (macOS Only)

☐ Password required to verify device enrollment

Show Password

☒ **No password required to verify device enrollment**

Certificate Authentication Authority

Issue device identity using:
Internal MobiControl CA

Back Next Cancel Help

Create Android Enterprise Device Rule

- Choose whether to enable Terms and Conditions, select Next
- Choose which permissions to prompt the user for, select Next
- Select Managed Google Play Accounts
- Select which account to use in the drop down, select Next

Create Add Devices Rule

☐ Enable Terms and Conditions to apply at Enrollment

Select the Terms and Conditions

Manage Preview

Back Next Cancel Help

Create Add Devices Rule

Permissions

Select the permissions to be granted at Enrollment

Draw Over Other Apps	<input type="checkbox"/>
Modify System Settings	<input checked="" type="checkbox"/>
Notification Access	<input type="checkbox"/>
Usage Access	<input type="checkbox"/>

Modify System Settings
Permission to modify system settings.

Back Next Cancel Help

Create Add Devices Rule

Android Enterprise Setup

For Access to the Managed Google Play Store, choose which method to use to Manage the Android Devices enrolling using this Add Device Rule. If access to the Managed Google Play Store is not required, you do not need to modify any of the options below and can continue with the Add Device Rule Creation.

☒ Managed Google Play Accounts

Available Enterprises

Test

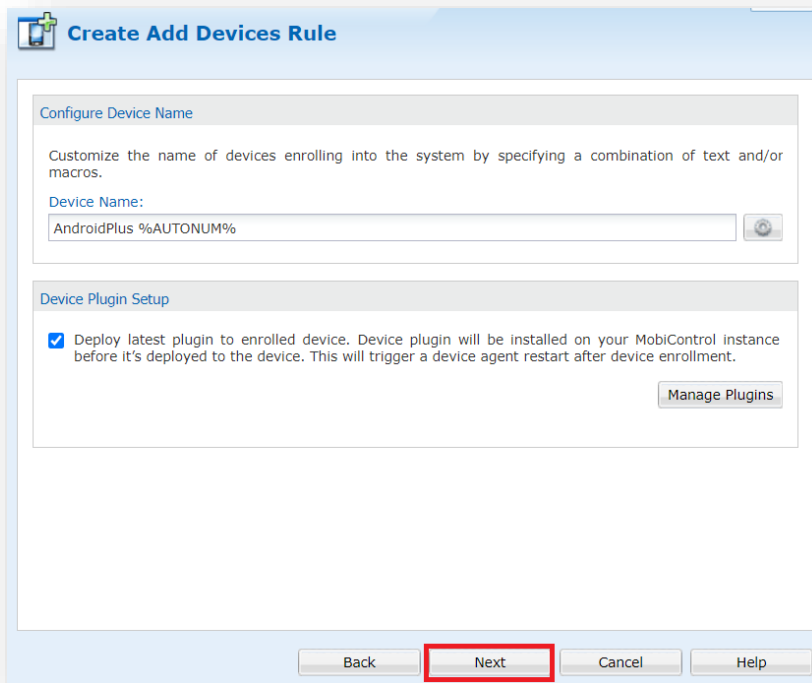
☐ Managed Google Accounts
Manage the Devices using Google Accounts created in the Google Admin Portal ([Admin.Google.Com](#))

☐ Skip Google Account Addition During Enrollment on Managed Android Devices

Back Next Cancel Help

Create Android Enterprise Device Rule

- Choose how you would like devices to be named
- Choose whether or not to add a plugin
- Select Next
- Select Finish
- Save the Enrollment ID, this will be used by your end users to enroll
- Select Close



Create Add Devices Rule

Configure Device Name

Customize the name of devices enrolling into the system by specifying a combination of text and/or macros.

Device Name:

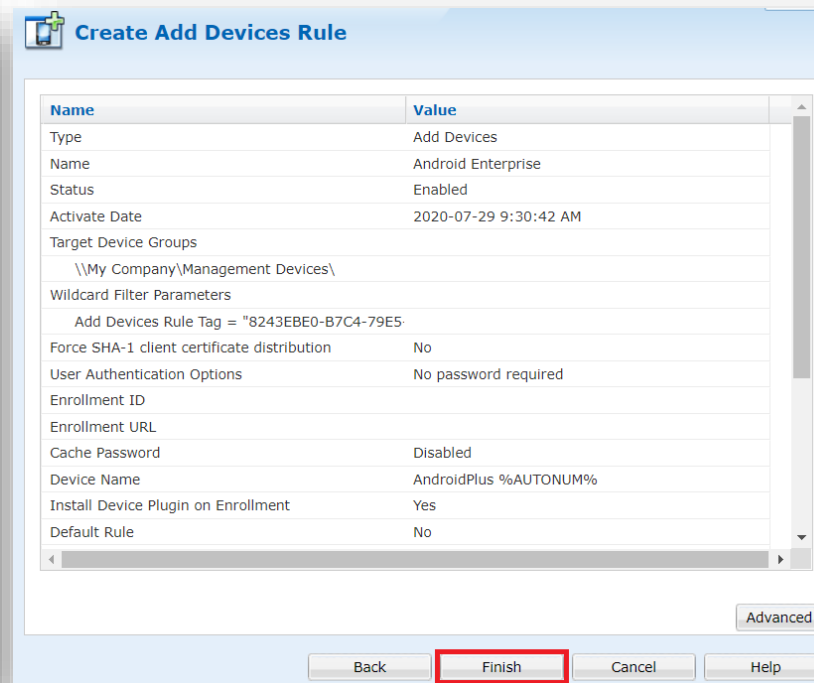
AndroidPlus %AUTONUM%

Device Plugin Setup

☒ Deploy latest plugin to enrolled device. Device plugin will be installed on your MobiControl instance before it's deployed to the device. This will trigger a device agent restart after device enrollment.

Manage Plugins

Back Next Cancel Help

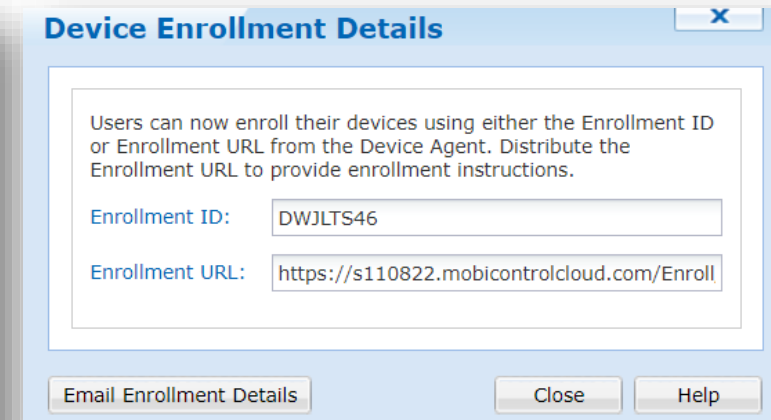


Create Add Devices Rule

Name	Value
Type	Add Devices
Name	Android Enterprise
Status	Enabled
Activate Date	2020-07-29 9:30:42 AM
Target Device Groups	\\My Company\Management Devices\
Wildcard Filter Parameters	Add Devices Rule Tag = "8243EBE0-B7C4-79E5"
Force SHA-1 client certificate distribution	No
User Authentication Options	No password required
Enrollment ID	
Enrollment URL	
Cache Password	Disabled
Device Name	AndroidPlus %AUTONUM%
Install Device Plugin on Enrollment	Yes
Default Rule	No

Advanced

Back Finish Cancel Help



Device Enrollment Details

Users can now enroll their devices using either the Enrollment ID or Enrollment URL from the Device Agent. Distribute the Enrollment URL to provide enrollment instructions.

Enrollment ID: DWJLTS46

Enrollment URL: https://s110822.mobicontrolcloud.com/Enroll

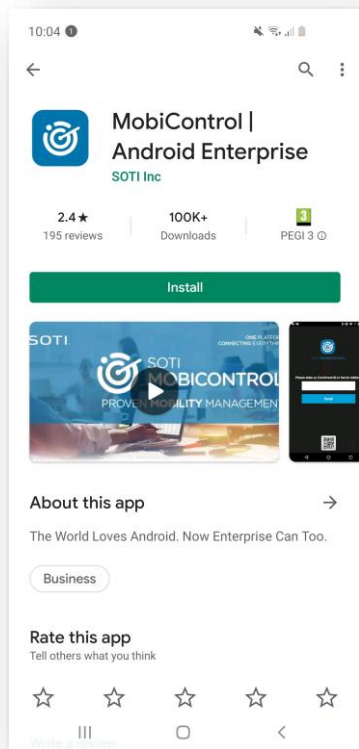
Email Enrollment Details Close Help

Android Enterprise: Work Profile Enrollment

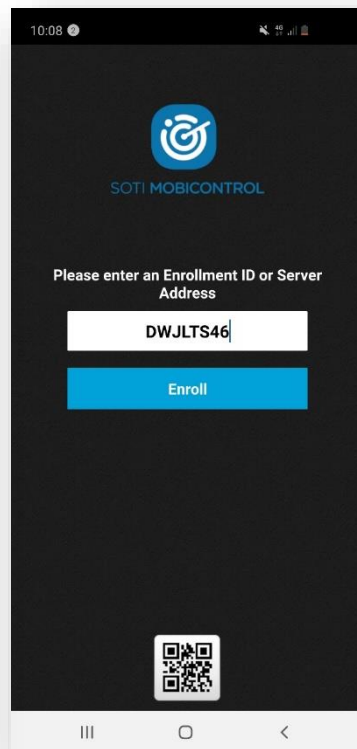
Android Enterprise BYOD Deployment

To enroll a device in the Android Enterprise BYOD deployment type, you simply need to use the EnrollmentID that was generated from the Device Rule from the previous slide.

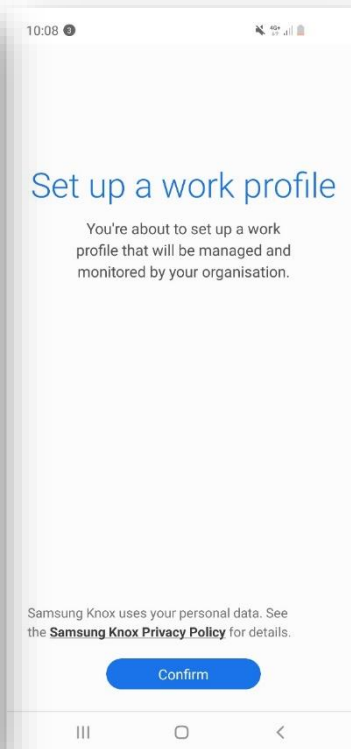
- On your device, go to the Google Play Store, download the MobiControl Android Enterprise client, and enroll your device into MobiControl.



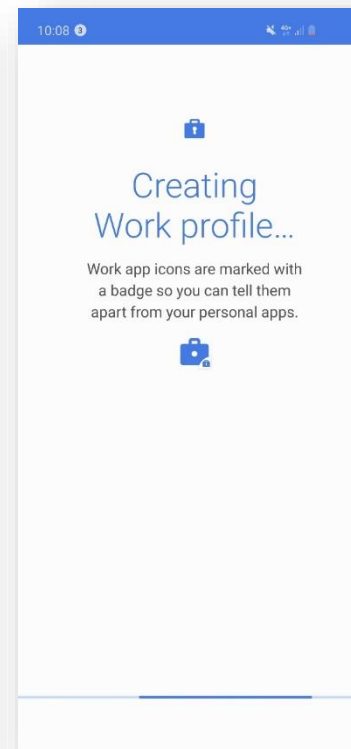
Install MobiControl from the Google Play Store



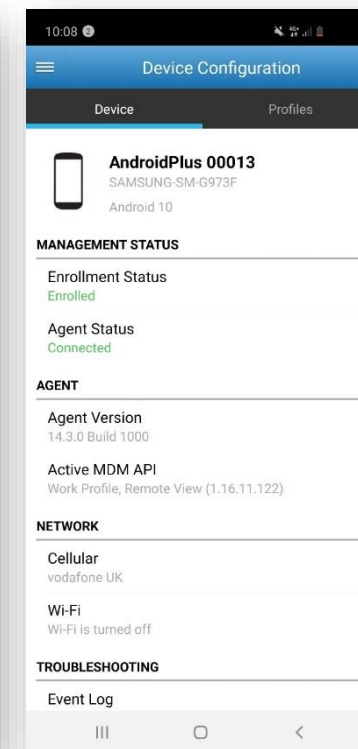
Open MobiControl, enter Your Enrollment ID and select Enroll



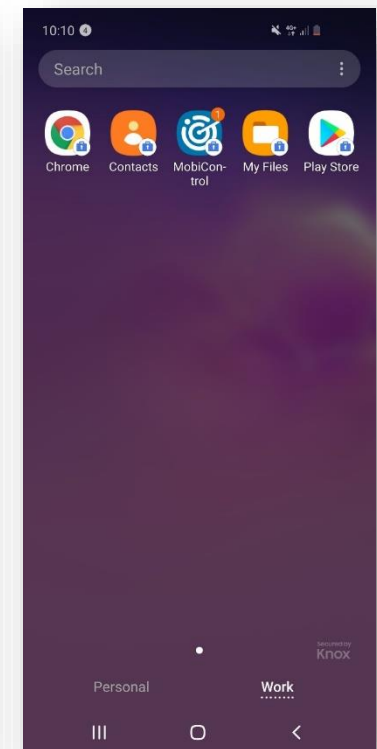
Confirm



Wait, Work Profile Will now configure



Your device is now enrolled, tap the home button



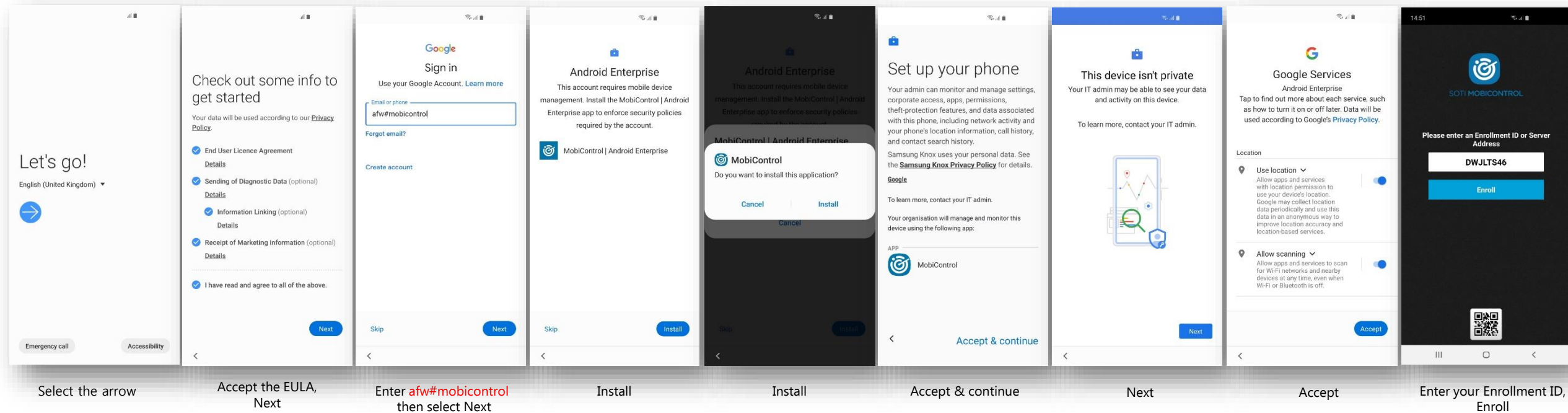
Work and Personal profiles are now separate

Android Enterprise: Fully Managed Enrollment

Android Enterprise Company-owned Device Deployment

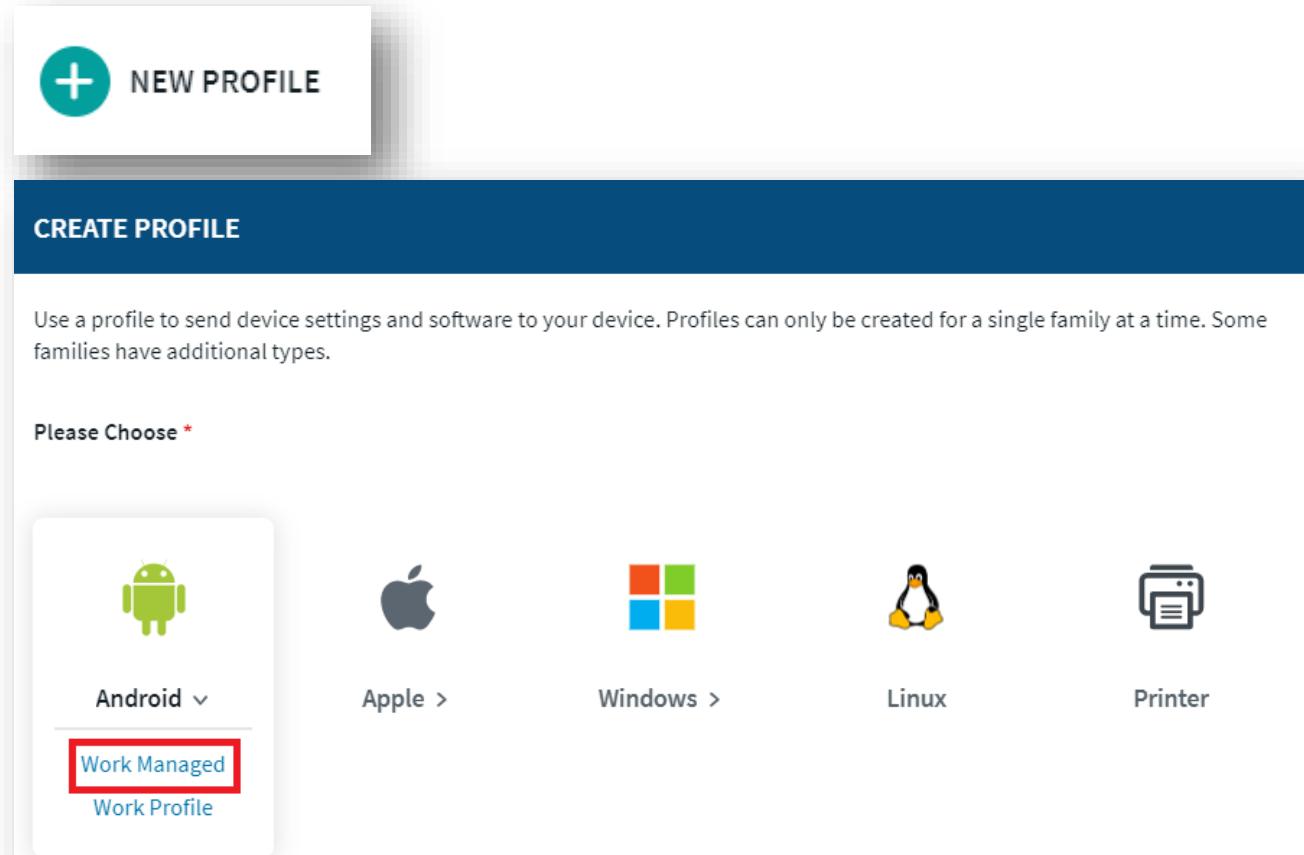
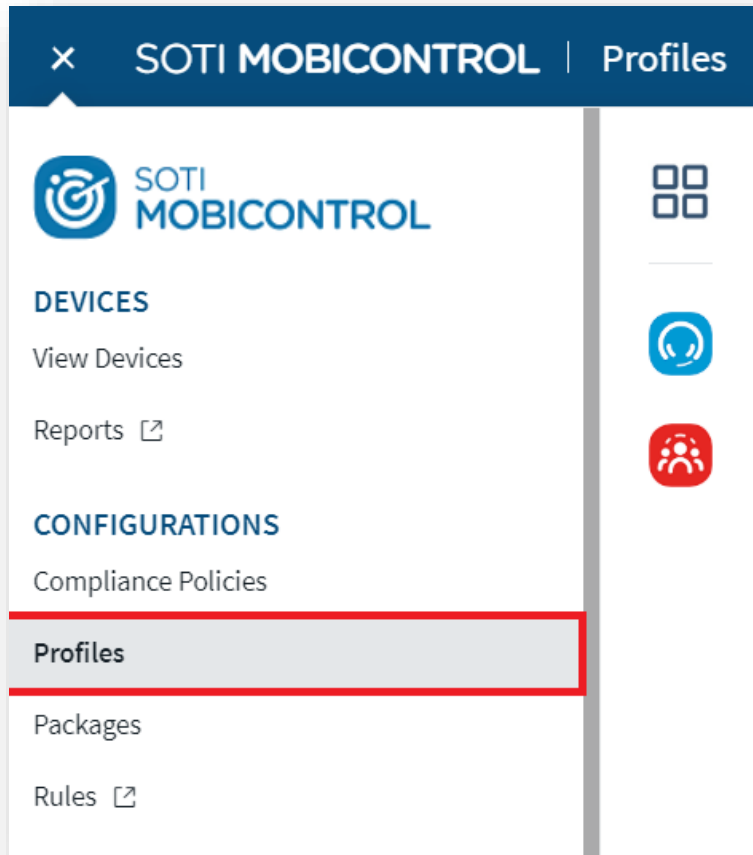
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into MobiControl UEM as an Android Enterprise Company-owned device. Use the same 'Android Enterprise Rule' configuration but start from a factory reset device.

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



Android Enterprise: Dedicated Device Configuration

- Click the navigation button in the top left corner of the main console and select Profiles
- Select NEW PROFILE on the left
- Select Android then Work Managed



Android Enterprise: Dedicated Device Configuration

- In the GENERAL tab, enter a Profile Name
- Select the CONFIGURATIONS tab and then click the + symbol
- Select Authentication
- Set an Administrator password of your choice then select the DEVICE tab

CREATE PROFILE

GENERAL CONFIGURATIONS PACKAGES

Profile Name * Kiosk

Description Profile description

Status n/a

Version 1.0

Family Android Plus

Type Android Enterprise - Work Managed Device

Configurations 0

Packages 0

CANCEL SAVE AND ASSIGN SAVE

CREATE PROFILE

GENERAL CONFIGURATIONS PACKAGES

PROFILE CONFIGURATION

NO CONFIGURATIONS ADDED

Configurations are added to profiles to push settings down to devices.

CANCEL SAVE AND ASSIGN SAVE

AUTHENTICATION

Create administrator and user password policies and set password complexity.

ADMINISTRATOR DEVICE

Device Administrator

Password * ****

CANCEL SAVE

Android Enterprise: Dedicated Device Configuration

- Select Disable Lockscreen and then SAVE
- Select the + symbol
- Select Lockdown

AUTHENTICATION

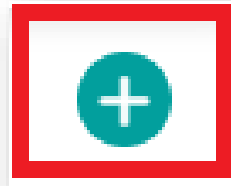
Create administrator and user password policies and set password complexity.

ADMINISTRATOR **DEVICE**

Device Password Policy

Password Policy Type: **Disable Lockscreen**

CANCEL **SAVE**



CREATE PROFILE

GENERAL **CONFIGURATIONS** PACKAGES

PROFILE CONFIGURATION

Configuration

Security

Virus Protection

Authentication

Certificates

Factory Reset Protection

Location of Contact

System Update Policy

Restrictions

Application Run Control

Browser

Browser Proxy

Feature Control

Lockdown

Web Filter

Connectivity

APN

VPN (2)

WiFi

Email & Others

Bookmarks

Email: Exchange For Gmail

Managed Google Play

Task Scheduler

SOTI Apps

Settings Manager

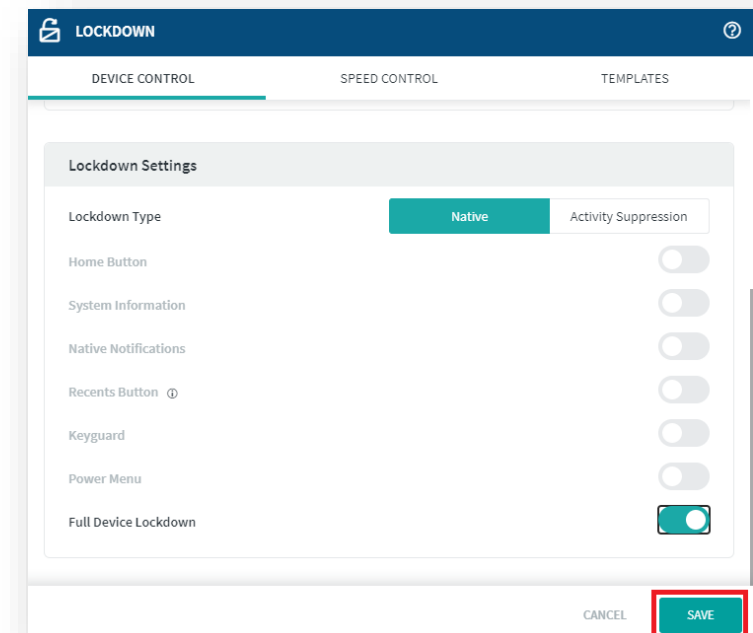
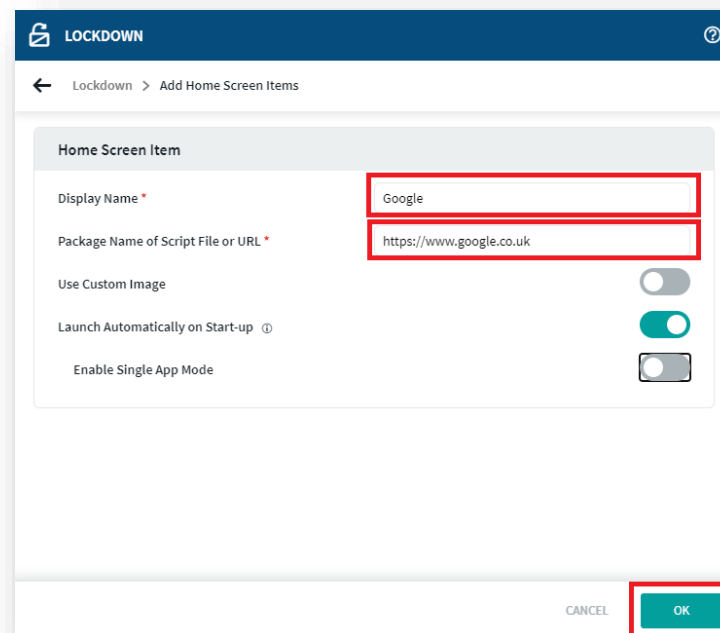
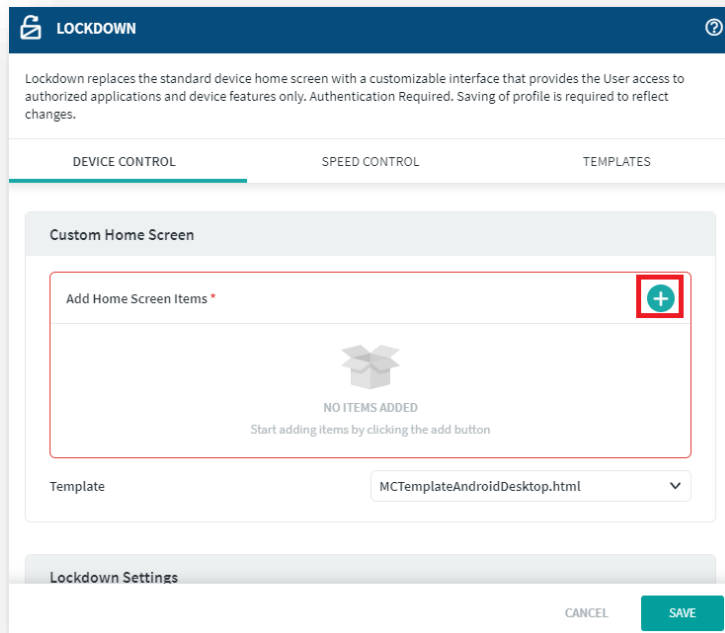
SOTI Hub

SOTI Surf

CANCEL **SAVE AND ASSIGN** **SAVE**

Android Enterprise: Dedicated Device Configuration

- Select the + symbol under Custom Home Screen
- Enter a Display Name and add either a package name or a URL for your chosen application
- Choose your desired Lockdown Settings and then select SAVE



Android Enterprise: Dedicated Device Configuration

- Select the SAVE AND ASSIGN
- Select a Device Group and then click ASSIGN

For Dedicated Device enrollment, follow the same enrollment steps as the Fully Managed on slide 13.

CREATE PROFILE

GENERAL CONFIGURATIONS PACKAGES

PROFILE CONFIGURATION

NAME	DESCRIPTION
Authentication	Authentication
Lockdown	Lockdown

CANCEL **SAVE AND ASSIGN** SAVE

ASSIGN | Kiosk Test

Select the devices or device groups this profile will be assigned to.

DEVICES USERS FILTERS

Device Groups

- My Company
 - DeX KSP demo
 - Management Devices**
 - Sales Devices
 - Warehouse Devices

Devices (1)

DEVICE NAME

- AndroidPlus 00017

1 Total Devices Targeted CANCEL **ASSIGN**



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:

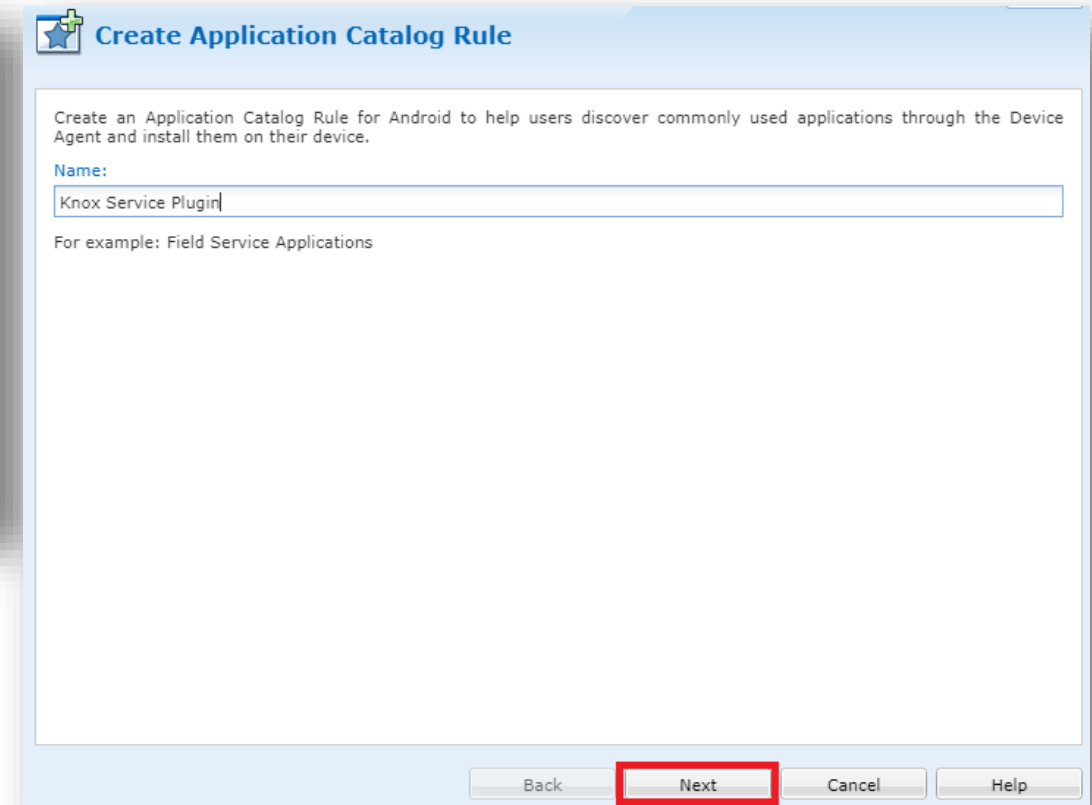
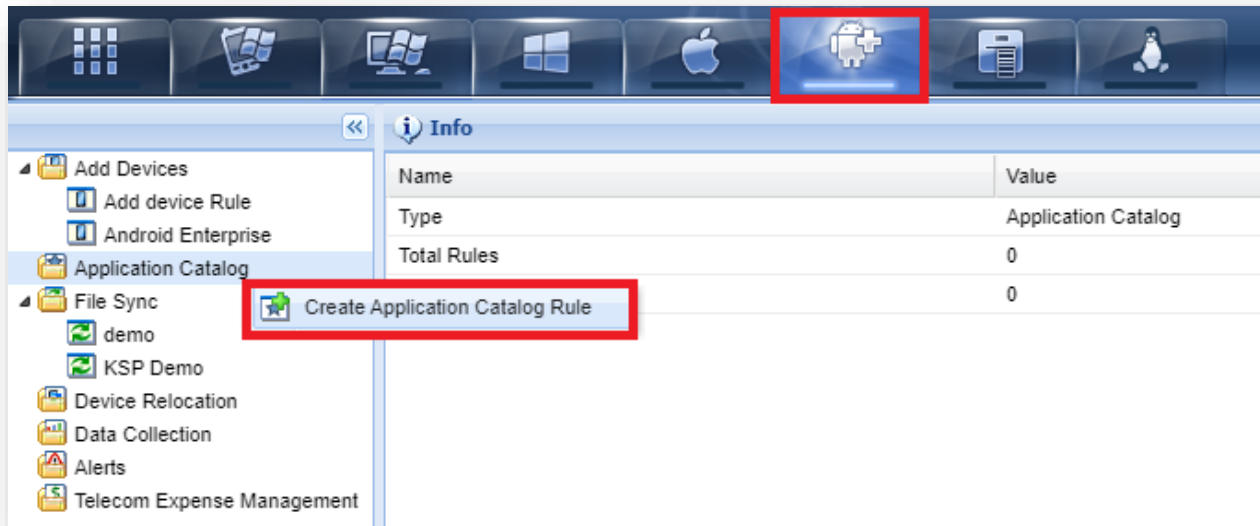
- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [\$]

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 Enterprise on Oreo or above.



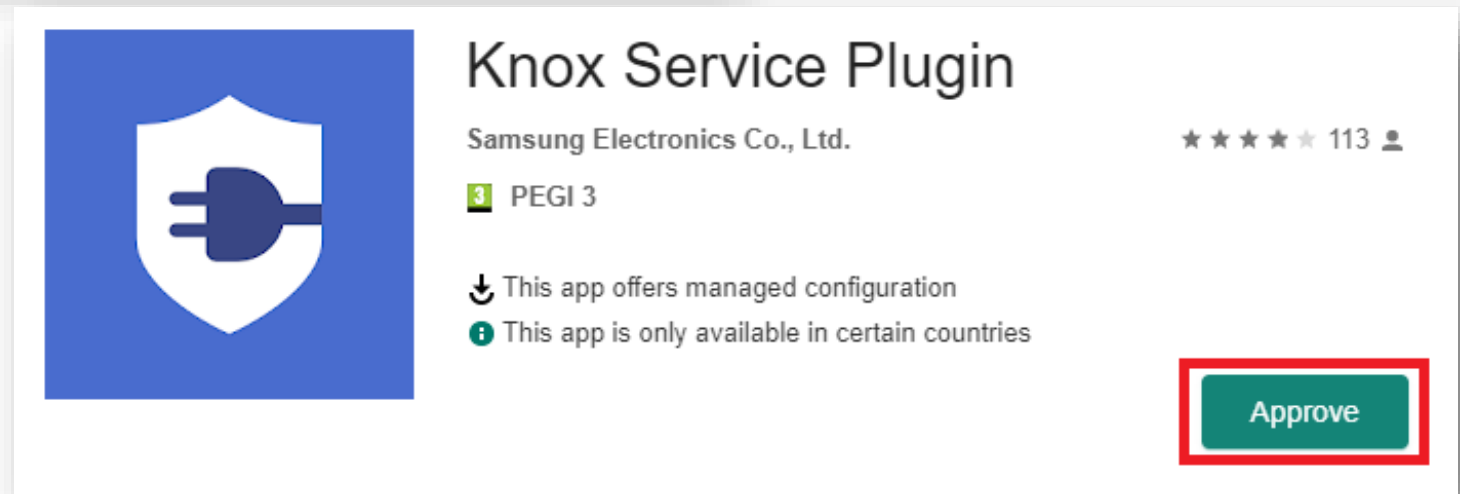
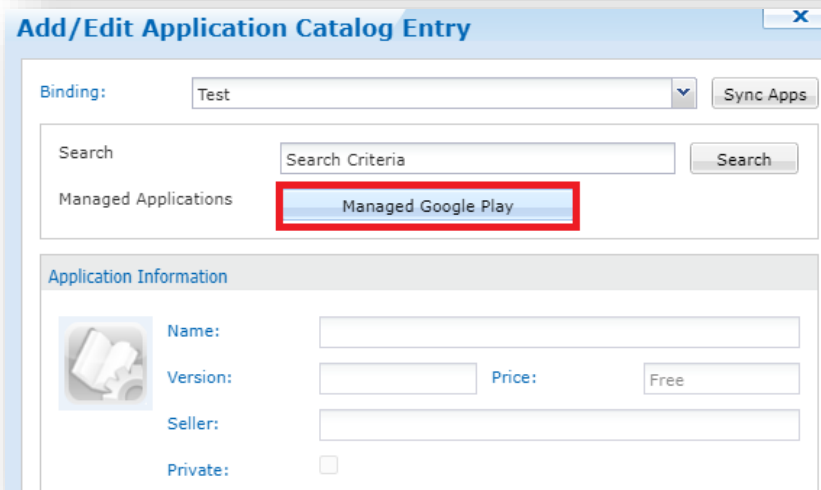
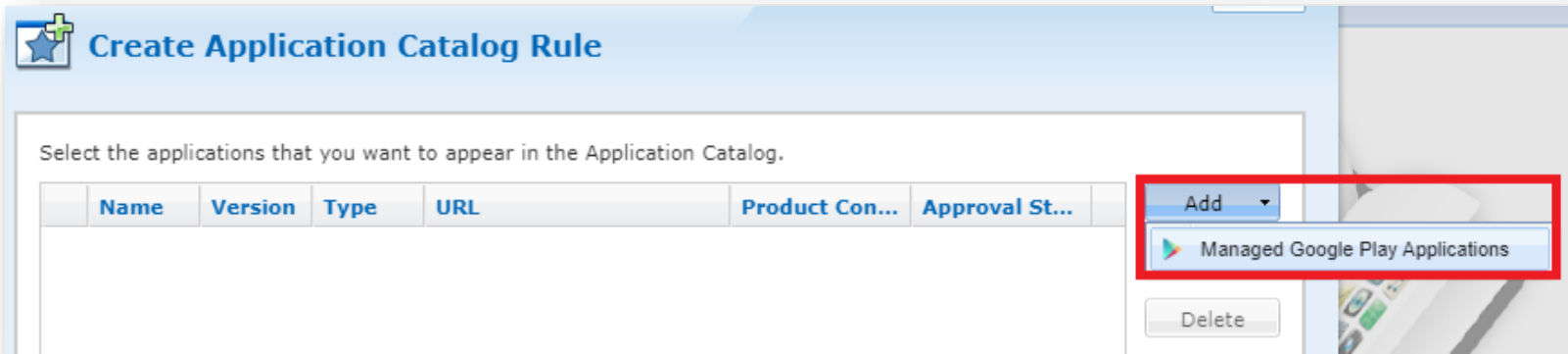
Configure Knox Platform for Enterprise using Knox Service Plugin

- Within Global Settings, Select Android Plus
- Right click on Application Catalog, select Create Application Catalog Rule
- Type a name of your choice, select Next



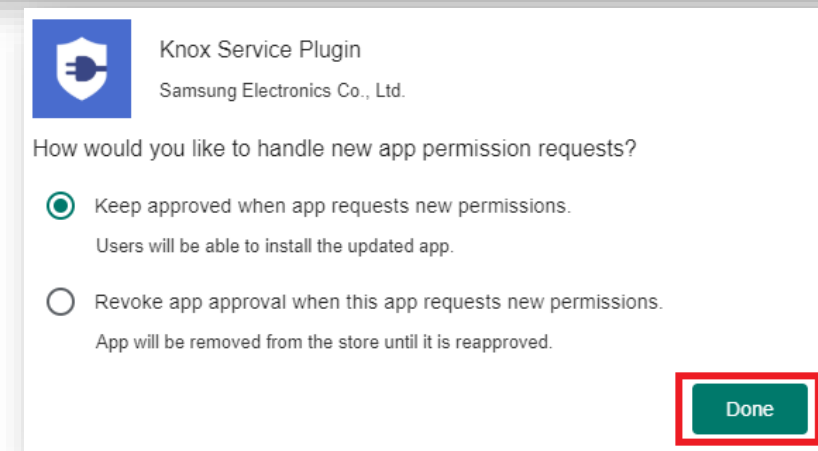
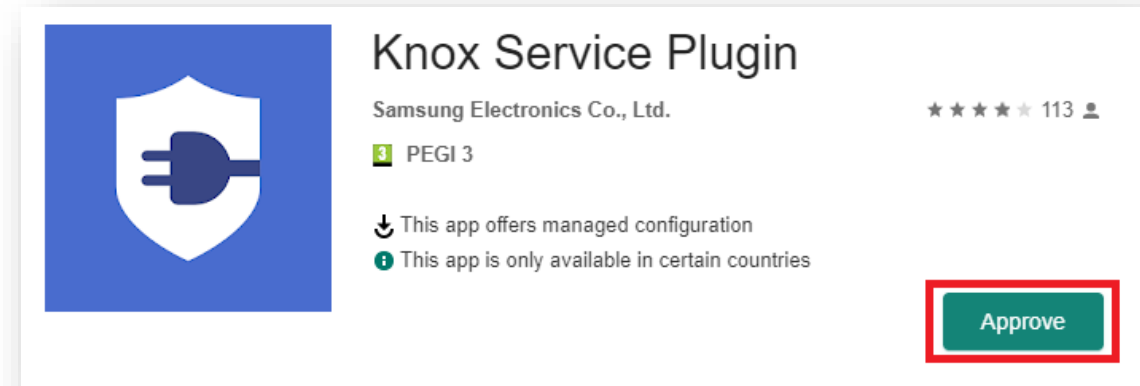
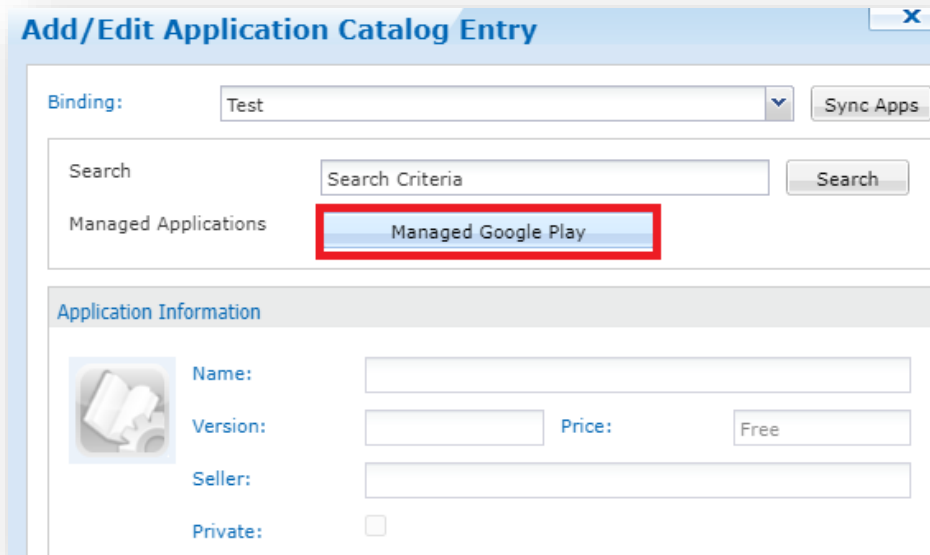
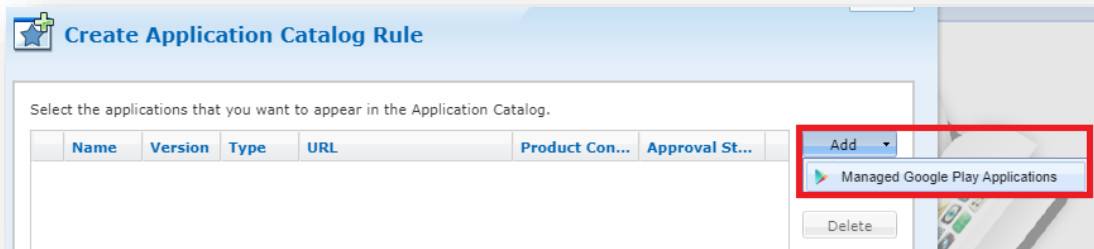
Configure Knox Platform for Enterprise using Knox Service Plugin

- Select Add, then Managed Google Play Applications
- Click Managed Google Play
- Search for and Approve the Knox Service Plugin



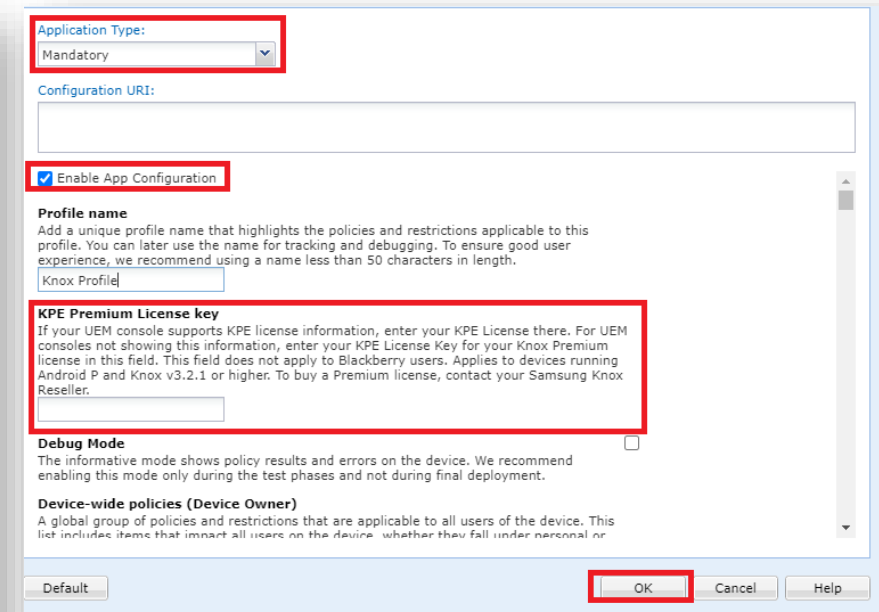
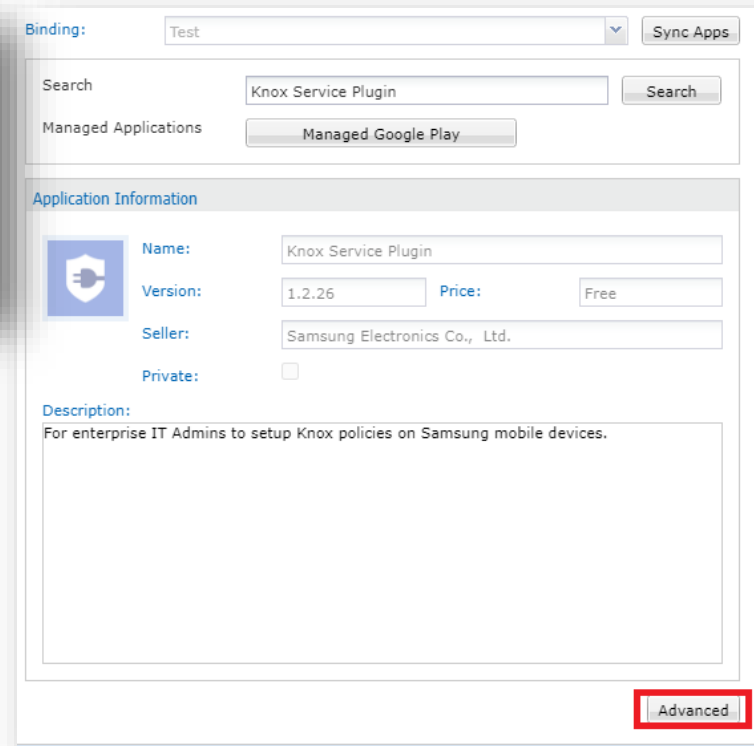
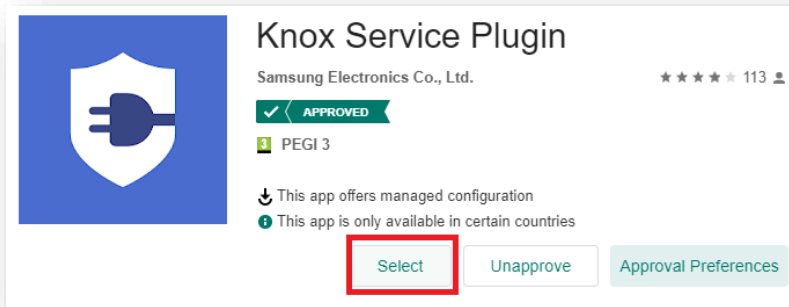
Configure Knox Platform for Enterprise using Knox Service Plugin

- Select Add, then Managed Google Play Applications
- Click Managed Google Play
- Search for and Approve the Knox Service Plugin
- Choose how you would like to handle new app permissions, select Done



Configure Knox Platform for Enterprise using Knox Service Plugin

- Click Select then Advanced
- Set Application Type to Mandatory and click Enable App Configuration
- Copy and Paste your KPE License key into the KPE premium field if you would like use the premium features
- Once you have enabled your required settings, select OK



Configure Knox Platform for Enterprise using Knox Service Plugin

- Click OK
- Select Next


Add/Edit Application Catalog Entry

Binding:

Search

Managed Applications

Application Information

 **Name:**

Version: **Price:**


Seller:

Private: ☐

Description:

Create Application Catalog Rule

Select the applications that you want to appear in the Application Catalog.

Name	Version	Type	URL	Product Con...	Approval St...	
Managed Google Play Applications (1 Item)						
 Knox S...	1.2.26	Sugges...	https://play.google.com/w...	{"profileName...	Approved	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Configure Knox Platform for Enterprise using Knox Service Plugin

- Choose your target device group, select Next
- Select Finish

Create Application Catalog Rule

Select the device(s) and/or device group(s) that the rule should target.

My Company

- DeX KSP demo
- ☒ Management Devices
- Sales Devices
- Warehouse Devices

Device Name
<input checked="" type="checkbox"/> AndroidPlus 00015

Page 1 of 1

☐ Child Selected ☒ Parent Selected ☒ Selected 1 Total Device(s) Targeted

Back **Next** Cancel Help

Create Application Catalog Rule

Name	Value
Type	Application Catalog
Name	Knox Service Plugin
Status	Enabled
Activate Date	2020-07-29 3:16:29 PM
Target Device Groups	\\My Company\Management Devices\
Managed Google Play Applications	Knox Service Plugin v1.2.26 https://play.google.com/work/apps/details?id=com.sam...

Advanced

Back **Finish** Cancel Help

This is version 2.1 of this document.

Thank you!

