SOTI MobiControl v15.4.1.4828

&

Knox Platform for Enterprise

February 2022

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
   - Dedicated Device
4. Android Enterprise configuration
5. Work Profile enrollment flow
6. Fully Managed enrollment flow
7. Fully Managed with a Work Profile enrollment flow
8. Work Profile on a Company-owned Device enrollment flow
9. Dedicated Device configuration
10. Configure Knox Service Plugin [KSP] Standard and Premium

SOTI Collateral & Contacts

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

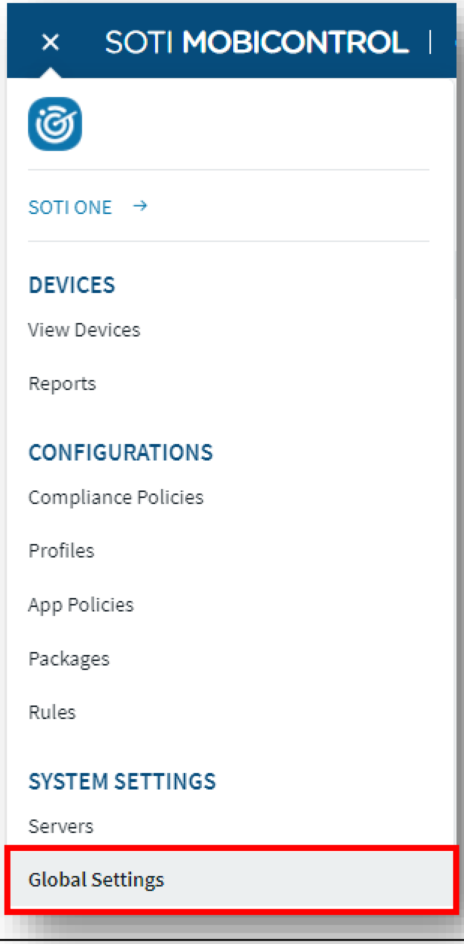
https://www.soti.net/mc/help/v15.1/en/start.html

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 Enterprise Bindings in the Android section**
- **Select the Add button to configure and bind your Managed Enterprise**



SOTI MOBICONTROL

SOTI ONE →

DEVICES

View Devices

Reports

CONFIGURATIONS

Compliance Policies

Profiles

App Policies

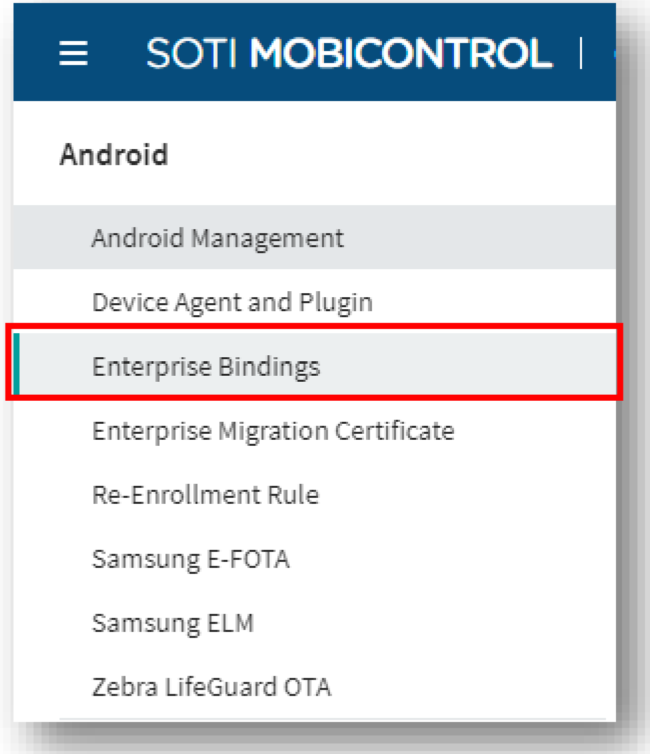
Packages

Rules

SYSTEM SETTINGS

Servers

Global Settings



SOTI MOBICONTROL

Android

Android Management

Device Agent and Plugin

Enterprise Bindings

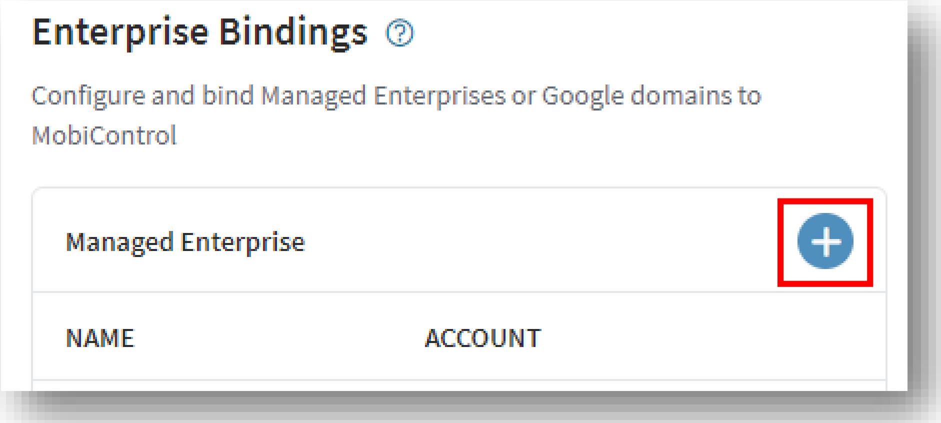
Enterprise Migration Certificate

Re-Enrollment Rule

Samsung E-FOTA

Samsung ELM

Zebra LifeGuard OTA



Enterprise Bindings

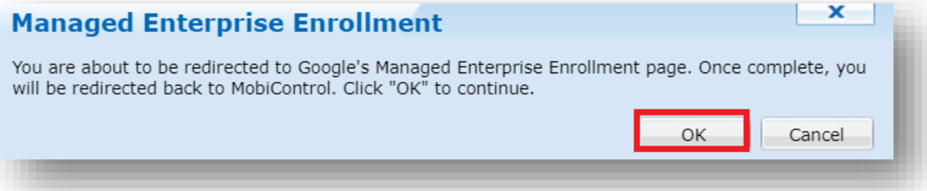
Configure and bind Managed Enterprises or Google domains to MobiControl

Managed Enterprise

NAME	ACCOUNT

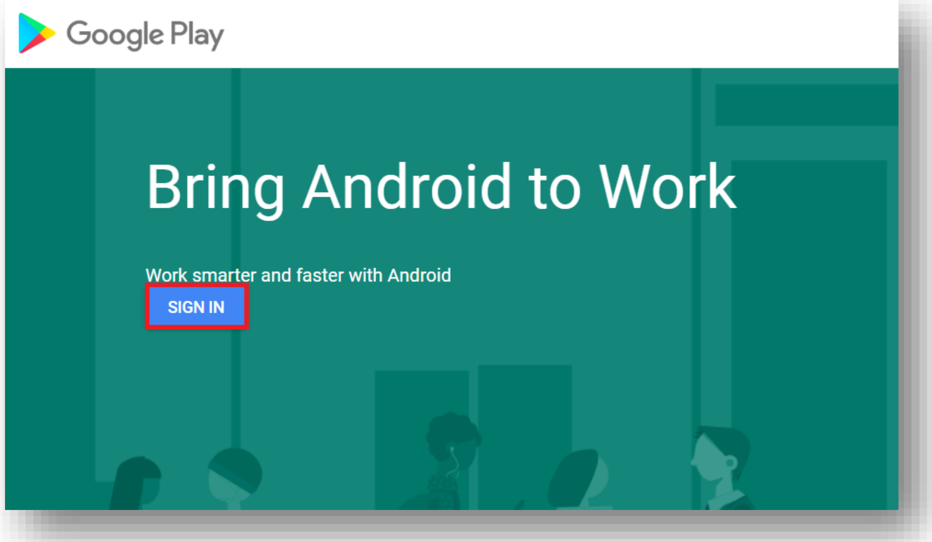
Configure Android Enterprise

- 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.



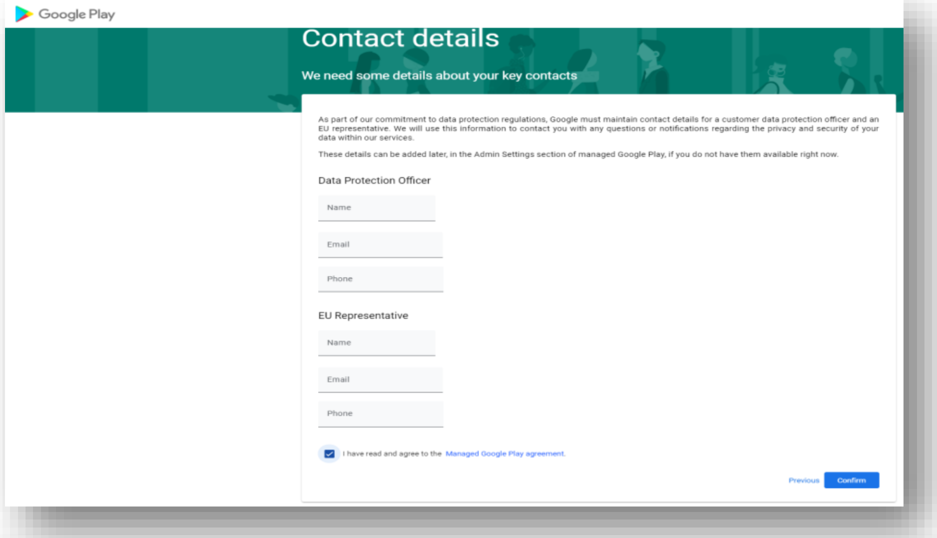
Managed Enterprise Enrollment

You are about to be redirected to Google's Managed Enterprise Enrollment page. Once complete, you will be redirected back to MobiControl. Click "OK" to continue.



Bring Android to Work

Work smarter and faster with Android



Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available right now.

Data Protection Officer

Name

Email

Phone

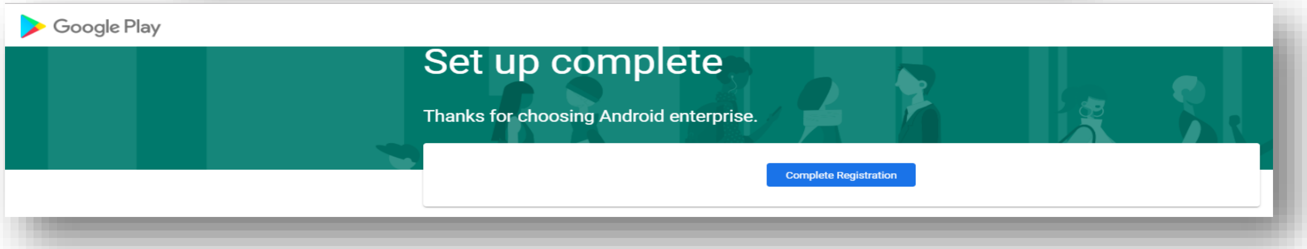
EU Representative

Name

Email

Phone

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



Set up complete

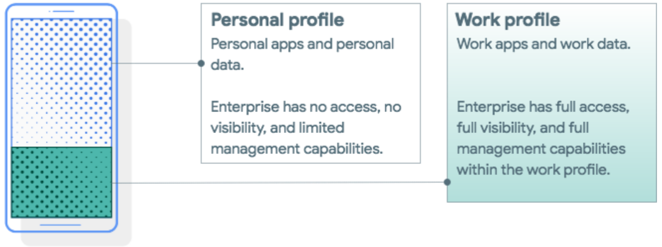
Thanks for choosing Android enterprise.

Android Enterprise Deployment Modes

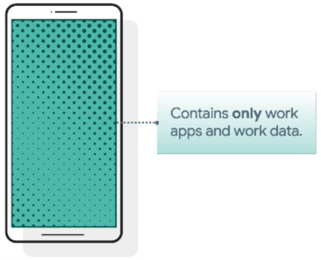
Android Enterprise can be deployed in the following 5 deployment modes:

1. Work Profile [*formerly known as Profile Owner*]
2. Fully Managed Device [*formerly known as Device Owner*]
3. Fully Managed Device with a Work Profile (Not Supported) [*formerly known as COMP*, up to Android 10]
4. Work Profile on Company-owned Device [WPC, on Andoid 11+]
5. Dedicated device [*formerly known as COSU*]

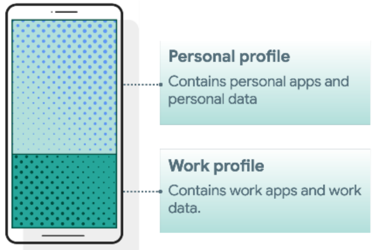
SOTI MobiControl can support all 5 of these deployment modes. In this next section we will show you how to configure each of these 5 deployment modes in SOTI MobiControl for your device fleet.


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.

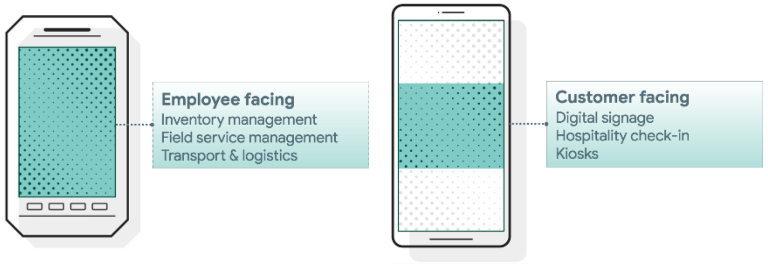
Work Profile



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 or Work Profile on a Company-owned Device

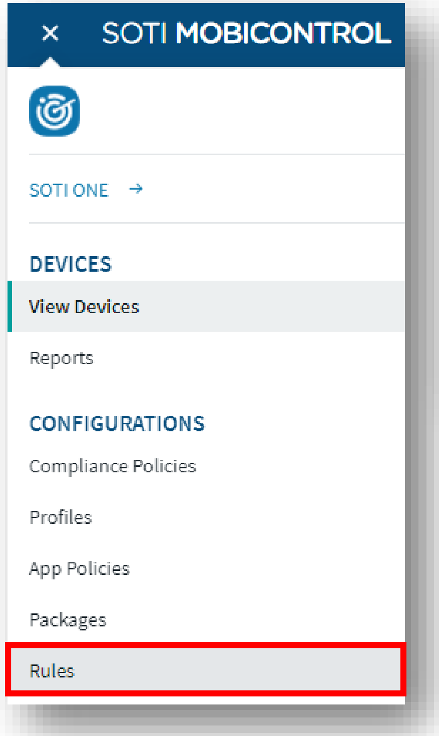


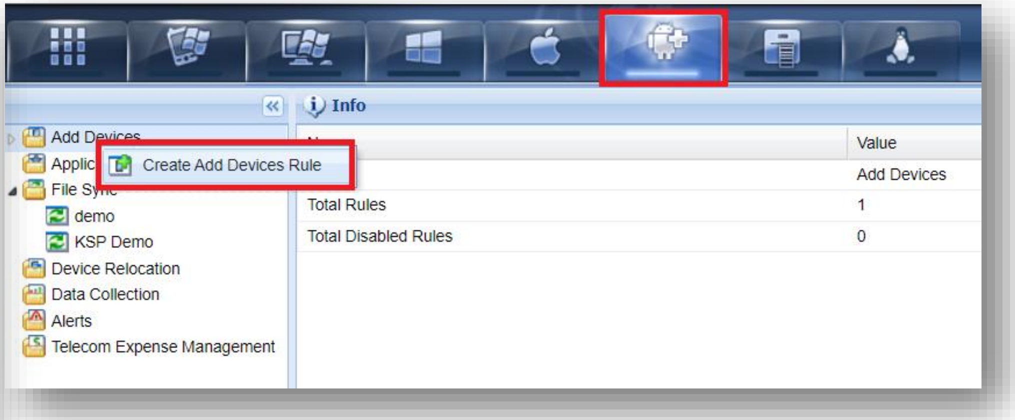
Dedicated Device

Create Android Enterprise Device Rule

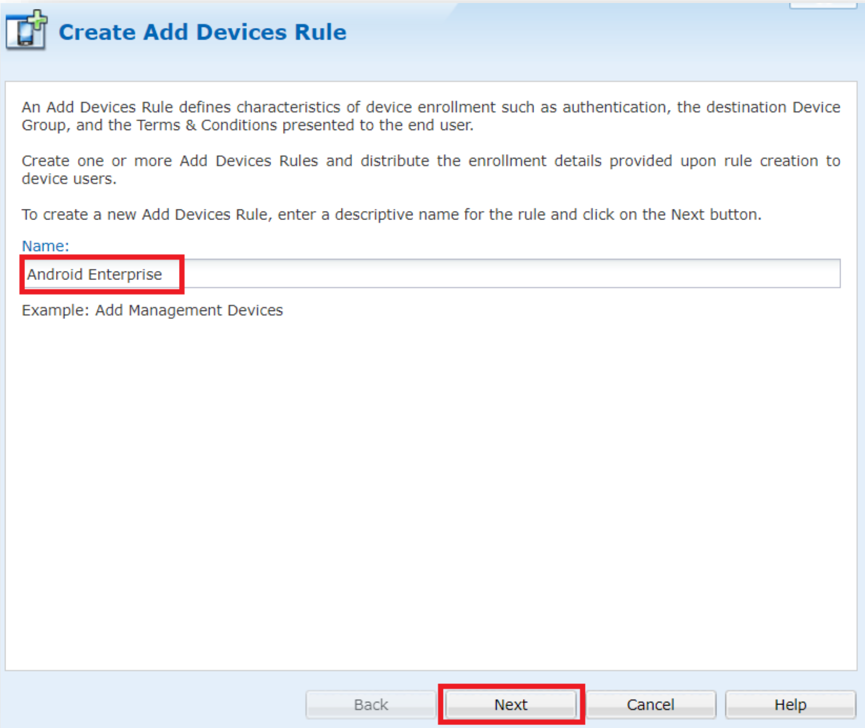
Creating an Android Enterprise Device Rule will enable the enrollment methods Work Profile, Fully Managed, Fully Managed with a Work Profile and Work Profile on Company Owned Device.
The steps below illustrate how this is done.

- **Select Rules from the SOTI MobiControl Menu to enter the legacy console**
- **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**





N	Value
	Add Devices
Total Rules	1
Total Disabled Rules	0



Create Add Devices Rule

An Add Devices Rule defines characteristics of device enrollment such as authentication, the destination Device Group, and the Terms & Conditions presented to the end user.

Create one or more Add Devices Rules and distribute the enrollment details provided upon rule creation to device users.

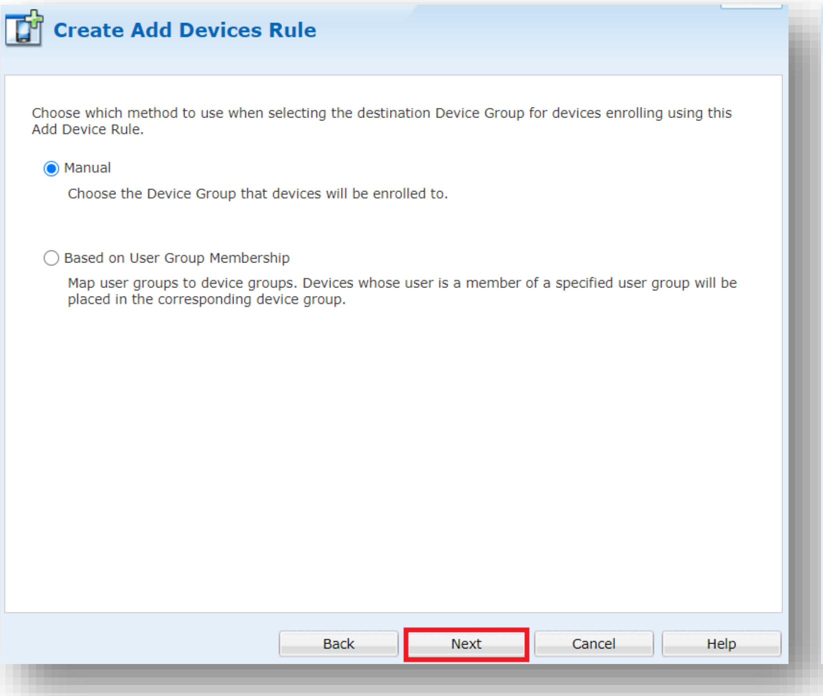
To create a new Add Devices Rule, enter a descriptive name for the rule and click on the Next button.

Name: Android Enterprise

Example: Add Management Devices

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

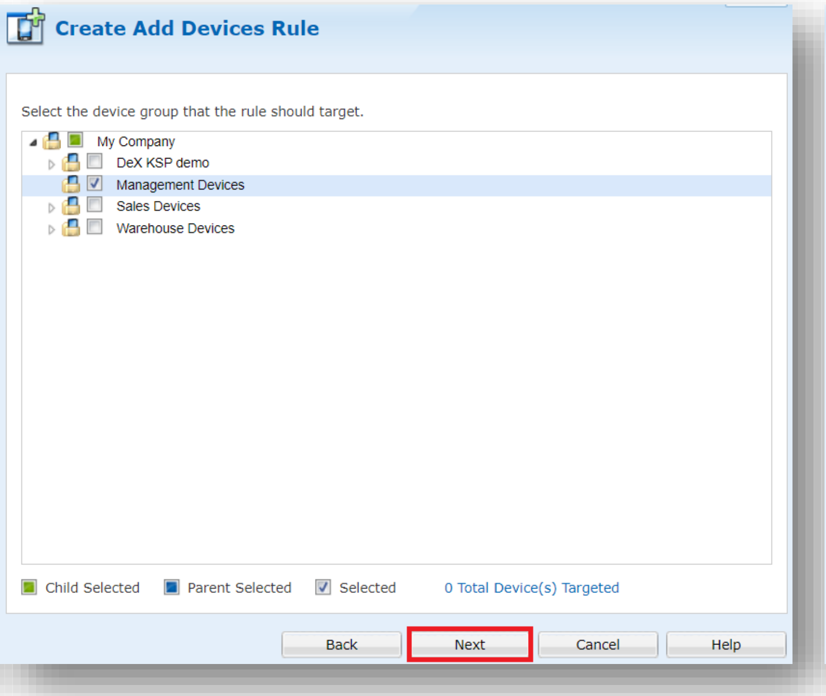
Choose which method to use when selecting the destination Device Group for devices enrolling using this Add Device Rule.

● 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.

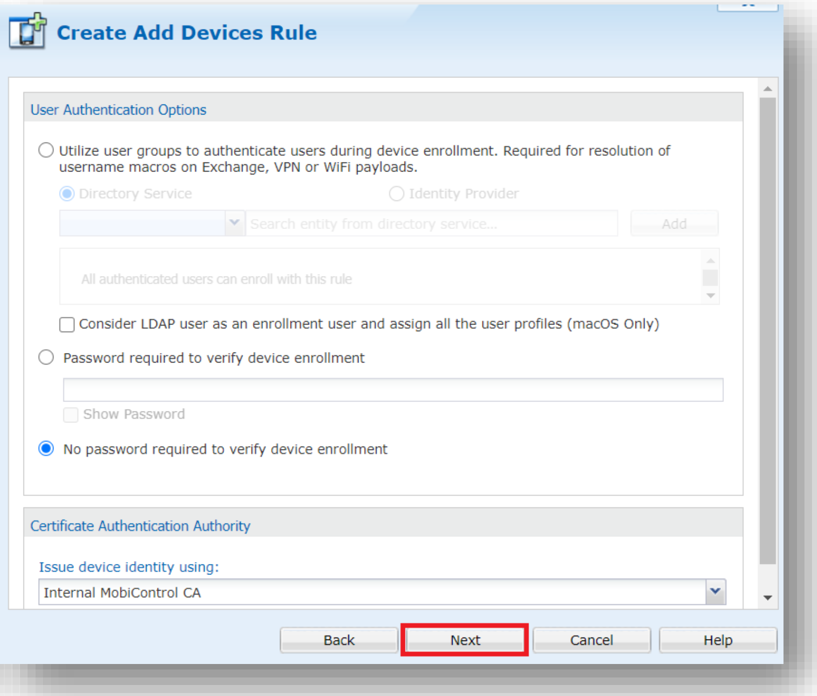


Create Add Devices Rule

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



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...

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

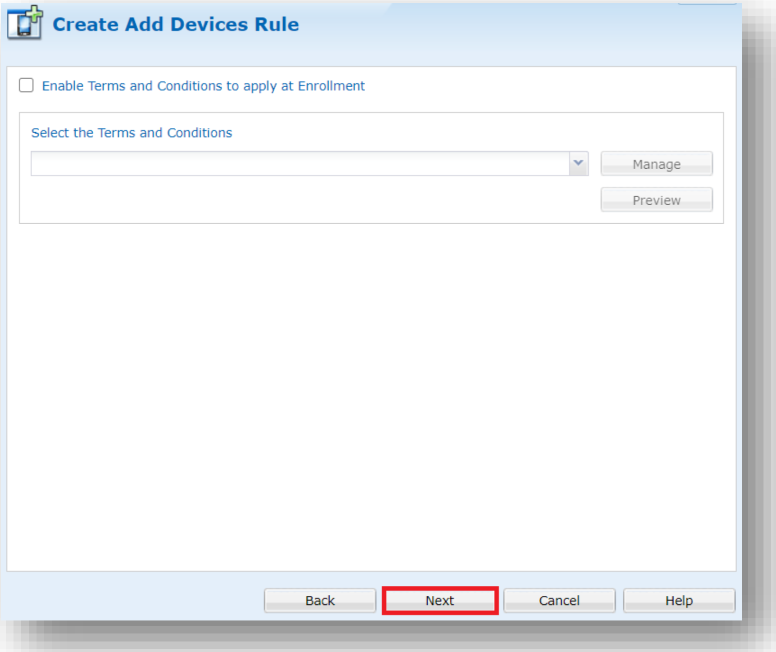
● No password required to verify device enrollment

Certificate Authentication Authority

Issue device identity using: Internal MobiControl CA

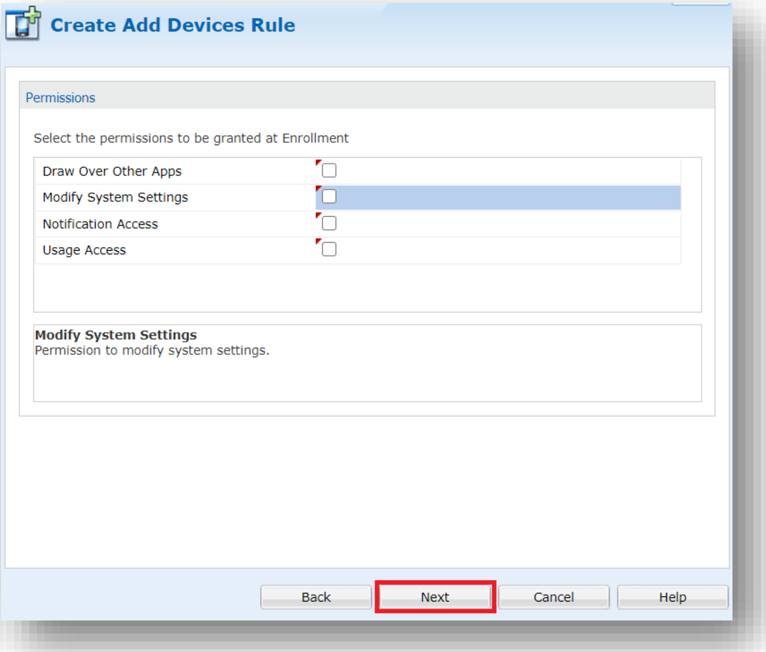
Create Android Enterprise Device Rule

- 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
- For Fully Managed with a Work Profile or Work Profile on Company-owned Device select the Checkbox labelled 'Enroll your fully managed device with a work profile'
- Select Next



☐ Enable Terms and Conditions to apply at Enrollment

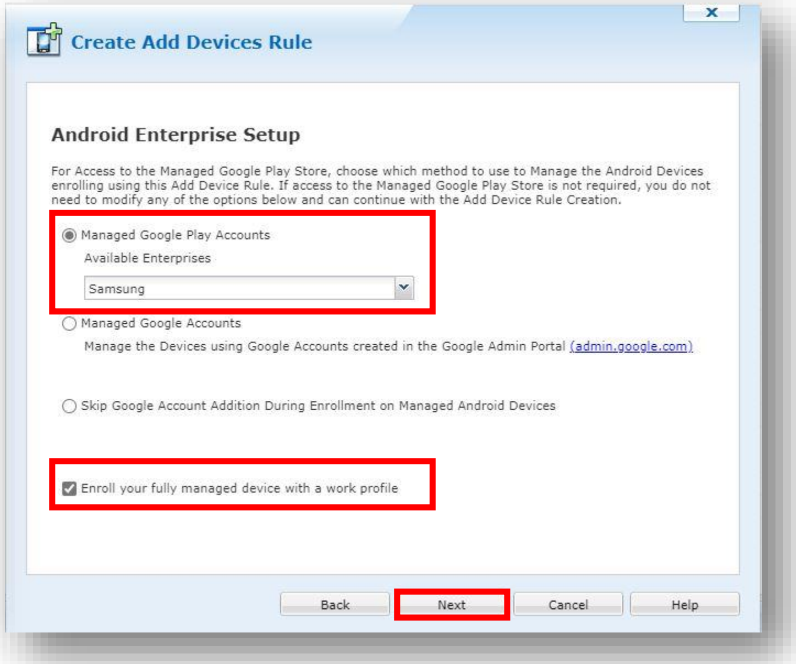
Select the Terms and Conditions



Select the permissions to be granted at Enrollment

Draw Over Other Apps	☐
Modify System Settings	☐
Notification Access	☐
Usage Access	☐

Modify System Settings
Permission to modify system settings.



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

Samsung

○ Managed Google Accounts

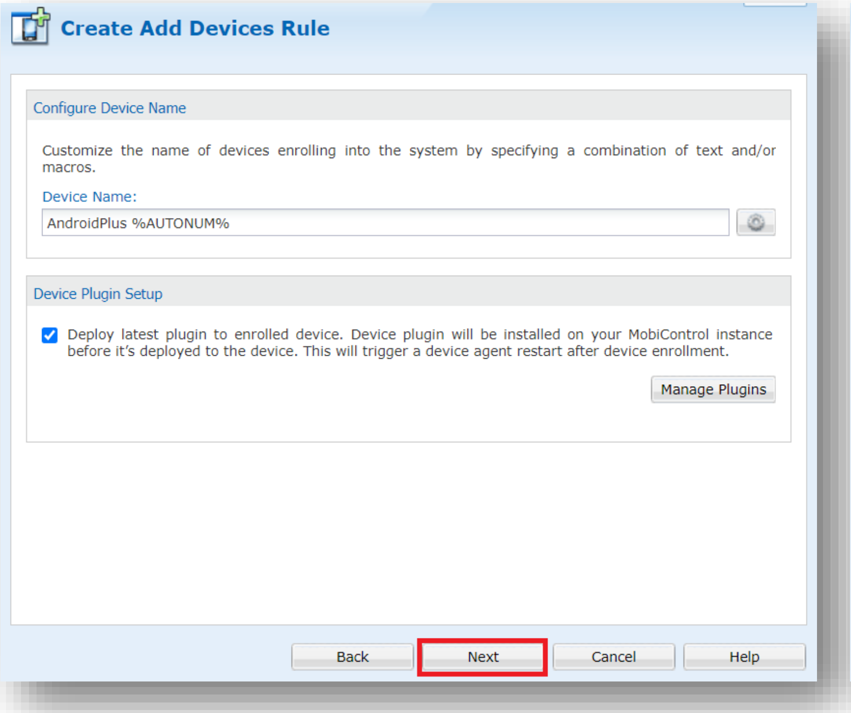
Manage the Devices using Google Accounts created in the Google Admin Portal (admin.google.com)

○ Skip Google Account Addition During Enrollment on Managed Android Devices

☑ Enroll your fully managed device with a work profile

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

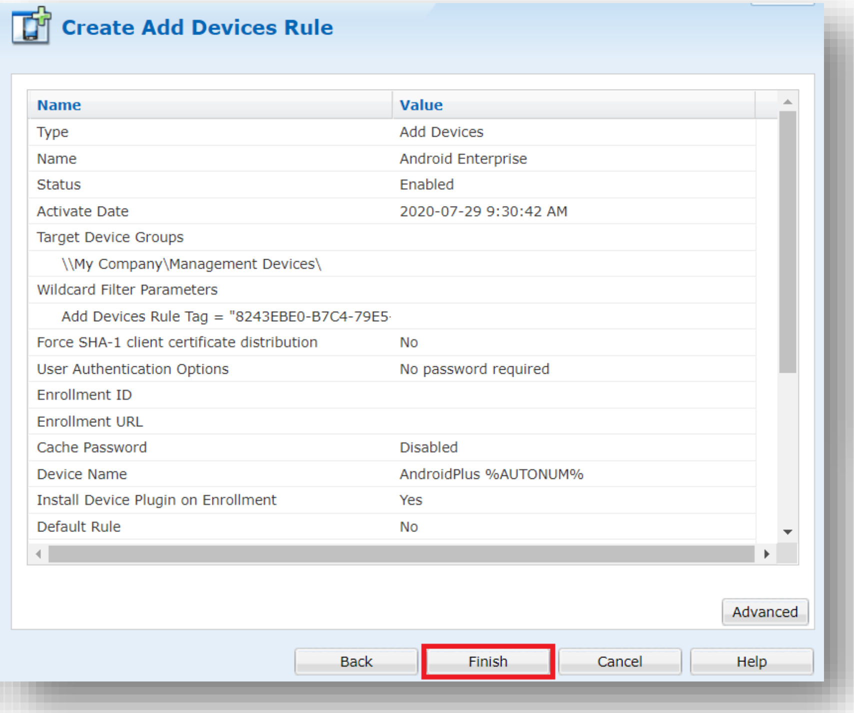
Configure Device Name

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

Device Name: AndroidPlus %AUTONUM%

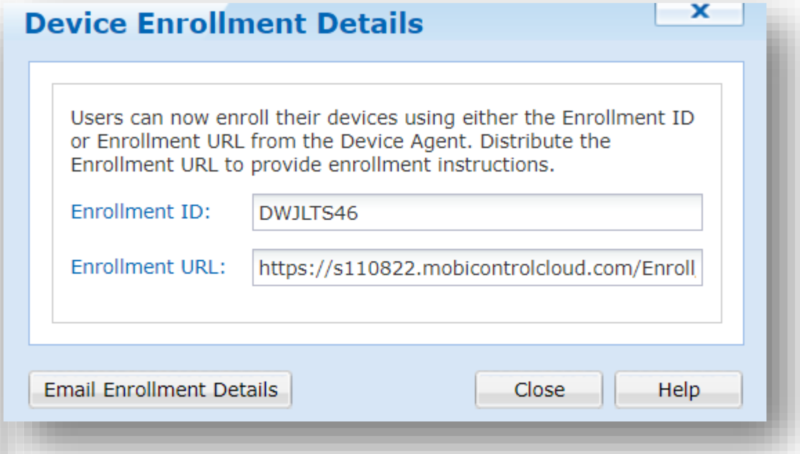
Device Plugin Setup

☑ 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.



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



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

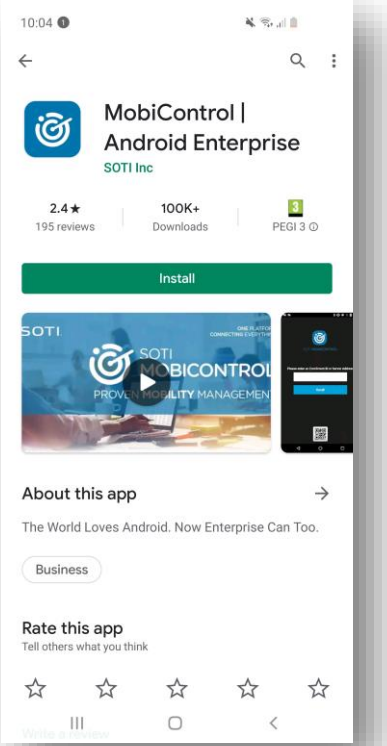
Enrollment URL: https://s110822.mobicontrolcloud.com/Enroll

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 Enrollment ID 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.**



10:04

MobiControl | Android Enterprise

SOTI Inc

2.4★ 195 reviews | 100K+ Downloads | PEGI 3

Install

About this app

The World Loves Android. Now Enterprise Can Too.

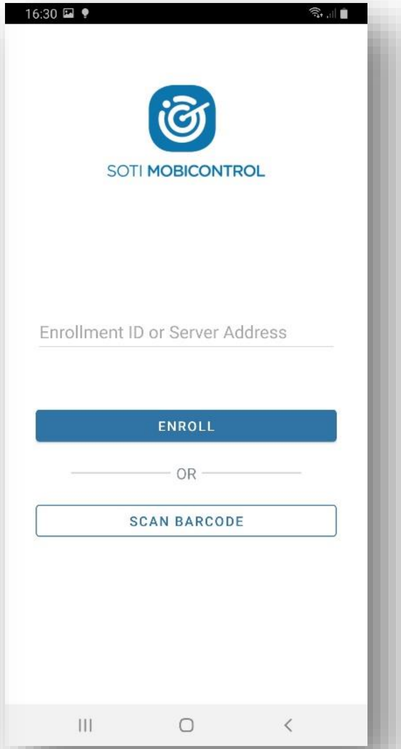
Business

Rate this app

Tell others what you think

☆ ☆ ☆ ☆ ☆

Install MobiControl
from the Google Play Store



16:30

SOTI MOBICONTROL

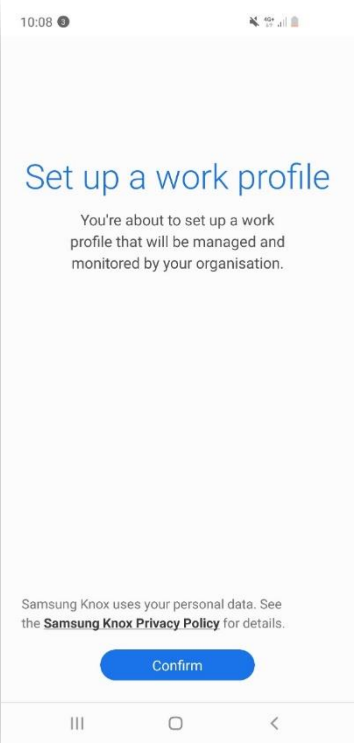
Enrollment ID or Server Address

ENROLL

OR

SCAN BARCODE

Open MobiControl, enter
Your Enrollment ID and select ENROLL



10:08

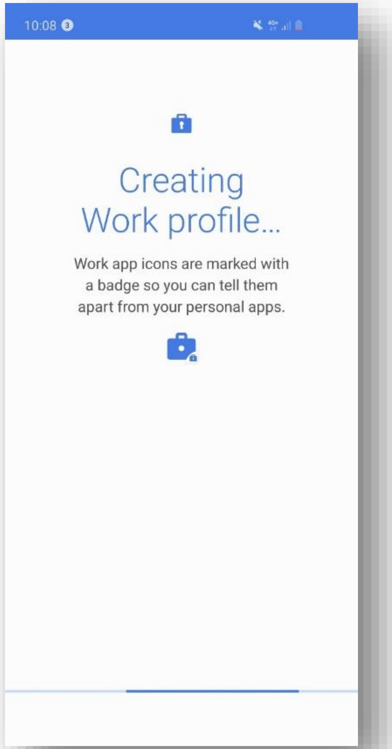
Set up a work profile

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

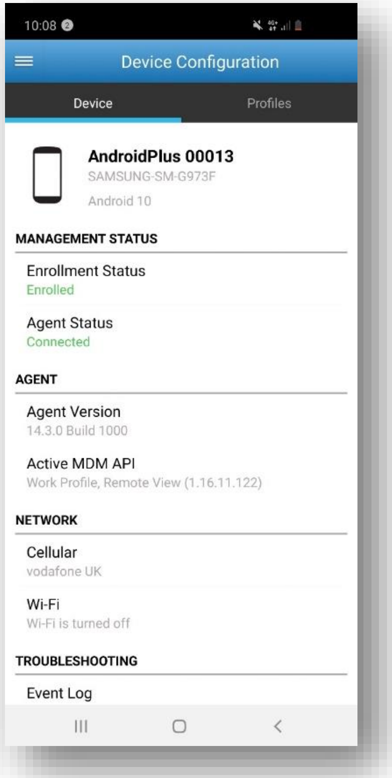


10:08

Creating Work profile...

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

Wait, Work Profile
Will now configure



10:08

Device Configuration

Device | Profiles

AndroidPlus 00013
SAMSUNG-SM-G973F
Android 10

MANAGEMENT STATUS

Enrollment Status
Enrolled

Agent Status
Connected

AGENT

Agent Version
14.3.0 Build 1000

Active MDM API
Work Profile, Remote View (1.16.11.122)

NETWORK

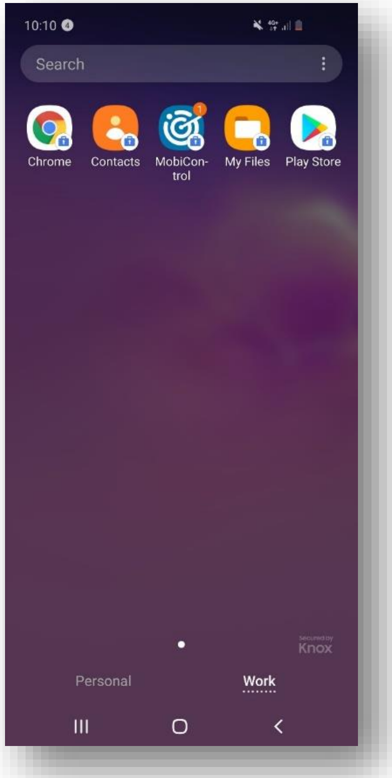
Cellular
vodafone UK

Wi-Fi
Wi-Fi is turned off

TROUBLESHOOTING

Event Log

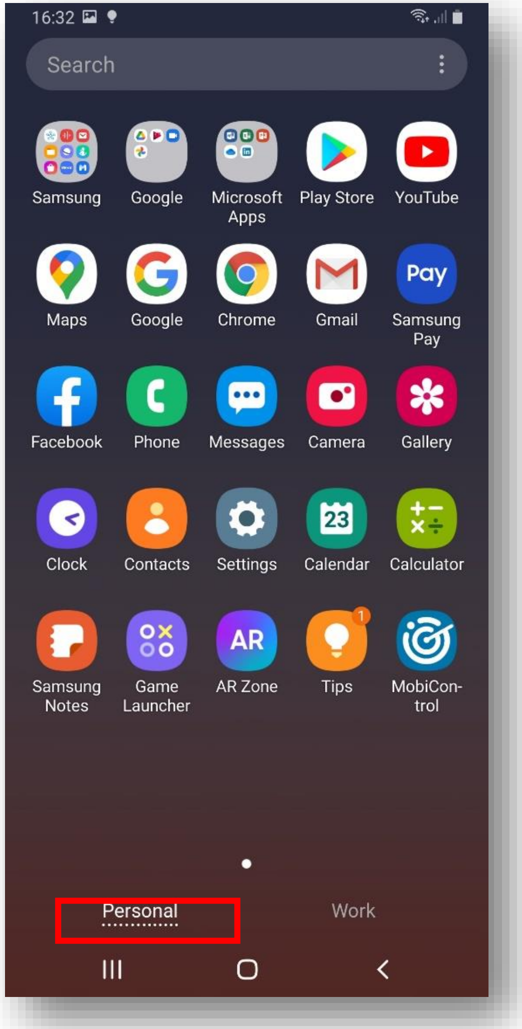
Your device is now enrolled,
tap the home button



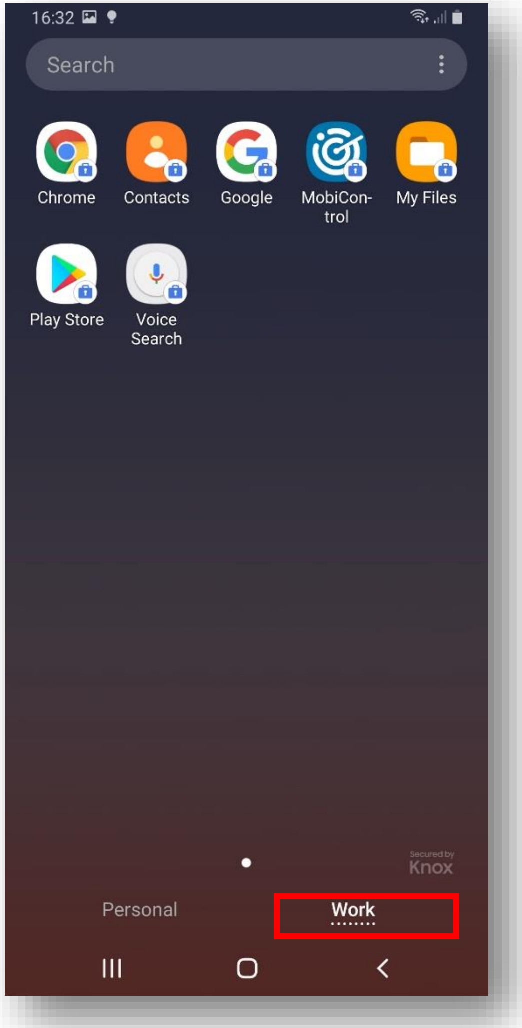
Work and Personal
profiles are now separate

Android Enterprise: Work Profile Enrollment

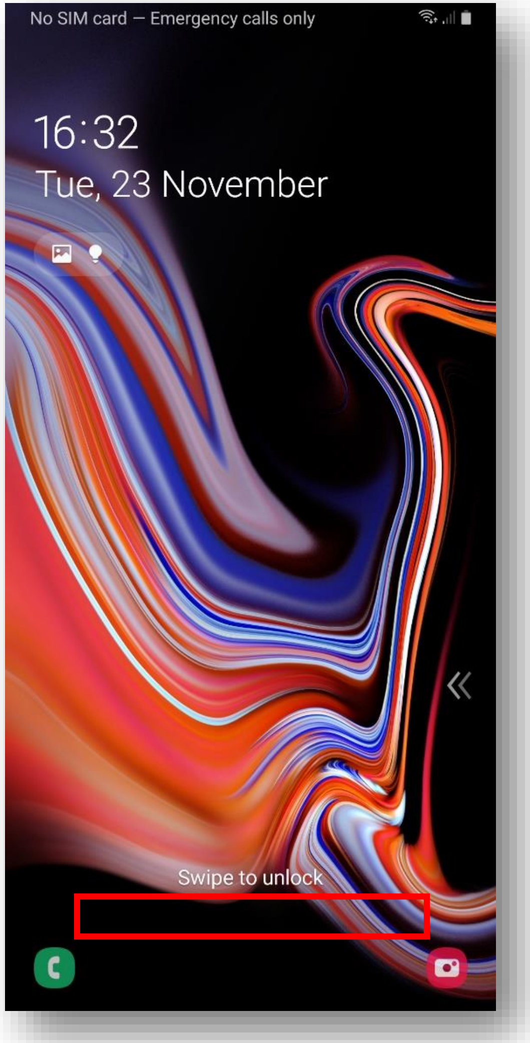
How to tell that Work Profile has been successfully set up:



Personal Tab



Work Tab



No mention of device belonging to your organization on lock screen

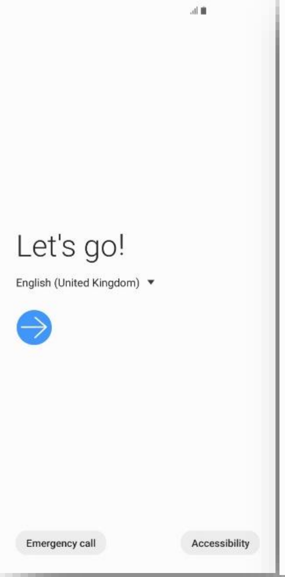
Android Enterprise: Fully Managed Enrollment

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. Make sure the 'Enroll your fully managed device with a work profile' box was not checked when creating the rule.

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

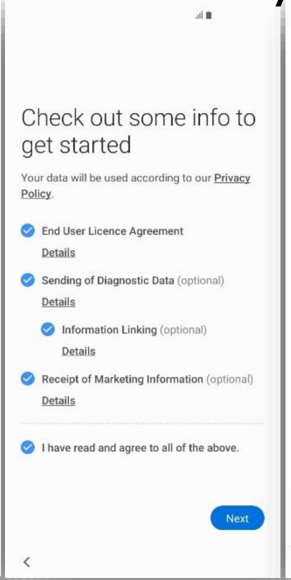
- **Below is a screen-by-screen play to enroll your device using the DPC Identifier method.**



Let's go!

English (United Kingdom) ▾

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

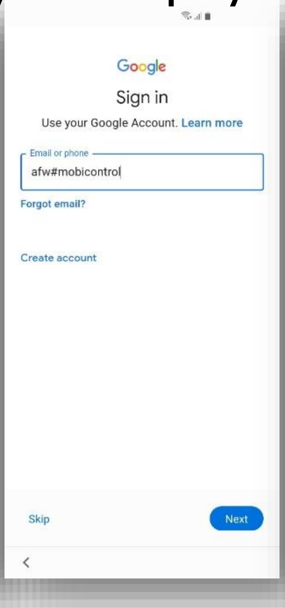
☑ Sending of Diagnostic Data (optional)
Details

☑ Information Linking (optional)
Details

☑ Receipt of Marketing Information (optional)
Details

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

Accept the EULA, Next



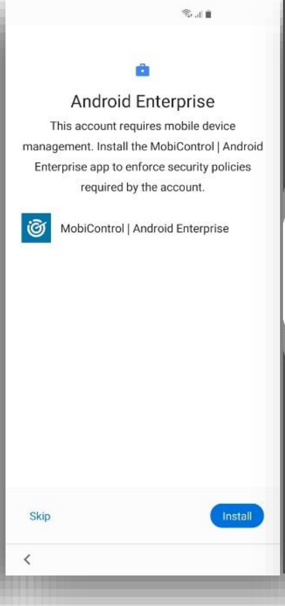
Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#mobicontrol

Enter afw#mobicontrol then select Next

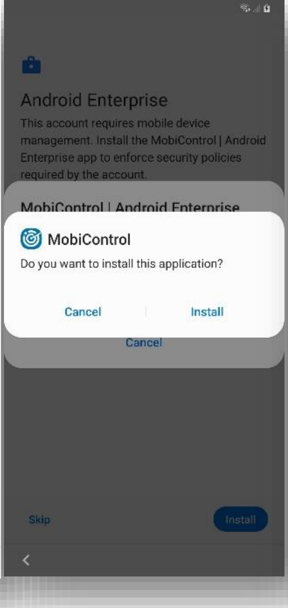


Android Enterprise

This account requires mobile device management. Install the MobiControl | Android Enterprise app to enforce security policies required by the account.

MobiControl | Android Enterprise

Install



Android Enterprise

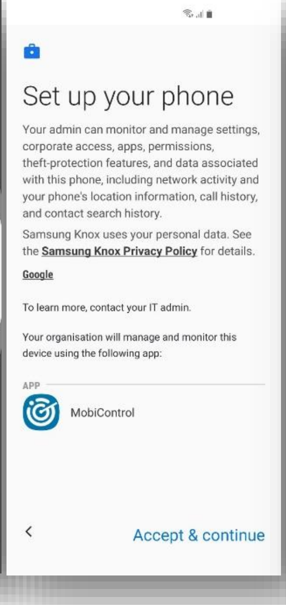
This account requires mobile device management. Install the MobiControl | Android Enterprise app to enforce security policies required by the account.

MobiControl | Android Enterprise

MobiControl

Do you want to install this application?

Install



Set up your phone

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information, call history, and contact search history.

Samsung Knox uses your personal data. See the Samsung Knox Privacy Policy for details.

Google

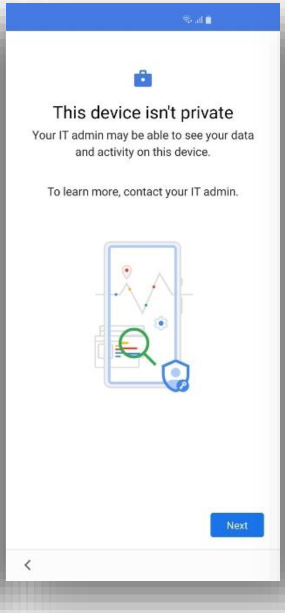
To learn more, contact your IT admin.

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

APP

MobiControl

Accept & continue

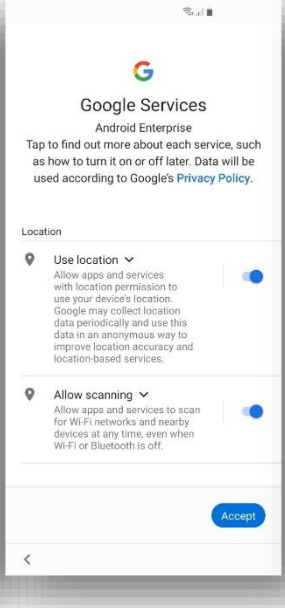


This device isn't private

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

To learn more, contact your IT admin.

Next



Google Services

Android Enterprise

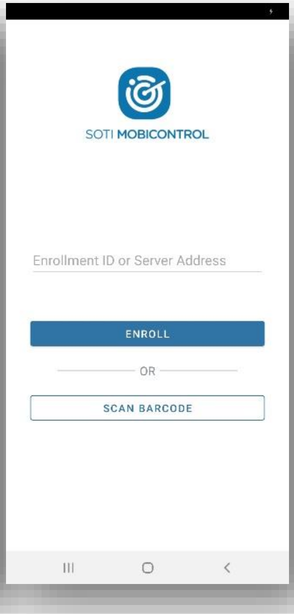
Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

Location

Use location: Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services. ●

Allow scanning: Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off. ●

Accept



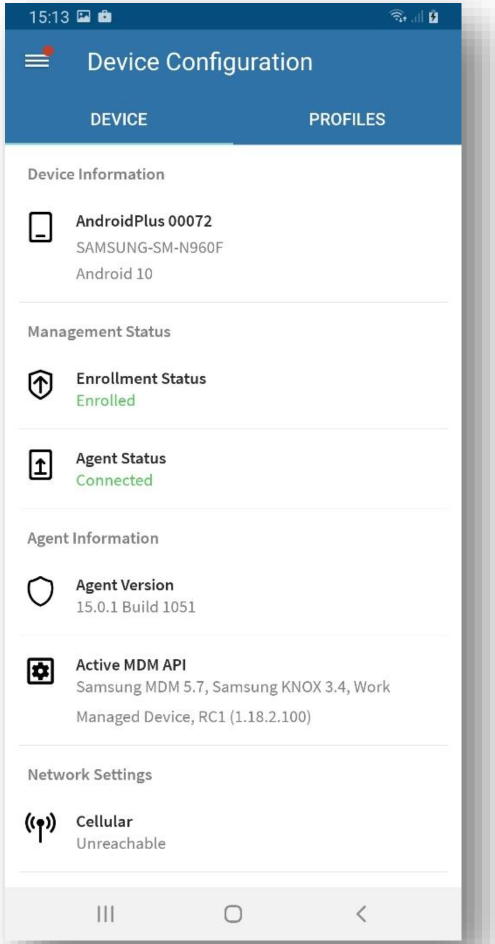
SOTI MOBICONTROL

Enrollment ID or Server Address

Enter your Enrollment ID, ENROLL

Android Enterprise: Fully Managed Device Enrollment

How to tell that a Fully Managed Device has been successfully set up:



15:13

Device Configuration

DEVICE | PROFILES

Device Information

AndroidPlus 00072
SAMSUNG-SM-N960F
Android 10

Management Status

Enrollment Status
Enrolled

Agent Status
Connected

Agent Information

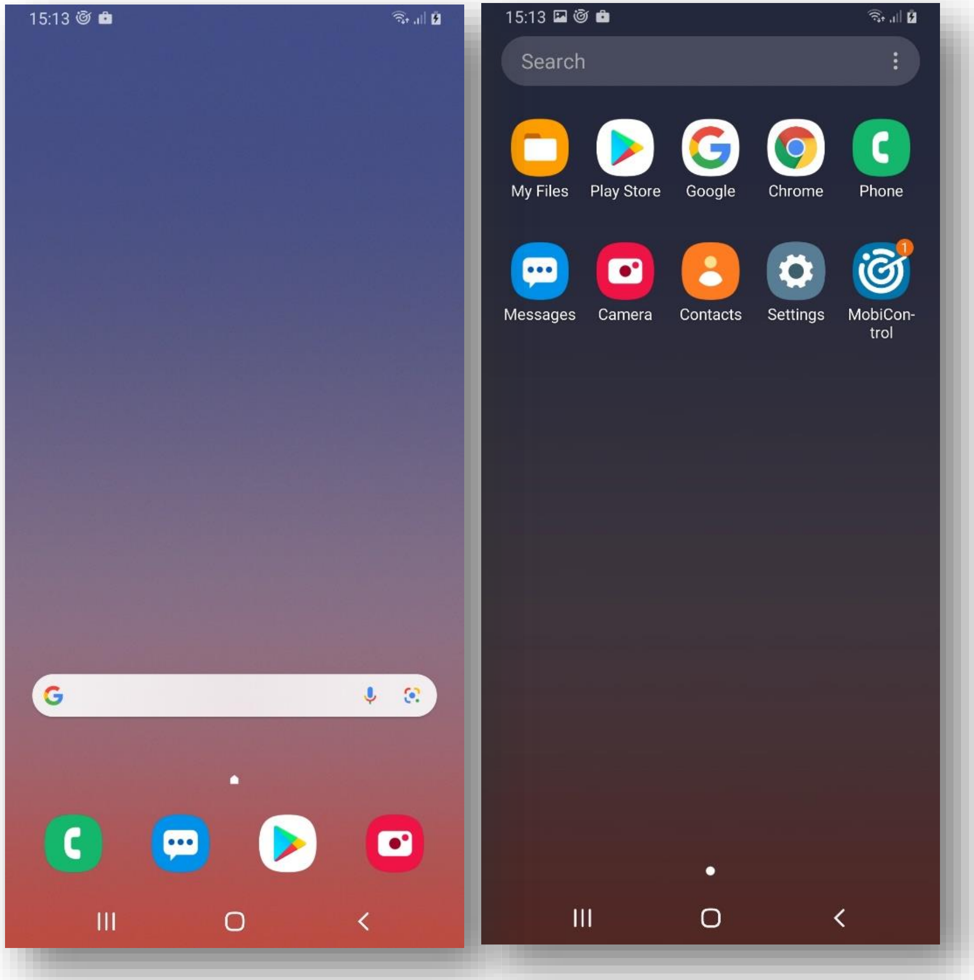
Agent Version
15.0.1 Build 1051

Active MDM API
Samsung MDM 5.7, Samsung KNOX 3.4, Work Managed Device, RC1 (1.18.2.100)

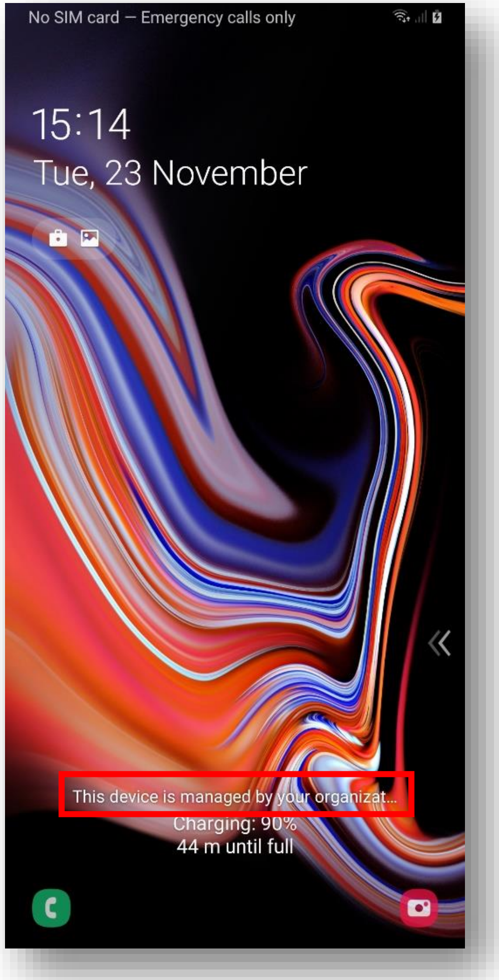
Network Settings

Cellular
Unreachable

Device is successfully enrolled



Sparse set of applications
including MobiControl



No SIM card – Emergency calls only

15:14
Tue, 23 November

This device is managed by your organizat...
Charging: 90%
44 m until full

Device belongs
to your organization
on lock screen

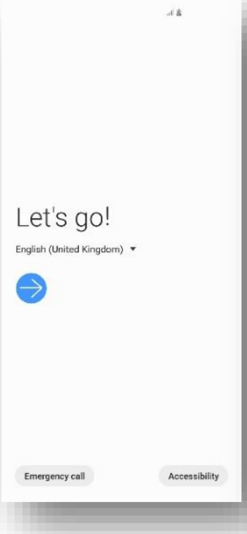
Android Enterprise: Fully Managed with a Work Profile Enrollment

To enroll your device as an Android Enterprise Fully Managed 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 SOTI MobiControl as an Android Enterprise Fully Managed Device with a Work Profile. Use an 'Android Enterprise Rule' configuration that had the 'Enroll your fully managed device with a work profile' box checked.

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

Note: this is only supported on Android 10 and below.

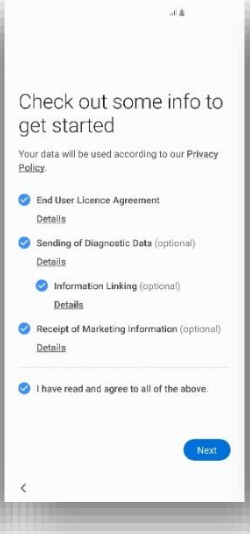
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Let's go!

English (United Kingdom)

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

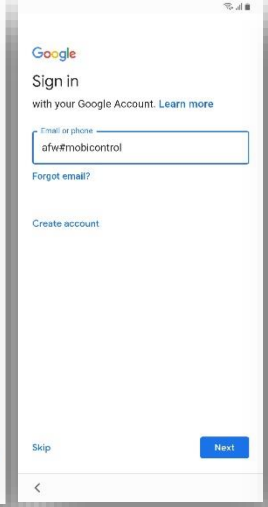
☑ Sending of Diagnostic Data (optional)
Details

☑ Information Linking (optional)
Details

☑ Receipt of Marketing Information (optional)
Details

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

Accept the EULA, Next



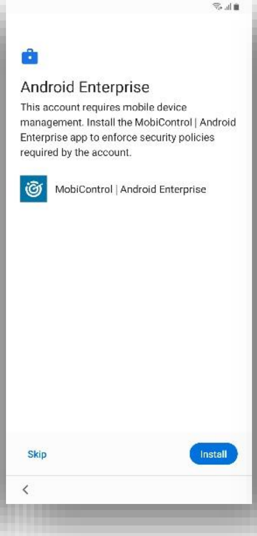
Google

Sign in

with your Google Account. Learn more

Email or phone: afw#mobicontrol

Enter afw#mobicontrol then select Next

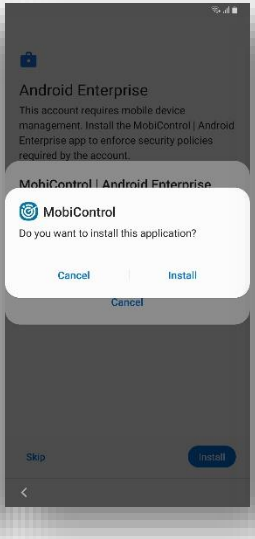


Android Enterprise

This account requires mobile device management. Install the MobiControl | Android Enterprise app to enforce security policies required by the account.

MobiControl | Android Enterprise

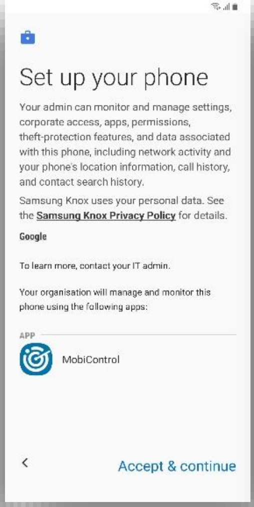
Install



MobiControl

Do you want to install this application?

Install



Set up your phone

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information, call history, and contact search history.

Samsung Knox uses your personal data. See the Samsung Knox Privacy Policy for details.

Google

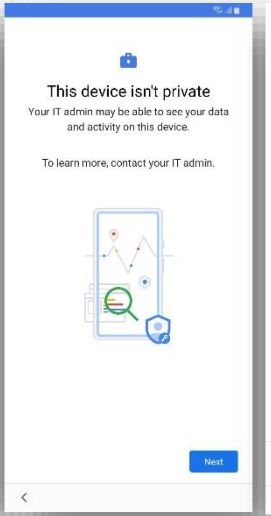
To learn more, contact your IT admin.

Your organisation will manage and monitor this phone using the following apps:

APP

MobiControl

Accept & continue

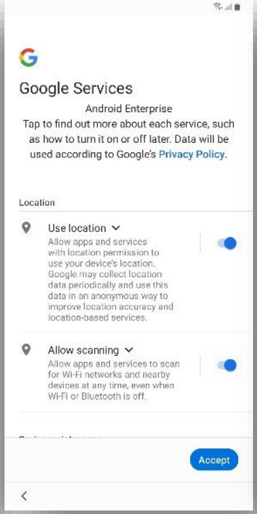


This device isn't private

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

To learn more, contact your IT admin.

Next



Google Services

Android Enterprise

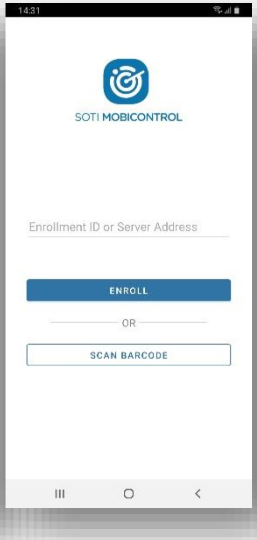
Tap to find out more about each service, such as how to turn it on or off later. Data will be used according to Google's Privacy Policy.

Location

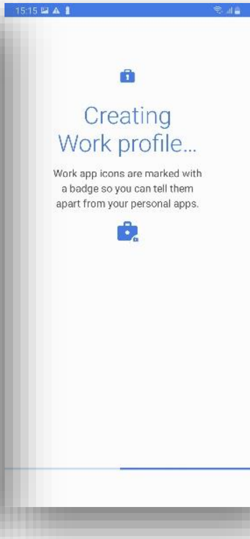
Use location
Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Allow scanning
Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

Accept



Enter your Enrollment ID and select ENROLL



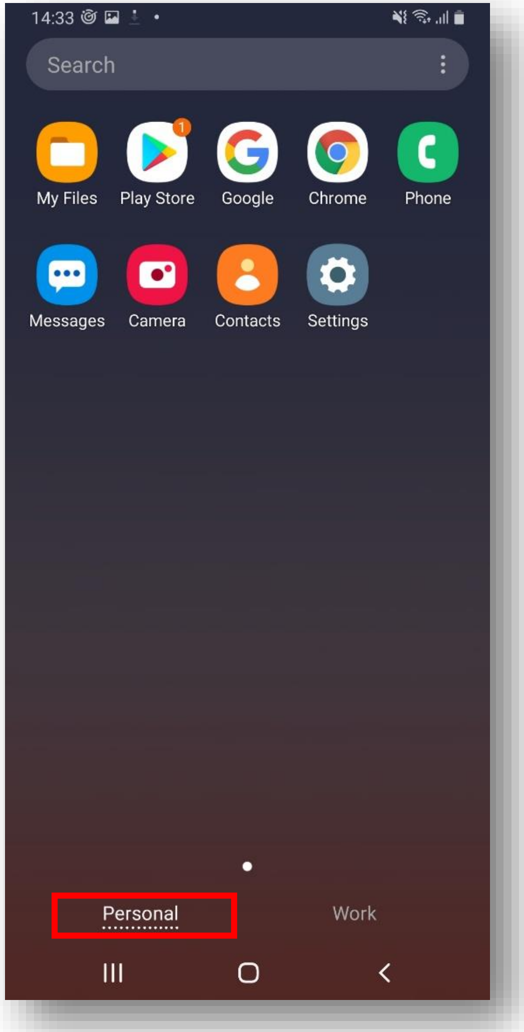
Creating Work profile...

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

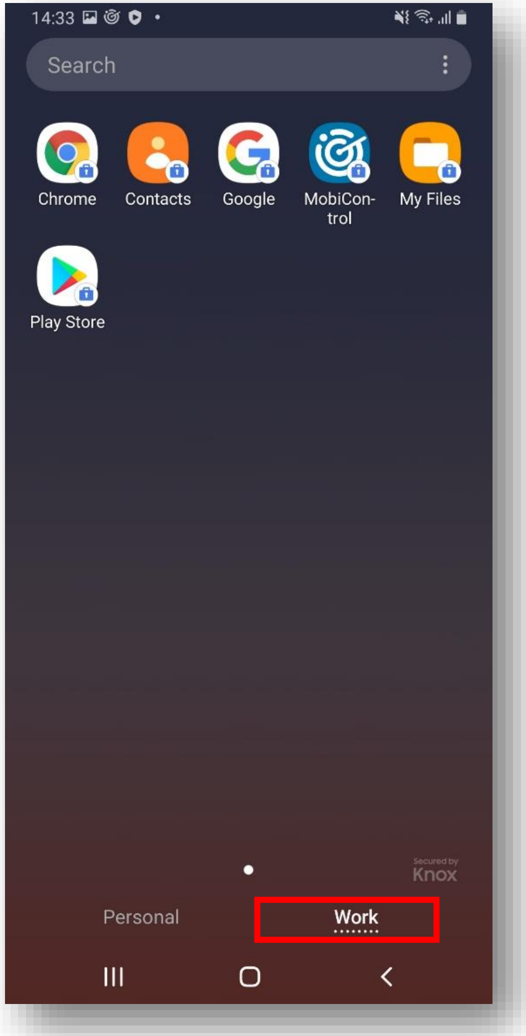
Creating Work profile...

Android Enterprise: Fully Managed with a Work Profile Enrollment

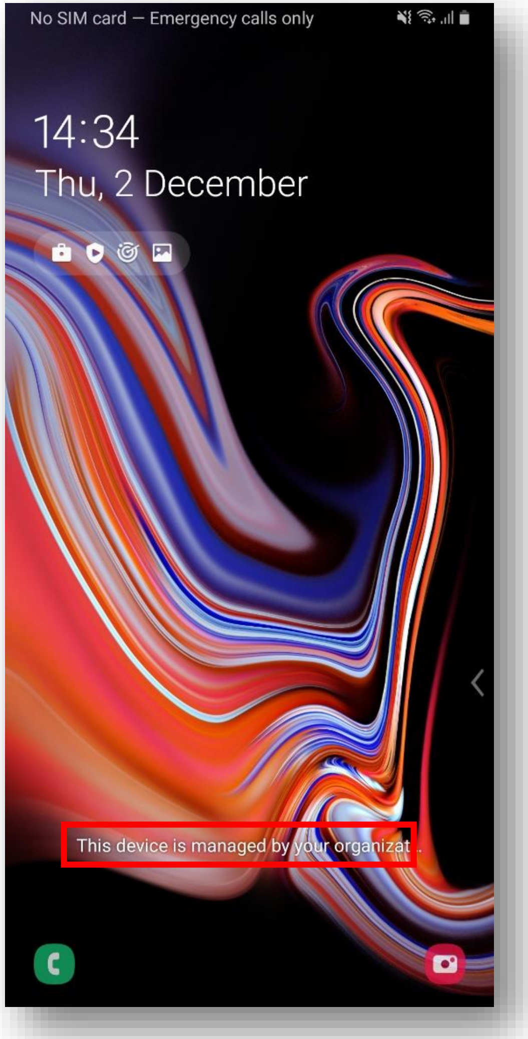
How to tell that Fully Managed with a Work Profile has been successfully set up:



Personal Tab



Work Tab



This device is managed by your organizat

Device is managed by your organization on lock screen

Android Enterprise: Work Profile on a Company Owned Device Enrollment

To enroll your device as an Android Enterprise Work Profile on a 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 SOTI MobiControl as an Android Enterprise Work Profile on a Company Owned Device. Use an 'Android Enterprise Rule' configuration that had the 'Enroll your fully managed device with a work profile' box checked.

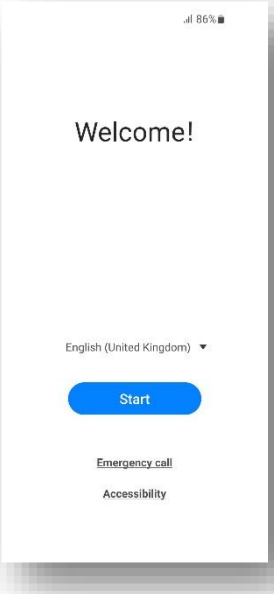
1. DPC Identifier [Also known as the hashtag method] afw#mobicontrol

2. QR Code Enrollment / NFC Enrollment

3. Knox Mobile Enrollment

Note: this is only supported on Android 12 and above. * Android 11 is not supported *****

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



Welcome!

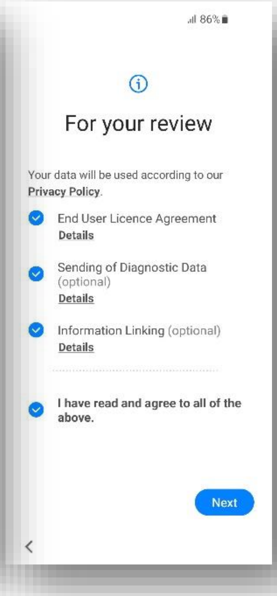
English (United Kingdom) ▾

Start

Emergency call

Accessibility

Select Start



For your review

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement
Details

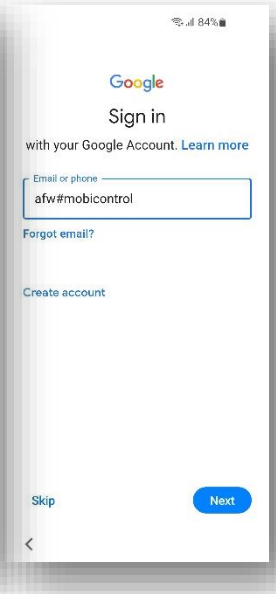
☑ Sending of Diagnostic Data (optional)
Details

☑ Information Linking (optional)
Details

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

Next

Review the Terms and Conditions and select Next



Google

Sign in

with your Google Account. Learn more

Email or phone: afw#mobicontrol

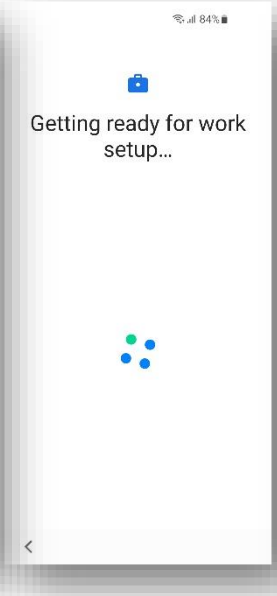
Forgot email?

Create account

Skip

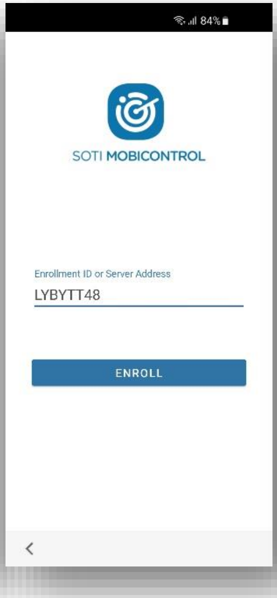
Next

Enter afw#mobicontrol select Next



Getting ready for work setup...

Getting ready for work setup...

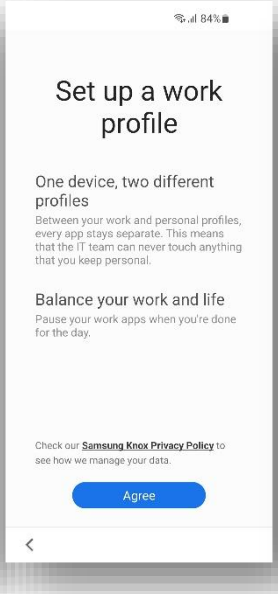


SOTI MOBICONTROL

Enrollment ID or Server Address: LYBYTT48

ENROLL

Enter your Enrollment ID, select ENROLL



Set up a work profile

One device, two different profiles

Between your work and personal profiles, every app stays separate. This means that the IT team can never touch anything that you keep personal.

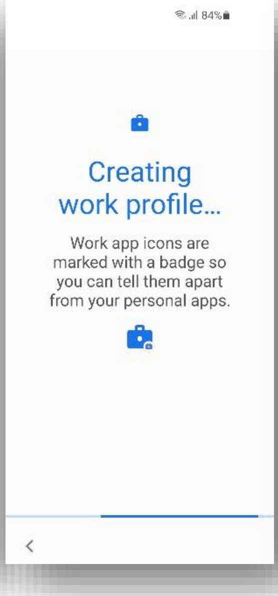
Balance your work and life

Pause your work apps when you're done for the day.

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

Agree

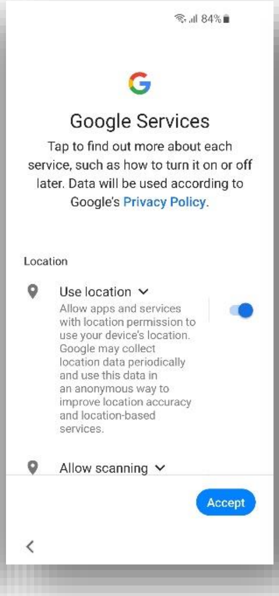
Set up a work profile, select Agree



Creating work profile...

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

Creating work profile...



Google Services

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.

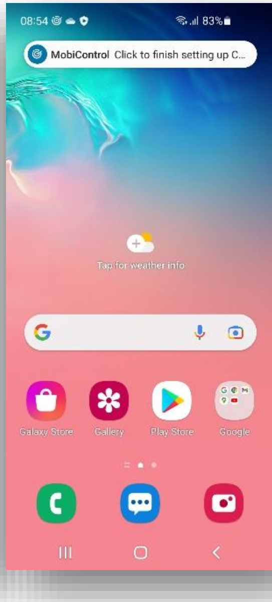
Location

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 ⌄

Accept

Accept Google Services



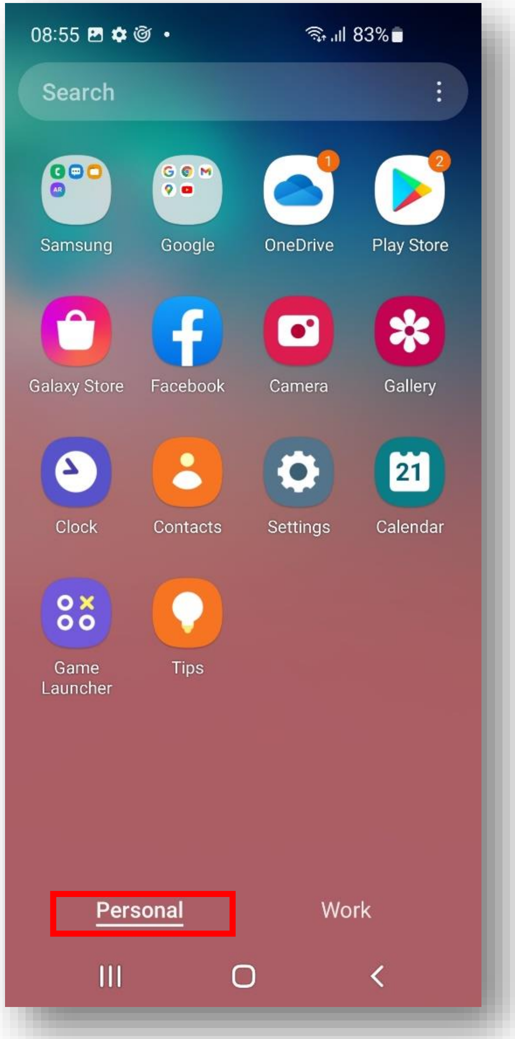
08:54

MobiControl Click to finish setting up C...

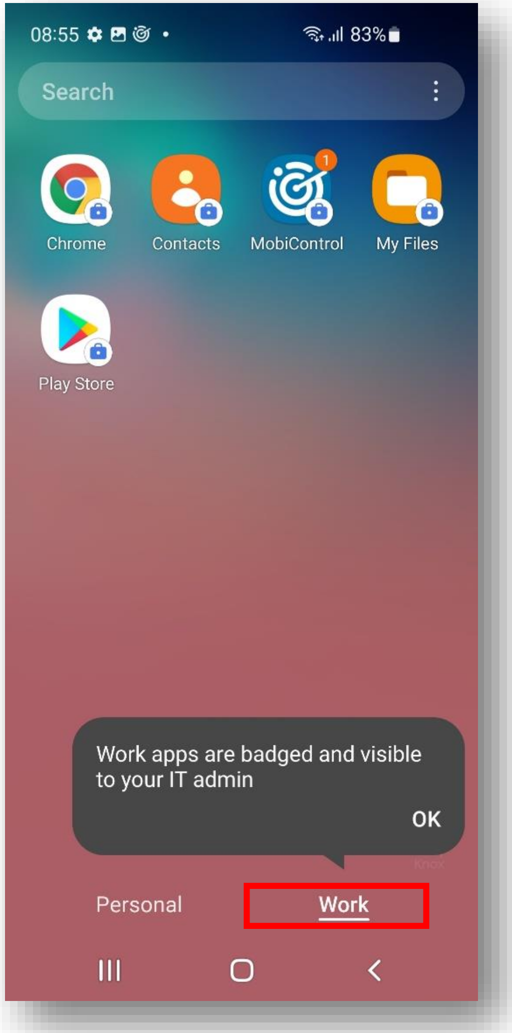
Installation complete

Android Enterprise: Work Profile on a Company Owned Device Enrollment

How to tell that Work Profile on a Company Owned Device has been successfully set up:



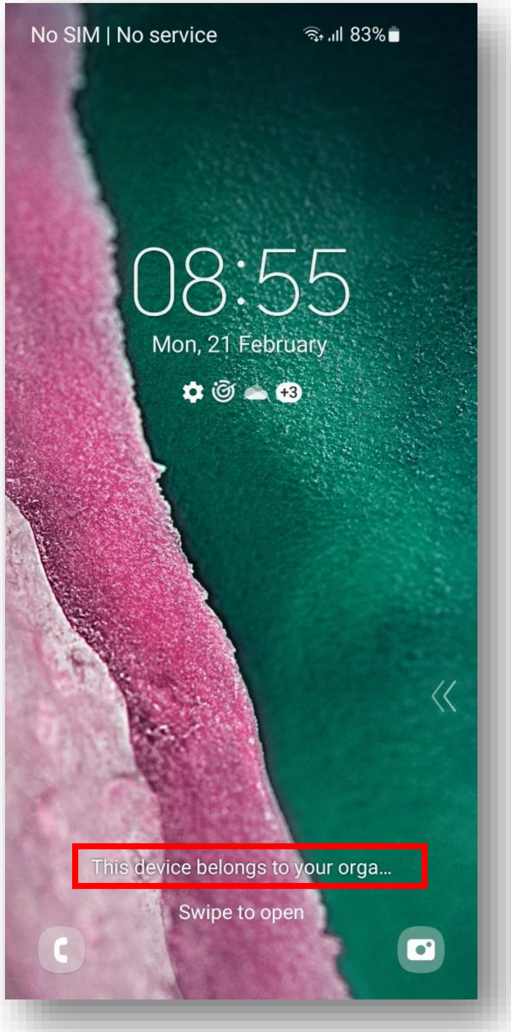
Personal Tab



Work apps are badged and visible to your IT admin

OK

Work Tab



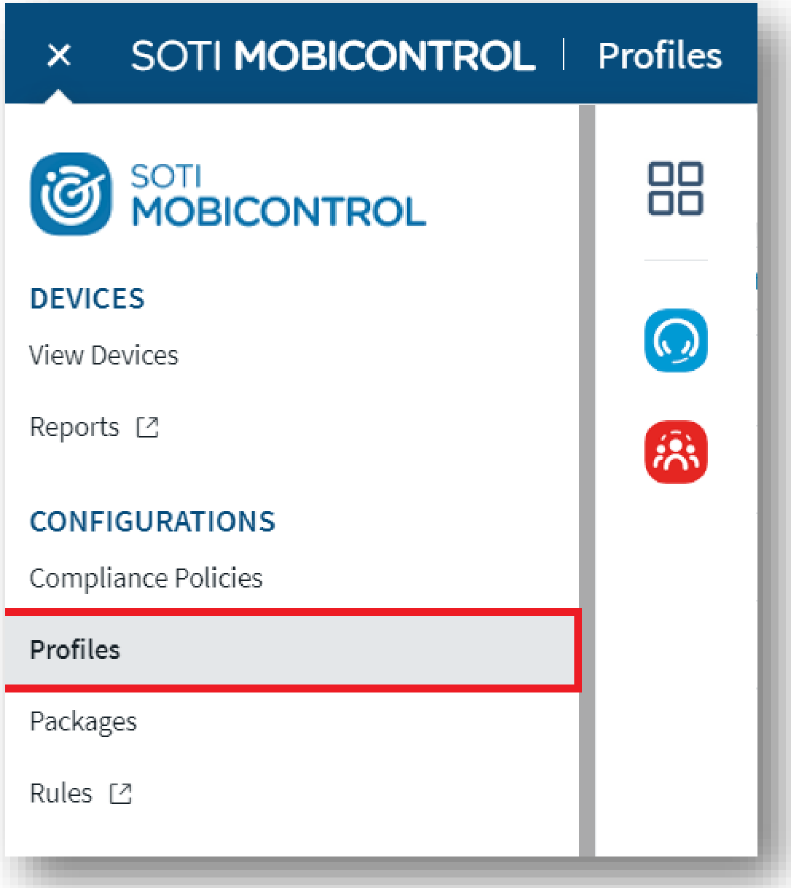
This device belongs to your orga...

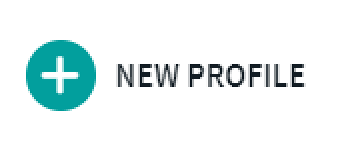
Device belongs to your organization on lock screen

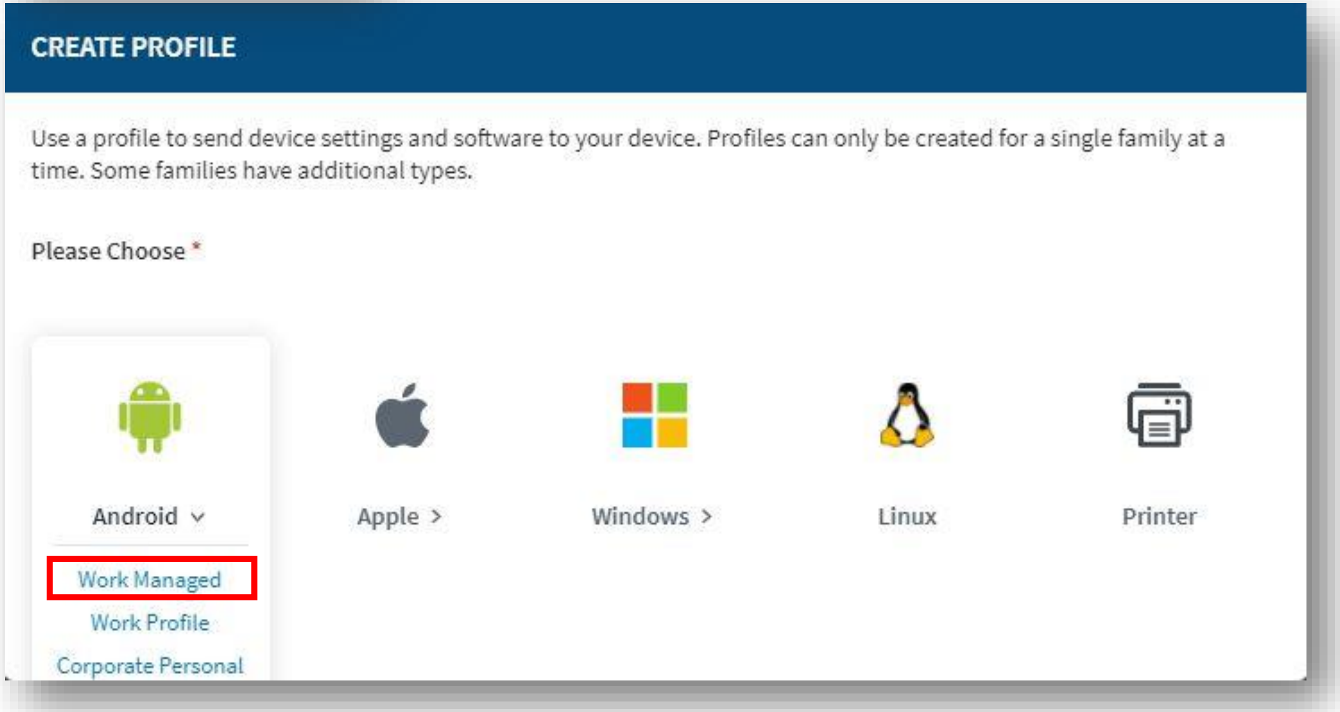
Android Enterprise: Dedicated Device Configuration

Knox

- 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







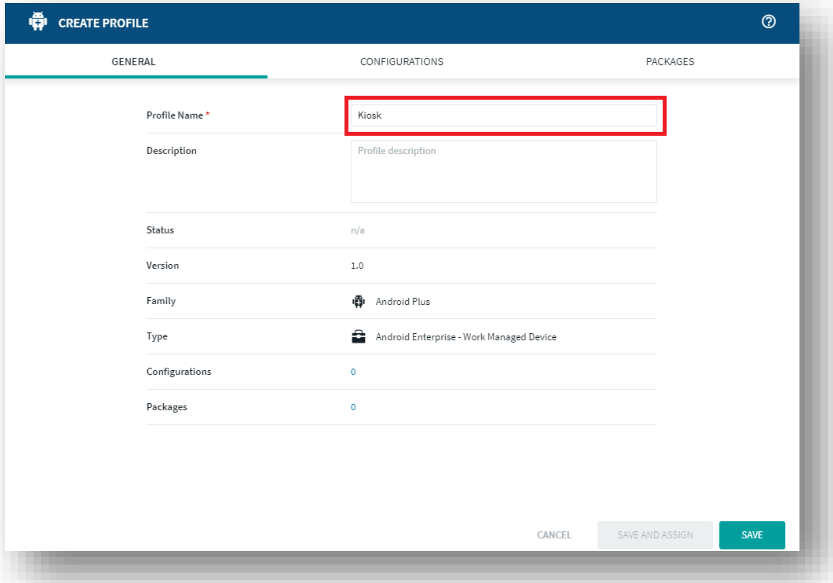
CREATE PROFILE

Use a profile to send device settings and software to your device. Profiles can only be created for a single family at a time. Some families have additional types.

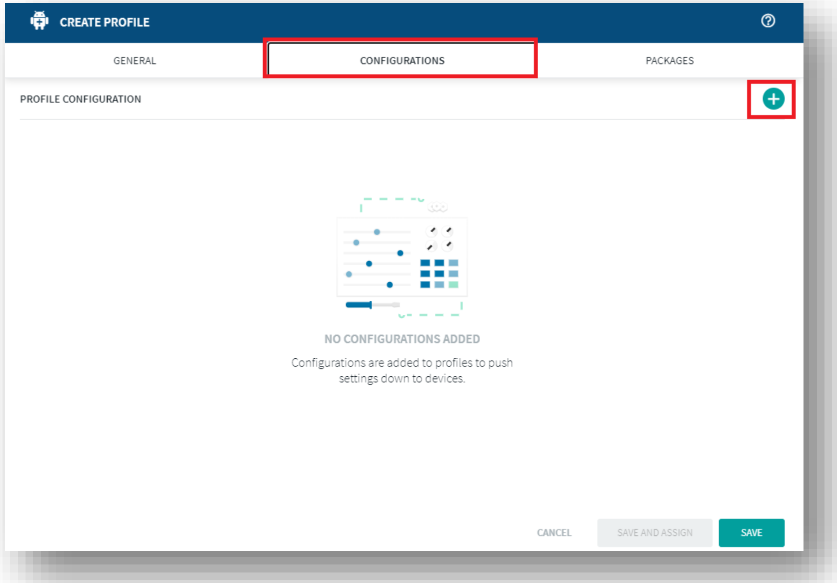
Please Choose *

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

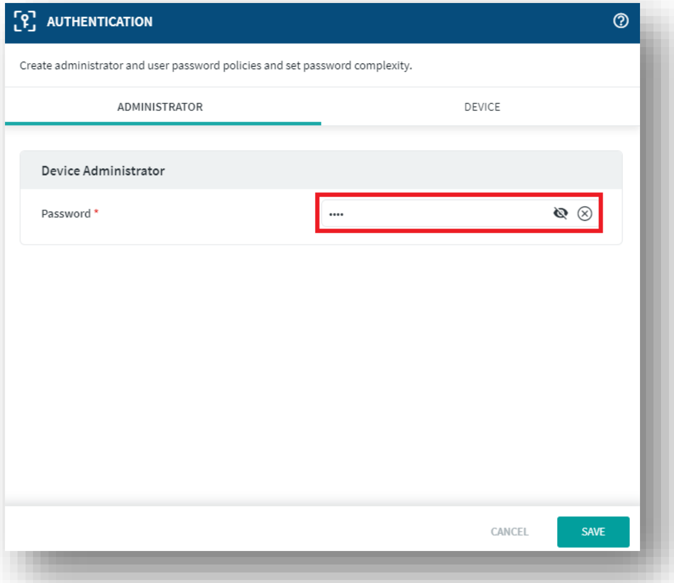


Profile Name *	Kiosk
Description	Profile description
Status	n/a
Version	1.0
Family	Android Plus
Type	Android Enterprise - Work Managed Device
Configurations	0
Packages	0



NO CONFIGURATIONS ADDED

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



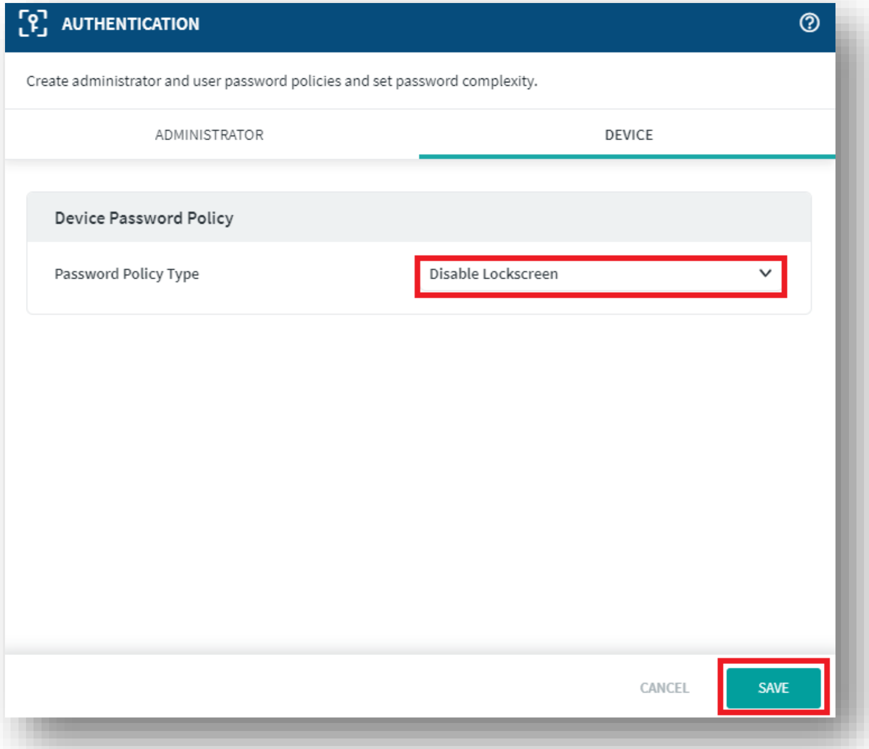
Create administrator and user password policies and set password complexity.

Device Administrator

Password * ••••

Android Enterprise: Dedicated Device Configuration

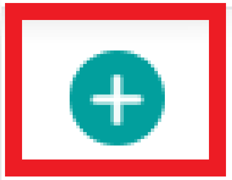
- Select Disable Lockscreen and then SAVE
- Select the + symbol
- Select Lockdown

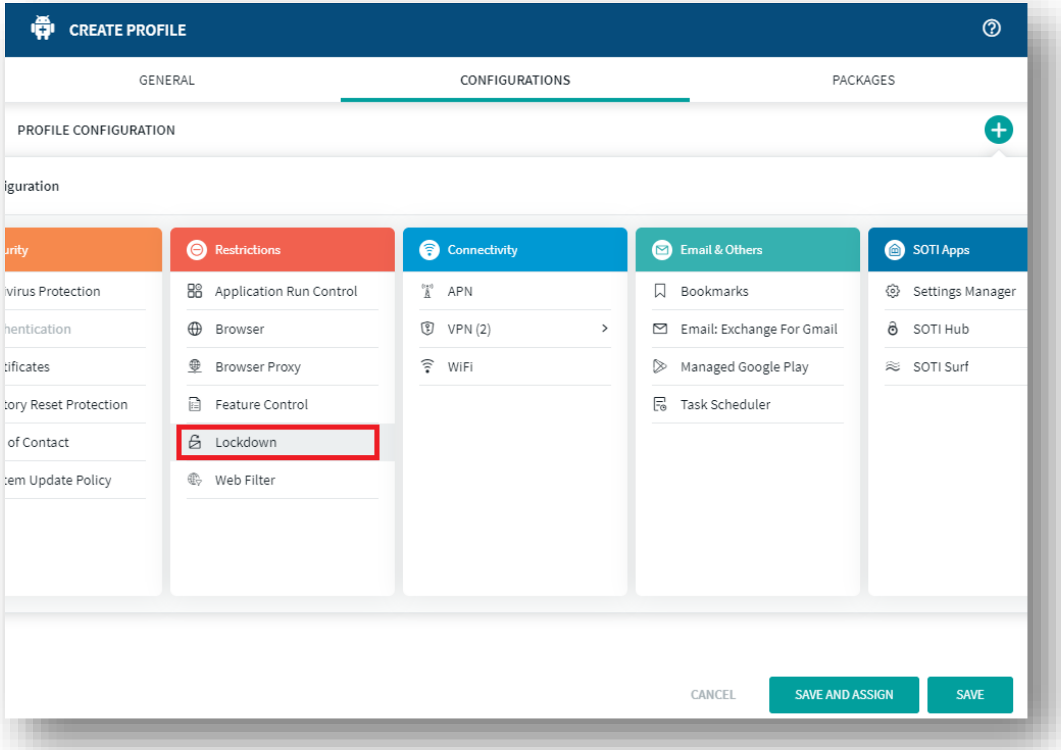


Create administrator and user password policies and set password complexity.

Device Password Policy

Password Policy Type: Disable Lockscreen

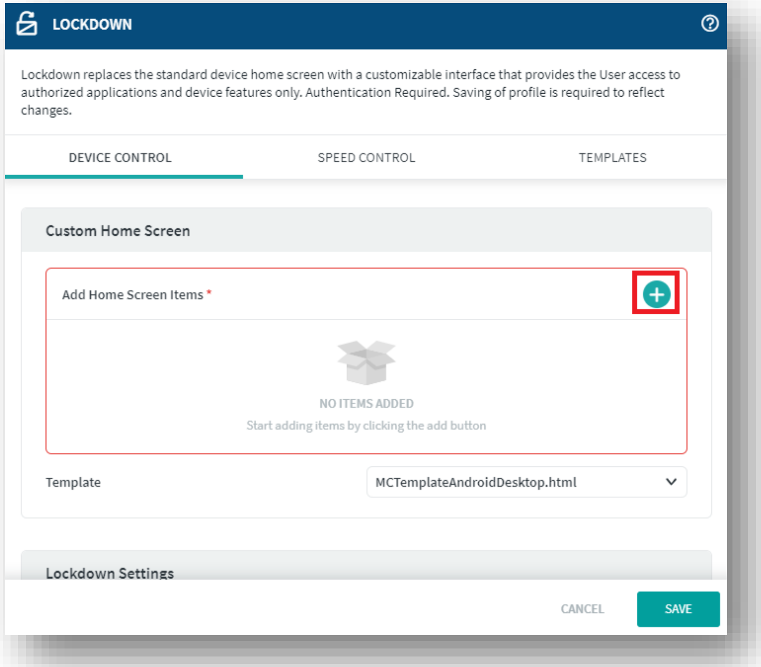




Android Enterprise: Dedicated Device Configuration

Knox

- 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



LOCKDOWN

Lockdown replaces the standard device home screen with a customizable interface that provides the User access to authorized applications and device features only. Authentication Required. Saving of profile is required to reflect changes.

DEVICE CONTROL | SPEED CONTROL | TEMPLATES

Custom Home Screen

Add Home Screen Items * ⊕

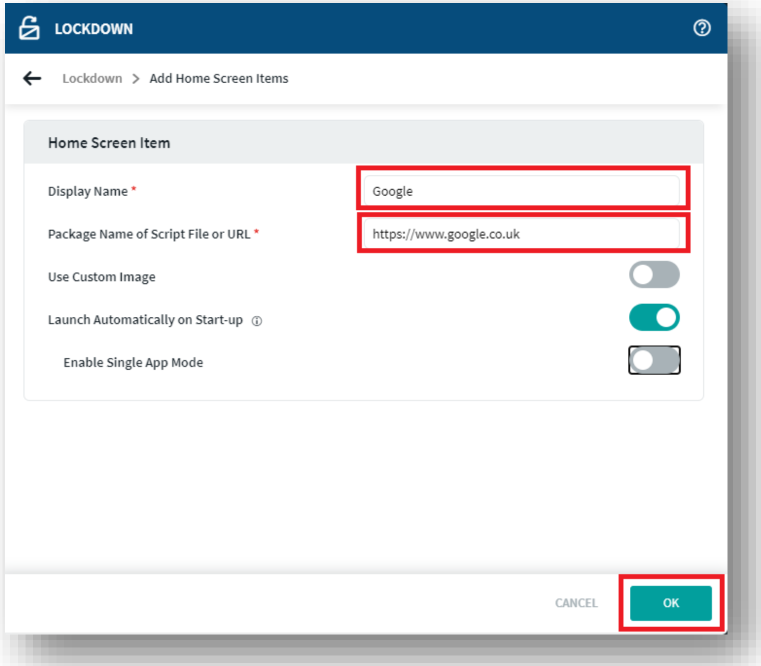
NO ITEMS ADDED

Start adding items by clicking the add button

Template: MCTemplateAndroidDesktop.html

Lockdown Settings

CANCEL | SAVE



LOCKDOWN

← Lockdown > Add Home Screen Items

Home Screen Item

Display Name *: Google

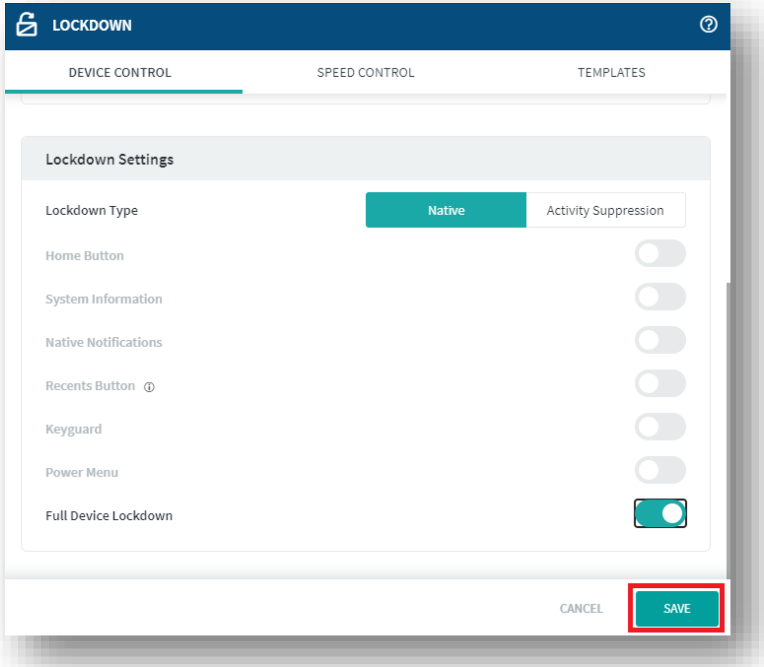
Package Name of Script File or URL *: https://www.google.co.uk

Use Custom Image ○

Launch Automatically on Start-up ●

Enable Single App Mode ○

CANCEL | OK



LOCKDOWN

DEVICE CONTROL | SPEED CONTROL | TEMPLATES

Lockdown Settings

Lockdown Type: [✓ Native] Activity Suppression

Home Button ○

System Information ○

Native Notifications ○

Recents Button ○

Keyguard ○

Power Menu ○

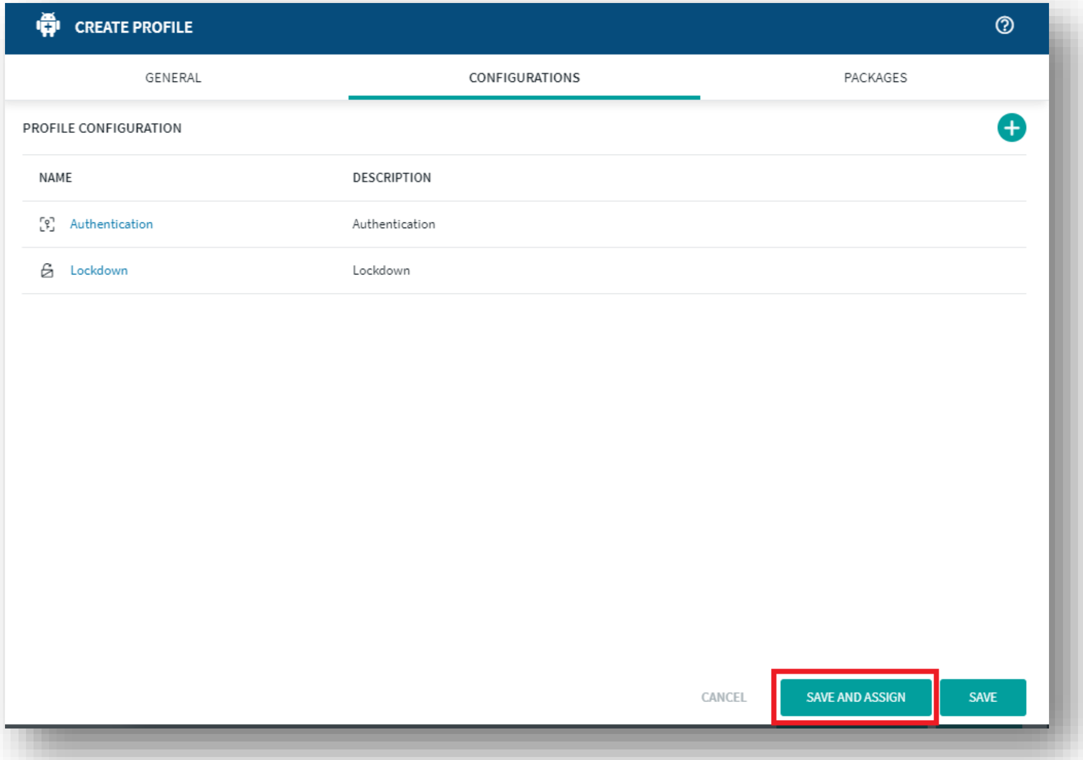
Full Device Lockdown ●

CANCEL | 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.

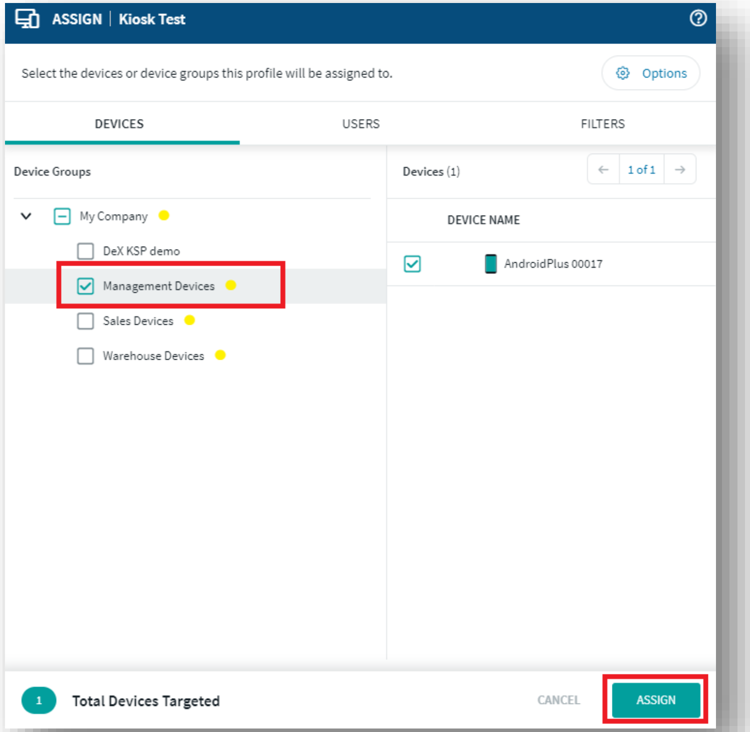


CREATE PROFILE

GENERAL | CONFIGURATIONS | PACKAGES

PROFILE CONFIGURATION

NAME	DESCRIPTION
Authentication	Authentication
Lockdown	Lockdown



ASSIGN | Kiosk Test

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

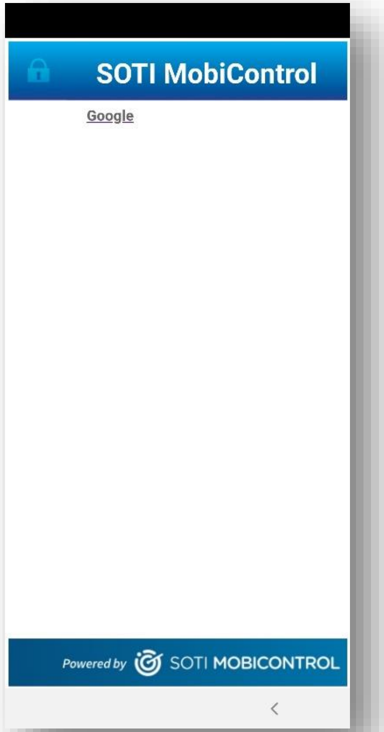
Device Groups

- My Company
  - ☐ DeX KSP demo
  - ☑ Management Devices
  - ☐ Sales Devices
  - ☐ Warehouse Devices

Devices (1) 1 of 1

	DEVICE NAME
☑	AndroidPlus 00017

1 Total Devices Targeted



Knox Platform for Enterprise

The Knox Platform for Enterprise solution provides a robust set of features on top of the core Android Enterprise platform, to fill security and management gaps and meet the strict requirements of highly regulated industries.

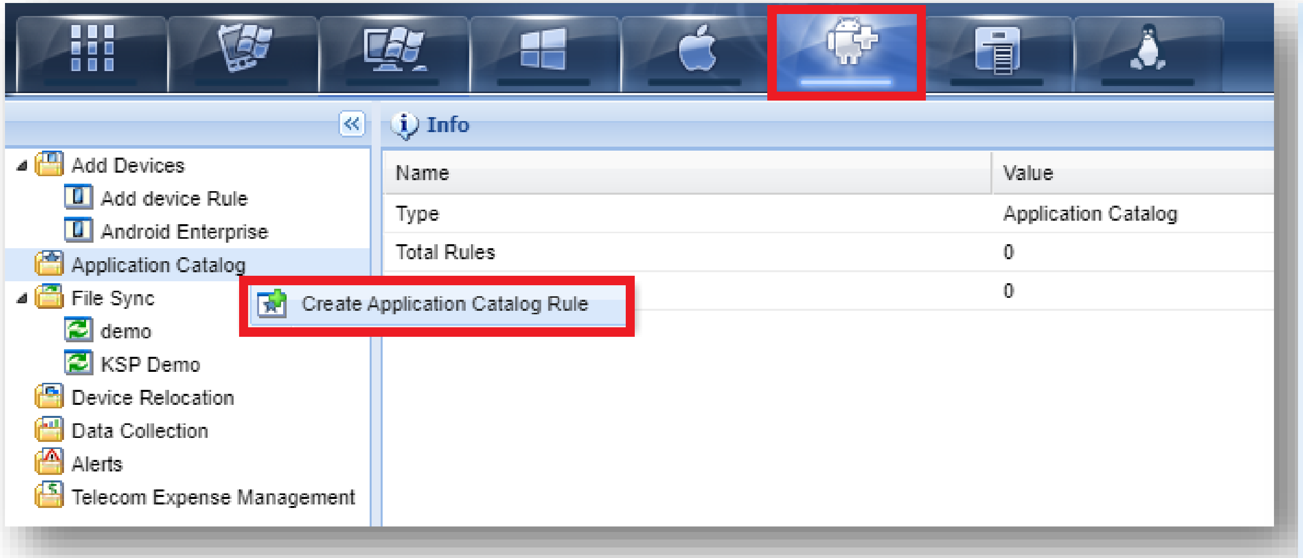
The Knox Platform for Enterprise solution comes in a two tiered offering:

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

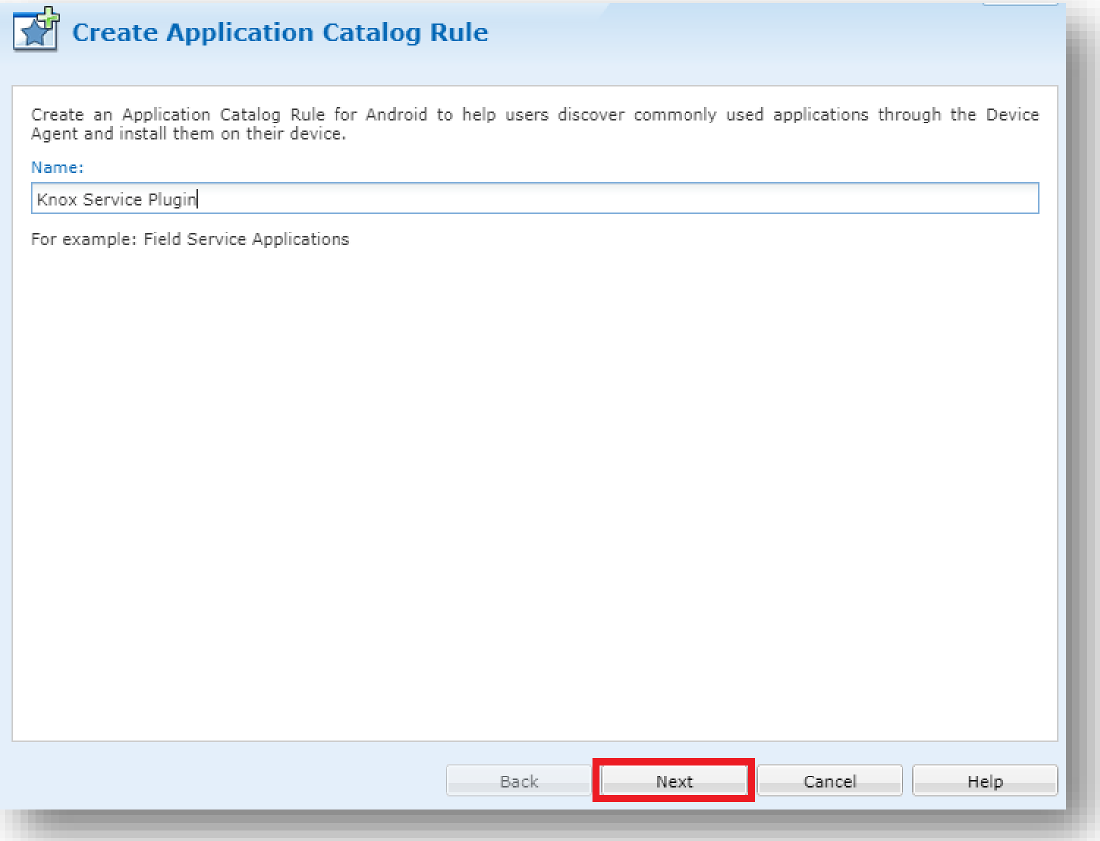
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise on Oreo or above.

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



Name	Value
Type	Application Catalog
Total Rules	0
	0



Create Application Catalog Rule

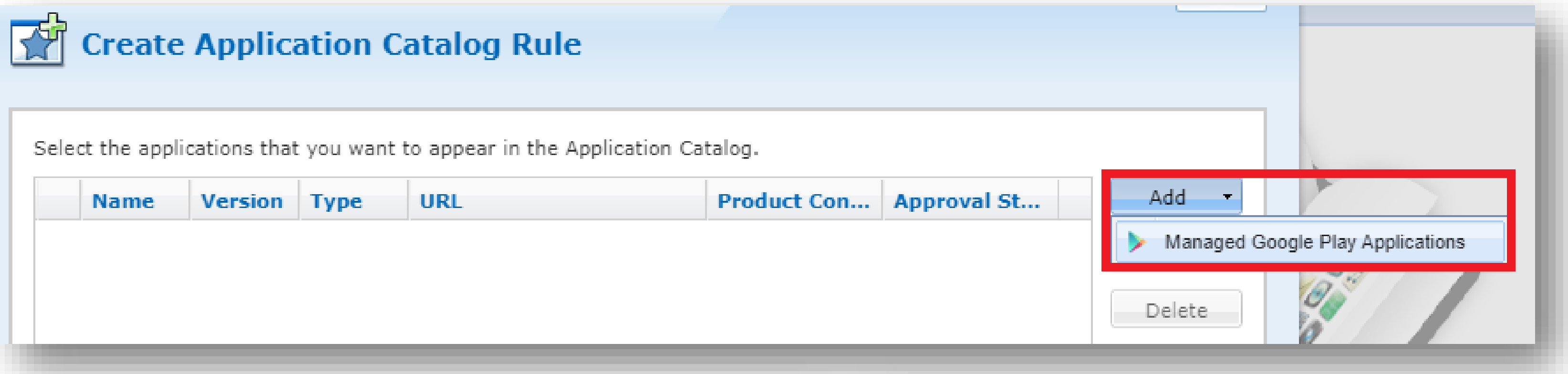
Create an Application Catalog Rule for Android to help users discover commonly used applications through the Device Agent and install them on their device.

Name: Knox Service Plugin

For example: Field Service Applications

Configure Knox Platform for Enterprise using Knox Service Plugin

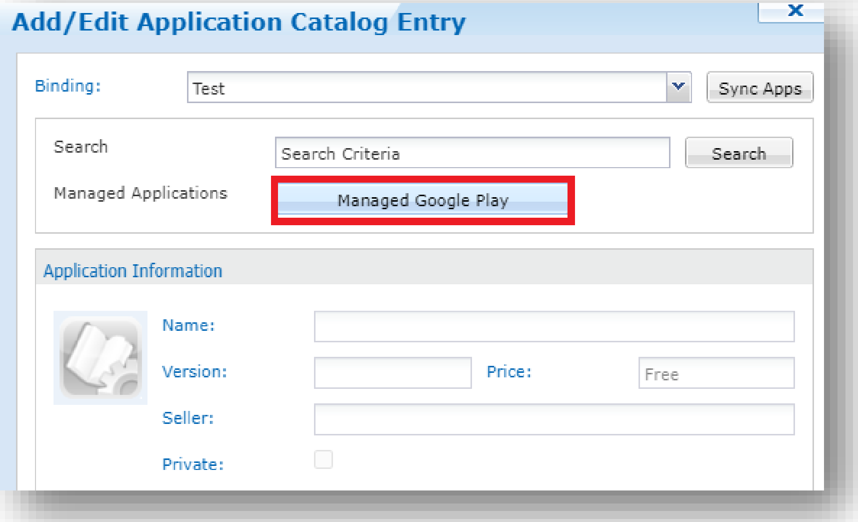
- Select Add, then Managed Google Play Applications
- Click Managed Google Play
- Search for and Approve the Knox Service Plugin



Create Application Catalog Rule

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

	Name	Version	Type	URL	Product Con...	Approval St...



Add/Edit Application Catalog Entry

Binding: Test

Search: Search Criteria

Managed Applications

Application Information

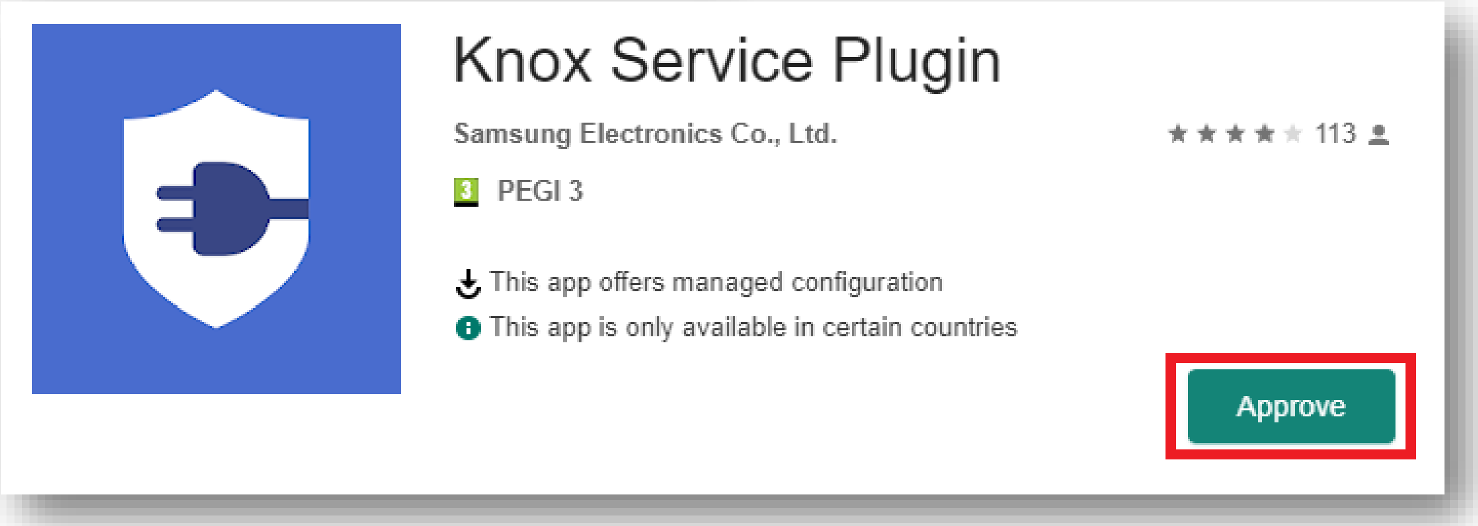
Name:

Version:

Price: Free

Seller:

Private: □



Knox Service Plugin

Samsung Electronics Co., Ltd.

★★★★☆ 113

PEGI 3

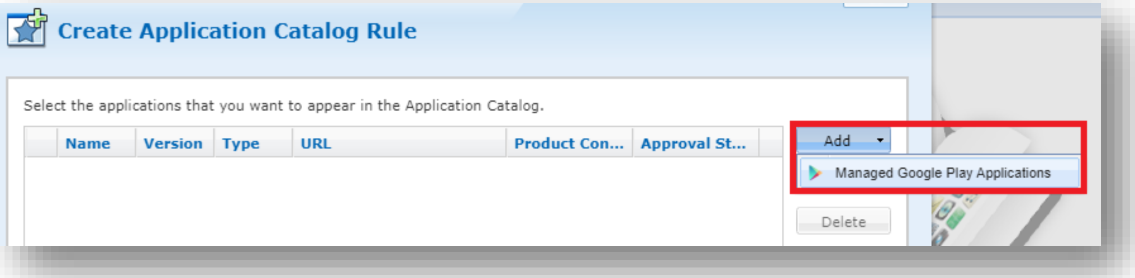
This app offers managed configuration

This app is only available in certain countries

Configure Knox Platform for Enterprise using Knox Service Plugin

Knox

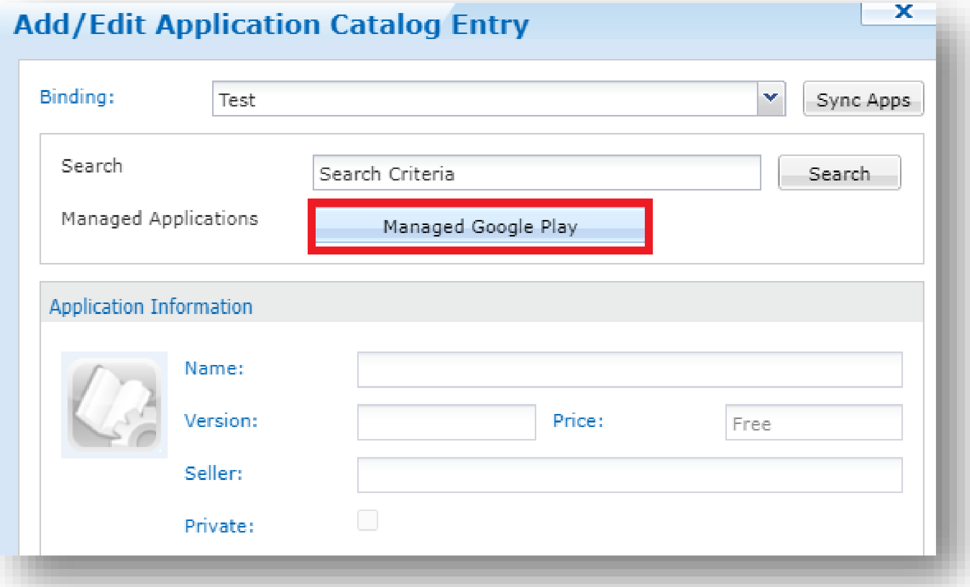
- Select Add, then Managed Google Play Applications
- Click Managed Google Play
- Search for and Approve the Knox Service Plugin
- Choose how you would like to handle new app permissions, select Done



Create Application Catalog Rule

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

Name	Version	Type	URL	Product Con...	Approval St...



Add/Edit Application Catalog Entry

Binding: Test

Search: Search Criteria

Managed Applications: Managed Google Play

Application Information

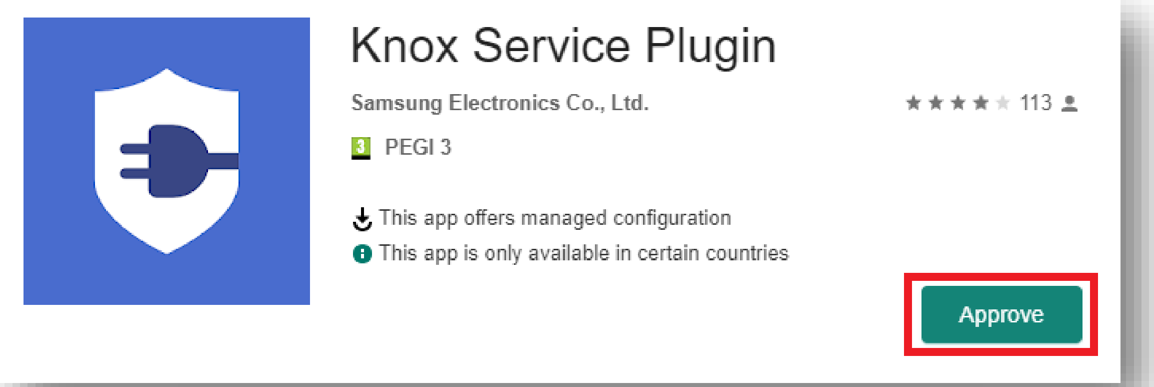
Name:

Version:

Price: Free

Seller:

Private: □



Knox Service Plugin

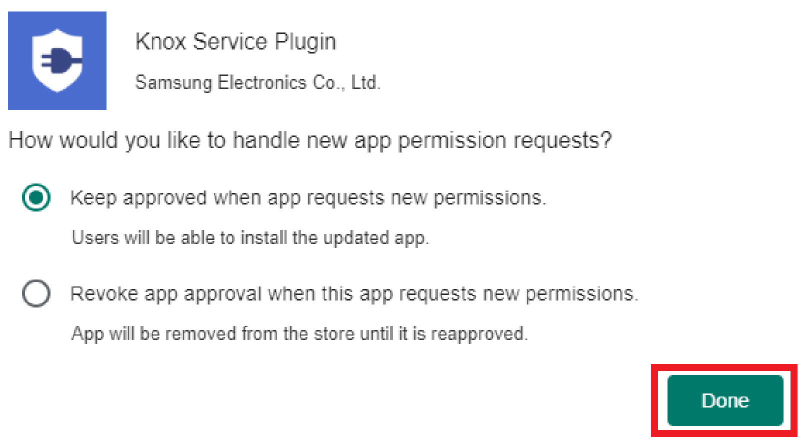
Samsung Electronics Co., Ltd.

★★★★☆ 113

PEGI 3

This app offers managed configuration

This app is only available in certain countries



Knox Service Plugin

Samsung Electronics Co., Ltd.

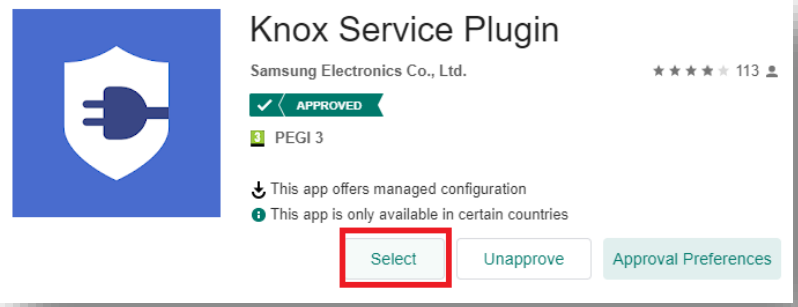
How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

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**



Knox Service Plugin

Samsung Electronics Co., Ltd.

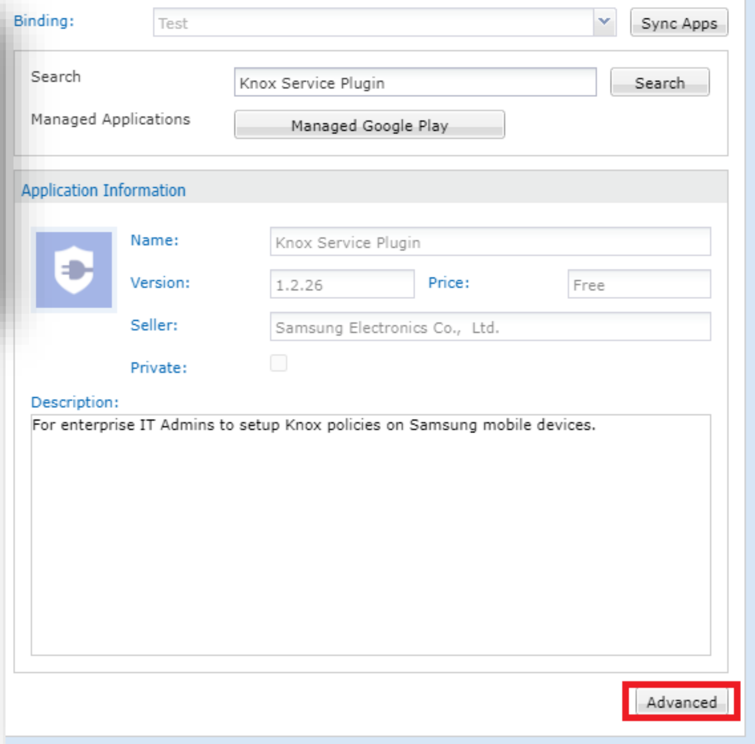
★★★★★ 113

APPROVED

PEGI 3

This app offers managed configuration

This app is only available in certain countries



Binding: Test

Search: Knox Service Plugin

Managed Applications: Managed Google Play

Application Information

Name: Knox Service Plugin

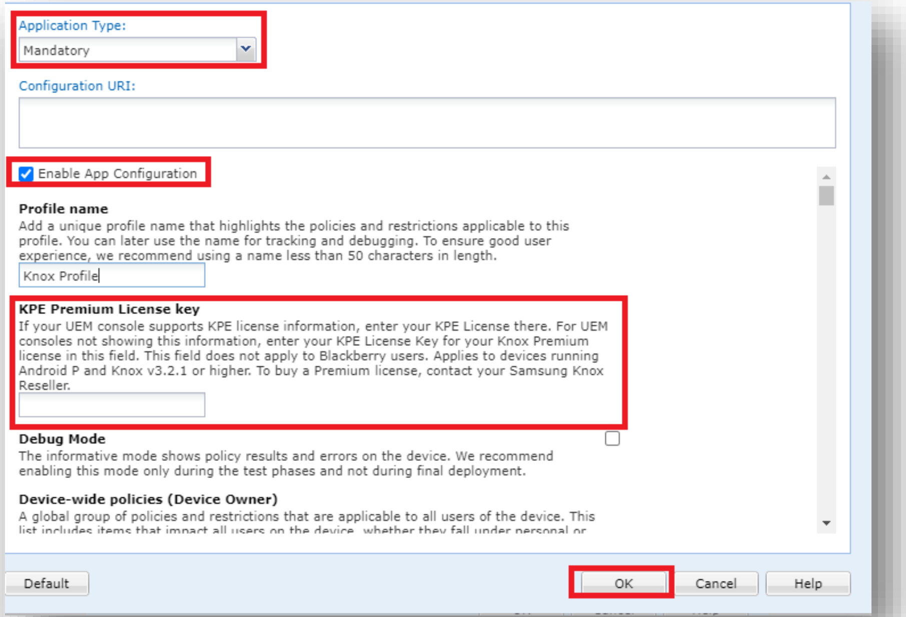
Version: 1.2.26

Price: Free

Seller: Samsung Electronics Co., Ltd.

Private: □

Description:
For enterprise IT Admins to setup Knox policies on Samsung mobile devices.



Application Type: Mandatory

Configuration URI:

☑ Enable App Configuration

Profile name
Add a unique profile name that highlights the policies and restrictions applicable to this profile. You can later use the name for tracking and debugging. To ensure good user experience, we recommend using a name less than 50 characters in length.

Knox Profile

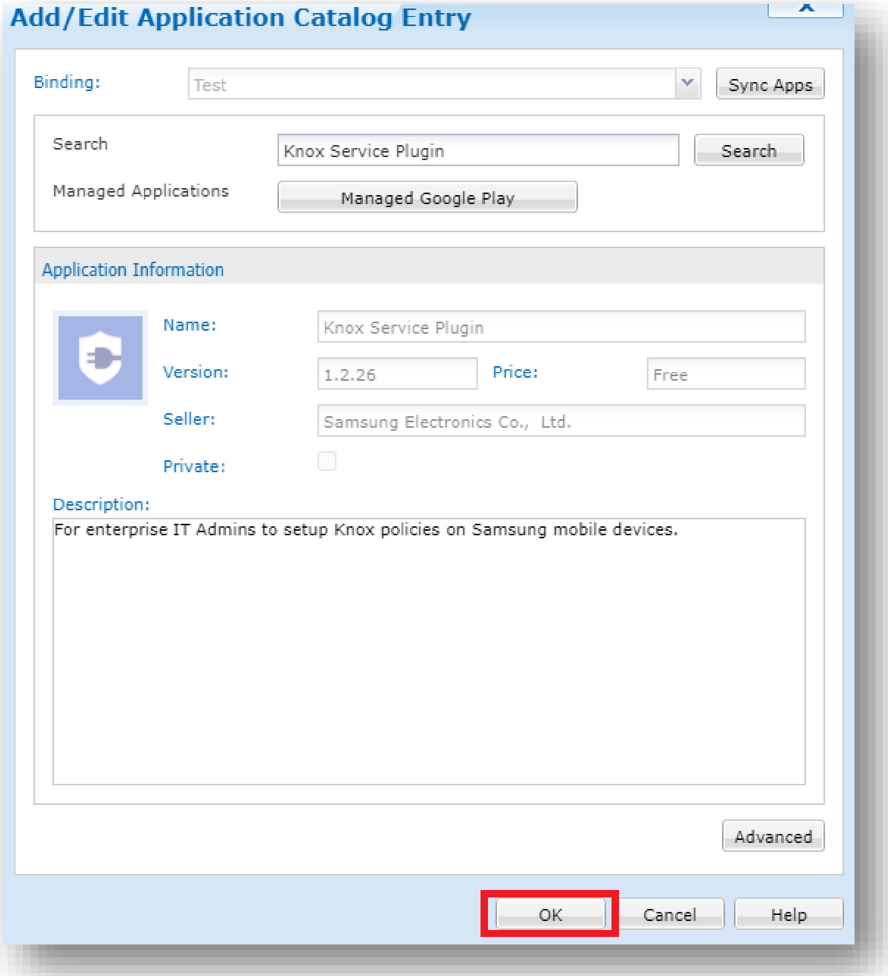
KPE Premium License key
If your UEM console supports KPE license information, enter your KPE License there. For UEM consoles not showing this information, enter your KPE License Key for your Knox Premium license in this field. This field does not apply to Blackberry users. Applies to devices running Android P and Knox v3.2.1 or higher. To buy a Premium license, contact your Samsung Knox Reseller.

Debug Mode □
The informative mode shows policy results and errors on the device. We recommend enabling this mode only during the test phases and not during final deployment.

Device-wide policies (Device Owner)
A global group of policies and restrictions that are applicable to all users of the device. This list includes items that impact all users on the device, whether they fall under personal or

Configure Knox Platform for Enterprise using Knox Service Plugin

- **Click OK**
- **Select Next**



Add/Edit Application Catalog Entry

Binding: Test

Search: Knox Service Plugin

Managed Applications: Managed Google Play

Application Information

Name: Knox Service Plugin

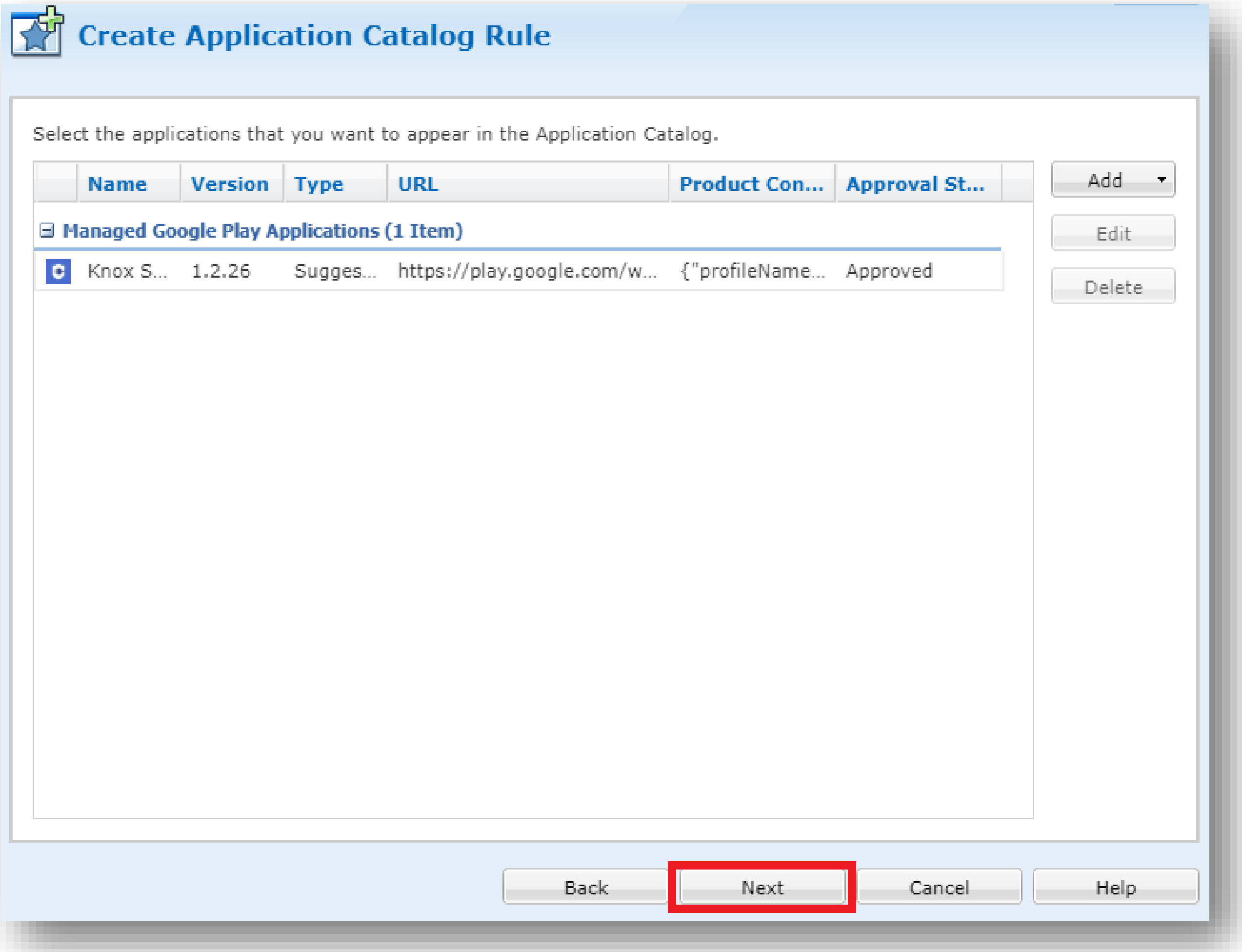
Version: 1.2.26

Price: Free

Seller: Samsung Electronics Co., Ltd.

Private: □

Description:
For enterprise IT Admins to setup Knox policies on Samsung mobile devices.



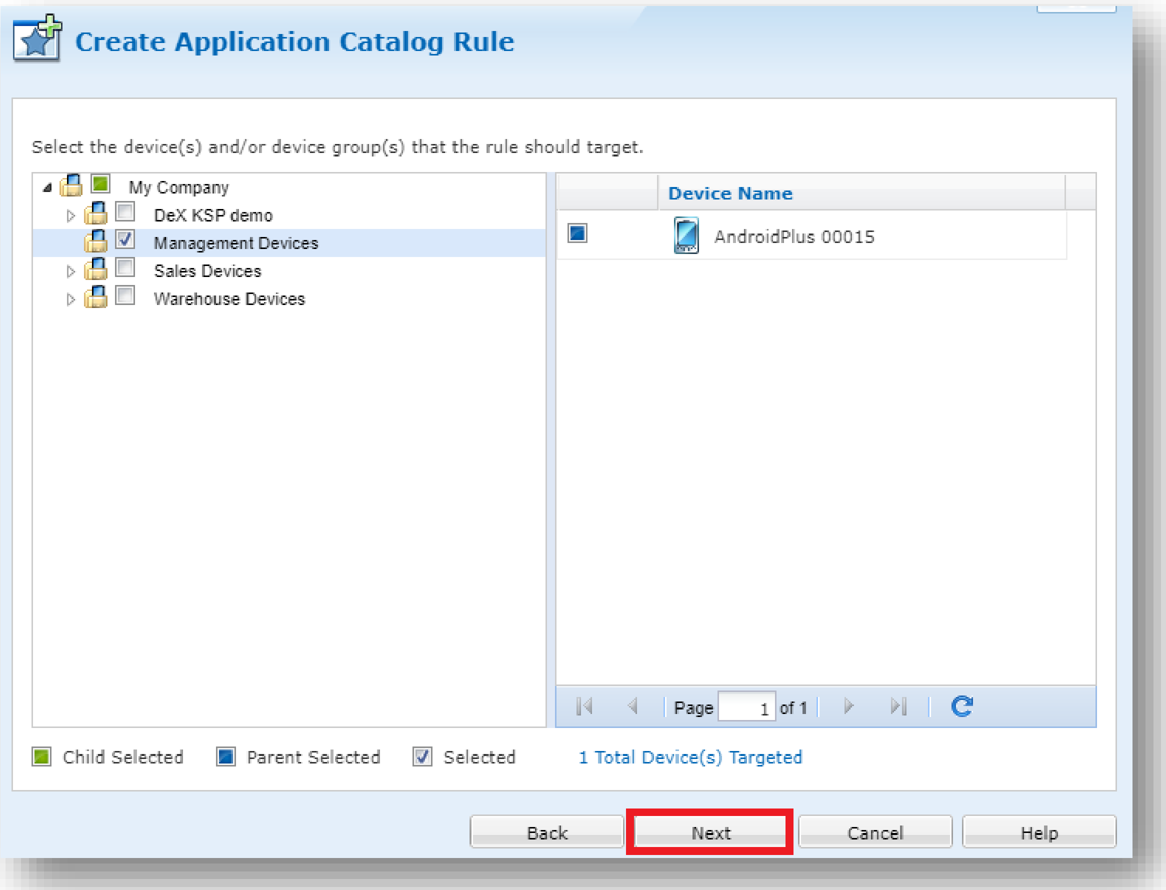
Create Application Catalog Rule

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

Configure Knox Platform for Enterprise using Knox Service Plugin

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



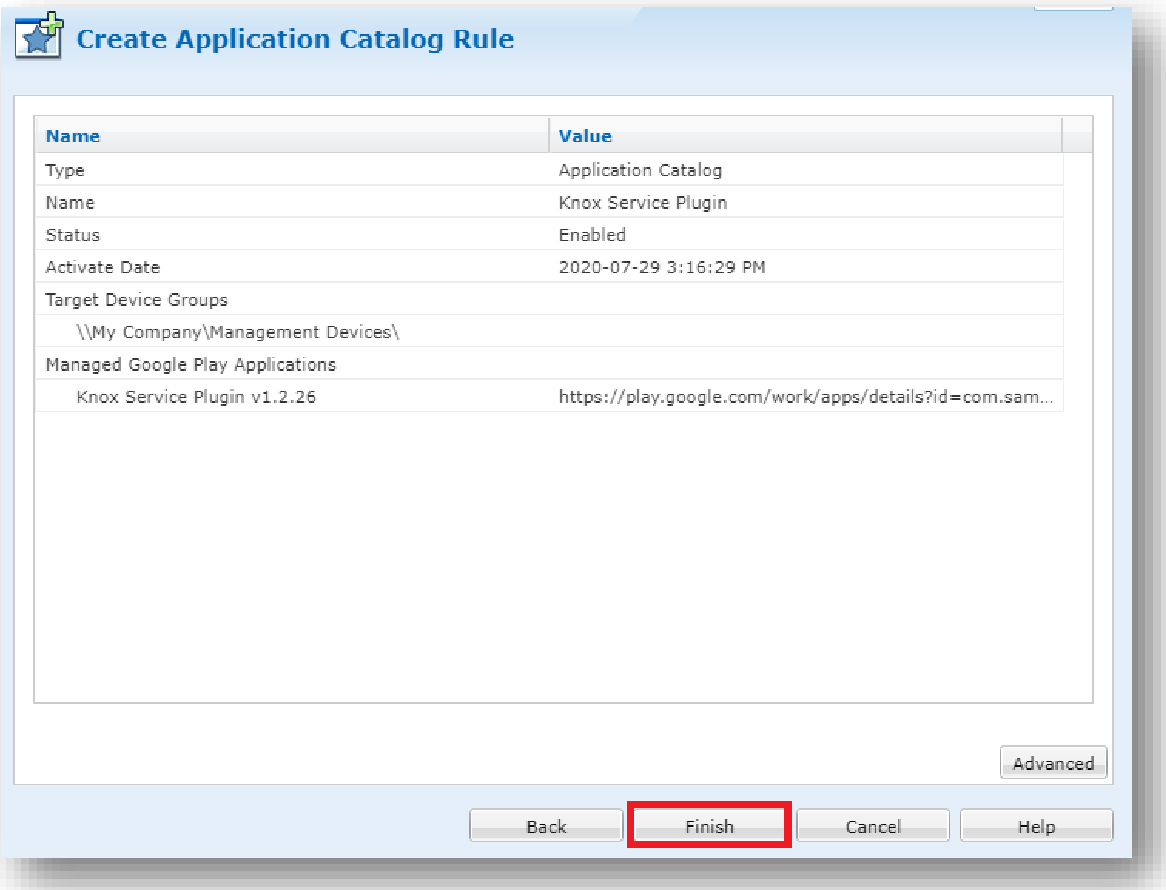
Create Application Catalog Rule

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
■	AndroidPlus 00015

🟩 Child Selected ■ Parent Selected ☑ Selected 1 Total Device(s) Targeted



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...

Document Information

This is version 2.2 of this document.

Thank you!

Knox