

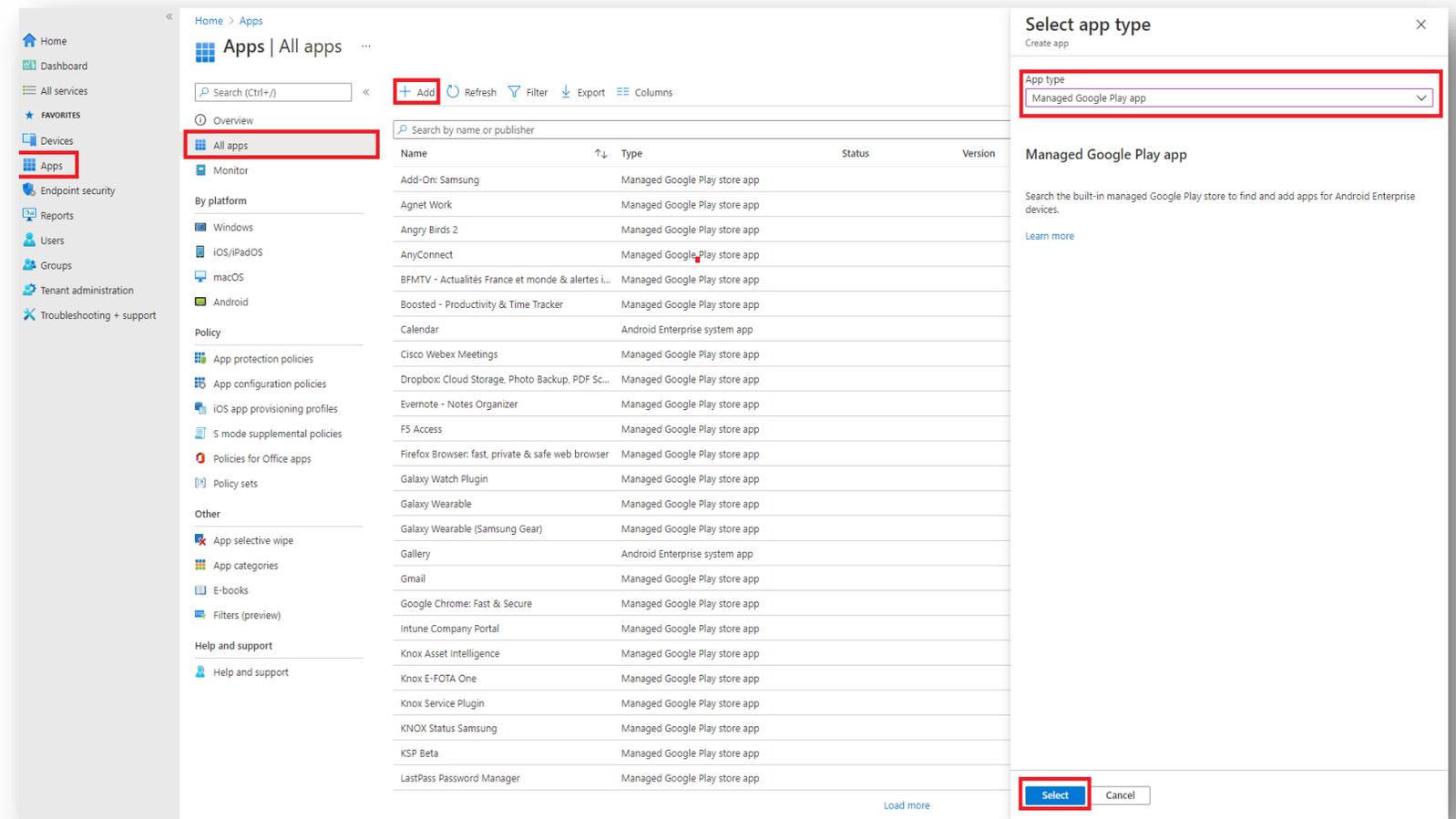
# Knox Asset Intelligence (KAI) – Intune Auto Enroll

July 2022  
Samsung R&D Centre UK  
(SRUK)

1. Add the Knox Asset Intelligence app to Intune
2. Deploy the KAI agent to the devices
3. Create and assign an Android Enterprise app configuration profile
4. Add the Knox Service Plugin app to Intune
5. Deploy the Knox Service Plugin app to the devices
6. Create an Android Enterprise OEMConfig profile
7. Check the KAI console to see if devices have successfully enrolled

# Add the Knox Asset Intelligence app to Intune

- Within the Intune console, select Apps
- Select All apps
- Select Add
- For App type, select Managed Google Play app
- Select

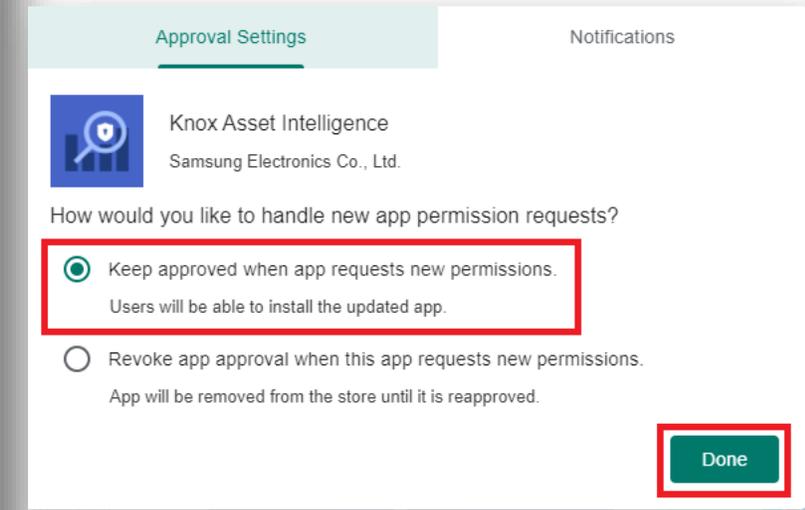
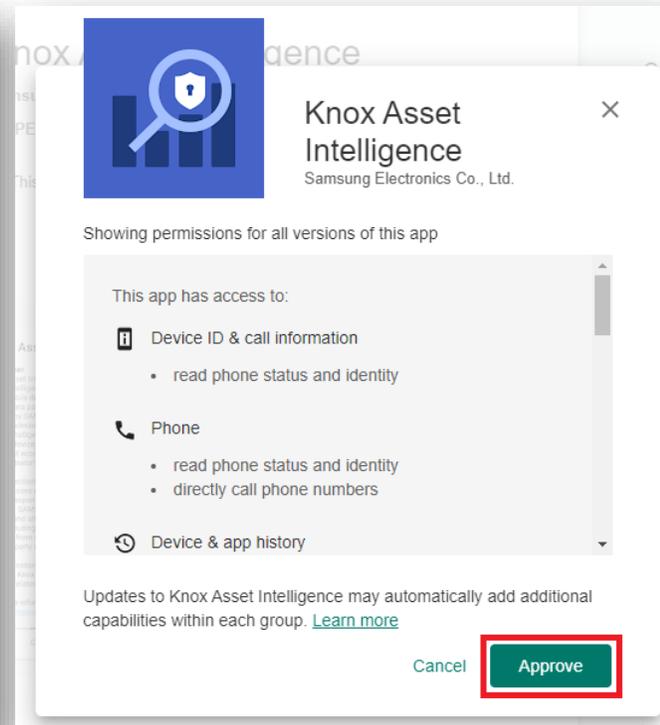
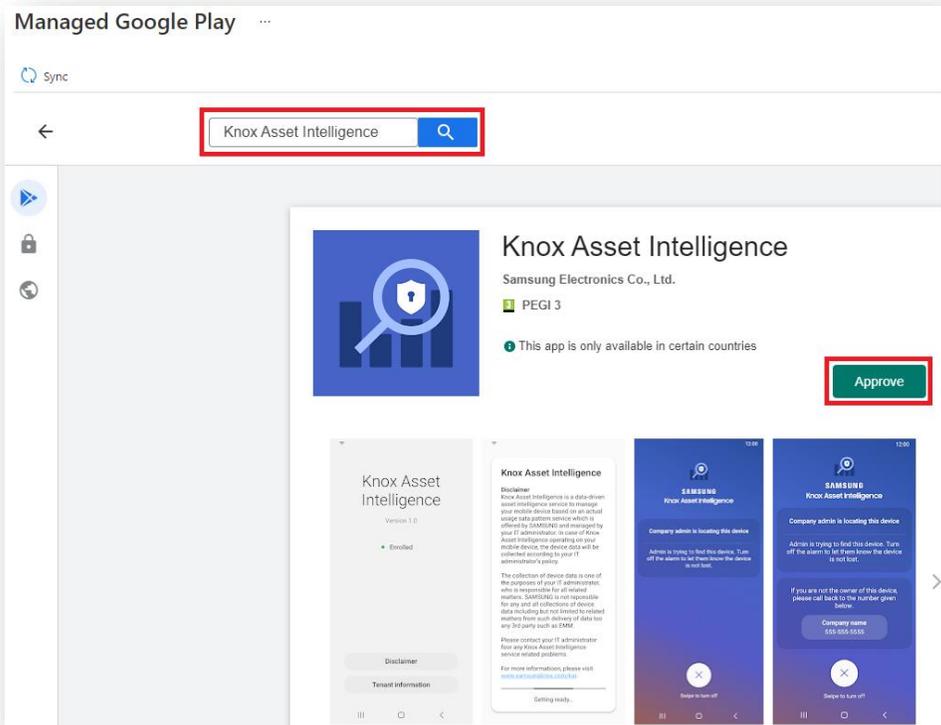


The screenshot shows the Microsoft Intune console interface. On the left, the navigation pane has 'Apps' selected. The main area displays 'Apps | All apps' with a search bar and an '+ Add' button highlighted with a red box. Below the search bar, there are tabs for 'Overview', 'Monitor', 'By platform', 'Policy', and 'Other'. The 'By platform' tab is active, showing a list of apps. A modal window titled 'Select app type' is open on the right, with 'Managed Google Play app' selected in the 'App type' dropdown menu, also highlighted with a red box. At the bottom of the modal, the 'Select' button is highlighted with a red box.

Name	Type	Status	Version
Add-On: Samsung	Managed Google Play store app		
Agnet Work	Managed Google Play store app		
Angry Birds 2	Managed Google Play store app		
AnyConnect	Managed Google Play store app		
BFMTV - Actualités France et monde & alertes i...	Managed Google Play store app		
Boosted - Productivity & Time Tracker	Managed Google Play store app		
Calendar	Android Enterprise system app		
Cisco Webex Meetings	Managed Google Play store app		
Dropbox: Cloud Storage, Photo Backup, PDF Sc...	Managed Google Play store app		
Evernote - Notes Organizer	Managed Google Play store app		
F5 Access	Managed Google Play store app		
Firefox Browser: fast, private & safe web browser	Managed Google Play store app		
Galaxy Watch Plugin	Managed Google Play store app		
Galaxy Wearable	Managed Google Play store app		
Galaxy Wearable (Samsung Gear)	Managed Google Play store app		
Gallery	Android Enterprise system app		
Gmail	Managed Google Play store app		
Google Chrome: Fast & Secure	Managed Google Play store app		
Intune Company Portal	Managed Google Play store app		
Knox Asset Intelligence	Managed Google Play store app		
Knox E-FOTA One	Managed Google Play store app		
Knox Service Plugin	Managed Google Play store app		
KNOX Status Samsung	Managed Google Play store app		
KSP Beta	Managed Google Play store app		
LastPass Password Manager	Managed Google Play store app		

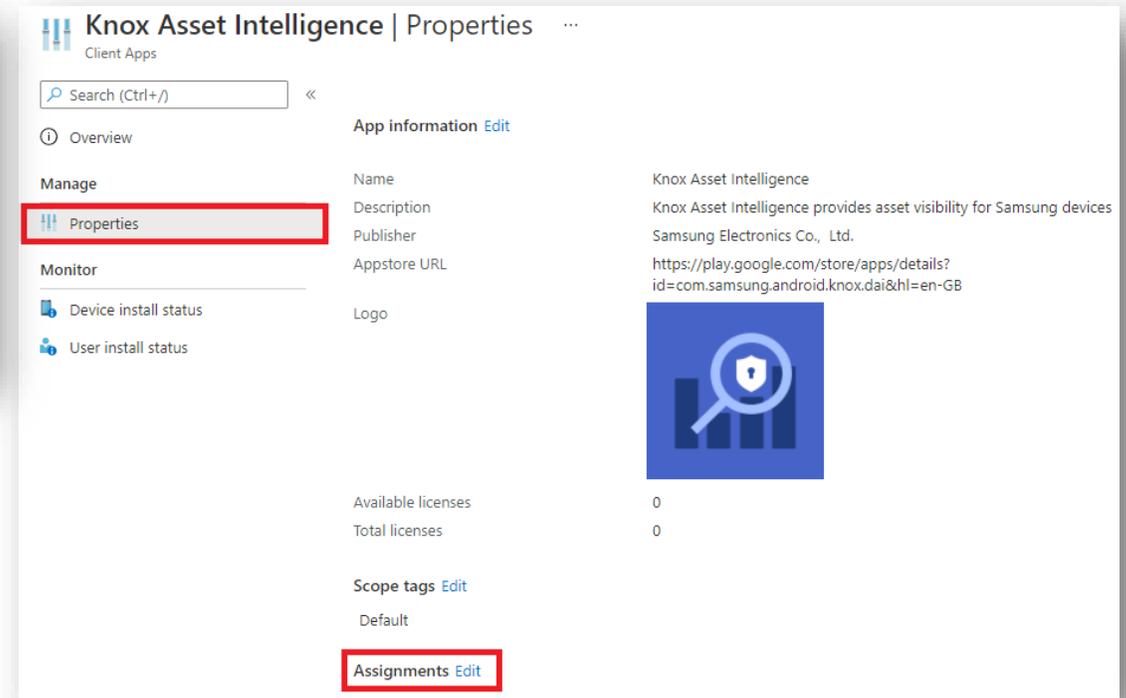
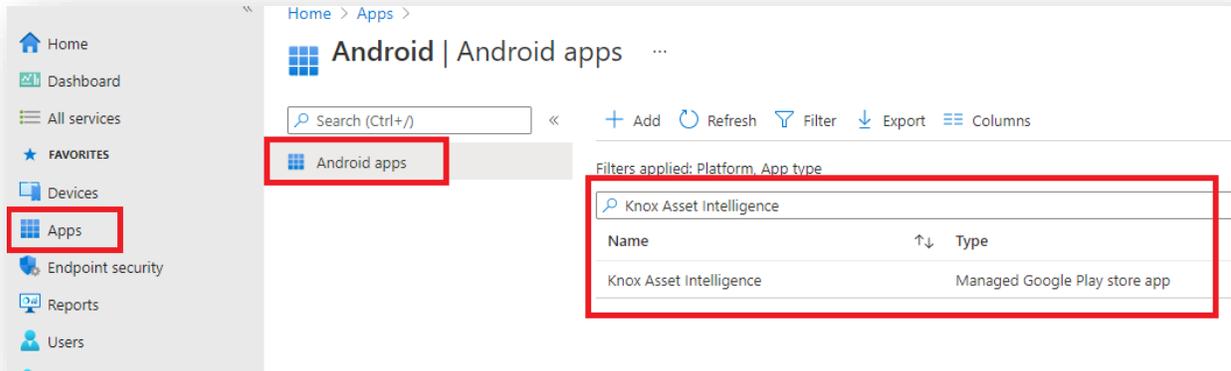
# Add the Knox Asset Intelligence app to Intune

- Search for the Knox Asset Intelligence App
- Select Approve
- Select Approve
- Select Keep approved when app requests new permissions
- Select Done



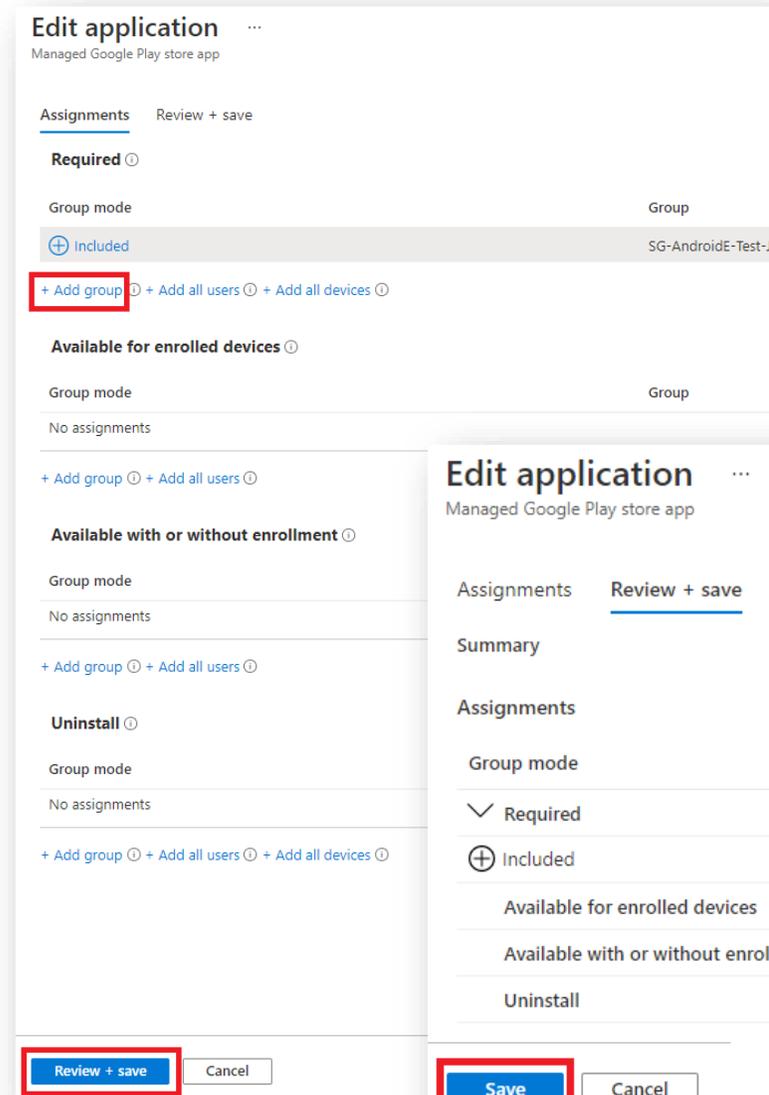
# Deploy the KAI agent to the devices

- Select Apps
- Select Android apps
- Search for and select Knox Asset Intelligence
- Select Properties
- Next to Assignments, select Edit



# Deploy the KAI agent to the devices

- Under Required, Select Add group
- Add an assignment group
- Select Review + save
- Select Save



**Edit application** ...  
Managed Google Play store app

Assignments [Review + save](#)

**Required** ⓘ

Group mode Group

**Included** ⓘ SG-AndroidE-Test-JK

**+ Add group** ⓘ + Add all users ⓘ + Add all devices ⓘ

**Available for enrolled devices** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ

**Available with or without enrollment** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ

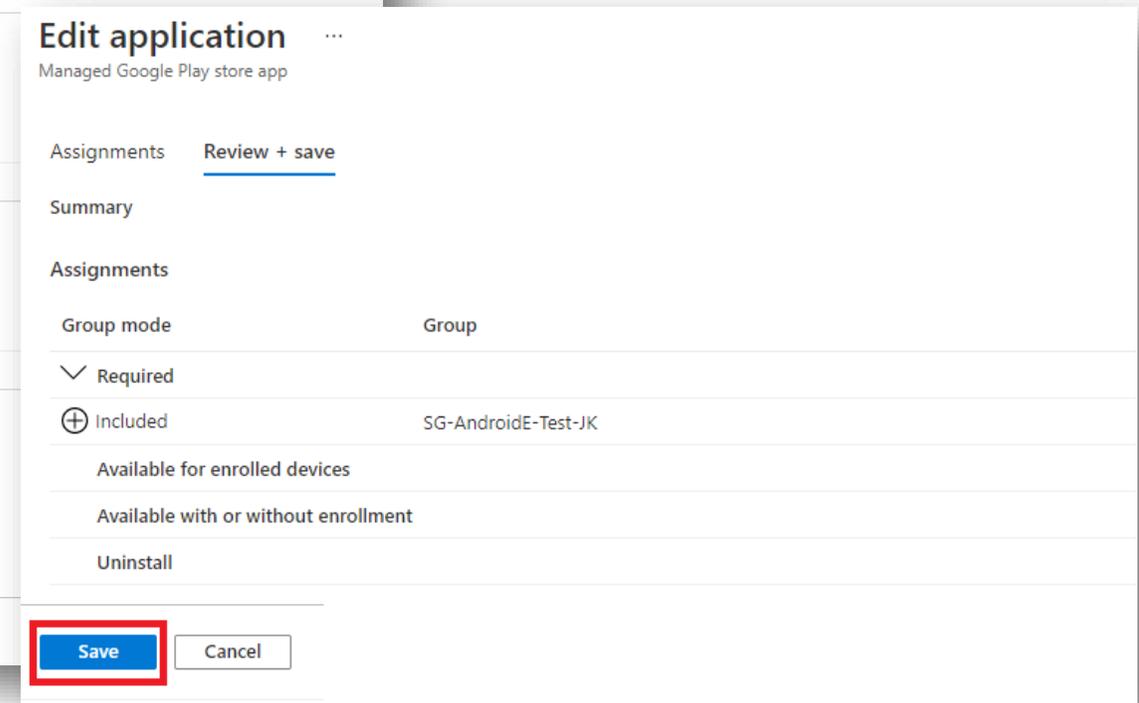
**Uninstall** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

**Review + save** Cancel



**Edit application** ...  
Managed Google Play store app

Assignments [Review + save](#)

Summary

Assignments

Group mode Group

✓ **Required**

**Included** ⓘ SG-AndroidE-Test-JK

Available for enrolled devices

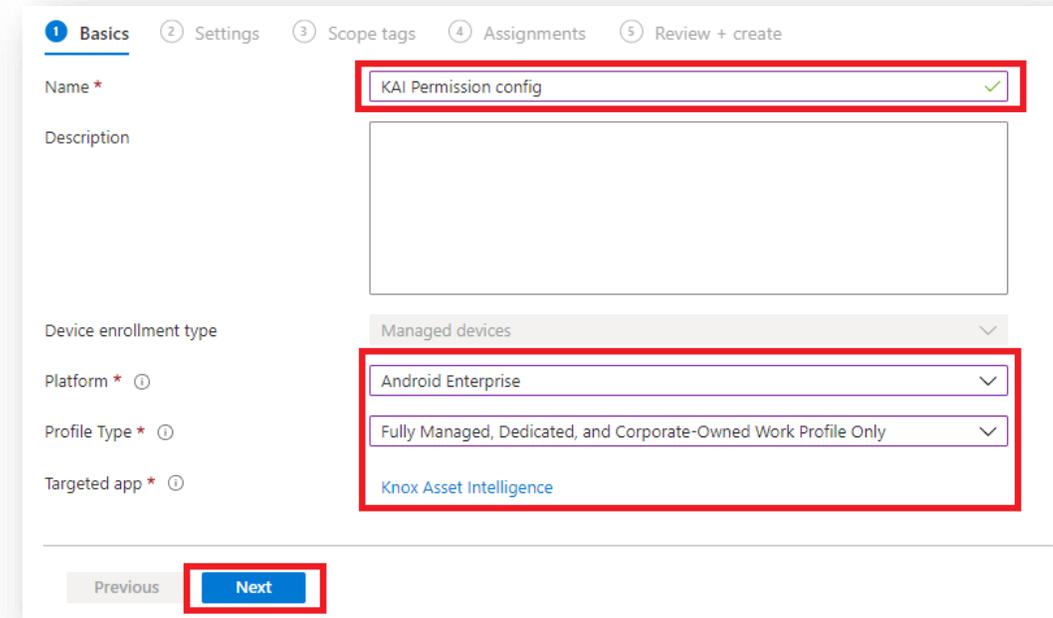
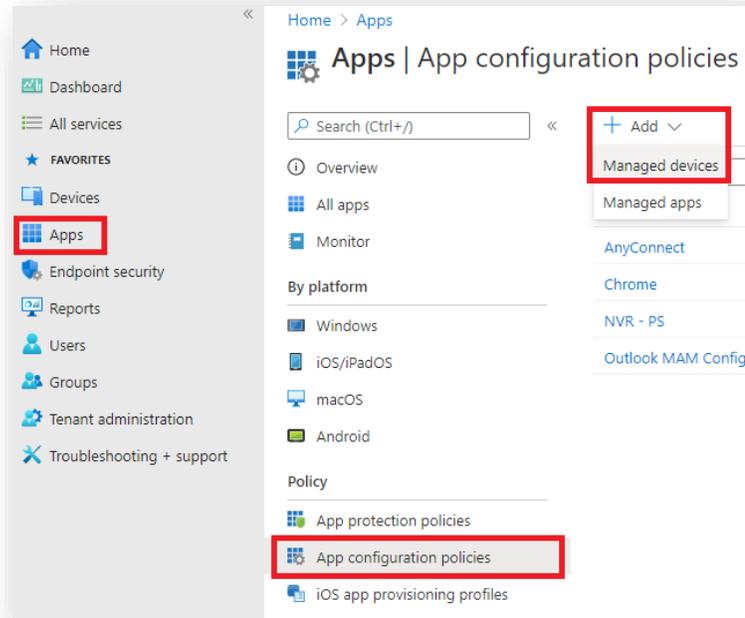
Available with or without enrollment

Uninstall

**Save** Cancel

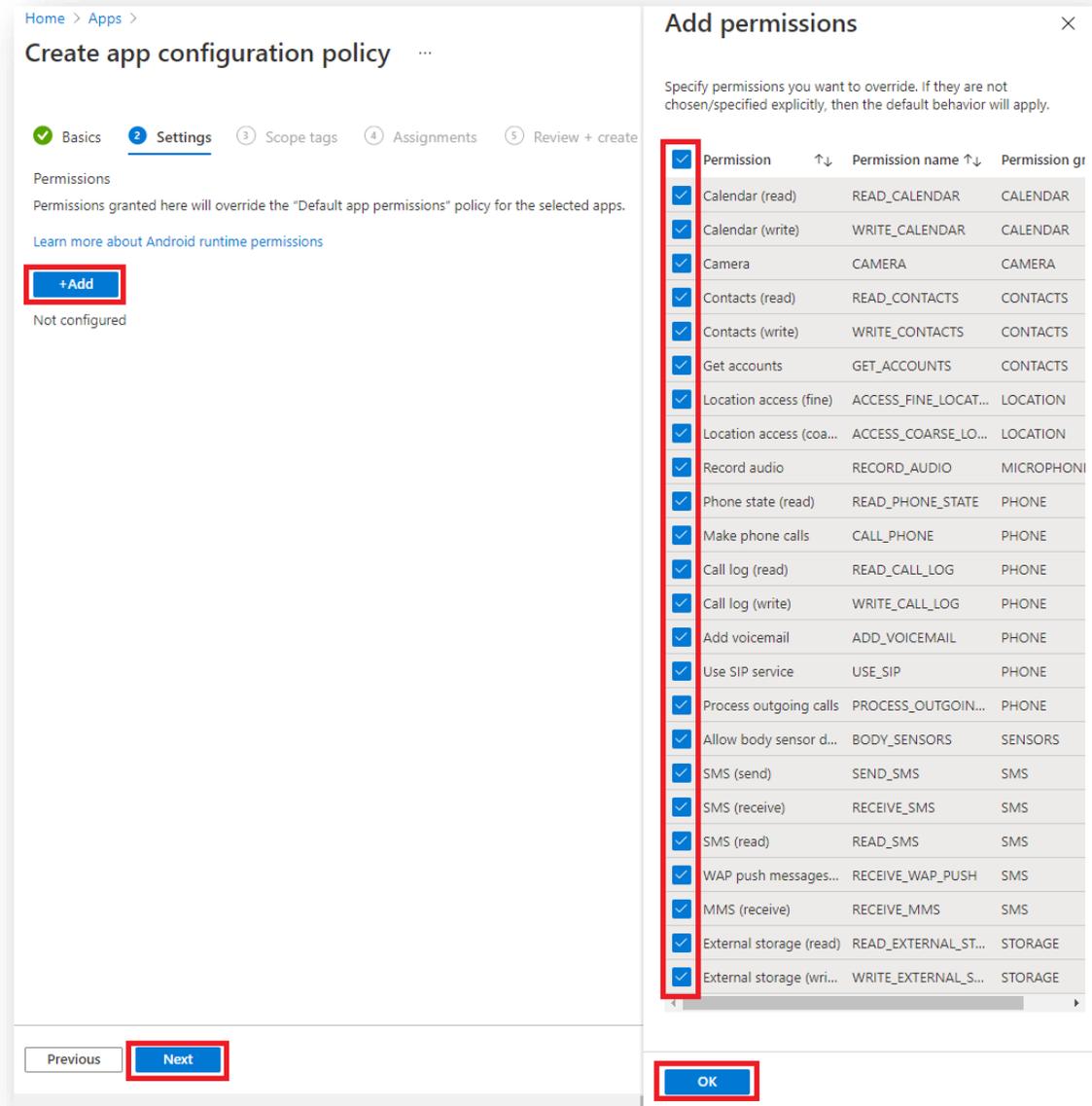
# Create and assign an Android Enterprise app configuration profile

- Select Apps
- Select App configuration policies
- Select Add
- Select Managed devices
- Enter a profile name of your choice
- For Platform, select Android Enterprise
- For Profile Type, select Fully Manage, Dedicated, and Corporate-Owned Work Profile Only
- For Targeted app, select Knox Asset Intelligence
- Select Next



# Create and assign an Android Enterprise app configuration profile

- Select Add
- Tick all the permission options
- Select OK
- Select Next



Home > Apps >

## Create app configuration policy ...

Basics
  **Settings**
 Scope tags
  Assignments
  Review + create

Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

[Learn more about Android runtime permissions](#)

**+Add**

Not configured

---

### Add permissions

Specify permissions you want to override. If they are not chosen/specified explicitly, then the default behavior will apply.

<input checked="" type="checkbox"/>	Permission	Permission name	Permission gr
<input checked="" type="checkbox"/>	Calendar (read)	READ_CALENDAR	CALENDAR
<input checked="" type="checkbox"/>	Calendar (write)	WRITE_CALENDAR	CALENDAR
<input checked="" type="checkbox"/>	Camera	CAMERA	CAMERA
<input checked="" type="checkbox"/>	Contacts (read)	READ_CONTACTS	CONTACTS
<input checked="" type="checkbox"/>	Contacts (write)	WRITE_CONTACTS	CONTACTS
<input checked="" type="checkbox"/>	Get accounts	GET_ACCOUNTS	CONTACTS
<input checked="" type="checkbox"/>	Location access (fine)	ACCESS_FINE_LOCAT...	LOCATION
<input checked="" type="checkbox"/>	Location access (coa...	ACCESS_COARSE_LO...	LOCATION
<input checked="" type="checkbox"/>	Record audio	RECORD_AUDIO	MICROPHONI
<input checked="" type="checkbox"/>	Phone state (read)	READ_PHONE_STATE	PHONE
<input checked="" type="checkbox"/>	Make phone calls	CALL_PHONE	PHONE
<input checked="" type="checkbox"/>	Call log (read)	READ_CALL_LOG	PHONE
<input checked="" type="checkbox"/>	Call log (write)	WRITE_CALL_LOG	PHONE
<input checked="" type="checkbox"/>	Add voicemail	ADD_VOICEMAIL	PHONE
<input checked="" type="checkbox"/>	Use SIP service	USE_SIP	PHONE
<input checked="" type="checkbox"/>	Process outgoing calls	PROCESS_OUTGOIN...	PHONE
<input checked="" type="checkbox"/>	Allow body sensor d...	BODY_SENSORS	SENSORS
<input checked="" type="checkbox"/>	SMS (send)	SEND_SMS	SMS
<input checked="" type="checkbox"/>	SMS (receive)	RECEIVE_SMS	SMS
<input checked="" type="checkbox"/>	SMS (read)	READ_SMS	SMS
<input checked="" type="checkbox"/>	WAP push messages...	RECEIVE_WAP_PUSH	SMS
<input checked="" type="checkbox"/>	MMS (receive)	RECEIVE_MMS	SMS
<input checked="" type="checkbox"/>	External storage (read)	READ_EXTERNAL_ST...	STORAGE
<input checked="" type="checkbox"/>	External storage (wri...	WRITE_EXTERNAL_S...	STORAGE

Previous **Next**

**OK**

# Create and assign an Android Enterprise app configuration profile

- For Permission state, select Auto grant for each Permission
- Select Next



Permission ↑↓	Permission state ↑↓	Permission name ↑↓	Permission group ↑↓
External storage (write)	Auto grant	WRITE_EXTERNAL_STORAGE	STORAGE
External storage (read)	Auto grant	READ_EXTERNAL_STORAGE	STORAGE
MMS (receive)	Auto grant	RECEIVE_MMS	SMS
WAP push messages (receive)	Auto grant	RECEIVE_WAP_PUSH	SMS
SMS (read)	Auto grant	READ_SMS	SMS
SMS (receive)	Auto grant	RECEIVE_SMS	SMS
SMS (send)	Auto grant	SEND_SMS	SMS
Allow body sensor data	Auto grant	BODY_SENSORS	SENSORS
Process outgoing calls	Auto grant	PROCESS_OUTGOING_CALLS	PHONE
Use SIP service	Auto grant	USE_SIP	PHONE
Add voicemail	Auto grant	ADD_VOICEMAIL	PHONE
Call log (write)	Auto grant	WRITE_CALL_LOG	PHONE
Call log (read)	Auto grant	READ_CALL_LOG	PHONE
Make phone calls	Auto grant	CALL_PHONE	PHONE
Phone state (read)	Auto grant	READ_PHONE_STATE	PHONE
Record audio	Auto grant	RECORD_AUDIO	MICROPHONE
Location access (coarse)	Auto grant	ACCESS_COARSE_LOCATION	LOCATION
Location access (fine)	Auto grant	ACCESS_FINE_LOCATION	LOCATION
Get accounts	Auto grant	GET_ACCOUNTS	CONTACTS
Contacts (write)	Auto grant	WRITE_CONTACTS	CONTACTS
Contacts (read)	Auto grant	READ_CONTACTS	CONTACTS
Camera	Auto grant	CAMERA	CAMERA
Calendar (write)	Auto grant	WRITE_CALENDAR	CALENDAR
Calendar (read)	Auto grant	READ_CALENDAR	CALENDAR

Previous **Next**

# Create and assign an Android Enterprise app configuration profile

- Scope tags are optional, select Next
- Select Add groups and then select an Assignment Group
- Select Next

The image displays two screenshots of the Android Enterprise app configuration profile setup wizard. The first screenshot shows the 'Scope tags' step, where the 'Next' button is highlighted. The second screenshot shows the 'Assignments' step, where the 'Add groups' button is highlighted.

**Scope tags step:**

- Progress: Basics (checked), Settings (checked), **3 Scope tags**, 4 Assignments, 5 Review + create
- Text: Configure scope tags for this app config policy
- Section: Scope tags
- Content: Default
- Link: + Select scope tags
- Buttons: Previous, **Next**

**Assignments step:**

- Progress: Basics (checked), Settings (checked), Scope tags (checked), **4 Assignments**, 5 Review + create
- Section: Included groups
- Buttons: **Add groups**, Add all users, + Add all devices
- Section: Groups
- Item: SG-AndroidE-Test (Remove)
- Section: Excluded groups
- Info: When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more.](#)
- Buttons: + Add groups
- Section: Groups
- Text: No groups selected
- Buttons: Previous, **Next**

# Create and assign an Android Enterprise app configuration profile

- Select Create

✓ Basics
✓ Settings
✓ Scope tags
✓ Assignments
5 Review + create

Summary

**Basics**

Name: KAI Permission config  
 Description: --  
 Device enrollment type: Managed devices  
 Platform: Android Enterprise  
 Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work Profile Only  
 Targeted app: Knox Asset Intelligence

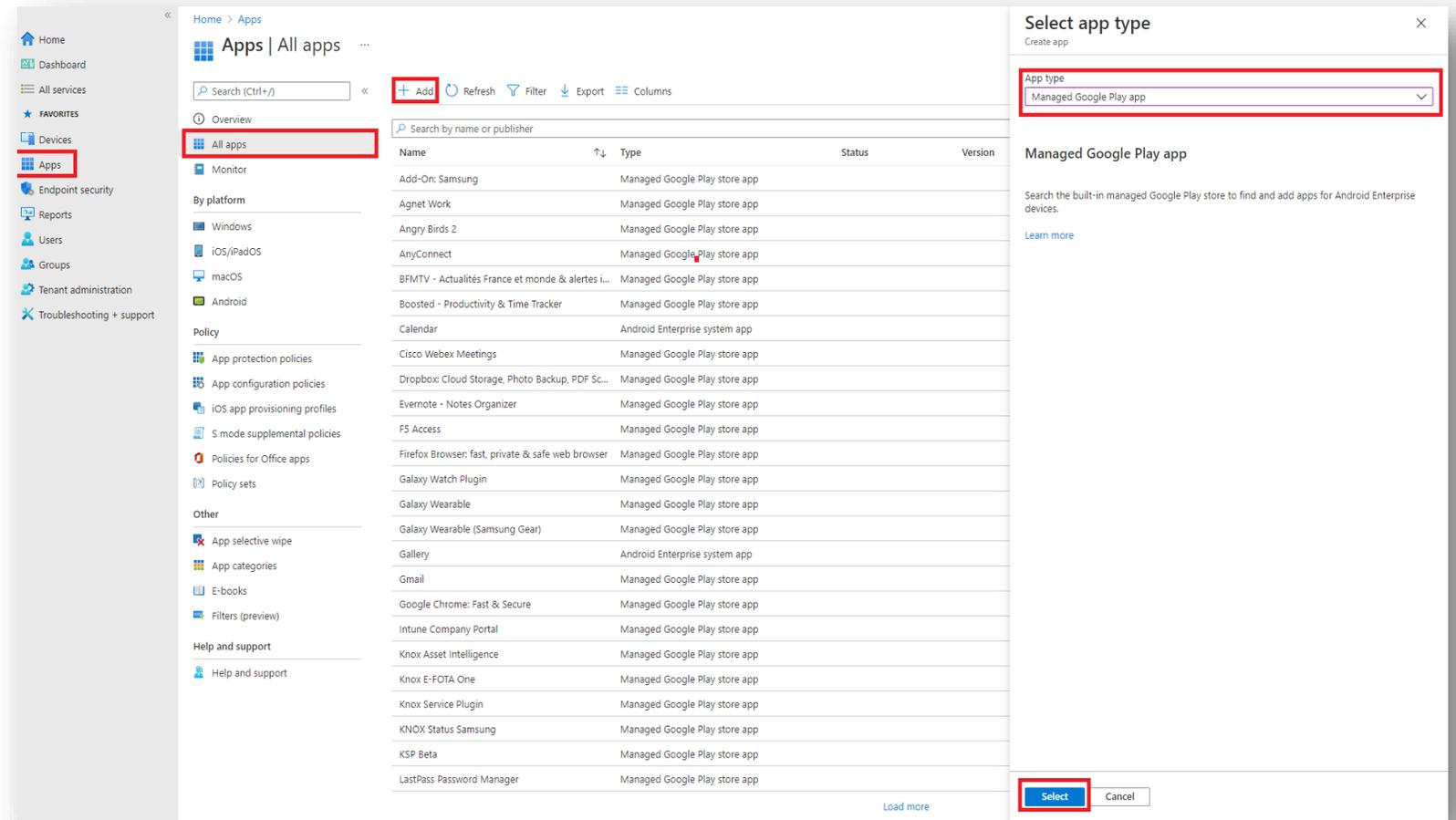
**Settings**

Permissions

Permission	Permission state	Permission name	Permission group
External storage (write)	Auto grant	WRITE_EXTERNAL_STORAGE	STORAGE
External storage (read)	Auto grant	READ_EXTERNAL_STORAGE	STORAGE
MMS (receive)	Auto grant	RECEIVE_MMS	SMS
WAP push messages (receive)	Auto grant	RECEIVE_WAP_PUSH	SMS
SMS (read)	Auto grant	READ_SMS	SMS
SMS (receive)	Auto grant	RECEIVE_SMS	SMS
SMS (send)	Auto grant	SEND_SMS	SMS
Allow body sensor data	Auto grant	BODY_SENSORS	SENSORS
Process outgoing calls	Auto grant	PROCESS_OUTGOING_CALLS	PHONE
Use SIP service	Auto grant	USE_SIP	PHONE
Add voicemail	Auto grant	ADD_VOICEMAIL	PHONE
Call log (write)	Auto grant	WRITE_CALL_LOG	PHONE
Call log (read)	Auto grant	READ_CALL_LOG	PHONE
Make phone calls	Auto grant	CALL_PHONE	PHONE
Phone state (read)	Auto grant	READ_PHONE_STATE	PHONE

# Add the Knox Service Plugin app to Intune

- Within the Intune console, select Apps
- Select All apps
- Select Add
- For App type, select Managed Google Play app
- Select

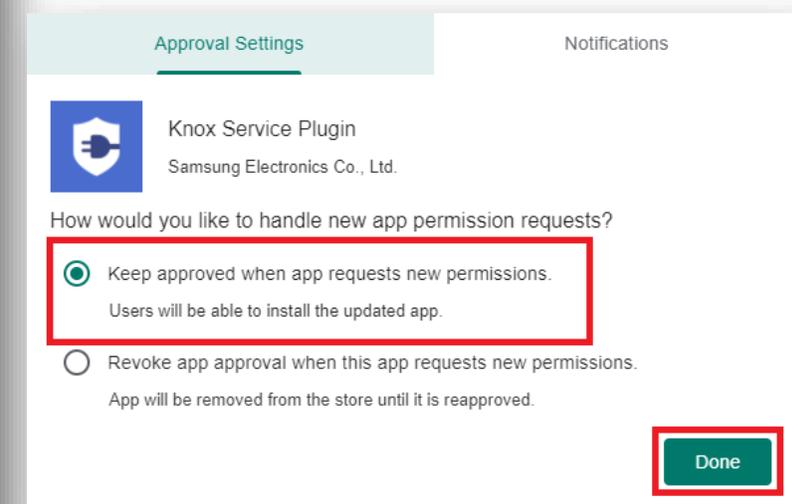
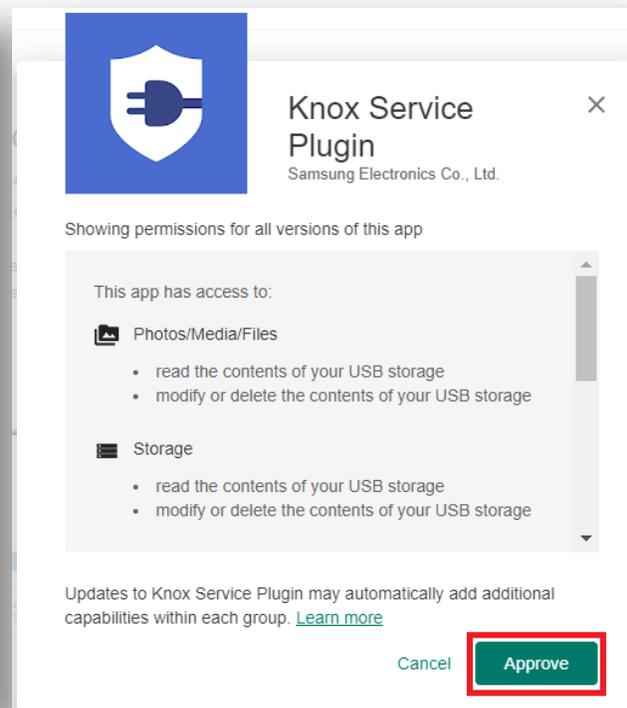
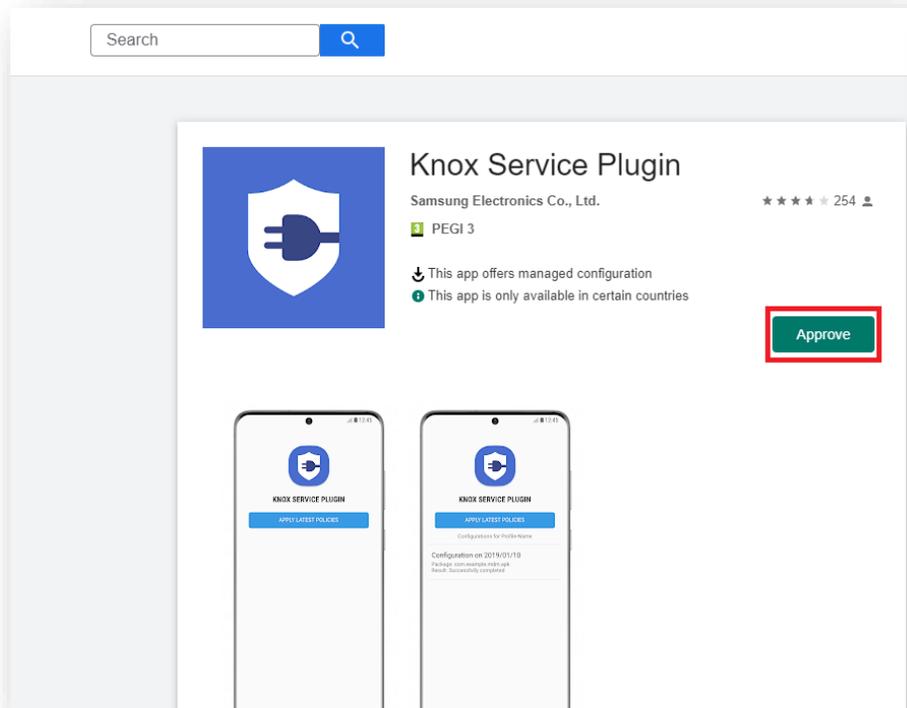


The screenshot shows the Microsoft Intune console interface. On the left is a navigation pane with 'Apps' selected. The main area displays 'Apps | All apps' with a table of installed applications. A red box highlights the '+ Add' button in the top right of the table area. Another red box highlights the 'All apps' link in the left-hand navigation pane. A third red box highlights the 'Managed Google Play app' option in the 'App type' dropdown menu of a 'Select app type' dialog box. The dialog also shows a 'Select' button highlighted with a red box.

Name	Type	Status	Version
Add-On: Samsung	Managed Google Play store app		
Agnet Work	Managed Google Play store app		
Angry Birds 2	Managed Google Play store app		
AnyConnect	Managed Google Play store app		
BFMTV - Actualités France et monde & alertes i...	Managed Google Play store app		
Boosted - Productivity & Time Tracker	Managed Google Play store app		
Calendar	Android Enterprise system app		
Cisco Webex Meetings	Managed Google Play store app		
Dropbox: Cloud Storage, Photo Backup, PDF Sc...	Managed Google Play store app		
Evernote - Notes Organizer	Managed Google Play store app		
F5 Access	Managed Google Play store app		
Firefox Browser: fast, private & safe web browser	Managed Google Play store app		
Galaxy Watch Plugin	Managed Google Play store app		
Galaxy Wearable	Managed Google Play store app		
Galaxy Wearable (Samsung Gear)	Managed Google Play store app		
Gallery	Android Enterprise system app		
Gmail	Managed Google Play store app		
Google Chrome: Fast & Secure	Managed Google Play store app		
Intune Company Portal	Managed Google Play store app		
Knox Asset Intelligence	Managed Google Play store app		
Knox E-FOTA One	Managed Google Play store app		
Knox Service Plugin	Managed Google Play store app		
KNOX Status Samsung	Managed Google Play store app		
KSP Beta	Managed Google Play store app		
LastPass Password Manager	Managed Google Play store app		

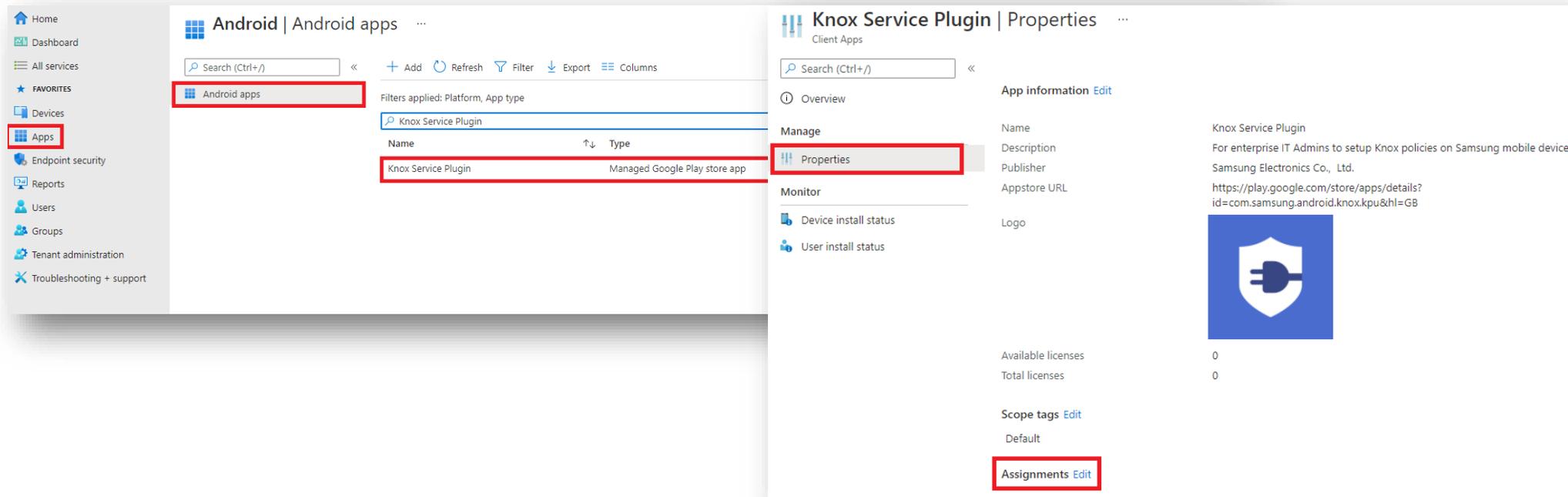
# Add the Knox Service Plugin app to Intune

- Search for the Knox Service Plugin App
- Select Approve
- Select Approve
- Select Keep approved when app requests new permissions
- Select Done



# Deploy the Knox Service Plugin app to the devices

- Select Apps
- Select Android apps
- Search for and select Knox Service Plugin
- Select Properties
- Next to Assignments, select Edit



The screenshot shows the Knox console interface with the following steps highlighted by red boxes:

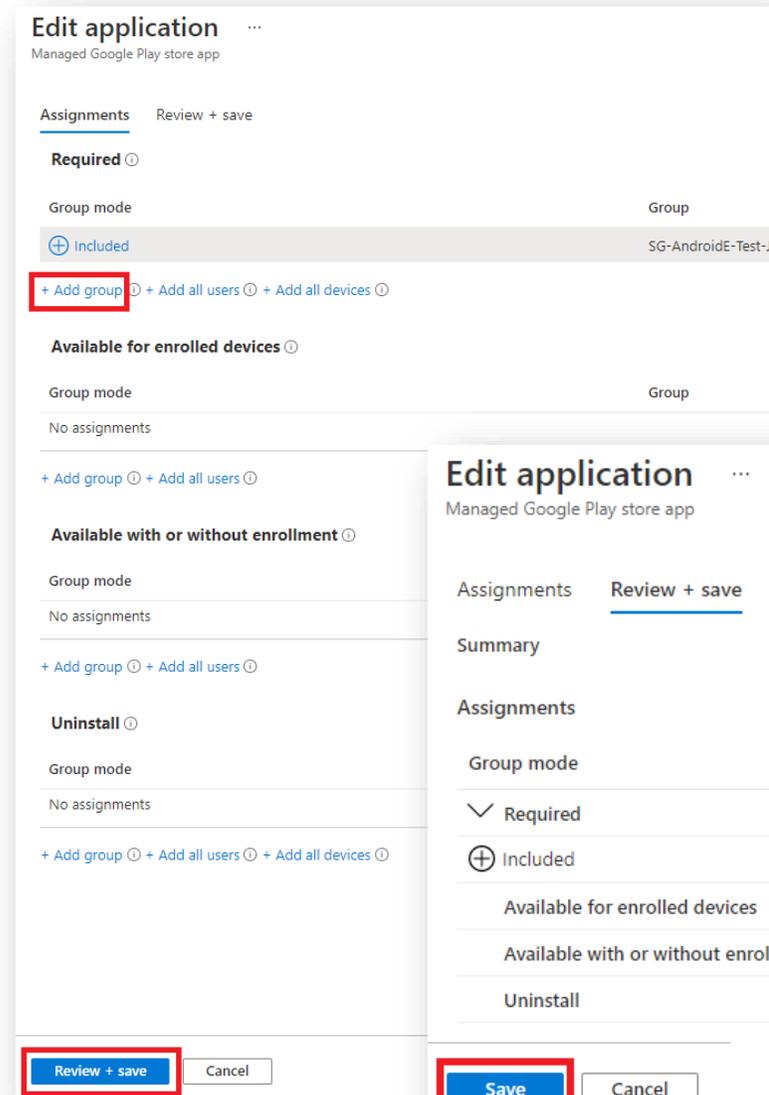
- Apps** in the left sidebar.
- Android apps** in the main content area.
- Knox Service Plugin** in the search results table.
- Properties** in the Manage section of the app details.
- Assignments** in the bottom right of the app details.

The app details for **Knox Service Plugin** are as follows:

Section	Item	Value
App information	Name	Knox Service Plugin
	Description	For enterprise IT Admins to setup Knox policies on Samsung mobile devices.
	Publisher	Samsung Electronics Co., Ltd.
	Appstore URL	<a href="https://play.google.com/store/apps/details?id=com.samsung.android.knox.kpu&amp;hl=GB">https://play.google.com/store/apps/details?id=com.samsung.android.knox.kpu&amp;hl=GB</a>
Monitor	Device install status	Logo
	User install status	
Licenses	Available licenses	0
	Total licenses	0
Scope tags	Default	
	Assignments	<a href="#">Edit</a>

# Deploy the Knox Service Plugin app to the devices

- Under Required, Select Add group
- Add an assignment group
- Select Review + save
- Select Save



**Edit application** ...  
Managed Google Play store app

Assignments [Review + save](#)

**Required** ⓘ

Group mode Group

⊕ Included SG-AndroidE-Test-JK

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

**Available for enrolled devices** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ

**Available with or without enrollment** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ

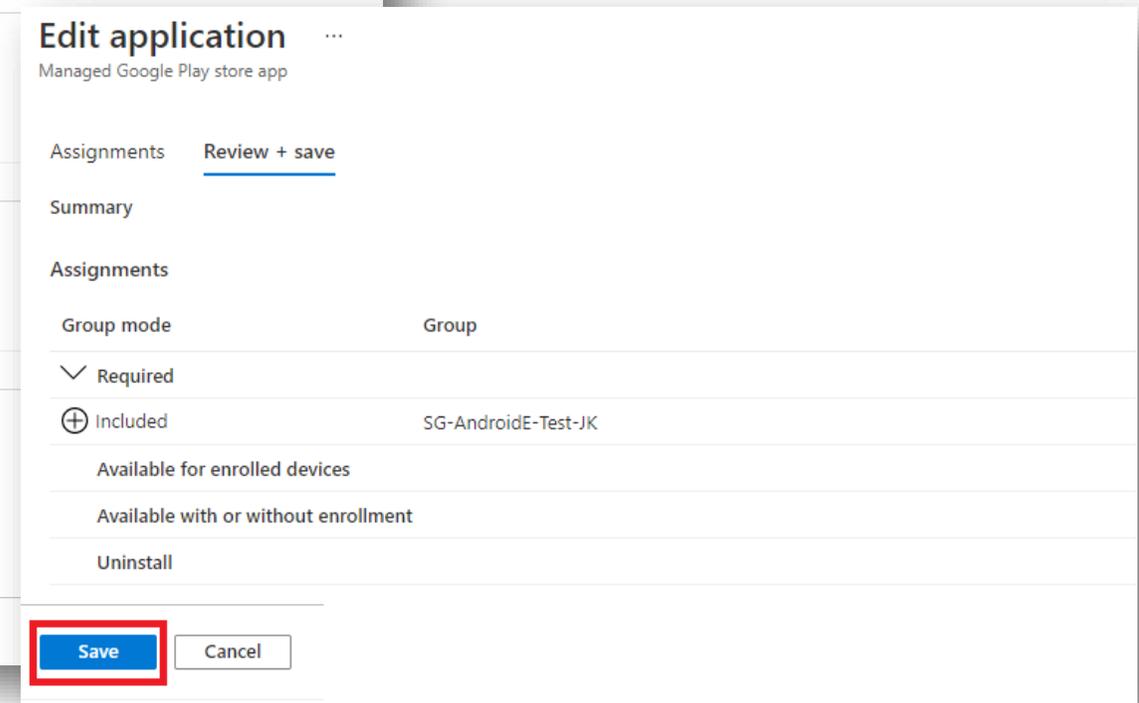
**Uninstall** ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

Review + save



**Edit application** ...  
Managed Google Play store app

Assignments [Review + save](#)

Summary

Assignments

Group mode Group

∨ Required

⊕ Included SG-AndroidE-Test-JK

Available for enrolled devices

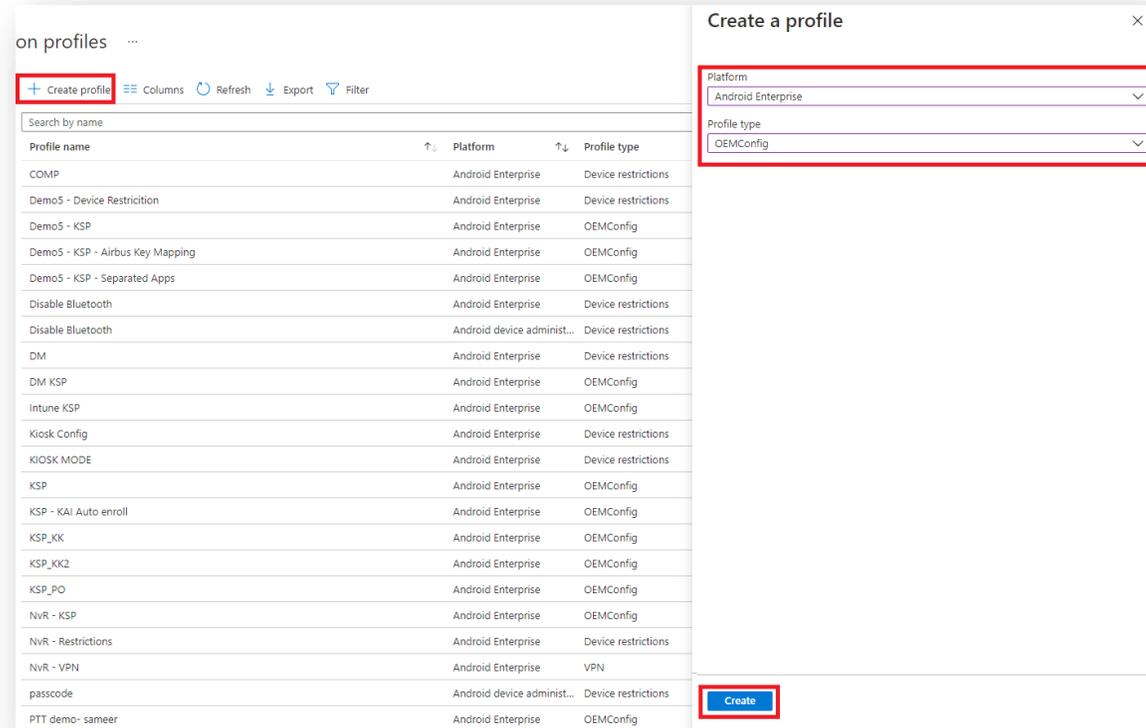
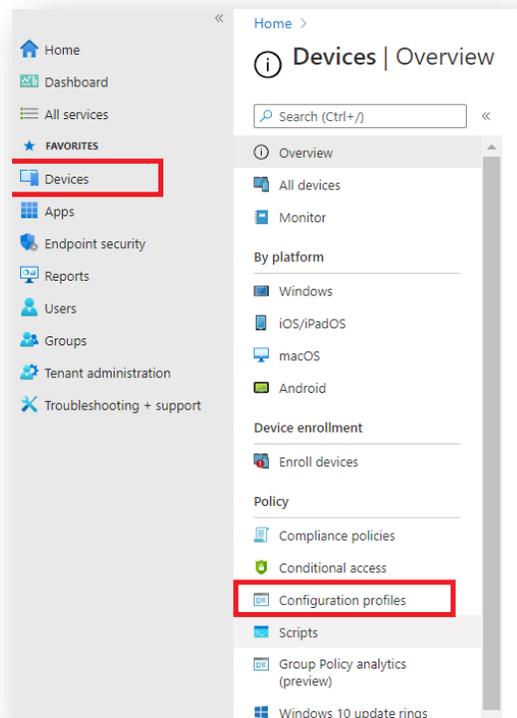
Available with or without enrollment

Uninstall

Save

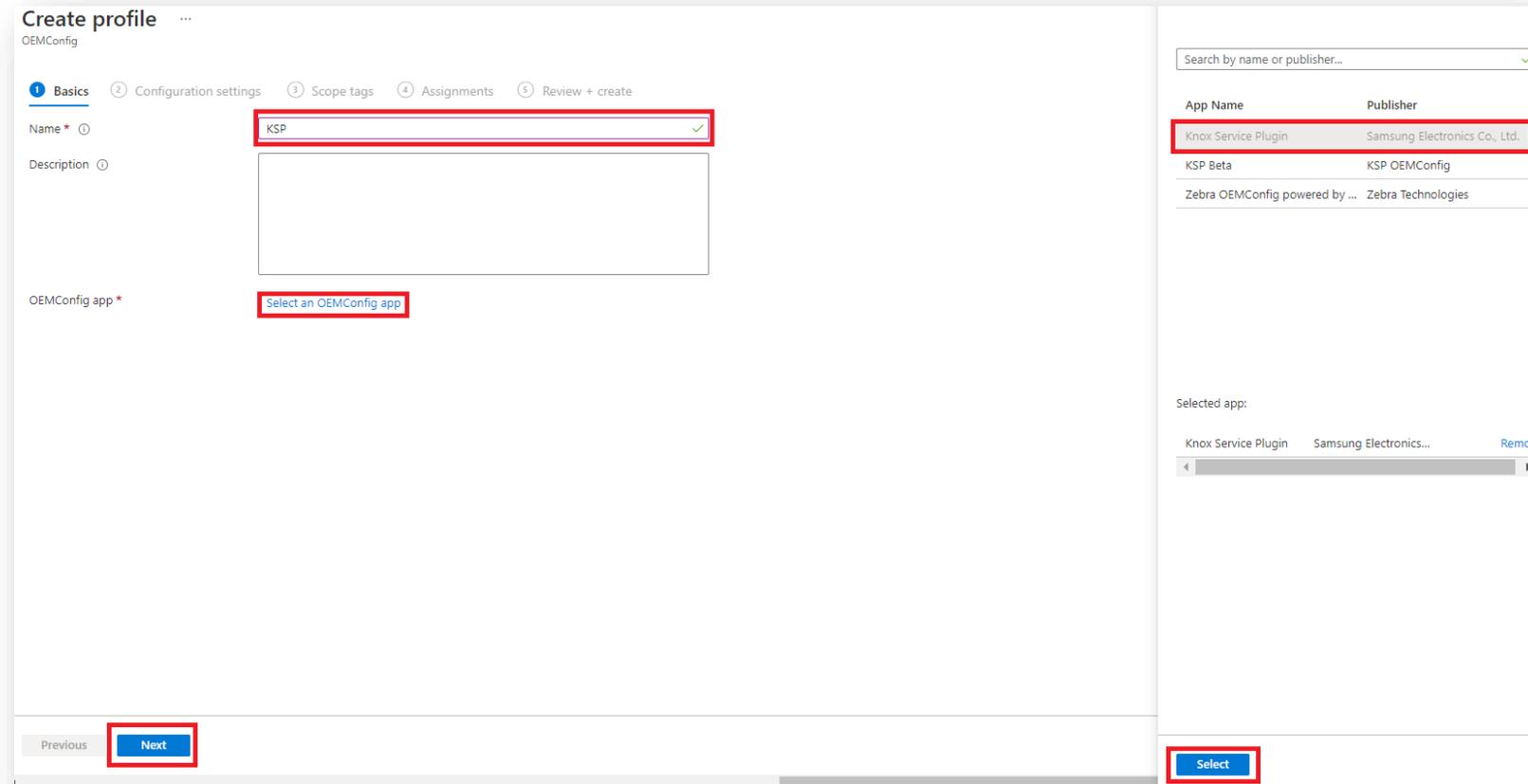
# Create an Android Enterprise OEMConfig profile

- Select Devices
- Select Configuration profiles
- Select Create profile
- For Platform, select Android Enterprise
- For Profile type, select OEMConfig
- Select Create



# Create an Android Enterprise OEMConfig profile

- Enter a profile Name
- Select an OEMConfig app
- Select the Knox Service Plugin
- Select
- Next



**Create profile** ...  
OEMConfig

1 Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

Name \*

Description

OEMConfig app \*

Previous

Search by name or publisher... ✓

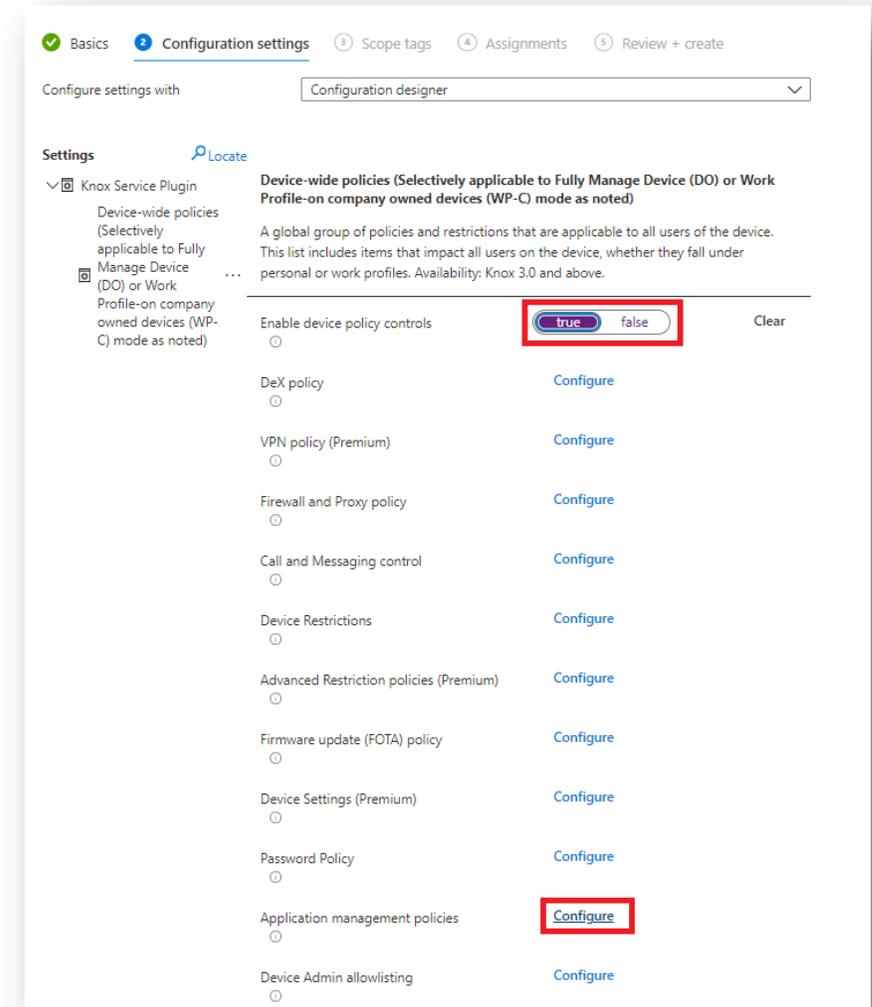
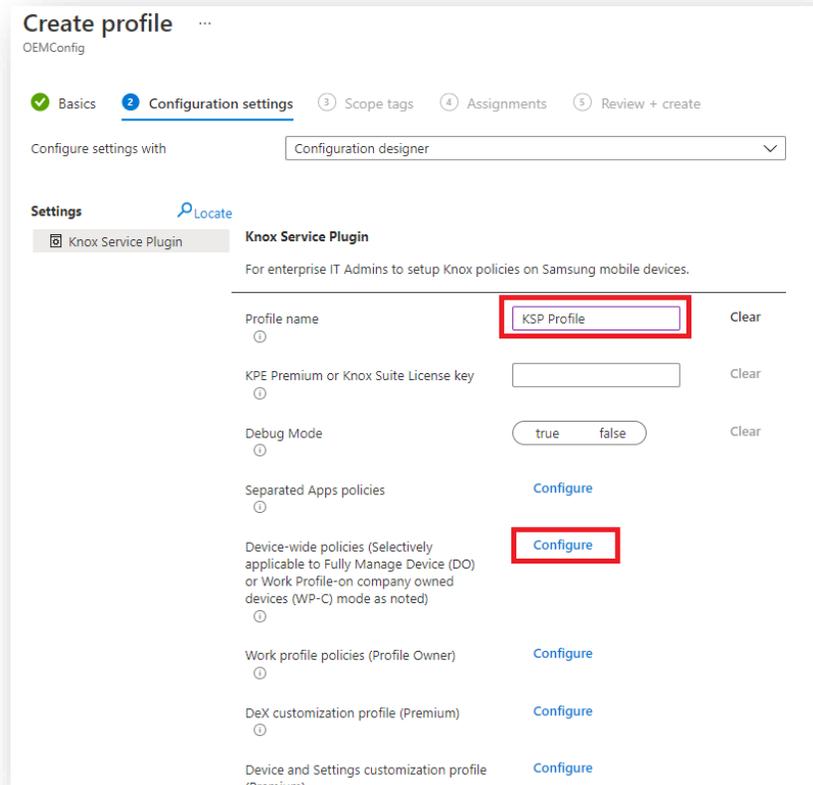
App Name	Publisher
Knox Service Plugin	Samsung Electronics Co., Ltd.
KSP Beta	KSP OEMConfig
Zebra OEMConfig powered by ...	Zebra Technologies

Selected app:

Knox Service Plugin Samsung Electronics...

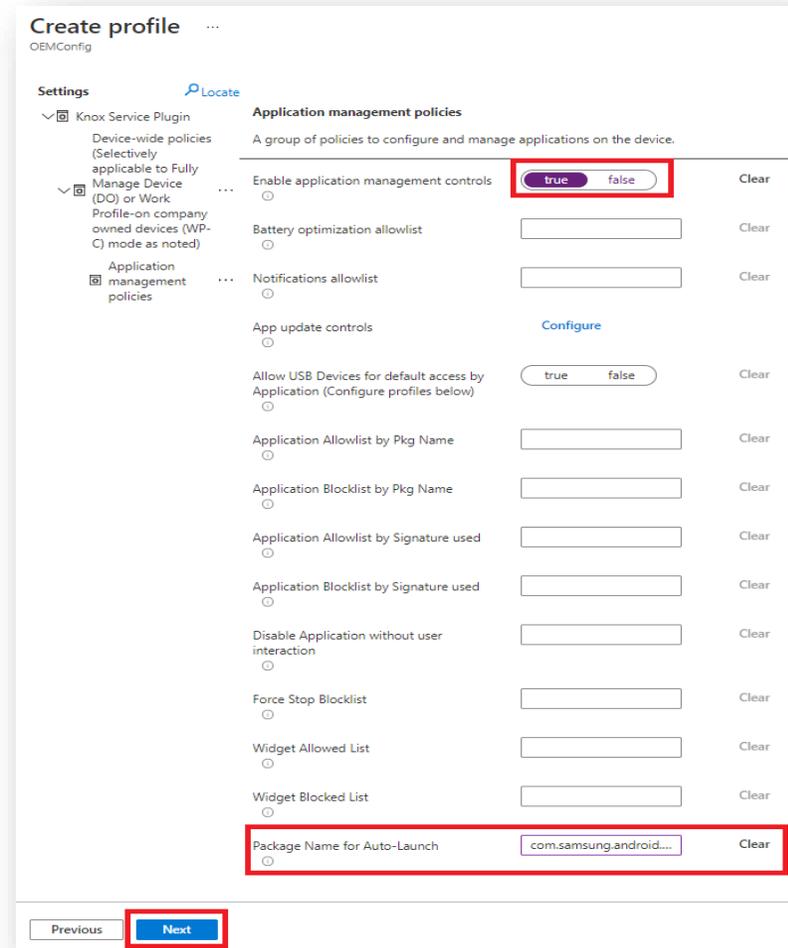
# Create an Android Enterprise OEMConfig profile

- Enter a Profile name
- For Device-wide policies, select Configure
- For Enable device policy controls, select True
- Select Configure next to Application management policies



# Create an Android Enterprise OEMConfig profile

- For Enable application management controls, select true
- For Package Name for Auto-Launch, enter: com.samsung.android.knox.dai
- Select Next



The screenshot shows the 'Create profile' screen for an OEMConfig profile. The 'Settings' section is expanded to show 'Application management policies'. The 'Enable application management controls' toggle is set to 'true'. The 'Package Name for Auto-Launch' field contains the value 'com.samsung.android.knox.dai'. The 'Next' button is highlighted.

Policy Name	Value	Action
Enable application management controls	true	Clear
Battery optimization allowlist		Clear
Notifications allowlist		Clear
App update controls	Configure	
Allow USB Devices for default access by Application (Configure profiles below)	true	Clear
Application Allowlist by Pkg Name		Clear
Application Blocklist by Pkg Name		Clear
Application Allowlist by Signature used		Clear
Application Blocklist by Signature used		Clear
Disable Application without user interaction		Clear
Force Stop Blocklist		Clear
Widget Allowed List		Clear
Widget Blocked List		Clear
Package Name for Auto-Launch	com.samsung.android.knox.dai	Clear

Navigation: Previous, **Next**

# Create an Android Enterprise OEMConfig profile

- Scope tags are optional, select Next
- Select Add groups and select your desired assignment group
- Select Next
- Select Create

The image displays three sequential screenshots of the 'Create profile' wizard in the OEMConfig interface, illustrating the steps from group selection to profile creation.

**First Screenshot (Left):** Shows the 'Create profile' wizard with the 'Assignments' step (4) highlighted. The 'Add groups' button is highlighted with a red box. Below the wizard, the 'Next' button is also highlighted with a red box.

**Second Screenshot (Middle):** Shows the 'Add groups' step where the 'SG-AndroidE-Test-JK' group is selected. The 'Next' button is highlighted with a red box.

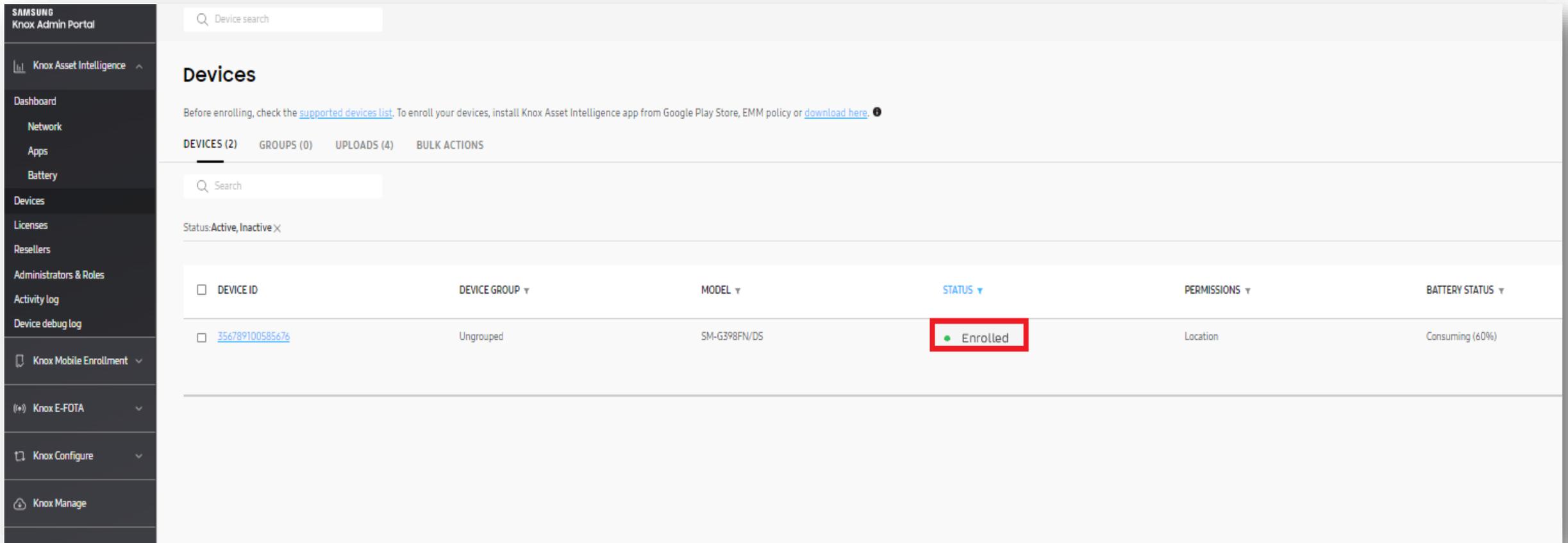
**Third Screenshot (Right):** Shows the 'Review + create' step (5) where the profile details are reviewed. The 'Create' button is highlighted with a red box.

**Profile Details (from the third screenshot):**

- Basics:** Name: KSP, Description: --, OEMConfig app: Knox Service Plugin
- Configuration settings:** Profile name: KSP Profile
- Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted):** Enable device policy controls: true
- Application management policies:** Enable application management controls: true, Package Name for Auto-Launch: com.samsung.android.knox.dai
- Scope tags:** Default
- Assignments:** Included groups: SG-AndroidE-Test-JK, Excluded groups: --

# Check the devices have enrolled

- Open Knox Asset Intelligence
- Select the Devices tab
- Check the Status of the devices are now marked as Enrolled

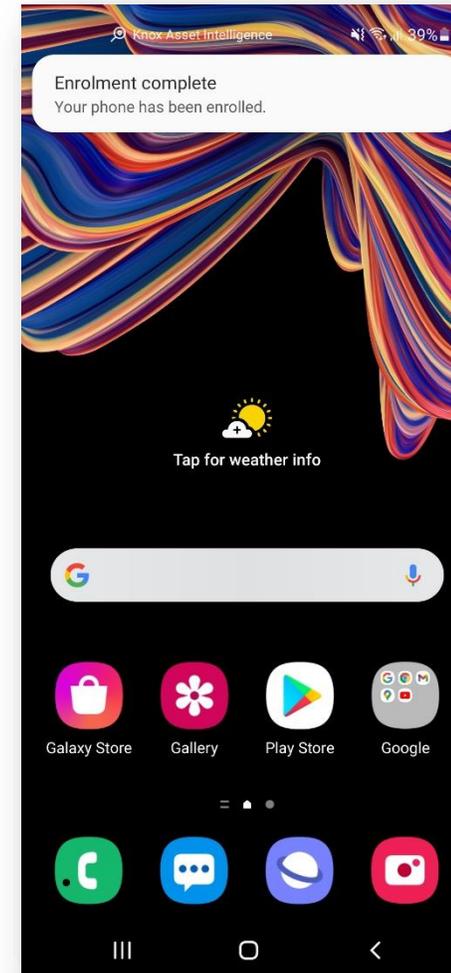
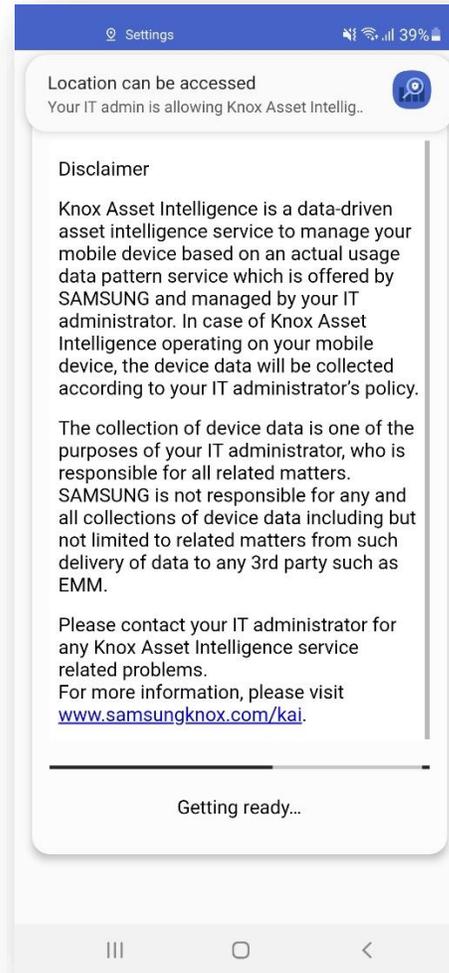
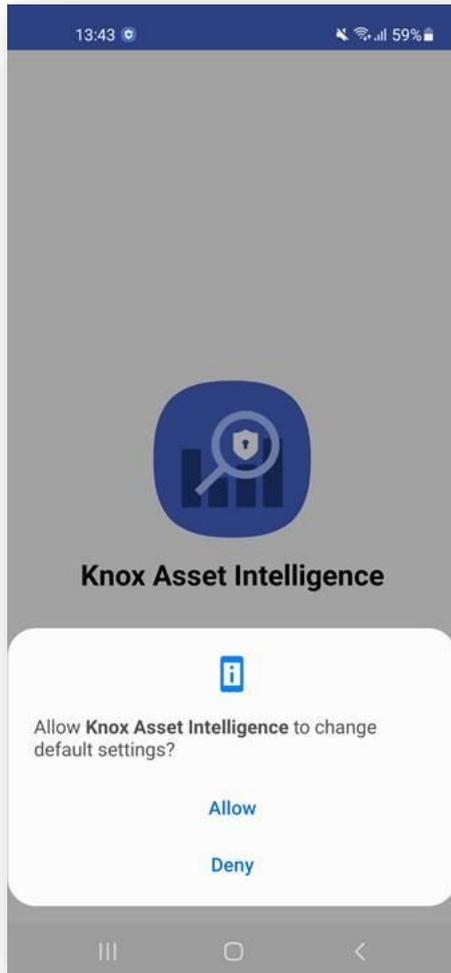


The screenshot shows the Samsung Knox Admin Portal interface. On the left is a dark sidebar with navigation options: Dashboard, Network, Apps, Battery, Devices, Licenses, Resellers, Administrators & Roles, Activity log, Device debug log, Knox Mobile Enrollment, Knox E-FOTA, Knox Configure, and Knox Manage. The main content area is titled 'Devices' and includes a search bar and a status filter set to 'Active, Inactive'. Below this is a table with columns for Device ID, Device Group, Model, Status, Permissions, and Battery Status. One device is listed with ID 356789100585676, Model SM-G398FN/DS, and Status 'Enrolled', which is highlighted with a red box.

DEVICES (2)	GROUPS (0)	UPLOADS (4)	BULK ACTIONS			
DEVICE ID	DEVICE GROUP	MODEL	STATUS	PERMISSIONS	BATTERY STATUS	
<input type="checkbox"/> <a href="#">356789100585676</a>	Ungrouped	SM-G398FN/DS	<span style="border: 2px solid red; padding: 2px;">● Enrolled</span>	Location	Consuming (60%)	

# KAI enrollment

- Once the KAI app has been deployed with the Android Enterprise permission profile, the end user will see the below steps.



# Document Information

This is version 1.1 of this document.

Thank you!

