

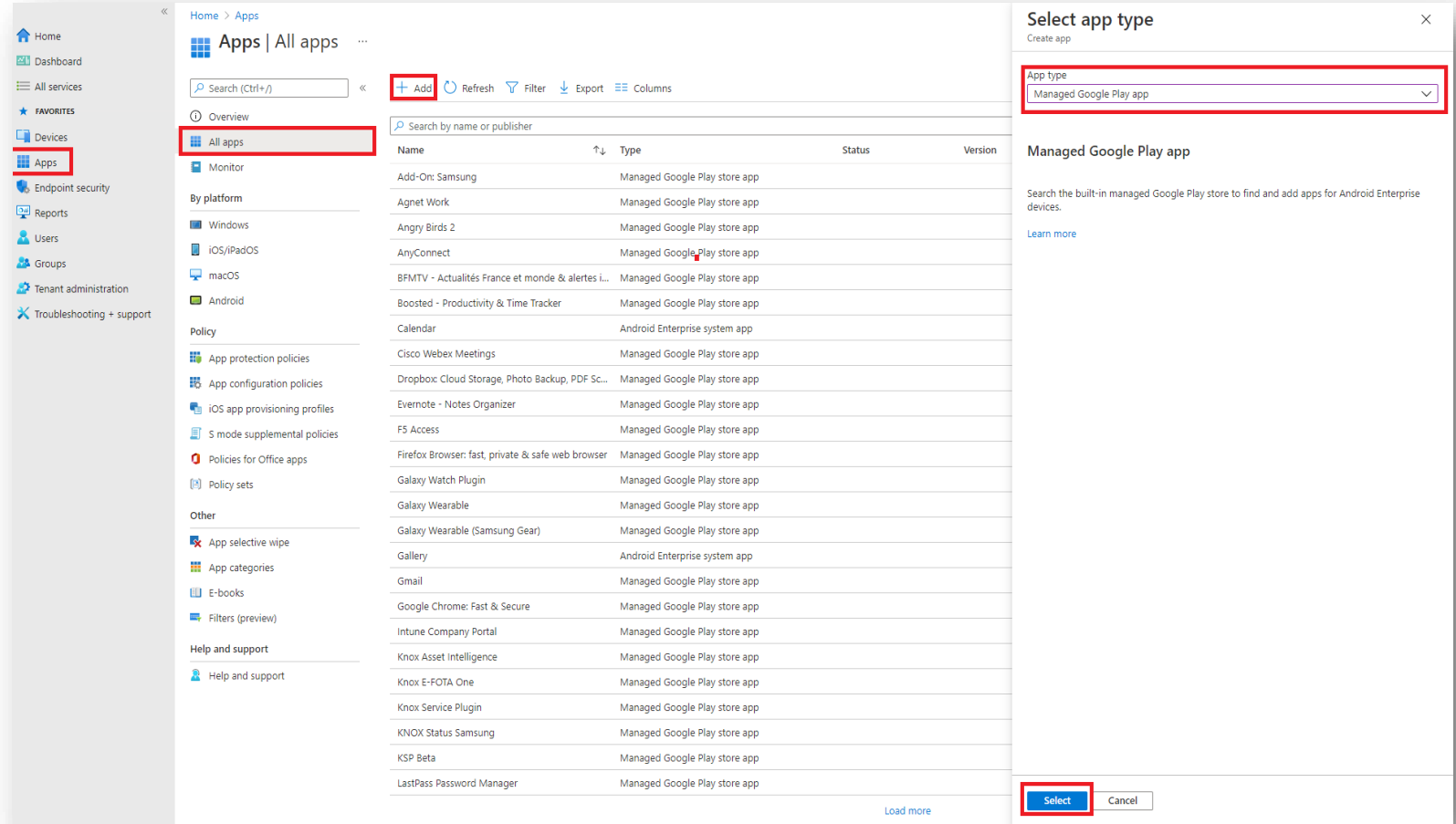
Knox Asset Intelligence (KAI) – Intune Auto Enroll

July 2021
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

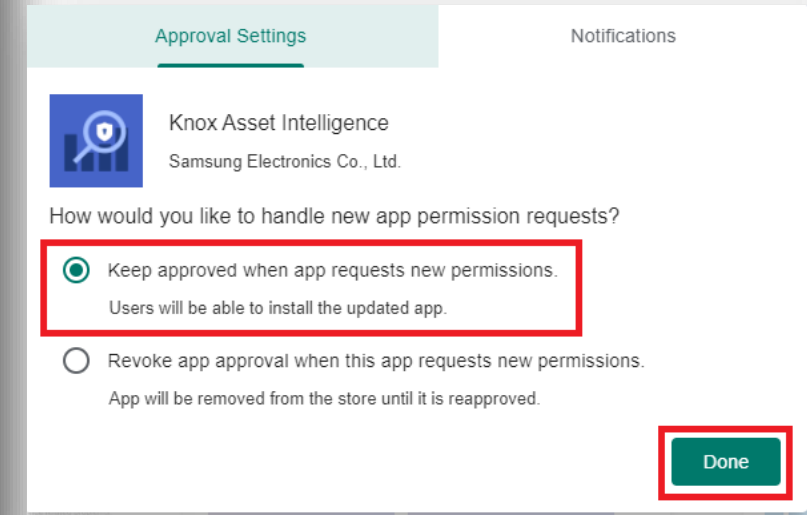
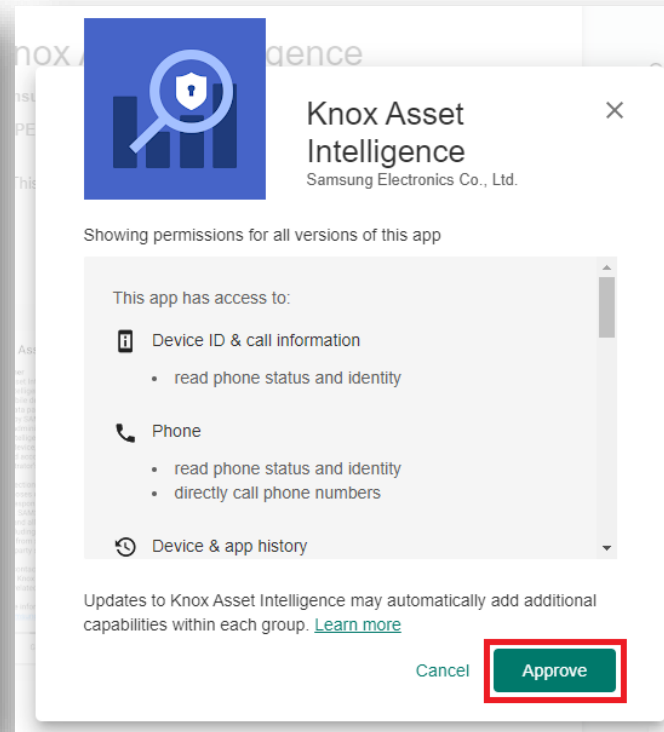
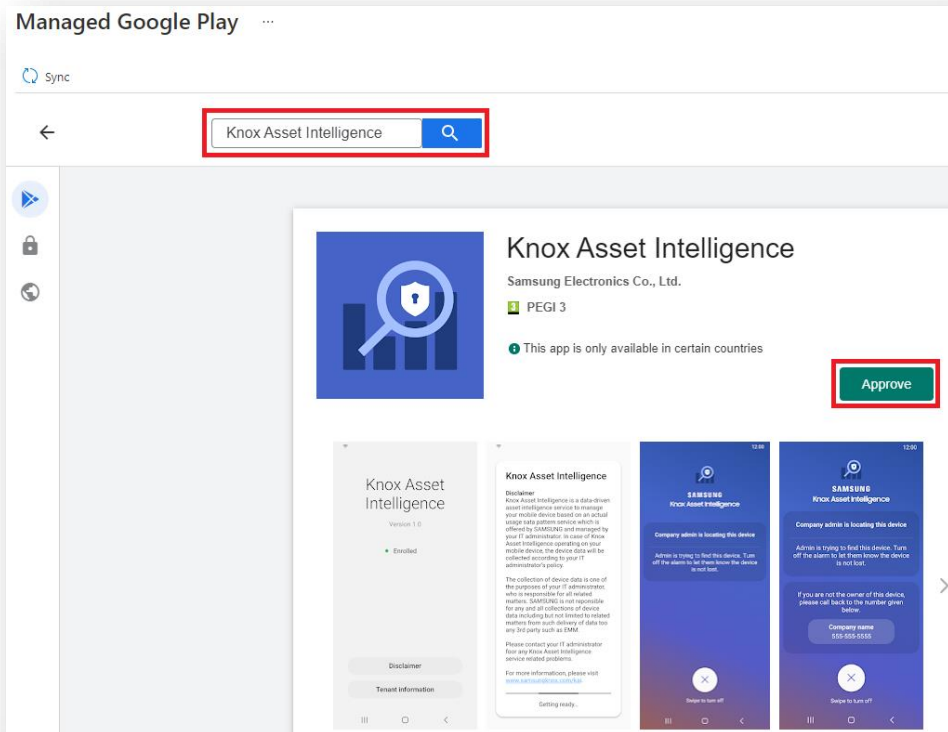


The screenshot shows the Microsoft Intune console interface. On the left sidebar, the 'Apps' section is highlighted. In the main content area, the 'All apps' link is selected. The 'Add' button is highlighted in the top bar. The 'Select app type' dialog is open, showing 'Managed Google Play app' as the selected option. The 'Select' button is highlighted at the bottom of the dialog.

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		

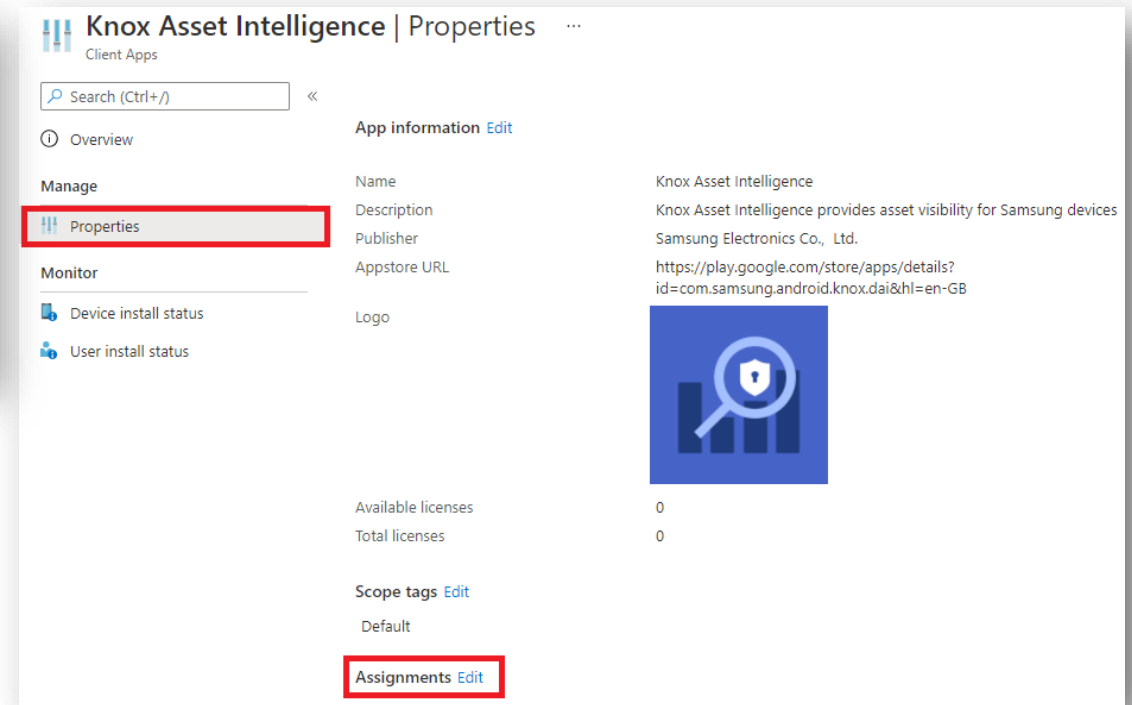
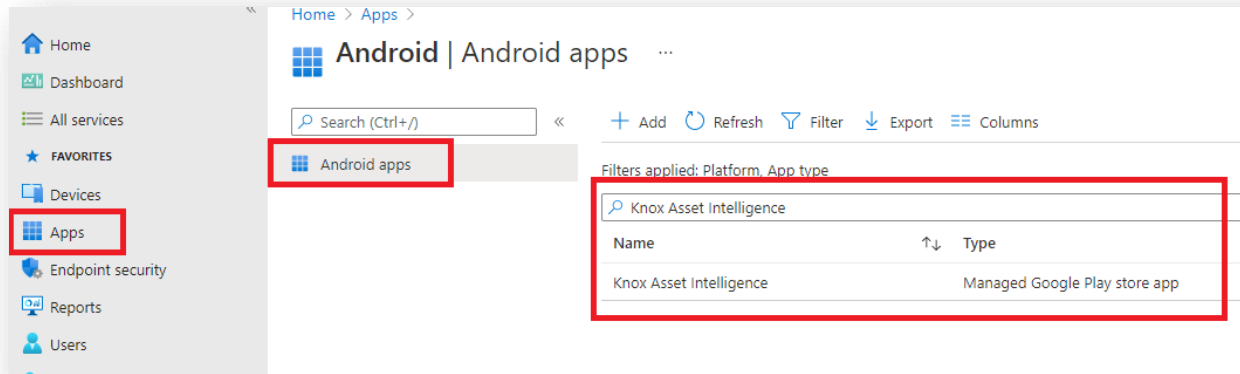
Add the Knox Asset Intelligence app to Intune

- 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

No assignments

+ Add group ⓘ

+ Add all users ⓘ

Uninstall ⓘ

Group mode

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

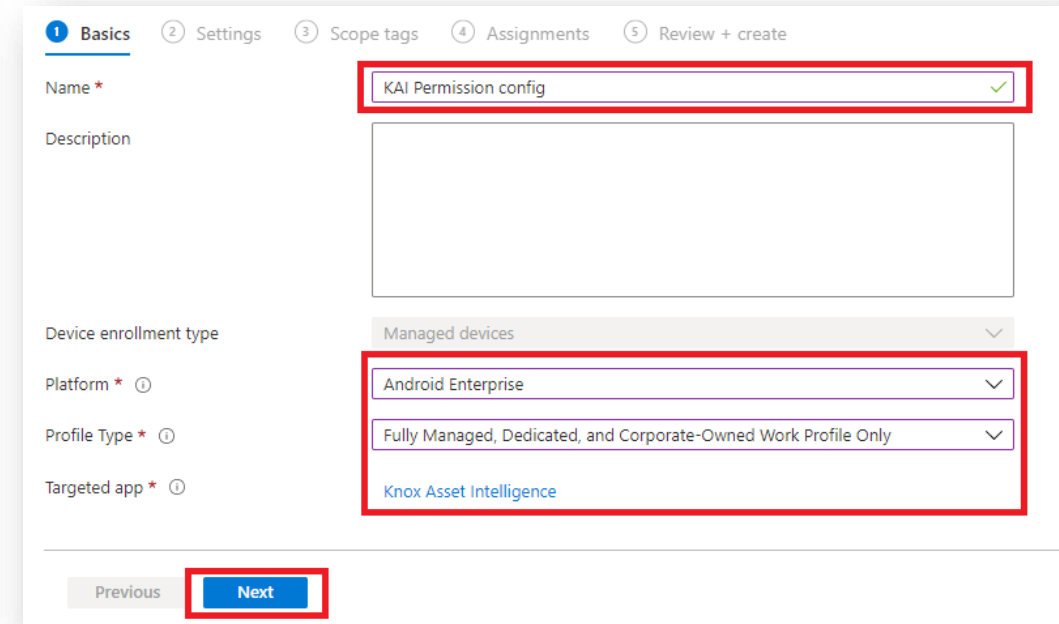
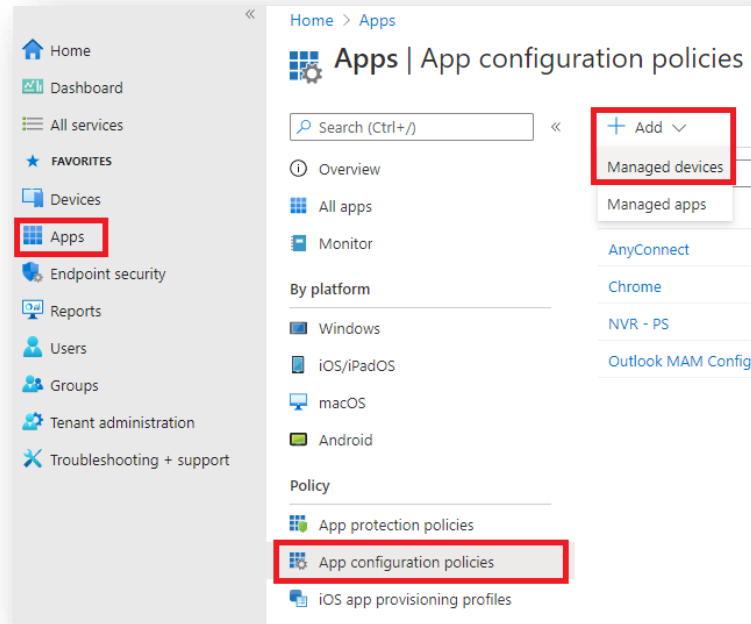
Uninstall

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

2 Settings

3 Scope tags

4 Assignments

5 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

+ Add

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 sequential screenshots of the Android Enterprise app configuration wizard interface.

First Screenshot (Scope tags step):

- Progress bar: Basics (checked), Settings (checked), **3 Scope tags** (active), 4 Assignments, 5 Review + create.
- Section: Configure scope tags for this app config policy.
- Scope tags: Default.
- Buttons: + Select scope tags, Previous, **Next** (highlighted with a red box).

Second Screenshot (Assignments step):

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

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

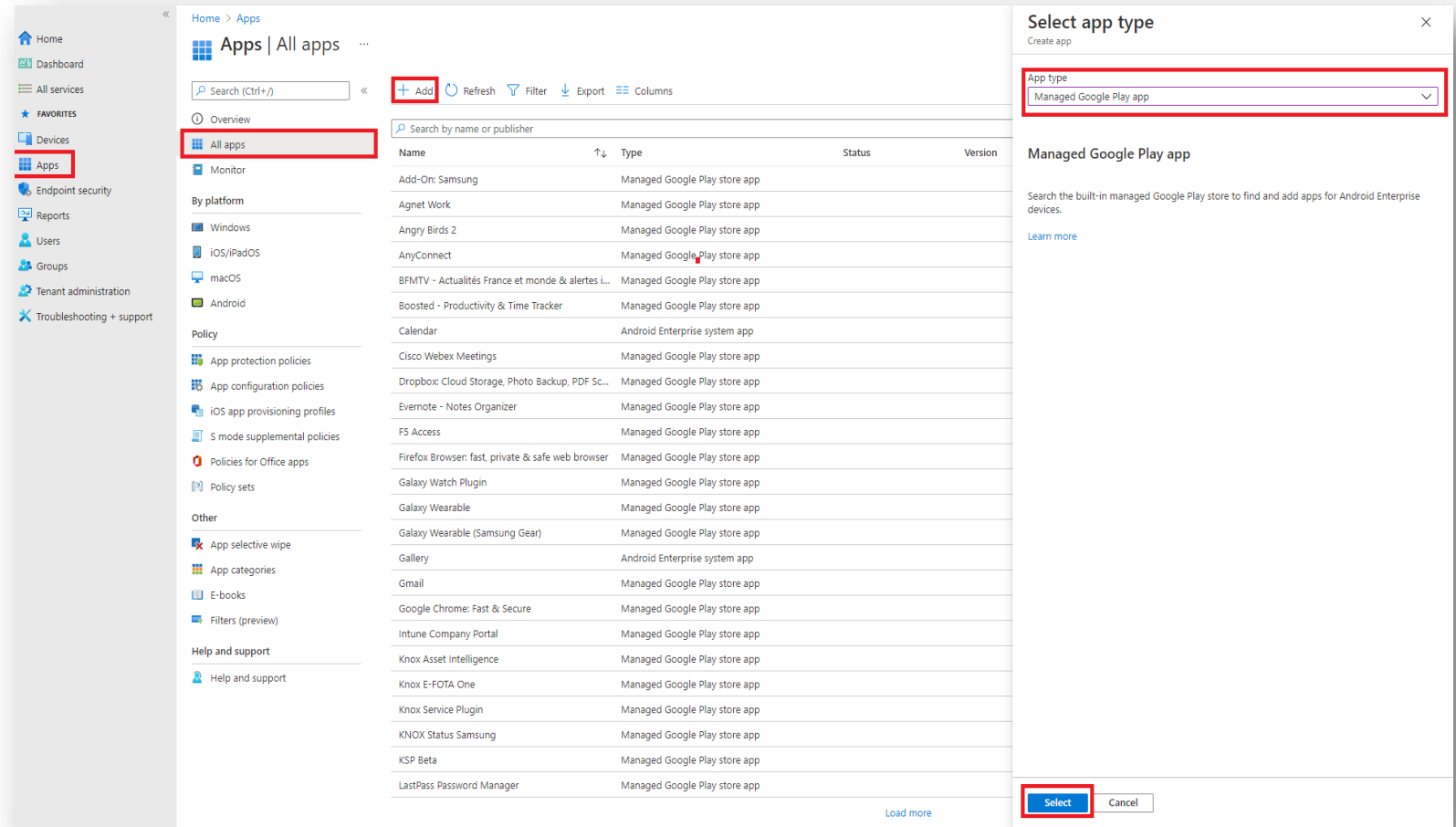
Permission	Permission state	Permission name	Permission group
External storage (write)	Auto grant	WRITE_EXTERNAL_STORAGE	STORAGE
External storage (read)	Auto grant	READ_EXTERNAL_STORAGE	STORAGE
MMS (receive)	Auto grant	RECEIVE_MMS	SMS
WAP push messages (receive)	Auto grant	RECEIVE_WAP_PUSH	SMS
SMS (read)	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

Previous

Create

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

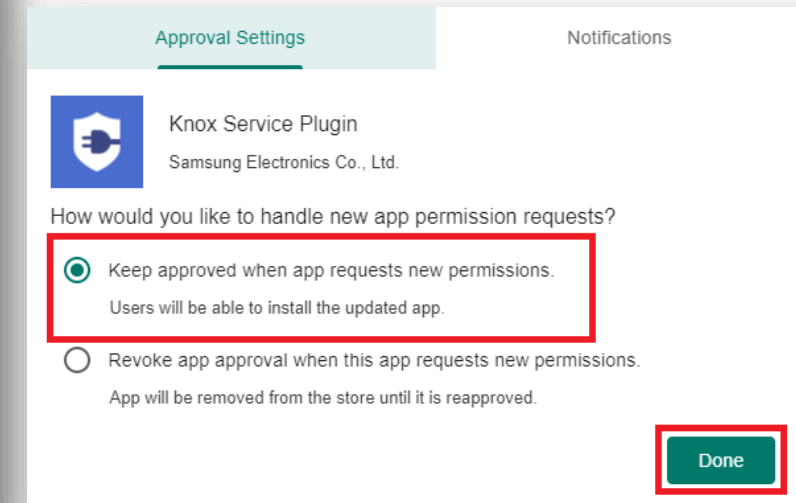
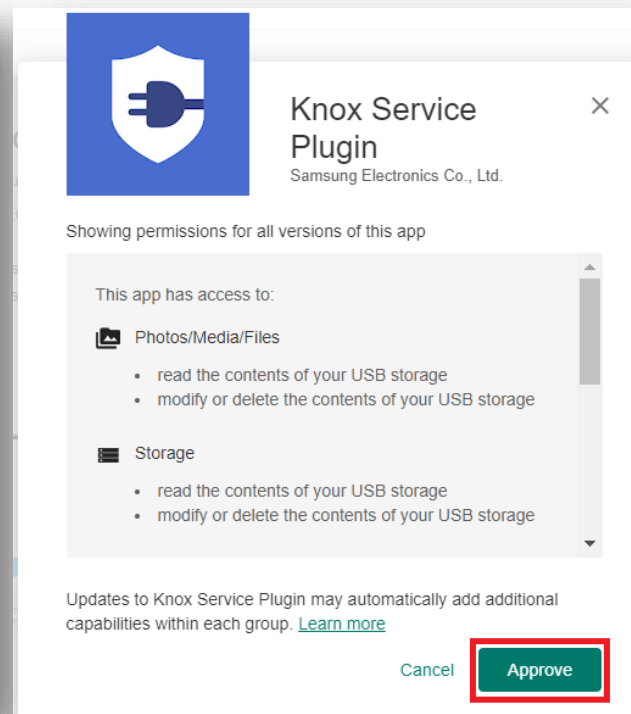
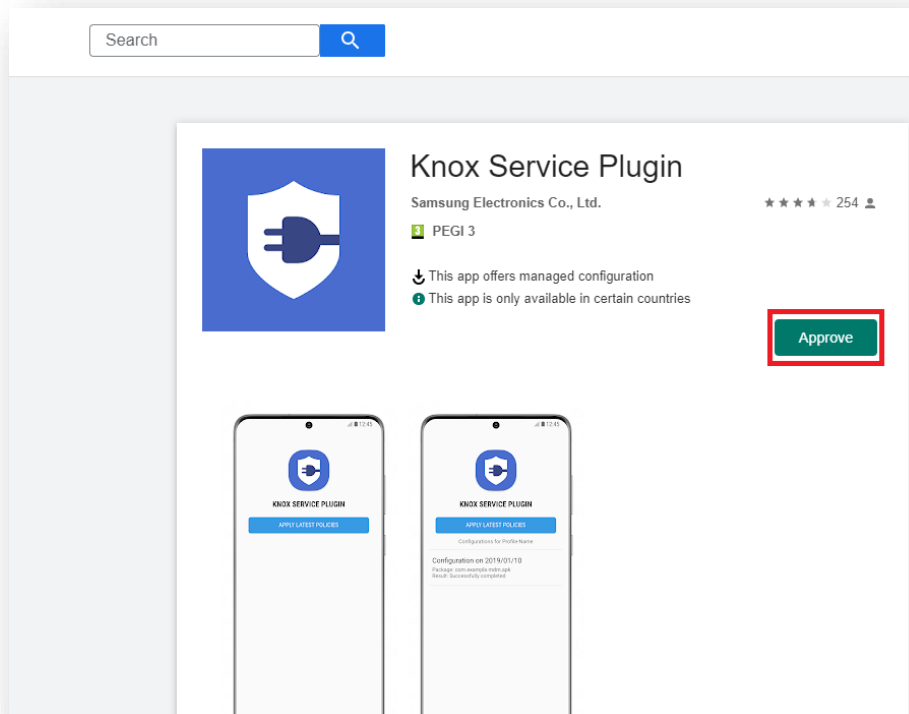


The screenshot shows the Microsoft Intune console interface. On the left sidebar, the 'Apps' section is selected. The main area displays the 'Apps | All apps' view. The 'Add' button is highlighted with a red box. A modal window titled 'Select app type' is open on the right, showing 'Managed Google Play app' as the selected option. 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		

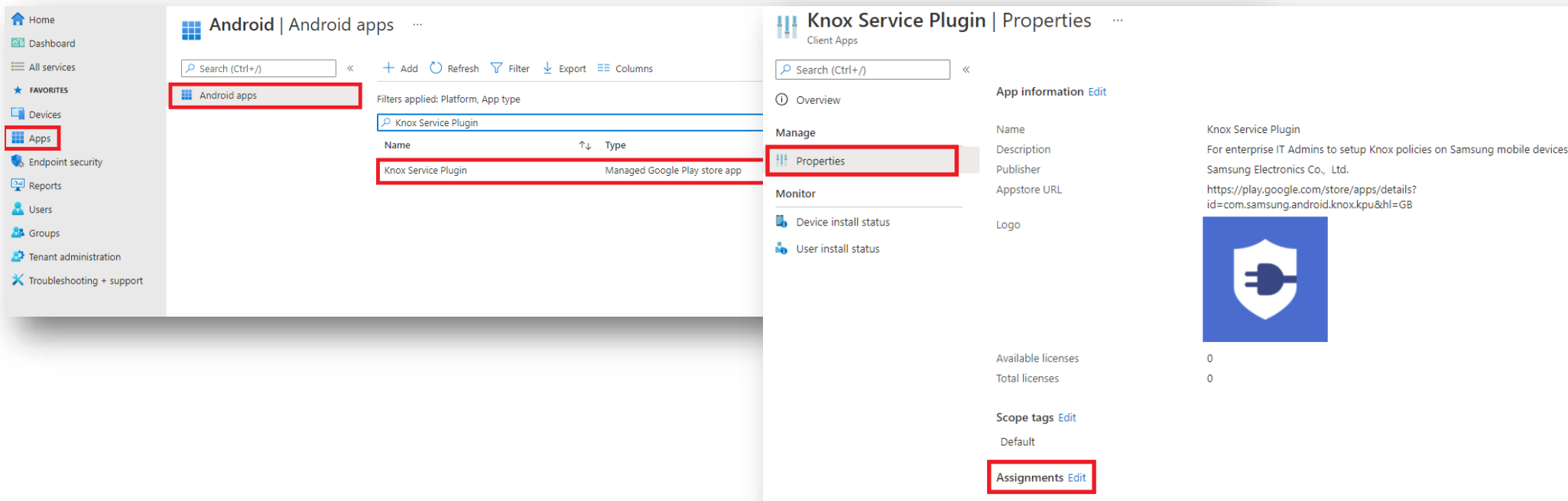
Add the Knox Service Plugin app to Intune

- 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 displays the Knox Service Plugin deployment interface, divided into two main panels. The left panel, titled "Android | Android apps", shows a list of apps with "Knox Service Plugin" selected. The right panel, titled "Knox Service Plugin | Properties", shows the app's details and the "Assignments" tab selected.

Left Panel: Android | Android apps

- Search bar: Search (Ctrl+/)
- Buttons: Add, Refresh, Filter, Export, Columns
- Filters applied: Platform, App type
- Table of apps:

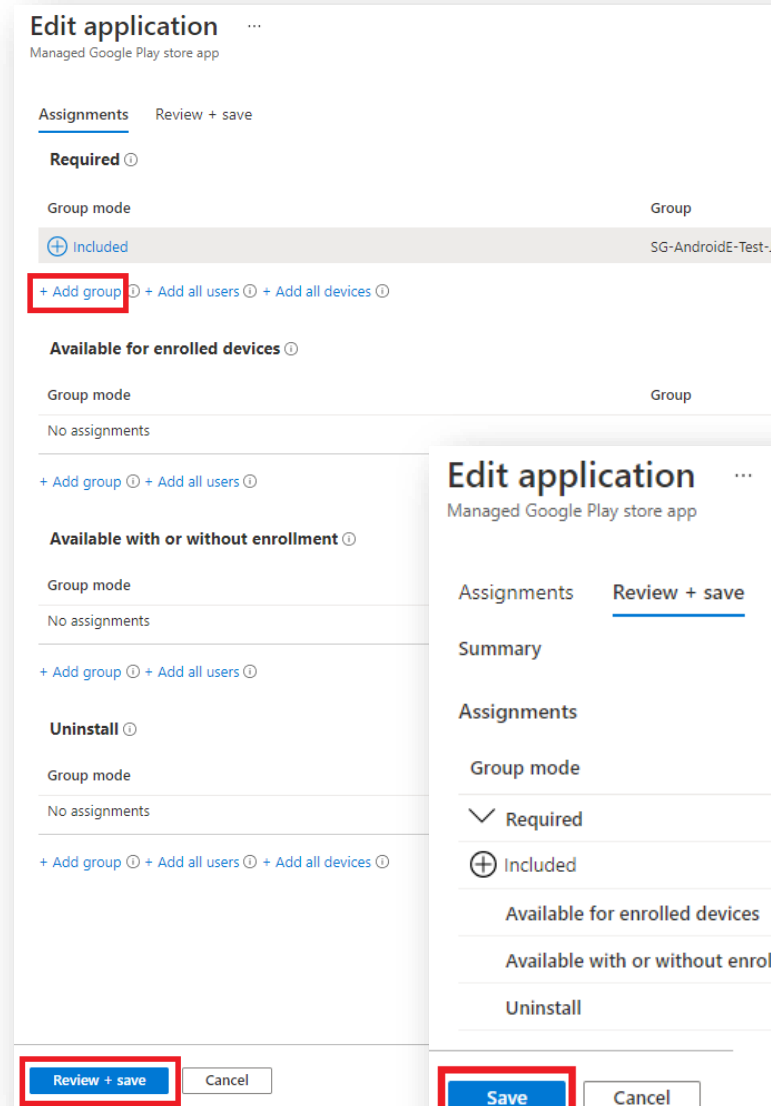
Name	Type
Knox Service Plugin	Managed Google Play store app

Right Panel: Knox Service Plugin | Properties

- Search bar: Search (Ctrl+/)
- Overview tab selected
- Manage tab selected
- Monitor tab selected
- Device install status
- User install status
- App information Edit
- Name: Knox Service Plugin
- Description: For enterprise IT Admins to setup Knox policies on Samsung mobile devices.
- Publisher: Samsung Electronics Co., Ltd.
- Appstore URL: <https://play.google.com/store/apps/details?id=com.samsung.android.knox.kpu&hl=GB>
- Logo: 
- Available licenses: 0
- Total licenses: 0
- Scope tags Edit
- Default
- Assignments Edit

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

No assignments

+ Add group ⓘ + Add all users ⓘ

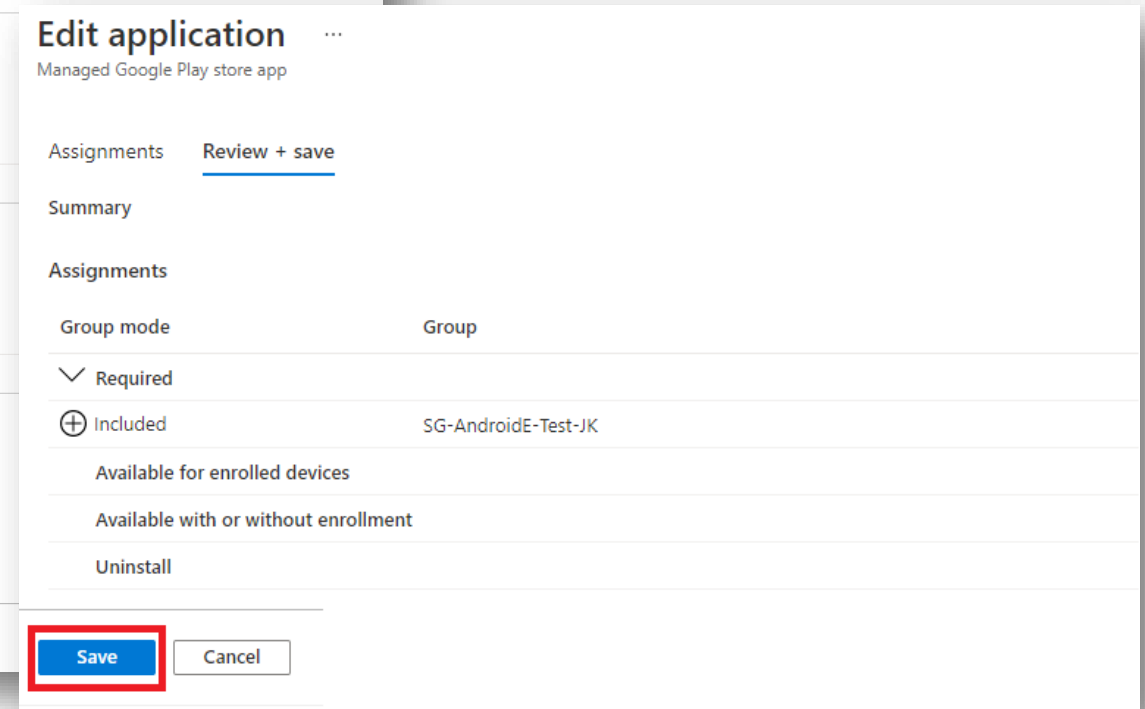
Uninstall ⓘ

Group mode

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

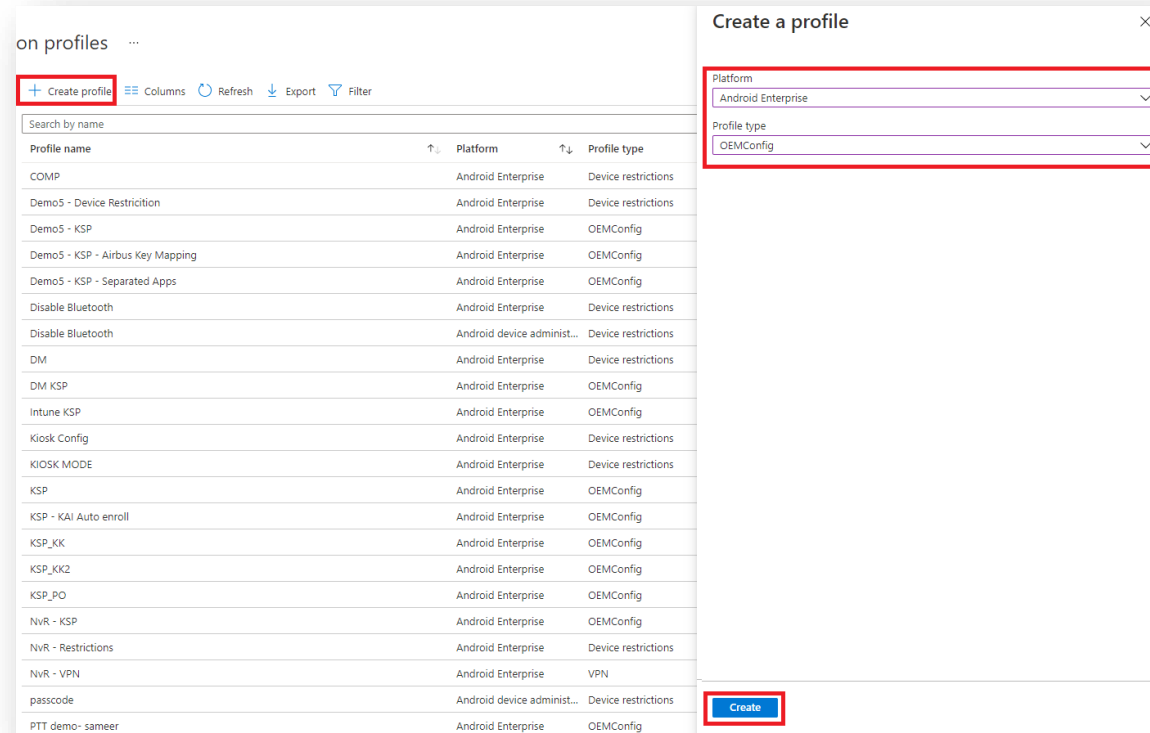
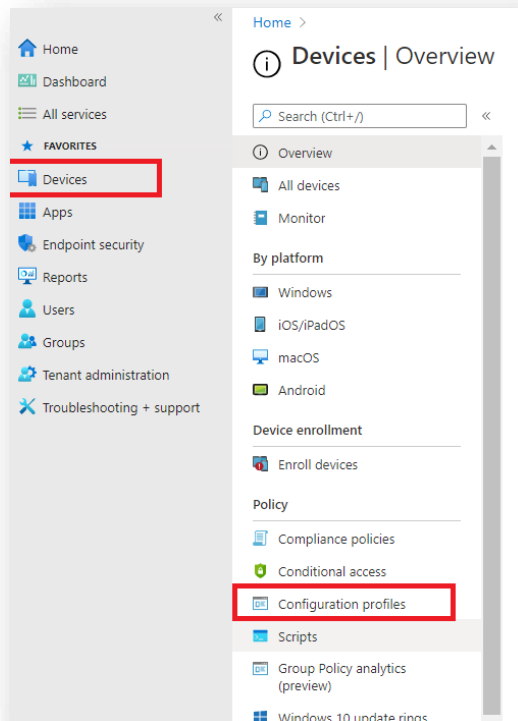
Available with or without enrollment

Uninstall

Save Cancel

Create 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 * ⓘ

KSP ✓

Description ⓘ

OEMConfig app *

Select an OEMConfig app

Previous

Next

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

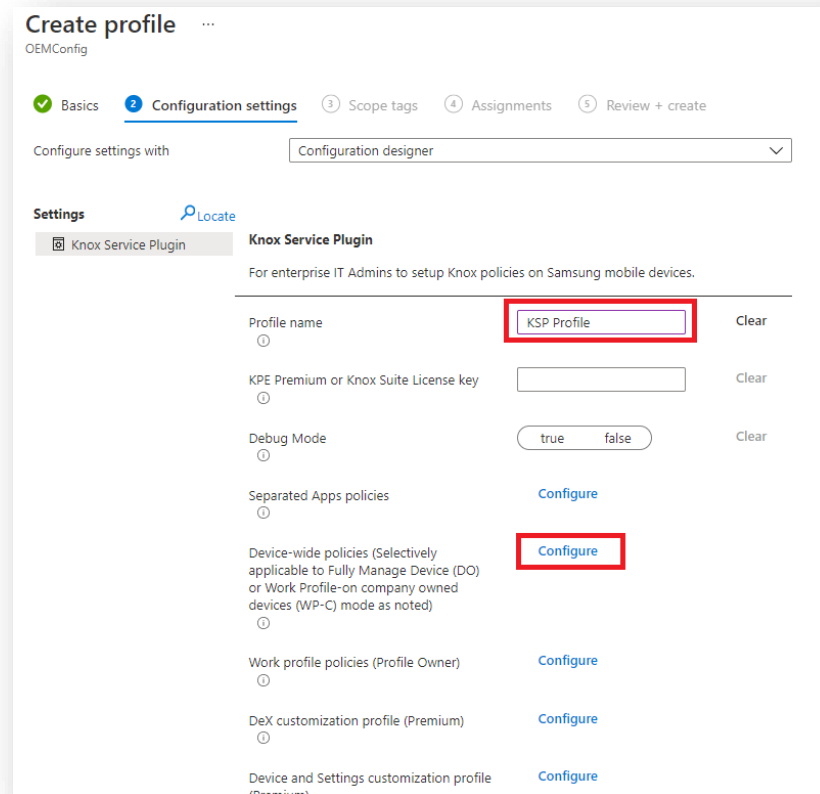
Samsung Electronics...

Remove

Select

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 profile ...

OEMConfig

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

Configure settings with Configuration designer

Settings [Locate](#)

Knox Service Plugin

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

Profile name Clear

KPE Premium or Knox Suite License key Clear

Debug Mode ☐ true ☐ false Clear

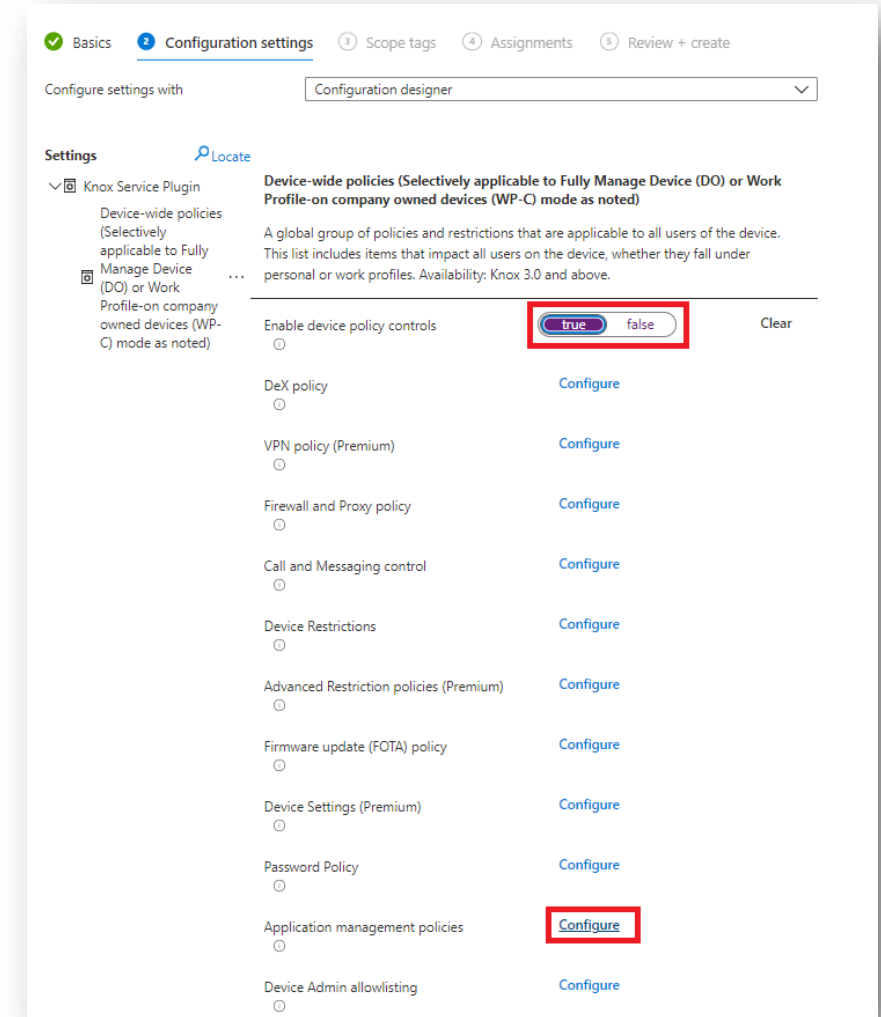
Separated Apps policies [Configure](#)

Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) [Configure](#)

Work profile policies (Profile Owner) [Configure](#)

DeX customization profile (Premium) [Configure](#)

Device and Settings customization profile (Premium) [Configure](#)



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

Configure settings with Configuration designer

Settings [Locate](#)

Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted)

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 work profiles. Availability: Knox 3.0 and above.

Enable device policy controls ☒ true ☐ false Clear

DeX policy [Configure](#)

VPN policy (Premium) [Configure](#)

Firewall and Proxy policy [Configure](#)

Call and Messaging control [Configure](#)

Device Restrictions [Configure](#)

Advanced Restriction policies (Premium) [Configure](#)

Firmware update (FOTA) policy [Configure](#)

Device Settings (Premium) [Configure](#)

Password Policy [Configure](#)

Application management policies [Configure](#)

Device Admin allowlisting [Configure](#)

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

Create profile

OEMConfig

Settings

Knox Service Plugin

Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted)

Application management policies

Application management policies

Enable application management controls

true

false

Clear

Battery optimization allowlist

Clear

Notifications allowlist

Clear

App update controls

Configure

Allow USB Devices for default access by Application (Configure profiles below)

true

false

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....

Clear

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 to create an Android Enterprise OEMConfig profile.

First Screenshot (Left): Shows the 'Create profile' wizard with the 'Basics' step selected. The 'Scope tags' section is visible, showing 'Default' and a '+ Select scope tags' link. The 'Next' button is highlighted with a red box.

Second Screenshot (Middle): Shows the 'Create profile' wizard with the 'Assignments' step selected. The 'Included groups' section is visible, showing 'SG-AndroidE-Test-JK' and a 'Remove' link. The 'Add groups' button is highlighted with a red box. The 'Next' button is also highlighted with a red box.

Third Screenshot (Right): Shows the 'Create profile' wizard with the 'Review + create' step selected. The 'Summary' section is visible, showing the profile name 'KSP', description '--', and OEMConfig app 'Knox Service Plugin'. The 'Create' button is highlighted with a red box.

Check the devices have enrolled

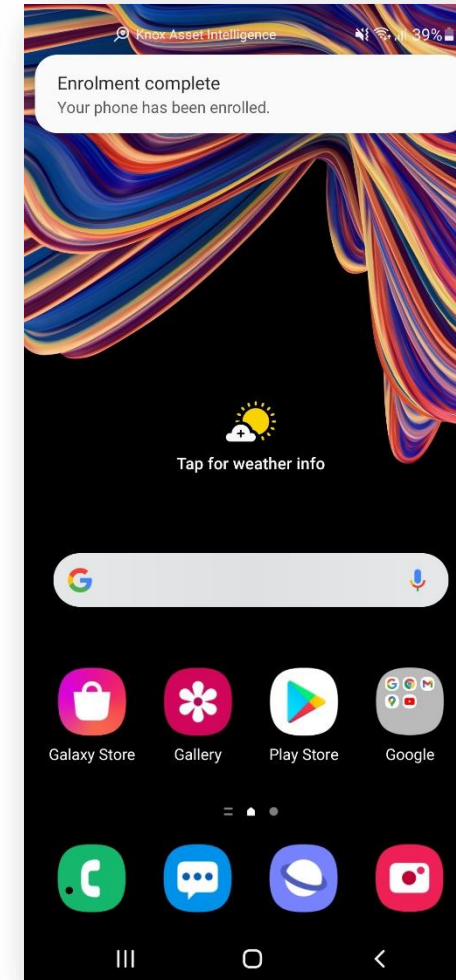
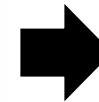
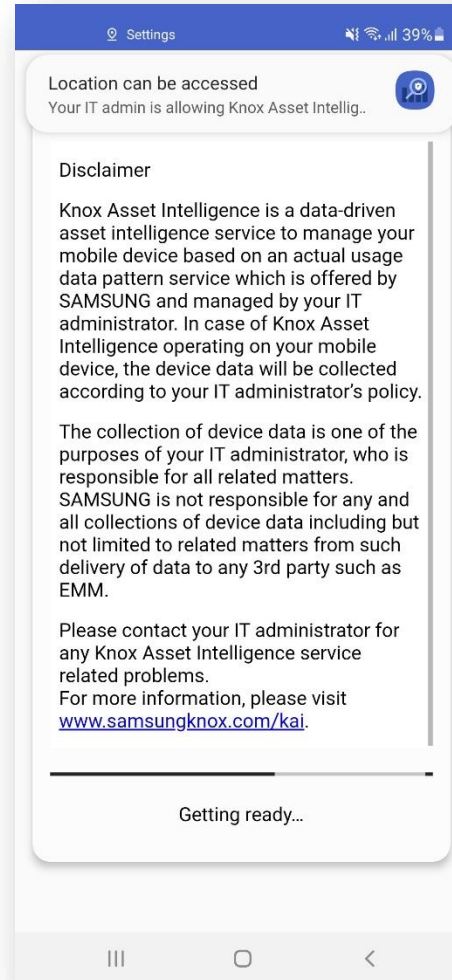
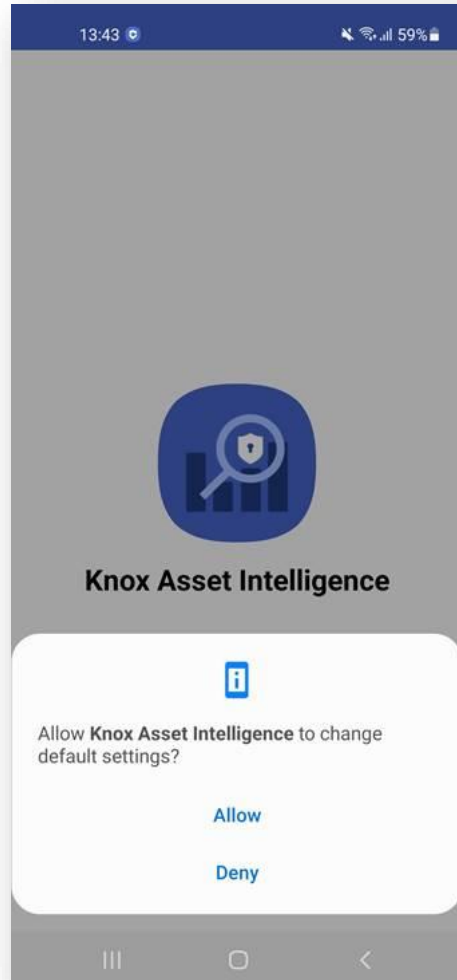
- Open Knox Asset Intelligence
- Select the Devices tab
- Check the Status of the devices are now marked as Enrolled

The screenshot displays the Samsung Knox Admin Portal interface. On the left, a dark sidebar contains the 'SAMSUNG Knox Admin Portal' header and a list of navigation items: 'Knox Asset Intelligence' (highlighted with a green square), 'Dashboard', 'Devices' (highlighted with a red rectangle), 'Licenses', 'Resellers', 'Administrators & Roles', 'Activity Log', 'Device Debug Log', 'Knox Mobile Enrollment' (with a red square), 'Knox Configure' (with a pink square), and 'Knox Manage' (with a yellow square). The main content area is titled 'Devices' and includes a sub-header 'To enroll your devices, install Knox Asset Intelligence app from Google Play Store, Knox Service Plugin, EMM policy or [download here](#). ⓘ'. Below this are tabs for 'DEVICES (1)', 'UPLOADS (1)', and 'BULK ACTIONS'. A search bar is present. A table lists the enrolled device with columns: 'DEVICE ID', 'MODEL', 'STATUS', 'OS VERSION', and 'FIRMWARE VERSION'. The first row shows a device with ID '352032112586570', model 'SM-G715FN/DS', status 'Enrolled' (highlighted with a red rectangle), OS version 'Android 11', and firmware version 'G715FNXXU8BUB8'.

DEVICE ID	MODEL	STATUS	OS VERSION	FIRMWARE VERSION
352032112586570	SM-G715FN/DS	Enrolled	Android 11	G715FNXXU8BUB8

KAI enrollment

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



This is version 1.0 of this document.

Thank you!

