Knox

Microsoft Intune MDM & KPE/KSP

AUG 2019
Samsung R&D Centre UK
(SRUK)

Agenda

1. How to gain access to Microsoft Intune EMM
2. Pre-requisites for Knox Platform for Enterprise
3. Configure Android Enterprise
4. Android Enterprise Deployment Modes
   - Personal devices with work profile (BYOD)
   - Corporate-owned dedicated Device
   - Fully Managed Device with a Work Profile (COMP Not Currently supported in Intune)
   - Corporate-owned fully managed user devices (Preview)
5. Managed Google Play [MGP] Configuration
6. Configure Knox Service Plugin [KSP]

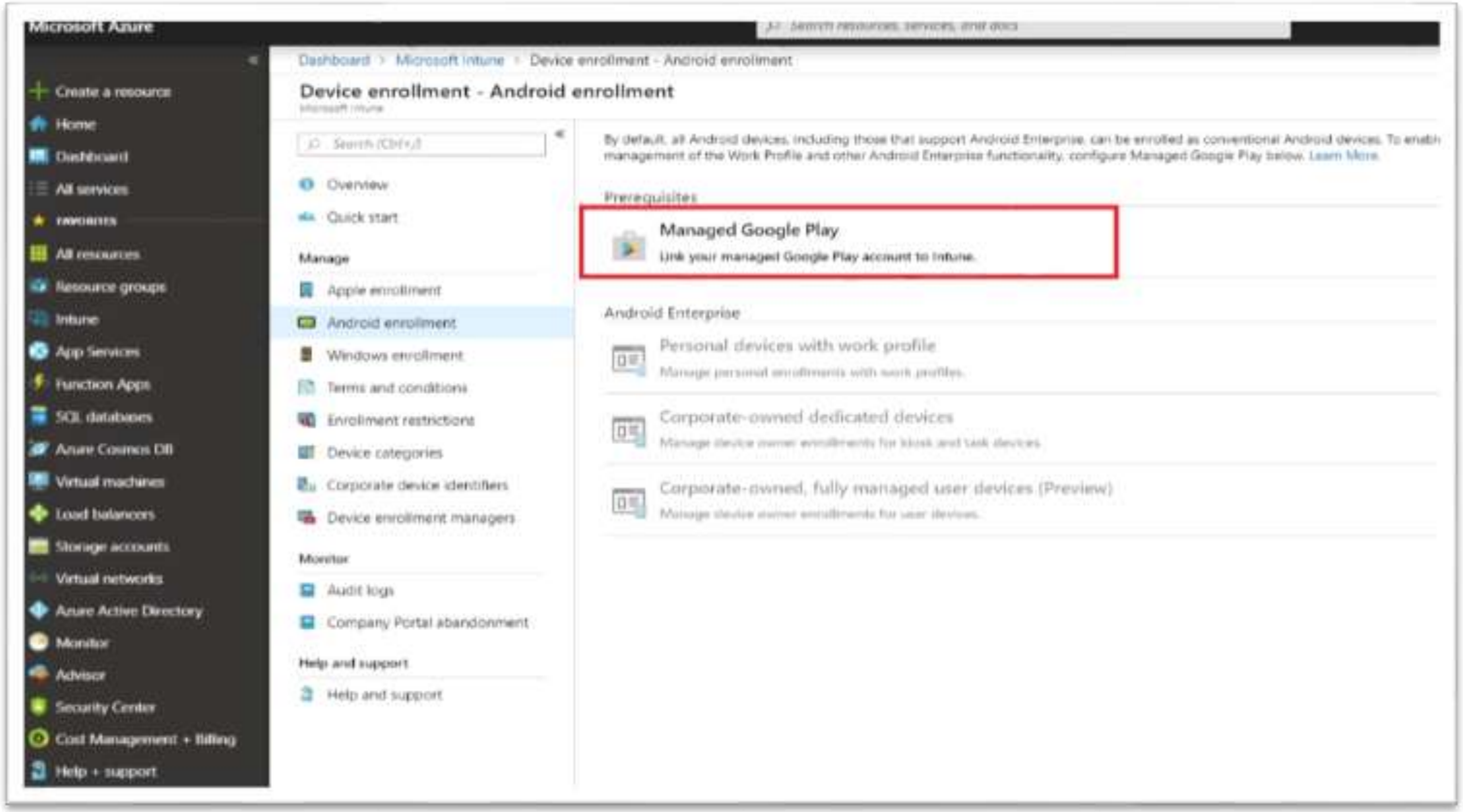
Pre-Requisites for Knox Platform for Enterprise

1. Obtain access to Microsoft Intune console
2. A Gmail account to map to Intune 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

Configure Android Enterprise

- Navigate to **Microsoft Intune > Device enrollment > Android enrollment**. Click **Managed Google Play – Link your managed Google Play account to Intune**



Device enrollment - Android enrollment

Microsoft Intune

By default, all Android devices, including those that support Android Enterprise, can be enrolled as conventional Android devices. To enabl management of the Work Profile and other Android Enterprise functionality, configure Managed Google Play below. Learn More

Prerequisites

Managed Google Play

Link your managed Google Play account to Intune.

Android Enterprise

Personal devices with work profile

Manage personal enrollments with work profiles.

Corporate-owned dedicated devices

Manage device owner enrollments for kiosk and task devices.

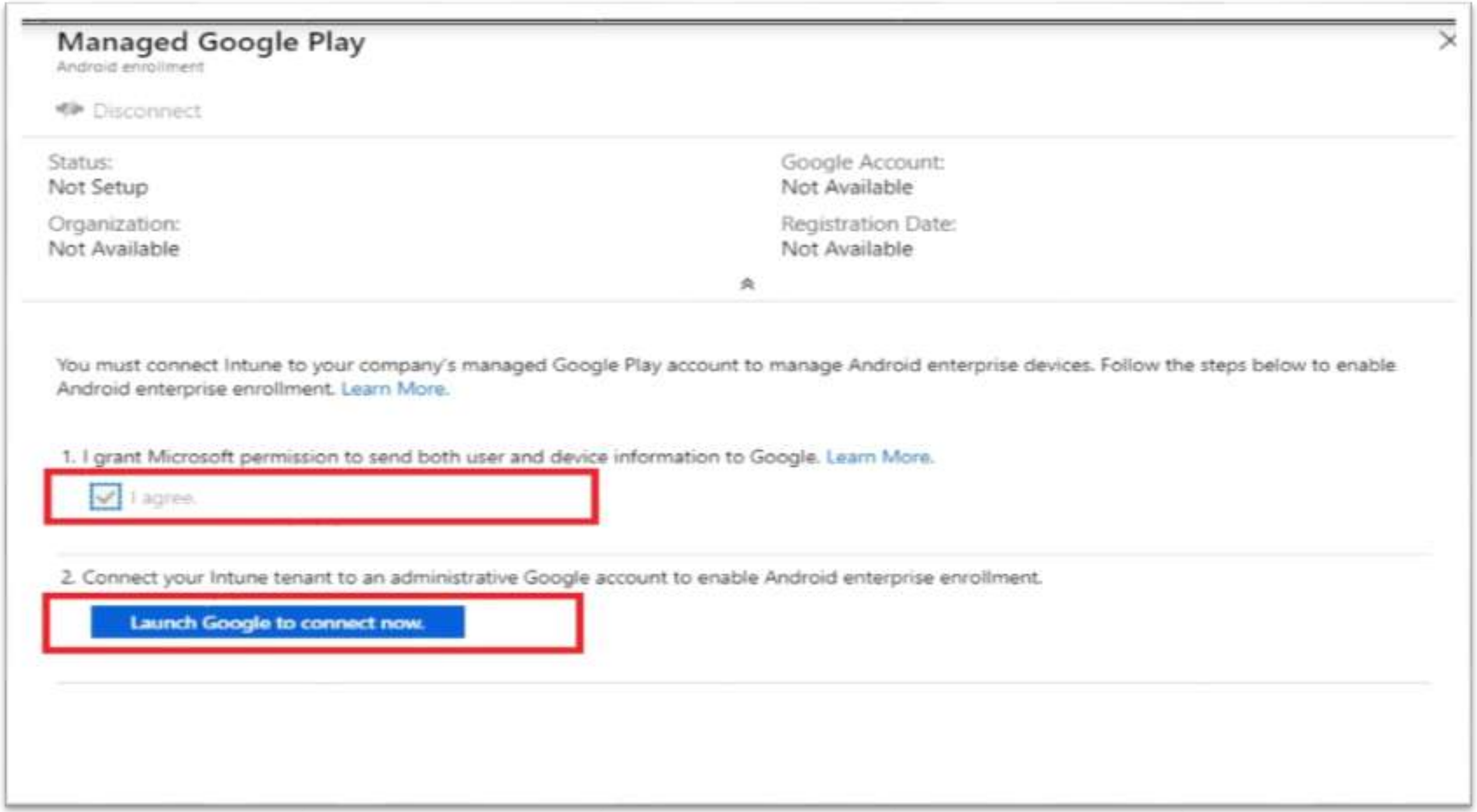
Corporate-owned, fully managed user devices (Preview)

Manage device owner enrollments for user devices.

Configure Android Enterprise

Configure Android Enterprise

- Checkmark I agree and click “Launch Google to connect now”.



Managed Google Play

Android enrollment

Disconnect

Status:
Not Setup

Google Account:
Not Available

Organization:
Not Available

Registration Date:
Not Available

You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. Learn More.

1. I grant Microsoft permission to send both user and device information to Google. Learn More.

☑ I agree.

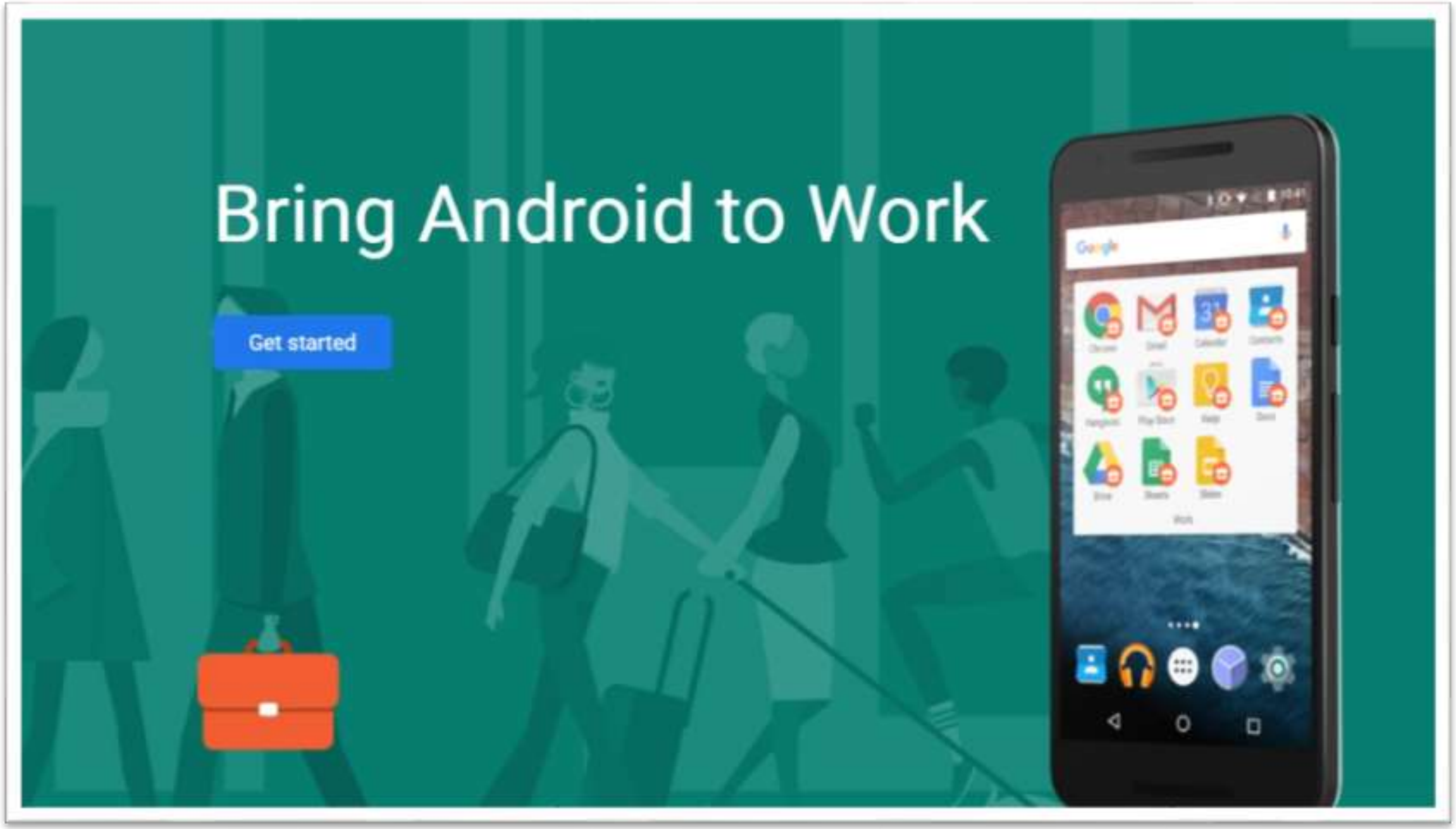
2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

Launch Google to connect now.

Configure Android Enterprise

Configure Android Enterprise

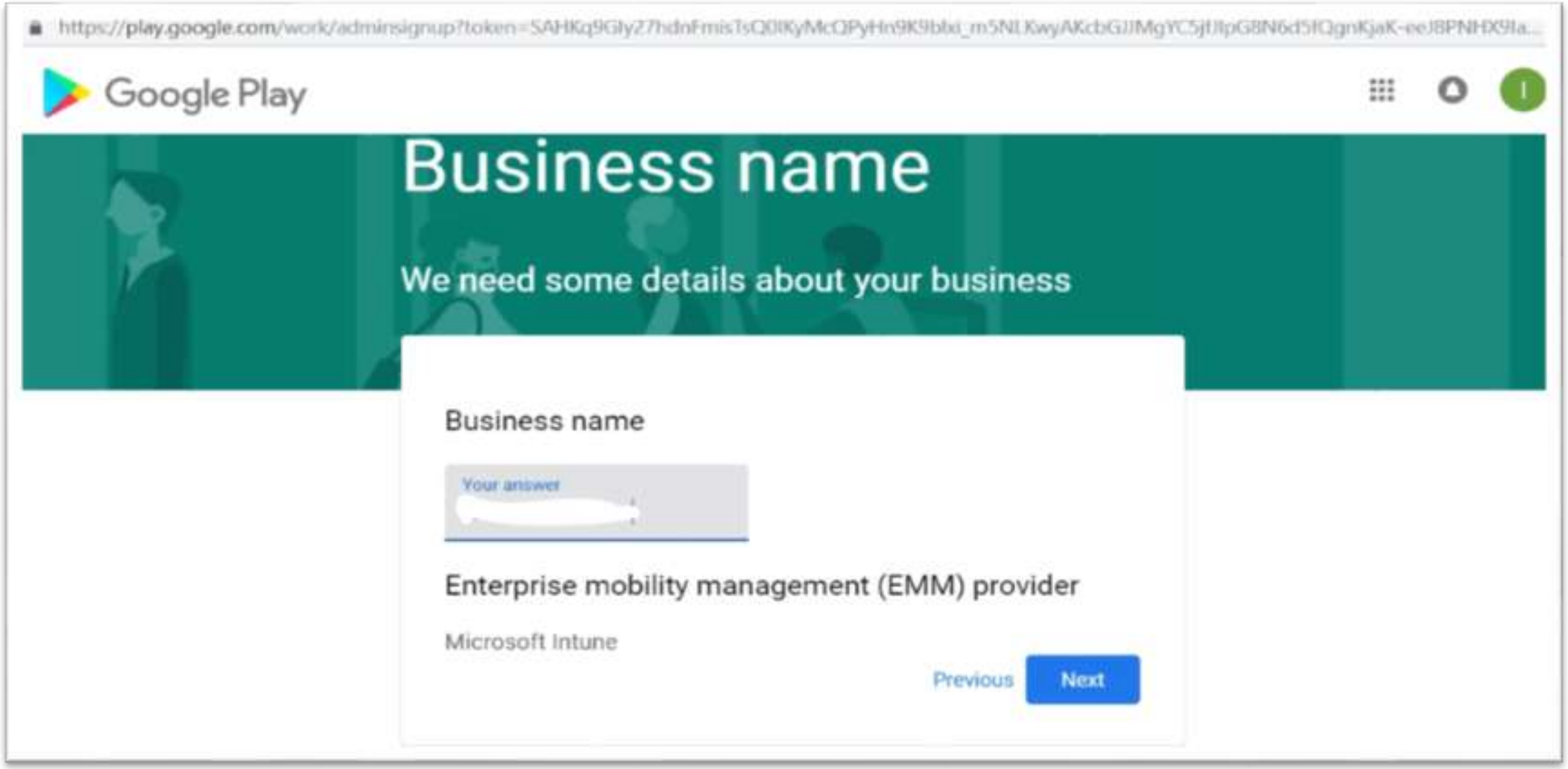
- Click Get started



Configure Android Enterprise

Configure Android Enterprise

- Fill in your Company/Business name and click **Next**



https://play.google.com/work/adminsignup?token=SAHKq9Gly27hdnFmisTsQ0IKyMcQPyHn9K9bbd_m5NLKwyAKcbGJMgYC5jtJlpG8N6d5fQgnKjaK-eeJ8PNHX9la...

Business name

We need some details about your business

Business name

Your answer

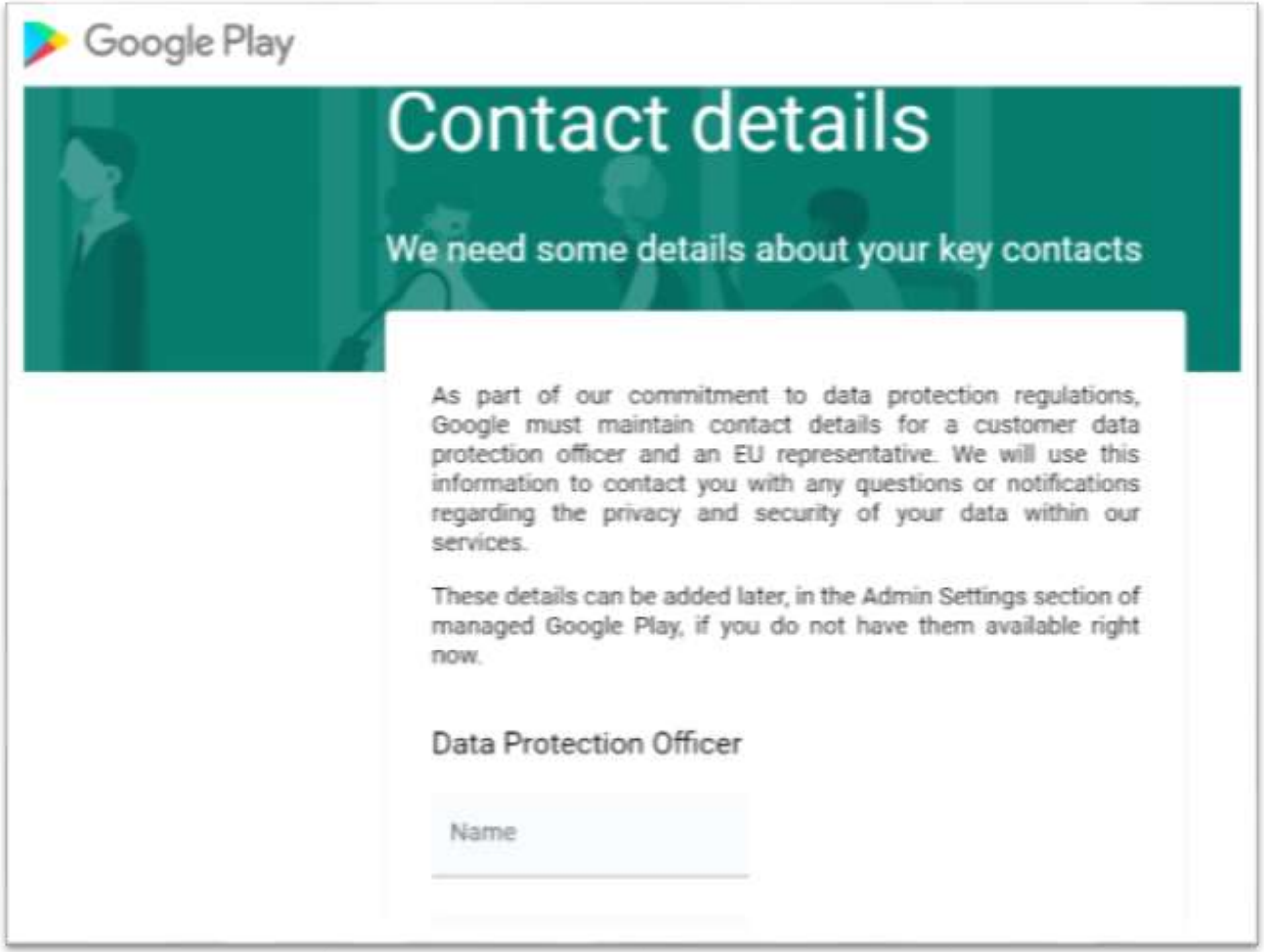
Enterprise mobility management (EMM) provider

Microsoft Intune

Configure Android Enterprise

Configure Android Enterprise

- This form is optional, you can skip it or fill it in. Scroll down this page.



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.

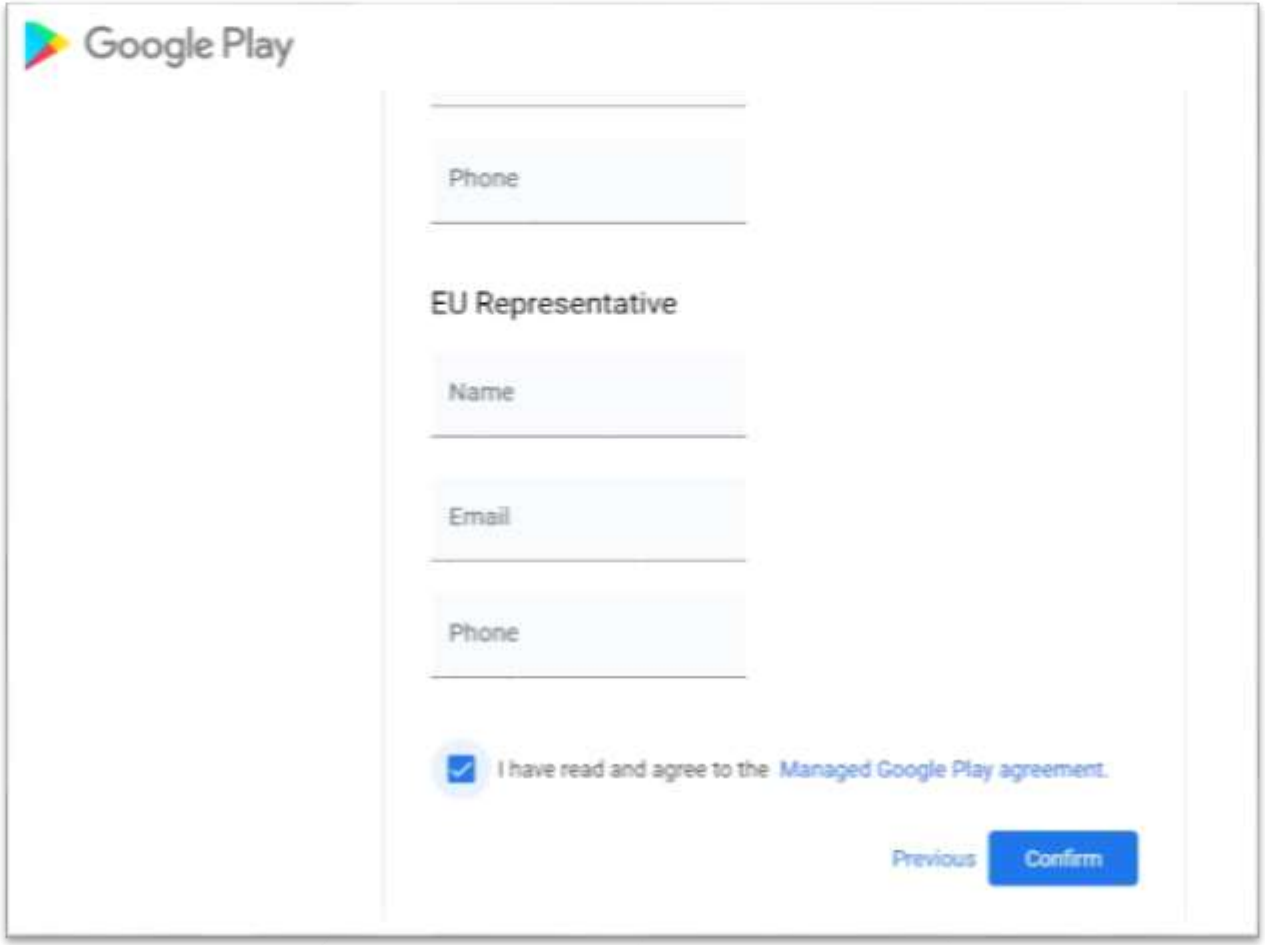
Data Protection Officer

Name

Configure Android Enterprise

Configure Android Enterprise

- Select **I have read and agree to the Managed Google Play agreement** (if you do) and click **Confirm**



Google Play

Phone

EU Representative

Name

Email

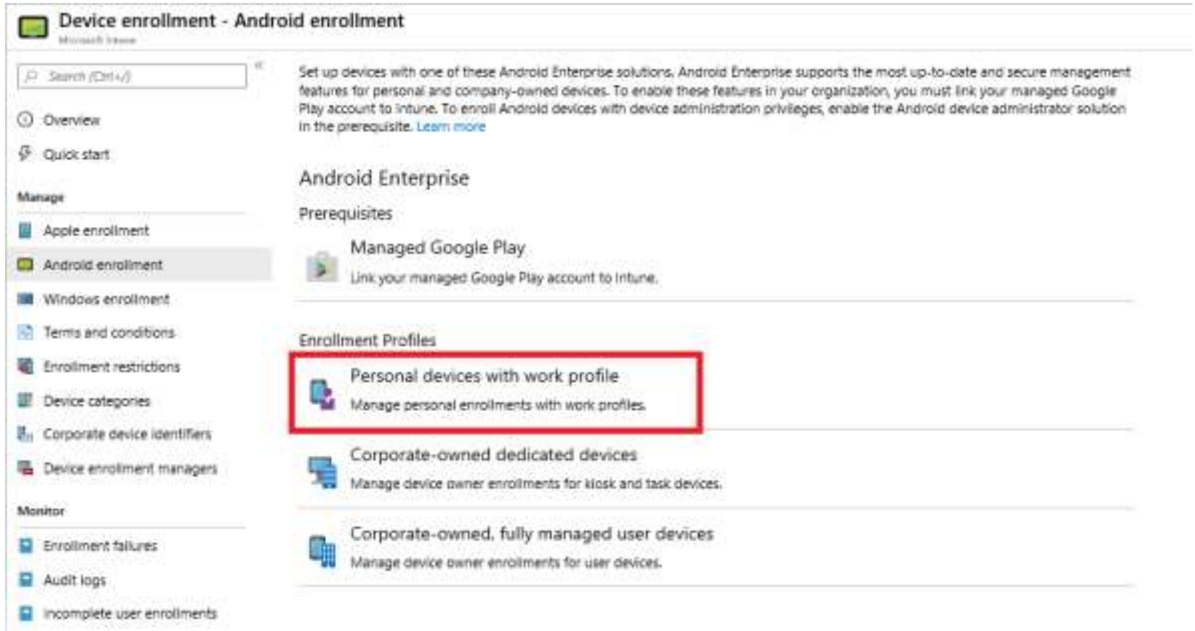
Phone

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

Android Enterprise: Personal devices with work profile

-First create the enrollment profile. Do this by going to **Microsoft Intune > Device enrollment > Android enrollment** and click **Personal devices with work profile.**

-You will see no further action is needed because this is enabled by default. You can however configure enrollment restrictions.



Set up devices with one of these Android Enterprise solutions. Android Enterprise supports the most up-to-date and secure management features for personal and company-owned devices. To enable these features in your organization, you must link your managed Google Play account to Intune. To enroll Android devices with device administration privileges, enable the Android device administrator solution in the prerequisite. Learn more

Android Enterprise

Prerequisites

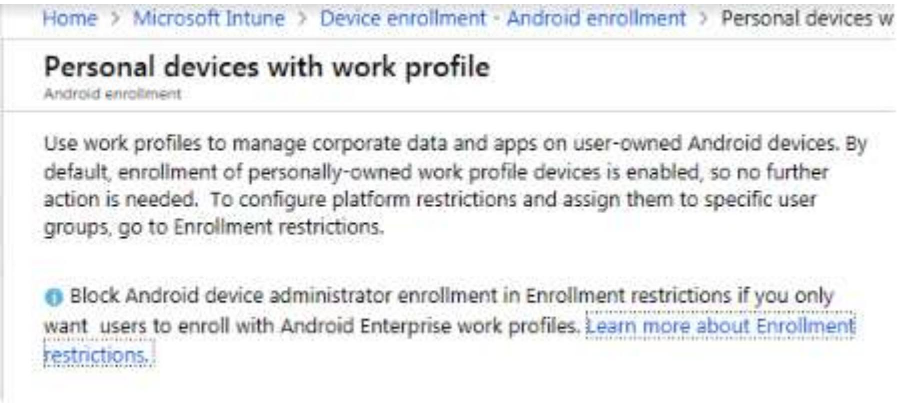
Managed Google Play
Link your managed Google Play account to Intune.

Enrollment Profiles

Personal devices with work profile
Manage personal enrollments with work profiles.

Corporate-owned dedicated devices
Manage device owner enrollments for kiosk and task devices.

Corporate-owned, fully managed user devices
Manage device owner enrollments for user devices.


Home > Microsoft Intune > Device enrollment - Android enrollment > Personal devices w

Personal devices with work profile
Android enrollment

Use work profiles to manage corporate data and apps on user-owned Android devices. By default, enrollment of personally-owned work profile devices is enabled, so no further action is needed. To configure platform restrictions and assign them to specific user groups, go to Enrollment restrictions.

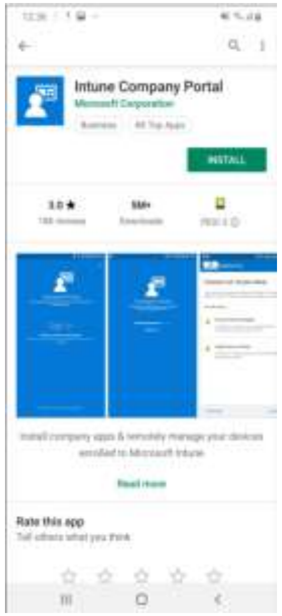
Block Android device administrator enrollment in Enrollment restrictions if you only want users to enroll with Android Enterprise work profiles. Learn more about Enrollment restrictions.

Apply Policies

Android Enterprise: Personal devices with work profile

-Next you will need to download the “Intune Company Portal” from the Google Play store and authenticate with a user that has a valid Intune license.

- Follow the screenshots below until device is successfully enrolled.



Intune Company Portal

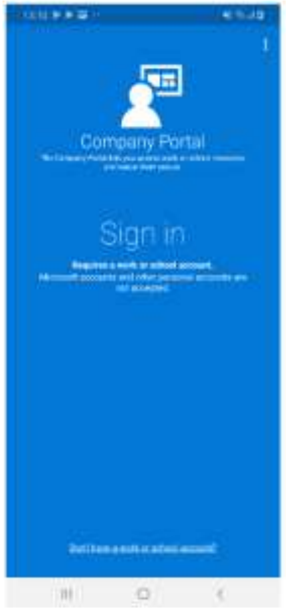
Microsoft Corporation

INSTALL

Read more

Rate this app

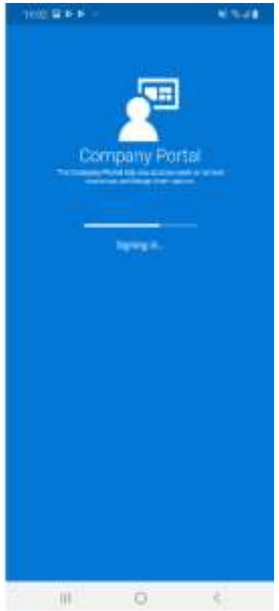
Install Intune Company Portal
from Google Play Store



Company Portal

Sign in

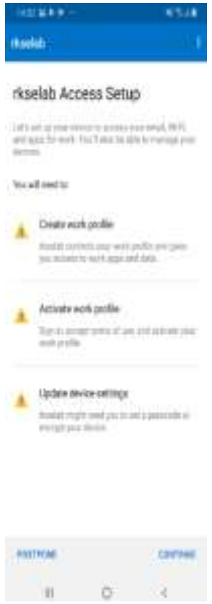
Click Sign in and authenticate with email address and password



Company Portal

Signing in...

Signing in



rkselab

rkselab Access Setup

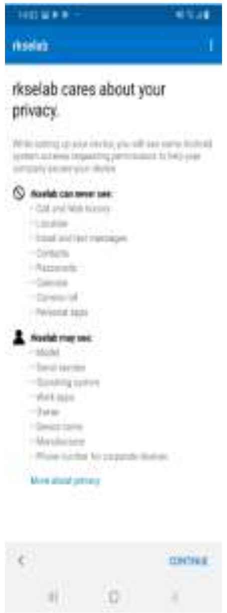
Create work profile

Activate work profile

Update device settings

POSTPONE CONTINUE

Accept Access Rights



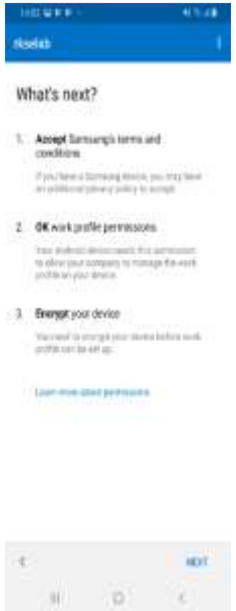
rkselab

rkselab cares about your privacy.

More about privacy

CONTINUE

Accept Privacy permissions



rkselab

What's next?

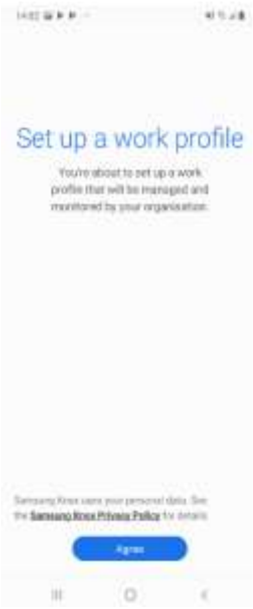
1. Accept Samsung's terms and conditions

2. OK work profile permissions

3. Encrypt your device

NEXT

Click Next

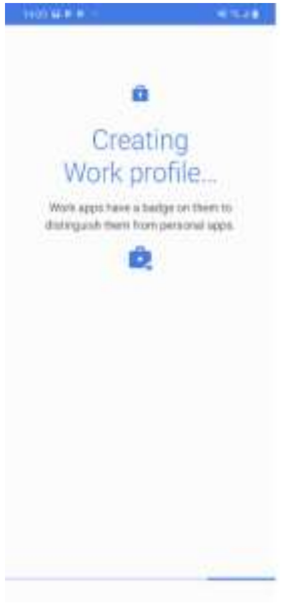


Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Agree

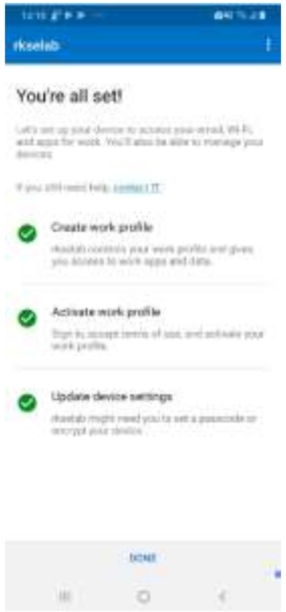
Agree



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Creating Work Profile



rkselab

You're all set!

Create work profile

Activate work profile

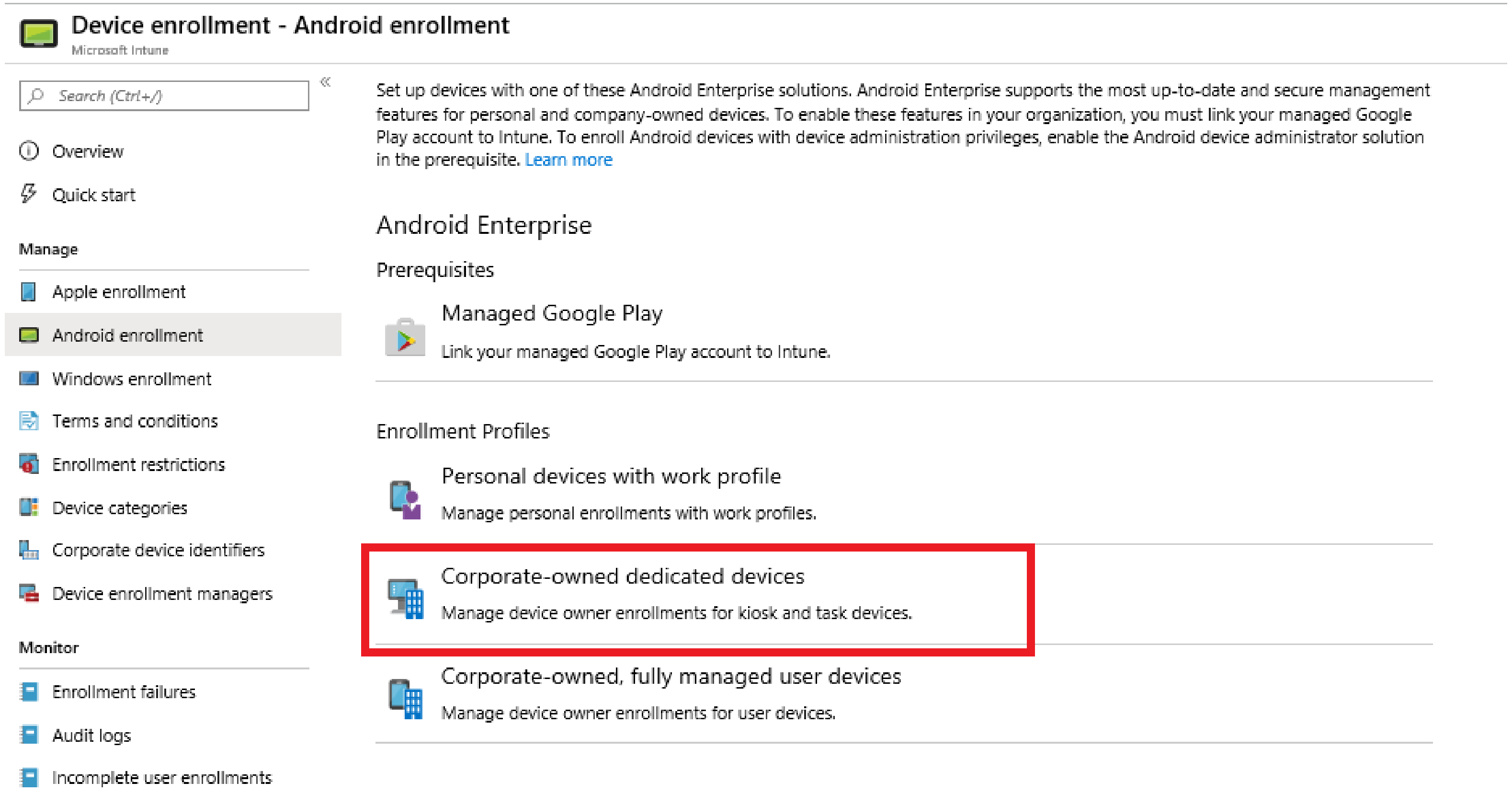
Update device settings

DONE

Device Enrollment Successful!

Android Enterprise: Corporate Owned Dedicated Device

-First create the enrollment profile. Do this by going to **Microsoft Intune** > **Device enrollment** > **Android enrollment** and click **Corporate-owned dedicated devices**



Device enrollment - Android enrollment
Microsoft Intune

Set up devices with one of these Android Enterprise solutions. Android Enterprise supports the most up-to-date and secure management features for personal and company-owned devices. To enable these features in your organization, you must link your managed Google Play account to Intune. To enroll Android devices with device administration privileges, enable the Android device administrator solution in the prerequisite. Learn more

Android Enterprise

Prerequisites

Managed Google Play
Link your managed Google Play account to Intune.

Enrollment Profiles

Personal devices with work profile
Manage personal enrollments with work profiles.

Corporate-owned dedicated devices
Manage device owner enrollments for kiosk and task devices.

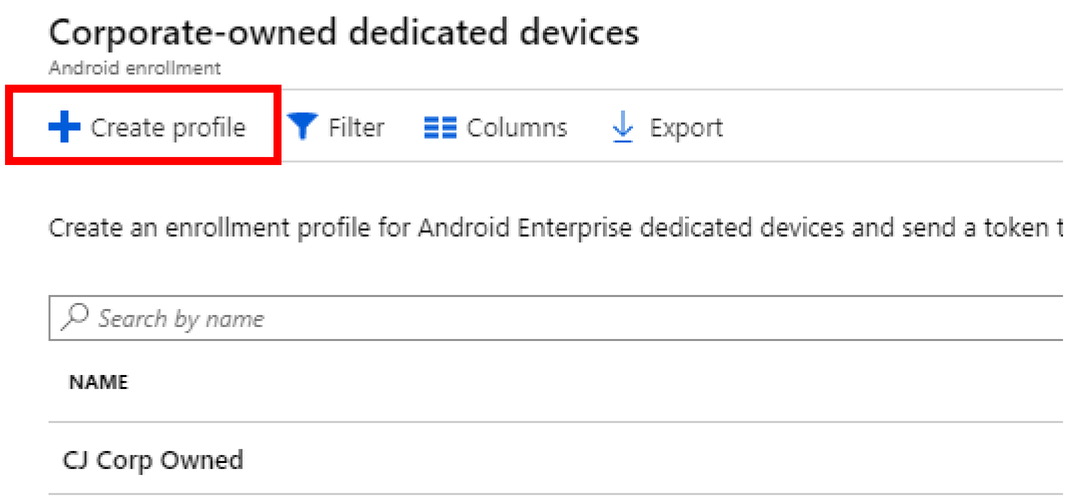
Corporate-owned, fully managed user devices
Manage device owner enrollments for user devices.

Android Enterprise: Corporate Owned Dedicated Device

Create Enrolment Profile

-Click Create Profile and then give it a name, description and a token expiry date (max 90 days)

-Click Create in the create profile window.



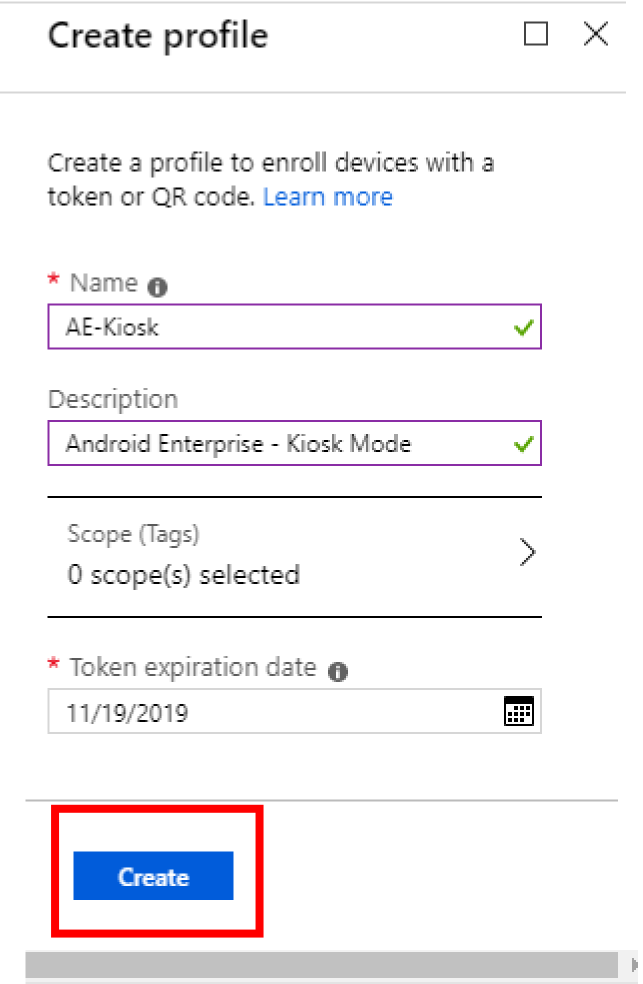
Corporate-owned dedicated devices

Android enrollment

Create an enrollment profile for Android Enterprise dedicated devices and send a token t

Search by name

NAME
CJ Corp Owned



Create profile

Create a profile to enroll devices with a token or QR code. Learn more

* Name: AE-Kiosk

Description: Android Enterprise - Kiosk Mode

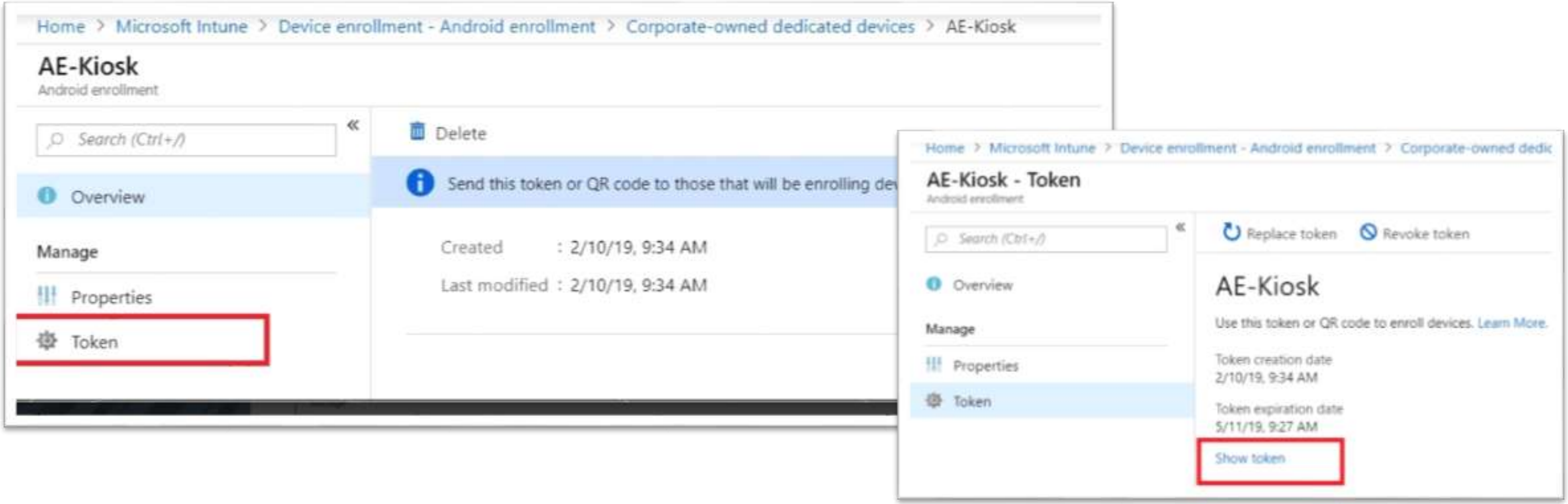
Scope (Tags): 0 scope(s) selected

* Token expiration date: 11/19/2019

Android Enterprise: Corporate Owned Dedicated Device

Create Enrolment Profile

- Click profile you just created
- Click Token then click show Token



Home > Microsoft Intune > Device enrollment - Android enrollment > Corporate-owned dedicated devices > AE-Kiosk

AE-Kiosk
Android enrollment

Send this token or QR code to those that will be enrolling de

Created : 2/10/19, 9:34 AM
Last modified : 2/10/19, 9:34 AM

Home > Microsoft Intune > Device enrollment - Android enrollment > Corporate-owned dedic

AE-Kiosk - Token
Android enrollment

AE-Kiosk

Use this token or QR code to enroll devices. Learn More.

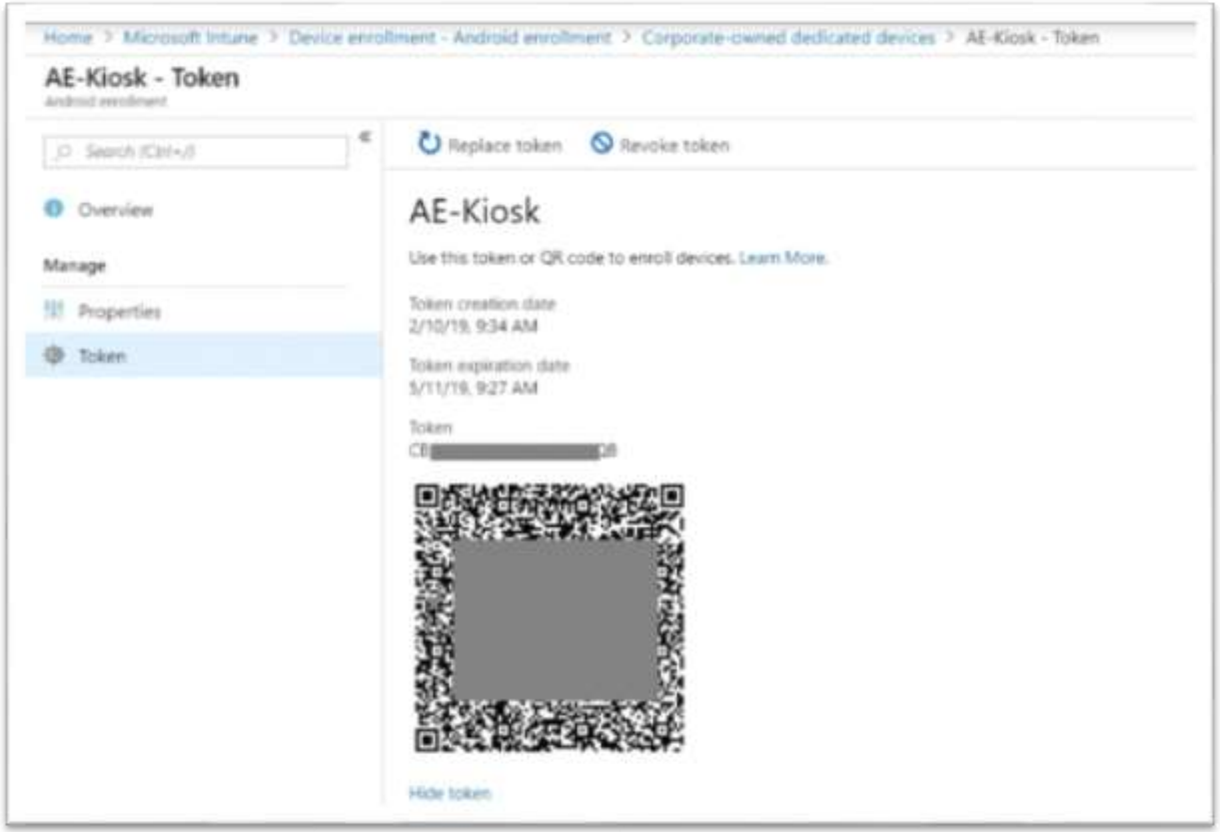
Token creation date
2/10/19, 9:34 AM

Token expiration date
5/11/19, 9:27 AM

Android Enterprise: Corporate Owned Dedicated Device

Create Enrolment Profile

- This token is required when enrolling the corporate owned dedicated devices.



Home > Microsoft Intune > Device enrollment - Android enrollment > Corporate-owned dedicated devices > AE-Kiosk - Token
Search (Ctrl+/)
Overview
Manage
Properties
Token
Replace token
Revoke token
Hide token

AE-Kiosk - Token
Android enrollment

AE-Kiosk

Use this token or QR code to enroll devices. Learn More.

Token creation date
2/10/19, 9:34 AM

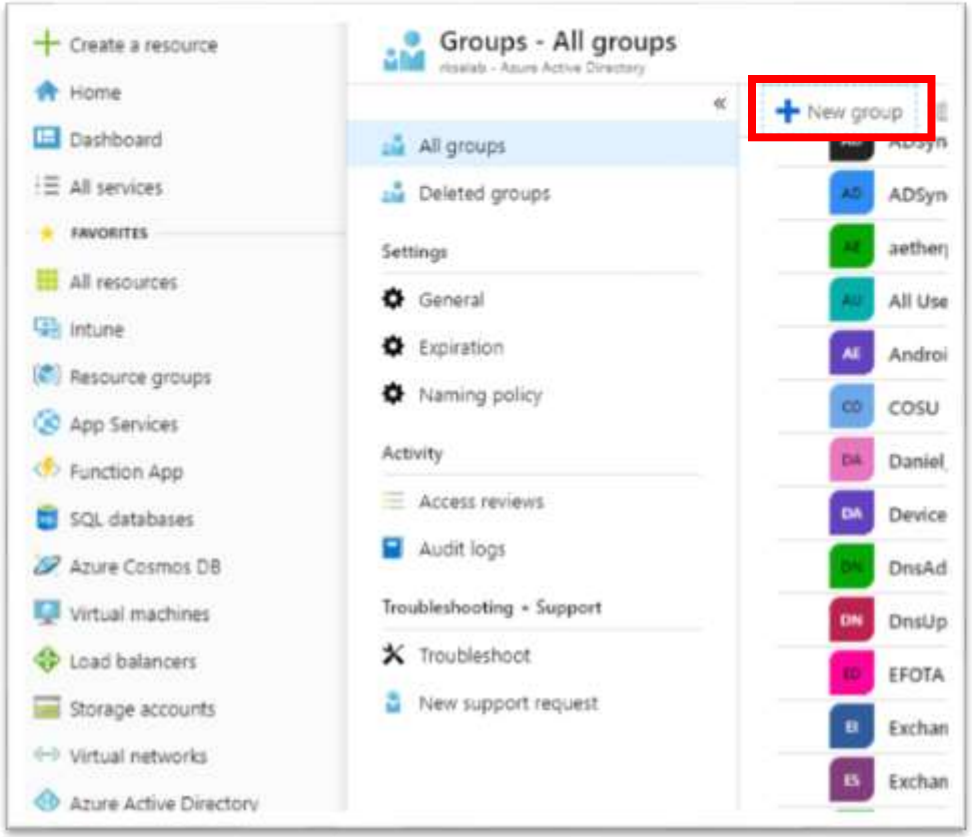
Token expiration date
5/11/19, 9:27 AM

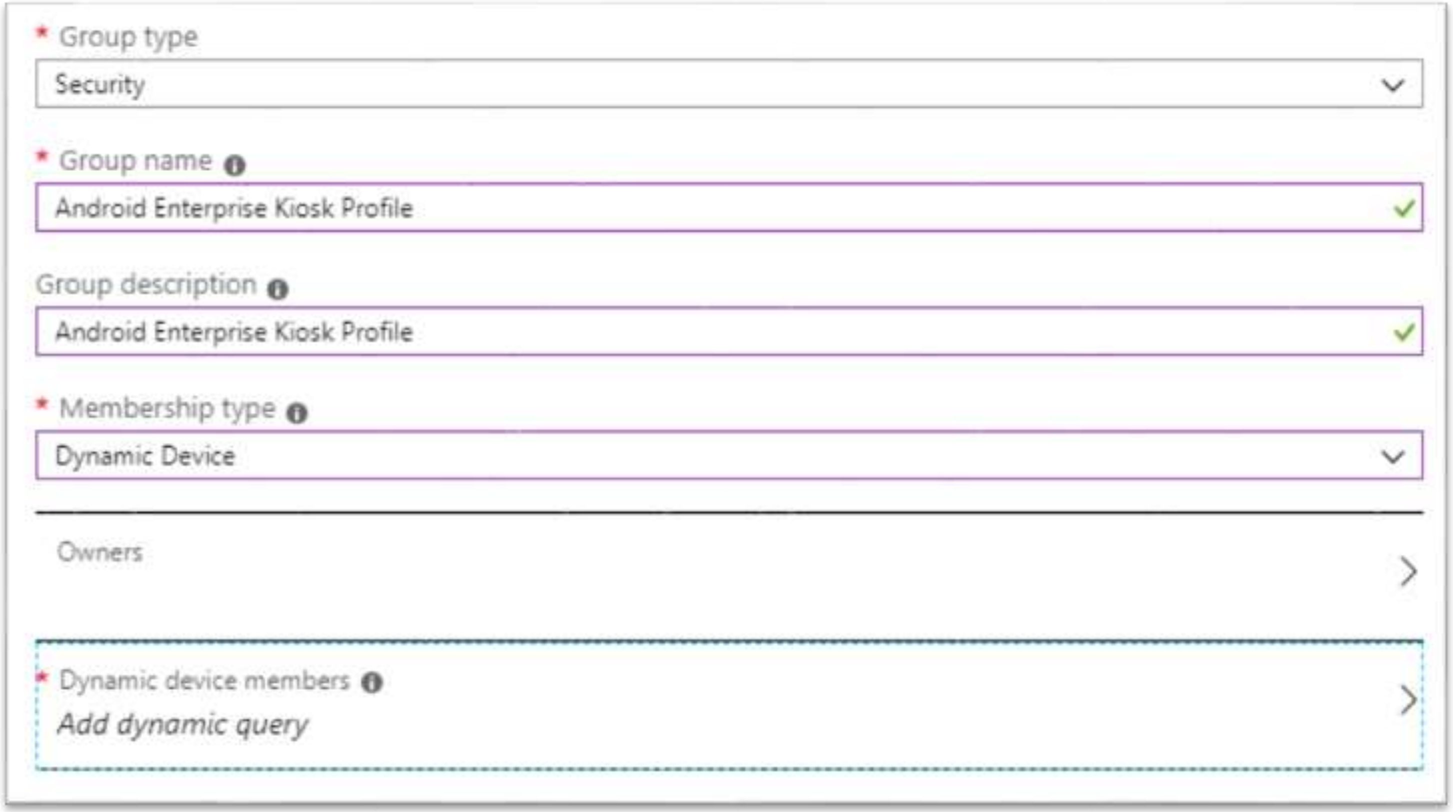
Token
[redacted]

Android Enterprise: Corporate Owned Dedicated Device

Create an Azure AD Group

Navigate to portal.azure.com, locate and select Azure Active Directory
Select Groups > New group
Group type should = Security
Provide a name for the group such as "Android Enterprise Kiosk Profile"
Membership type = Dynamic device





* Group type
Security

* Group name
Android Enterprise Kiosk Profile

Group description
Android Enterprise Kiosk Profile

* Membership type
Dynamic Device

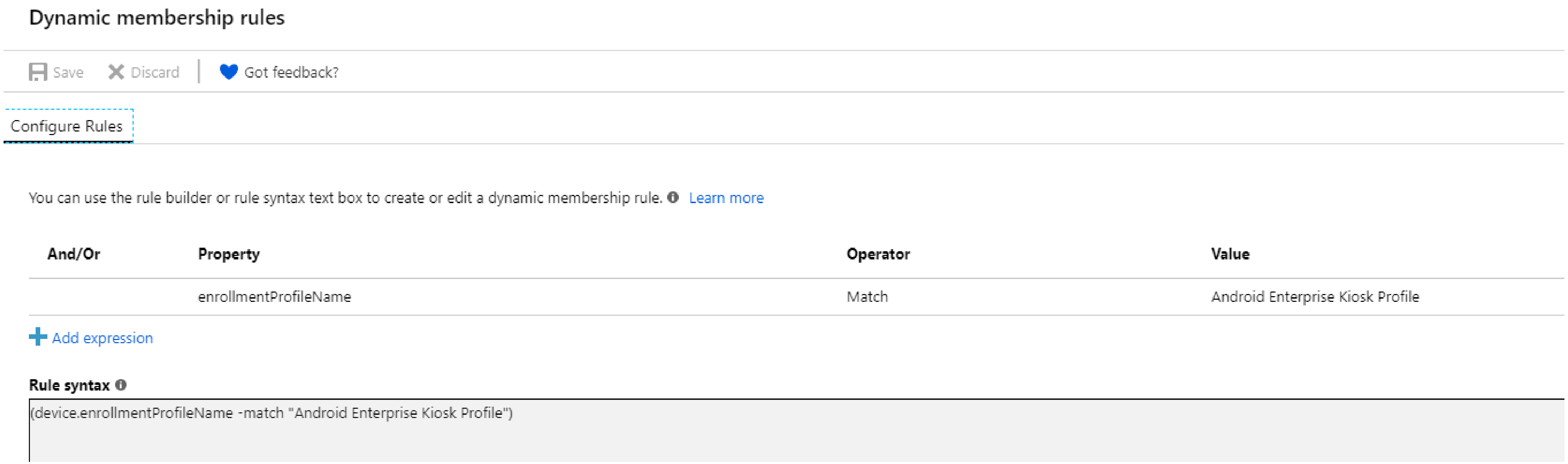
Owners

* Dynamic device members
Add dynamic query

Android Enterprise: Corporate Owned Dedicated Device

Create an Azure AD Group

- Select Dynamic device members
- Use a simple rule using the "enrollmentProfileName" attribute to create the dynamic rule as shown below:



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	enrollmentProfileName	Match	Android Enterprise Kiosk Profile

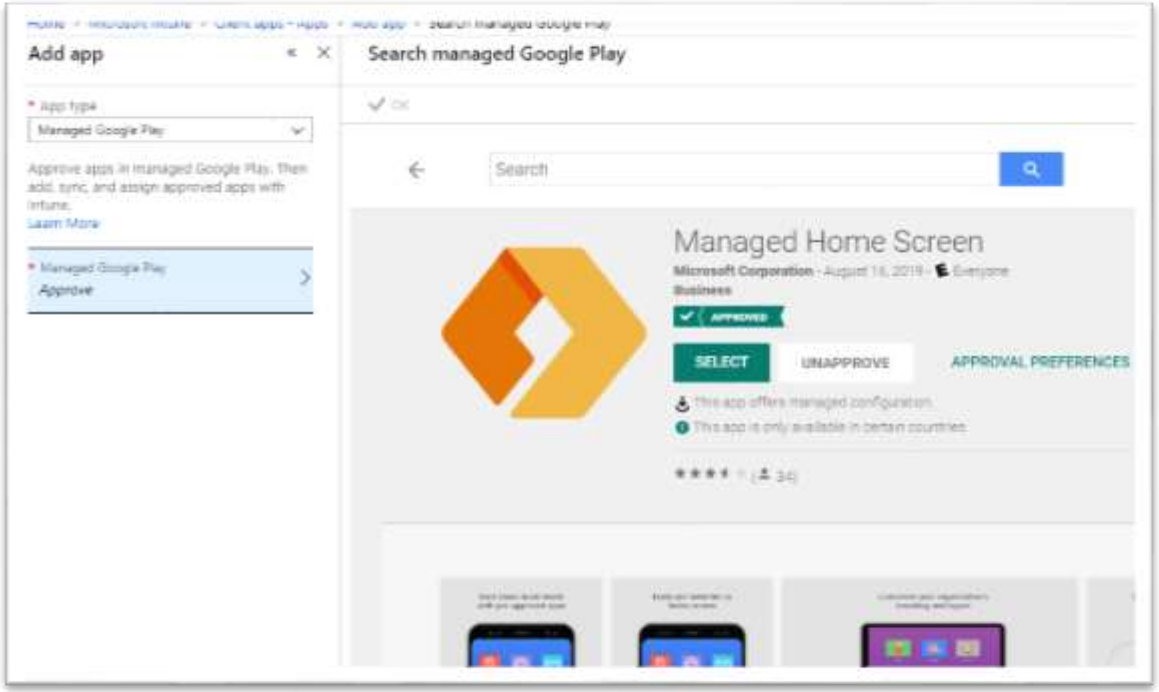
Rule syntax

```
(device.enrollmentProfileName -match "Android Enterprise Kiosk Profile")
```

Android Enterprise: Corporate Owned Dedicated Device

Add apps from Managed Google Play

Go to Microsoft Intune > Client apps – Apps > Add App
Select Managed Google Play > Approve
Search for "Managed Home Screen" and any other apps needed in Kiosk mode.
Press Sync to add these apps to the apps list.



Home > Microsoft Intune > Client apps - Apps > Add app > Search managed Google Play

Add app

* App type
Managed Google Play

Approve apps in managed Google Play. Then add, sync, and assign approved apps with Intune.
Learn More

* Managed Google Play
Approve

Search managed Google Play

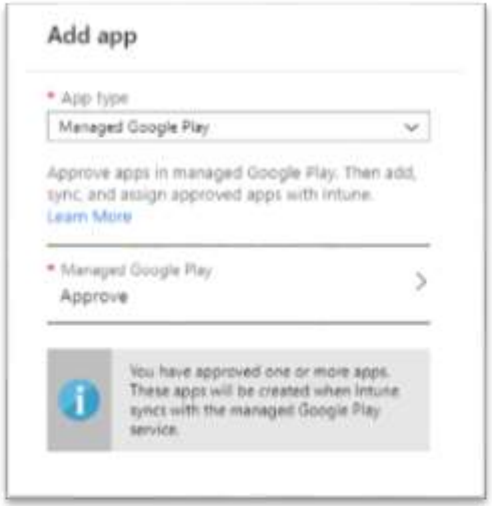
✓ OK

Search

Managed Home Screen
Microsoft Corporation · August 16, 2019 · Everyone
Business
✓ APPROVED

This app offers managed configuration.
This app is only available in certain countries.

★★★★ (34)



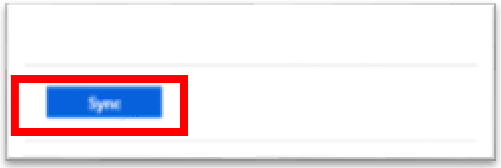
Add app

* App type
Managed Google Play

Approve apps in managed Google Play. Then add, sync, and assign approved apps with Intune.
Learn More

* Managed Google Play
Approve

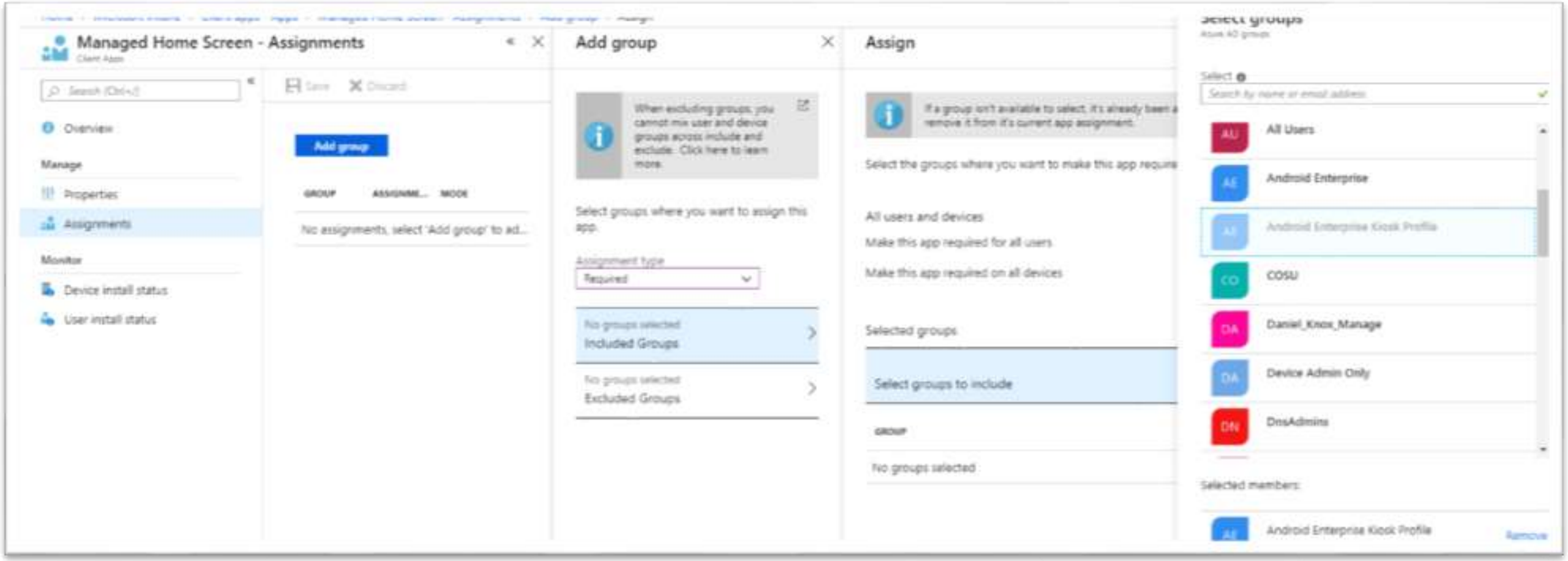
You have approved one or more apps. These apps will be created when Intune syncs with the managed Google Play service.



Android Enterprise: Corporate Owned Dedicated Device

Add apps from Managed Google Play

- Assign the apps to the “Android Enterprise Kiosk Profile” group.



No assignments, select 'Add group' to ad...

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Assignment type: Required

No groups selected
Included Groups

No groups selected
Excluded Groups

If a group isn't available to select, it's already been a... remove it from it's current app assignment.

Select the groups where you want to make this app require...

All users and devices

Make this app required for all users

Make this app required on all devices

Selected groups

Select groups to include

GROUP

No groups selected

All Users

Android Enterprise

Android Enterprise Kiosk Profile

COSU

Daniel_Knox_Manage

Device Admin Only

DnsAdmins

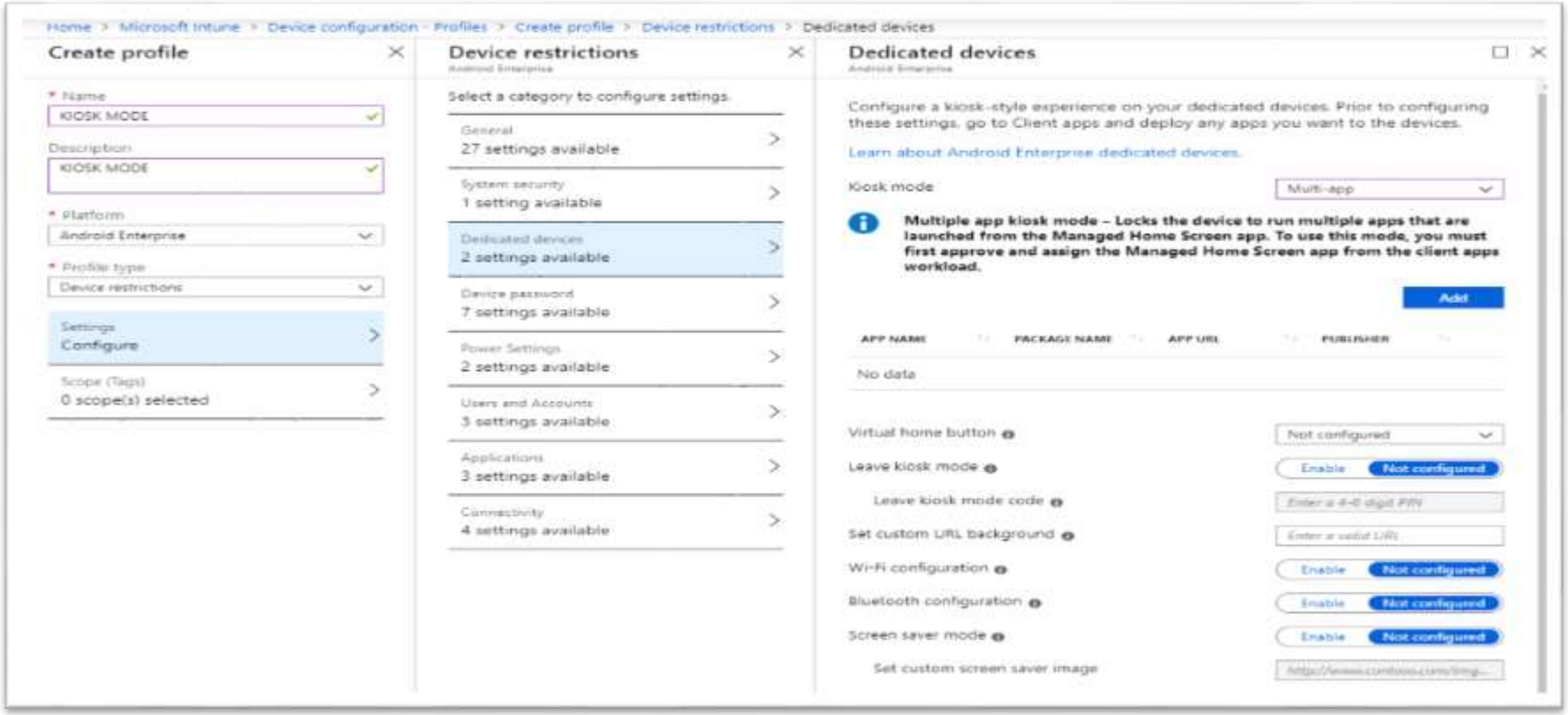
Selected members:

Android Enterprise Kiosk Profile

Android Enterprise: Corporate Owned Dedicated Device

Creating an Android enterprise kiosk configuration profile

- Within Intune select Device configuration > Profiles > Create Profile
- Select Properties > Platform = Android Enterprise, Profile type = Device restrictions
- Select Settings > Dedicated devices and choose Single or Multi app Kiosk mode.
- Select Add and add the apps previously added to Managed Google Play that were synced with Intune. Do not add the Managed Home Screen app



Home > Microsoft Intune > Device configuration - Profiles > Create profile > Device restrictions > Dedicated devices

Create profile

* Name: KIOSK MODE

Description: KIOSK MODE

* Platform: Android Enterprise

* Profile type: Device restrictions

Settings: Configure

Scope (Tags): 0 scope(s) selected

Device restrictions

Android Enterprise

Select a category to configure settings

General: 27 settings available

System security: 1 setting available

Dedicated devices: 2 settings available

Device password: 7 settings available

Power Settings: 2 settings available

Users and Accounts: 3 settings available

Applications: 3 settings available

Connectivity: 4 settings available

Dedicated devices

Android Enterprise

Configure a kiosk-style experience on your dedicated devices. Prior to configuring these settings, go to Client apps and deploy any apps you want to the devices.

Learn about Android Enterprise dedicated devices.

Kiosk mode: Multi-app

Multiple app kiosk mode – Locks the device to run multiple apps that are launched from the Managed Home Screen app. To use this mode, you must first approve and assign the Managed Home Screen app from the client apps workload.

Add

APP NAME	PACKAGE NAME	APP URL	PUBLISHER
No data			

Virtual home button: Not configured

Leave kiosk mode: Enable / Not configured

Leave kiosk mode code: Enter a 4-6 digit PIN

Set custom URL background: Enter a valid URL

Wi-Fi configuration: Enable / Not configured

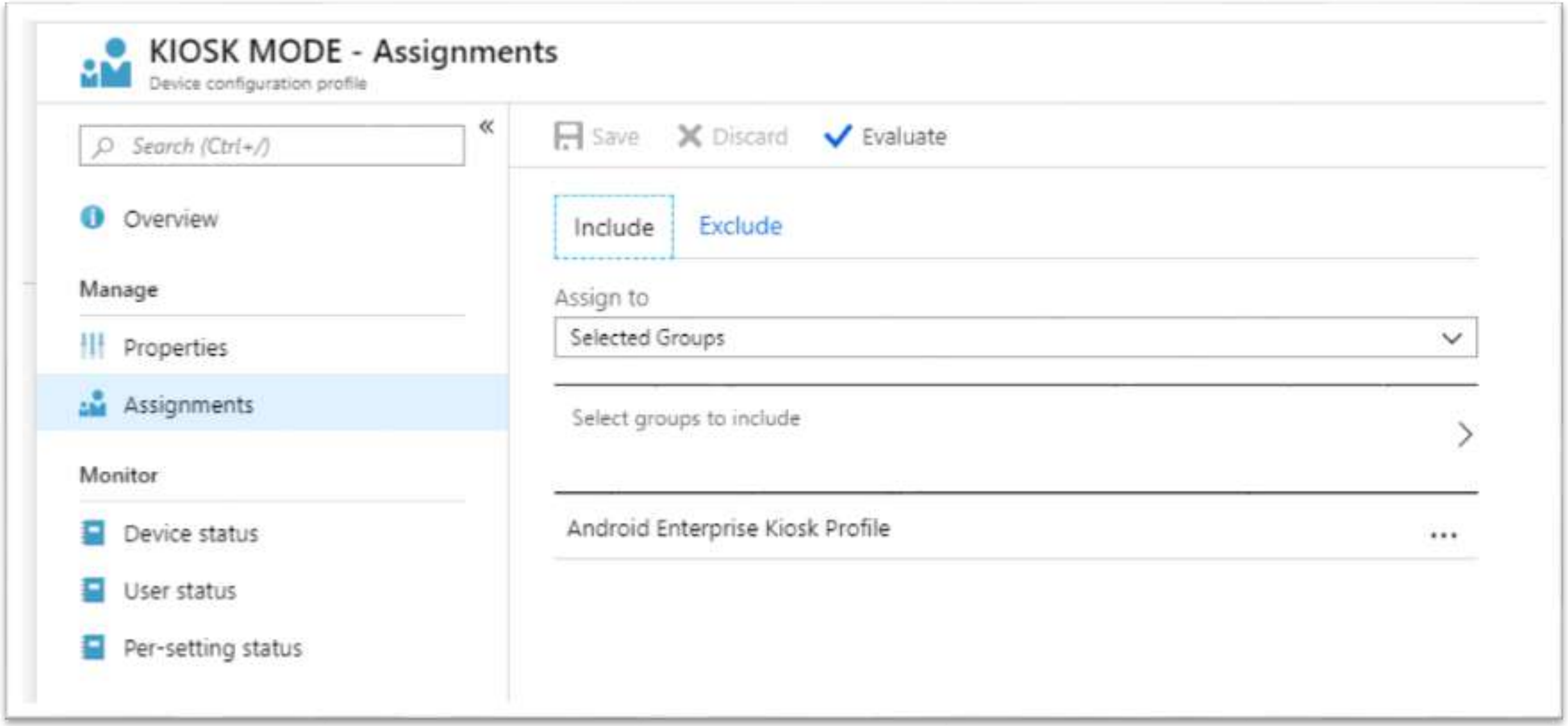
Bluetooth configuration: Enable / Not configured

Screen saver mode: Enable / Not configured

Set custom screen saver image: http://www.contoso.com/img...

Android Enterprise: Corporate Owned Dedicated Device

- Go to Intune > Device Configuration > Profiles.
- Select the Kiosk mode profile
- Assign the Azure AD group created earlier.



KIOSK MODE - Assignments

Device configuration profile

Assign to: Selected Groups

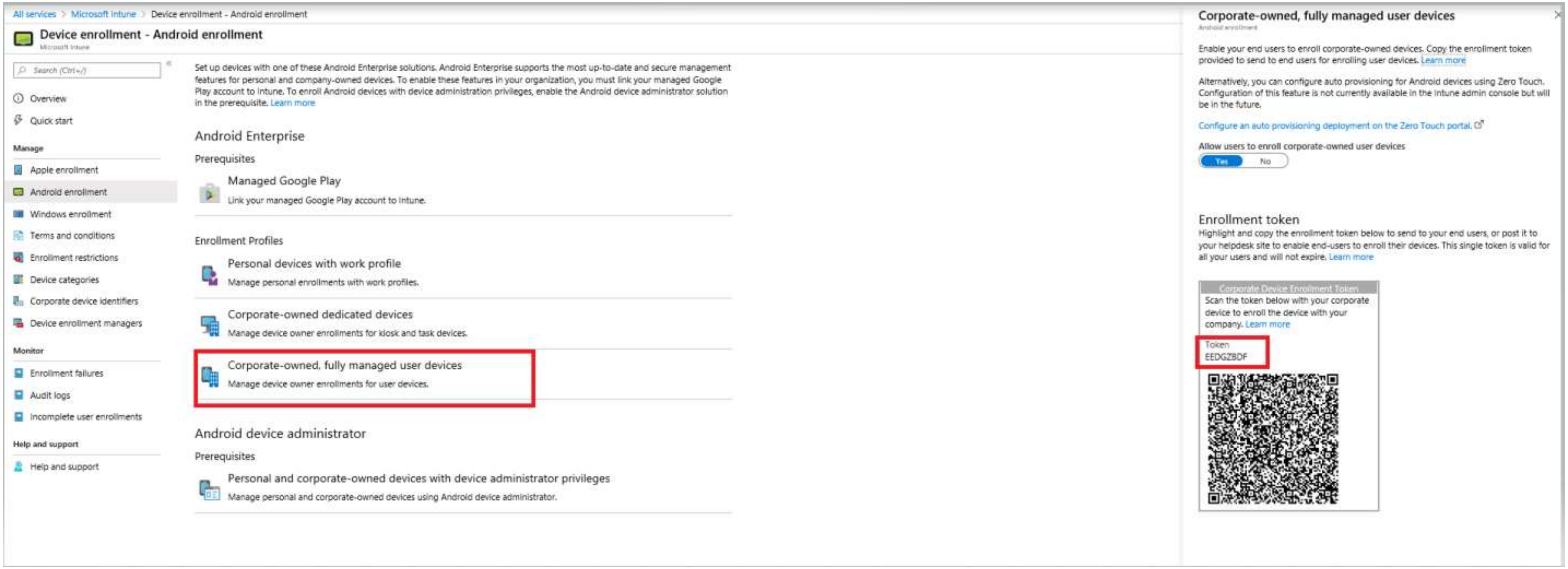
Select groups to include

Android Enterprise Kiosk Profile

Android Enterprise: Corporate Owned, fully managed user devices

-First create the enrollment profile. Do this by going to **Microsoft Intune > Device enrollment > Android enrollment** and click **Corporate-owned, fully managed user devices**

- You will then see an Enrolment Token appear on the right hand blade. Take note of this token as it will be required for enrolment using the methods later in this document.



All services > Microsoft Intune > Device enrollment - Android enrollment

Device enrollment - Android enrollment
Microsoft Intune

Search (Ctrl+/)

Overview
Quick start

Manage
- Apple enrollment
- Android enrollment
- Windows enrollment
- Terms and conditions
- Enrollment restrictions
- Device categories
- Corporate device identifiers
- Device enrollment managers

Monitor
- Enrollment failures
- Audit logs
- Incomplete user enrollments

Help and support
- Help and support

Set up devices with one of these Android Enterprise solutions. Android Enterprise supports the most up-to-date and secure management features for personal and company-owned devices. To enable these features in your organization, you must link your managed Google Play account to Intune. To enroll Android devices with device administration privileges, enable the Android device administrator solution in the prerequisite. Learn more

Android Enterprise

Prerequisites

Managed Google Play
Link your managed Google Play account to Intune.

Enrollment Profiles

Personal devices with work profile
Manage personal enrollments with work profiles.

Corporate-owned dedicated devices
Manage device owner enrollments for kiosk and task devices.

Corporate-owned, fully managed user devices
Manage device owner enrollments for user devices.

Android device administrator

Prerequisites

Personal and corporate-owned devices with device administrator privileges
Manage personal and corporate-owned devices using Android device administrator.

Corporate-owned, fully managed user devices
Android enrollment

Enable your end users to enroll corporate-owned devices. Copy the enrollment token provided to send to end users for enrolling user devices. Learn more

Alternatively, you can configure auto provisioning for Android devices using Zero Touch. Configuration of this feature is not currently available in the Intune admin console but will be in the future.

Configure an auto provisioning deployment on the Zero Touch portal.

Allow users to enroll corporate-owned user devices
[✓ Yes] No

Enrollment token
Highlight and copy the enrollment token below to send to your end users, or post it to your helpdesk site to enable end-users to enroll their devices. This single token is valid for all your users and will not expire. Learn more

Corporate Device Enrollment Token
Scan the token below with your corporate device to enroll the device with your company. Learn more

Token
EEDGZBDF

Android Enterprise: Corporate Owned device enrolment

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 Intune as an Android Enterprise Company-owned device.

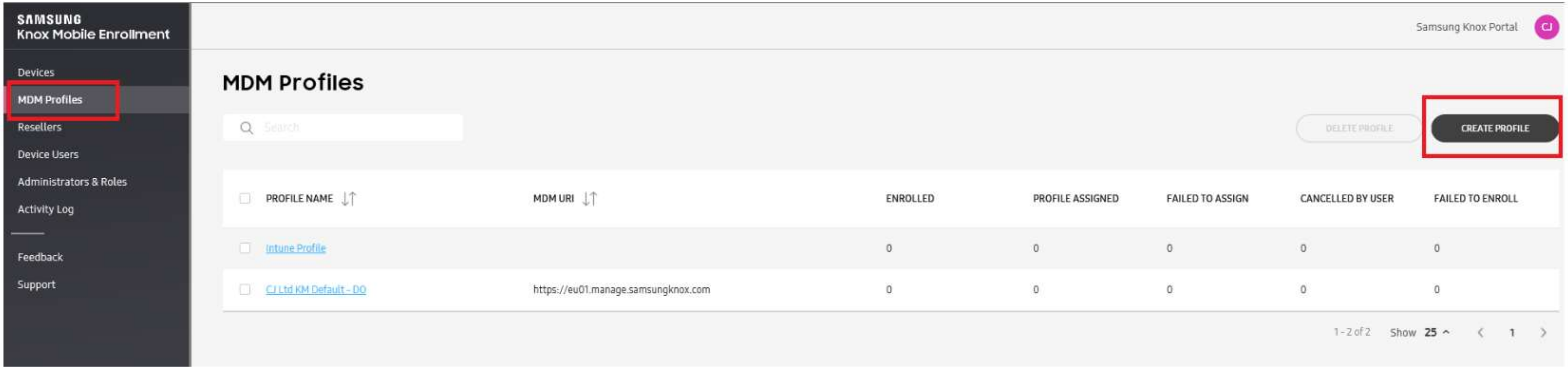
1. DPC Identifier [Also known as the hashtag method] **afw#setup**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

The following slides will take you through the KME enrollment process.

Android Enterprise: Corporate Owned device enrolment

KME Enrollment

- To automate with KME, log into the KME console via https://www.samsungknox.com/ and select MDM Profiles.
- Then select “Create Profile”

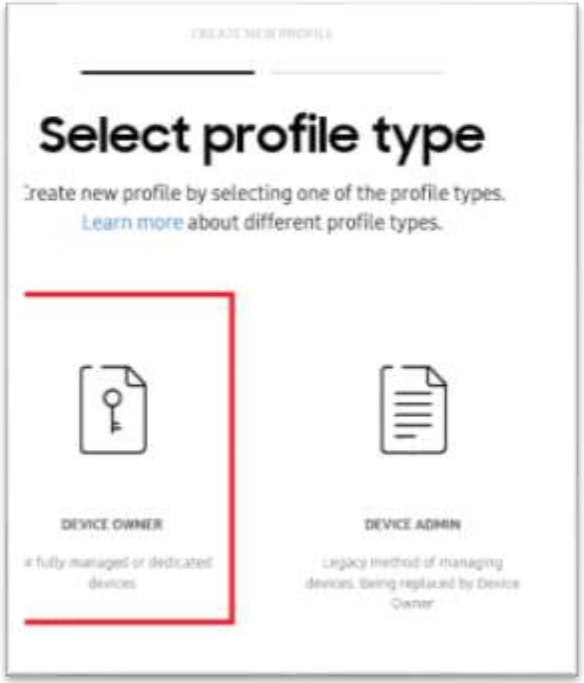


PROFILE NAME	MDM URI	ENROLLED	PROFILE ASSIGNED	FAILED TO ASSIGN	CANCELLED BY USER	FAILED TO ENROLL
Intune Profile		0	0	0	0	0
CJ Ltd KM Default - DO	https://eu01.manage.samsungknox.com	0	0	0	0	0

Android Enterprise: Corporate Owned device enrolment

KME Enrollment

- Give the profile a name and pick “Microsoft Intune” as the MDM
- Enter “https://aka.ms/intunekme_deviceowner” as the MDM Agent APK
- Click Continue



CREATE NEW PROFILE

Select profile type

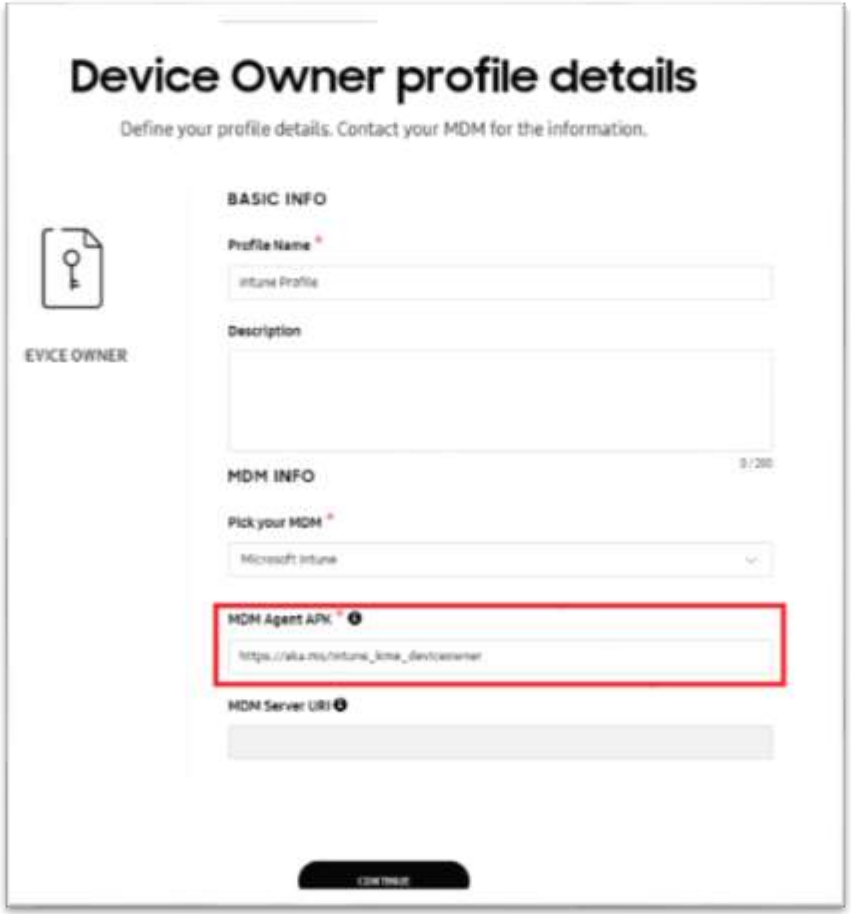
:reate new profile by selecting one of the profile types.
Learn more about different profile types.

DEVICE OWNER

r fully managed or dedicated devices

DEVICE ADMIN

Legacy method of managing devices. Being replaced by Device Owner



Device Owner profile details

Define your profile details. Contact your MDM for the information.

EVICE OWNER

BASIC INFO

Profile Name *: Intune Profile

Description

0 / 200

MDM INFO

Pick your MDM *: Microsoft Intune

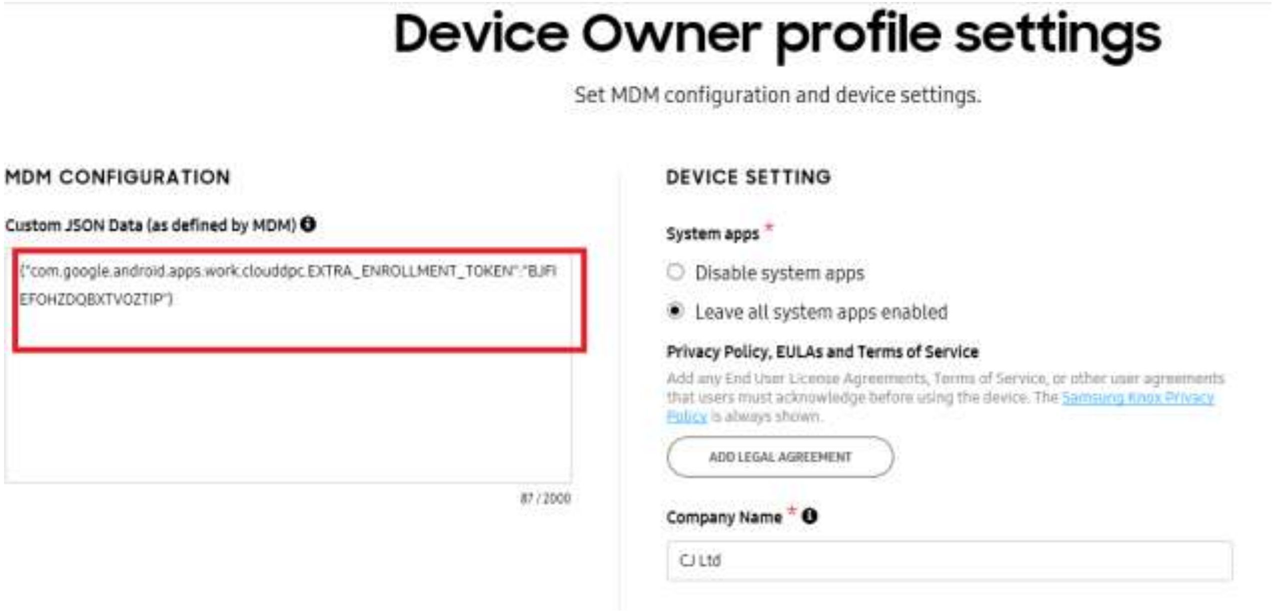
MDM Agent APK *: https://aka.ms/intune_kme_deviceowner

MDM Server URI

Android Enterprise: Corporate Owned device enrolment

KME Enrollment

- Enter {"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"YOUR TOKEN"} in the JSON box.
- Your token will be found in your enrollment profile in the Intune console.



Device Owner profile settings

Set MDM configuration and device settings.

MDM CONFIGURATION

Custom JSON Data (as defined by MDM)

{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"BJFIEFOHZDQBXTVOZTIP"}

87 / 2000

DEVICE SETTING

System apps *

○ Disable system apps

● Leave all system apps enabled

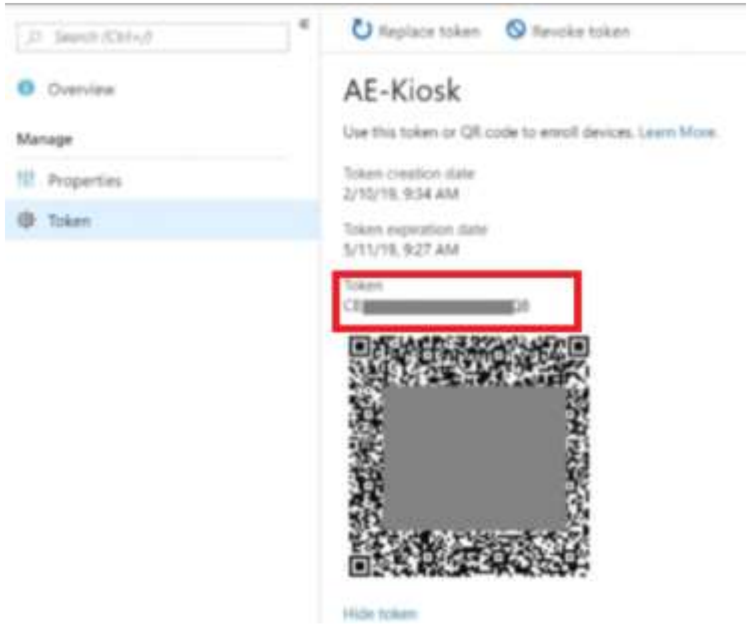
Privacy Policy, EULAs and Terms of Service

Add any End User License Agreements, Terms of Service, or other user agreements that users must acknowledge before using the device. The Samsung Knox Privacy Policy is always shown.

ADD LEGAL AGREEMENT

Company Name *

CJ Ltd



Search (Ctrl+/)

Overview

Manage

Properties

Token

Replace token

Revoke token

AE-Kiosk

Use this token or QR code to enroll devices. Learn More.

Token creation date
2/10/18, 9:34 AM

Token expiration date
5/11/18, 9:27 AM

Token
[redacted]

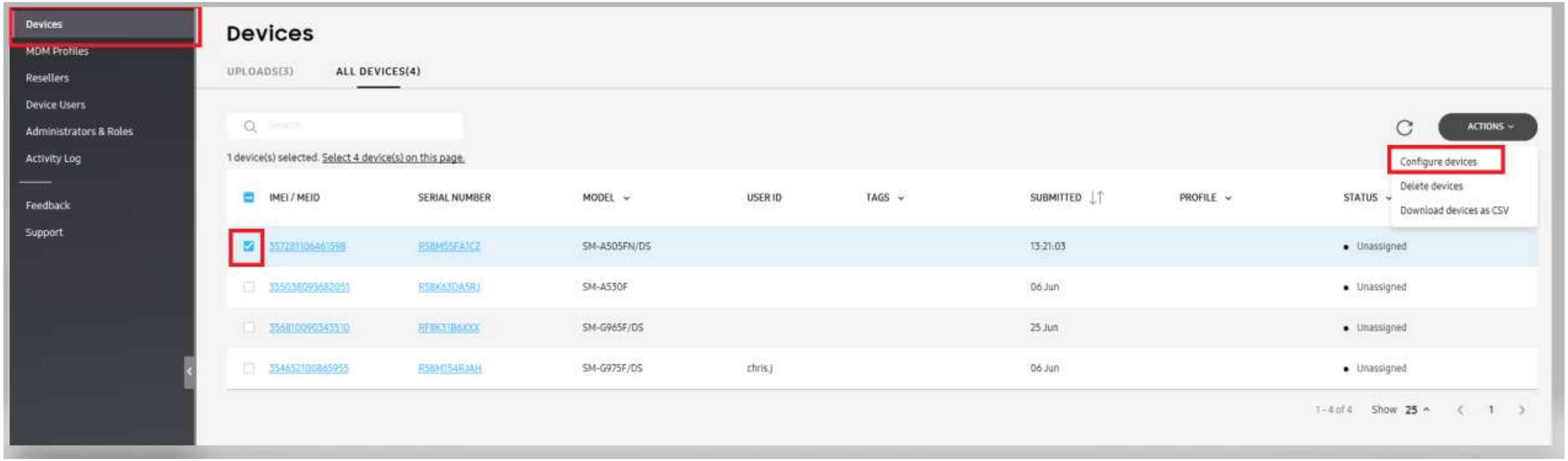
[redacted]

Hide token

Android Enterprise: Corporate Owned Dedicated Device

KME Enrollment

- Next go to Devices in KME and select the device(s) you want to assign the Intune profile to.
- Select Actions drop down and select “Configure devices”



Devices

1 device(s) selected. Select 4 device(s) on this page.

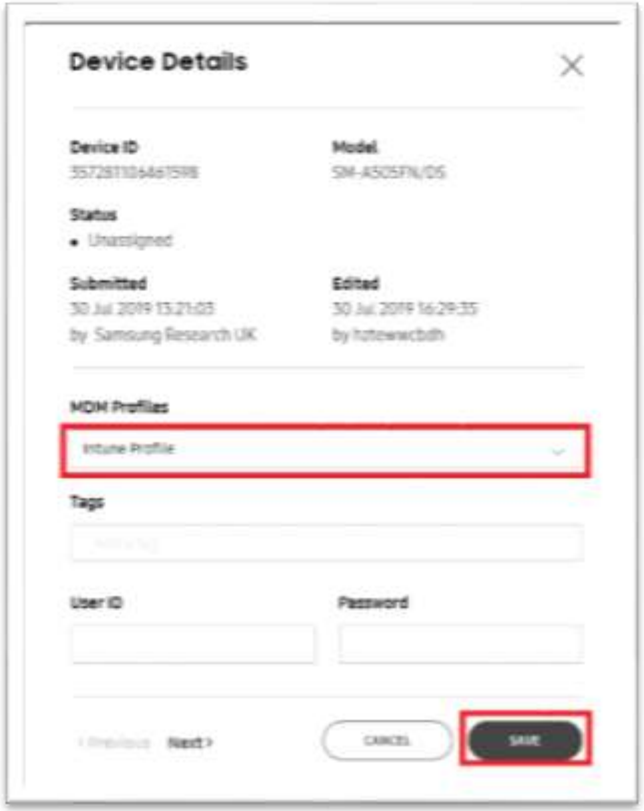
	IMEI / MEID	SERIAL NUMBER	MODEL	USER ID	TAGS	SUBMITTED	PROFILE	STATUS
☑	357281106461598	R58M55FA1CZ	SM-A505FN/DS			13:21:03		● Unassigned
□	355038095682051	R58K63DA5RJ	SM-A530F			06 Jun		● Unassigned
□	356810090343510	RF8K31B6KXX	SM-G965F/DS			25 Jun		● Unassigned
□	354652100865955	R58M154RJAH	SM-G975F/DS	chris.j		06 Jun		● Unassigned

1 - 4 of 4 Show 25 ‹ 1 ›

Android Enterprise: Corporate Owned Dedicated Device

KME Enrollment

- Select the Intune profile you created and press Save.
- You will see “Profile assigned” as the status on the following screen.



Device Details

Device ID
357281106461598

Model
SM-A505FN/DS

Status
● Unassigned

Submitted
30 Jul 2019 13:21:03
by Samsung Research UK

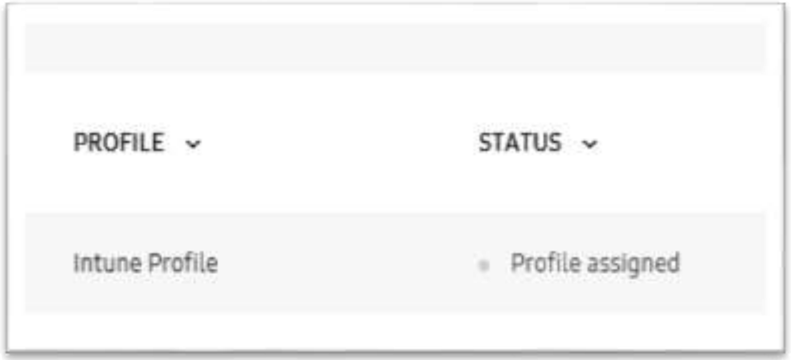
Edited
30 Jul 2019 16:29:35
by hztewecbdh

MDM Profiles
Intune Profile

Tags

User ID

Password

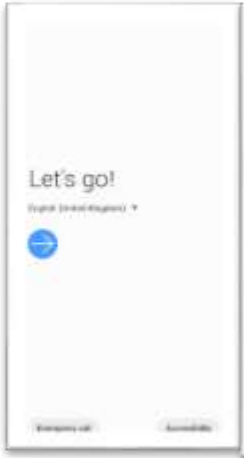


PROFILE	STATUS
Intune Profile	● Profile assigned

Android Enterprise: Dedicated Device

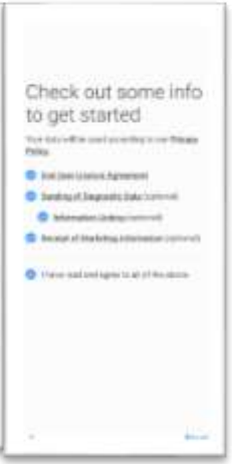
KME Enrollment – Device Config

- See the steps required below on the device to complete successful enrollment.



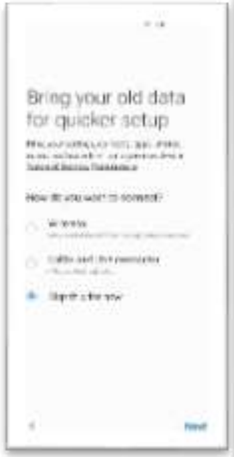
Let's go!

Click Start arrow



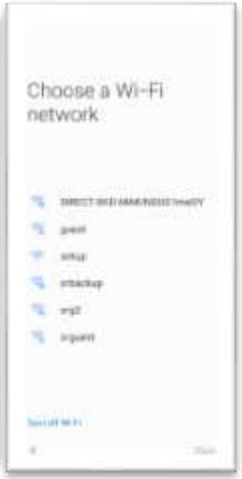
Check out some info to get started

Accept T's & C's



Bring your old data for quicker setup

Skip Backup

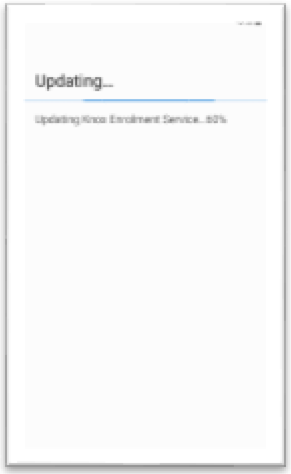


Choose a Wi-Fi network

guest

setup

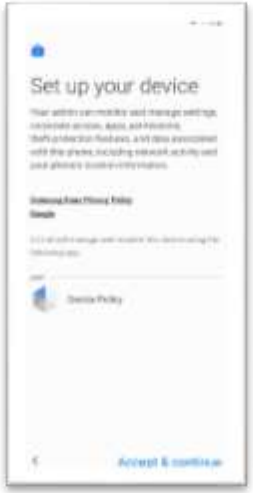
Connect Wi-Fi or Cellular



Updating...

Updating Knox Enrollment Service...60%

KME Detection

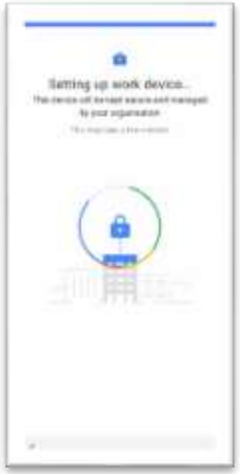


Set up your device

Device Policy

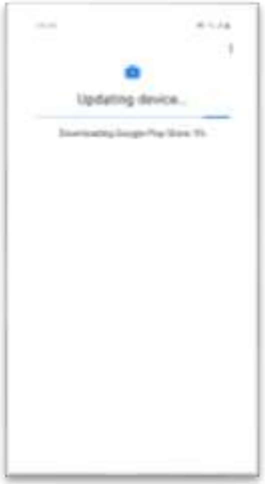
Accept & continue

Accept and Continue



Setting up work device...

Setup Device



Updating device...

Apply Policies

14 16

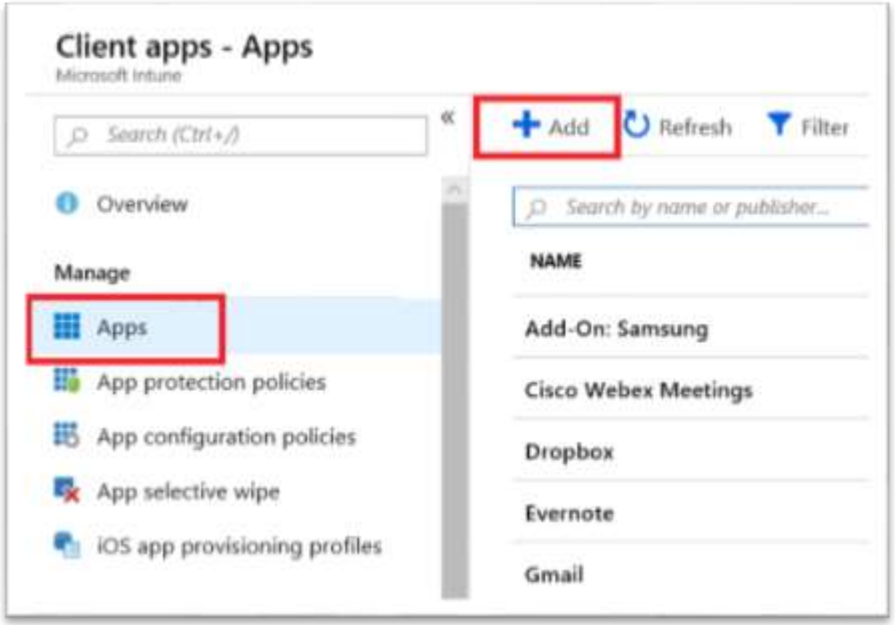
Tue 30 July

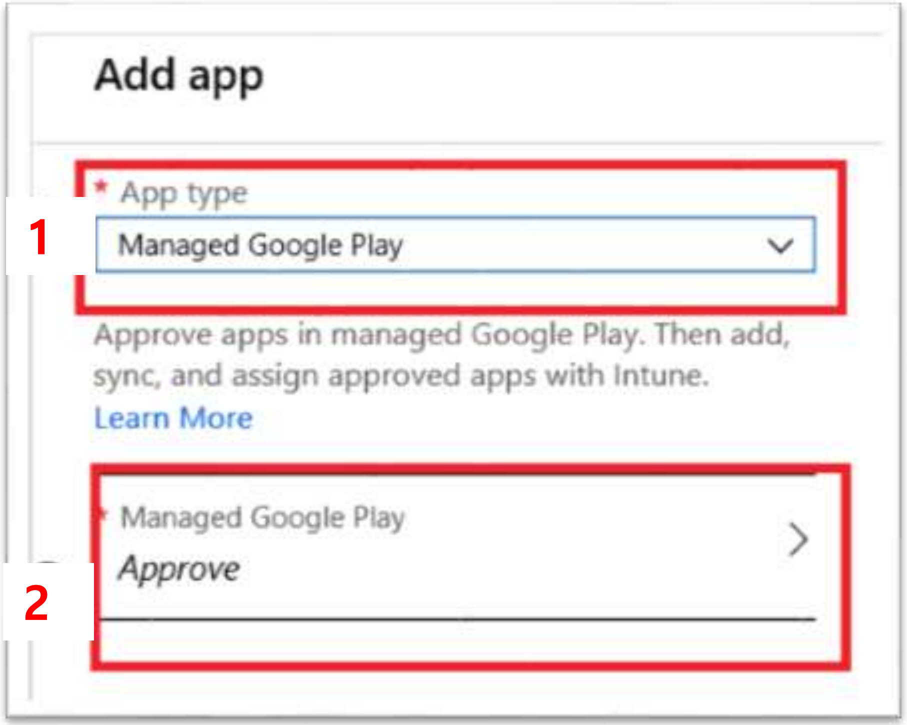
Device Enrollment Successful

Knox Service Plugin (KSP)

The Knox Service Plugin (KSP) is a solution that enables Enterprise Customers – through the use of their chosen UEM Partners – to deploy existing and new Knox features as soon as they are commercially available.

- First you will need to go to the Client apps section, select Apps and then click Add.
- Then choose the App type as “Managed Google Play” from the first drop down menu
- Click on “Approve” under the Managed Google Play sub section.




Add app

1

* App type

Managed Google Play

Approve apps in managed Google Play. Then add, sync, and assign approved apps with Intune.

Learn More

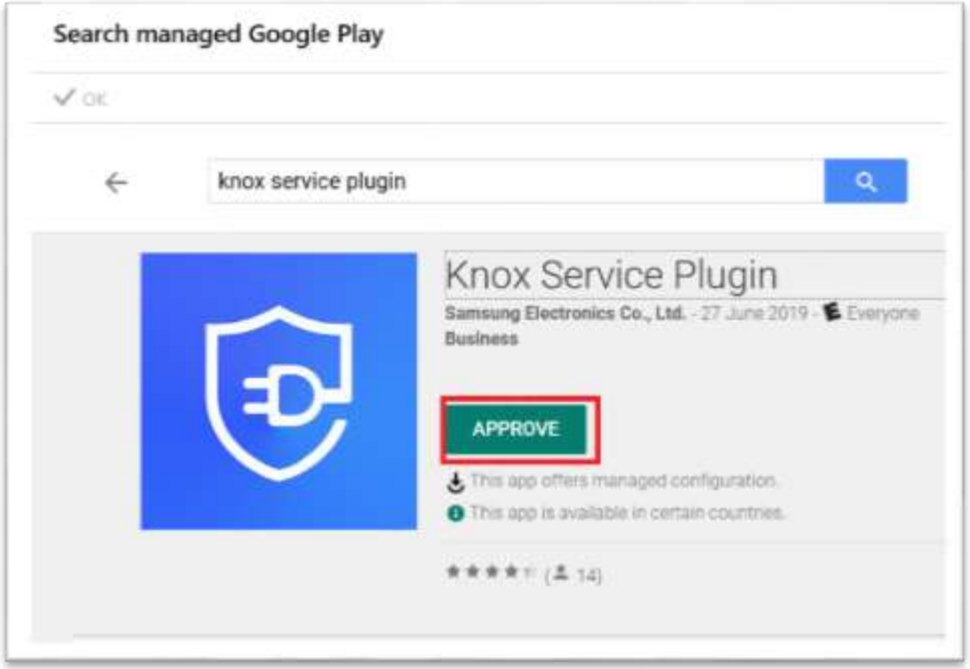
2

* Managed Google Play

Approve

Knox Service Plugin (KSP)

- Search for the “Knox service plugin” in the Search managed Google Play window
- Once found click on the app and choose Approve
- Approve the KSP permissions that are prompted on the next page



Search managed Google Play

✓ OK

knox service plugin

Knox Service Plugin

Samsung Electronics Co., Ltd. - 27 June 2019 - Everyone

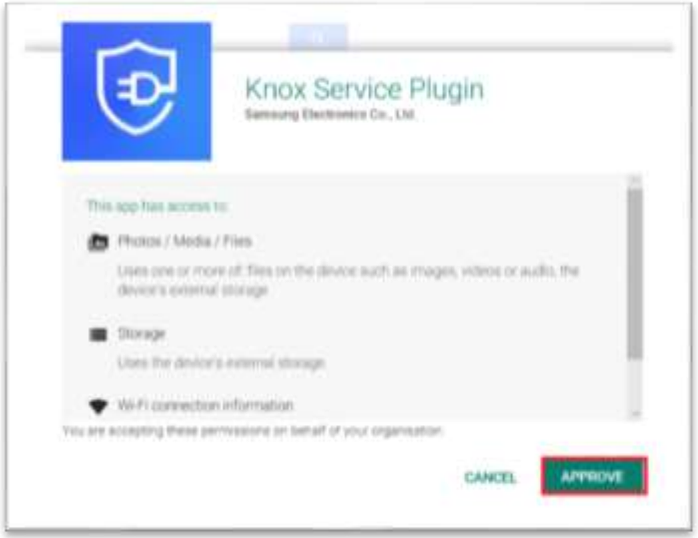
Business

APPROVE

This app offers managed configuration.

This app is available in certain countries.

★★★★☆ (14)



Knox Service Plugin

Samsung Electronics Co., Ltd.

This app has access to:

Photos / Media / Files

Uses one or more of: files on the device such as images, videos or audio, the device's external storage

Storage

Uses the device's external storage

Wi-Fi connection information

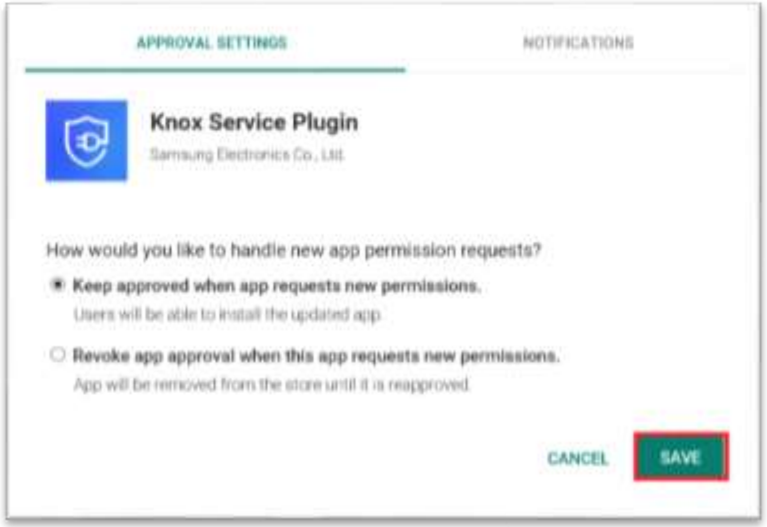
You are accepting these permissions on behalf of your organisation.

CANCEL

APPROVE

Knox Service Plugin (KSP)

- Ensure the *"Keep approved when app requests new permissions"* selected and then select save.
- When you are taken back to the "Search managed Google Play" window select the OK button shown below.



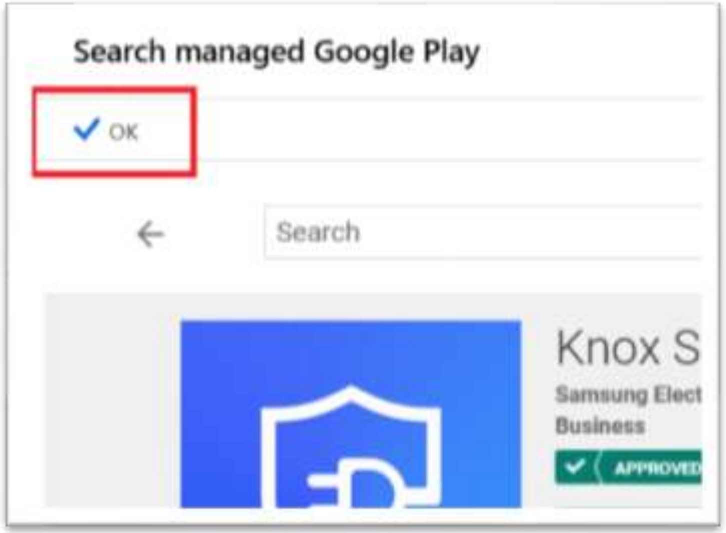
Knox Service Plugin

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

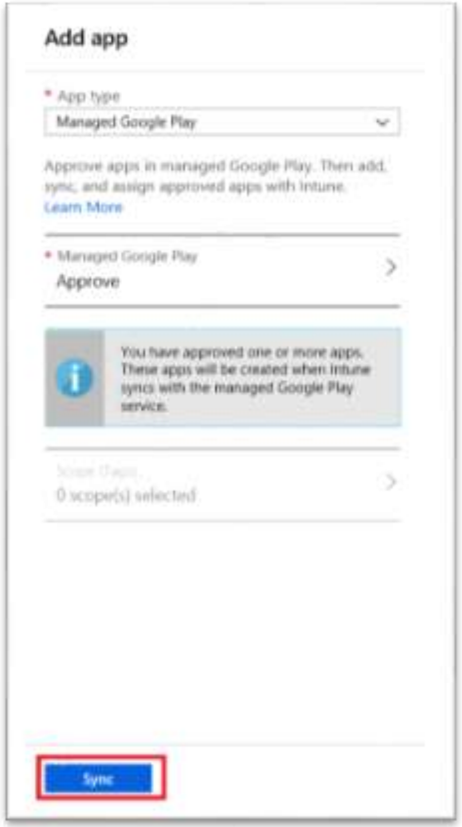
○ **Revoke app approval when this app requests new permissions.**
App will be removed from the store until it is reapproved.



Search managed Google Play

Knox Service Plugin (KSP)

- Click the Sync button to ensure that the apps that have been recently approved appear in the Managed Google Play apps.
- Then go back to the apps list to ensure that the Knox Service Plugin is listed.



Add app

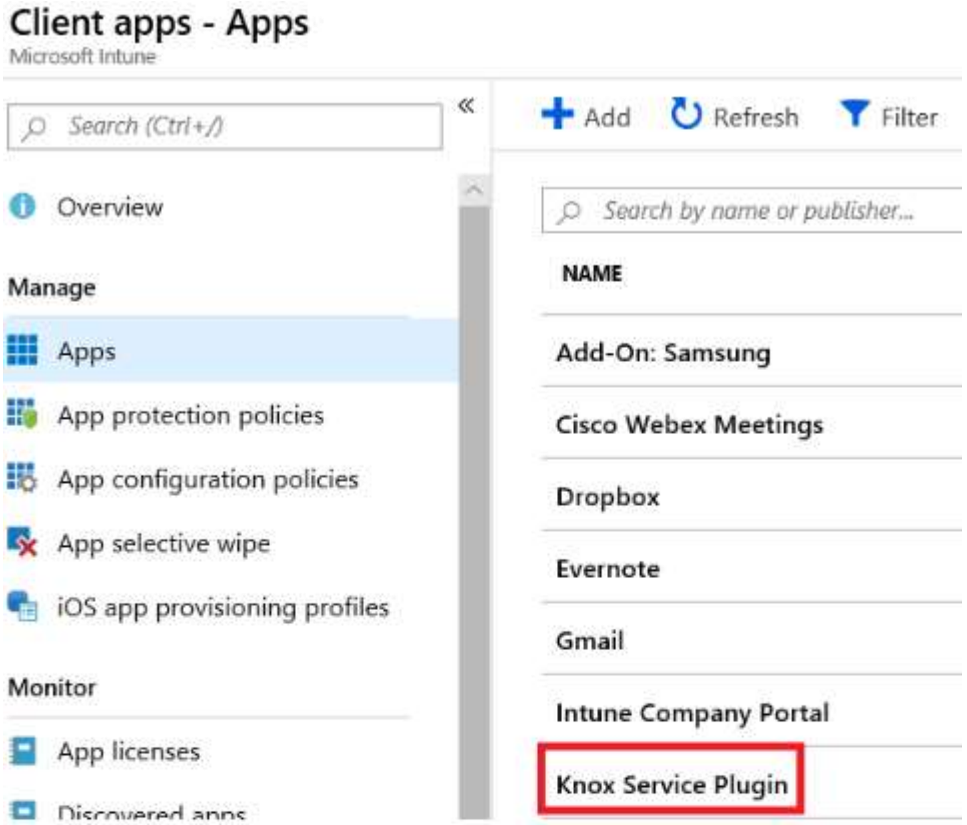
* App type: Managed Google Play

Approve apps in managed Google Play. Then add, sync, and assign approved apps with Intune. Learn More

* Managed Google Play: Approve

You have approved one or more apps. These apps will be created when Intune syncs with the managed Google Play service.

Scope (Tags): 0 scope(s) selected



Client apps - Apps

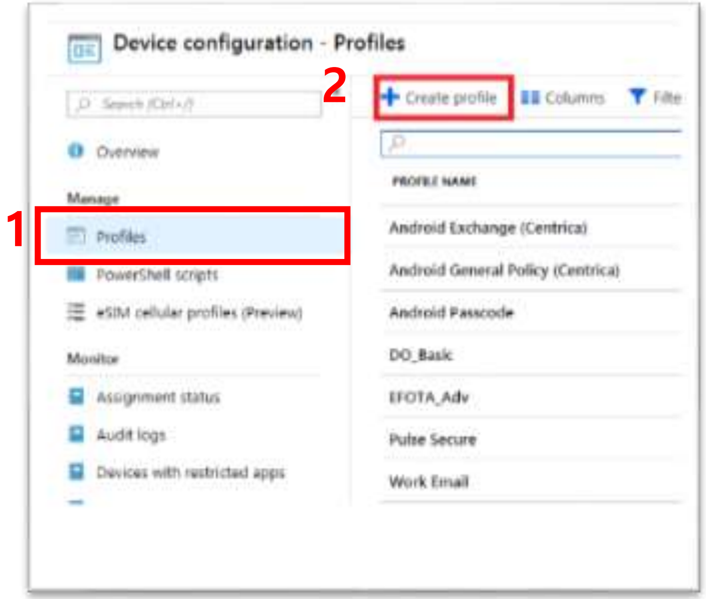
Microsoft Intune

NAME
Add-On: Samsung
Cisco Webex Meetings
Dropbox
Evernote
Gmail
Intune Company Portal
Knox Service Plugin

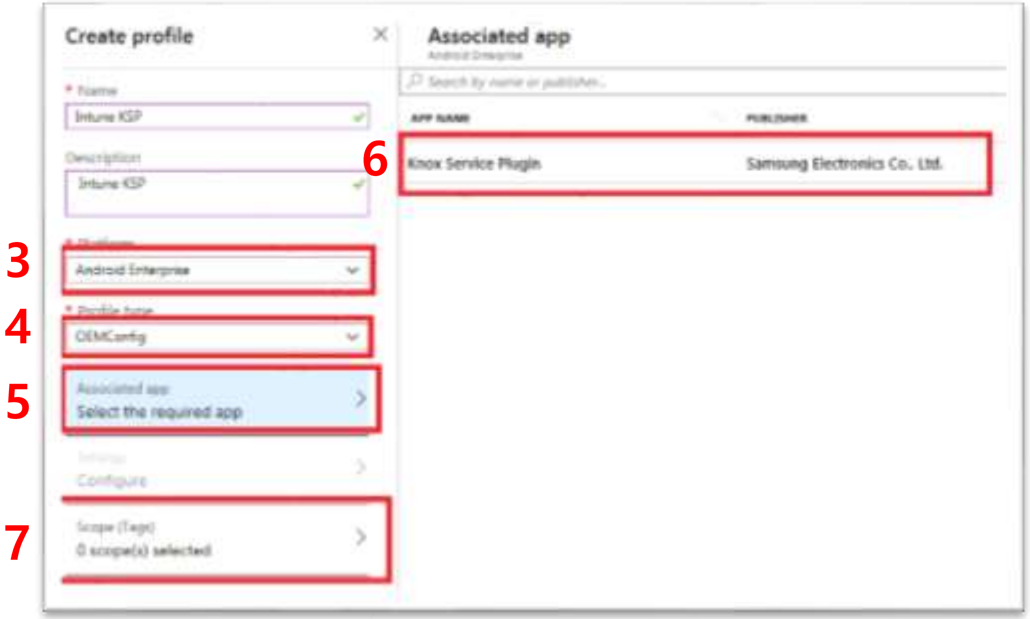
Knox Service Plugin (KSP)

Create an OEMConfig profile

1. Go to Device Configuration then choose “Profiles” under the Manage section.
2. Click the “Create profile” button
3. Give the profile a name and Choose Android Enterprise as the platform
4. Profile type is OEMConfig
5. Click Associated app
6. Then choose the Knox Service Plugin.
7. Optional – Choose whether to scope this profile to a subset of users/devices.



PROFILE NAME
Android Exchange (Centrica)
Android General Policy (Centrica)
Android Passcode
DO_Basic
EFOTA_Adv
Pulse Secure
Work Email



* Name: Intune KSP

Description: Intune KSP

* Platform: Android Enterprise

* Profile type: OEMConfig

Associated app: Select the required app

Settings: Configure

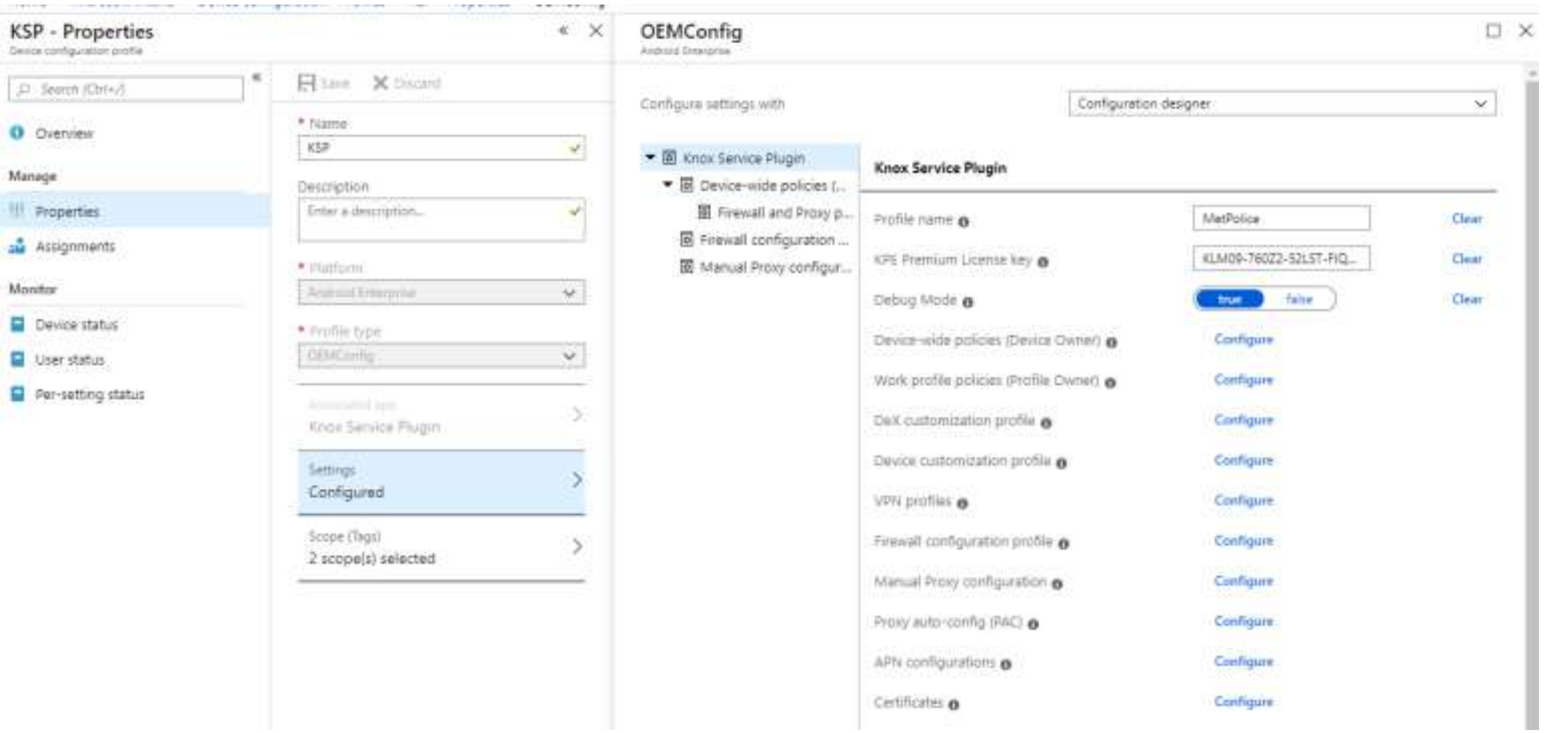
Scope (Tags): 0 scope(s) selected

APP NAME	PUBLISHER
Knox Service Plugin	Samsung Electronics Co., Ltd.

Knox Service Plugin (KSP)

Create an OEMConfig profile - Configuration designer

- Choose the Configure option under settings to display the Configuration designer.
- You can see all of the settings available to you via this view and change accordingly. If you want to use the JSON file editor to assign the configuration then this is also an option.



KSP - Properties
Device configuration profile

* Name: KSP
Description: Enter a description...
* Platform: Android Enterprise
* Profile type: OEMConfig
Associated app: Knox Service Plugin
Settings: Configured
Scope (Tags): 2 scope(s) selected

OEMConfig
Android Enterprise

Configure settings with: Configuration designer

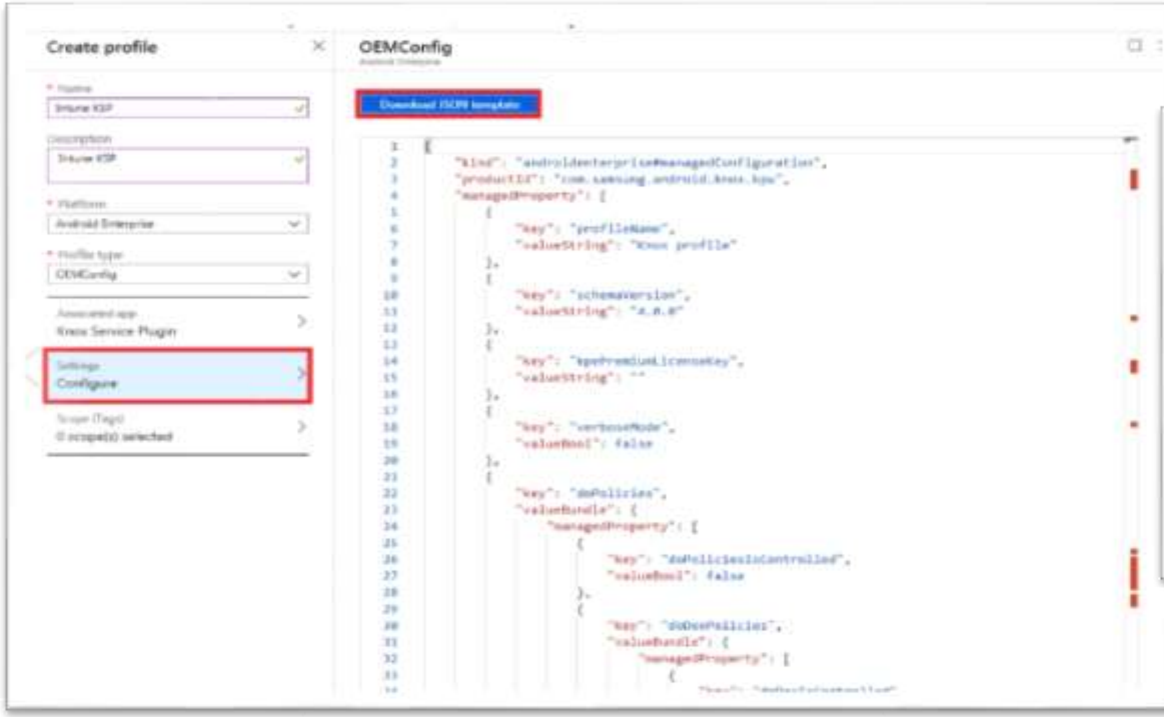
Knox Service Plugin

Profile name: MetPolice
KPE Premium License key: KLM09-760Z2-52LST-FIQ...
Debug Mode: true

Knox Service Plugin (KSP)

Create an OEMConfig profile – JSON Editor

- Choose the Configure option under settings to display the JSON file.
- You can choose to download the file and edit using a text editor or save as it is.
- Click OK once you have finished and then click Create



* Name: Intune KSP

Description: Intune KSP

* Platform: Android Enterprise

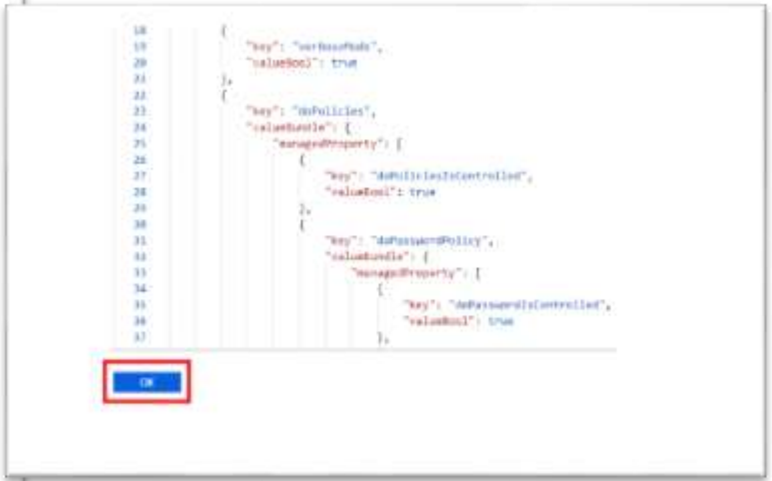
* Profile type: OEMConfig

Associated app: Knox Service Plugin

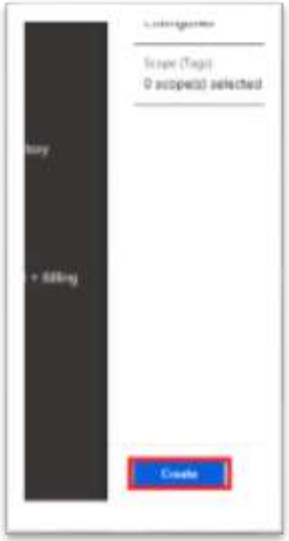
Settings: Configure

Scope (Tags): 0 scope(s) selected

```
{
    "kind": "androidenterprise#managedConfiguration",
    "productId": "com.samsung.android.knox.kpu",
    "managedProperty": [
        {
            "key": "profileName",
            "valueString": "Knox profile"
        },
        {
            "key": "schemaVersion",
            "valueString": "x.0.0"
        },
        {
            "key": "kpePremiumLicenseKey",
            "valueString": ""
        },
        {
            "key": "verboseMode",
            "valueBool": false
        },
        {
            "key": "doPolicies",
            "valueBundle": {
                "managedProperty": [
                    {
                        "key": "doPoliciesIsControlled",
                        "valueBool": false
                    },
                    {
                        "key": "doDexPolicies",
                        "valueBundle": {
                            "managedProperty": [
                                {
```



```
        {
            "key": "verboseMode",
            "valueBool": true
        },
        {
            "key": "doPolicies",
            "valueBundle": {
                "managedProperty": [
                    {
                        "key": "doPoliciesIsControlled",
                        "valueBool": true
                    },
                    {
                        "key": "doPasswordPolicy",
                        "valueBundle": {
                            "managedProperty": [
                                {
                                    "key": "doPasswordIsControlled",
                                    "valueBool": true
                                },
```

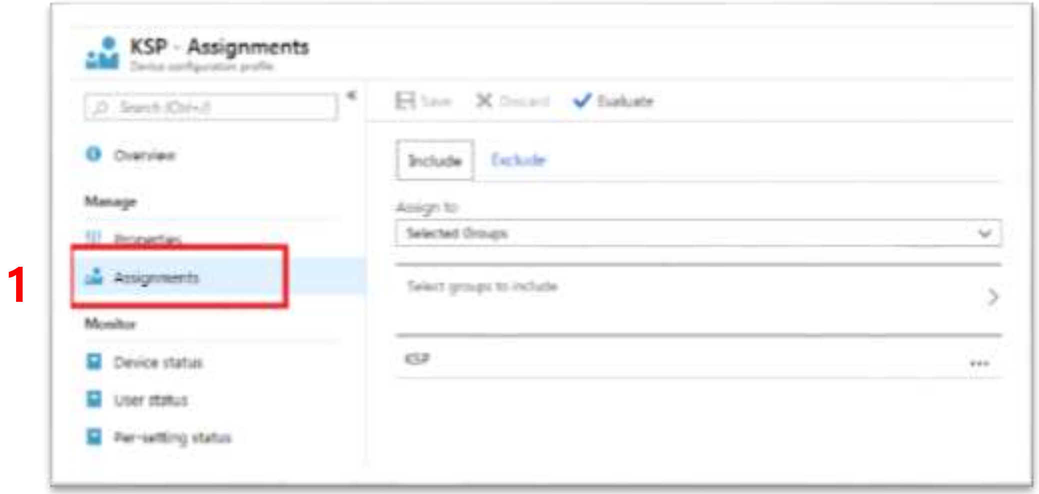


Scope (Tags): 0 scope(s) selected

Knox Service Plugin (KSP)

Create an OEMConfig profile

1. Next assign the profile by going to Assignments
2. Then you can choose to assign to all devices, users or selected groups.



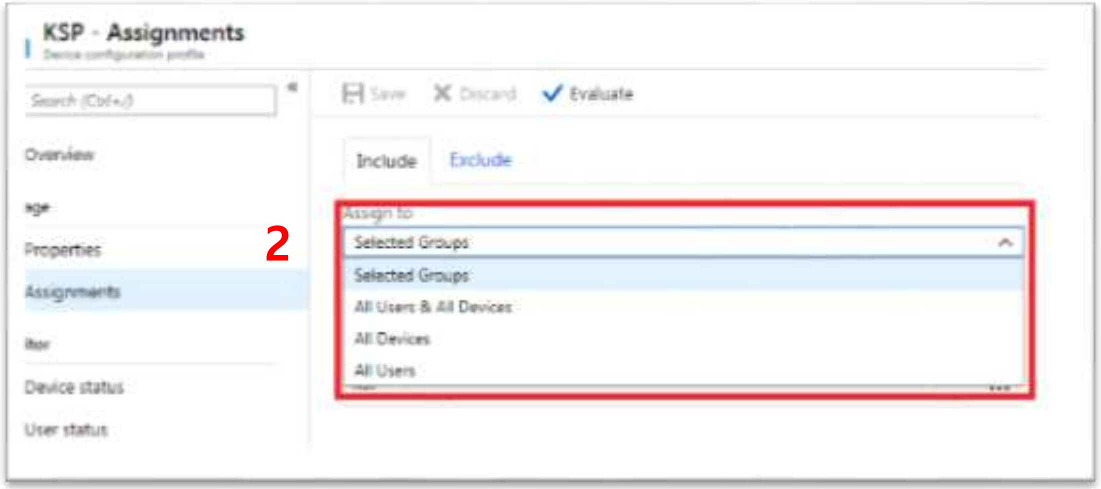
1

KSP - Assignments

Device configuration profile

Assign to: Selected Groups

KSP



2

KSP - Assignments

Device configuration profile

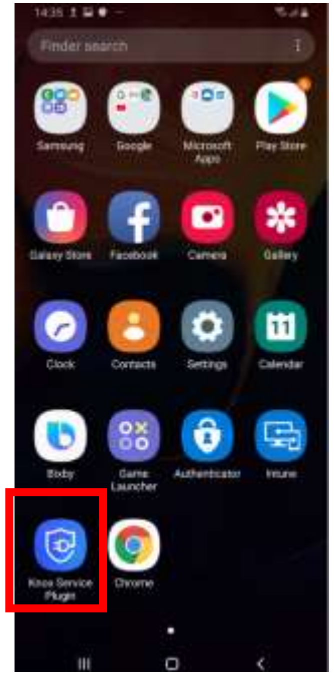
Assign to: Selected Groups

- Selected Groups
- All Users & All Devices
- All Devices
- All Users

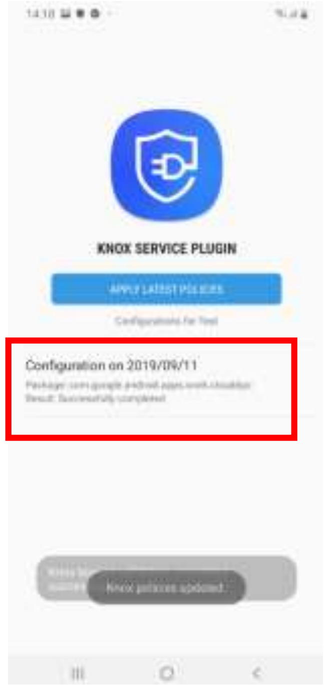
Knox Service Plugin (KSP)

Deploy on device

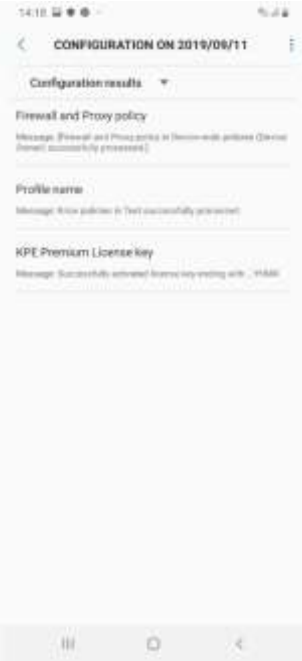
The KSP app will now install on the device and download the assigned configuration. See the screenshots below on what you can expect to see.



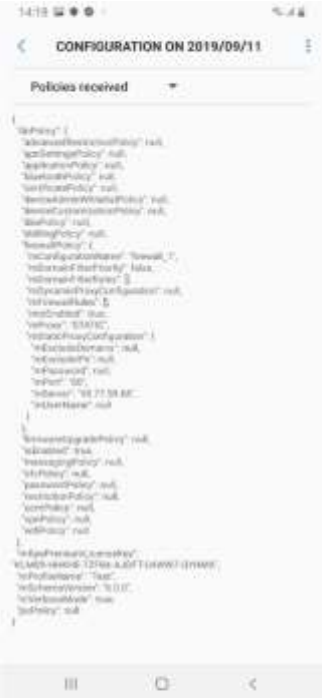
Open the KSP app



Click on Configuration



Check configuration results



Check policies received